KKIK - FSRD

Jurnal Sosioteknologi

Website: https://journals.itb.ac.id/index.php/sostek/index

Evaluating Security Challenges in Digital Access Systems for Technology-Enabled Vocational Education: A Systematic Literature Review

Mengevaluasi Tantangan Keamanan dalam Sistem Akses Digital untuk Pendidikan Kejuruan yang Didukung Teknologi: Tinjauan Literatur Sistematis

Kennedy B. Y. Agyeibi, Budi Mulyanti, Agus Setiawan, Lala Septem Riza, Ilhamdaniah

Universitas Pendidikan Indonesia, Bandung, Indonesia

k.agyeibi@upi.edu

https://doi.org/10.5614/sostek.itbj.2026.25.2.3
Submitted: February 7, 2026 Accepted: June 2, 2026 Published: July 31, 2026

ARTICLE INFO

Keywords:
digital access security, vocational education, learning continuity, socio-technical systems, cybersecurity governance

ABSTRACT

The rapid expansion of technology-enabled vocational education has increased reliance on digital access systems that regulate entry to learning platforms, simulations, and assessment environments. This study examines how security challenges in these systems affect learning continuity in vocational education and identifies factors that intensify disruption risks. A systematic review of peer-reviewed studies published between 2020 and 2025 was conducted using five academic databases, applying predefined inclusion criteria and synthesizing findings through descriptive and thematic analysis. Results show that weaknesses in data confidentiality, integrity, and especially system availability frequently interrupt instructional activities, particularly practice-based learning dependent on digital laboratories and assessment tools. Disruptions are often amplified by misalignment between technical infrastructure, user practices, and institutional governance, with institutions lacking governance capacity and user training facing higher risks of learning interruption. Although technical and administrative mitigation strategies exist, they are often implemented without sufficient alignment to pedagogical needs. The study concludes that digital access security should be treated not merely as a technical concern but as a prerequisite for equitable and resilient vocational learning, calling for integrated socio-technical and pedagogically informed security strategies.

INFO ARTIKEL

Kata kunci:
keamanan akses digital, pendidikan kejuruan, kesinambungan pembelajaran, sistem sosio-teknis, tata kelola keamanan siber

ABSTRAK

Ekspansi pesat pendidikan kejuruan yang didukung teknologi telah meningkatkan ketergantungan pada sistem akses digital yang mengatur akses ke platform pembelajaran, simulasi, dan lingkungan penilaian. Studi ini mengkaji bagaimana tantangan keamanan dalam sistem ini memengaruhi kelangsungan pembelajaran dalam pendidikan vokasi dan mengidentifikasi faktor-faktor yang mengintensifkan risiko gangguan. Tinjauan sistematis studi peer-reviewed *yang diterbitkan antara tahun 2020 dan 2025 dilakukan menggunakan lima database akademik, menerapkan kriteria inklusi yang telah ditentukan sebelumnya dan mensintesis temuan melalui analisis deskriptif*

dan tematik. Hasil penelitian menunjukkan bahwa kelemahan dalam kerahasiaan data, integritas, dan terutama ketersediaan sistem sering mengganggu kegiatan instruksional, terutama pembelajaran berbasis praktik yang bergantung pada laboratorium digital dan alat penilaian. Gangguan sering diperkuat oleh ketidakselarasan antara infrastruktur teknis, praktik pengguna, dan tata kelola kelembagaan, dengan institusi yang tidak memiliki kapasitas tata kelola dan pelatihan pengguna menghadapi risiko gangguan pembelajaran yang lebih tinggi. Meskipun ada strategi mitigasi teknis dan administratif, strategi ini sering diterapkan tanpa penyelarasan yang memadai dengan kebutuhan pedagogis. Studi ini menyimpulkan bahwa keamanan akses digital harus diperlakukan tidak hanya sebagai masalah teknis, tetapi juga sebagai prasyarat untuk pembelajaran kejuruan yang adil dan tangguh. Hal ini memerlukan strategi keamanan yang terintegrasi secara sosial-teknis dan pedagogis.

Introduction

Digital transformation has reshaped vocational education and training (VET), extending learning beyond physical workshops into hybrid and cloud-based environments that depend on continuous digital access (Eisenbart, 2023; Hernández-Serrano et al., 2025; Pittich & Tenberg, 2020). Learning management systems, single sign-on (SSO) infrastructures, biometric authentication, and smart access controls now mediate access to simulations, assessments, and competency-based training activities (Ahmed et al., 2024; Coverdale et al., 2024; Fecke et al., 2022). In vocational education, where learning relies heavily on timely hands-on practice and continuous competency development aligned with workforce readiness objectives, access systems function not merely as administrative tools but as core pedagogical infrastructures (ILO, 2024).

Early VET digitalization research primarily emphasized platform adoption and online resource integration, while cybersecurity remained a secondary technical concern (Pittich & Tenberg, 2020). Following the COVID-19 pandemic, however, vocational institutions became increasingly dependent on cloud-based learning systems, remote simulations, and digital assessment environments, expanding exposure to authentication failures, ransomware attacks, and access disruptions (Eisenbart, 2023; Hernández-Serrano et al., 2025). Consequently, cybersecurity has shifted from an operational IT issue to a critical factor influencing instructional continuity and assessment reliability in technology-enabled vocational education (Mahmood et al., 2024).

This dependence has introduced vulnerabilities with direct pedagogical consequences. Security breaches and access failures can interrupt practical sessions, invalidate assessments, and weaken institutional trust (Ibrahim et al., 2024; Nguyen & Adhikari, 2025). Unlike general higher education, where asynchronous learning can partially absorb disruptions, vocational learning is structured around tightly scheduled, practice-oriented activities and competency verification (Gruenhagen et al., 2024; LaFlair et al., 2022). As a result, access failures in VET directly affect skill acquisition, credential credibility, and learner progression (Aboobaker & Abdulkhader, 2021; Ellis, 2025; Pigola & Meirelles, 2025).

Existing cybersecurity research extensively examines authentication systems, identity management, and institutional security governance but treats educational institutions as generic organizational environments without addressing the pedagogical implications of access disruption in practice-based learning contexts (Davies et al., 2023; Rafiq et al., 2025). Conversely, technology-enabled learning and vocational education research often focuses on digital inclusion, instructional design, and platform adoption while giving limited attention to cybersecurity as a learning-critical condition (Hernández-Serrano et al., 2025; Rahmawati et al., 2025). Prior studies frequently evaluate access systems in terms of usability or compliance efficiency, yet rarely examine how authentication failures disrupt competency-based learning cycles or compromise assessment credibility in vocational settings (Long et al., 2025; Mahmood et al.,

2024). Consequently, the relationship between cybersecurity vulnerability and pedagogical disruption in vocational education remains theoretically fragmented.

This systematic literature review addresses this gap through an integrated confidentiality–integrity–availability (CIA), socio-technical systems (STS), and technology-enabled learning (TEL) framework. Rather than cataloguing security threats or technologies alone, the review examines how technical vulnerabilities are commonly associated with socio-technical misalignment and how they manifest as pedagogical disruptions to learning continuity in practice-based vocational environments (Lallie et al., 2025; Mahmood et al., 2024). In this review, socio-technical misalignment refers to the disconnect between technical controls, user capabilities, governance structures, and instructional practices that collectively shape security performance (Haryadi et al., 2023; Pollini et al., 2022). Security inequity refers to the uneven distribution of cybersecurity-related learning risks resulting from disparities in governance capacity, training infrastructure, and access system resilience (Khadka & Ullah, 2025; Lallie et al., 2025).

The review makes three interrelated contributions. First, it advances a socio-technical and pedagogical interpretation of digital access security by framing cybersecurity failures as disruptions to learning continuity and assessment credibility rather than isolated IT incidents (Pollini et al., 2022; Vierke et al., 2023). Second, it identifies availability as the most pedagogically disruptive dimension of the CIA triad in vocational education because downtime directly interrupts simulations, digital laboratories, and competency-based assessments (du Plooy et al., 2024; Long et al., 2025). Third, it conceptualizes security inequity as a systemic outcome of socio-technical misalignment, where disparities in governance, training, and system design expose institutions to unequal risks of instructional disruption (Haryadi et al., 2023; Khadka & Ullah, 2025). Together, these contributions reposition digital access security as an analytical condition for pedagogical stability, institutional trust, and educational equity in technology-enabled vocational education.

Guided by an integrated CIA–STS–TEL framework, this review addresses four research questions:

1. How do prevailing digital access system architectures in vocational education embody implicit security and pedagogical assumptions from a socio-technical perspective?
2. Through what socio-technical mechanisms do confidentiality, integrity, and availability vulnerabilities emerge and interact within vocational digital access systems?
3. How do availability-centered security failures disrupt learning continuity, assessment credibility, and skill acquisition in technology-enabled vocational education?
4. To what extent do existing mitigation strategies address the combined technical, socio-technical, and pedagogical dimensions of digital access security in vocational contexts?

The review employs three complementary theoretical perspectives. The CIA triad provides the foundation for analyzing confidentiality, integrity, and availability vulnerabilities in access systems (Iyengar et al., 2025; Osazuwa, 2024). STS theory explains how interactions between users, institutional culture, and technical systems shape security performance, particularly through issues such as password fatigue, phishing susceptibility, and resistance to security controls (Gamage et al., 2025; Haryadi et al., 2023). The TEL framework contextualizes these vulnerabilities pedagogically by emphasizing how system reliability and uninterrupted access influence learning continuity, assessment integrity, and learner trust (Long et al., 2025; Penberthy, 2020; Vierke et al., 2023). Together, these frameworks provide a layered analytical structure linking technical vulnerabilities, socio-technical causes, and pedagogical consequences (Mahmood et al., 2024).

The findings of this review are intended to support vocational educators, institutional leaders, cybersecurity practitioners, accreditation bodies, and policymakers seeking to strengthen resilient, equitable, and workforce-responsive technology-enabled vocational learning systems (ILO, 2024; OECD, 2023; UNESCO, 2023). To address the research questions systematically and transparently, the study employed a structured systematic literature review methodology grounded in PRISMA 2020 reporting guidelines and theory-informed thematic synthesis (Braun & Clarke, 2006; Page et al., 2021).

Method

A structured, multi-database search was conducted for peer-reviewed literature published between January 2020 and September 2025. Five databases commonly used in education and cybersecurity research were included: IEEE Xplore, Scopus, ScienceDirect, ERIC, and Google Scholar. The search strategy combined controlled vocabulary and free-text keywords using Boolean operators, with database-specific adaptations applied as required. The final search strings executed for each database are presented in Table I.

Table I Database-Specific Search Strings Used in The Systematic Review (Executed on 20/09/2025)

No	Database	Final Search String (Executed on 20/09/2025)
1	Scopus	TITLE-ABS-KEY (("digital access" OR "authentication system" OR "single sign-on" OR sso) AND ("vocational education" OR "technical education" OR vet OR "tvet") AND ("cybersecurity" OR "security challenge*" OR vulnerability) AND ("e-learning" OR "technology-enabled learning" OR "digital learning")) AND PUBYEAR > 2019
2	IEEE Xplore	("Abstract": "access management") AND ("Abstract": "vocational") AND ("Abstract": "security")
3	ScienceDirect	title-abstr-key("digital access system" AND "vocational" AND "security")
4	ERIC	("authentication" OR "login") AND "vocational education" AND "cybersecurity")
5	Google Scholar	("digital access" OR "authentication system" OR "login system" OR "access management" OR "access control" OR "single sign-on" OR SSO) AND ("vocational education" OR "vocational training" OR "technical education" OR "VET" OR "TVET" OR "skills training" OR "career education") AND ("technology-enabled learning" OR "e-learning" OR "online learning" OR "digital learning" OR "hybrid learning" OR "blended learning") AND ("security challenge" OR "cybersecurity" OR "vulnerability" OR "threat" OR "data breach" OR "privacy risk" OR "authentication risk")

For Google Scholar, screening was limited to the first 50 results ranked by relevance. This search was used to supplement database searches and to identify additional peer-reviewed studies not indexed elsewhere. Backward and forward citation tracing was also conducted.

Inclusion and Exclusion Criteria

Eligibility criteria were applied to define the scope of the review.

Inclusion criteria:

1. Focus: Studies addressing digital access systems (e.g., LMS, SSO, RFID, biometrics).
2. Scope: Empirical findings or frameworks examining security challenges, vulnerabilities, or mitigations.
3. Timeframe: 2020–2025, primarily to capture post-pandemic digital transformation.
4. Language: English.
5. Type: Peer-reviewed journal articles or conference papers.

Exclusion criteria:

1. Studies on general cybersecurity without an educational dimension.
2. Discussions of digital learning tools without addressing access/security mechanisms.
3. Purely theoretical work without application to real institutions or learners.
4. No explicit relevance to vocational training contexts.

Study Selection Process

The study selection process followed the PRISMA 2020 guidelines (Page et al., 2021). The systematic review methodology was applied to support theory-informed synthesis rather than exhaustive enumeration of findings. The initial search yielded 412 records across all databases. After duplicate removal, 356 unique records were screened by title and abstract. Following full-text assessment of 81 articles, 58 studies met all inclusion criteria for data extraction and synthesis. The complete process, including reasons for exclusion at each stage, is detailed in the PRISMA flow diagram (Figure 1).

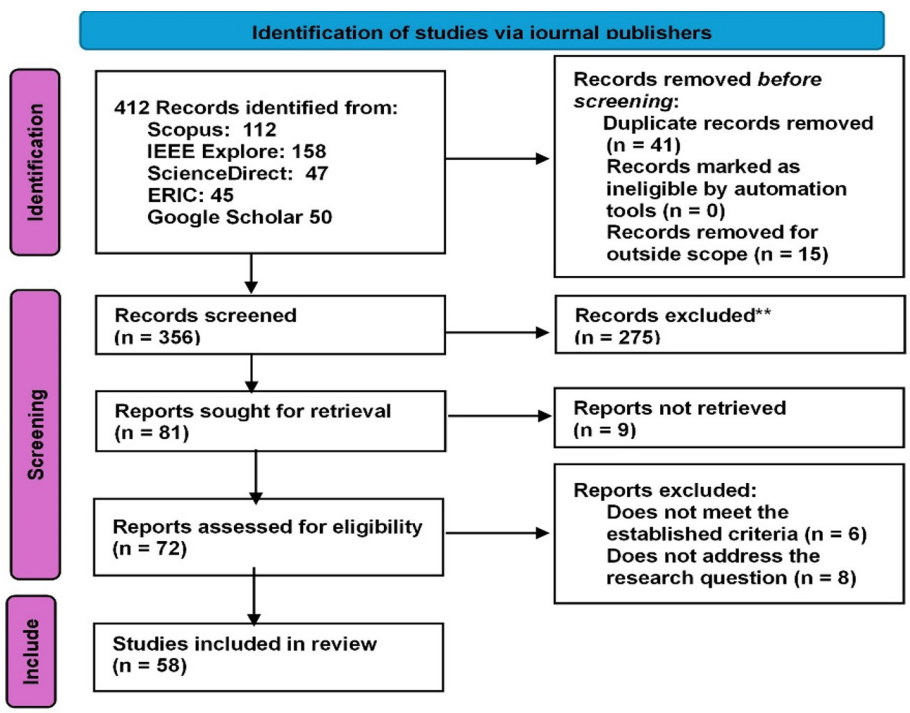

Figure 1 PRISMA Flow Diagram of Study Selection

Quality Assessment

A five-item checklist was used to appraise the methodological characteristics of the included studies, covering clarity of research objectives, transparency of methods, strength of evidence, validity of data collection and analysis, and relevance to vocational education or technology-enabled learning. Each study was rated on a five-point scale. Studies scoring three or above were retained for synthesis (Kitchenham & Brereton, 2013; McKenzie et al., 2016). Quality scores ranged from 3 to 5 (M = 4.1, SD = 0.6). No studies were excluded based on quality score, as they all met the predefined inclusion threshold. The primary limitations were a lack of longitudinal design and small sample sizes in context-specific case studies.

Data Extraction and Synthesis

A structured data extraction matrix was used to record publication details, access system type, identified security threats, research methodology, reported impacts on teaching and learning, and proposed mitigation strategies. A mixed-methods synthesis approach was applied:

- Descriptive statistics quantified threat prevalence (e.g., frequency of weak authentication).
- Thematic analysis, guided by the CIA triad, STS theory, and TEL framework, identified cross-study patterns in human factors, institutional practices, and pedagogical consequences. This approach is appropriate for complex, interdisciplinary reviews (Braun & Clarke, 2006; Zangana et al., 2025).

Thematic analysis was conducted by two authors independently. Initial codes were derived deductively from the CIA/STS/TEL frameworks and inductively from the data. Discrepancies were resolved through discussion to reach consensus. Analysis was supported by NVivo 14. The complete data extraction matrix is available in Supplementary Data S1.

Characteristics of Included Studies

A summary of the 58 included studies, detailing author, year, geographical context, research design, focal access system, and key security findings, is provided in Supplementary Table S1.

Ethical Note on the Use of Generative AI

During manuscript preparation, the authors used OpenAI solely for the purpose of complex analysis, English language proofreading, grammar checking, and ensuring consistent academic tone across sections translated by non-native speakers. All conceptual development, literature analysis, data interpretation, and critical writing were performed by the human authors. The final content is entirely the responsibility of the authors.

As a systematic literature review, the analysis reflects patterns reported in published studies and may not capture undocumented institutional practices or unpublished security incidents. The findings should therefore be interpreted as indicative of recurring trends rather than exhaustive representations of all vocational education contexts.

Results and Discussion

This section synthesizes evidence from 58 studies reporting on digital access systems, security vulnerabilities, and mitigation practices in vocational education contexts. The synthesis identifies recurring access architectures, prevalent confidentiality, integrity, and availability vulnerabilities, and documented impacts on instructional activities and assessment processes. Findings are organized to reflect observed patterns across system design, user behavior, and institutional practice, without advancing interpretive or theoretical claims, which are developed in the subsequent Discussion section (McKenzie et al., 2016; Snyder, 2019).

Digital Access Architectures and Security Assumptions (STS–CIA)

Digital access in vocational education is dominated by a small set of architectures whose design choices systematically shape both security exposure and learning continuity (Aboobaker & Abdulkhader, 2021; Ahmed et al., 2024; Ellis, 2025):

- Cloud-based LMS authentication centralizes access control but increases dependency on continuous connectivity (Acheampong et al., 2025). Security weaknesses included outdated plugins, poor session management, and weak password enforcement (Arina & Anatolie, 2021; Lallie et al., 2025).
- Single sign-on (SSO) Federations: SSO centralized access across platforms but expanded the attack surface; misconfigured trust relationships were a noted vulnerability (Bradatsch et al., 2023; Pigola & Meirelles, 2025).
- Biometric Authentication Systems: Employed for physical lab access, raising concerns about template storage and spoofing (Malik, 2024; Protasenko & Ivashura, 2022; Ragab et al., 2025).
- RFID/Smart Card Systems: Used for attendance and equipment access but were susceptible to cloning and replay attacks (Mohamed et al., 2024; Osegbue et al., 2025).

CIA Vulnerabilities Activated Through Socio-technical Dynamics

Across the reviewed studies, confidentiality, integrity, and availability failures emerge not as isolated technical flaws but as recurring patterns produced by the interaction of system design, user behavior, and institutional practice (Osazuwa, 2024):

- Confidentiality breaches: The most cited issue was weak authentication, including password reuse, low-complexity credentials, and unencrypted logins, enabling credential stuffing and phishing (Aboobaker & Abdulkhader, 2021; Coopamootoo et al., 2017; Yusop et al., 2025). Poorly secured SSO tokens were another risk (Cahyanto et al., 2024).
- Availability threats: Denial-of-service attacks, ransomware, and misconfigurations caused system downtime, directly disrupting time-sensitive practical sessions (Davies et al., 2023; du Plooy et al., 2024; Ibrahim et al., 2024). Such outages significantly impacted skill-based assessment performance (Coombs et al., 2020).
- Integrity challenges: Incidents of identity impersonation, grade tampering, and unauthorized role access compromised assessment validity and institutional trust (Gruenhagen et al., 2024; LaFlair et al., 2022; Omirali et al., 2025).

Across studies, CIA vulnerabilities were consistently amplified by socio-technical dynamics, producing compounded risk rather than isolated failure modes. For instance, password fatigue and low security literacy (LSL) directly enabled credential stuffing and phishing attacks (CIA-Confidentiality). Successful social engineering (SSE) often served as the initial vector for ransomware deployment (CIA-Availability). To clarify the prevalence and distribution of reported vulnerabilities across the reviewed literature, Table II summarizes the most frequently reported CIA-related security challenges identified across the included studies (du Plooy et al., 2024; Lallie et al., 2025).

Table II Frequency of Reported CIA Vulnerabilities in Reviewed Studies

Vulnerability Type	Common Examples	Frequency Trend
Confidentiality	Password reuse, phishing, weak MFA	High
Integrity	Assessment impersonation, grade tampering	Moderate
Availability	Ransomware, downtime, DoS attacks	Very High

As shown in Table II, availability-related failures were reported most consistently across vocational education contexts, reinforcing their significant role in disrupting learning continuity and practical skill development (Long et al., 2025). Table II is an extract from Supplementary Table SII.

Pedagogical Consequences of Access Failures (TEL Perspective)

The review indicates that digital access security failures in vocational education translate directly into pedagogical disruption, undermining learning continuity, assessment integrity, and institutional trust:

- Disrupted learning continuity and skill acquisition: Over half of the studies documented that system downtime (CIA-Availability) directly interrupted scheduled, firsthand sessions. From a TEL perspective, these interruptions break deliberate practice cycles essential for psychomotor skill mastery (Korchagin, 2025; Nguyen & Adhikari, 2025). A confidentiality breach (e.g., stolen credentials) can lead to a ransomware attack (availability failure), which results in missed simulation time and degraded skill performance (TEL) (Bhandari, 2025; Jasso, 2025).
- Erosion of institutional trust and compromised assessment integrity: Integrity breaches (CIA), such as impersonation or data manipulation, strike at the core of VET's mission: credible skill certification (Momanyi et al., 2024). When learners and industry partners perceive that assessment systems are vulnerable, institutional trust erodes (TEL) (Penberthy, 2020; Raza et al., 2024).

This erosion is exacerbated when incidents reveal poor governance or inadequate user training (STS), demonstrating a misalignment between the institution's social and technical subsystems. Consequently, security failures transition from IT incidents to crises of pedagogical credibility and institutional legitimacy.

A failure in one pillar of the CIA triad, often precipitated by STS dynamics, produces direct, negative consequences within the TEL environment, affecting everything from minute-to-minute skill practice to the long-term value of vocational credentials. Figure 2 presents the conceptual socio-technical interaction model developed from thematic synthesis. The model illustrates how CIA-related vulnerabilities interact with governance capacity, user behavior, and instructional dependence on uninterrupted access to produce pedagogical disruption and security inequity in vocational education contexts (Haryadi et al., 2023; Mahmood et al., 2024).

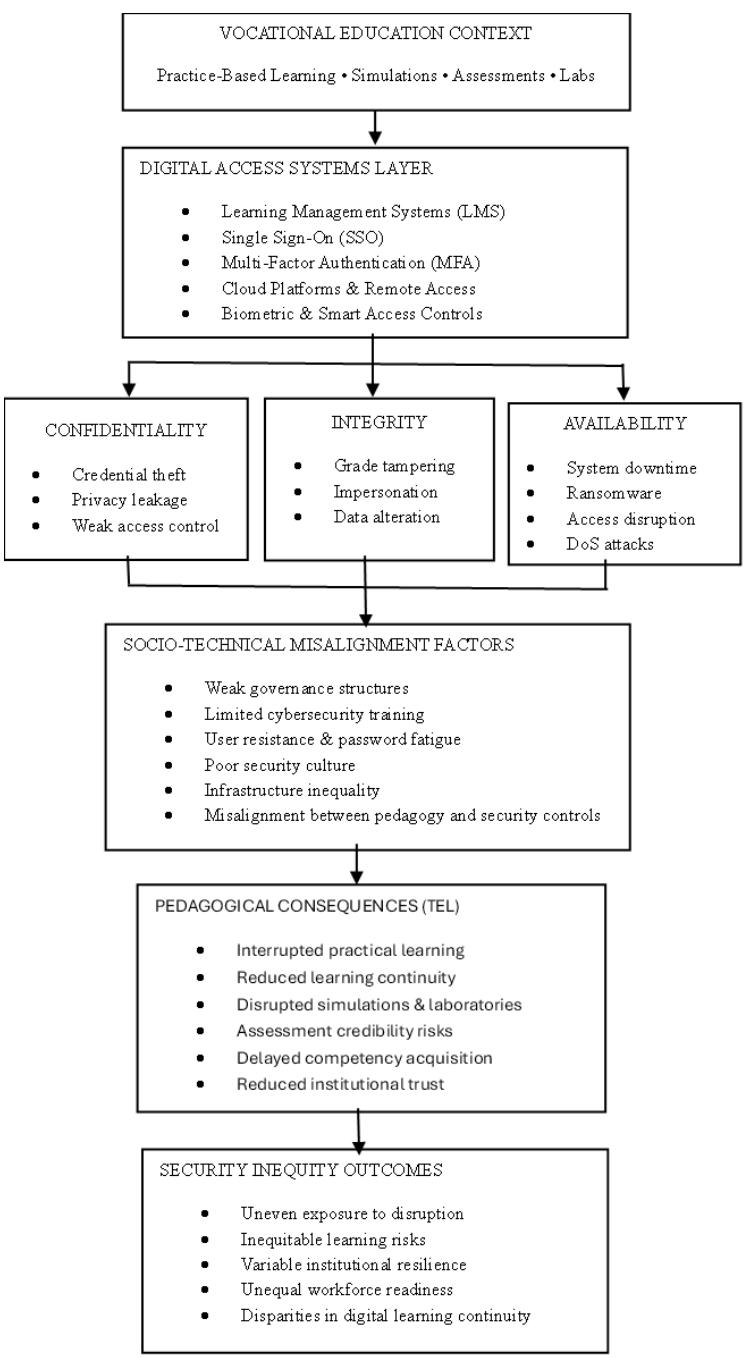

Figure 2 Conceptual Socio-Technical Interaction Model of Digital Access Security in Vocational Education

The model demonstrates that cybersecurity failures in vocational education are not isolated technical events but interconnected socio-technical processes whose pedagogical consequences emerge through the interaction between access system vulnerabilities, institutional governance conditions, and technology-enabled learning dependencies (Pollini et al., 2022; Vierke et al., 2023).

Fragmented Mitigations Across Technical, Socio-technical, and Pedagogical Layers

The literature proposes numerous technical and administrative mitigations, yet these are rarely integrated or aligned with vocational pedagogical realities:

- Technical controls: Included Multi-Factor Authentication (MFA) (Cahyanto et al., 2024; Yusop et al., 2025), Zero-Trust Architectures (Lallie et al., 2025; Pigola & Meirelles, 2025), blockchain for credential integrity (Bhawna et al., 2025; Wang et al., 2025), and improved encryption/SSO configuration (Mookherji et al., 2023).
- Administrative & socio-technical controls: Emphasized mandatory cybersecurity awareness training (Alrobaian et al., 2023; Ojala et al., 2025; Taherdoost, 2024), robust incident response plans (Mohd Kassim et al., 2023; Ren et al., 2025), user-centered policy redesign (Acheampong et al., 2025), and aligning IT maintenance with instructional schedules.

A noted gap was the lack of holistic frameworks integrating these technical and human-centric solutions within a pedagogical VET context (Ika Sari et al., 2024; Othman et al., 2025). Taken together, these findings indicate recurring patterns in how digital access vulnerabilities intersect with instructional activities in vocational education, which are interpreted in the following Discussion section.

Building on the findings in the preceding sections, this discussion interprets digital access security failures in vocational education as socio-technical and pedagogical breakdowns rather than isolated technical incidents (Khadka & Ullah, 2025; Mahmood et al., 2024). Across the reviewed studies, confidentiality, integrity, and availability vulnerabilities consistently co-occur through misalignment between access system design, user practices, and institutional governance (Haryadi et al., 2023; Lallie et al., 2025). From a socio-technical systems (STS) perspective, these failures reflect tensions between usability, compliance capacity, and instructional demands in practice-oriented learning environments (du Plooy et al., 2024; Long et al., 2025). From a technology-enabled learning (TEL) perspective, the consequences extend beyond system reliability to directly affect learning continuity, assessment credibility, and institutional trust (Vierke et al., 2023).

The synthesis further indicates that availability is the most immediately pedagogically disruptive dimension of the CIA triad in vocational education. While confidentiality and integrity breaches primarily undermine trust and legitimacy, availability failures interrupt access to simulations, digital laboratories, and competency-based assessments during critical instructional periods (du Plooy et al., 2024; Long et al., 2025). Consequently, downtime functions not as a temporary technical inconvenience but as a structural barrier to skill development and learning continuity (Mahmood et al., 2024; Vierke et al., 2023).

The findings also show that security inequity extends beyond uneven resource distribution and is strongly associated with socio-technical misalignment across governance, training capacity, and access system design. Institutions with limited governance structures, inadequate infrastructure, or weak user-centered security practices face disproportionately greater risks of disruption, positioning cybersecurity as an issue of educational equity linked to fairness, inclusion, and learning opportunity in vocational systems (Haryadi et al., 2023; Khadka & Ullah, 2025; Lallie et al., 2025).

Persistent Authentication Weaknesses

A recurring finding is the continued reliance on weak authentication practices, including password-only systems, despite well-established security risks (Alsirhani et al., 2022; Kausar & Laghari, 2025; Lallie et al., 2025). STS theory suggests that these weaknesses reflect socio-technical misalignment rather than

purely technical failure. Password fatigue, limited security literacy, and resistance to procedural change continue to undermine secure authentication practices (Al-Slais & Elmedany, 2022; Carroll, 2021; Khadka & Ullah, 2025). Although single sign-on (SSO) systems improve usability, they also centralize identity risk, meaning that poor session management or token misconfiguration can produce large-scale compromise (Bradatsch et al., 2023; EDUCAUSE, 2025).

Availability as a Pedagogical Constraint

Within the CIA triad, availability emerged as the most pedagogically critical dimension in vocational education. Availability failures rarely occur in isolation and often represent downstream consequences of prior confidentiality or integrity breaches that escalate into downtime and instructional disruption. Because vocational education depends on scheduled access to simulations, laboratories, and specialized digital tools, ransomware attacks or denial-of-service incidents directly interrupt competency development and reduce skill retention (du Plooy et al., 2024; Ghosh & Ravichandran, 2024; Korchagin, 2025). Unlike confidentiality and integrity breaches, which primarily affect trust after instructional activities occur, availability failures intervene during learning itself, disrupting skill acquisition in real time.

Comparison with Non-Vocational Educational Contexts

Compared with general higher education environments, vocational education demonstrates a stronger dependency on uninterrupted real-time access because practical training activities are tightly scheduled and competency-based (Gruenhagen et al., 2024; Long et al., 2025). In many non-vocational university contexts, asynchronous learning models partially absorb access interruptions through flexible deadlines and recorded instructional materials (Mahmood et al., 2024). By contrast, vocational learning disruptions frequently affect psychomotor skill development, laboratory sequencing, and industry certification processes, increasing the pedagogical severity of availability failures.

Integrity Risks and Credential Credibility

Although reported less frequently, integrity breaches such as assessment impersonation, unauthorized grade modification, and record tampering pose serious risks to the credibility of vocational qualifications (Gruenhagen et al., 2024; LaFlair et al., 2022). These failures undermine trust among learners, institutions, and employers and are commonly associated with weak access governance and poor identity lifecycle management (Molla-Esparza et al., 2025; Tulin, 2024).

The Socio-Technical Gap

Human behavior remains a persistent cross-cutting vulnerability. Credential sharing, phishing susceptibility, and workarounds designed to bypass cumbersome controls routinely weaken technical safeguards (Al-Husari et al., 2025; Pollini et al., 2022). This misalignment is especially visible in resource-constrained institutions that lack advanced security infrastructure or comprehensive training programs. As a result, learners in under-resourced environments face disproportionately greater risks of disruption and breach, reinforcing cybersecurity as an issue of educational equity rather than technical capability alone. STS theory emphasizes that sustainable security depends on alignment between technical systems, institutional culture, workload realities, and user capabilities (Mahmood et al., 2024). In many vocational settings, however, this alignment remains limited (Ali, 2025).

Unexpected Findings and Alternative Interpretations

An unexpected finding across the reviewed studies was the extent to which availability failures overshadowed confidentiality and integrity concerns in terms of immediate pedagogical disruption. Traditional cybersecurity literature typically prioritizes confidentiality and data protection as primary

institutional concerns (NIST, 2024; Osazuwa, 2024). However, within vocational education environments, system downtime consistently produced more immediate instructional consequences because practical learning activities depend on synchronized access to simulations, laboratories, and competency assessments (Candido et al., 2023; Long et al., 2025; Vierke et al., 2023).

An alternative interpretation is that these disruptions may partly reflect broader institutional digital maturity limitations rather than cybersecurity weaknesses alone. Institutions with limited infrastructure redundancy, inadequate instructional contingency planning, or unstable connectivity may experience amplified disruption regardless of attack severity (Mahmood et al., 2024). Nevertheless, the reviewed studies consistently demonstrate that security-related availability failures remain a major trigger for pedagogical interruption in technology-enabled vocational settings (du Plooy et al., 2024).

Fragmented Mitigations and the Need for Holistic Models

The literature proposes a range of technical solutions, including multi-factor authentication, zero-trust models, and blockchain-based verification, alongside administrative interventions such as security training and policy reform (Abduhari et al., 2025; Bhawna et al., 2025; Fadli et al., 2024). However, these approaches remain fragmented and rarely integrate pedagogical, technical, and organizational dimensions simultaneously (Candido et al., 2023; Mukherjee et al., 2024). This fragmentation reflects a broader research-practice divide in which cybersecurity scholarship seldom engages with pedagogical theory, while educational research often underestimates security as a learning-critical condition (Mahmood et al., 2024; Mukherjee et al., 2024): The absence of vocational-specific security standards further forces institutions to adapt generic corporate IT policies that may not align with practice-based learning environments. Consequently, sustainable security in vocational education requires integrated models that align technological safeguards, instructional continuity, and socio-technical capacity building (NIST, 2021).

Practical Implications Across Diverse Contexts

The findings demonstrate that digital access security in vocational education cannot be addressed through uniform technical solutions because institutional capacity, infrastructure maturity, and governance conditions differ across contexts (Mahmood et al., 2024; UNESCO, 2023). Effective mitigation therefore requires context-sensitive strategies aligned with pedagogical continuity, institutional resources, and workforce development priorities.

In resource-rich vocational systems, institutions are better positioned to implement integrated identity management infrastructures, adaptive authentication, cloud redundancy, and continuous monitoring systems while maintaining uninterrupted access to simulations and assessments (Ahmed et al., 2024; Coverdale et al., 2024; Nguyen & Adhikari, 2025). However, sophisticated controls may also create usability friction if implemented without adequate training or pedagogical alignment (Motamed, 2024; Pollini et al., 2022).

In resource-constrained contexts, the primary challenges are often structural rather than technological. Limited infrastructure redundancy, unstable connectivity, insufficient cybersecurity staffing, and restricted training budgets increase vulnerability to prolonged disruption (Haryadi et al., 2023; Khadka & Ullah, 2025). In these environments, scalable governance interventions, phased implementation strategies, and user-awareness programs may provide more sustainable improvements than technically complex solutions beyond institutional capacity (Sari et al., 2024; UNESCO, 2023).

Institutional scale also shapes implementation priorities. Large vocational institutions managing multiple campuses and digital platforms face greater exposure to identity management complexity, third-party integration risks, and distributed governance challenges (Rafiq et al., 2025). Smaller institutions may face fewer integration challenges but often depend heavily on external vendors and outsourced

cloud services because of limited technical expertise and financial flexibility (Fecke et al., 2022; Pigola & Meirelles, 2025).

The findings additionally carry implications for policymakers and accreditation agencies. Existing digital education policies frequently prioritize platform adoption without adequately evaluating system resilience under security stress conditions (OECD, 2023; UNESCO, 2023). The review therefore suggests that accreditation and quality assurance frameworks should incorporate indicators related to authentication resilience, learning continuity, and incident recovery preparedness (Long et al., 2025; Mahmood et al., 2024). This is particularly important because availability failures affect not only institutional operations but also competency development, certification credibility, and workforce readiness (ILO, 2024).

Across all contexts, the findings reinforce that cybersecurity in vocational education should be understood as a pedagogical and governance issue rather than solely a technical responsibility. Security controls that fail to account for instructional realities, user behavior, and institutional constraints may unintentionally create additional barriers to learning continuity and equitable participation (Pollini et al., 2022; Vierke et al., 2023).

Limitations

Several limitations should be acknowledged. First, the review synthesized only English-language peer-reviewed studies published between 2020 and 2025 and may therefore exclude relevant regional or non-indexed literature. Second, the rapidly evolving nature of cybersecurity means that some technological vulnerabilities and mitigation practices may develop faster than the academic publication cycle (Lallie et al., 2025). Third, the studies included varied methodological design, institutional context, and technological infrastructure, limiting direct comparability across findings. Finally, although the review integrated CIA, STS, and TEL frameworks, the conclusions remain interpretive and should be validated through empirical longitudinal and comparative research designs (Braun & Clarke, 2006; Mahmood et al., 2024). These limitations also highlight important directions for future empirical and comparative research on digital access security in vocational education contexts.

Conclusion

This systematic literature review highlights digital access security as a learning-critical condition in technology-enabled vocational education. Synthesizing evidence from recent studies, the review shows that access disruptions are not peripheral technical events but recurring constraints on skill acquisition, assessment credibility, and institutional trust in practice-based learning environments (Mahmood et al., 2024; Momanyi et al., 2024; Vierke et al., 2023). The findings underscore that vulnerabilities in digital access systems have immediate instructional consequences in vocational contexts, where learning depends on timely, continuous engagement with digital and simulated training resources (Candido et al., 2023; du Plooy et al., 2024).

A central contribution of this review is the identification of availability as the most pedagogically consequential dimension of the CIA triad in vocational education. While breaches of confidentiality and integrity erode trust and legitimacy, failures of availability immediately interrupt deliberate practice cycles by denying access to simulations, digital laboratories, and assessment environments at critical instructional moments (du Plooy et al., 2024; Long et al., 2025). From a TEL perspective, such interruptions constitute structural barriers to learning rather than temporary technical inconveniences. These findings reposition availability from an operational metric to a core pedagogical requirement in technology-enabled vocational systems (Mahmood et al., 2024; Vierke et al., 2023).

The review further demonstrates that security inequity in vocational education is not simply a function of uneven resource distribution. Instead, it reflects systemic socio-technical misalignment, where limited governance capacity, insufficient training infrastructures, and poorly aligned access system designs expose certain institutions and learner populations to disproportionate risk (Haryadi et al., 2023;

Khadka & Ullah, 2025). This positions cybersecurity as an issue of educational equity, linking digital access security to broader questions of fairness, inclusion, workforce preparedness, and lifelong learning opportunity within vocational systems (ILO, 2024; Lallie et al., 2025).

The findings indicate that effective digital access security in vocational education requires a shift from tool-centric protection toward pedagogically informed socio-technical alignment. Access systems should be evaluated based on their capacity to sustain learning continuity in time-bound, practice-oriented environments, rather than solely on compliance or threat mitigation metrics (Pollini et al., 2022). Security governance must integrate technical controls with user training, instructional scheduling, and institutional workflows, recognizing that human behavior and organizational practice are integral to security performance (Khadka & Ullah, 2025). Importantly, strengthening digital access security should be treated as an equity intervention to prevent systematic exposure of learners in resource-constrained institutions to higher disruption risks (Haryadi et al., 2023).

At the policy level, the findings call for cybersecurity frameworks that move beyond technical compliance to explicitly address pedagogical risk and socio-technical alignment in vocational education (Lallie et al., 2025). Accrediting bodies and regulators should recognize availability failures as learning-critical events and incorporate pedagogical continuity into digital security standards. This is particularly important in TVET systems where uninterrupted access to digital learning environments increasingly shapes employability, workforce adaptability, and lifelong learning capacity (ILO, 2024). Future research should empirically test the integrated CIA–STS–TEL framework advanced in this review, particularly through longitudinal and comparative studies examining how access disruptions affect learning outcomes across vocational and non-vocational contexts (Mahmood et al., 2024; Vierke et al., 2023).

This review advances a conceptual shift in how digital access security is understood in vocational education. By demonstrating that cybersecurity failures function as socio-technical and pedagogical breakdowns rather than isolated technical incidents, it supports the view that digital access security functions as a core condition for effective, equitable, and trustworthy vocational learning systems.

Declaration of Generative Artificialintelligence (AI) Use

"During the preparation of this work, the authors used Grammarly and ChatGPT (OpenAI) in order to proofread, check grammar and ensure consistent academic tone across sections translated by non-native English speakers. After using this tool/service, the authors reviewed and edited the content as needed and take full responsibility for the content of the published article."

References

Abduhari, E. S., Shaik, T. C., Adidul, A. B., Ladja, J. H., Saliddin, E. S., Adin, A. J., Rumbahali, F. A., Sali, A. B., Jemser, J. M., & Tahil, S. K. (2025). Access control mechanisms and their role in preventing unauthorized data Access: A comparative analysis of RBAC, MFA, and strong passwords. *Natural Sciences Engineering and Technology Journal*, *5*(1), 418–430. https://doi.org/10.37275/nasetjournal.v5i1.62

Aboobaker, N., & Abdulkhader, Z. (2021). Digital learning orientation and innovative behavior in the higher education sector: Effects of organizational learning culture and readiness for change. *International Journal of Educational Management*, *ahead-of-print*. https://doi.org/10.1108/IJEM-09-2019-0345

Acheampong, R., Balan, T. C., Popovici, D.-M., Tuyishime, E., Rekeraho, A., & Voinea, G. D. (2025). Balancing usability, user experience, security, and privacy in XR systems: A multidimensional approach. *International Journal of Information Security*, *24*(3), 112. https://doi.org/10.1007/s10207-025-01025-z

Ahmed, K. I., Tahir, M., Lau, S. L., Habaebi, M. H., Ahad, A., & Pires, I. M. (2024). Dataset for authentication and authorization using physical layer properties in indoor environment. *Data in Brief*, *55*. Scopus. https://doi.org/10.1016/j.dib.2024.110589

Al-Husari, F., Nakov, O., & Nakov, P. (2025). Multi-factor authentication fatigue: A growing concern in user experience and security. *2025 60th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)*, 1–4. https://doi.org/10.1109/ICEST66328.2025.11098219

Ali, M. G. (2025). Cybersecurity governance and policy development in higher education institutions: A strategic framework for resilience and compliance. In *Online Submission*. https://eric.ed.gov/?id=ED675147

Alrobaian, S., Alshahrani, S., & Almaleh, A. (2023). Cybersecurity awareness assessment among trainees of the technical and vocational training corporation. *Big Data and Cognitive Computing*, *7*(2), Article 2. https://doi.org/10.3390/bdcc7020073

Alsirhani, A., Ezz, M., & Mostafa, A. M. (2022). Advanced authentication mechanisms for identity and access management in Cloud computing. *Computer Systems Science and Engineering*, *43*(3), 967–984. Scopus. https://doi.org/10.32604/csse.2022.024854

Al-Slais, Y., & Elmedany, W. (2022). User-centric adaptive password policies to combat password fatigue. *International Arab Journal of Information Technology*, *19*(1), 55–62. Scopus. https://doi.org/10.34028/iajit/19/1/7

Arina, A., & Anatolie, A. (2021). Cybersecurity threat analysis in higher education institutions as a result of distance learning. *International Journal of Scientific & Technology Research*, *10*(03).

Bhandari, B. (2025). Cybersecurity awareness amongst university students: Legal remedies and policies to mitigate risks. *Unity Journal*, *6*(1), 120–135. https://doi.org/10.3126/unityj.v6i1.75557

Bhawna, Gupta, P., & Rai, P. (2025). Can blockchain revolutionize educational practices? An in-depth analysis of applications and challenges. *Sustainable Futures*, *10*, 101171. https://doi.org/10.1016/j.sftr.2025.101171

Bradatsch, L., Miroshkin, O., & Kargl, F. (2023). ZTSFC: A service function chaining-enabled zero trust architecture. *IEEE Access*, *11*, 125307–125327. Scopus. https://doi.org/10.1109/ACCESS.2023.3330706

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Cahyanto, I., Madihah, H., Budiarso, I., Sutrisno, A., & Hidayat, T. (2024). Effectiveness of multifactor authentication technology for protecting student privacy: A systematic literature review. *Edum Journal*, *7*(2), 253–269. https://doi.org/10.31943/edumjournal.v7i2.286

Candido, V., Raemy, P., Amenduni, F., & Cattaneo, A. (2023). Could vocational education benefit from augmented reality and hypervideo technologies? An exploratory interview study. *International Journal for Research in Vocational Education and Training*, *10*(2), 138–167. https://doi.org/10.13152/IJRVET.10.2.1

Carroll, C. (2021). Security fatigue and its effects on perceived password strength among university students. *Honors Theses*. https://scholar.utc.edu/honors-theses/290

Coombs, C., Hislop, D., Taneva, S. K., & Barnard, S. (2020). The strategic impacts of Intelligent automation for knowledge and service work: An interdisciplinary review. *The Journal of Strategic Information Systems, 2020 Review Issue*, *29*(4), 101600. https://doi.org/10.1016/j.jsis.2020.101600

Coopamootoo, K. P., Gross, T., & Pratama, M. F. R. (2017). An empirical investigation of security fatigue: The case of password choice after solving a {CAPTCHA}. *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2017)*, 39–48.

Coverdale, A., Lewthwaite, S., & Horton, S. (2024). Digital accessibility education in context: Expert perspectives on building capacity in academia and the workplace. *ACM Trans. Access. Comput.*, *17*(2), 10:1-10:21. https://doi.org/10.1145/3649508

Davies, A., Donald, B., & Gray, M. (2023). The power of platforms—Precarity and place. *Cambridge Journal of Regions, Economy and Society*, *16*(2), 245–256. https://doi.org/10.1093/cjres/rsad011

du Plooy, E., Casteleijn, D., & Franzsen, D. (2024). Personalized adaptive learning in higher education: A scoping review of key characteristics and impact on academic performance and engagement. *Heliyon*, *10*(21), e39630. https://doi.org/10.1016/j.heliyon.2024.e39630

Educause. (2025). *Higher education cybersecurity: Challenges, choices, and the case for training*. Educause Review. https://er.educause.edu/articles/sponsored/2025/7/higher-education-cybersecurity-challenges-choices-and-the-case-for-training

Eisenbart, M. (2023). *Boundary crossing within hybrid learning environments in vocational education in the northern netherlands* [B]. https://campus-fryslan.studenttheses.ub.rug.nl/287/

Ellis, D. (2025). *Technology education teacher professional learning: Enabling the future*. https://doi.org/10.25918/thesis.519

Fadli, R., Surjono, H. D., Sari, R. C., Hidayah, Y., & Eliza, F. (2024). Assessing cybersecurity awareness among vocational students in office administration. *International Journal of Safety and Security Engineering*, *14*(4), 1115–1123. Scopus. https://doi.org/10.18280/ijsse.140410

Fecke, M., Fehr, A., Schlütz, D., & Zillich, A. F. (2022). The ethics of gatekeeping: How guarding access influences digital child and youth research. *Media and Communication, Article*, *10*(1), 361–370. https://doi.org/https://doi.org/10.17645/mac.v10i1.4756

Gamage, I., Malik, M., Andargoli, A., & Chavez Clavijo, R. (2025). Theorizing lean as a sociotechnical system: Examining the reciprocal interactions between lean social and technical subsystems. *IEEE Transactions on Engineering Management*, *72*, 2456–2472. https://doi.org/10.1109/TEM.2025.3569876

Ghosh, L., & Ravichandran, R. (2024). Emerging technologies in vocational education and training. *Journal of Digital Learning and Education*, *4*(1), 41–49. https://doi.org/10.52562/jdle.v4i1.975

Gruenhagen, J. H., Sinclair, P. M., Carroll, J.-A., Baker, P. R. A., Wilson, A., & Demant, D. (2024). The rapid rise of generative AI and its implications for academic integrity: Students' perceptions and use of chatbots for assistance with assessments. *Computers and Education: Artificial Intelligence*, *7*, 100273. https://doi.org/10.1016/j.caeai.2024.100273

Haryadi, E., Karim, A., & Salahuddin, L. (2023). Socio-technical perspective in determining the factors and components for minimizing cybersecurity threat. *TEM Journal*, *12*(3), 1825–1837. Scopus. https://doi.org/10.18421/TEM123-66

Hernández-Serrano, M. J., Cullen, J., Jones, B., & Romo, N. M. (2025). A flexible framework integrating digital and social competences in vocational education across diverse contexts. *Media and Communication, Article*, *13*. https://doi.org/https://doi.org/10.17645/mac.8974

Ibrahim, N., Rajalakshmi, R., & Hammadeh, K. (2024). Exploration of defensive strategies, detection mechanisms, and response tactics against advanced persistent threats APTs. *Nanotechnology Perceptions*, *20*(S4), 439–455. Scopus. https://doi.org/10.62441/nano-ntp.v20is4.33

Ika Sari, G., Winasis, S., Pratiwi, I., Wildan Nuryanto, U., & Basrowi. (2024). Strengthening digital literacy in Indonesia: Collaboration, innovation, and sustainability education. *Social Sciences & Humanities Open*, 101100. https://doi.org/10.1016/j.ssaho.2024.101100

ILO. (2024). *Skills and lifelong learning* [Advancing social justice, promoting decent work]. ILO. International Labour Organization. https://www.ilo.org/topics-and-sectors/skills-and-lifelong-learning

Iyengar, S. S., Nabavirazavi, S., Hariprasad, Y., HB, P., & Mohan, C. K. (2025). Cybersecurity Foundations: Theories, Technologies, and Applications. In S. S. Iyengar, S. Nabavirazavi, Y. Hariprasad, P. HB, & C. K. Mohan (Eds.), *artificial intelligence in practice: Theory and application for cyber security and forensics* (pp. 27–87). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-89327-8_2

Jasso, J. (2025). Advancing cybersecurity awareness and training strategies. *Social Science Research Network*. https://doi.org/10.2139/ssrn.5244103

Kausar, S., & Laghari, A. R. (2025). Social engineering attacks in pakistan: Analyzing the weakest link in cyber security. *Journal of Development and Social Sciences*, *6*(1), 364–374. https://doi.org/10.47205/jdss.2025(6-I)32

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, *24*(3), 119. https://doi.org/10.1007/s10207-025-01032-0

Kitchenham, B., & Brereton, P. (2013). A systematic review of systematic review process research in software engineering. *Information and Software Technology*, *55*(12), 2049–2075. https://doi.org/10.1016/j.infsof.2013.07.010

Korchagin, S. (2025, September 22). *How educational facilities across Australia can safeguard its systems from power outages*. Treske Pty Limited. https://treske.com.au/blogs/treske-business-blogs/how-educational-facilities-across-australia-can-safeguard-it-systems-from-power-outages-1

LaFlair, G. T., Langenfeld, T., Baig, B., Horie, A. K., Attali, Y., & von Davier, A. A. (2022). Digital-first assessments: A security framework. *Journal of Computer Assisted Learning*, *38*(4), 1077–1086. https://doi.org/10.1111/jcal.12665

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. *Computers*, *14*(2), 49. https://doi.org/10.3390/computers14020049

Long, Y., Zhang, X., & Zeng, X. (2025). Application and effect analysis of virtual reality technology in vocational education practical training. *Education and Information Technologies*, *30*(7), 9755–9786. https://doi.org/10.1007/s10639-024-13197-7

Mahmood, S., Chadhar, M., & Firmin, S. (2024). Addressing cybersecurity challenges in times of crisis: Extending the sociotechnical systems perspective. *Applied Sciences (Switzerland)*, *14*(24). Scopus. https://doi.org/10.3390/app142411610

Malik, G. (2024). Biometric authentication-risks and advancements in biometric security systems. *Journal of Computer Science and Technology Studies*, *6*(3), 159–180. https://doi.org/10.32996/jcsts.2024.6.3.14

McKenzie, J. E., Beller, E. M., & Forbes, A. B. (2016). Introduction to systematic reviews and meta-analysis. *Respirology*, *21*(4), 626–637. https://doi.org/10.1111/resp.12783

Mohamed, I., Hefny, H. A., & Darwish, N. R. (2024). Enhancing cybersecurity defenses: A multicriteria decision-making approach to mitre attack mitigation strategy. *International Journal of Computer Networks and Communications*, *16*(4), 19–35. Scopus. https://doi.org/10.5121/ijcnc.2024.16402

Mohd Kassim, S. R. B., Li, S., & Arief, B. (2023). Understanding how national csirts evaluate cyber incident response tools and data: Findings from focus group discussions. *Digital Threats: Research and Practice*, *4*(3). Scopus. https://doi.org/10.1145/3609230

Molla-Esparza, C., Gómez-Núñez, M. I., & García-García, F. J. (2025). Applications for learning analytics in the study of academic performance in higher education: A pilot-tested meta-review protocol. *International Journal of Educational Research Open*, *8*, 100433. https://doi.org/10.1016/j.ijedro.2024.100433

Momanyi, C., Riechi, A. R., & Khatete, I. (2024). Digital skills and the use of digital platforms in the informal sector: A case study among Jua Kali artisans in Nairobi in Kenya. *International Journal for Research in Vocational Education and Training*, *11*(1), 96–118. Scopus. https://doi.org/10.13152/IJRVET.11.1.5

Mookherji, S., Odelu, V., Prasath, R., Das, A. K., & Park, Y. (2023). Fog-based single sign-on authentication protocol for electronic healthcare applications. *IEEE Internet of Things Journal*, *10*(12), 10983–10996. Scopus. https://doi.org/10.1109/JIOT.2023.3242903

Motamed, A. (2024). The zero trust security model and its application in organizations. *Journal of Resource Management and Decision Engineering*, *3*(3), 21–32. https://doi.org/https://doi.org/10.61838/kman.jrmde.3.3.3

Mukherjee, M., Le, N. T., Chow, Y.-W., & Susilo, W. (2024). Strategic approaches to cybersecurity learning: a study of educational models and outcomes. *Information*, *15*(2), 117. https://doi.org/10.3390/info15020117

Nguyen, T. D., & Adhikari, S. (2025). Bridging the gap: Enhancing bim education for sustainable design through integrated curriculum and student perception analysis. *Computers*, *14*(11), 463. https://doi.org/10.3390/computers14110463

NIST. (2021). *2020 cybersecurity and privacy annual report*. National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-214

NIST, N. I. of S. and T. (2024). *The NIST cybersecurity framework (CSF) 2.0*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

OECD. (2023). *OECD digital education outlook 2023: Towards an effective digital education ecosystem*. OECD Publishing. https://doi.org/10.1787/c74f03de-en

Ojala, A.-L., Sipola, T., & Saharinen, K. (2025). Cybersecurity awareness and hygiene development in Finnish vocational education: Staff perceptions, training gaps, and diverse learning pathways. *Information and Computer Security*, *34*(1), 66–85. https://doi.org/10.1108/ICS-12-2024-0311

Omirali, A., Kozhakhmet, K., & Zhumaliyeva, R. (2025). Digital trust in transition: Student perceptions of AI-enhanced learning for sustainable educational futures. *Sustainability*, *17*(17), 7567. https://doi.org/10.3390/su17177567

Osazuwa, O. M. C. (2024). *Confidentiality, integrity, and availability in network systems: A review of related literature*. *8*(12). https://doi.org/10.5281/ZENODO.10464076

Osegbue, G. C., Ohamobi, I. N., & Alordiah, C. O. (2025). Enhancing school safety and security: Developing and implementing effective protocols for a secured learning environment. *African Journal of Social and Behavioural Sciences*, *15*(2).

Othman, N., Sarkam, N., Baharun, N., Hoon, T., Masrom, S., Faezah, N., & Abd Rahman, A. S. (2025). Enhancing teachers' digital literacy for security: A systematic review of frameworks and analytical methods in education. *International Journal of Evaluation and Research in Education (IJERE)*, *14*, 4276. https://doi.org/10.11591/ijere.v14i6.32613

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Systematic Reviews*, *10*(1), 89. https://doi.org/10.1186/s13643-021-01626-4

Penberthy, W. J. (2020). *Remediation approaches for the recovery of trust after a privacy breach at an educational institution: An exploratory case study*. Northcentral University ProQuest Dissertations & Theses. ProQuest. https://www.proquest.com/openview/230e94b11e706162d82a9db99069f429/1?pq-origsite=gscholar&cbl=51922&diss=y

Pigola, A., & Meirelles, F. de S. (2025). Zero trust in cybersecurity: Managing critical challenges for effective implementation. *Journal of Systems and Information Technology*, *27*(4), 517–564. https://doi.org/10.1108/JSIT-08-2024-0326

Pittich, D., & Tenberg, R. (2020). Editorial: Hybrid learning landscapes in vocational education. *Journal of Technical Education (JOTED)*, *8*(2), 1–12. https://doi.org/10.48513/joted.v8i2.208

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Protasenko, O., & Ivashura, A. (2022). *Effectiveness and safety of students' work with digital learning ecosystems*. *51*(2), 337-349.

Rafiq, J. E., Namir, A., Zakrani, A., Amraouy, M., & Bennane, A. (2025). A systematic mapping study of the evolution of educational practices using disruptive digital technology. *Journal of Educators Online*, *22*(1). Scopus. https://doi.org/10.9743/JEO.2025.22.1.19

Ragab, M., Alghamdi, B. M., Alakhtar, R., Alsobhi, H., Maghrabi, L. A., Alghamdi, G., Nooh, S., & AL-Ghamdi, A.-M. (2025). Enhancing cybersecurity in higher education institutions using optimal deep learning-based biometric verification. *Alexandria Engineering Journal*, *117*, 340–351. Scopus. https://doi.org/10.1016/j.aej.2025.01.012

Rahmawati, S., Prestridge, S., Abdullah, A. G., & Widiaty, I. (2025). Unpacking the digital competence challenge in vocational education: A case from Indonesia. *Social Sciences & Humanities Open*, *12*, 101803. https://doi.org/10.1016/j.ssaho.2025.101803

Raza, M., Jasim Saeed, M., Riaz, M. B., & Awais Sattar, M. (2024). Federated learning for privacy-preserving intrusion detection in software-defined networks. *IEEE Access*, *12*, 69551–69567. Scopus. https://doi.org/10.1109/ACCESS.2024.3395997

Ren, Y., Wang, Z., Sharma, P. K., Alqahtani, F., Tolba, A., & Wang, J. (2025). Zero trust networks: Evolution and application from concept to practice. *Computers, Materials and Continua*, *82*(2), 1593–1613. Scopus. https://doi.org/10.32604/cmc.2025.059170

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Taherdoost, H. (2024). Towards an innovative model for cybersecurity awareness training. *Information (Switzerland)*, *15*(9). Scopus. https://doi.org/10.3390/info15090512

Tulin, K. (2024). Academic integrity in the digital age: Challenges and assurance strategies. *Visnyk Taras Shevchenko National University of Kyiv. Pedagogy*, *1*, 73–77. Https://doi.org/10.17721/2415-3699.2024.19.12

UNESCO. (2023). *Global education monitoring report 2023, Southeast Asia: Technology in education: A tool on whose terms? - UNESCO Digital Library*. https://unesdoc.unesco.org/ark:/48223/pf0000387214

Vierke, I., Syarief, R., Fahmi, I., & Sailah, I. (2023). Comprehensive framework for addressing the challenges of technology-enhanced learning (TEL). *International Journal of Social Science and Human Research*, *6*(9), 5519–5526. https://doi.org/10.47191/ijsshr/v6-i9-24

Wang, J., Fang, F., Han, G., Wang, N., & Wang, X. (2025). Joint secrecy rate achieving and authentication enhancement via tag-based encoding in chaotic UAV communication environment. *IEEE Internet of Things Journal*, *12*(8), 9491–9507. Scopus. https://doi.org/10.1109/JIOT.2025.3529737

Yusop, M. I. M., Kamarudin, N. H., Suhaimi, N. H. S., & Hasan, M. K. (2025). Advancing passwordless authentication: a systematic review of methods, challenges, and future directions for secure user identity. *IEEE Access*, *13*, 13919–13943. https://doi.org/10.1109/ACCESS.2025.3528960

Zangana, H., Sallow, Z., & Omar, M. (2025). The human factor in cybersecurity: Addressing the risks of insider threats. *Jurnal Ilmiah Computer Science*, *3*, 76–85. https://doi.org/10.58602/jics.v3i2.37