Advances in Artificial Intelligence and Machine Learning; Review 6 (4) 6065-6085 Received 10-05-2026; Accepted 14-08-2026; Published online 21-08-2026

Technologies in Education – Security and Innovations

Nikola Staffenova nikola.staffenova@fri.uniza.sk
University of Žilina,
Faculty of Management Science and Informtics,
Univerzitna 8215/1, Zilina 010 26,
Slovakia.

Dominika Dupakova findrikova@stud.uniza.sk
University of Žilina,
Faculty of Management Science and Informtics,
Univerzitna 8215/1, Zilina 010 26,
Slovakia.

Milan Kubina milan.kubina@fri.uniza.sk
University of Žilina,
Faculty of Management Science and Informtics,
Univerzitna 8215/1, Zilina 010 26,
Slovakia.

Corresponding Author: Nikola Staffenova

Abstract

The article deals with the issue of the security of educational technologies used in formal and informal education in the context of the increasing digitalization of the educational process. The article aim is to identify the greatest security threats, analyze the readiness of educational institutions for the implementation and use of digital technologies in education, and propose recommendations for increasing their security and synthesize knowledge into an integrated conceptual framework for educational technology security. The article uses the method of analysis of secondary sources from professional literature, the method of content analysis, and the method of comparative synthesis of knowledge. It was found that the frequency of cyber incidents is increasing, with personal data leaks and ransomware attacks being among the most common incidents. A striking finding is that educational institutions have insufficient awareness of security and are limitedly prepared for cyber incidents. The reason for this is mainly insufficient funding and a lack of qualified personnel. The proposed recommendations emphasize the importance of an interdisciplinary approach to education, as well as the development of cybersecurity education in educational institutions. Educational institutions are primarily recommended to use modern solutions such as zero-trust architecture, blockchain, and artificial intelligence. The originality of the article lies in pointing out what educational institutions are currently facing and what forms of protection they should use.

Keywords: Education, Technology, Innovations, Security

Citation: Nikola Staffenova, et al. Technologies in Education – Security and Innovations. **Advances in Artificial Intelligence and Machine Learning**. 2026;6(4):336. https://dx.doi.org/10.54364/AAIML.2026.64336

1. INTRODUCTION

The digitalization of educational processes has been facilitated by several events, such as Covid-19. Since then, educational institutions have implemented various digital technologies that were intended to ensure the continuity of education from home as a priority. It started with communication platforms (e.g. MS Teams, Zoom, Webex), educational systems (in Slovakia, e.g. EduPage, LMS Moodle) and continued with applications using artificial intelligence (e.g. Duolingo, Copilot, Kahoot!, Canva, Techambition, WocaBee).

Thanks to such modern digital technologies, the accessibility of education is increasing even for those who cannot attend in person. In addition, education is much more personalized and more effectively managed within the framework of teaching in the form of a hybrid module (both in person and online). The growing trend of using digital technologies also leads to an increase in risks associated, in particular, with the security of such technologies. Individual educational technologies often process personal data (including a special category, the so-called sensitive data) not only of pupils and students but also of teachers, which poses potential cyber threats.

The reason is also the fact that currently only very few educational institutions have established rules in the form of guidelines or policies that clearly state how to work with digital technologies, how to respond to a cyber threat, or what to do if we lose data. This is why attacks in the form of phishing, unauthorized access or user tracking are increasingly aimed at personal data.

Educational institutions often do not know how to react, also because they do not have enough qualified personnel who understand IT and security. Time and financial capacities are also a problem, which prevent them from implementing protective measures. For this reason, the security of educational institutions from the point of view of information security is a strategic issue rather than a technical one. Secure educational technologies influence the trust of pupils and students, as well as their parents and teachers themselves. It also affects the quality of education. Despite this, insufficient attention is paid to this issue.

The article aims to identify the greatest security threats, analyze the readiness of educational institutions for the implementation and use of digital technologies in education, and propose recommendations for increasing their security. The article deals with the issue of educational technologies and their security, taking into account their connection with data protection.

2. THEORETICAL REVIEW

2.1 Educational Technologies: Types, Trends, and Significance

Education represents formal and informal processes in which knowledge is transferred, knowledge, skills and values are developed and critical thinking is promoted. Theoretical frameworks emphasize networked learning, i.e. learning in the digital age. This is education where knowledge exists in information structures outside the individual and learning itself is realized through network connections - data, people, educational institutions [1].

Educational technologies (edtech) represent, according to the Association for Educational Communication and Technology (2024), "the study and ethical practice of facilitating learning and improving performance through the creation, use and management of appropriate technological processes and resources". According to Pascal et al. (2024) [2], these technologies focus mainly on the application of learning psychology and scientific knowledge to effective and high-quality educational processes and practices.

Educational technologies include various digital tools, such as learning management systems (LMS), mobile applications (m-learning), cloud platforms, virtual and augmented reality systems, learning analytics using artificial intelligence, automated assessment, gamification, and virtual laboratories. The connection between education, digital technologies, and their security is currently the subject of several scientific conferences and research, focusing on the areas of artificial intelligence in innovative teaching [3], data security and protection [4], privacy concerns in educational innovative technologies [5], cybersecurity education and awareness [6], as well as ethical aspects of education using artificial intelligence [7]. These areas emphasize that edtech is not only innovative but also a potentially vulnerable framework that requires deep theoretical reflection [2].

Edtech includes:

- Theoretical and systematic approaches (eg, course design, methodology, evaluation).
- Specific tools and platforms: LMS (Learning Management Systems), LRS (Learning Record Stores), virtual environments, e-learning, mobile learning, and adaptive systems.
- Moving towards Education 3.0, where technologies are integrated through neuroscience, cognitive psychology and digital media, enabling personalized and flexible learning.

This implies that edtech is not only about innovative technology, but primarily about a process-oriented, systematic, and contextual approach to education that uses innovative technology as a means to support learning, not as an end in itself.

2.2 Security Challenges: Information and Cybersecurity

Information security (InfoSec) covers the protection of information in all forms (digital and physical) against unauthorized access, destruction, or modification. The basic objectives are known as the CIA Triad: Confidentiality, Integrity, and Availability [8].

Definitions according to various authorities:

- ISO/IEC 27000 (2018): "Preservation of confidentiality, integrity and availability of information." [9]
- CNSS (2010): protection of information systems against unauthorized activities [10].

Cybersecurity is a specific area focused on protecting systems, networks, devices, applications, and data in the cyber environment – eg., the internet and related technologies. ITU-T defines

cybersecurity as a set of tools, policies, concepts, and measures that protect the cyber environment and user assets from threats [11].

Cybersecurity ensures the confidentiality, integrity, and availability of data throughout its lifecycle and protects against threats such as phishing, malware, DoS, encryption, and authentication are common measures [12].

Cybersecurity is essentially a subset of information security, focused exclusively on the digital environment and assets [13].

Educational technologies process a large amount of sensitive data – personal and academic records, health information, academic performance. This makes them an attractive target for cyber attacks. Threats include data leaks, phishing, unauthorized access, surveillance, and misuse of data for commercial or discriminatory purposes. In addition, the practice of unauthorized or ”unsanctioned” use of applications by teachers (so-called shadow IT) increases the risk. A new study examines these risks: teachers often use unsanctioned applications without understanding their security implications for the institution [14].

Educational technologies often process personal data of students, teaching staff, or administrative records. Therefore, they are a natural target for security threats [15]:

- Data vulnerability – leakage of personal and academic information.
- Shadow IT – Using unsanctioned applications without security checks increases the risk (eg, no encryption, authentication).
- Technical attacks – phishing, malware, DoS/DDoS, which can disrupt the functioning of LMS, data storage or portals.

Information and cyber security frameworks applied to edtech include [16]:

1. Implementation of data governance, authentication, and encryption policies.
2. Technological measures: secure API, data transfer protection (SSL/TLS), regular audits, incident response.
3. Educational aspects: training students and teachers on safety principles.
4. Strategic framework: integrating security into edtech design (security by design).

2.3 Security Frameworks, Policies and Education

Connectivism: emphasizes learning through connectivity and digital networks. Edtech is both a means and an environment for learning; security must be integrated into these networks, where learning takes place through real-time data sharing [17].

TPACK (Technological Pedagogical Content Knowledge): a framework that emphasizes that the effective use of technology in teaching requires knowledge of content, pedagogy, and technology.

We should also integrate security knowledge into this framework so that edtech is used safely and effectively [18].

A systematic approach to edtech – theorists such as Luppicini see edtech as a multidisciplinary systemic approach that uses tools, methods, and theories from various fields for the effective design and evaluation of educational systems. Security would be part of this systemic design of educational solutions [19].

Education 3.0: includes flexible, personalized, and technologically connected learning, which also creates new security challenges – mobile learning, adaptive systems, cloud environments – require robust security frameworks [20].

For the effective use of technology in education without security concerns, it is essential to ensure synergy between technological, organizational and educational measures. Otherwise, it is a risk that will affect all stakeholders - teachers, parents, pupils and students [21].

2.4 Interoperability, Standards and Ethical Aspects

Interoperability of educational technologies is the ability of systems, platforms and tools to work together seamlessly, such as exchanging data, sharing content, storing records in compatible formats. In the context of information security, interoperability is very important. Because a lack of standardization can lead to various types of vulnerabilities, incompatible encryption protocols or erroneous data transmission. Key standards in this area are xAPI (Experience API) and SCORM (Sharable Content Object Reference Model). These standards determine the format and method of how user learning data will be collected [21].

Security standards, such as ISO/IEC 27001, which focuses on information security management systems, or GDPR (within the European Union), define the secure handling of personal data, i.e. how institutions should process, store, transfer and protect personal data, not only analog but also digital. These standards require that the system be auditable, that institutions have strict access management, that they encrypt data thoroughly and that they consistently verify the user's identity [22].

When using educational technologies, institutions must also consider ethical considerations related to various technological ethics debates, especially with regard to Artificial Intelligence (AI). Educational institutions are increasingly discussing [23]:

- Privacy of students and teaching staff – especially when using biometric attendance systems (retina scan, fingerprint, photo), psychometric data collection (attitude, intelligence, or personality) or camera-monitored learning.
- Accountability for AI algorithm – when AI is used to assess students or teachers, or when AI is used to recommend content or to automatically diagnose the learning needs of students or teachers.
- AI algorithm bias – educational institutions may obtain biased results due to working with an unbalanced data set, which may ultimately affect educational equity.

- Transparency of decision-making processes – institutions need ”explainable AI” that allows them to understand how, based on what, the AI output was generated.

The ethical aspects of education using AI tools, including concerns about privacy, security and data protection, or blockchain for content authentication and user rights management, are key in the discussion of educational technologies. If educational institutions were to implement blockchain technology, they would be able to record learning outcomes and verify certificates without unauthorized changes, contributing to greater data security and higher trust in online education systems [24]. As a result, there is a need for a framework that connects technology with ethics and that:

- respects fundamental human rights (privacy, equality, freedom of choice),
- promotes transparency and accountability in technology,
- takes into account the consequences of using AI in sensitive environments, such as education undoubtedly is.

The security of educational technologies requires the integration of interoperability, standards, and intuitive design. Key ethical issues include transparency of the educational system and technologies, user privacy, and responsible use of AI. The ethical aspects of educational technologies using artificial intelligence, the fear of loss of privacy, security and data protection, or the management of user rights in the online space and the blockchain used for content authentication, emphasize the need for a theoretical framework that will connect and emphasize the importance of three key elements, namely moral values, transparency and trust [25].

Artificial intelligence significantly interferes with the educational process, which on the one hand enriches it with new possibilities, but on the other hand brings threats to education in the form of cyber attacks. These include, for example, personalized instruction, automated assessment, and the early identification of individual learning needs. However, it is important to keep in mind that the use of artificial intelligence also carries certain security risks. In the field of education, we work with various types of student data that could be misused or manipulated. As a result, AI may unintentionally make biased and non-transparent decisions, and this data could also be compromised if not properly protected. It is therefore important that the use of AI in education be based on several principles. These include, in particular, transparency, explainability, data minimization, human oversight, and compliance with privacy and cybersecurity standards [26, 27].

2.5 Multidisciplinary Approach: Linking Technology, Pedagogy and Safety

Modern educational technologies do not exist in a vacuum – they are both an output and an input to various fields: information technology, pedagogy, learning psychology, data management, and legal frameworks. Therefore, the safe and effective use of edtech solutions requires a multidisciplinary approach that integrates these areas into a single whole [28].

According to approaches such as TPACK (Technological Pedagogical Content Knowledge), teachers must master three pillars: curriculum content, pedagogical strategies, and technology. Today,

digital security is added as a fourth key component that influences the effectiveness and credibility of learning [18].

The connection with security practice is carried out on the basis of three dimensions [29]:

- Technological – which focuses on the selection process of platforms that are considered secure, the implementation of mechanisms designed for user authentication, as well as encryption and regular updates of IT infrastructure.
- Educational – the essence of which is the training of teachers and students in the safe use of technologies, including the rules of safe behavior in the online environment, and last but not least the critical thinking used when working with digital content, especially that generated by AI tools.
- Organizational – the essence of which lies in the management of access rights, the setting of incident response processes and communications between senior staff and technical administrators or digital coordinators.

Research by the European Union Agency for Cybersecurity - ENISA (2024) [30], points to the fact that many schools and universities have implemented educational technologies, but they lack clearly defined security policies. This leads to discrepancies between the technical security and capabilities of schools on the one hand and the pedagogical practice of teachers on the other.

The rapid development and evolution of educational technologies has made it important to consider this issue in a multidisciplinary framework, which consists not only in focusing on technological innovations, but also on their impact on the practice of teachers working in schools or universities, as well as on the organizational structure of educational institutions and, last but not least, on information and cybersecurity [31]. Educational technologies such as AI [32], cloud computing [33], virtual and augmented reality (VR/AR) [34], learning management systems (LMS) [35], or mobile learning (m-learning) are key tools for educational institutions to increase the efficiency, personalization and accessibility of education [36]. However, they also present challenges in the areas of cybersecurity and ethics.

Potential threats such as loss or misuse of personal data, poor IT infrastructure, and inadequate policies highlight the need for systematic protection of information assets in educational institutions. These threats are not only technical in nature, but are also closely related to the culture of the educational institution, legislation and the level of digital literacy of stakeholders [37].

Therefore, the educational and organizational context plays a key role. Managing cyber risks requires consistent technical measures, raising security awareness, developing policies and regular training focused on the security and ethical aspects of the use of educational technologies. Promoting digital literacy and critical thinking among stakeholders is among the key prerequisites for the successful and secure implementation of educational technologies [38].

Another important aspect is the aforementioned interoperability of systems and support for open-access standards, which ensure rapid data exchange and reduce technology dependence on proprietary solutions. Therefore, blockchain technologies are increasingly being discussed, as one of

the tools for ensuring the integrity, availability and confidentiality of data, or the verifiability of certificates [39].

When evaluating and implementing educational technologies, a multidisciplinary approach must be applied that takes into account technological, pedagogical and security aspects. Only in this way can the digitalization of education be achieved not only by the formal introduction of digital technologies, but by a transformation supporting inclusiveness, quality and trust in the educational process [40].

One of the biggest trends in educational technology is the integration of artificial intelligence into educational platforms. This ensures personalization of education and increases security thanks to systems for detecting and identifying suspicious user behavior. Adaptive educational systems can monitor various patterns of user behavior and their interactions, which allows for early detection of integrity violations or identification of suspicious logins. Such systems contribute to the prevention of security incidents [41]. Holmes et al. (2022) [42], argue that an intelligent and digital educational environment can combine the goals of teachers and education with security goals, thus creating a safe educational environment that respects ethics and legislation.

Artificial intelligence should not be introduced into education only as a tool to improve the results of pupils and students, or the educational process itself. It should be seen as a pedagogical and ethical aspect that requires an assessment from the technical and legal fields. Educational institutions should be cautious when working with AI and devote enough time to working with AI and its outputs. Because it is important what data AI collects, what outputs result from it and how these outputs influence the decision-making of teachers themselves. Monitoring users who rely exclusively on artificial intelligence without critically evaluating its outputs is also important. Therefore, educational institutions should support cooperation between IT specialists, digital coordinators, lawyers, ethicists, institutional management and educators [43, 26].

Another trend is the implementation of blockchain, which is mainly used in the management of educational data. This technology allows for the storage of records without changes and the verification of the authenticity of digital certificates. Thanks to it, it is possible to increase transparency and reduce the risk of possible fraud or unauthorized manipulation of data [44]. Wang et al. (2024) [45], argue that blockchain allows for the decentralization of data management, thereby strengthening the control of all users over their own data. Blockchain, together with encryption, can create a reliable digital infrastructure. Nowadays, gamification is increasingly being incorporated into educational processes, which can diversify mandatory training so that the user enjoys the training and learns something from it.

3. METHODOLOGY

The article presents a qualitatively oriented review research based on the analysis of secondary scientific sources. The research has the character of a structured narrative literature review, which is intended to synthesize current knowledge in the field of educational technology security, identify the main security risks, analyze the preparedness of educational institutions and formulate recommendations for the secure implementation of digital technologies in education.

Given the interdisciplinary nature of the research topic, the aim was to connect knowledge from the fields of information security, cybersecurity, pedagogy, information technology and digital education. The chosen research design allowed for the identification of common trends, recurring security issues and recommended approaches across individual scientific disciplines.

The aim of the article is to identify the biggest security threats, analyse the preparedness of educational institutions for the implementation and use of digital technologies in education and propose recommendations for increasing their security. The article deals with the issue of educational technologies and their information and cyber-security with regard to their connection with data protection.

This part of the research is descriptive and analytical in nature, based on a combination of secondary data analysis and expert content analysis of relevant literature.

The search for scientific sources was carried out using the Web of Science, SpringerLink, IEEE Xplore and Google Scholar databases (TABLE 1.). These databases were chosen due to their broad coverage of scientific publications in the fields of information technology, information security, pedagogy, artificial intelligence and educational technologies.

Table 1: Keyword selection

Field	Terms used
EdTech	educational technology, edtech, digital learning
Security	cybersecurity, information security
AI	artificial intelligence, AI in education
LMS	learning management system, LMS
Data	privacy, data protection, GDPR
Emerging technologies	blockchain, cloud computing

The search combined individual keywords using logical operators (“and”). Publications from the time range 2018–2025 were analyzed, with older works included only in cases where they represented significant theoretical foundations (e.g. definitions or basic conceptual frameworks). Literature selection consisted of four consecutive phases: initial database search, removal of duplicate records, screening of titles and abstracts, and evaluation of the full text according to predefined inclusion and exclusion criteria (TABLE 2).

In preparing this article, we used a number of qualitative scientific methods:

- Analysis of secondary sources – was conducted based on scientific articles, reports, and research publications available through databases such as Web of Science, Google Scholar, SpringerLink, and IEEE Xplore. Emphasis was placed on sources focused on edtech, cybersecurity, and digital ethics.
- Content analysis – focused on identifying thematic areas in published surveys and expert reports (eg ENISA, EDUCAUSE, UNESCO, OECD) that relate to security threats in education and data management.

- Qualitative synthesis – was used to integrate knowledge from various professional domains: information security, educational technology, and pedagogy. This synthesis enabled the development of a multidisciplinary framework, which is presented in the theoretical part.
- Comparison of data from selected studies and surveys – enabled comparison of the readiness of educational institutions in the area of edtech solution security.

Table 2: Inclusion and exclusion criteria

Inclusion criteria	**Rationale**
Peer-reviewed journal articles	Scientific quality
Conference papers	Current technologies
International reports	Practical recommendations
English language	Consistency of analysis
Full text	Possibility of content analysis
EdTech safety	Consistency with the aim of the article
Exclusion criteria	**Rationale**
Duplicates	Removed
Outside the scope of educational technologies	Unrealted to RQ
No cybersecurity or information security focus	Did not meet article objective
Short abstracts	Insufficient data

The selected publications were assessed according to several quality criteria to increase the credibility of the review. The assessment focused on relevance to the research objective; scientific quality of the publication, with preference given to articles from peer-reviewed journals and internationally recognized institutional reports; timeliness of the publication; and finally, contributions to answering the defined research questions. This quality assessment supported the selection of literature used for the thematic synthesis.

Following data extraction, recurring themes were identified and then grouped into thematic categories that corresponded to the aim of the article. These thematic clusters formed the basis for the synthesis of knowledge presented in the results.

Based on the identified gaps in the scientific literature and the stated aim of the article, the following research questions were formulated:

- RQ1: What are the most common security threats and risks associated with the use of educational technologies and applications today?
- RQ2: To what extent are educational institutions prepared to face these risks in terms of technological, organizational, and personnel security?
- RQ3: What are the recommended practices, standards, and approaches that can help integrate security measures into the design and use of educational technologies?

The study is based on the analysis of secondary sources, therefore the results do not represent empirical verification of individual security measures. The aim was to synthesize existing knowledge and

identify common trends across the scientific literature. Future research should verify the proposed concept through empirical case studies or questionnaire research.

This methodological concept enabled the development of a multidisciplinary evidence-informed synthesis of current knowledge on thesecurity of educational technologies, with the findings presented in the following section. Transparency in describing the strategy for how articles were searched, as well as the establishment of selection criteria, data extraction, and thematic synthesis, was intended to improve the reproducibility of the review process.

4. RESULTS

The results are organized according to the three research questions set out in the methodology. Their interpretation is supported by the proposed Integrated Security Framework for Educational Technologies (Figure 1.), which provides a multidisciplinary perspective on the technological, organizational, and educational aspects of cybersecurity in digital learning environments.

RQ1: What are the key security threats and risks currently linked to the use of educational technologies and digital learnings applications?

- Shocking frequency of attacks – The education sector was among the most affected: in Q2 2025, there were an average of 4,388 cyberattacks per week per organization—more than double the global average [46].
- The trend of increasing data leaks – According to the Verizon DBIR report, 1,075 security incidents were recorded in 2025, of which 851 were confirmed as data breaches. Approximately 80% of these cases were caused by system intrusion, human error, or phishing [46].
- Ransomware attacks are exploding – In the lower (K 12) segment, the incidence was 80% of institutions, while in 2024, up to 97% of universities reported attacks, with up to 66% of them confirming ransomware attacks. The cost of incidents runs into millions – the average cost of a data breach is up to $3.65 million; other statistics cite figures of up to $3.79 [46].
- Neglecting policies and training – Vısledky sú, že samotné technické opatrenia nie sú postaèujúce bez systematického rozvoja bezpečnostného povedomia a kybernetickıch kompetencií použíl'ov. Kybernetická bezpečnos vo vzdelávaní si vyžaduje pravidelné vzdelávanie, rozvoj praktickıch zruèností a aktívne zapojenie uèitel'ov, rodièov a ïalších aktérov do budovania bezpečnostnej kultúry [47].
- Shadow IT poses real risks – Educators often use unsanctioned applications despite security risks; less than a third were familiar with internal policies, and many knowingly violated them.

Key finding (RQ1): Educational institutions are increasingly exposed to sophisticated cyber threats, the successful mitigation of which requires coordinated technological, organizational, and educational measures.

The findings suggest that cyber threats affecting educational technology should not be viewed as isolated technical incidents, but rather as manifestations of systemic weaknesses in the digital trans-

formation of education. The high incidence of phishing attacks, ransomware, data breaches, and shadow IT demonstrates that technological innovations have often outpaced the implementation of adequate security management and user awareness. As the proposed framework illustrates (Figure 1), the identified threats form the first layer of the security ecosystem and create requirements for coordinated technological, organizational, and educational responses, rather than isolated technical countermeasures.

RQ2: To what level are educational institutions prepared to face these risks from a technological, organizational, and personnel perspective?

- Preparedness vs. Unpreparedness – according to the CDW 2024 Cybersecurity Report, 61% of institutions said they were ”very” or ”somewhat prepared” to handle incidents, while 28% said the opposite [48].
- Insufficient professional teams and budgets – only 10% of respondents described their organization as fully staffed; as many as 13% reported a significant shortage of staff, and 40% described the situation as below average. More than 38% do not use outsourcing in the area of IT security, which increases pressure on the internal team [48].
- Concerns about financial and reputational impacts – 22% of those who were able to estimate the damage said that the attack cost them between $1 million and $5 million [48].
- Insurance as a preparedness tool – 47% use cyber insurance as part of their strategy, but 21% still have no insurance whatsoever [48].
- Visibility and technical measures – 78% of respondents believe they have sufficient insight into the cyber status of their organization; they identified cloud security posture management and identity and access management (IAM) as effective tools (~74% of respondents) [48].

Key finding (RQ2): The readiness of educational institutions is limited primarily by organizational capacity, rather than the absence of technological solutions.

The results reveal a significant gap between the perceived preparedness of educational institutions and their actual organizational capabilities. While many institutions report having put in place basic technical safeguards, significant gaps remain in staffing, financial resources and long-term security planning. This suggests that cybersecurity preparedness cannot be assessed solely on the basis of the presence of technical controls, but also needs to consider governance mechanisms, institutional capacity and human resources. These findings correspond to the dimensions of governance and organization, highlighting that effective cybersecurity requires strategic management alongside technological implementation.

RQ3: What best practice guidelines, standards, and approaches support the effective integration of security measures into the development and use of educational technologies?

- Interdisciplinary frameworks and training – ENISA highlights the need to expand the number of study programs for cybersecurity; the number of graduates is expected to double in the next 2–3 years, but with a low representation of women (~20%). Initiatives such as the European Cybersecurity Challenge, which stimulate talent and awareness among young people in the field of cybersecurity, are also supported [30].

- Policies for AI use – Ghimire & Edwards (2024) [49] identify a significant gap in ethical and specific policies for AI deployment in schools (more than 60% of policies are incomplete in terms of AI); measures often lack essential elements such as data protection and algorithm transparency.
- Security literacy and protection culture – need for clear internal policies and communication, as more than 70% of teachers often use tools that pose a security risk because they ignore internal security rules for software use.
- Technological solutions such as zero trust, IAM, and cloud security – CDW research has highlighted the effectiveness of IAM and cloud security in increasing visibility and control; however, only 23% of institutions have adopted the zero trust model (compared to 42% in other sectors) [48].

Key finding (RQ3): The most effective cybersecurity strategies combine governance, technological safeguards, and ongoing cybersecurity education within a unified institutional framework.

The proposed recommendations for RQ3 demonstrate that effective cybersecurity in educational technology requires the integration of complementary measures, rather than relying on individual technological solutions. While approaches such as zero-trust architecture, identity and access management, cloud security, and artificial intelligence contribute significantly to technical protection, their effectiveness depends on institutional governance, clearly defined security policies, and ongoing cybersecurity education of teachers, students, and administrators. The proposed conceptual framework therefore emphasizes that sustainable cybersecurity in education is only achieved through a balanced interaction of technological, organizational, and educational dimensions.

The literature synthesis shows that cybersecurity in educational technology represents a multidimensional challenge that goes far beyond the implementation of isolated technical safeguards. The results consistently indicate that educational institutions face a combination of technological vulnerabilities, organizational constraints, and a lack of cybersecurity awareness among users. These factors reinforce each other and collectively reduce institutional resilience to increasingly sophisticated cyber threats.

The proposed framework provides an integrated interpretation of these findings by linking identified security risks to governance mechanisms, technological protection measures, and educational interventions. This multidimensional perspective emphasizes that effective protection of educational technology requires coordinated implementation across all three dimensions, rather than isolated investments in technical infrastructure.

Overall, the results suggest that strengthening cybersecurity in education should focus not only on adopting advanced technologies such as Zero Trust, artificial intelligence or blockchain-based solutions, but also on developing institutional governance, security culture and digital competencies of all stakeholders involved in the educational process.

Based on the synthesis of the analyzed scientific literature, an integrated conceptual framework for the security of educational technologies (Figure 1.) was proposed. The framework represents the author's synthesis of knowledge identified in the analyzed studies and connects technological, organizational and pedagogical aspects of the security of educational technologies into a single

logical model. Unlike most published approaches that focus only on individual areas (e.g. technological security, risk management or development of digital competencies), the proposed framework emphasizes their interconnectedness and the need for coordinated implementation.

The model also reflects the three research questions formulated in this article. The individual layers of the framework depict a logical flow from the educational technologies used through the identification of security risks, security management and implementation of protective measures to organizational and pedagogical support that leads to the creation of a safe and trustworthy digital educational environment. The proposed framework does not represent a new security standard, but an integrative conceptual model that emerged from the synthesis of knowledge presented in the analyzed literature.

FIGURE 1. shows the proposed conceptual framework, which consists of six interconnected layers. The first layer represents the main categories of educational technologies used in today's digital education. The second layer identifies the most significant security threats and risks associated with their use, thus directly reflecting the research question RQ1.

The next two layers represent the technological and organizational dimensions of security. The Security Governance and Policies layer emphasizes the importance of strategic security management through policies, standards, legislative requirements and risk management, while the Security Implementation Controls layer represents specific technical measures, such as Zero Trust architecture, identity and access management, data encryption, cloud service protection or the use of artificial intelligence in monitoring security incidents. These layers are directly related to the research question RQ2, which examines the readiness of educational institutions from a technological and organizational perspective.

The fifth layer represents the pedagogical dimension, which includes the development of digital literacy, cybersecurity education for educators and students, promotion of a security culture, ethical use of technology, and commitment of educational institution leadership. This dimension emphasizes that technological measures alone cannot provide an adequate level of protection without sufficient user readiness.

The final layer represents the expected benefits of implementing the framework in the form of increased confidentiality, integrity, and availability of data, increased resilience of educational institutions to cyber incidents, strengthened user trust, and support for a sustainable digital transformation of education. At the same time, the framework creates a logical connection between all three research questions and provides a unified view of educational technology security from a technological, organizational, and pedagogical perspective.

Overall, the results show that the security of educational technologies cannot be ensured by the isolated implementation of technical measures. The identified threats, the level of preparedness of educational institutions, and the recommended security measures create an interconnected system that is captured in the proposed ISF-EdTech framework. This framework emphasizes the need for coordination of technological, organizational, and pedagogical measures in managing the security of the digital educational environment.

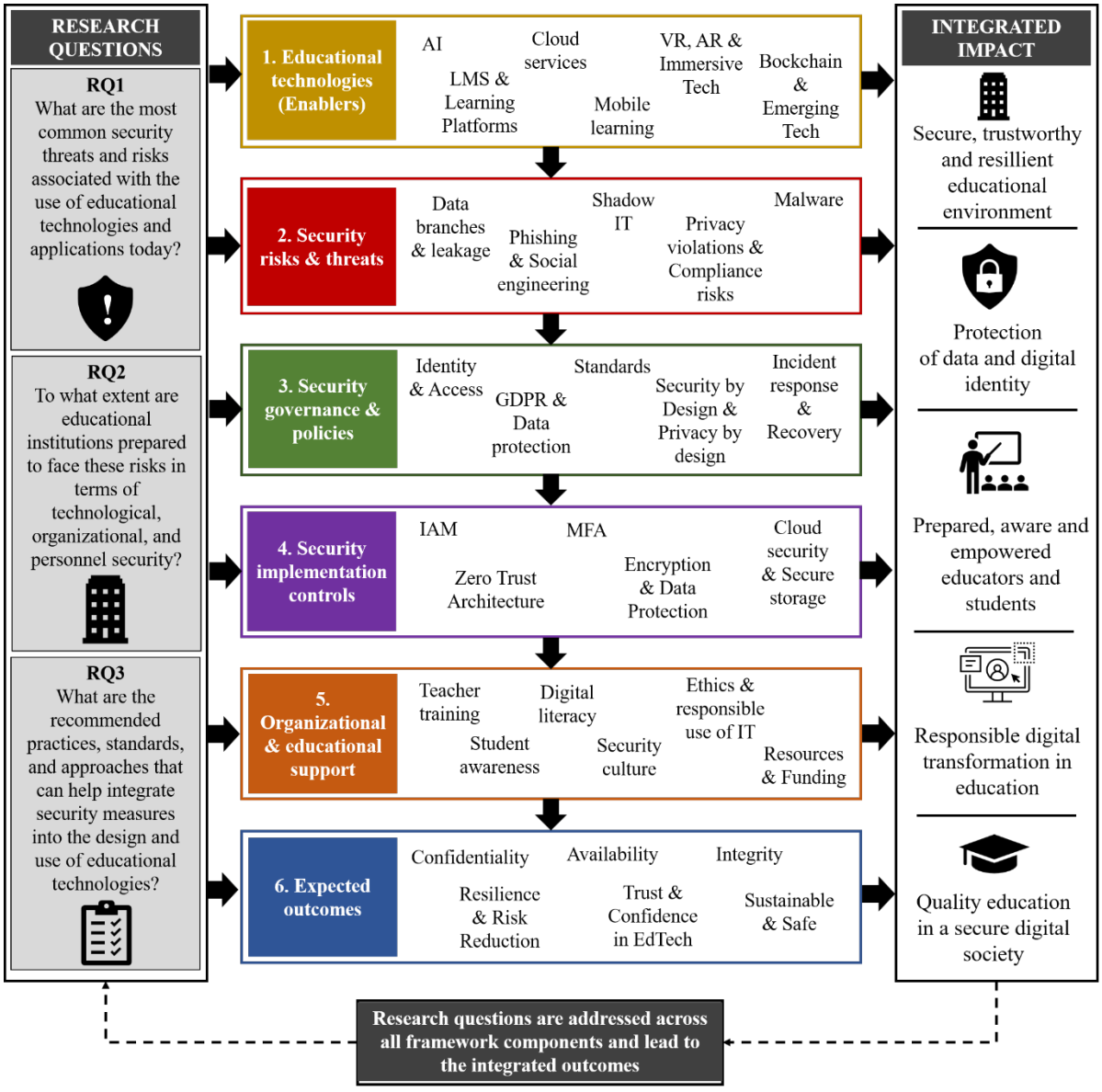

Figure 1: Integrated Multidimensional Security Framework for Educational Technologies

5. DISCUSSION AND CONCLUSION

The results show that educational technology security can no longer be seen as a technical issue alone. Most of the identified incidents arise from a combination of technological vulnerabilities, inadequate security management, and low levels of user security awareness. This suggests that successfully protecting digital learning environments requires a coordinated approach that combines technological, organizational, and pedagogical measures.

These findings also support the proposed conceptual framework (Figure 1.), which links the technological, organizational, and pedagogical dimensions of security into a single integrated model. The results suggest that long-term resilience of educational institutions cannot be achieved by isolated technical measures, but only by their coordinated implementation across all three dimensions.

The results of the analyzed literature clearly confirm that the current challenge for the education sector is the security of educational technologies and applications. The high rate of cyber attacks specifically on the education sector and frequent data leaks reveal the vulnerability of educational institutions that lack sufficient qualified personnel and financial resources for effective prevention and defense.

The results also point to the fact that the technological development of educational institutions is proceeding faster than the development of their security management. The implementation of cloud services, artificial intelligence and digital platforms brings significant benefits to the educational process, but at the same time expands the scope for new types of cyber threats. This confirms the need to integrate security requirements into the process of design, implementation and operation of educational technologies (security by design).

Shadow IT and low levels of security literacy among educators highlight the need for systematic and lifelong learning and clearly defined internal security policies. In addition, slow implementation of security models and lack of outsourcing can increase the risk of cyber incidents. The analysis also suggests that the human factor remains one of the most important determinants of cybersecurity success. Even a technologically well-secured environment can be significantly weakened by an insufficient security culture, the absence of regular training, or low compliance with internal security rules.

On the positive side, there is a growing interest in cyber incident insurance and an increase in trust in digital educational technologies. Educational programs and initiatives, such as the European Cyber Security Challenge, represent a positive step towards reducing security incidents. However, ethical aspects remain insufficiently supported and respected. Equally important is the creation of clear rules for the use of artificial intelligence in education. Without defined ethical principles, transparency of algorithms, and protection of personal data, the implementation of AI may create new security and legal risks despite its significant potential to support education. Their integration into legislation and organizational policies is very important, especially for building user trust and responsible use of educational technologies.

The analysis showed that the security of educational technologies is a multidimensional problem, the solution of which requires the simultaneous operation of technological, organizational and pedagogical measures. It is their mutual integration that constitutes the main benefit of the proposed framework, which provides a unified view of the security management of the digital educational environment.

Based on the synthesis of the analyzed scientific studies and the identified security challenges, the individual recommended measures were supplemented with their practical aspects of implementation. The aim is not to propose a new security standard, but to systematically summarize the recommended approaches from the literature, along with their possible limitations and examples of indicators that educational institutions can use to assess the effectiveness of implemented security

measures (TABLE 3.). The review prepared in this way also expands the interpretative value of the results and connects the recommendations with their practical application.

Table 3: Practical implementation framework for recommended security measures

Recommended measure	Practical implementation	Limitations	Success indicator
Zero Trust	MFA, IAM	Network segmentation, higher costs	Decrease in unauthorized access
IAM	Central identity management	Administrative complexity	Number of compromised accounts
AI	Anomaly detection	False positives	Incident detection time
Blockchain	Certificate verification	Interoperability	Record integrity
Security awareness	Regular training	Time complexity	Phishing test success
Governance	Internal policies, audits	Resistance to change	Audit results

Successful implementation of security measures requires not only the introduction of appropriate technologies, but also consideration of organizational, personnel and economic aspects of their implementation. Individual measures complement each other and their effectiveness depends on coordinated implementation throughout the organization. The proposed indicators also represent examples of measurable indicators that can support the ongoing assessment of the level of cybersecurity and the identification of areas requiring further improvement.

One of the main contributions of this work is the creation of an integrative conceptual framework (Figure 1.), which was created by synthesizing the knowledge identified in the analyzed literature. The proposed framework connects the technological, organizational and pedagogical dimensions of educational technology security into a unified model that allows for a more comprehensive interpretation of the identified security risks, the preparedness of educational institutions and the recommended security measures. The framework also provides a basis for future empirical verification and assessment of the level of cyber preparedness of educational institutions.

The strengths of the article are the analysis of current scholarly articles and the integration of interdisciplinary knowledge with an overview of security challenges in educational technologies. The contribution of the article also lies in the creation of an integrative conceptual framework, which connects knowledge from the fields of information security, pedagogy, and educational technologies and can serve as a basis for future empirical verification. Limitations include the analysis of secondary sources, without primary research, which is planned for the near future. As well as the rapid increase in changes in the technological environment, which requires constant updating of the findings.

Future research should focus on a specific analysis of the conditions of educational technology security in a real educational institution. This would contribute to the specific design of a security framework that would integrate new technologies, security culture and would also take into account

ethical principles. The financial side of the educational institution and the volume of investments in cybersecurity education in schools will also play an important role. Future research should also focus on validating the proposed framework through case studies, questionnaire research, or assessments of the level of cyber readiness of educational institutions. Such empirical validation will allow assessing the practical applicability of the proposed model and identifying opportunities for its further development.

Security of educational technologies must be considered an integral part of the digital transformation of education. Sustainable digital education cannot be achieved through technological innovation alone, but requires a balanced combination of technological safeguards, effective organizational management, and continuous development of cybersecurity competencies among all participants in the educational process. The proposed framework provides a conceptual basis for achieving this goal and creates opportunities for future empirical research and practical implementation.

References

[1] Sadiqzade Z, Alisoy H. Cybersecurity and Online Education – Risks and Solutions. Lumin Appl Sci Eng. 2025;2:4-12.

[2] Pascal UO, Cadet E, Osundare OS, Fakeyede GO, Ige BA, et al. The Crucial Role of Education in Fostering Sustainability Awareness and Promoting Cybersecurity Measures. Int J Frontline Res Sci Technol. 2024;4:018-034.

[3] Yu HT, Mi Y. Application Model for Innovative Sports Practice Teaching in Colleges Using Internet of Things and Artificial Intelligence. Electronics. 2023;12:874.

[4] Papic A, Radoja KK, Szombathelyi D. Cyber Security Awareness of Croatian Students and the Personal Data Protection. 11th international scientific symposium Region, Entrepreneurship, Development (RED 2022). Sveučilište Josipa Jurja Strossmayera u Osijeku, Ekonomski fakultet u Osijeku. 2022:563-574.

[5] Solak Ü, Solak TK, Yurttaş A. Nursing Students' Attitudes Toward Metaverse Applications and Their Online Privacy Concerns: A Correlational Study. BMC Nurs. 2025;24:1465.

[6] Martin F, Zhuang M, Byker E, Wang WC, Bacak J, et al. Multimedia-Based Cybersecurity and Privacy Professional Development on Educational Technology for K-12 Personnel. Educ Technol Res Dev. 2025;74:849-873.

[7] Marougkas A, Troussas C, Krouska A, Sgouropoulou C, Voyiatzis I. Virtual Reality in Classrooms: Addressing Ethical Challenges in Educational Technology. Novel Intelligent Digital Systems Conferences. Cham: Springer Nature Switzerland. 2024:500-506.

[8] Kotrikadze G. Information Security and Cyber Security. Georgian Sci. 2023;5:322-333.

[9] https://www.iso.org/standard/73906.html

[10] https://data.socialsciences.cornell.edu/dataset.xhtml?persistentId=doi:10.6077/J5/MN8VF8

[11] Ismail T, Gayathri P. Navigating the Digital Frontier: A Comprehensive Analysis of Cybersecurity and Information Security in the Modern Era. I-manager J Digit Forensics Cyber Sec. 2024;2:1-9.

[12] Wagner N, Damodaran SK, Reavey M. Towards Optimal Sensor Placement for Cybersecurity: An Extensible Model for Defensive Cybersecurity Sensor Placement Evaluation. Sensors. 2025;25:6022.

[13] Salminen M, Candelin N, Cullen K, Latvanen S, Lindroth M, et al. Cybersecurity Education in European Higher Education Institutions. 9th International Conference on Higher Education Advances. 2023:1357-1364.

[14] Hernández RM, Ugaz DW, Tarrillo DS, Vasquez DS, Ordoñez SE, et al. Exploring Software Infrastructures for Enhanced Learning Environments to Empowering Education. J Wirel Mob Netw Ubiquitous Comput Dependable Appl. 2024;15:231-243.

[15] Bozkurt A. Educational Technology Research Patterns in the Realm of the Digital Knowledge Age. J Interact Media Educ. 2020;2020:18.

[16] Adams C, Groten S. A Technoethical Framework for Teachers. Learn Media Technol. 2023;49:701-718

[17] Cueva Delgado JL, García Chávez A, Martínez Molina OA. El Conectivismo Y Las Tic: Un Paradigma Que Impacta El Proceso Enseñanza Aprendizaje. Rev Sci. 2019;4:205-227.

[18] Esposito M, Moroney R. Teacher Candidates Perception of Acquiring Tpack in the Digital Age Through an Innovative Educational Technology Masters Program. J. Leadersh. Instr. 2020;19:25-30.

[19] Luppicini R. A Systems Definition of Educational Technology in Society. Educ Technol Soc. 2005;8:103-109.

[20] Borden JD. Education 3.0: What Is It and How Do We Achieve It?. Education 3.0 and eLearning across modalities. IGI Global Scientific Publishing. 2022:1-24.

[21] Marshall R, Pardo A, Smith D, Watson T. Implementing Next Generation Privacy and Ethics Research in Educational Technology. Br J Educ Technol. 2022;53:737-755.

[22] Chituc CM, Rittberger M. Understanding the Importance of Interoperability Standards in the Classroom of the Future. IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society. IEEE. 2019:6801-6806.

[23] Pulijala SK. Ethical Considerations in Educational Technology: Balancing Innovation and Responsibility. Int J Sci Res Comput Sci Eng Inf Technol. 2024;10:315-325.

[24] Savelyeva T, Park J. Blockchain Technology for Sustainable Education. Br J Educ Technol. 2022;53:1591-1604.

[25] Krutka DG, Heath MK, Willet KB. Foregrounding Technoethics: Toward Critical Perspectives in Technology and Teacher Education. J Technol Teach Educ. 2019;27:555-574.

[26] Alfiras MI, Emran AQ, Mohamed AM. Ethics and Governance of Generative AI in Education: A Systematic Review on Responsible Adoption. Discov Educ. 2026;5:37.

[27] García-López IM, Trujillo-Liñán L. Ethical and Regulatory Challenges of Generative AI in Education: A Systematic Review. Front Educ. 2025;10:1565938.

[28] Hosseini Z, Kinnunen J. Integration of Pedagogy Into Technology: A Practical Paradigm. In: Education and New Developments. In Science Press. 2021:406-410.

[29] Fournier E, Sedaghatjou M, Namukasa I. Connect to Learn: Assemblage of Pedagogies in Higher Education in a Community of Practice. OTESSA J. 2021;1:1-19.

[30] https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

[31] Bello-Pintado A, Bianchi C. Educational Diversity, Organizational Structure and Innovation Performance: Evidence From Uruguayan Industry. Estud Econ. 2018;45:203-229.

[32] Kuklin O, Ivanova İ, Borovyk T. Modelling Artificial Intelligence Integration Into Educational Environment. Information technologies and learning tools (ITLT). 2024;103:207-232.

[33] Naved M, Sanchez DT, Dela Cruz AP, Peconcillo LB, Peteros ED, et al. Identifying the Role of Cloud Computing Technology in Management of Educational Institutions. Mater Today Proc. 2022;51:2309-2312

[34] Al-Salami SB. An Account of Virtual and Augmented Reality in Educational Institutions. Int J Comput Sci Netw Secur. 2022;22:137-142.

[35] Piña AA. An Educational Leader's View of Learning Management Systems. Leading and managing e-learning: What the e-learning leader needs to know. Cham: Springer International Publishing. 2017:101-113.

[36] Salhab R, Daher W. The Impact of Mobile Learning on Students' Attitudes Towards Learning in an Educational Technology Course. Multimodal Technol Interact. 2023;7:74.

[37] Bozza TC, Vinha TP. Cyberbullying, Cyber Agressão E Riscos On-Line: Como a Escola Pode Atuar Diante Dos Problemas Da (Cyber) Convivência. Rev Ibero-Am Estud E. 2023;18:e023059.

[38] Pötzsch H. Critical Digital Literacy: Technology in Education Beyond Issues of User Competence and Labour-Market Qualifications. TripleC. 2019;17:221-240.

[39] Stewart MS, Pier E, Ralyea D, Rice A. Interoperability and Data Standards in the K-12 Education Sector: Intersections With Data Justice. Learn Media Technol. 2023;48:324-336.

[40] Li WH. A Comparative Study of Multidisciplinary Education Models in Science, Technology, and Arts: Global Perspectives and Practices. In International Conference on Human-Computer Interaction. Cham: Springer Nature Switzerland. 2025:364-377.

[41] Reddy P. The Current State of AI Education: Security as an Afterthought. Proceedings of the 26th ACM Annual Conference on Cybersecurity & Information Technology Education. 2025:233-239.

[42] Holmes W, Porayska-Pomsta K, Holstein K, Sutherland E, Baker T, et al. Ethics of AI in Education: Towards a Community-Wide Framework. Int J Artif Intell Educ. 2022;32:504-526.

[43] Kamali J, Alpat MF, Bozkurt A. AI Ethics as a Complex and Multifaceted Challenge: Decoding Educators' AI Ethics Alignment Through the Lens of Activity Theory. Int J Educ Technol High Educ. 2024;21:62.

[44] Al Samarai B, Morato J. The Use of Blockchain Technology in the Educational Field in Bahrain. In International Congress on Blockchain and Applications. Cham: Springer Nature Switzerland. 2023:527-535.

[45] Wang X, Younas M, Jiang Y, Imran M, Almusharraf N. Transforming Education Through Blockchain: A Systematic Review of Applications, Projects, and Challenges. IEEE Access. 2025;13:13264-13284

[46] Li J, Xiao W, Zhang C. Data Security Crisis in Universities: Identification of Key Factors Affecting Data Breach Incidents. Humanit Soc Sci Commun. 2023;10:270.

[47] Manganello F, Earp J, Fante C, Bassi G, Fabbri S, et al. Shaping the Foundation of the Supercyberkids Learning Framework: A Comprehensive Analysis of Cybersecurity Education Initiatives. Front Educ. 2024;9:1375853.

[48] https://edtechmagazine.com/higher/article/2024/06/survey-reveals-top-cybersecurity-issues-education?utm

[49] Ghimire A, Edwards J. From Guidelines to Governance: A Study of AI Policies in Education. Artificial Intelligence in Education. Posters and Late Breaking Results, Workshops and Tutorials, Industry and Innovation Tracks, Practitioners, Doctoral Consortium and Blue Sky. AIED 2024. Communications in Computer and Information Science. 2024;2151:299-307.