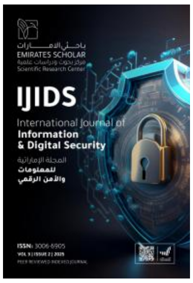

International Journal of Information & Digital Security
Vol 3 Issue 2 (2025)
Pages (19 - 32)

Available at
www.emiratesscholar.com

Digital Gaps and Cyber Risks: Strategies to Ensure Equal Opportunities and Digital Education Security

Driss Abbadi
Public Law, Politics, Economics, and Management Laboratory, Faculty of polydisciplinary, Taza, Sidi Mohamed Ben Abdellah University of Fès, Morocco
driss.abbadi@usmba.ac.ma

ARTICLE HISTORY

Received: 21 November 2025.
Accepted: 10 December 2025.
Published: 26 December 2025.

PEER - REVIEW STATEMENT:

This article was reviewed under a double-blind process by three independent reviewers.

HOW TO CITE

Abbadi , D. . (2025). Digital Gaps and Cyber Risks: Strategies to Ensure Equal Opportunities and Digital Education Security. *International Journal of Information & Digital Security*, *3*(2), 19-32. https://doi.org/10.54878/ba2nbk39

ABSTRACT

This research aims to explore strategies for bridging the digital divide that affects equal opportunities in digital education, while ensuring a safe learning environment protected from cyber risks. The study addresses the challenges faced by students in remote and underserved areas in accessing digital resources, along with the growing cybersecurity risks in educational systems. It also seeks to provide technological solutions and educational policies aimed at ensuring the continuity of digital education and protecting the personal data of students and educators. The research relies on a descriptive analytical approach to analyze the impact of digital gaps and cybersecurity risks on the educational process. It also uses a systems approach to study the relationship between improving digital infrastructure and data security. The results show that digital gaps pose a significant challenge to fair access to digital education, while cybersecurity remains a continuous threat to educational institutions, exposing them to risks such as data breaches or cyberattacks. The study also indicates that strategies focusing on improving access to technology and educating students and educators about cybersecurity risks contribute to bridging these gaps and creating a safe learning environment. The research highlights the importance of bridging digital gaps by enhancing digital infrastructure in underserved areas and stresses the need for collaboration between the public and private sectors to provide effective technological solutions. It also emphasizes the necessity of implementing advanced security policies to protect personal data and maintain the confidentiality of academic information amidst growing cybersecurity risks.

Keywords: *Digital Divide, Cybersecurity Risks, Digital Education, Equal Opportunities, Cybersecurity.*

1. Introduction

Amidst the rapid digital transformations occurring in the education sector today, significant opportunities have arisen to enhance the quality of education and broaden access to it. However, these opportunities face fundamental challenges primarily linked to digital divides and cybersecurity risks that could impact the sustainability and effectiveness of digital education. Despite advancements in digital technologies, there is a considerable disparity in the distribution of these technologies across different social groups and sectors, resulting in digital divides that prevent some students from accessing digital educational tools. These divides manifest in various forms, such as geographical divides, where students in remote areas struggle to access high-speed internet or appropriate devices, and economic divides, which hinder low-income students from owning the necessary digital devices, thereby limiting their educational opportunities in comparison to others (Matsieli, M., & Mutula, S., 2024).

In addition to these divides, another issue arises concerning the growing cybersecurity risks that come with the increasing reliance on the internet in the educational process. Cybersecurity presents a critical challenge, given the potential threats to the academic and personal data of both students and teachers. Educational systems could face cyberattacks that lead to the leakage or manipulation of sensitive data, which threatens the credibility of educational institutions and endangers academic privacy (Jawaid, S. A., 2023).

1.1. Importance of the Topic

Digital transformations in the education sector offer vast opportunities to enhance the quality of education and broaden access to it. However, these opportunities are accompanied by significant challenges related to digital divides and cybersecurity risks that could impact the sustainability and effectiveness of digital education. The digital divides between students in remote or low-income areas contribute to disparities in access to digital educational tools. Moreover, the increasing reliance on the internet in education exposes educational systems to cybersecurity threats that endanger the security of sensitive data and put educational institutions at risk of data breaches or cyberattacks. Therefore, studying these divides and developing strategies to ensure equal opportunities and protect cybersecurity is essential to improving the effectiveness of digital education and ensuring its continuity.

1.2. Theoretical Framework

On a theoretical level, the research addresses digital divides by analyzing the challenges faced by students and educational institutions due to unequal access to digital resources. It also explores the cybersecurity risks that threaten the digital security of educational institutions, focusing on technical tools such as encryption and advanced protection techniques that can safeguard academic and personal data. Furthermore, the research delves into theoretical frameworks related to the development of educational policies that raise awareness of cybersecurity risks and preventive measures. The goal is to construct educational models that consider the digital impacts from a scientific perspective, contributing to the formulation of effective solutions to these challenges.

1.3. Practical Implications

On a practical level, the research discusses actionable strategies for bridging the digital divides and ensuring equal access to digital education. This includes improving digital infrastructure in underserved areas and providing technical support to students in these regions. The research also emphasizes the importance of fostering digital literacy among both students and teachers, which will increase awareness of how to use digital tools securely and effectively. In the realm of cybersecurity, the research explores the implementation of protection technologies such as encryption and continuous monitoring within educational institutions, as well as the adoption of advanced security policies to ensure the protection of personal and academic data.

1.4. Previous Studies

Previous studies in this context are of great importance for understanding the impact of digital transformations on culture, education, and cybersecurity. In this regard, the book *"Digital Culture: The Changing Dynamics"* by Alexandra Ozilatch and Biserka Kvitichanin is a comprehensive study on the impact of information and communication technology on culture and creativity. The book discusses the transformations brought about by the digital revolution in our understanding of culture, the intersection of culture and technology, and how the internet affects cultural diversity and intercultural interaction. It also addresses the challenges posed by cultural policies in the face of digital transformations and their impact on traditional cultural identities. The book provides an innovative vision of the cultural future in the digital age.

In the field of cybersecurity, the study *"Cybersecurity Threats in the Age of Artificial Intelligence: Exploiting Advanced Technologies and Enhancing Cybersecurity"* by Dr. Idriss Abadi and Abdelkader Lachkar, published in October 2024 in the *International Journal of Sciences and Research Archives*, focuses on the relationship between artificial intelligence and cybersecurity threats. The study explains how AI is used to develop advanced cyberattacks and enhance security defenses. It also discusses the challenges arising from the evolution of this technology and its ability to surpass traditional defense systems. The study emphasizes the importance of adopting balanced strategies that integrate AI into defending digital systems while preparing to face new threats, recommending increased cooperation between government and the private sector and training cybersecurity professionals.

In the context of higher education, the study by *Matsieli, M., & Mutula, S* published in *Education Sciences* examines the impact of the COVID-19 pandemic on higher education and the digital transformation of educational institutions, focusing on promoting equitable and inclusive access to quality education. The study shows that students from vulnerable groups were significantly affected by difficulties in accessing online education and lacking digital infrastructure. Despite the benefits of digital transformation in ensuring the continuity of education, it posed significant challenges such as the digital divide and social discrimination. The study recommends that higher education institutions and governments take responsibility for addressing these challenges through comprehensive strategies to ensure equal educational opportunities for all students, with an emphasis on adopting digital teaching practices that promote justice and equality in access to education.

These studies intersect to highlight the role of technology in cultural change, digital education transformations, and the importance of cybersecurity in protecting these transformations.

1.5.Research Problem

This research raises an issue related to determining how to bridge the digital divides that undermine equality of opportunity in digital education while ensuring the protection of individuals and institutions from cybersecurity risks. Therefore, the research addresses two main areas: the first focuses on studying the digital divides and cybersecurity risks in digital education, including the challenges faced by students and educational institutions. The second area concerns studying strategies for bridging digital divides and enhancing cybersecurity, through the development of technologies and mechanisms that contribute to ensuring fair and secure access to digital education for all.

From this issue, a set of sub-questions arises, the most important of which are:

-What are the main factors contributing to digital divides in digital education?

-What are the main cybersecurity risks facing digital education, and how can their impacts be mitigated?

-What are the effective strategies that can be adopted to bridge digital divides in education?

-How can cybersecurity be enhanced in digital education to protect sensitive data and information?

To answer these questions, they will be addressed through two main areas: the first area addresses digital divides and cybersecurity risks in digital education, where we will review the factors contributing to digital divides and the main cybersecurity risks threatening digital education. The second area focuses on strategies for bridging digital divides and enhancing cybersecurity, with a discussion on effective methods for closing digital divides in education and how to strengthen cybersecurity to protect sensitive data and information.

2.Digital Divides and Cybersecurity Risks in Digital Education

Digital education is evolving rapidly in the current era, with technology becoming an integral part of the educational process (Ally, M., 2008). However, this swift transformation raises significant challenges related to digital divides and cybersecurity risks, which affect students and educators unequally across various environments. Many individuals, especially in low-income communities or remote areas, face difficulties in accessing the necessary technology and digital resources for education (DiMaggio & Hargittai, 2001; Hilbert, 2015). Cybersecurity risks also emerge as a major concern, threatening the security of data and personal information in educational systems, thus emphasizing the need to protect information security and ensure a safe educational environment (A. Kifaru, F., Kavuta, K., & Semlambo, A., 2023).

In this section, we will explore the digital divides that hinder some students from accessing equal educational opportunities, as well as the cybersecurity risks that threaten the stability of the digital education process. Additionally, we will discuss strategies to address these challenges to ensure equal educational opportunities and protect information security in digital educational systems.

2.1. Digital Divides in Digital Education

The concept of the "digital divide" is generally defined as the gap between individuals who have access to information and communication technology (ICT) and those who do not. This technology primarily includes computers and the internet, and sometimes extends to mobile phones, especially smartphones, as well as other digital devices and software. This concept arises in discussions of social and informational inequality. Additionally, the notions of inclusion and exclusion within various social units play a key role in these contexts (Van Dijk, 2020). In the educational context, the digital divide refers to the unequal access to essential technology and digital resources among students, teachers, and schools, which directly impacts the support provided for the learning process (Smith, R. F., 2023; Adhikari, J., Mathrani, A., & Scogings, C., 2016). According to data from the New America Foundation, African-American and Latino households experienced the most significant digital challenges during the peak of remote learning. This lack of access typically reflects the socioeconomic status or geographic location of communities, thus deepening existing learning disparities. The rapid shift to digital education has exacerbated the gap in internet access, particularly in educational systems that heavily relied on digital learning, especially during the COVID-19 pandemic. This has negatively affected students who lacked electronic devices or internet connectivity. The persistence of this divide continues to have profound impacts on students' academic performance, potentially hindering their future opportunities (Smith, R. F., 2023, August 29).

The digital divide has emerged as a result of several accumulated social and economic factors that significantly affect individuals and communities' ability to access modern technology and digital resources. Some of the main causes include:

2.1.1. Lack of Infrastructure: Weak technological infrastructure in many areas, especially rural and remote ones, is a primary factor contributing to the widening digital divide. Students and teachers in these areas suffer from the absence of fast, stable internet connections, making it difficult to access information and digital educational resources. The lack of digital devices, such as computers and smartphones, further exacerbates this problem (Van Dijk, 2020; Tahmasebi, F., 2023).

2.1.2. High Technology Costs: The cost of digital devices and internet access is another significant contributor to the digital divide. Many low-income families find it difficult to afford the necessary devices for their children, in addition to the expensive internet subscriptions required to access online education. This disparity in access to technology across social classes increases educational inequalities among students (OECD, 2019).

2.1.3. Access Differences Between Urban and Rural Areas: The divide in internet access between urban and rural areas is a key factor contributing to the widening of the digital divide. In urban areas, individuals have access to high-speed internet, which facilitates their ability to benefit from digital educational resources and stay updated with modern educational developments. In contrast, students in rural areas face significant challenges accessing the internet due to weak technological infrastructure, making it difficult to participate in remote learning or use digital applications for education. This disparity in internet access leads to unequal educational opportunities, as students in rural areas struggle to follow digital curricula and engage with online educational content, negatively impacting their academic performance. According to the OECD report (OECD, 2019), these differences result in achievement gaps, as students without internet access experience a decline in their digital skills and their opportunities to participate in the knowledge economy (OECD, 2019).

2.1.4. Lack of Digital Skills: A lack of digital skills is another factor contributing to the deepening digital divide in education. Even when students and teachers have access to devices and the internet, many struggle to use digital tools effectively if they lack the necessary basic skills, such as using educational software or conducting online research. Studies suggest that the digital divide manifests in three key indicators: access (access to devices and the internet), skills (the ability to use technology effectively), and usage (effective interaction with digital content) (Younis, M. A., 2021). Furthermore, educational institutions face technological challenges that hinder their digital transformation efforts, such as a lack of clear strategies, high training costs, and resistance from teachers accustomed to traditional teaching methods (James, S., 2025).

2.1.5. Social and Cultural Discrimination: In some communities, individuals face social or cultural discrimination that negatively affects their ability to access technology. This discrimination may be based on gender, race, or social class, depriving certain groups of access to digital tools. These divides are most pronounced in developing countries or conservative societies, where specific groups are marginalized and denied access to technological resources (Liotta, L. A., 2023).

2.1.6. Lack of Government Supportive Policies: Many countries lack effective government policies to support and enhance access to technology in education. The absence of government investments in digital infrastructure or a lack of government support for providing affordable internet access exacerbates the digital divide. Moreover, many governments fail to provide free or subsidized internet access, making it harder for individuals to access it, particularly in remote areas (Selwyn, 2016).

2.1.7. Impact of the COVID-19 Pandemic: The COVID-19 pandemic significantly worsened the digital divide, as many students found themselves unable to continue their studies online due to a lack of devices or poor internet connectivity in their homes. Numerous studies have shown that the pandemic deepened educational disparities between students who had access to technology and the internet and those who did not, negatively affecting their academic performance and future opportunities (UNESCO, 2020).

The digital divide refers to the disparities in access to information and communication technology among individuals, which negatively impacts learning. Students who lack technology or the ability to use it effectively fall behind academically and struggle to acquire digital skills. This also hinders effective communication between teachers and students, exacerbating the educational gap (Okafor, U. O., et al., n.d.).

2.2. Cybersecurity Risks in Digital Education

These risks are associated with the use of technology in education, particularly cybersecurity threats that could impact the data of students and educational institutions. The focus is on issues related to protecting and securing privacy, as well as the threats that could lead to breaches of educational systems or the illegal exploitation of data. With the evolution of digital education and the growing reliance on technology in educational institutions, numerous cybersecurity risks have emerged, threatening personal data and privacy within this field. These risks manifest in several forms, including cyberattacks and malicious software, which require special attention from those overseeing the educational process to ensure data protection and maintain a safe and sustainable learning environment. Below are the most significant of these risks:

2.2.1. Breach of Educational Systems: Data breaches are major security incidents that occur when institutions fail to implement appropriate cybersecurity measures, allowing cybercriminals to steal sensitive data and personally identifiable information. The education sector, particularly higher education, has experienced a significant increase in cyberattacks in recent years, leading to massive data breaches and the loss of sensitive information. According to a report by Check Point Research, as schools increasingly depend on remote learning and cloud servers, the risk of attacks and vulnerabilities has grown, necessitating universities and colleges to adopt effective strategies to prevent data breaches and protect sensitive information (Chin, K., 2024).

2.2.2. Threats of Personal Data Leakage: Educational institutions face substantial challenges in cybersecurity, as they are prime targets for cyberattacks due to their retention of sensitive data, such as student and staff information. For instance, in 2024, the Los Angeles Unified School District (LAUSD) suffered a significant breach, with personal information about students and staff stolen. Similarly, in 2023, a breach of the MOVEit program affected about 900 schools in the U.S., exposing sensitive data such as names and Social Security numbers. In 2023, the University of Michigan was breached, compromising the information of 230,000 individuals, including financial and medical data. The New Haven Public Schools district also fell victim to a cyberattack in 2023, resulting in a $6 million theft through CEO identity fraud. In February 2023, the Medusa gang launched an attack on Minneapolis Public Schools, exposing sensitive data of 105,000 individuals. Ransomware and DDoS attacks are among the most dangerous forms of malicious software targeting educational institutions. Ransomware encrypts data and demands a ransom for decryption, while DDoS attacks disrupt internet services for educational institutions by overwhelming servers with traffic, disrupting academic and administrative operations. These incidents highlight how education has become a primary target for cyberattacks due to weak security and the lack of ongoing data protection training, underlining the need to enhance cybersecurity and raise awareness among users in educational institutions (Jelen, S., 2024).

2.2.3. Lack of Cybersecurity Awareness: A significant challenge faced by both individuals and institutions is the lack of cybersecurity awareness, particularly within academic environments. University students often lack a basic understanding of cybersecurity concepts and best practices for protecting their devices and personal data. This lack of awareness makes them easy targets for cyberattacks such as fraud, viruses, ransomware, and cyberbullying. In many cases, students fall victim to phishing messages or share sensitive information without considering the potential consequences. Studies have shown that students in advanced educational environments, such as Silicon Valley, do not utilize two-factor authentication sufficiently, which increases their vulnerability to attacks. A UK security survey also indicated that educational institutions became the primary targets for successful cyberattacks or data breaches in 2020. Therefore, it is essential for academic institutions to adopt continuous awareness programs to foster a cybersecurity culture among students, including training them to identify cybersecurity threats and protect themselves from digital risks (Khader, M., et al., 2021).

To mitigate cybersecurity risks in educational institutions, various security measures must be strengthened, such as data encryption, antivirus software usage, and training staff on how to counter cyberattacks. Furthermore, it is crucial to periodically update protection systems to ensure their ability to confront emerging threats. Through these measures, digital divides can be closed, and cybersecurity can be effectively strengthened. The second section focuses on practical strategies aimed at enhancing digital security in educational institutions, while providing innovative solutions to address current challenges.

3. Strategies for Bridging the Digital Divide and Enhancing Cybersecurity

Educational institutions in the era of modern technology are increasingly vulnerable to cybersecurity threats due to their growing reliance on digital systems and modern technologies for managing educational and administrative processes. As the use of the internet and digital devices increases, digital gaps have emerged, which can expose these institutions to significant risks. Therefore, it has become essential to adopt effective strategies to bridge these gaps and strengthen cybersecurity to protect sensitive data and ensure the continuity of the educational process. There are several strategies and measures that educational institutions can adopt to strengthen their cybersecurity defenses, ranging from system updates and staff training to implementing innovative digital security solutions. These efforts aim to reduce risks and protect the educational environment from escalating cyberattacks.

3.1. Strategies for Bridging the Digital Divide

Digital gap closure strategies are effective means that help achieve equal opportunities in accessing technology and digital knowledge. In this context, I will address a set of strategies that can contribute to reducing these gaps, thus enhancing the ability to interact with rapid digital transformations.

3.1.1. Improving Digital Infrastructure: Improving digital infrastructure is a key step to ensuring equal opportunities for all students to access digital education. Therefore, efforts must be made to provide high-speed internet and appropriate electronic devices in underserved areas, enhancing students' ability to benefit from available digital resources. Improving technological infrastructure and ensuring equitable access to these resources significantly contributes to reducing digital gaps and promoting equal learning opportunities. It is important that investments in modern technologies within classrooms extend to rural and remote areas, not just urban centers, enabling all students, regardless of their location or social status, to benefit from equal educational opportunities (OECD, 2019).

3.1.2. Supporting Technologies and Technical Assistance: Digitalization opens new horizons for education by transforming educational data into a key tool supporting the learning, teaching, and decision-making processes within educational institutions. While education has always relied on data such as grades and administrative information, using this data in innovative ways to improve learning effectiveness and develop education at both individual and institutional levels is still in its early stages. While technologies such as radio, television, and the internet have been used to enhance education without making drastic changes, modern digital technologies such as artificial intelligence and educational data analytics have real potential to radically change how education is delivered. These technologies can transform traditional teaching methods, allowing robots and smart systems to replace teachers in some tasks, leading to improved efficiency and increased productivity (OECD, 2021).

In light of these technological shifts, supporting technologies and providing technical assistance become critical to ensuring the sustainable and effective use of these technologies in educational environments. Digitalization not only improves educational systems but also requires strong digital infrastructure that ensures equal opportunities for all students, especially in areas lacking such infrastructure. Providing continuous technical support to these regions can help bridge the digital divide and foster innovation in educational policies, leading to more effective use of technology. Furthermore, the integration of smart technologies, such as artificial intelligence, to enhance personalized learning and analyze student performance, will be necessary. This requires investments in teacher training and providing technical support to ensure the successful implementation of these technologies in classrooms. Moreover, the ongoing digital transformation in education will require a greater focus on developing skills that are difficult to automate, such as critical thinking, creativity, and collaboration—skills that will remain central to the educational process in the future. Thus, the sustainability of digital technology use largely depends on continuous technical support and the development of robust infrastructure to ensure these technologies are smoothly and effectively integrated into the educational process (OECD, 2021).

3.1.3. Raising Awareness of Digital Culture: Raising awareness of digital culture is a cornerstone for ensuring that everyone benefits from the opportunities offered by digitalization in education. In a world increasingly reliant on technology, it is crucial to spread cultural and educational awareness about the importance of digital education. Through this, students and teachers can develop the digital skills necessary to participate effectively in the educational process. Studies have shown that acquiring digital skills is a crucial means of reducing the digital divide between individuals and communities, as providing sustainable educational programs in this area helps enhance learners' ability to adapt to rapid technological changes (OECD, 2021).

Digital culture is a dynamic and open process that relies on information and communication technologies, such as the internet, which help accelerate the interaction of different cultures and open new horizons in the arts and communication. Therefore, it is essential to promote digital culture awareness among students, as understanding and mastering this culture helps bridge the digital divide caused by unequal access to technology or a lack of digital skills. Education in digital culture can empower students to use modern technologies effectively, enhancing their interaction with cultural and artistic content on online platforms and providing equal learning opportunities. Thus, raising awareness of digital culture is a key tool for enhancing students' understanding of the digital world and achieving educational equity, as well as narrowing the gap between students amid rapid technological changes (Selwyn, N., 2016, UNESCO, 2023).

3.2. Strategies for Enhancing Cybersecurity

Cybersecurity threats to educational institutions are increasing in the era of digital transformation. Therefore, implementing comprehensive strategies to ensure cybersecurity has become essential, using advanced protection technologies, raising awareness among stakeholders, and fostering collaboration between the public and private sectors to ensure a safe educational environment. This is explained as follows:

3.2.1. Advanced Protection Technologies: It has become crucial for educational institutions to use advanced technologies to ensure the protection of personal and academic data from cyberattacks. Some of the most prominent of these technologies include:

-Advanced Encryption and Blockchain Technologies: In the context of cybersecurity enhancement strategies in educational institutions, integrating advanced encryption and blockchain technologies is a vital step in securing and protecting data from cyberattacks. In institutions that increasingly rely on digital systems to manage academic and personal data for students and staff, the need to protect this data is more important than ever. With advanced encryption, the confidentiality of data transmitted between educational systems or between students and teachers can be ensured, reducing the risk of unauthorized access (Abbadi, D., Lachkar, A., Sood, K. et al., 2022).

On the other hand, blockchain provides an effective solution in ensuring data integrity in digital learning environments, where it can be used to record academic records such as grades and certificates in a tamper-proof manner once recorded. This is especially useful in combating fraud and verifying the validity of academic records, as blockchain ensures that all recorded data is protected and authenticated by a decentralized network of nodes. Additionally, educational systems can benefit from smart contracts linked to blockchain to automate verification processes such as student registration, grading, and certificate documentation, thus enhancing security and reducing the chances of manipulation or human error in these processes. The integration of advanced encryption and blockchain technologies into the cybersecurity strategies of educational institutions provides a comprehensive framework to protect academic and personal data from cyberattacks, enhancing the efficiency of the digital educational system. This helps build a secure educational environment that ensures the protection of sensitive information and boosts trust among all stakeholders. The integration of these advanced technologies into the security framework of educational institutions represents a strategic step towards fortifying educational systems against cyber risks and enhancing overall digital security (Abbadi, D., Lachkar, A., 2024, Alsaadi, A. H., & Bamasoud, D. M., 2021).

These technologies transform data into an unreadable form except by the person who holds the correct decryption key, preventing unauthorized access to sensitive information.

-Multi-Factor Authentication (MFA): Multi-Factor Authentication (MFA) is a security measure that uses additional layers to verify a user's identity and enhance data security, alongside the traditional username and password. MFA requires two or more verification methods, such as something the user knows (password), something the user has (such as a bank card or mobile device), and something the user is (such as biometric data like fingerprints). With these multiple layers, it becomes more difficult for hackers to access accounts even if they obtain traditional login details, as they would need more data that only the user possesses. Thus, MFA provides an effective and quick means of enhancing account security without overburdening the user with additional information to remember (Williamson, J., & Curran, K., 2021).

MFA relies on three main types of factors to enhance security: **Knowledge Factors**, **Possession Factors**, and **Inherence Factors**. Knowledge factors include what the user knows, such as passwords, PINs, and security questions. Possession factors depend on something the user has, such as connected or disconnected tokens, which can be used for authentication when the user provides the token. Inherence factors relate to the user's own characteristics, such as fingerprints, facial recognition, or retina scanning, which are biometric methods that do not require the user to remember or carry anything but only to interact with a device. By combining these different factors, security levels increase significantly, as each additional factor enhances the verification process in protecting accounts and data from attackers (Williamson, J., & Curran, K., 2021).

-Continuous Monitoring: The implementation of continuous monitoring and analysis tools in educational institutions that increasingly rely on digital systems to manage academic and personal data becomes crucial to ensuring the protection of this data from cyber threats. Intrusion Detection Systems (IDS) are among the key tools that help detect early threats within educational networks. These systems monitor and analyze events on the network to detect any unusual activities attempting to breach or carry out a cyberattack threatening the integrity of students' and faculty members' academic and personal data. Using these tools, educational institutions can identify potential violations of security policies or illegal system use, which helps mitigate risks and prevent potential leaks or loss of sensitive data (Azhagiri, M., et al., 2015, Igbokwe, I. C., 2024).

Moreover, Intrusion Prevention Systems (IPS) and Security Information and Event Management (SIEM) systems are essential tools for continuous security monitoring within digital education environments. These systems provide comprehensive information and detailed analysis regarding system performance, aiding in the early detection of potential threats. In an educational environment where networks contain sensitive data such as grades, certificates, and personal data, these systems enable security administrators to take proactive measures to counter cyberattacks before they escalate. By monitoring suspicious patterns and unusual interactions, security systems can identify potential threats and respond immediately to ensure the protection of academic data and the smooth functioning of academic work in a secure environment (Younus, Z. S., & Alanezi, M., 2023).

3.2.2. Security Policies and Cybersecurity Awareness: Adopting security policies and providing cybersecurity awareness is vital to ensuring the sustainability of cybersecurity in educational institutions. Policies help establish a framework to protect data, while awareness fosters a digital security culture among all stakeholders (Abrahams, et al., 2024).

-Awareness of Cybersecurity Risks: Awareness programs aim to educate students, teachers, and administrators about the importance of cybersecurity and potential risks such as phishing attacks and viruses. This can be achieved through workshops and training courses that review data protection methods and how to avoid falling victim to cyberattacks (Bada, M., et al., 2015, Arishi, et al., 2024). Additionally, students are encouraged to adopt safe behaviors, such as using strong passwords and avoiding connecting to untrusted networks.

-Data Protection Policies: Data protection in educational institutions is one of the primary priorities to ensure the privacy of students and teachers and protect it from unauthorized access. With the continuous rise of digital transformation in schools, it is necessary to implement effective technical and organizational policies and procedures to protect sensitive data such as grades, health information, and personal communication. Schools must comply with legal requirements, such as the General Data Protection Regulation (GDPR), ensuring transparency in data collection and usage while obtaining informed consent from relevant individuals. Additionally, schools must train all stakeholders and raise awareness about the importance of data protection, thus building a safe and sustainable educational environment (DATUREX GmbH, 2024).

-Ongoing Training: Educational institutions must commit to providing regular training for their staff on cybersecurity threats and how to prevent them, ensuring everyone is prepared to face the growing digital challenges. This training includes teaching teachers how to handle malicious software and breaches, as well as establishing effective response plans for cybersecurity incidents. Ongoing training is crucial in reducing human errors, which are among the main causes of cyberattacks. Continuous training improves staff ability to recognize and respond effectively to threats, reducing the likelihood of institutions facing severe security risks (Ucar, A., 2024).

3.2.3. Public-Private Partnership: Cooperation between the public and private sectors is a critical step in ensuring the sustainability of cybersecurity in educational environments. These partnerships provide information exchange and advanced technologies that contribute to enhancing cybersecurity (Younus, M., et al., 2024).

-Collaboration with Governments: Collaborating with governments helps enhance cybersecurity in educational institutions. Governments need to establish specific regulatory policies that govern the cybersecurity of digital educational systems, such as setting mandatory security standards to protect information and systems. Additionally, governments can provide financial and technical support to help develop innovative security solutions that meet the needs of educational institutions, as seen with federal initiatives such as the FCC program in the United States, which offers funding and security services to schools. According to studies, government collaboration enhances educational institutions' ability to respond faster and more effectively to cyber threats, contributing to long-term cybersecurity sustainability. This cooperation also ensures the availability of specialized training resources, which strengthens the culture of cybersecurity awareness in schools and universities, ensuring a safe educational environment (Barlet, G., 2024, CISA, n.d.).

-Partnerships with Technology Companies: The relationship between the state and the private sector in cybersecurity underscores the importance of partnerships between technology companies and educational institutions. Similar to public-private cooperation in critical infrastructure protection, private companies contribute advanced solutions to protect networks and digital systems. Technology companies such as Cisco and Microsoft offer advanced technologies to protect educational institutions from cybersecurity threats. These companies not only provide tools for threat detection but also develop preventive systems and specialized consultations to improve security practices, enhancing educational institutions' ability to build secure infrastructure using advanced cloud solutions and integrated security systems. Additionally, partnering with these companies improves the institutions' response to cyber threats and helps meet the growing digital security needs as modern technologies evolve, ensuring a safe and reliable educational environment (Kruhlov, V., et al., 2019, Yankson, B., et al., 2024).

-Collective Emergency Response: In the event of a cyberattack, there must be quick and effective coordination between government institutions, educational institutions, and private companies, along with the establishment of Cybersecurity Incident Response Teams (CERT) to ensure an immediate and efficient response. This requires forming specialized response teams that collaborate in an organized and swift manner to handle crises arising from a cyberattack. This also involves identifying available tasks and resources and organizing the rebuilding of affected educational systems to restore their functionality quickly and effectively. This coordination between various parties enhances the ability of educational institutions to handle threats and ensures that cybersecurity systems are resilient and can recover quickly in the face of increasing crises (Rohman, H., et al., 2022, UNESCO, 2022).

By using advanced protection technologies, enhancing cybersecurity awareness, and developing partnerships between the public and private sectors, educational institutions can ensure a secure and effective learning environment. Undoubtedly, activating these strategies is necessary to build a digital educational community capable of facing ongoing cybersecurity threats.

Conclusion

From the above, the importance of bridging the digital divide and ensuring data protection in digital education becomes clear. The disparities in access to digital resources among students, especially in remote or low-income areas, pose a barrier to achieving equal educational opportunities. At the same time, the increasing reliance on the internet for education amplifies the need to protect personal data, highlighting the role of cybersecurity as a key element in safeguarding the data of students and teachers and maintaining the security of educational institutions.

Hence, the importance of developing strategies that include improving digital infrastructure and providing technical support to underserved areas is evident. It is also necessary to strengthen digital culture among students and teachers and raise awareness of the importance of cybersecurity.

Furthermore, the following recommendations are required:

-Achieving digital equity: Efforts should be made to reduce the digital divide by providing tools and technologies that allow all students access to digital education, regardless of their economic or geographical background (Adam, T. 2025);

-Integrating cybersecurity into curricula: Cybersecurity concepts should be regularly included in educational curricula at various educational levels, focusing on training students and teachers on how to protect their personal data and deal with cybersecurity threats (Mouheb, D., et al., 2019);

-Investing in advanced protection technologies: Educational institutions should strive to adopt advanced security technologies, such as encryption, malware protection, and multi-factor authentication techniques, to ensure the security of information and protect it from cyber-attacks (Vain, C., 2024, Akhyadov, E. S.-M., et al., 2019);

-Enhancing collaboration between the public and private sectors: Governments and private companies should collaborate to develop innovative technological solutions aimed at securing a safe digital educational environment, while providing the necessary technical support and infrastructure to overcome cybersecurity challenges (Walsh, C., Mital, A., Ratcliff, M., & Jamaleddine, Z. 2020).

Finally, it is worth noting that the subject of this research opens new horizons for researchers, as it may be important to expand and deepen the research to address other dimensions, such as the role of artificial intelligence and machine learning in enhancing cybersecurity in educational institutions, and how to integrate these technologies into digital education strategies to keep up with the rapid changes in this field.

References

1-Abbadi, D., &Lachkar, A. (2024).Cyber threats in the age of artificial intelligence: Exploiting advanced technologies and strengthening cybersecurity. International Journal of Science and Research Archive, 13(01), 2576-2588.Retrieved from: https://doi.org/10.30574/ijsra.2024.13.1.1961

2-Abrahams, et al., (2024). Cybersecurity awareness and education programs: A review of employee engagement and accountability. *Computer Science & IT Research Journal, 5*(1), 100-119. https://doi.org/10.51594/csitrj.v5i1.708

3-Adam, T. (2025). Towards more justice-oriented digital education. In B. Bachmann & A. Sander (Eds.), *Short informative paper*. The European Digital Education Hub (EDEH). https://www.daad-brussels.eu/files/2025/02/Justice-Oriented-Digital-Education.pdf

4-Adhikari, J., Mathrani, A., & Scogings, C. (2016). Bring Your Own Devices classroom: Exploring the issue of digital divide in the teaching and learning contexts. *Interactive Technology and Smart Education, 13*(4), 323-343. https://doi.org/10.1108/ITSE-04-2016-0007

5-Akhyadov, E. S.-M., et al., (2019). Digital economy: Investing in digital learning technologies. *International Journal of Engineering and Advanced Technology, 9*(1), 6570-6576. https://doi.org/10.35940/ijeat.A1829.109119.

6-Ally, M. (2008).Foundations of educational theory for online learning.In T. Anderson (Ed.).The theory and practice of online learning (pp.15-44).Athabasca, AB: Athabasca University Press. Retrieved from: https://tinyurl.com/24m7ach7

7-Alsaadi, A. H., & Bamasoud, D. M. (2021). Blockchain technology in education system. *International Journal of Advanced Computer Science and Applications, 12*(5). https://doi.org/10.14569/IJACSA.2021.0120585.

8-Arishi, A. et al., (2024). Cybersecurity awareness in schools: A systematic review of practices, challenges, and target audiences. *International Journal of Advanced Computer Science and Applications, 15*(12), 467.

9-Azhagiri, M., et al. (2015). Intrusion detection and prevention system: Technologies and challenges. International Journal of Applied Engineering Research, 10(87), 1.Retrieved from: https://tinyurl.com/mrya8zak

10-Bada, M., et al., (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? In Proceedings of the International Conference on Cyber Security for Sustainable Society. Retrieved from:https://tinyurl.com/3txdp5ss

11-Barlet, G., (2024, July 18). K-12 Cybersecurity: Why federal-education partnerships are critical for cybersecurity. Illumio. Retrieved from:https://tinyurl.com/43z947na

12-Chin, K., (2024, November 18). How colleges & universities can prevent data breaches. Retrieved from: https://tinyurl.com/3yjft9xu

13-CISA. (n.d.). Educational institutions. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/audiences/educational-institutions

14-DATUREX GmbH., (2024, August 7). Data protection in education: Protecting student and teacher data. Privacy. Retrieved from:https://tinyurl.com/tttync87

15-DiMaggio, P., &Hargittai, E., (2001). From the "digital divide" to "digital inequality": Studying internet use as penetration increases. Princeton University, 1-39, retrieved from:https://tinyurl.com/mj95re2n

16-Hilbert, M. (2015). Digital Divide(s). In *The International Encyclopedia of Digital Communication and Society.* (pp. 1-9). John Wiley & Sons, Inc. https://doi.org/10.1002/9781118767771.wbiedcs012

17-Igbokwe, I. C. (2024). Cyber security in the era of digitalization: Implications for educational management. *UNIZIK Journal of Educational Research and Policy Studies, 6*(2), 71-77. https://tinyurl.com/3bpz8a7d

18-James, S. (2025, February 14). *Digital transformation in education.* Education Walkthrough. https://educationwalkthrough.com/digital-transformation-in-education/

19-Jawaid, S. A., (2023).Cybersecurity threats to educational institutes: A growing concern for the new era of cybersecurity. International Journal of Data Science and Big Data Analytics, 2(2), 11-17. https://doi.org/10.51483/IJDSBDA.2.2.2022.11-17

20-Jelen, S., (2024, August 8). Education sector common breaches and cyber threats.Retrieved from: https://tinyurl.com/46a4uncb

21-Khader, M., et al., (2021).Cybersecurity Awareness Framework for Academia.Information, 12(10), 417, pp. 1-2. Retrieved from:https://doi.org/10.3390/info12100417

22-Kifaru, F., Kavuta, K., &Semlambo, A. A., (2023). Assessment of the impacts of cyber security on student information management systems: A case of Ruaha Catholic University. The Journal of Information Technology and Innovation, 3(1).Retrieved from:https://doi.org/10.59645/tji.v3i1.127.

23-Kruhlov, V., et al., (2019).Public-private partnership in cybersecurity.Conference Paper. Retrieved from:https://tinyurl.com/2snertm2

24-Liotta, L. A., (2023). Digitalization and social inclusion: Bridging the digital divide in underprivileged communities. Global International Journal of Innovative Research, 1(1), 7-14. Retrieved from:https://doi.org/10.59613/global.v1i1.2

25-Matsieli, M., &Mutula, S., (2024). COVID-19 and digital transformation in higher education institutions: Towards inclusive and equitable access to quality education. Education Sciences, 14(8), 819.Retrieved from: https://doi.org/10.3390/educsci14080819

26-Mouheb, D., et al., (2019). Cybersecurity curriculum design: A survey. In *Transactions on Edutainment XV* (Lecture Notes in Computer Science). https://doi.org/10.1007/978-3-662-59351-6_9

27-Okafor, U. O., et al. (n.d.).Impact of digital divide on learning. Federal College of Education (Technical) Umunze. https://www.fcetumunze.edu.ng/publications

28-OECD. (2019). The Future of Education and Skills: Education 2030. OECD Publishing, Retreived from: https://tinyurl.com/4n9zmftv

29-OECD. (2021). OECD digital education outlook 2021: Pushing the frontiers with artificial intelligence, blockchain, and robots. OECD Publishing.

retreivedfrom:https://doi.org/10.1787/589b283f-en

30-Rohman, H., et al. (2022).Collaboration of ministries/institutions and the private sector in handling cyber threats through the establishment of Computer Security Incident Response Team (CSIRT).Technium Social Sciences Journal, 38, 87-102. Retrieved from:https://www.techniumscience.com

31-Selwyn, N. (2016).Education and Technology: Key Issues and Debates. Bloomsbury Publishing.

32-Smith, R. F., (2023, August 29). The digital divide in education: Navigating learning inequities. Retrieved from:https://tinyurl.com/3mpur7z7

33-Sood, K., et al. (Eds.). (2022). *Blockchain technology in corporate governance: Transforming business and industries*. Wiley.

34-Tahmasebi, F. (2023). The digital divide: A qualitative study of technology access in rural communities. *AI and Tech in Behavioral and Social Sciences, 1*(2), Serial Number 2. https://doi.org/10.61838/kman.aitech.1.2.6

35-Ucar, A., (2024, June 13). The critical importance of cybersecurity awareness training.LinkedIn, retreived from: https://tinyurl.com/2bnktk2h

36-UNESCO. (2020). Education: From disruption to recovery. United Nations Educational, Scientific and Cultural Organization.Retrieved from :https://tinyurl.com/3fe2jkxf

37-UNESCO. (2022). *Minding the data: Protecting learners' privacy and security.* https://doi.org/10.54675/NNAA4843. ISBN 978-92-3-100525-1.

38- UNESCO. (2023). Global Education Monitoring Report 2023: Technology in education - A tool on whose terms? Paris, UNESCO. https://doi.org/10.54676/UZQV8501

39-Uzelac, A., &Cvjetièanin, B. (Eds.). (2008). Digital culture: The changing dynamics. Institute for International Relations. UNESCO-BRESCE.

40-Van Dijk, J. A. G. M., (n.d.).Digital divide: Impact of access (p. 1). University of Twente, Netherlands. Retrieved from:https://tinyurl.com/2v6cvmhj

41-Walsh, C., et al., (2020). A public-private partnership to transform online education through high levels of academic student support. *Australasian Journal of Educational Technology, 36*(5), 30-45. https://doi.org/10.14742/ajet.6107

42-Yankson, B., et al. (2024). The role of industry-academia partnerships can play in cybersecurity: Exploring collaborative approaches to address cybercrime. *International Conference on Cyber Warfare and Security, 19*(1), 26-33. https://doi.org/10.34190/iccws.19.1.2169.

43-Williamson, J., & Curran, K., (2021).The role of multi-factor authentication for modern day security.Semiconductor Science and Information Devices, 3(1), 16.Retrieved from:https://doi.org/10.30564/ssid.v3i1.3152

44-Younis, M., & Al-Gharib, S. (2021). The digital divide in higher education: A socio-cultural study from an educational perspective on students of the Faculty of Education at Tanta University. *Journal of Scientific Research in Education*, 22(3), 30. https://doi.org/10.21608/jsre.2021.59542.1258. [translated from Arabic]

45-Younus, M., et al, (2024). Public-private collaboration to overcome the digital divide in digital transformation of government. *Digital Zone Jurnal Teknologi Informasi dan Komunikasi, 15*(1). https://doi.org/10.31849/digitalzone.v15i1.17027

46-Younus, Z. S., &Alanezi, M., (2023). A survey on network security monitoring: Tools and functionalities. Mustansiriyah Journal of Pure and Applied Sciences, 1(2), 60.Retrieved from:https://doi.org/10.47831/mjpas.v1i2.33