Mesopotamian Journal of Computer Science

Volume 5 | Issue 1 Article 8

1-1-2025

# Enhancing Cybersecurity in Smart Education with Deep Learning and Computer Vision: A Survey

Follow this and additional works at: https://map.researchcommons.org/mjcsc

 Part of the Computer Sciences Commons

## How to Cite This Article

(2025) "Enhancing Cybersecurity in Smart Education with Deep Learning and Computer Vision: A Survey," *Mesopotamian Journal of Computer Science*: Vol. 5: Iss. 1, Article 8.
DOI: https://doi.org/10.58496/MJCSC/2025/008
Available at: https://map.researchcommons.org/mjcsc/vol5/iss1/8

This Article is brought to you for free and open access by Mesopotamian Academic Press. It has been accepted for inclusion in Mesopotamian Journal of Computer Science by an authorized editor of Mesopotamian Academic Press.

Mesopotamian journal of Computer Science
Vol. **(2025)**, 2025, **pp**. 115–158
DOI: https://doi.org/10.58496/MJCSC/2025/008; ISSN: 2958-6631
https://mesopotamian.press/journals/index.php/cs

Review Article

# Enhancing Cybersecurity in Smart Education with Deep Learning and Computer Vision: A Survey

Guma Ali [1,2] *, Aziku Samuel [1], Maad M. Mijwil [3,4,5], Kholoud Al-Mahzoum [6], Malik Sallam[7,8,9], Ayodeji Olalekan Salau[10, 11], Indu Bala[12], Klodian Dhoska[13], Engin Melekoglu[14]

[1] *Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda*

[2] *Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu, India*

[3] *College of Administration and Economics, Al-Iraqia University, Baghdad, Iraq*

[4] *Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq*

[5] *Faculty of Engineering, Canadian Institute of Technology, Albania*

[6] *Sheikh Jaber Al-Ahmad Al-Sabah Hospital, Ministry of Health, Kuwait City, Kuwait*

[7] *Department of Pathology, Microbiology and Forensic Medicine, School of Medicine, The University of Jordan, Amman, Jordan*

[8] *Department of Clinical Laboratories and Forensic Medicine, Jordan University Hospital, Amman, Jordan*

[9] *Department of Translational Medicine, Faculty of Medicine, Lund University, Malmö, Sweden*

[10] *Department of Electrical/Electronic and Computer Engineering, Afe Babalola University, Ado-Ekiti, Nigeria*

[11] *Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India*

[12] *School of Electrical and Electronics Engineering, Lovely Professional University, Punjab, India*

[13] *Department of Mechanics, Polytechnic University of Tirana, Albania*

[14] *AAB Collage, Computer Sciences Prishtinë, Kosova*

**Article Info**

Article History

Received 15 Feb 2025
Revised 2 Apr 2025
Accepted 23 May 2025
Published 28 Jun 2025

Keywords

Smart Education
Cybersecurity
Deep Learning
Computer Vision
Privacy Protection

CC BY

**Abstract**

The rapid digital transformation of education, driven by the widespread adoption of smart devices and online platforms, has ushered in the era of smart education. While this shift enhances learning experiences, it also introduces significant cybersecurity risks that threaten the confidentiality, integrity, and availability of educational resources, student data, and institutional systems. This survey examines how deep learning (DL) and computer vision (CV) techniques can enhance cybersecurity in smart education environments. By reviewing 202 peer-reviewed research papers published between January 2022 and June 2025 across leading publishers such as ACM Digital Library, Frontiers, Wiley Online Library, IGI Global, Nature, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, Taylor & Francis, Sage, BMC, and Google Scholar, the study explores the integration of these advanced technologies to address emerging threats. It highlights the use of DL in intrusion detection, anomaly detection, and biometric authentication to protect digital learning platforms. It also examines how CV techniques, such as facial recognition, behavioral analysis, and emotion detection, enhance security and foster adaptive learning environments. The survey also addresses key challenges, including data quality, model interpretability, computational costs, and ethical considerations. By identifying research gaps and proposing future directions, this survey offers valuable insights for researchers, educators, and policymakers aiming to develop robust, scalable, and ethical AI-driven cybersecurity solutions for smart education.

## 1. INTRODUCTION

Education has undergone significant evolution, and in today's digital age, it continues to undergo profound transformations [1]. The rapid advancement and widespread adoption of information technology have positioned smart education as a central trend in modern education. Smart education and innovative learning approaches are progressively replacing traditional

*Corresponding author. Email: a.guma@muni.ac.ug

teaching methods by transforming how instruction, management, and services are delivered, making them more intelligent and efficient [2]. According to Shu and Gu [3], Badshah et al. [4], and Aggarwal et al. [5], smart education, also known as Education 4.0, is defined as the use of advanced technologies like artificial intelligence, big data, cloud computing, and the Internet of Things (IoT) to enhance learning to create a more personalized, interactive, and efficient educational environment by integrating these tools into the teaching and learning process. E-learning, online tutorials, massive open online courses (MOOCs), mobile education (M-education), and other innovative learning methods are being increasingly adopted across education systems worldwide [6]. The use of smart education surged dramatically after the COVID-19 pandemic, as the global shift to remote communication led to the rapid adoption of these technologies [7].

Smart education integrates smart universities, classrooms, and learning environments, all centered on intelligence, adaptability, transparency, and personalized learning. It utilizes technologies such as artificial intelligence and machine learning to power adaptive systems, automate grading, and provide customized learning recommendations. IoT devices and wearables collect real-time data to support contextual and inclusive learning, particularly for students with remote learning or disabilities. Cloud computing enables scalable, accessible virtual classrooms, while Blockchain secures academic records, verifies credentials, supports content sharing, and simplifies tuition processes. Edge computing ensures faster, local data processing, though infrastructure challenges persist. Educational robots and collaborative robots (cobots) enhance hands-on learning and teamwork through human–robot interaction. Augmented reality and virtual reality technologies immerse learners in experiential, personalized environments, particularly in fields such as engineering and healthcare. With 6G connectivity, virtual classrooms benefit from high-quality, 360-degree streaming, while advanced analytics and big data empower educators to monitor performance and personalize instruction. Smart devices and platforms further boost access, motivation, and DL [3][4][8-10]. These technologies require innovative, flexible pedagogies that promote inclusive, human-centered education [9]. At its core, smart education relies on smart learners, effective pedagogies, and supportive environments, where learners develop both hard and soft skills, educators foster engagement and collaboration, and knowledge exchange flourishes. Ultimately, it cultivates adaptable, innovative, and socially skilled individuals [11].

The global smart education market reached approximately US$395 billion in 2024 and is projected to grow at a compound annual growth rate (CAGR) of 22.5%, reaching US$484 billion by 2025 and US$1,079 billion by 2029. This rapid growth is fueled by the widespread adoption of AI, IoT, virtual reality/augmented reality, data analytics, and cloud-based platforms. In recent years, the market has expanded exponentially, driven by increased access to remote and customized learning, the growing demand for flexible and accessible education options, rising Internet penetration, and strong support through government initiatives and corporate funding. The continued shift toward e-learning methods is expected to further accelerate this upward trajectory.

Smart education integrates context-awareness, adaptive support, and flexible interfaces that respond to each learner's real-world and online circumstances. Smartphones, laptops, and wearables facilitate personalized interactions and immerse students in authentic contexts. A smart learning environment continuously adjusts tasks, interfaces, and feedback to provide cross-context support tailored to individual needs [12]. It rests on six key pillars: seamlessly embedding ICT into teaching for interactive learning; delivering personalized, adaptive content to meet diverse student needs; leveraging data analytics to inform decisions and monitor progress; promoting lifelong learning through easily accessible online resources; blending online and offline methods in flexible hybrid models; and ensuring robust digital infrastructure with reliable Internet, devices, and software [13].

Smart education leverages advanced technologies to enhance academic performance, personalize learning at scale, and improve efficiency by automating administrative tasks, allowing teachers to focus more on pedagogy. It engages students through interactive, multimedia, and gamified content, making complex concepts accessible and motivating learners, especially those with strong knowledge-seeking tendencies [14]. By supporting personalized learning paths, smart education enables students to progress at their own pace with targeted support, improving concentration and success rates [15]. It promotes flexible, mobile, and autonomous learning, increasing accessibility for remote and underserved communities. Smart classrooms foster higher-order thinking, digital literacy, and professional skills essential for the 21st century, while providing teachers with immediate feedback and data analytics to tailor instruction [15][16]. Additionally, smart education encourages collaboration, creativity, and intercultural understanding, preparing learners for a digital society and lifelong success [16]. It drives sustainable development by adapting rapidly to changing educational needs. It expands access to quality education worldwide through online and hybrid models, breaking traditional boundaries and fostering global learning networks [11][14-21]. Ultimately, smart education addresses the growing demand for upskilling and reskilling, promotes lifelong learning, and creates a more efficient, inclusive, and adaptable learning environment for students, faculty, and administrators [9][22].

These advancements have revolutionized the learning experience, but they have also introduced new cybersecurity threats and vulnerabilities. These include privacy violation, unauthorized access and data breaches, phishing and social engineering attacks, man-in-the-middle (MitM) attacks, credential stuffing and brute force attacks, distributed denial-of-service (DDoS) attacks, malware and ransomware infections, eavesdropping and data interception, insider threats, zero-day exploit, SQL

injection and session hijacking, IoT-related vulnerabilities, Insecure network communications, weak authentication, third-party service risks, software vulnerabilities, physical security risks, and unsecured Bring Your Own Device (BYOD) policies [4][9][22-34]. The stakes are exceptionally high because schools increasingly depend on digital infrastructures for both administrative and educational functions, and any compromise could expose sensitive student information and severely disrupt the learning process.

Traditional cybersecurity measures form a critical foundation, but they often fall short against the evolving and complex threats targeting smart education environments. To address these challenges, researchers are leveraging DL and CV to strengthen cybersecurity and provide more adaptive, intelligent defenses. DL and CV algorithms offer robust solutions for detecting anomalies, monitoring behavior, and identifying threats within large datasets, thereby addressing the challenges that traditional security measures face in combating sophisticated attacks. DL significantly enhances cybersecurity in smart education environments by enabling advanced, real-time detection and prevention of evolving cyber threats, including malware, phishing, intrusion attempts, and deepfake misinformation. Techniques such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) automatically extract complex features from diverse, high-dimensional data generated by IoT devices, smart classrooms, and digital platforms, outperforming traditional methods in terms of accuracy and scalability. Deep learning-driven intrusion detection systems continuously adapt to new threats, including zero-day attacks. At the same time, self-supervised frameworks reduce reliance on labeled data and enhance autonomy in dynamic educational networks. By modeling user behavior over time, DL enables the identification of insider threats and anomalous activities with high precision. Moreover, adaptive and federated learning approaches enable privacy-preserving, distributed cybersecurity defenses across edge and cloud infrastructures, maintaining robustness in decentralized smart education settings. Beyond defense, DL powers adaptive cybersecurity education tools that personalize learning, simulate realistic attack scenarios, automate assessment, and safeguard platform integrity [35-53]. Computer vision strengthens cybersecurity in smart education by enabling real-time monitoring, threat detection, and anomaly recognition across physical and digital environments. It powers advanced applications such as person and weapon detection, behavioral analysis, and biometric access control to secure school facilities and prevent unauthorized entry. In network security, vision-based techniques, such as CNNs, analyze visual representations of data to identify malware and traffic anomalies with high accuracy and scalability. Computer vision also detects forgeries, deepfakes, and phishing attempts by scrutinizing visual inconsistencies in images, videos, and documents. By integrating physical surveillance with cyber data through multi-modal fusion, CV provides unified threat intelligence that identifies insider risks and correlates physical and network anomalies. This synergy improves situational awareness, supports human operators with automated alerts and forensic evidence, and enables predictive threat analysis. Despite challenges such as adversarial attacks and evolving threats, CV delivers intelligent, context-aware security solutions that make smart educational environments safer, more accessible, and more resilient [36][44][54-60]. These innovations provide intelligent, scalable, and robust security solutions that safeguard sensitive data and IoT devices while upholding educational integrity in increasingly connected and distributed learning environments. By leveraging emerging technologies, intelligent systems enhance cybersecurity in smart education, safeguarding sensitive information and ensuring the confidentiality, integrity, and availability of critical data and platforms [51][61].

This survey examines how DL and CV techniques can improve the security of smart education systems. It aims to offer a comprehensive understanding of their potential to strengthen security by enabling more adaptive and intelligent defense mechanisms. The contributions of this survey are:

- To examine the major security threats, attacks, and challenges encountered by smart education systems.
- To describe the role of DL and CV in strengthening cybersecurity measures for smart education platforms.
- To explain the synergistic integration of DL and CV for enhancing cybersecurity in smart education.
- To identify the challenges and limitations encountered when implementing DL and CV to strengthen cybersecurity measures for smart education platforms.
- To highlight the future research directions.

This survey is structured as follows: Section 2 outlines the materials and methods used in the study, while Section 3 provides a review of the current state of the art. Section 4 examines security threats and attacks in smart education, and Section 5 discusses how DL and CV techniques enhance this domain. Section 6 presents the challenges and limitations encountered during the implementation of DL and CV in securing smart education. Section 7 explores the key future research directions, and Section 8 concludes the survey.

## 2. MATERIALS AND METHODS

The survey comprehensively explores and synthesizes current research on the integration of DL and CV techniques for enhancing cybersecurity in smart education environments. The goal was to identify, categorize, and analyze existing approaches, highlighting their strengths, limitations, and open challenges, to provide a roadmap for future research. The

authors achieved this by conducting a comprehensive literature search across several academic databases, including ACM Digital Library, Frontiers, Wiley Online Library, IGI Global, Nature, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, Taylor & Francis, Sage, BMC, and Google Scholar. They focused on publications from January 2022 to June 2025. They used a combination of keywords and Boolean operators, including terms like "smart education" OR "intelligent tutoring systems" OR "e-learning" AND "cybersecurity" OR "cyber threats" OR "attack detection" AND "DL" OR "neural networks" OR "machine learning" AND "CV" OR "image analysis" OR "visual surveillance." They refined the search using Boolean logic to target relevant subdomains and limited the results to peer-reviewed journal articles, conference papers, and book chapters written in English.

The researchers ensured the relevance and quality of the selected studies by applying specific inclusion and exclusion criteria. They included studies that explicitly addressed cybersecurity issues within smart or digital education systems, incorporated DL and/or CV techniques for detecting, preventing, or mitigating cyber threats, and presented original research, reviews, frameworks, or empirical evaluations published in English between January 2022 and June 2025. They excluded studies unrelated to education or focused solely on general cybersecurity without an educational context, as well as research studies lacking technical depth, such as news reports, editorials, and extended abstracts. Additionally, they removed duplicates or redundant publications by the same authors with overlapping content. Research studies published before January 2022 and those in languages other than English were also excluded.

The selection process adhered to the PRISMA guidelines and involved four stages: (1) identifying studies by screening titles and abstracts for relevance, (2) retrieving and assessing full texts based on predefined inclusion and exclusion criteria, (3) evaluating methodological quality and technical relevance, and (4) including 202 studies in the final analysis. To comprehensively examine these studies, the researchers developed a multi-dimensional classification framework. They categorized each study according to cybersecurity objectives (e.g., authentication, intrusion detection, data privacy, user behavior analysis), DL models (e.g., CNNs, RNNs, Long Short-Term Memory networks, Autoencoders, Generative Adversarial Networks, Transformers), CV tasks (e.g., facial recognition, behavioral monitoring, object detection, visual anomaly detection), and application contexts, e.g., virtual classrooms, learning management systems (LMS), examination proctoring, biometric access control.

Five reviewers manually extracted and independently verified the data, documenting the authors and publication year, methodologies and algorithms used, datasets and experimental setups, cybersecurity goals addressed, and performance outcomes with comparative baselines for each selected study. Out of the 202 research studies selected from various digital libraries for the final analysis, 3 from ACM Digital Library, 2 from Frontiers, 1 from Wiley Online Library, 3 from IGI Global, 3 from Nature, 26 from Springer, 29 from ScienceDirect, 22 from MDPI, 36 from IEEE Xplore Digital Library, 2 from Taylor & Francis, 1 from Sage, 1 from BMC, and 73 from Google Scholar. Fig. 1 illustrates how these research papers selected for the survey are categorized.

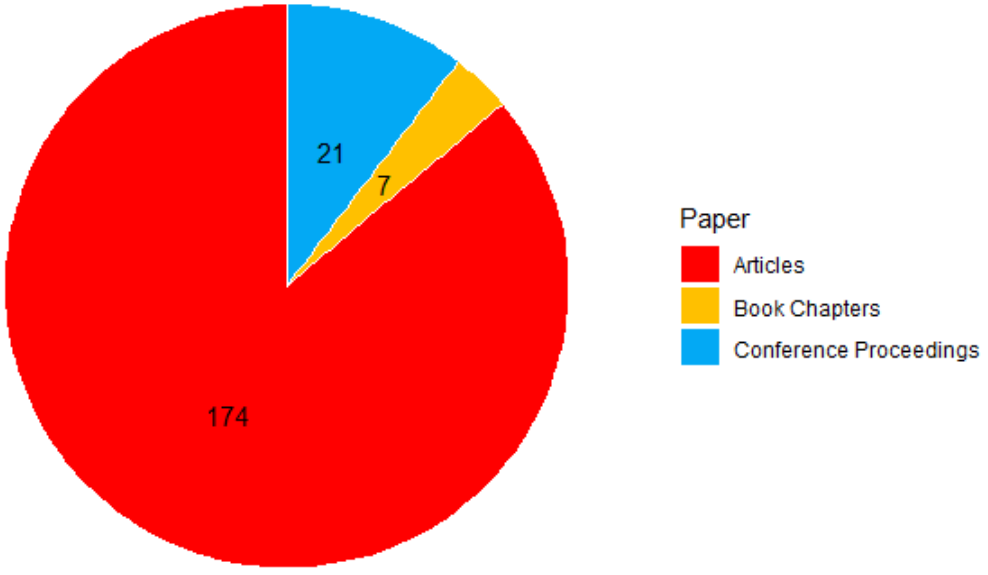


Fig. 1. Illustrates the categories of these research papers.

Fig. 2 shows the digital databases used to retrieve the research papers for this survey.

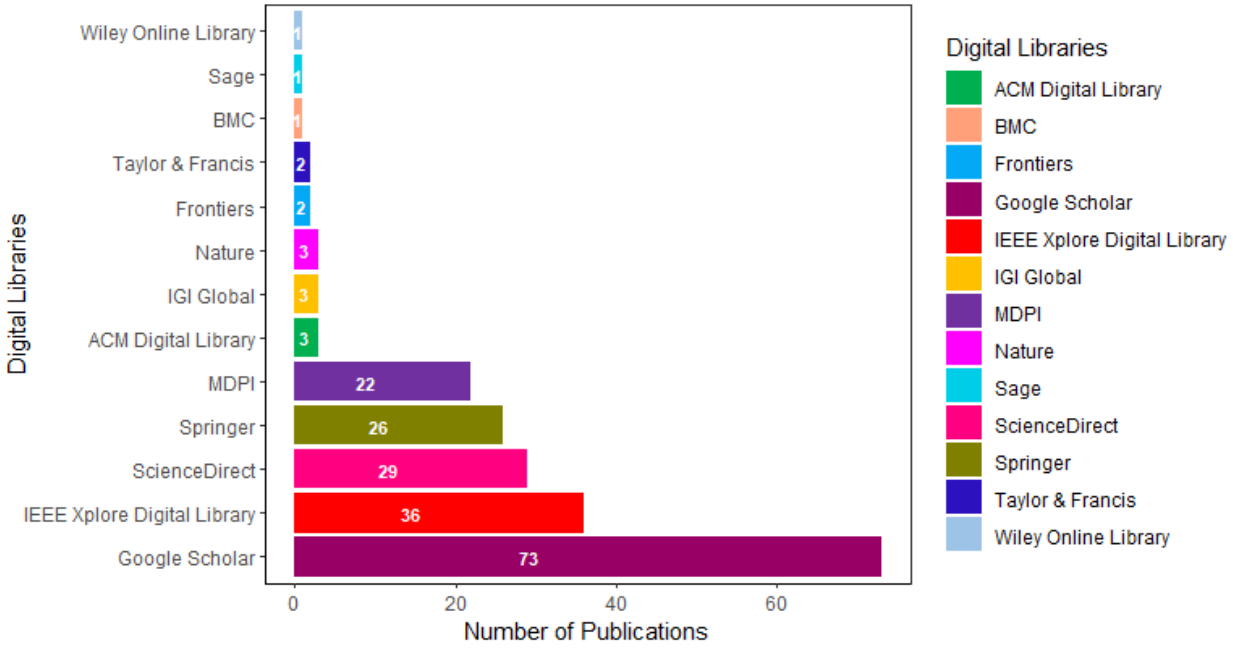


Fig. 2. Illustrates the digital databases used to retrieve the research papers for this survey.

Fig. 3 illustrates the distribution of research paper sources across various digital libraries.

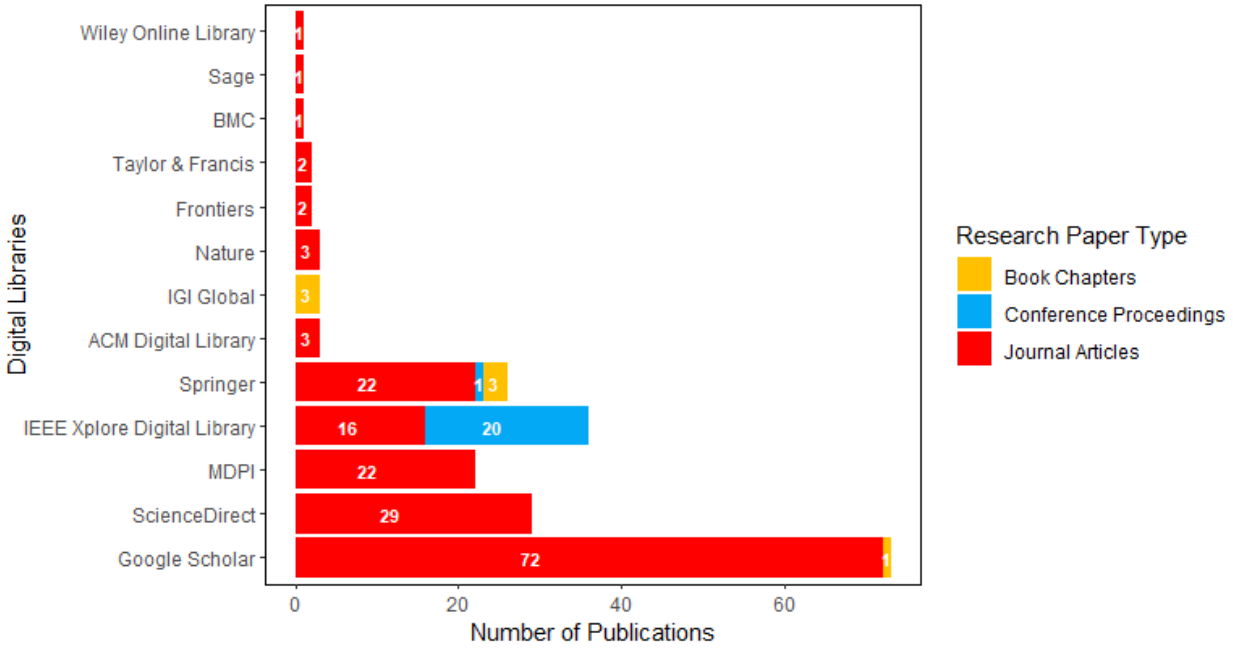


Fig. 3. Illustrates the distribution of research paper sources across various digital libraries.

Fig. 4 shows how digital libraries distribute the selected papers by publication year.

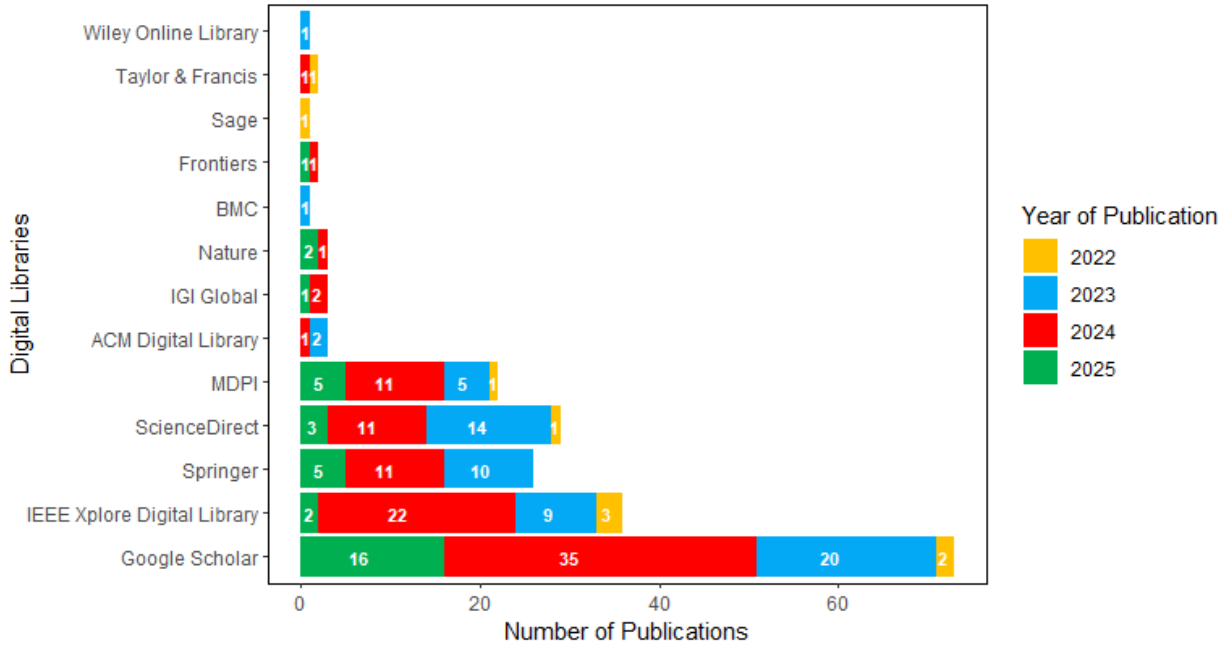


Fig. 4. Shows how digital libraries distribute the selected papers by publication year.

The researchers conducted a comprehensive analysis of selected studies to examine how DL and CV techniques enhance cybersecurity in smart education environments. They gathered data on publication details, research focus, technologies used, such as DL models and CV algorithms, and cybersecurity domains addressed, including authentication, intrusion detection, and data privacy. They categorized each study by its application area, ranging from student behavior monitoring to biometric authentication and anomaly detection.

Using qualitative synthesis and thematic analysis, they organized the studies by application areas and smart education domains and further classified them based on the technological approaches employed. To validate their findings, they consulted subject matter experts, cross-referenced results with existing literature, and critically assessed the robustness of their conclusions. They evaluated each study's quality based on methodological rigor, the reliability and validity of findings, and relevance to the use of DL and CV in cybersecurity for smart education. As the review relied solely on secondary literature, no primary data collection was necessary, and therefore, no ethical approval was required. However, the researchers adhered to ethical standards by properly citing sources and avoiding plagiarism.

Although these criteria provide a structured framework for the review, they also introduce several limitations and potential biases. First, limiting the time frame to studies published between January 2022 and June 2025 may exclude foundational research that offers critical insights into the evolution of DL and CV in smart education. Second, by focusing solely on DL and CV, the review may overlook interdisciplinary or comparative studies that could enrich the understanding of their interaction with other educational technologies. Third, restricting the review to English-language publications introduces language bias and excludes valuable research published in other languages, thereby limiting the global perspective. Fourth, narrowing the scope to peer-reviewed literature may omit cutting-edge research presented in non-traditional formats, such as technical reports or corporate research from organizations like Google AI or DeepMind. While peer-reviewed sources emphasize established methodologies, non-peer-reviewed work often explores experimental or emerging approaches. Moreover, the absence of quantitative data may weaken the review's analytical depth, as qualitative evaluations alone provide limited support for claims. This focus on theoretical perspectives may also cause the review to overlook practical implementation challenges, thereby reducing its relevance as smart education technologies continue to evolve.

## 3. STATE-OF-THE-ART

### 3.1. Overview of Smart Education

The concept of smart education continues to evolve and varies across institutional, national, and regional contexts. Smart education is a technology-enhanced learning paradigm for the digital age that advances beyond traditional web-based, mobile, and ubiquitous learning. It prioritizes effective technological design and innovative pedagogical strategies to boost learning efficiency and effectiveness [3][62]. It is also described as a self-regulated, motivated, flexible, and resource-rich system that connects smart students, smart pedagogy, and smart environments, encompassing both formal and non-formal

settings, and promotes personalized learning to help students acquire essential knowledge, skills, and competencies [62]. Smart education integrates features such as adaptive and personalized learning, intelligent tutoring systems, real-time emotion recognition, IoT-enabled smart classrooms, collaborative tools, multimodal learning support, gamification, and interactive learning [63]. Fig. 5 illustrates an environment where these elements collaborate to create a dynamic, learner-centered educational experience.

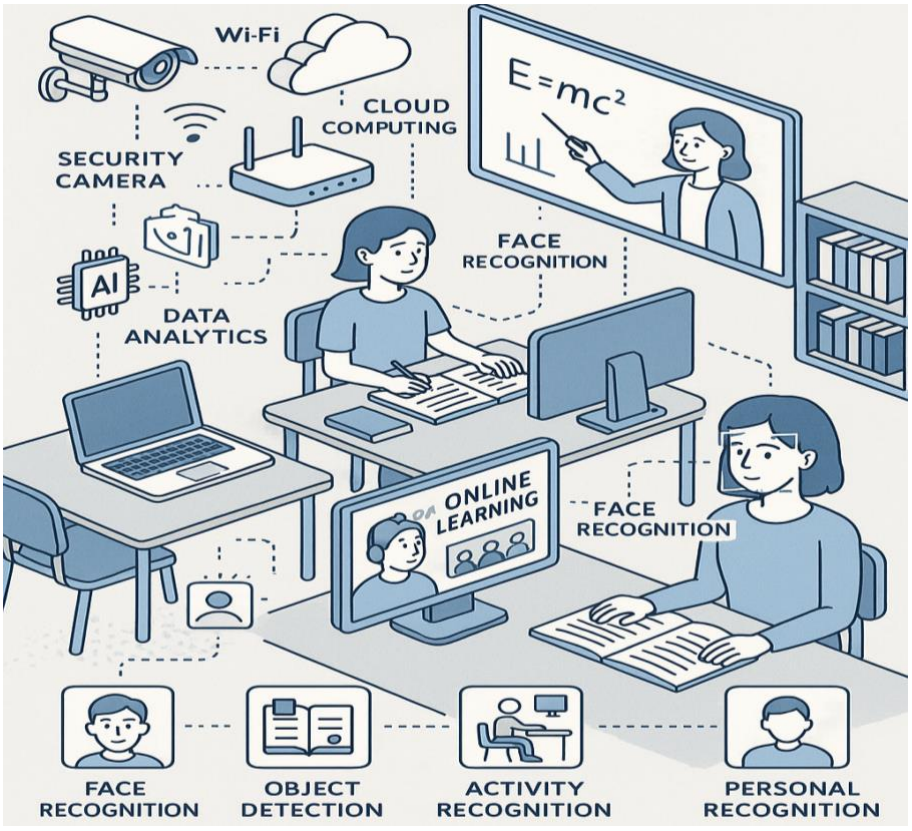


Fig. 5. Illustrates a smart education environment.

A complete smart education system relies on three key elements: smart learners, smart pedagogies, and smart environments [64]. Smart learners not only develop sustainable hard skills but also cultivate essential soft skills, including personal and social competencies such as communication, teamwork, negotiation, and leadership [11]. Smart pedagogies utilize ICT tools and innovative teaching techniques to create meaningful and high-quality learning experiences for future educators, enabling them to understand and engage in activities relevant to modern learning [65]. Smart environments integrate software, hardware, digital resources, and learner-centered pedagogies to accommodate students from diverse backgrounds, proficiency levels, and interests, ultimately fostering the development of crucial skills [11][66].

## 3.2. Development Stages of Smart Education

Smart education has progressed through four distinct stages, each shaped by advances in technology, evolving pedagogical theories, and changing educational practices. From 1983 to 2007, smart education began to emerge, laying the groundwork for its development. Between 2008 and 2012, it evolved further as new tools and methods enhanced learning experiences. From 2012 to 2018, scholars focused on theorizing smart education, developing conceptual frameworks and models. Since 2019, educators and institutions have applied these theories and technologies in practice [17].

### 3.2.1. Emerging stage (1983–2007): Foundation and early concepts

From 1983 to 2005, the term “smart education” began to appear, although “smart” primarily described the cultivation of human wisdom rather than advanced technologies. During this period, foundational technologies and conceptual frameworks that would later define smart education started to develop. The widespread use of personal computers, the growth of the Internet, and the introduction of early computer-assisted instruction characterized this stage. While the concept of “smart education” had not yet been fully established, key elements, such as digital learning materials, multimedia teaching tools, and early adaptive learning systems, emerged to support teaching and learning. Efforts during this phase focused on using technology to enhance traditional instructional methods rather than to fundamentally transform educational models [17].

### 3.2.2. Evolving stage (2008–2012): Rise of smart technologies in education

During this stage, the integration of mobile technologies, cloud computing, and data analytics significantly advanced educational tools and environments. The emerging concept of "smart education," inspired by the broader "smart" paradigm in urban development and information systems, gained widespread attention. Educational platforms evolved to offer more interactive and personalized experiences, featuring real-time feedback, mobile learning, and early forms of learning analytics. As a result, educators and developers increasingly focused on learner-centered approaches that enhance flexibility, engagement, and customization in the learning process [17].

### 3.2.3. Theorizing stage (2012–2018): Conceptual consolidation and research expansion

During this period, scholars and institutions formalized the concept of smart education by defining its scope, principles, and goals, connecting it to theories such as ubiquitous learning, personalized learning, and intelligent environments. Researchers intensified their efforts to integrate AI, big data, and the IoT into education, highlighting how these technologies can enable adaptive learning paths, competency-based instruction, and real-time monitoring. They also broadened the focus to address ethical considerations, digital literacy, and equitable access [17].

### 3.2.4. Application stage (2019–Present): Implementation and system integration

The current stage of education is characterized by the widespread implementation and institutionalization of smart education practices, which have been rapidly accelerated by global events such as the COVID-19 pandemic. Educational systems adopt AI-driven platforms, virtual and augmented reality tools, and cloud-based learning ecosystems to create smart classrooms, intelligent tutoring systems, and data-informed decision-making processes across all levels. They focus on delivering personalized, adaptive learning tailored to individual needs while building holistic, scalable, and sustainable environments that support diverse learners and promote lifelong learning through flexible, remote options. Institutions cultivate critical thinking, problem-solving, creativity, and digital literacy skills because these abilities are essential for success in today's workforce [10][17]. Fig. 6 summarizes the essential technologies involved in the four stages of smart education development.

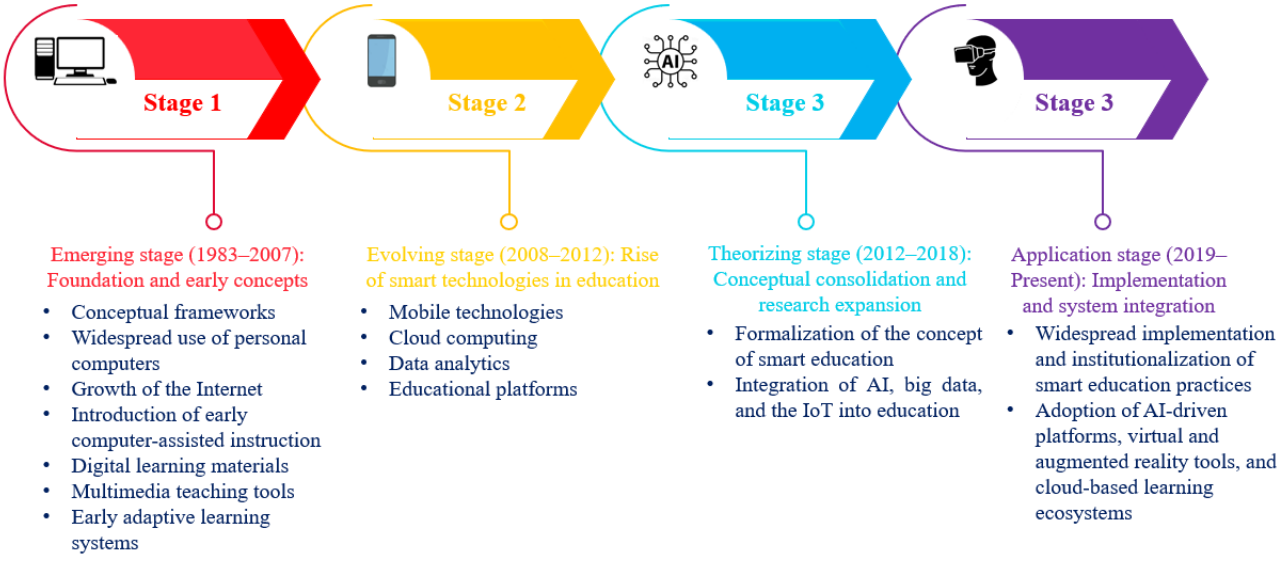


Fig. 6. Summary of the essential technologies involved in the four stages of smart education development.

## 3.3. Key Enabling Technologies in Smart Education

Smart education relies on several key technologies, which are briefly described below.

### 3.3.1. Internet of Things (IoT)

The IoT connects physical devices, vehicles, buildings, and other objects embedded with sensors, software, and network capabilities, enabling them to collect and exchange real-time data. In education, the IoT plays a crucial role by integrating diverse devices into learning environments, transforming traditional teaching into dynamic, personalized, and collaborative experiences. For instance, smart whiteboards enhance interactivity and resource sharing in classrooms. IoT supports Education 4.0 by improving learning outcomes, increasing student engagement and retention, and facilitating task-based learning, inclusiveness, remote education, and resource management. It enables students and teachers to stay connected and access support at any time, promoting inclusivity by aiding students with disabilities through technologies such as automated

translation, augmented reality, virtual reality, and smart navigation tools. Remote learning platforms such as Google Classroom and Tynker exemplify IoT-enabled global connectivity and flexible learning. Additionally, IoT tracking systems enhance student safety and provide valuable insights to educators while automating administrative tasks, reducing teachers' workload, and allowing them to focus on meaningful academic activities [9][10].

### 3.3.2. Big data

Big data encompasses vast amounts of structured and unstructured information that is difficult to manage but crucial for informed decision-making, significantly transforming sectors such as education. In the context of Industry 5.0, big data enables educational institutions to personalize learning, monitor student engagement and performance, and align curricula with industry needs through predictive modeling and data-driven insights. By integrating big data with technologies such as Blockchain and LMS, institutions can secure records, track student interactions, provide real-time feedback, and offer personalized recommendations. Applications such as student monitoring systems and automated evaluation tools utilize big data to predict concentration levels, identify students who are disengaged, and uncover underlying issues that affect learning. Administrative bodies leverage big data to make timely, informed decisions that address evolving market demands. Big data drives efficient resource allocation, supports distance learning, fosters continuous improvement, and strengthens educational research, ultimately making education more responsive, personalized, and aligned with the dynamic requirements of Industry 5.0 [10][67].

### 3.3.3. Artificial intelligence and machine learning

Artificial intelligence and machine learning play pivotal roles in transforming traditional education into smart, adaptive learning environments. These technologies enable machines to learn from data, recognize patterns, and make decisions with minimal human input. AI-powered tools analyze individual learning styles, preferences, and progress to deliver personalized instruction, automate assessments, and support data-driven decision-making. Intelligent tutoring systems, for example, can adjust to each learner's needs and provide targeted feedback, enhancing the learning experience in various contexts, including video games [9][67].

### 3.3.4. Robotics

Robotics technology encompasses the design, construction, and operation of robots capable of performing tasks autonomously or semi-autonomously, and its integration into education offers numerous benefits. In classrooms and training environments, robots, especially collaborative robots or "cobots," facilitate hands-on learning, teach programming and engineering concepts, assist students with special needs, and foster effective human-robot interaction [9]. Cobots enable students to conduct experiments, receive real-time guidance and feedback, and work within immersive virtual reality and augmented reality environments. They provide personalized support to students with disabilities, help them navigate learning spaces, and promote teamwork and collaboration. By taking on repetitive or hazardous tasks, cobots reduce risks and administrative burdens, such as grading, allowing teachers to focus on personalized instruction. Although their integration may require infrastructure adjustments, incur significant costs, and raise ethical and data security concerns, cobots greatly enrich the educational ecosystem. For instance, the Mirobot Professional Kit by WLKATA Robotics exemplifies a versatile cobot designed to enhance teaching and learning through precise, flexible, and multi-platform control. By working with cobots, students engage more deeply, develop critical thinking and creativity, and gain practical skills in robotics, automation, and programming—skills vital for future industry roles [10][67].

### 3.3.5. Blockchain

Blockchain is a decentralized, distributed digital ledger technology that securely records and verifies transactions across multiple computers, ensuring transparent, immutable, and tamper-resistant data storage. As an enabling technology that emphasizes human-centric collaboration, Blockchain offers significant educational benefits. It maintains the integrity of academic records, certifications, and credentials in a secure, tamper-proof manner, allowing schools and universities to store and manage students' performance records reliably and access them from anywhere. By tracking students' progress over time, educators can design personalized, effective learning experiences and securely store and share educational content. Blockchain also facilitates secure, efficient payment systems for tuition and other fees, which particularly benefits international students in distance learning programs. For example, institutions can record degrees and certificates on the Blockchain, enabling employers and other institutions to instantly verify their authenticity, reducing fraud and streamlining administrative processes. Blockchains enhance transparency, security, and efficiency, making them a transformative tool for modern education [10].

### 3.3.6. Augmented reality

Augmented reality technologies create immersive, interactive digital environments that significantly enhance education by simulating real-world scenarios and offering engaging, experiential learning opportunities. In fields such as healthcare, engineering, and architecture, students can safely practice skills in virtual settings before applying them in real-world

situations. Augmented reality combines digital visuals, sounds, and other sensory inputs to enrich traditional teaching, making lessons more interactive and improving comprehension and retention through virtual examples. It reduces training costs, enhances learner engagement, and offers flexible access to educational materials at any time and from anywhere. Augmented reality also supports inclusive education by catering to diverse learning styles and abilities, helping students with disabilities through multi-sensory experiences and improved orientation skills. In medical education, augmented reality allows students to interact with virtual anatomical models and practice complex procedures, deepening their understanding of intricate concepts. Similarly, augmented reality and virtual reality enable surgeons to rehearse challenging techniques on 3D models, thereby enhancing their skills without risk to patients. By presenting scientific and technical subjects visually, augmented reality and virtual reality boost retention rates, capitalizing on humans' strong visual learning abilities, supported by research showing that people process images far faster than text [9][10][67][68].

### 3.3.7. Virtual reality

Virtual reality is an immersive, computer-generated technology that simulates realistic or fictional three-dimensional environments, playing an increasingly vital role in education. By offering interactive, hands-on experiences, virtual reality helps students develop both technical and human-centered skills such as problem-solving and creativity. At the same time, personalized learning features track progress and adapt content to individual needs. Its remote collaboration capabilities connect geographically dispersed learners and faculty, fostering interdisciplinary teamwork. Virtual reality also provides a safe and cost-effective alternative for training in hazardous or complex scenarios, enhancing visualization to prepare workers for the evolving demands of the industry. For instance, Harvard University uses virtual reality in its introductory computer science course (CS50), allowing over three million students worldwide to feel present in a virtual lecture hall regardless of location. Teachers benefit from virtual reality's capacity to boost student engagement and creativity, supported by 3D visuals that stimulate curiosity and imagination. Moreover, virtual reality helps overcome language barriers by offering real-time translation or transcription, enabling smoother comprehension and encouraging hesitant students to interact without fear of mispronunciation [10][67][68].

### 3.3.8. 6G and Beyond

6G and beyond fulfill the requirements of a fully connected world by delivering ultra-fast, reliable wireless communication, higher data transfer rates, and increased network capacity compared to previous generations. This advanced connectivity ensures seamless communication, instant access to educational resources, and effective learning experiences through high-speed, low-latency networks. By supporting technologies such as augmented reality, virtual reality, and the IoT, 6G enables immersive, real-time educational interactions and mobile learning, allowing for learning anytime, anywhere. It fosters global collaboration among students, teachers, and experts while safeguarding sensitive data with enhanced security features. In laboratories, 6G allows remote access and control of equipment via virtual interfaces, expanding opportunities for distant learners. 6G promises to revolutionize smart education by enabling high-resolution 360° video streaming that closely replicates physical classroom presence, thereby enhancing remote learning through realistic and immersive experiences. Its ultra-low latency and dedicated bandwidth also support precise teleoperation and robotics integration, empowering students to engage in dynamic, interactive, and adaptive learning environments that redefine smart education [10].

### 3.3.9. Edge computing

Edge computing decentralizes computation and data storage by moving them closer to the network's edge, enabling devices near end users—known as edge devices—to process and manage data locally. In education, where numerous IoT devices and sensors collect diverse student data, edge computing efficiently handles large data volumes, supports real-time tracking of student progress, and allows personalized instructional strategies. By processing sensitive information locally, edge computing enhances security and privacy, reducing the risks of data breaches and unauthorized access. It also enables seamless interaction in virtual classrooms and enriches learning experiences through low-latency communication. For instance, sensors in a smart classroom can record attendance and process the data on-site, eliminating the need for cloud validation and providing immediate insights. Edge computing offers substantial benefits, including faster processing, reduced latency, improved resource management, and enhanced real-time analytics. Integrating Blockchain with edge computing can secure student records, credentials, and credit transfers. Blockchain ensures that digital certificates remain tamper-proof and verifiable even if the issuing institution ceases to exist, eliminating intermediaries and enabling smart contracts for automatic credit transfers. Educators can also timestamp and track open educational resources on the Blockchain, supporting copyright protection and usage monitoring [10]. By combining edge computing and Blockchain, institutions can significantly enhance data security, streamline administrative processes, and elevate learning outcomes.

### 3.3.10. Advanced analytics

Educators in smart education utilize advanced analytics, including predictive and prescriptive techniques, to analyze historical data, forecast trends, and recommend optimal actions. By uncovering patterns in student performance, behavior, and engagement, they make informed, data-driven decisions that boost student success and enhance learning outcomes [9].

Adaptive learning systems further individualize education by adjusting content pace and assessments according to each student's mastery level and activity patterns, providing tailored support that meets evolving educational needs. Moreover, AI-driven learning models foster greater collaboration, creativity, and academic achievement within structured learning environments [67]. Fig. 7 summarizes the key enabling technologies in smart education.

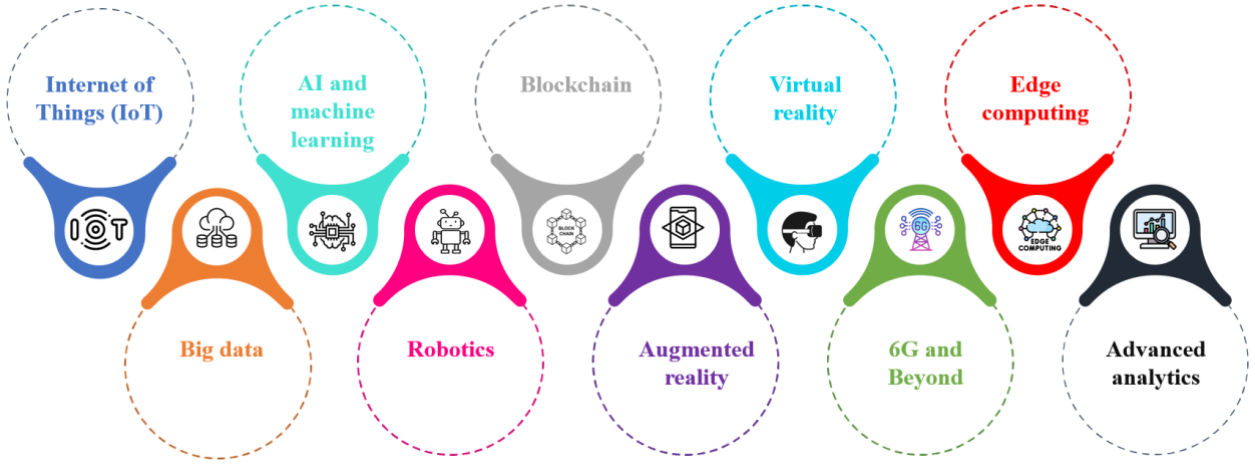


Fig. 7. Summary of the key enabling technologies in smart education.

## 3.4. Benefits of Smart Education

Table 1 provides brief descriptions of the benefits of smart education.

TABLE I: SUMMARY OF KEY BENEFITS OF SMART EDUCATION.

| S/No | Benefits | Brief Description | References |
|---|---|---|---|
| 1 | Personalized learning | Smart education platforms often adapt to individual learning styles and paces by tracking students' progress, pinpointing areas where they need extra support, and offering customized resources and activities. For example, when a student finds mathematics challenging, the platform offers easier problems and suggests extra videos to help build a stronger understanding. Conversely, if a student excels, the platform can introduce more challenging issues to foster further growth. | [69][70] |
| 2 | Improved communication and collaboration | Smart education technologies facilitate effective communication among learners, teachers, parents, and administrators by utilizing email, online platforms, and messaging applications, thereby creating a more connected teaching and learning community. For example, teachers can quickly share assignments, provide feedback, and send updates. | [71] |
| 3 | Data-driven insights | LMS and other intelligent education platforms generate valuable data about student performance, enabling teachers and administrators to identify learning gaps, track progress, and adjust their teaching strategies as needed. | [72] |
| 4 | Enhanced engagement and motivation | Digital tools, including multimedia content, interactive simulations, and educational games, engage students and make learning more enjoyable. These resources capture students' attention and spark greater interest in the subject matter. For example, rather than simply reading about historical events, students can watch videos or explore virtual reality simulations that create a more immersive learning experience. | [69] |
| 5 | Mobility, ubiquity, continuity, and ease of access | Smart education uses mobile and wireless networks to enable learning beyond traditional classroom boundaries and schedules. By making educational resources and opportunities available anytime and anywhere, it integrates learning seamlessly into daily life and ensures continuous access. This ubiquity bridges formal and informal learning environments, enabling students to engage with content and collaborate seamlessly. Many smart education tools prioritize user-friendly design, ensuring that learners from diverse backgrounds and with varying technical skills can easily navigate and benefit from these resources and platforms. | [73-75] |
| 6 | Environmental sustainability | Smart education contributes to environmental sustainability by minimizing the use of physical resources such as textbooks and paper. Online learning platforms lower the carbon footprint by reducing the demand for printed materials and decreasing the need for commuting, which in turn lessens the environmental impact compared to traditional education systems. | [76] |

## 3.5. Smart Education Platforms

Table 2 provides an overview of smart education platforms that support and advance educational sustainability. By integrating advanced technologies with innovative teaching methods, these platforms optimize learning processes, minimize resource use, and promote sustainable practices that ensure long-term benefits for education systems.

TABLE I. OVERVIEW OF SMART EDUCATION PLATFORMS.

| S/No | Platform | Brief Description | References |
|---|---|---|---|
| 1 | Blackboard | Blackboard has a range of tools that enable educators to design interactive lessons and manage assessments with flexibility. It supports virtual classes, allowing students to learn remotely while engaging in interactive discussions. This approach strengthens both self-directed learning and collaborative education, making the learning experience more effective and dynamic. | [67] |
| 2 | Moodle | This platform creates an inclusive learning environment by providing forums, interactive activities, and self-assessment tests. It enables educators to tailor content to students' individual needs and supports continuous evaluation, ensuring a focused and effective learning experience. | [67] |
| 3 | Zoom | Zoom is a leading online meeting platform that facilitates live lectures and discussion sessions, helping reduce the need for travel and saving time and resources for both students and teachers. By streamlining communication and minimizing physical mobility, Zoom supports a more sustainable and efficient educational process. | [67] |
| 4 | Canvas | Canvas enables teachers to design flexible educational content, such as online lectures and assignments while fostering dynamic interaction with students. By promoting continuous communication and collaboration, the platform enhances the overall learning experience and facilitates the achievement of exceptional educational outcomes. | [67] |
| 5 | Schoology | Schoology enables educators to design curricula, manage duties, and assess students' academic progress effectively. It fosters collaboration between students and teachers through interactive features, such as group discussions and projects, which enhance the overall quality of education. | [67] |
| 6 | Google Classroom | The platform integrates seamlessly with other Google tools, enabling teachers to distribute assignments and assessments with ease. It also offers an interactive space where students can submit their work and receive direct feedback, fostering effective communication and enhancing knowledge sharing. | [67] |
| 7 | Coursera | Coursera offers thousands of online courses from leading universities worldwide, provides certified certificates, and actively supports continuous education and professional skills development to enhance students' opportunities in the labor market. | [67] |
| 8 | Udemy | Udemy offers a diverse range of online courses across multiple fields, enabling learners to access flexible content that supports continuous education and professional growth. It also allows instructors to create and share training courses, enriching the platform's content and expanding learning opportunities worldwide. | [67] |
| 9 | Khan Academy | Khan Academy provides a vast library of educational videos and interactive exercises across numerous subjects. Students can access this platform at any time and from anywhere, allowing them to take control of their learning and enhance their individual educational experience. | [67] |
| 10 | Duolingo | Duolingo makes language learning fun and interactive by using games and exercises that engage learners and tailor content to their skill level. This approach makes it an ideal tool for both beginners and more advanced learners. | [67] |

## 3.6. Security Threats and Attacks in Smart Education

Integrating smart technologies into modern educational environments provides. However, these technologies also create serious security risks and open potential attack vectors that threaten the confidentiality, integrity, and availability of smart educational data and services. Below are brief descriptions of the various security threats and attacks that smart education systems face.

### 3.6.1. Privacy violation

Smart education uses advanced technologies to enrich teaching and learning experiences. However, these technologies continuously collect, process, and store large volumes of sensitive personal information, which raises serious privacy concerns. Smart classrooms, for example, may deploy facial recognition cameras to monitor attentiveness, emotion-detection software to assess engagement, and wearable devices to track physiological signals, such as heart rate and stress levels. While these tools aim to personalize learning and boost academic performance, they simultaneously generate detailed student profiles that can be misused or inadequately safeguarded. Unauthorized sharing of student data with third-party providers and EdTech companies often results in targeted advertising without explicit consent, leaving students and parents insufficiently informed about data usage and storage. Weak cybersecurity measures further heighten the risk, as cyberattacks on educational institutions and EdTech platforms have exposed sensitive information, including grades and disciplinary histories, leading to identity theft and reputational harm. Moreover, some smart learning applications embed location-tracking features that monitor students outside the classroom, raising ethical concerns about surveillance and autonomy. Researchers have extensively examined privacy risks and proposed various solutions to mitigate illegitimate data access and

ensure authenticated data handling, highlighting the urgent need for robust privacy protections in smart education [4][9][12][27][67].

### 3.6.2. Unauthorized access and data breaches

The integration of smart technologies in education has significantly improved teaching and learning, but has also introduced substantial security risks, including unauthorized access and data breaches. Unauthorized access occurs when individuals infiltrate educational systems without permission, often exploiting weak passwords, phishing attacks, or software vulnerabilities, enabling them to alter records, steal sensitive data, or disrupt system operations, as seen in the 2020 Clark County School District ransomware attack. Similarly, data breaches involve the unauthorized extraction or exposure of protected information, such as students' academic records, health data, financial details, and behavioral analytics, as exemplified by the 2017 Edmodo breach, which compromised 77 million user accounts. Smart classroom IoT devices, including smart whiteboards, connected projectors, and student tablets, often lack robust security measures, making them easy targets for attackers if they run outdated firmware or lack proper authentication. Internal threats, such as careless or malicious actions by staff, accidental leaks, or the abuse of privileges, also contribute to data breaches. Additionally, social engineering and phishing attacks trick employees into revealing confidential information or performing harmful actions, bypassing technical safeguards. These vulnerabilities, if left unaddressed, can lead to severe privacy violations, financial losses, reputational damage, and non-compliance with regulations, underscoring the urgent need for comprehensive security measures in smart education environments [22].

### 3.6.3. Phishing and social engineering attacks

Phishing and social engineering attacks create significant security challenges in smart education environments. As educational institutions increasingly rely on digital platforms, cloud-based LMS, and interconnected smart devices, cybercriminals find more opportunities to exploit vulnerabilities. Phishing involves tricking users into revealing sensitive information, such as login credentials or financial data, through emails, messages, or websites that appear legitimate. Attackers often pose as trusted entities, such as university IT departments, faculty, or administrative offices, to deceive students, instructors, and staff. For example, an attacker might send a fake LMS password reset request, prompting recipients to enter their credentials on a counterfeit site, which criminals then use to access course materials, alter grades, or infiltrate institutional networks. Social engineering encompasses a broader range of deceptive tactics that exploit human psychology to gain unauthorized access, including pretexting (posing as support staff), baiting (leaving infected USB drives on campus), and tailgating (following authorized individuals into restricted areas). Attackers may also exploit online collaboration tools and virtual classrooms by impersonating guest lecturers to eavesdrop or steal data. These threats thrive in academic settings due to high student turnover, varying levels of cybersecurity awareness, and the collaborative nature of education. The widespread use of IoT-enabled devices, such as smartboards, projectors, and remote learning tools, further increases the attack surface if institutions lack strong authentication and robust network security. Notably, cybercriminals often impersonate trusted parties to breach credentials and internal systems, making phishing hard to detect due to the close resemblance of fake and genuine messages. For instance, a 2020 phishing attack cost a college approximately €30,000 in recovery expenses, and a separate password compromise that year impacted users at multiple universities, compromising around 1,000 accounts and requiring nearly 80 days to resolve [29][30][33].

### 3.6.4. Man-in-the-middle (MitM) attacks

A MitM attack is a cyber threat where an attacker secretly intercepts and potentially alters communication between two parties who believe they are communicating directly. In smart education systems, MitM attacks pose serious security risks by compromising sensitive data and eroding trust. These environments rely on network connections through Wi-Fi or the Internet, linking various devices and tools such as online learning platforms, video conferencing systems, digital assessments, and smart classroom equipment. Attackers can position themselves between a student's or teacher's device and the educational server or LMS, enabling them to eavesdrop on data exchanges, steal login credentials, alter grades or exam content, redirect users to malicious websites, or impersonate legitimate parties. For example, attackers may intercept login information over unsecured public Wi-Fi, impersonate a university's LMS through DNS spoofing or ARP poisoning, hijack live video conferences to spy or inject disruptive content and tamper with online assessments by modifying questions or answers during transmission—seriously undermining data security and the integrity of smart education systems [77].

### 3.6.5. Credential stuffing and brute force attacks

Credential stuffing is a cyberattack in which attackers use large volumes of stolen username-password pairs—typically obtained from previous data breaches—to access user accounts on different platforms, exploiting the fact that many people reuse the same credentials across multiple services. Smart education platforms, such as online LMS, digital libraries, and virtual classrooms, often require students, teachers, and staff to log in and store sensitive data like grades, personal details, and course materials. Attackers exploit leaked credentials from unrelated breaches, e.g., a compromised social media account, to attempt automated logins on these educational systems. If a student reuses the same email and password, an

attacker can easily gain unauthorized access, manipulate grades, steal personal data, or disrupt classes. In contrast, brute force attacks involve systematically guessing every possible password or encryption key until the attacker finds the correct one. Without robust security measures, such as rate limiting or CAPTCHA, smart education platforms become vulnerable to brute force attacks targeting student, instructor, or admin accounts. For instance, an attacker might run automated software to crack a university's virtual classroom admin password, gaining control to disrupt sessions, access confidential records, or alter course content [78][79].

### 3.6.6. Distributed denial-of-service (DDoS) attacks

DDoS attacks pose a significant cybersecurity threat to smart education systems, which rely on interconnected digital platforms, online LMS, video conferencing tools, cloud services, and IoT devices. In a DDoS attack, attackers control numerous compromised devices, often as part of a botnet, to flood a targeted network or service with excessive traffic, overwhelming its bandwidth, processing power, or memory. This overload prevents legitimate users from accessing services or causes severe performance issues. In smart education, DDoS attacks can disrupt online exams, virtual classrooms, and cloud-hosted resources, resulting in class cancellations, data loss, and a decline in trust in digital infrastructure. For instance, attackers have launched volumetric attacks on online exam platforms during critical assessment periods, targeted video conferencing tools during peak class hours with protocol-level attacks, and overloaded cloud storage hosting e-books and course materials, delaying assignments and study sessions. A botnet attack using compromised IoT devices can compromise a university's entire network, impacting both educational and administrative operations. Reports indicate that DDoS attacks against educational institutions have surged in recent years; for example, 66 UK universities experienced attacks in 2016, the University of Edinburgh faced a successful attack in 2019, and the education sector saw a 102% increase in DDoS incidents in 2021, with attacks occurring every three seconds [22][80].

### 3.6.7. Malware and ransomware infections

Smart education systems utilize digital technologies to enhance teaching and learning experiences; however, this digital integration also exposes institutions to significant cybersecurity threats, particularly malware and ransomware attacks. Malware, which includes viruses, worms, trojans, spyware, and adware, infiltrates devices like student laptops, teacher workstations, interactive whiteboards, and network servers, often spreading through email attachments, malicious downloads, or compromised websites. For example, trojans disguised as educational apps or spyware hidden in seemingly harmless software can grant attackers unauthorized access to sensitive information, such as student records and exam materials. Meanwhile, viruses and worms can infect entire school networks, disrupting teaching and administrative activities [22][23][31][81]. Ransomware, a highly disruptive form of malware, encrypts victims' data or locks systems and demands a ransom, typically in cryptocurrency, to restore access. Educational institutions, which heavily depend on digital resources yet often operate with limited cybersecurity budgets, have become attractive targets for ransomware attacks; notable cases include the University of Utah, Clark County School District in Nevada, Blacon High School in Cheshire, and Lebanon School District in New Hampshire, where attacks caused system shutdowns, class cancellations, and extensive recovery costs. As ransomware tactics become increasingly sophisticated, employing strong encryption and data exfiltration for extortion, traditional cybersecurity methods often fall short [12][23][24][32].

### 3.6.8. Eavesdropping and data interception

In smart education, where digital platforms, IoT devices, and cloud-based services play a central role in facilitating learning, eavesdropping and data interception pose serious security and privacy risks. Unauthorized parties can covertly capture sensitive information as it travels across communication channels, exposing students, teachers, and institutions to threats like identity theft and academic fraud. Attackers may deploy techniques such as network sniffing to capture unencrypted data packets on Wi-Fi or LAN networks, execute MitM attacks to intercept video streams and chat messages during online lectures, or exploit poorly secured wireless networks through wireless eavesdropping. They can intercept video conferencing sessions on platforms like Zoom or Microsoft Teams, capture login credentials and personal data from LMS, eavesdrop on IoT devices such as smartboards and connected cameras, and tamper with shared educational content. Such breaches compromise student confidentiality, facilitate intellectual property theft, erode academic integrity, and undermine trust in digital learning environments, underscoring the urgent need for robust security measures.

### 3.6.9. Insider threats

Insider threats in smart education pose unique and significant challenges, as they involve individuals within an organization, such as employees, faculty, or students, who misuse their authorized access to systems, data, or facilities, either intentionally or unintentionally, causing harm. Smart campuses are particularly vulnerable to these threats. Malicious insiders may steal sensitive data, alter academic records, disrupt learning platforms, or steal intellectual property. In contrast, negligent insiders can cause breaches through careless practices, such as weak password management or falling victim to phishing scams. Additionally, compromised insiders, whose credentials or devices attackers have hijacked, can unintentionally facilitate further security breaches. For instance, a disgruntled employee might sell student data, an administrator could manipulate

grades, or a staff member might tamper with IoT devices to violate privacy. Such actions jeopardize data, network, and physical security, damage the institution's reputation, and undermine trust in smart education systems [22].

### 3.6.10. Zero-day exploit

A zero-day exploit is a cyberattack that leverages a previously unknown vulnerability in software or hardware, one that developers and security experts have had no time to detect or fix [82]. As educational institutions rapidly adopt technology, the attack surface for cybercriminals expands, making zero-day exploits a serious threat. Attackers can bypass traditional defenses and remain undetected, potentially exposing sensitive student data, disrupting learning activities, or manipulating educational content (Waheed et al., 2024). For instance, undisclosed flaws in LMS, vulnerabilities in IoT devices such as smart whiteboards or biometric attendance systems, and weaknesses in AI-powered exam proctoring tools or cloud storage platforms can all serve as entry points. Real-world scenarios include attackers injecting malicious scripts into online learning platforms to alter exams and grades, hijacking IoT classroom devices to spoof attendance or cause disruptions, or exploiting AI proctoring software to disable monitoring and facilitate cheating. Such attacks risk compromising students' data privacy, disrupting operations, undermining trust in digital tools, and threatening academic integrity.

### 3.6.11. SQL injection and session hijacking

SQL injection (SQLi) is a code injection technique where attackers insert malicious SQL statements into input fields or API requests to exploit vulnerabilities in an application's database layer, thereby enabling unauthorized access or data manipulation. Smart education platforms, which store sensitive student information, grades, course materials, and user credentials, are particularly vulnerable when input fields, such as login forms, registration pages, or search bars, lack proper sanitization. Attackers can exploit these weaknesses to retrieve confidential data, alter grades or attendance records, delete educational content, or bypass authentication. Similarly, session hijacking occurs when attackers steal or predict valid session tokens, often through network sniffing or cross-site scripting, to impersonate users and access private accounts, manipulate content, or perform unauthorized actions. For instance, if an online learning platform stores session IDs in cookies without encryption or secure flags, attackers on the same network can intercept these cookies with tools like Wireshark and gain full account access. These threats pose serious risks to educational institutions, especially in remote learning environments where databases support online classes and administrative functions. SQLi attacks can disrupt learning, expose confidential information, and compromise data integrity, as demonstrated by the shutdown of Malaysia's School Examination Analysis System following an SQLi attack [26][83][84].

### 3.6.12. IoT-related vulnerabilities

The integration of the IoT in smart education environments, such as smart classrooms, connected devices, and remote learning systems, offers many benefits but also exposes significant security and privacy risks. Educators, policymakers, and developers must understand these vulnerabilities to address them effectively. Many IoT devices, including smart boards, student tablets, and connected projectors, often rely on weak or default credentials, allowing unauthorized users to manipulate content or access sensitive student data. For example, a smart classroom's control system can be breached if default admin passwords remain unchanged. These devices continuously collect personal information, such as student identities, learning progress, and biometric data, including facial recognition, which becomes vulnerable without strong encryption and access controls. Unsecured webcams and microphones in remote learning can be exploited to eavesdrop on or record students without their consent. Many devices run outdated firmware that attackers exploit to infiltrate networks, such as smart sensors with unpatched software, providing entry to school systems. IoT devices often share networks with critical systems, allowing attackers to move laterally—for instance, a compromised smart printer could grant access to sensitive student records. Physical access also poses risks, as devices installed in public areas can be tampered with or disabled by unauthorized individuals, such as students. Finally, the wide variety of IoT devices and vendors creates inconsistent security standards and interoperability issues, as new third-party systems may introduce vulnerabilities when integrated with older devices due to incompatible security protocols.

### 3.6.13. Insecure network communications

In smart education, network communications are critical for enabling seamless data exchange among students, teachers, administrative staff, and smart devices; however, insecure channels pose a threat to the confidentiality, integrity, and availability of educational data. When sensitive information travels over unencrypted or weakly encrypted networks or when strong authentication and authorization are not in place, risks escalate. For example, many campuses offer open or weakly protected Wi-Fi to support learning anywhere. Without protocols like WPA3, attackers can intercept login credentials, emails, or student records via MitM attacks. Similarly, vulnerable mobile apps or LMS that use outdated encryption, such as obsolete SSL/TLS versions or lack enforced HTTPS, expose data to eavesdropping and manipulation, potentially leading to academic fraud or data breaches. Smart classroom IoT devices, such as smartboards, cameras, and interactive tools, often transmit real-time data to cloud platforms. Suppose these communications rely on unsecured channels or default settings

without proper encryption and device authentication. In that case, attackers can exploit vulnerabilities to gain unauthorized access, inject malicious commands, or disrupt classroom operations.

### 3.6.14. Weak authentication

Weak authentication occurs when systems use easily compromised or insufficient methods to verify user identities, posing serious security and privacy risks in smart education environments that rely on digital platforms, IoT devices, and cloud resources. In these ecosystems, students, teachers, administrators, and sometimes parents access LMS, smart classrooms, online exam portals, and educational IoT devices, but weak authentication, such as simple or default passwords, single-factor authentication, shared accounts, and infrequent credential updates, allows unauthorized users to infiltrate these systems. For example, attackers can guess or obtain weak passwords to access exam portals prematurely, exploit default credentials on smartboards or attendance devices to manipulate or disable them, and use brute-force methods to gain unauthorized access to LMS accounts, potentially altering grades or stealing personal data. These vulnerabilities erode trust in smart education technologies, compromise student privacy, expose institutions to data breaches, and disrupt the learning process, ultimately hindering the effective adoption of innovative educational tools.

### 3.6.15. Third-party service risks

Educational institutions in smart education environments are increasingly relying on third-party service providers for critical functions, such as cloud storage, LMS, video conferencing, and AI-driven educational tools. These tools enhance teaching flexibility and quality but also introduce significant risks that institutions must manage. These risks include data privacy and security vulnerabilities, as vendors often handle sensitive student and staff information that may be exposed through breaches or unauthorized sharing, potentially violating laws such as the General Data Protection Regulation (GDPR) or the Family Educational Rights and Privacy Act (FERPA), as illustrated by incidents like "Zoombombing" disruptions in 2020. Institutions also face service reliability challenges, as their dependence on external providers limits control over uptime, which can lead to interruptions during crucial periods, such as exams, that harm academic performance and the institution's reputation. Compliance and legal risks arise when vendors operate under differing jurisdictions or fail to meet contractual obligations, potentially exposing institutions to regulatory violations, as seen with apps transferring data without safeguards. Vendor lock-in further complicates matters by making it costly and difficult to switch providers, especially when proprietary technologies obscure data processing practices and reduce transparency. Finally, ethical and pedagogical concerns arise from algorithm-driven tools that may introduce bias or misalign with educational values, such as AI plagiarism detectors that produce false positives, requiring careful human oversight to avoid unfair outcomes.

### 3.6.16. Software vulnerabilities

Smart education environments increasingly rely on diverse software platforms, including LMS, virtual classrooms, mobile apps, and cloud services, which enhance interactivity and accessibility but also introduce significant software vulnerabilities. Attackers exploit weak authentication mechanisms, such as simple passwords without strong policies or multi-factor authentication, to launch brute-force or credential-stuffing attacks. For example, in 2020, several universities suffered unauthorized access due to unchanged default passwords and misconfigured role-based access controls. Many educational applications also lack proper input validation, leaving them open to SQLi and cross-site scripting attacks that compromise databases and sensitive data, as seen when a popular online quiz platform leaked exam answers and student records. Furthermore, outdated third-party plugins and libraries expose systems to breaches, as exemplified by a virtual classroom tool that was exploited via an obsolete video conferencing library to eavesdrop on live classes. Storing credentials in plain text on mobile devices and using insecure data transmission methods put accounts at risk of misuse if someone loses or compromises the devices. Finally, poor session management, like indefinite login sessions without timeouts, enables attackers to hijack user sessions, as demonstrated by phishing attacks that stole session cookies to access instructors' grading dashboards.

### 3.6.17. Physical security risks

Physical security risks in smart campuses pose a threat to the safety of facilities, equipment, and personnel, potentially leading to property loss, personal injury, and disruptions to school operations. Theft poses a significant risk, as numerous devices and equipment, such as computers, projectors, and laboratory tools, are essential for teaching and learning. Inadequate security measures, including weak locks, insufficient surveillance, and poor theft prevention, make these assets vulnerable. Unauthorized access to sensitive areas, including computer rooms, laboratories, and administrative offices, also compromises security when access controls are lax or ineffective, risking the leakage of confidential information, damage to equipment, and a reduction in overall campus safety. Additionally, natural disasters, such as earthquakes, fires, and floods, and artificial emergencies, including false alarms and terrorist threats, can cause severe damage to facilities, harm individuals, and disrupt services. Without robust emergency plans, communication systems, and disaster prevention infrastructure, schools cannot effectively manage these crises, thereby increasing their physical security risks [22].

### 3.6.18. Unsecured bring your own devices (BYOD) policies

In smart education, BYOD policies enable students, teachers, and staff to use their personal laptops, tablets, and smartphones for learning and administrative tasks, promoting flexibility, collaboration, and easy access to educational materials [34]. However, BYOD significantly increases cybersecurity risks by expanding the attack surface and introducing inconsistent security measures across diverse devices [25]. Without robust guidelines for device configuration, authentication, network segmentation, and data encryption, personal devices often connect directly to institutional servers and IoT-based smart classroom systems without proper isolation or access controls. This lack of safeguards exposes sensitive educational data to breaches; for instance, an infected student tablet could spread malware throughout the network or allow unauthorized access to internal databases if secure VPNs or multi-factor authentication are not in place. Insecure BYOD environments also tend to lack mobile device management and endpoint security, thereby increasing the risk of data leaks from lost or stolen devices that contain cached credentials or downloaded course content. Furthermore, students often fail to update operating systems or install antivirus software, leaving devices vulnerable and complicating efforts to secure the network and protect confidential information.

## 4. DEEP LEARNING AND COMPUTER VISION

The increasing complexity of attacks against smart education systems frequently outpaces the capabilities of traditional security solutions. As cyber threats become more advanced, these conventional defenses cannot adequately protect the unique vulnerabilities of interconnected learning platforms. However, emerging technologies such as DL and CV algorithms offer powerful tools for detecting anomalies, monitoring user behavior, and identifying threats within vast datasets [51][61]. By protecting sensitive information and ensuring the confidentiality, integrity, and availability of critical data and platforms, these intelligent systems greatly enhance cybersecurity in smart education.

### 4.1. Deep Learning

Deep learning has transformed artificial intelligence by strengthening the security of smart education systems. Ali et al. [85], Ali et al. [86], and Ali et al. [87] define DL as a branch of machine learning that relies on artificial neural networks with many layers to automatically identify and extract intricate patterns and features from vast datasets. Deep learning networks analyze vast amounts of unstructured data, such as images, speech, and text, by recognizing patterns and making data-driven decisions. Inspired by the human brain, these networks use layers of interconnected nodes to process information through input, hidden, and output layers. Data enters through the input layer, passes through hidden layers where the system extracts complex features, and emerges as results at the output layer, as shown in Fig. 8.

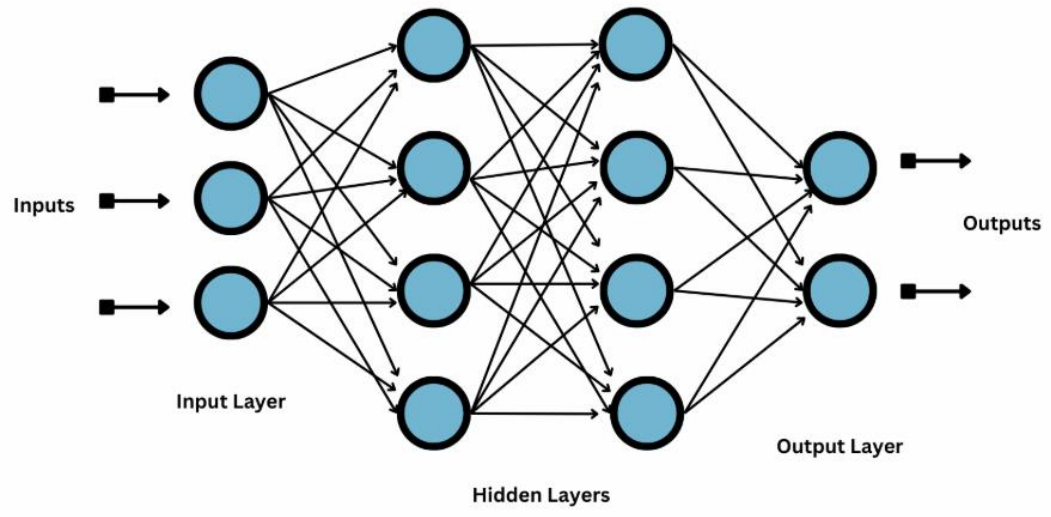


Fig. 8. Shows how a neural network works.

This layered structure enables DL models to identify intricate patterns in high-dimensional data and represent raw information in a more abstract and meaningful form [88][89]. DL systems enhance their performance as the volume and complexity of data grow, enabling them to model complex relationships, solve challenging problems, and operate without explicit programming. This capability has fueled their widespread use in data analysis, prediction, decision-making, and tasks like classification and automatic feature extraction, which help address challenges in detecting partial or inaccessible features [89]. Training these models on large datasets further improves their effectiveness in high-level tasks and supports supervised, semi-supervised, and unsupervised learning. Deep learning continues to show great promise in enhancing the

accuracy and efficiency of cybersecurity systems, excelling in applications such as image and speech recognition [88]. It holds tremendous promise for transforming educational practices by leveraging algorithms that mimic the human brain's neural networks to analyze complex data and uncover patterns for tailoring learning content. While industries such as healthcare, finance, and autonomous vehicles have already realized significant benefits from personalized solutions driven by DL, their full potential in education, particularly for large-scale personalized learning in higher education, remains untapped [90]. With its strength in processing vast amounts of unstructured data, DL excels at classification and automatic feature extraction, effectively addressing challenges related to partial detectability and feature accessibility [85]. The rapid evolution of GPUs has accelerated the training of large models, boosting both performance and accessibility. As these models process increasing amounts of data through multiple computational layers, they continuously refine their predictions, achieving higher accuracy and establishing DL as a powerful tool for solving complex, data-intensive problems across various domains [87].

Deep learning techniques can be categorized into four main areas: deep supervised learning, unsupervised learning, reinforcement learning, and hybrid learning, as illustrated in Fig. 9 below.

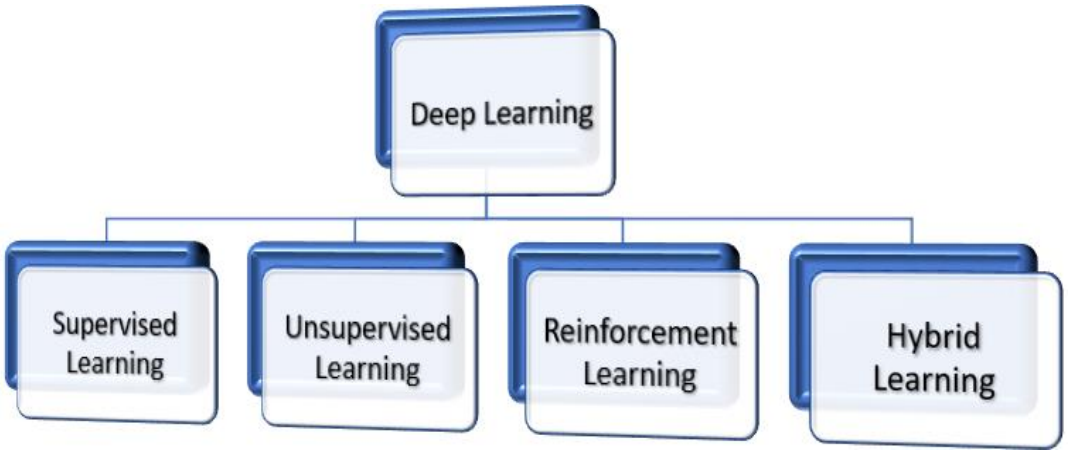


Fig. 9. Illustrates the different DL techniques.

- **Supervised learning**

Supervised learning trains neural networks using labeled datasets, where each input feature is paired with a known output. The models predict outcomes based on input data and then compare these predictions to the actual labels to adjust and improve accuracy. Deep learning algorithms, such as CNNs and RNNs, are used to perform supervised tasks, including image classification, object detection, language translation, and speech recognition. For example, CNNs can automatically detect unauthorized individuals in real-time campus surveillance, while spam detection models classify emails as 'spam' or 'not spam' by learning from previously labeled examples. These techniques effectively leverage known input-output relationships to identify specific threats or anomalies across various applications.

- **Unsupervised learning**

In unsupervised learning, neural networks discover patterns and structures within unlabelled datasets by analyzing them without predefined labels. Deep learning models, such as autoencoders and generative adversarial networks (GANs), excel at uncovering hidden relationships and generating realistic synthetic images. These algorithms perform tasks like clustering, anomaly detection, and dimensionality reduction. In education, unsupervised learning helps reveal patterns in student behavior and learning styles; for example, clustering algorithms can detect unusual access patterns in student login data, signaling potential account compromises. A typical application in smart education security involves using anomaly detection models to learn normal network behaviors and flag deviations that may indicate security threats [91][92].

- **Reinforcement learning**

In reinforcement learning, an agent learns to make sequential decisions by interacting with its environment and using feedback in the form of rewards or penalties to maximize cumulative rewards. By leveraging DL, the agent continuously refines its actions through a feedback loop, learning from both positive and negative outcomes until it identifies the optimal strategies. In smart education, this technique powers adaptive tutoring systems that adjust lesson difficulty and recommend resources based on student performance, effectively acting as a virtual tutor to maximize each learner's progress. Likewise, reinforcement learning enhances security systems by enabling intelligent access control that dynamically optimizes door lock schedules and alarm settings according to usage patterns and threat levels.

- **Hybrid learning**

Hybrid learning combines multiple techniques to leverage their strengths and improve performance across various domains [61]. For example, semi-supervised learning utilizes a small set of labeled data alongside abundant unlabeled data to enhance results where the availability of labeled scans is limited. Another hybrid approach combines supervised learning with reinforcement learning to train robots that utilize pre-trained visual models for enhanced navigation in dynamic environments. By integrating two or more DL architectures or combining DL with traditional machine learning methods, such as Support Vector Machines (SVM), hybrid models enhance accuracy, efficiency, and resilience. For instance, they can apply supervised methods to classify known security threats while using unsupervised techniques to identify novel anomalies, ensuring robust protection in smart educational environments. Such hybrid frameworks, like fusing CNN with RNN, excel in complex tasks, including medical diagnosis, cybersecurity, and natural language processing, where a single model often falls short in capturing diverse data patterns [93].

Deep learning encompasses various model types, including CNNs, Recursive Neural Networks (RvNNs), GANs, Federated Learning, Transfer Learning, RNNs, Long Short-Term Memory (LSTM) networks, Autoencoders and Variational Autoencoders (VAEs), Transformer models, Gated Recurrent Units (GRUs), deep Autoencoders (AEs), Graph Neural Networks, Multilayer Perceptrons (MLPs), Deep Belief Networks (DBNs), Self-Taught Learning (STL), Restricted Boltzmann Machines (RBMs), Reinforcement Learning (RL), and Deep Neural Networks (DNNs) [85][87][89][94]. Various DL methods are employed to tackle complex cybersecurity challenges, selected based on factors such as data volume, issue sensitivity, and decision tolerance [95-97].

Deep learning is revolutionizing smart education by enabling systems to analyze large volumes of student and institutional data, recognize patterns, and make intelligent, real-time decisions that enhance personalization, automation, and adaptive feedback [98][99]. Educators and institutions are increasingly relying on DL to create personalized learning paths, generate tailored educational content, power intelligent tutoring systems, automate grading, and provide detailed feedback —all of which save time and reduce bias [46]. Advanced neural networks support adaptive learning platforms that adjust content difficulty and recommend resources based on individual progress, while predictive analytics identify at-risk students early, allowing timely interventions [63][100]. Integrated with IoT and big data, DL improves smart classroom management by monitoring teaching quality and student engagement, recommending content aligned with students' interests and daily activities, and optimizing resource use [63][101-103]. Deep learning continues to transform education by freeing teachers from routine tasks and enabling data-driven, student-centered learning experiences with high accuracy in complex tasks such as image and audio recognition [46][63][104]. Deep learning-powered security frameworks enhance public safety by detecting suspicious activities, preventing unauthorized access, and thwarting security breaches [89]. These methods significantly improve anomaly detection, system security, fault diagnosis, and intrusion detection by analyzing real-time network traffic and identifying threats more effectively than traditional systems. Unlike conventional approaches that rely on static rules, DL focuses on behavioral patterns, enabling more robust malware and fraud detection by recognizing malicious actions and uncovering fraudulent transactions within massive datasets. Its capacity to model complex relationships enhances predictive maintenance and fraud prevention, although challenges such as large dataset requirements and high false-positive rates remain [87]. Overall, DL algorithms demonstrate considerable potential in improving the precision of cyberattack detection by autonomously extracting hierarchical features from raw data [86].

### 4.1.1. Roles of DL in Ensuring Cybersecurity for Smart Education

Recent advances in DL are transforming nearly every facet of computer science, with significant implications for cybersecurity, one of the most challenging areas for computers [105]. By adopting DL technologies, organizations can strengthen their abilities to detect and counter cyber threats, thereby safeguarding sensitive information and critical infrastructure [106]. This section highlights the pivotal roles that DL plays in advancing cybersecurity within smart education environments.

- **Intrusion detection and prevention system (IDPS)**

Intrusion detection and prevention systems (IDPS) proactively prevent security attacks by analyzing data patterns and identifying abnormal behaviors based on stored records [107-109]. CNNs and RNNs effectively detect malware through self-learning. Artificial neural networks monitor network traffic to detect imminent threats [106][110]. In smart education environments, IDPS monitors, detects, and blocks malicious activities to safeguard sensitive data, such as student records, from malware, unauthorized access, and DDoS attacks [111]. Deep learning significantly enhances intrusion detection accuracy and adaptability by automatically extracting complex features from diverse, high-dimensional educational IoT data, enabling real-time threat detection with reduced false alarms and improved response to emerging threats such as zero-day attacks. Advanced frameworks, such as self-supervised and online DL, enable continuous adaptation without manual labeling, making them ideal for dynamic educational networks [46][112]. Overall, DL techniques enhance cybersecurity in smart education by efficiently analyzing large-scale data, detecting a wide range of cyber threats, including malware,

phishing, intrusion attempts, and deepfake misinformation, and providing adaptive, scalable defenses that surpass traditional methods in both accuracy and reliability [35].

- **Malware detection and classification**

Malware remains one of the most persistent threats in cybersecurity, negatively impacting systems and data. It takes many forms, including viruses, trojans, worms, ransomware, adware, miners, and downloaders [113]. The rise of DL has transformed malware detection by enabling automatic feature extraction and outperforming traditional machine learning methods, particularly through models like Deep Neural Networks (DNN). Deep learning techniques analyze patterns in executable files, system logs, and network behaviors to identify and classify malware. Methods such as Autoencoders and LSTM networks effectively detect zero-day malware and polymorphic viruses [114]. By quickly detecting and categorizing threats like viruses, ransomware, and spyware using DL, signature-based scanning, and behavioral analysis, cybersecurity solutions protect smart education platforms from malicious software that could steal sensitive student information or disrupt online learning [115]. This proactive defense enables educational institutions to secure digital resources and safeguard the privacy of students and staff.

- **Behavioral analysis and insider threat mitigation**

Deep learning effectively models student and staff behavior over time by capturing sequential patterns, such as login times and resource access, using architectures like LSTM and Bidirectional LSTM to identify deviations that may signal compromised accounts. In smart education systems with IoT sensors or augmented reality/virtual reality components, it dynamically learns normal usage patterns and detects unauthorized interventions. By analyzing user activities, including access patterns, communication behaviors, and system interactions, DL algorithms establish baseline profiles that reveal potentially malicious actions or compromised credentials. Unlike rule-based systems, these models adapt to evolving threats by learning from new data instantly, enabling the detection of novel insider tactics, such as unauthorized data access, data exfiltration, or unusual privilege escalations. Deep learning also integrates diverse data sources, including network logs, emails, and biometric data, to enhance detection accuracy and reduce false positives. RNNs and CNNs capture temporal and contextual nuances, thereby improving predictive capabilities. Overall, DL empowers organizations to proactively identify and mitigate insider threats with dynamic, scalable, and precise behavioral insights before significant damage occurs [43].

- **Spam and botnet detection**

Malicious actors rapidly spread spam and botnet attacks by commandeering devices connected to the Internet, often forming botnets through infected victim devices controlled via email spam to launch large-scale attacks, such as DDoS attacks [116-118]. Deep learning techniques, including autoencoders, CNNs, Graph Neural Networks (GNNs), LSTMs, and Deep Belief Networks (DBNs), enhance defense by analyzing social network graphs, detecting abnormal behaviors, and extracting deep features from network traffic [116][117][119]. These models, including LSTMs, CNNs, transformers, and GNNs, automatically identify spam messages and suspicious activities associated with botnets by analyzing text, user behavior, and network patterns [120]. By training on real user data and behavior, DL systems effectively flag suspicious content and accounts, thereby improving the safety and reliability of online education environments.

- **Fraud detection**

Deep learning models excel at detecting complex patterns and anomalies in large datasets, resulting in more accurate fraud identification than rule-based or shallow learning methods [121][122]. For instance, RNNs specialize in modeling sequential data, such as transaction histories, by capturing patterns, trends, and dependencies, which enables them to detect unusual behaviors indicative of fraud [123]. In smart education platforms, fraud detection plays a critical role in preventing cheating, fake registrations, unauthorized access, and financial fraud. Deep learning algorithms, such as CNNs, RNNs, LSTMs, and autoencoders, analyze user behavior and transactions to identify subtle anomalies in data. By continuously learning from real-time data, these models strengthen security, protect student information, and promote fairness in smart education [124].

- **Threat intelligence and prediction**

In recent years, network system attacks have posed severe security challenges, prompting researchers to adopt DL models for more effective threat detection [125]. Cybersecurity threat intelligence is crucial in proactively defending against constantly evolving attacks [126]. RNNs excel at analyzing time-series data and can detect persistent threats by monitoring event sequences over time. Autoencoders effectively identify anomalies by learning normal network behavior and flagging deviations that signal potential cyber threats. By analyzing user behavior, network traffic, and system logs, DL enhances threat intelligence and prediction in innovative education platforms. RNNs, GNNs, and transformers recognize patterns associated with malware, phishing, and other attacks, continuously adapting to new methods to ensure a safer and more secure learning environment.

- **Adaptive and federated security in distributed learning environments**

Smart education environments increasingly rely on distributed systems, including classroom IoT devices, remote labs, and mobile apps, where edge computing and federated DL enable on-device model training that preserves privacy while sharing learned patterns crucial for scalable cybersecurity. By applying transfer learning, lightweight CNNs can be deployed effectively on resource-limited devices, ensuring robust yet practical security for smart educational platforms. In these decentralized learning settings, DL enhances security and privacy by powering adaptive and federated mechanisms. Adaptive security models dynamically detect and respond to evolving threats, such as adversarial attacks, data poisoning, and unauthorized access, by analyzing complex patterns in network traffic, user behavior, and model updates, enabling real-time resilience without relying on fixed rules. Federated learning collaborates across devices to train models without sharing raw data, and DL enhances this approach by supporting encrypted model aggregation and detecting anomalies in local updates, thereby validating their integrity and filtering out malicious contributions. Together, these DL-driven, adaptive, and federated security techniques deliver scalable, intelligent, and privacy-preserving defenses that are essential for maintaining trust and robustness in distributed learning environments [43][44].

- **Defense against adversarial attacks**

DL systems remain vulnerable to adversarial attacks, where attackers manipulate input data to deceive models, posing significant risks in sensitive areas such as autonomous vehicles, healthcare, and defense. To strengthen defenses, researchers employ adversarial training by augmenting datasets with adversarial examples, enabling models to learn robust features and resist attacks more effectively. Additionally, DL models detect and filter suspicious inputs by recognizing anomalies, while novel architectures preprocess data to remove adversarial noise. Techniques such as gradient masking and regularization further reduce the effectiveness of attacks by obscuring gradient information and enhancing model stability. Integrating Explainable AI (XAI) helps educators and administrators interpret alerts and make informed security decisions. In smart education, these DL defenses protect sensitive student data, secure IoT devices, and ensure the integrity of online assessments and communications [36-38][40-42][46][51][52]. Moreover, incorporating DL into cybersecurity curricula equips future professionals to counter sophisticated AI-driven threats, such as deepfakes [37]. Overall, DL significantly enhances cybersecurity in education by providing intelligent, adaptive defenses; however, ongoing research remains essential to address the evolving tactics of adversaries [35].

- **Secure and adaptive cybersecurity education tools**

Deep learning, a neural network–based subset of machine learning, is transforming cybersecurity education by powering intelligent, adaptive, and secure learning tools. These tools personalize content in real-time by analyzing learners' data, such as interaction patterns and quiz results, to adjust the difficulty, suggest targeted resources, and tailor scenarios to individual needs. They simulate realistic cyberattack scenarios using generative models, giving students hands-on experience with sophisticated threats. Deep learning also automates complex assessments, such as code analysis and threat detection, delivering precise and timely feedback that reduces instructor workload. Additionally, it monitors learner behavior to detect anomalies such as disengagement or cheating, safeguarding the integrity of the learning environment. Furthermore, by embedding DL–based security measures, such as evolving intrusion detection systems, educational platforms can protect sensitive data and intellectual property. Altogether, DL drives the development of more innovative, more responsive cybersecurity education, equipping professionals to defend effectively against advanced cyber threats [53].

## 4.2. Computer Vision

Computer vision is transforming the way computers interpret digital images and videos, playing a vital role in smart education environments. Computer vision is a branch of AI and computer science that focuses on designing algorithms and models that enable machines to detect, classify, and analyze visual information, such as images and videos, in ways that mimic human vision and perception [89][127-130]. By integrating image processing, video analytics, and advanced AI techniques, CV allows machines to automatically interpret their surroundings and extract meaningful insights from visual data, thereby replicating key aspects of human visual understanding.

With the surge in data availability and computational power, CV has become increasingly vital for accurate object recognition and generating actionable insights in fields such as education. A CV system interprets visual data through interconnected stages: capturing images or videos, preprocessing to enhance data quality, extracting key features such as edges and corners, recognizing objects by comparing these features to known databases, tracking detected objects over time, and analyzing the results to produce meaningful outputs. Techniques such as classification, object detection, image segmentation, and facial recognition automate tasks like monitoring and tracking, which support student safety during transportation. Powered by AI and CNNs, CV systems efficiently detect, classify, and track objects by learning from vast datasets and leveraging advanced GPUs [89][127]. These capabilities enable real-time processing in complex environments, supporting applications in autonomous vehicles, medical imaging, surveillance, industrial automation, and education. While facial recognition offers benefits like enhanced student monitoring and safety, it also raises concerns about data privacy and potential misuse due to data leaks. By integrating object detection and facial recognition, modern systems improve situational

awareness, support law enforcement, and enhance security measures, ensuring timely responses to emergencies and effective traffic management.

Computer vision employs a range of techniques that enable machines to analyze and interpret visual information from the real world. These algorithms address a variety of tasks, including image classification, object detection, and image segmentation. Additionally, they support feature detection and description, image alignment and registration, as well as optical flow and motion estimation [89]. The widely used CV algorithms include:

- **Scale-Invariant Feature Transform (SIFT) algorithm**

The SIFT algorithm, developed by David Lowe in 2004 at the University of British Columbia, is a robust CV method for detecting and describing local features in digital images. By identifying key points and generating distinctive descriptors, SIFT effectively supports object detection and recognition while remaining invariant to changes in scale, rotation, illumination, and viewpoint shifts [131]. The algorithm operates through four main steps: detecting scale-space extrema using the Difference of Gaussian (DoG); refining key points for stability; assigning orientations based on local gradient directions to achieve rotation invariance; and generating key point descriptors that create resilient feature vectors [132][133]. In smart education, SIFT enhances CV applications, boosting interactivity, monitoring, and security. It ensures accurate student identity verification and automated attendance by reliably matching facial features under varying conditions. During online examinations, SIFT detects cheating and anomalies by comparing frames to spot unauthorized objects or suspicious movements. It also enables gesture recognition and interaction tracking in AR-based learning, facilitating smooth recognition of educational materials and physical actions. Furthermore, SIFT strengthens smart classroom surveillance by analyzing student behavior and identifying unusual activities, thus improving safety and engagement [134][135].

- **Speeded Up Robust Features (SURF)**

SURF is a patented CV algorithm renowned for its speed and accuracy in feature detection and description, making it a popular choice for tasks such as object recognition, classification, image matching, and 3D reconstruction [136]. It works in two main stages: first, it extracts features by selecting interest points using a Hessian matrix approximation; then, it generates descriptors by analyzing wavelet responses within oriented square regions around each key point [137][138]. By using box filters to approximate the DoG and leveraging integral images, SURF achieves high computational efficiency. Its robustness to image transformations and fast processing make it widely adopted in applications like object and face recognition, real-time tracking, image stitching, and 3D modeling [139].

- **Viola-Jones object detection algorithm**

Developed by Paul Viola and Michael Jones in 2001, the Viola-Jones object detection algorithm pioneered real-time face detection and can be trained to detect various objects in images. While its training phase is relatively slow, it achieves fast and accurate detection during execution [140]. The algorithm scans multiple sub-regions of an image at various scales and positions, utilizing Haar-like features to capture key facial structures. It operates through four main steps: selecting Haar-like features, such as edge, line, and four-sided features, creating an integral image for efficient computation, applying AdaBoost to choose the most relevant features and boost accuracy, and constructing classifier cascades to discard non-face regions and accelerate detection quickly [141][142]. This method remains widely used in real-time applications, including face and object tracking and video-based attendance systems, and it laid the foundation for modern face detection technologies [143].

- **Eigenfaces Approach using Principal Component Analysis (PCA) algorithm**

The Eigenfaces approach, a foundational face recognition technique based on linear algebra and dimensionality reduction through principal component analysis (PCA), identifies faces by projecting high-dimensional images onto principal axes derived from the most significant eigenvectors of the image covariance matrix. First introduced by Sirovich and Kirby in 1987 and formalized by Turk and Pentland in 1991, this method efficiently captures the most significant features of facial data while reducing dimensionality without losing critical information [144]. Beyond face recognition, researchers have applied Eigenfaces to handwriting recognition, lip-reading, medical image analysis, and other fields [145]. Although easy to implement and computationally efficient, the technique relies on well-centered training images and remains sensitive to variations in lighting and scale.

Computer vision encompasses a wide range of techniques and applications, including 3D vision and reconstruction through structure-from-motion and stereo vision, as well as face identification and recognition using algorithms such as Viola-Jones, Fisherfaces, and FaceNet. It also enables image synthesis with GANs and variational autoencoders, pose estimation through tools like OpenPose and MediaPipe, and super-resolution using methods like Bicubic Interpolation and Super-Resolution CNNs. Researchers apply Autoencoders and One-Class SVM for anomaly detection, employ tracking algorithms such as the Kalman Filter, Mean-Shift, and CamShift, and develop augmented reality experiences using Simultaneous Localization and Mapping or Marker-based AR. Additionally, they enhance and denoise images using techniques such as Non-Local Means, Total Variation Denoising, and Gaussian and Bilateral Filters [89].

By leveraging data from cameras and CCTV, CV enhances surveillance, supports informed decision-making, and facilitates effective forest management and conservation efforts [89]. In smart education, CV plays a crucial role by enabling the real-time analysis of visual data to enhance teaching, learning, and classroom management. These systems monitor student posture and engagement, providing teachers with immediate feedback to adjust instruction and boost learning outcomes [131][146][147]. They also track teachers' gestures, making lessons more interactive and dynamic and enhancing educational content design through advanced visual processing and 3D coordinate transformations. Computer vision frameworks enable intelligent education assistance systems that provide interactive visualizations, simplify complex information, and facilitate personalized learning [148]. In immersive virtual reality settings, these technologies analyze students' cognitive engagement, enabling the provision of tailored guidance and support [131]. For young learners, vision-based systems recognize objects and track interactions, creating individualized and engaging early education experiences [147]. When integrated with the IoT, CV further enables smart learning environments that monitor attention and streamline classroom management. Overall, these technologies enhance education by making it more interactive, adaptive, and data-driven, with proven benefits for student engagement, instructional quality, and educational research [131][146-148].

### 4.2.1. Roles of CV in Enhancing the Security of Smart Education

Computer vision significantly strengthens cybersecurity by integrating intelligent surveillance, biometric authentication, automated anomaly detection, advanced video analytics, facial recognition, flaw detection, and object detection into physical security systems. These technologies work together to identify suspicious activities and potential threats more accurately and efficiently. Some of the roles of CV in enhancing the security of smart education include the following.

- **Enhancing physical access and monitoring**

Computer vision integrates physical and cybersecurity in educational facilities by utilizing biometric facial and iris recognition to prevent unauthorized access to labs, data centers, exam halls, and offices. Additionally, tailgating detection alerts authorities when multiple individuals attempt entry with a single credential. Beyond access control, CV enhances physical access and monitoring across various domains, including healthcare, security, transportation, and smart infrastructure. It supports inclusive navigation for the visually impaired through obstacle detection and real-time guidance, enables touchless gesture-based interfaces in hygiene-sensitive areas, and automates identity verification for secure entry. Additionally, it enhances monitoring and surveillance by identifying real-time activities, detecting environmental hazards such as fires or spills, and managing crowd flow and traffic to prevent congestion and accidents. By precisely processing visual data and interpreting context, CV bridges digital intelligence with physical environments, creating safer, more accessible, and responsive spaces [36][44][54][55].

- **Secure smart classrooms and student surveillance**

Computer vision, through advanced systems like YOLOv5, plays a crucial role in enhancing security, monitoring, and learning outcomes in smart classrooms by detecting unusual behaviors, such as unattended devices or unauthorized access, to prevent insider threats and equipment tampering. It controls access and verifies identities using facial recognition, ensuring only authorized individuals enter school facilities. Automated tracking records attendance in real-time, reducing administrative work and maintaining consistent oversight. By analyzing facial expressions, body language, and posture, it assesses student engagement and emotional states, enabling teachers to adjust their methods dynamically. Surveillance cameras equipped with CV detect intrusions or suspicious activities, generating real-time alerts to address potential threats. These systems also monitor student participation and interaction, track gaze and gestures to evaluate teaching effectiveness and detect cheating during exams by spotting unauthorized behaviors or devices. Additionally, CV enforces health protocols, including mask usage, social distancing, and temperature checks, while logging visual data for retrospective analysis, dispute resolution, or as evidence in incidents such as bullying or vandalism. Overall, video-based analysis strengthens both learning analytics and cybersecurity by providing actionable insights and ensuring academic integrity in proctored settings.

- **Detecting forgery, deepfakes, and phishing**

Detecting forgery, deepfakes, and phishing requires analyzing digital content to uncover signs of manipulation or deception. Advanced techniques examine images, videos, and messages for inconsistencies, altered elements, and fraudulent patterns, enabling swift identification and prevention of these threats. Computer vision combats forgery, deepfakes, and phishing by analyzing subtle visual and behavioral cues that reveal manipulation or deception. In forgery detection, it uncovers tampering by spotting inconsistencies in lighting, shadows, textures, duplicated image regions, and splicing artifacts that humans often miss. For deepfake detection, CV exposes AI-generated content by identifying facial anomalies, such as unnatural eye blinking and lip-syncing, detecting irregular motion across frames, analyzing physiological signals like micro-expressions, and training classifiers on real versus synthetic data. In phishing detection, it automatically compares website screenshots to legitimate designs, extracts and examines text through optical character recognition (OCR) to spot spoofed branding, applies visual similarity models to detect counterfeit login pages, and verifies logos to flag unauthorized usage. Together, these advanced image and video analysis techniques empower CV systems to identify malicious manipulations efficiently and accurately [58][59].

- **Analysis of integrated cyber-physical threat**

Computer vision enhances integrated cyber-physical threat analysis by enabling real-time interpretation of visual data from physical environments, thereby bridging cyber and physical security domains. It strengthens unified threat intelligence and insider risk detection through continuous monitoring, detecting anomalies such as unauthorized physical access or suspicious behavior before data leaks occur. Specifically, CV systems detect physical intrusions by recognizing human presence, tampering, and restricted objects; identify anomalies signaling cyber-attack precursors or consequences; and fuse visual data with network logs, sensor readings, and user behavior analytics for a comprehensive threat perspective. Additionally, these systems automate monitoring tasks, provide visual evidence for investigations, support forensic event reconstruction, and contribute to predictive threat models by learning from past incidents. Together, these capabilities enhance situational awareness, expedite incident response, and substantially improve the security of modern cyber-physical systems [44][54][59].

- **Intrusion and anomaly detection**

In smart education environments that rely on interconnected devices, IoT infrastructure, and continuous access to digital resources, robust security remains crucial. Intrusion and anomaly detection play a vital role in protecting these systems from internal misuse and external cyber threats. By integrating CV technologies with advanced DL algorithms, institutions can automatically monitor and analyze visual data streams, such as CCTV footage, classroom cameras, and biometric access points, to detect suspicious activities in real-time. Using techniques like object detection, facial recognition, and behavioral pattern analysis, CV systems can identify unauthorized access, detect abnormal behaviors, and flag unusual activities that deviate from expected patterns. For example, these systems can secure physical entry points to prevent unauthorized individuals from accessing sensitive areas and monitor virtual learning spaces to detect anomalies, such as credential sharing or identity spoofing. By combining CV with DL methods, such as CNNs for feature extraction and RNNs for modeling sequential behavior, the accuracy in distinguishing harmless irregularities from genuine threats is improved, thereby reducing false positives and enhancing automated alerts. Additionally, CV offers visual intelligence capabilities that analyze data from surveillance cameras, satellites, and digital devices to identify threats [149][150].

- **Detection of suspicious objects**

In smart education environments, advanced technologies such as IoT devices, smart classrooms, and surveillance systems drive the need for robust security measures. Among the various risks, unauthorized or potentially dangerous objects within school premises pose a serious threat to the safety of students and staff. Computer vision automates the detection and assessment of such suspicious items, significantly strengthening campus security. Using high-resolution cameras and DL algorithms, CV systems continuously monitor classrooms, hallways, entrances, and other sensitive areas. They rely on object detection models, such as CNNs, and advanced architectures like Faster R-CNN, YOLO, and Single Shot MultiBox Detector to identify unattended bags, concealed weapons, or unusual objects in real-time with high accuracy. When these systems detect a threat, they instantly trigger alerts, lock access points, and notify security personnel to enable swift intervention, minimizing harm and reducing reliance on error-prone manual monitoring. Integrating CV-based object detection with access control and emergency response systems creates a multi-layered security framework that enhances situational awareness and supports proactive threat mitigation. For example, if the system spots an unattended package near an entrance, it can cross-check entry logs to trace its source while restricting access until the area is secure. This capability to detect and respond to suspicious objects in real-time ensures a safer educational environment [151][152].

- **Real-time indoor mapping**

Real-time indoor mapping utilizes advanced CV algorithms to generate accurate, continuously updated representations of indoor spaces, including classrooms, laboratories, libraries, and dormitories. Unlike static blueprints, these dynamic maps capture changing spatial layouts and detect structural or occupancy modifications in real-time by leveraging depth cameras, LiDAR sensors, and simultaneous localization and mapping (SLAM) techniques. In smart education, this technology enhances security and situational awareness by enabling precise tracking of individuals' movements without relying solely on manual surveillance. Computer vision systems can automatically detect unusual behaviors, like unauthorized access or unexpected gatherings, and trigger instant alerts to security teams. Integrated with facial recognition and access control, real-time mapping ensures seamless identity verification and reduces risks of impersonation or unauthorized entry. During emergencies such as fires or intrusions, dynamic maps provide first responders and administrators with up-to-date information on evacuation routes, occupancy, and obstacles, supporting rapid and informed decision-making. By embedding real-time indoor mapping into smart education infrastructures, institutions foster a proactive and adaptive security framework that not only deters threats but also promotes a safer, more resilient learning environment aligned with intelligent campus management goals. Additionally, by generating digital maps and tracking real-time movement through security cameras, CV helps optimize space usage and improve emergency response effectiveness [153].

Computer vision significantly enhances cybersecurity in smart education by enabling advanced real-time monitoring, threat detection, and anomaly recognition within educational settings. By employing techniques such as person detection, weapon identification, and behavioral anomaly detection—often integrated with digital twin models of school buildings—these systems monitor and respond rapidly to security incidents, improving the safety of students and staff [57]. In network security, CV methods, particularly CNNs, transform network data into visual formats to detect phishing, malware, and traffic anomalies more effectively, delivering high accuracy and scalability that are well-suited for the dynamic nature of smart educational environments [60]. Overall, CV technologies provide intelligent, automated, and context-aware security solutions that enhance cybersecurity in smart education. Ongoing research aims to overcome current limitations and optimize their implementation [57][60].

## 4.3. Synergistic Integration of DL and CV for Enhancing Cybersecurity in Smart Education

Integrating DL and CV technologies offers a transformative approach to enhancing cybersecurity in smart education environments. These systems, which rely on interconnected digital devices, IoT infrastructure, and cloud-based resources, face significant cybersecurity challenges due to the large volume of sensitive data and the constant need for real-time interactions. By combining DL's robust pattern recognition with CV's ability to interpret and analyze visual data, institutions can deploy a comprehensive, proactive defense mechanism. The key applications of this integration in smart education cybersecurity include:

### 4.3.1. Real-time intrusion detection through video surveillance

In modern smart education environments, protecting students, staff, and infrastructure is vital, and real-time intrusion detection through video surveillance plays a key role in comprehensive cybersecurity. This advanced system integrates DL and CV to deliver precise, efficient, and automated monitoring across campuses. High-resolution cameras, strategically installed, continuously stream live video feeds to DL models—primarily CNNs, that detect, classify, and analyze human activity. Using architectures such as YOLO or Faster R-CNN, the system quickly identifies multiple individuals in each frame, distinguishing authorized personnel from intruders based on visual cues and access data. It goes beyond detection by employing behavioral anomaly detection with RNNs or transformer-based models to examine motion patterns over time, flagging suspicious behaviors like loitering, trespassing, or unauthorized entry. This adaptive system continually improves its detection accuracy and reduces false alarms by learning from new data. Coupled with IoT-enabled access controls and alarms, it can automatically alert security staff, lock doors, or trigger deterrents, ensuring swift mitigation of threats. By focusing on behavior and object detection rather than identity, the system upholds privacy while enhancing safety and enabling proactive, responsive protection for smart education facilities [154-159].

### 4.3.2. Facial recognition for secure access control

In smart educational environments, secure and efficient access control is vital to safeguard sensitive data, protect physical resources, and ensure the safety of students and staff. By combining DL and CV, facial recognition technology provides an advanced, non-intrusive solution for real-time, automated identity verification. DL-based facial recognition systems authenticate students, staff, and visitors at entry points by matching live camera feeds with stored biometric data with high accuracy. This approach minimizes identity fraud and guarantees that only authorized individuals can access restricted areas, such as laboratories and data centers [160-163].

### 4.3.3. Behavioral anomaly detection in classrooms and halls

Behavioral anomaly detection utilizes DL and CV to continuously monitor and analyze individuals' behaviors in educational settings, such as classrooms and hallways. In smart education cybersecurity, this proactive approach enhances the safety of students and staff by detecting harmful or suspicious activities early. By combining CV with RNNs or transformer-based models, the system learns normal patterns of behavior. It quickly flags deviations such as loitering, aggressive gestures, or unusual group formations, which enables timely intervention to prevent bullying, violence, or other security threats [164-166].

### 4.3.4. Weapon and object detection for threat prevention

In smart education environments, safeguarding students and staff requires effective weapon and object detection systems that leverage DL and CV technologies to identify and neutralize threats in real time. Advanced DL models, primarily CNNs, trained on extensive datasets of weapons and suspicious objects, extract complex spatial and semantic features from visual data to accurately distinguish threats from harmless items. These systems analyze continuous video feeds from strategically placed cameras, utilizing techniques such as region proposal networks and multi-scale feature pyramids to locate and classify objects in each frame. Popular architectures such as YOLO, Single Shot MultiBox Detector, and Faster R-CNN strike a crucial balance between accuracy and real-time performance, ensuring timely detection. To minimize false positives and enhance reliability, the system incorporates contextual awareness by assessing object size, shape, and behavior and utilizes temporal tracking to detect concealed weapons across multiple frames. Upon identifying a threat, it instantly sends automated alerts to security personnel and connected cybersecurity systems, facilitating swift investigation and response. Integration

with digital twin models of school facilities further streamlines threat localization and coordinated action. Additionally, continual learning mechanisms enable the system to adapt to new threats and varied environments by updating detection models with fresh data, sustaining high accuracy over time [167-169].

#### 4.3.5.Automated attendance and identity verification

Automated attendance and identity verification systems enhance the security and efficiency of educational environments by integrating advanced DL and CV technologies. These systems use state-of-the-art architectures, including CNNs and transformer-based models, to analyze video feeds or images captured at entry points and within classrooms. They first detect and isolate human faces with high precision, employing robust algorithms such as Multi-task Cascaded Convolutional Networks (MTCNN) or YOLO to ensure real-time, reliable face localization, even under challenging conditions like poor lighting, occlusion, or varied poses. Next, they perform facial recognition by converting detected faces into compact, high-dimensional feature vectors using deep feature extraction networks, such as FaceNet or ArcFace, and compare these vectors against a secure, pre-enrolled database to verify identities instantly. To prevent spoofing, integrated liveness detection models distinguish between live faces and fake inputs, such as photos, videos, or masks. Once verified, the system automatically records attendance with precise timestamps and locations, thereby minimizing manual errors and providing audit trails to meet security and administrative needs. Seamless integration with school information systems enables real-time alerts for unauthorized access attempts, supporting proactive threat mitigation. These systems also uphold data privacy and regulatory compliance through encryption, secure storage, and strict access controls. By replacing manual roll calls with facial recognition or gait analysis, CV-based attendance systems maintain data integrity, prevent proxy attendance, and ensure high accuracy under diverse conditions, ultimately strengthening both academic management and campus cybersecurity [170-174].

#### 4.3.6.Cyber-physical threat detection through digital twin models

In smart education environments, robust cybersecurity relies on protecting both cyber and physical assets from increasingly sophisticated threats through the synergistic integration of DL, CV, and digital twin models. Digital twins serve as high-fidelity virtual replicas of physical and educational infrastructure, including buildings, network devices, IoT sensors, and connected endpoints, continuously mirroring real-time data streams to simulate and dynamically monitor operational states. By replicating physical spaces and digital interactions, they create a comprehensive framework for identifying threats that span both domains. Deep learning algorithms, including CNNs and RNNs, analyze complex data from sensors, network traffic, and video feeds to detect subtle anomalies, such as suspicious access attempts or unusual device behavior. Simultaneously, CV systems enable real-time visual surveillance through advanced object detection, facial recognition, and behavioral analysis, allowing for the identification of unauthorized individuals and suspicious activities. By feeding these visual insights into the digital twin, the system enhances situational awareness and correlates data across multiple sources. For example, if anomaly detection flags an unusual network login, CV can verify it by confirming the presence of an unauthorized person in the physical location, allowing the digital twin to orchestrate early warnings and rapid responses in real-time [175-177].

#### 4.3.7.Network security enhancement with visual data analysis

In smart education environments, securing network infrastructure against sophisticated cyber threats is crucial due to the growing number of connected devices and sensitive data. By integrating DL and CV techniques, institutions can enhance security through real-time monitoring, anomaly detection, and proactive threat mitigation using visual data from cameras and IoT sensors distributed across their facilities. CNNs process this visual input to identify unusual behaviors or unauthorized access, such as detecting unauthorized personnel in restricted areas or suspicious tampering with network devices. Combining these visual insights with network traffic analysis through multimodal data fusion enables comprehensive situational awareness, allowing DL models to identify anomalies such as unusual data flows, unauthorized connections, or potential DDoS attacks. This fusion of physical and digital threat detection enables faster and more precise responses. Additionally, analyzing temporal visual data sequences helps predict emerging threats by tracking subtle changes over time, thereby preventing advanced persistent threats and insider attacks in educational institutions [178][179].

#### 4.3.8.Emotion recognition for mental health and security monitoring

Emotion recognition, driven by the combined power of DL and CV, supports mental health and enhances security monitoring in smart education environments. Advanced algorithms analyze facial expressions, micro-expressions, voice intonations, and physiological signals captured by cameras and sensors embedded in schools. Deep learning models, especially CNNs and RNNs, train on large, annotated datasets to detect subtle emotional cues such as stress, anxiety, frustration, or distress from real-time video streams. Computer vision techniques, such as facial landmark detection, action unit recognition, and spatiotemporal analysis, precisely identify nuanced emotions across diverse student populations, taking into account factors like age, ethnicity, and environmental influences. By integrating visual data with audio and physiological inputs, these systems achieve greater accuracy and robustness. Continuous emotion recognition allows educators and counselors to detect early signs of emotional distress or mental health issues, providing actionable insights for timely intervention and

personalized support that promote student well-being and reduce stigma through unobtrusive monitoring. Anonymized aggregated data help shape institutional policies that foster healthier educational ecosystems. Beyond mental health, emotion recognition enhances cybersecurity and physical safety by detecting emotional signals associated with aggression, fear, or suspicious behavior, alerting security personnel to potential threats such as bullying, violence, or unauthorized access. When combined with other CV security tools, such as person detection, weapon identification, and behavioral anomaly detection, it creates a multi-layered defense that enables rapid response and ensures a safer learning environment [180-182].

#### 4.3.9.Crowd density estimation and emergency evacuation management

Deep learning and CV enhance intelligent cybersecurity in smart educational environments by enabling real-time crowd density estimation and emergency evacuation management. Utilizing advanced CNNs and transformer-based architectures, these systems analyze surveillance video feeds to accurately detect, track, and count individuals, even in crowded spaces such as hallways and auditoriums. By continuously analyzing spatial-temporal movement patterns, they identify abnormal gatherings, predict crowd flows, and pinpoint bottlenecks, allowing schools to optimize occupancy and traffic flow. In emergencies such as fires or threats, AI-powered models dynamically assess exit accessibility and congestion, guiding occupants through digital signage or mobile alerts. When integrated with digital twin simulations of school infrastructure, these systems test various threat scenarios to develop and refine evacuation plans. This combination not only boosts situational awareness for security teams but also enables autonomous, rapid, and coordinated evacuations, thereby strengthening the resilience of smart educational institutions against physical and cybersecurity risks [183-186].

#### 4.3.10. Enhanced data privacy through on-device AI processing

In smart education, protecting sensitive personal, behavioral, and biometric data is essential, especially given the advanced surveillance and monitoring technologies in use. By integrating DL and CV with on-device AI processing—where algorithms run directly on local edge devices, such as smart cameras and sensors, instead of sending raw data to centralized servers—educational institutions can enhance cybersecurity while safeguarding privacy. This approach minimizes data exposure by transmitting only critical metadata, ensures compliance with regulations such as GDPR and FERPA by limiting the storage and transmission of personally identifiable information, and preserves privacy in real time through the automatic redaction or anonymization of sensitive details before the data leaves the device. Additionally, on-device processing reduces latency, speeds up threat detection, and strengthens security by eliminating vulnerabilities during data transfer. Modern edge devices equipped with AI accelerators efficiently run CNNs for detecting persons, weapons, or abnormal behaviors, enabling continuous, privacy-conscious monitoring and proactive threat mitigation. Ultimately, deploying on-device AI processing in smart education strikes a balance between technological innovation and ethical data protection, thereby building trust and meeting regulatory demands without compromising the confidentiality of students and staff [187-189].

### 4.4. Real-World Scenarios and Practical Implementations of DL and CV in Enhancing Cybersecurity in Smart Education

This section showcases practical examples and real-world applications where DL and CV protect smart educational environments by securing the confidentiality, integrity, and availability of essential educational data and systems.

#### 4.4.1.Real-time surveillance for campus security

Ali et al. [88] present an advanced AI-powered surveillance system specifically designed for smart campuses. Their solution integrates CV-enabled smart CCTV cameras equipped with object detection models, such as YOLOv5, to detect unauthorized intrusions and suspicious behaviors, thereby preventing physical security breaches. By combining DL and sensor fusion, the system automates surveillance tasks, identifies threats, and issues real-time alerts, all while addressing privacy concerns and ensuring interoperability within the campus infrastructure.

#### 4.4.2.Biometric-based authentication

Zhang et al. [190] present a biometric authentication system that secures access within a smart campus by leveraging DL to enhance accuracy, robustness, and user convenience. Their system employs physiological biometrics, such as facial and iris recognition, alongside behavioral traits like gait or typing patterns to manage entry to campus facilities. By integrating DL-based facial recognition and iris scanning into smart classrooms, they minimize the risks associated with password-based authentication and identity fraud. Their findings demonstrate strong authentication performance under real-world campus conditions while addressing challenges related to privacy, environmental variability, and practical deployment.

#### 4.4.3.Anomaly detection in network traffic

Chen and Wang [191] investigate how deep-learning techniques, particularly LSTM, 1D-CNN, and autoencoders, can effectively detect anomalies in campus-wide educational networks. They develop a deep-learning-based system designed to identify intrusions, suspicious activities, and misuse by applying CNNs and RNNs to continuously monitor and analyze large

data streams. This approach enables the system to recognize abnormal patterns that signal potential security breaches within educational environments.

#### 4.4.4.Behavioral biometrics for continuous authentication

Hossain and Roy [192] present a cutting-edge continuous authentication framework designed specifically for smart education platforms, which leverages behavioral biometrics and DL to detect unauthorized access in real time. Their work adapts and validates these methods for online classrooms and digital campuses, demonstrating their effectiveness in realistic settings and analyzing the practical trade-offs of implementation. By continuously verifying users through immersive behavioral patterns, such as keystroke dynamics and gait recognition, rather than relying on single-point logins, the framework prevents session takeover and unauthorized access throughout digital learning sessions, thereby strengthening the security of smart learning environments.

#### 4.4.5.Deepfake detection

Rahman et al. [193] propose a hybrid deep-learning system that combines visual and audio analysis over time to detect deepfakes in educational media. Their method achieved strong benchmark results and offers practical benefits for enhancing cybersecurity in learning platforms. By addressing the growing threat posed by GANs, which have made deepfake creation more sophisticated, their system helps maintain authenticity and protect smart learning environments. Recent deep-learning models play a crucial role in identifying forged video and audio content that could otherwise enable the impersonation of students or staff.

#### 4.4.6.Phishing attack mitigation

Patel and Gupta [194] present PhishNet, a specialized deep-learning framework designed to detect phishing emails targeting educational institutions. It tackles threats such as spoofed administrative notices, fake scholarship offers, and credential theft through impersonated campus services. By combining natural language processing models with CNNs, PhishNet analyzes email content for suspicious language and uses vision-based algorithms to identify malicious attachments or counterfeit institutional logos. This targeted approach integrates rich semantic features and advanced hybrid deep-learning techniques, delivering a robust defense that outperforms traditional detectors. Overall, PhishNet provides a strong foundation for securing campus email systems.

#### 4.4.7.Privacy-preserving smart cameras

Nguyen et al. [195] propose a novel framework for privacy-aware, edge-based AI analytics designed explicitly for smart classrooms. Their system processes video data locally on edge devices, safeguarding students' biometric and behavioral information while providing actionable insights such as attention detection and behavior monitoring. By employing lightweight DL models optimized for resource-constrained hardware, the framework delivers scalable, low-latency analytics that do not rely on external cloud processing. Although this approach enhances privacy and reduces data transfer, it must overcome common challenges in edge computing, including hardware limitations, model accuracy issues, and system maintenance concerns.

#### 4.4.8.Access control in IoT-enabled classrooms

Lee et al. [196] present a CV and DL system designed to control access in IoT-enabled smart classrooms. Their system authenticates students and staff, automates attendance tracking, and secures room entry by using intelligent visual analysis. They describe how face recognition and anomaly detection work together to verify authorized users and detect unusual behavior, thereby improving security and convenience compared to traditional badge-based systems. It also examines edge-based inference techniques and presents real-world deployment results, addressing key considerations such as accuracy, privacy, and hardware constraints. Additionally, the proposed system can regulate access to restricted areas or sensitive laboratory equipment by verifying users through face recognition and pose estimation.

#### 4.4.9.Adversarial attack defense

Singh et al. [197] developed a DL and CV-based system to detect and prevent online exam malpractice, including cheating, impersonation, and unauthorized assistance, thereby strengthening academic integrity in remote assessments. They implemented robust DL models capable of resisting adversarial inputs, ensuring that manipulated images or videos cannot deceive facial recognition or object detection tools used in educational contexts. By applying advanced AI techniques, their system enhances the integrity and fairness of remote exams, effectively overcoming the limitations of conventional proctoring methods.

## 5. CHALLENGES AND LIMITATIONS

Deep learning and CV hold immense promise for strengthening cybersecurity in smart education environments, but their practical implementation faces notable challenges and limitations. Below are brief descriptions of the key challenges and constraints that hinder the optimal implementation of DL and CV in enhancing cybersecurity in smart education.

### 5.1. Data privacy and confidentiality

The integration of DL and CV into smart education systems presents significant challenges for data privacy and confidentiality, given the extensive and sensitive nature of the data required for training and deploying these technologies. Smart classrooms often rely on continuous video surveillance and real-time analytics, capturing students' facial images, biometric identifiers, and behavioral patterns, which raises concerns about unauthorized data collection and misuse, especially when informed consent, particularly for minors, is insufficiently addressed. Storing and transmitting high-resolution images and videos increases the risk of data breaches and unauthorized access, and even robust encryption cannot entirely prevent adversarial attacks or insider threats. Sharing datasets across institutions or storing them in centralized cloud services further exposes this data to cyber threats and complicates compliance with privacy laws, such as GDPR, COPPA, and FERPA. Moreover, attackers can exploit trained models through inversion or membership inference attacks to extract sensitive information. This risk is amplified by the smaller, context-specific datasets typical in educational settings, where anonymization can degrade model performance. Deep learning models may also perpetuate biases in training data, resulting in unfair or discriminatory outcomes that compromise both privacy and the integrity of the educational system. Therefore, balancing the demand for large, high-quality datasets with the imperative to protect student privacy remains a critical and unresolved challenge in smart education [198].

### 5.2. Limited labeled data for training

A major challenge in applying DL and CV to cybersecurity in smart education environments is the lack of sufficiently labeled datasets. Deep learning models for tasks such as anomaly detection, facial recognition, and suspicious activity monitoring rely on large volumes of high-quality, annotated data to learn robust, generalizable patterns. However, collecting such data in educational settings raises practical and ethical concerns, as it often involves recording sensitive information, such as student identities, behavior patterns, and access logs, which are limited by privacy regulations and institutional policies. Furthermore, cyber-attacks and security breaches are infrequent compared to routine activities, creating highly imbalanced datasets where malicious instances are scarce. This imbalance hampers effective model training and increases the likelihood of false positives and false negatives. Manual labeling demands significant human effort and domain expertise to distinguish subtle threats from normal behavior, but many institutions lack the resources and skilled personnel to perform this at scale. The limited availability of labeled data not only restricts initial model training but also hinders continuous retraining, which is necessary to counter evolving threats, thereby risking model obsolescence. Additionally, data collected in educational environments often suffers from missing values, inconsistencies, insufficient metadata, and a lack of real-time updates, further degrading model performance. Meeting the high data requirements for DL remains a significant hurdle, as manual labeling remains labor-intensive and time-consuming [199][200].

### 5.3. High computational requirements

One major challenge in utilizing DL and CV to enhance cybersecurity in smart education environments is their high computational demands. Deep learning models, such as CNNs, RNNs, and transformer-based architectures, consume a significant amount of processing power and memory during both training and inference. In smart education settings, these models handle tasks such as real-time video monitoring to detect unauthorized access, analyzing student behavior for anomalies, and identifying malicious content on digital platforms. Processing high-resolution video streams or large volumes of multimodal data in real-time requires powerful GPUs or specialized hardware, such as Tensor Processing Units, which many institutions, especially in low-resource regions, cannot afford or maintain. Training robust models also demands vast datasets and repeated iterations, which necessitate distributed computing or cloud-based solutions, adding costs and introducing potential security and privacy concerns. Deploying these models on edge devices, such as campus cameras or student devices, further complicates matters due to limited processing power and energy constraints, requiring model compression, lightweight architectures, or edge-cloud collaboration. These technical and financial burdens increase latency and operational complexity, thereby undermining the timely detection and mitigation of security threats and posing a persistent barrier to the widespread adoption of smart education systems [51][201].

### 5.4. Model interpretability and explainability

Deep learning and CV models, especially CNNs used for facial recognition, anomaly detection, and real-time threat monitoring, often operate as "black boxes," limiting their interpretability and explainability in smart education cybersecurity. This lack of transparency undermines trust because administrators, educators, students, and parents need clear justifications for automated decisions, such as flagging malicious student behavior or blocking access to resources. It also complicates compliance with data protection laws, such as the EU's GDPR, which requires explainable automated decisions and raises

risks of bias and legal issues in AI-driven surveillance or proctoring systems. Moreover, the inability to interpret model decisions hinders security experts from diagnosing errors, refining training data, and adapting defenses in response to evolving threats and behaviors. To ensure trust, legal compliance, effective incident response, and continuous improvement, smart education environments must prioritize XAI models over relying on opaque DL systems [51][201].

### 5.5. Evolving threat landscape

Enhancing cybersecurity in smart education environments using DL and CV presents a critical challenge due to the rapidly evolving threat landscape. As smart education systems increasingly depend on interconnected devices, real-time data exchange, and pervasive connectivity to deliver personalized learning, they also expand their attack surfaces, exposing sensitive data and infrastructure to sophisticated cyberattacks. Attackers continuously develop novel techniques, such as adversarial, evasion, and poisoning attacks, that manipulate DL models and CV systems used for student authentication, surveillance, and behavior analysis, compromising their reliability. The widespread adoption of BYOD policies and remote access further complicates threat detection, as diverse personal devices with varying security levels create entry points for malware and unauthorized access. Additionally, zero-day vulnerabilities and advanced persistent threats exploit weaknesses in legacy systems, which can limit user cybersecurity awareness and enable infiltrations of networks and disruptions to services [201].

### 5.6. Integration with legacy systems

Deploying DL and CV solutions to enhance cybersecurity in smart education environments presents a critical challenge, as they are often integrated with existing legacy systems. Many educational institutions rely on outdated IT infrastructures and software architectures that cannot support the computational demands and real-time data processing of modern AI-based security frameworks. Legacy systems often feature limited processing power, rigid data formats, and proprietary protocols, which hinder interoperability with contemporary DL models and CV pipelines. For example, incorporating real-time video surveillance powered by CV into older networks can strain bandwidth and storage, resulting in latency and reduced system reliability. Additionally, legacy systems often lack standardized interfaces, such as APIs, which prevents seamless data exchange with student information systems, LMS, and administrative databases. This fragmentation creates data silos that undermine the training and deployment of DL algorithms, which require large, diverse, high-quality datasets to detect anomalies and cyber threats effectively. Retrofitting these systems to comply with modern cybersecurity protocols, such as secure authentication and encrypted communication, often demands costly modifications or complete infrastructure replacement, which many institutions cannot afford. Overall, managing the coexistence of legacy infrastructure and cutting-edge AI technologies remains a significant barrier to realizing robust, AI-driven cybersecurity in smart education.

### 5.7. Real-time processing constraints

A significant challenge in enhancing cybersecurity in smart education environments using DL and CV lies in meeting the stringent demands for real-time or near-real-time processing. These systems continuously monitor activities, including video surveillance, facial recognition for authentication, and anomaly detection in user behavior, to detect and respond to security threats promptly. However, DL models for image and video analysis involve millions of parameters and intensive computations, requiring powerful hardware like GPUs or specialized edge AI chips, which many educational settings cannot afford. Furthermore, security applications require minimal latency to avoid missed or delayed responses, yet edge devices deployed in classrooms or exam halls often have limited computational power, memory, and energy. Streaming extensive video data to central servers also strains network bandwidth and introduces latency, especially in areas with unstable Internet connectivity. Balancing model complexity and speed complicates this further, as simpler models run faster but risk lower accuracy, which can lead to increased false alarms and undermine trust. Consequently, deploying accurate, low-latency DL solutions for real-time cybersecurity in resource-constrained smart education environments remains a significant technical hurdle.

### 5.8. Adversarial Attacks on AI Models

Integrating DL and CV into smart education environments faces a major challenge from adversarial attacks, where attackers deliberately manipulate input data to deceive models into producing incorrect results without noticeable changes to humans. These attacks pose a threat to the integrity, reliability, and security of systems that support personalized learning, student authentication, proctoring, and performance assessment. Although CNNs excel at facial recognition, gesture detection, and behavioral monitoring, their high-dimensional, nonlinear structures make them vulnerable to subtle perturbations, such as altering a student's face image to bypass identity verification or fool plagiarism detectors and automated grading tools. The black-box nature of many deployed models complicates real-time detection and interpretation of such attacks, while adversarial techniques evolve faster than defenses. Although strategies such as adversarial training, input preprocessing, and model regularization can mitigate risks, they often increase computational costs and compromise accuracy on clean data, leaving AI-based security measures vulnerable to new attack vectors through carefully crafted adversarial inputs [201].

### 5.9. Ethical and social implications

Integrating DL and CV to enhance cybersecurity in smart education environments presents significant ethical and social challenges. These technologies enhance threat detection, access control, and monitoring, but also raise concerns about privacy, data ownership, consent, and potential misuse. Computer vision applications, such as automated surveillance, facial recognition, and behavior analysis, continuously collect and process sensitive visual data from students, staff, and visitors across classrooms, hallways, and online platforms, potentially infringing on privacy and creating a climate of constant surveillance that undermines students' freedom of expression and sense of security. Additionally, DL algorithms can perpetuate bias and unfairness when trained on non-representative data, resulting in unequal treatment across demographic groups and exacerbating social inequalities in education. Often, students and guardians lack clear information or control over data collection, which limits informed consent and weakens trust between stakeholders, potentially hindering technology adoption and leading to legal issues under regulations such as GDPR and COPPA. Moreover, the misuse of collected data through breaches or the repurposing of surveillance for intrusive monitoring poses critical risks to security, personal freedoms, and civil liberties. Excessive monitoring risks fostering distrust and compromising student autonomy and well-being, making it essential to strike a balance between security objectives and robust ethical safeguards.

### 5.10. Cost and scalability

Integrating DL and CV into smart education systems to enhance cybersecurity poses substantial financial and scalability challenges. Educational institutions must invest heavily in high-performance GPUs or specialized hardware accelerators to develop and deploy robust models while also managing the costs of collecting and annotating large, diverse datasets required for accurate training. Installing and maintaining high-resolution cameras and edge devices across physical and virtual learning environments adds further expenses. As these systems expand to serve more students, campuses, and online platforms, they require additional hardware and adaptive model architectures to handle increasing data streams in real time without sacrificing performance. Institutions must continuously update and retrain models to counter evolving cyber threats, demanding ongoing resources and specialized expertise that may not always be available. Consequently, deploying DL and CV solutions at scale across diverse educational settings presents a complex financial and logistical burden, requiring careful management to maintain effective, secure, and cost-efficient cybersecurity protections [67].

### 5.11. Model robustness and generalization

Applying DL and CV to enhance cybersecurity in smart education environments faces significant challenges in ensuring model robustness and generalization. Robustness demands that models maintain reliable performance despite unexpected, noisy, or adversarial inputs, while generalization requires them to effectively handle unseen data that differs subtly from their training sets. Smart education systems generate heterogeneous, dynamic data streams, such as real-time video surveillance, biometric authentication, and behavioral logs, that are prone to noise, variation, and deliberate attacks. Consequently, models for tasks such as anomaly detection, identity verification, and behavioral monitoring must be robust against input perturbations and be able to adapt to evolving threats. However, many models overfit to curated training data, resulting in poor performance under real-world conditions. For example, intrusion detection systems may miss novel attacks, and facial recognition systems may fail under poor lighting conditions or in the presence of spoofing attempts. Adversarial attacks further undermine robustness by introducing subtle, human-imperceptible perturbations that mislead models and bypass security measures. The diversity of devices and environments, ranging from high-resolution classroom cameras to low-quality remote learner devices, complicates the development of universally robust models capable of handling variations in student behavior, curricula, and assessment methods while minimizing bias. Additionally, challenges such as data scarcity, domain shifts, and biased datasets threaten the accuracy and fairness of models, ultimately hindering the effectiveness of cybersecurity in smart education [202].

### 5.12. Scalability challenge

Scalability poses a challenge when deploying DL and CV solutions to enhance cybersecurity in smart education environments. As educational institutions increasingly integrate IoT-enabled classrooms, intelligent surveillance, and automated identity verification, they must process vast and diverse data streams from multiple campuses in real-time. These DL models require substantial computational power, often unavailable in resource-limited settings. They must adapt continuously to varying sensor types, image qualities, and network conditions through frequent retraining, which increases operational costs. Moreover, maintaining low-latency inference across concurrent video and sensor feeds is crucial for timely threat detection, but it becomes increasingly complex as the system scales. Additionally, scaling these solutions requires careful management of data privacy and compliance with regulations such as GDPR, as distributed deployments involve sensitive information shared across nodes.

## 6. FUTURE RESEARCH DIRECTIONS

As smart education systems increasingly leverage DL and CV to enhance cybersecurity, researchers can explore new directions to address unresolved challenges and expand existing capabilities. Below are detailed future research directions that can drive cybersecurity in smart education through the use of DL and CV.

### 6.1. Development of Lightweight DL Models

Future research should prioritize designing and deploying lightweight DL models tailored for cybersecurity in smart education environments. As smart education systems integrate more interconnected devices and edge-based learning platforms, they face challenges such as limited computational power, memory, and energy resources. Traditional DL models, though accurate, often require substantial processing and storage, which can impede real-time threat detection and increase latency on resource-constrained devices. To overcome these limitations, researchers should develop compact neural network architectures and apply model compression techniques, such as pruning, quantization, and knowledge distillation, to reduce computational demands while maintaining high detection accuracy. Deploying these lightweight models on edge devices, such as smart cameras, wearable devices for students, and IoT sensors, enables real-time monitoring and anomaly detection locally, thereby minimizing reliance on continuous cloud communication. This decentralized approach not only lowers network bandwidth usage but also strengthens data privacy by keeping sensitive information on the device. Researchers should leverage automated neural architecture search and meta-learning to design models that adapt to varying device capabilities and evolving cybersecurity threats. Combining these models with federated learning can further enhance system resilience by enabling collaborative learning across institutions without requiring the sharing of raw data. Advancing lightweight DL solutions will support scalable, efficient, and privacy-preserving cybersecurity in smart education, ensuring robust protection for students, educators, and infrastructure in increasingly connected learning environments.

### 6.2. Integration with Federated Learning

Integrating federated learning into DL and CV frameworks offers a promising direction for strengthening cybersecurity in smart education environments. Federated learning enables multiple decentralized devices or institutions to collaboratively train a shared global model without exchanging raw data, directly addressing privacy and security concerns associated with sensitive educational information such as student records, behavioral patterns, and surveillance feeds. By keeping data local and transmitting only model updates or gradients, federated learning reduces the risks associated with centralized data storage and transmission, minimizes the attack surface, and supports compliance with data protection regulations such as GDPR and FERPA. It also enhances model generalizability and robustness across diverse educational contexts, accommodating the heterogeneity of smart classrooms, online platforms, and campus security systems that operate under varying hardware, network, and privacy constraints. Combining federated learning with secure aggregation techniques and differential privacy further safeguards against adversarial attacks, model inversion, and gradient leakage. Future research should prioritize the development of efficient federated learning protocols tailored to the resource limitations of edge cameras, mobile devices, and IoT sensors used in smart education, with a focus on lightweight models, communication-efficient updates, and resilient aggregation mechanisms. Additionally, exploring the synergy between federated learning and advanced CV tasks, such as real-time anomaly detection, facial recognition, and behavior analysis, can enable proactive, adaptive cybersecurity measures.

### 6.3. Context-Aware Anomaly Detection

A promising direction for future research is the development of context-aware anomaly detection frameworks designed explicitly for smart education environments. Unlike traditional systems that flag anomalies without considering the dynamic contexts of educational activities, context-aware models can significantly reduce false positives and missed threats in diverse settings with various users, devices, and applications. Smart education involves real-time interactions among students, educators, intelligent tutoring systems, IoT devices, and cloud-based platforms, each generating context-dependent data shaped by user roles, lesson schedules, pedagogical goals, locations, and device status. By integrating contextual information, such as temporal patterns, user profiles, and situational cues, into anomaly detection, researchers can enhance accuracy and responsiveness. Hybrid approaches that combine DL techniques, such as RNNs or GNNs, with contextual embedding can capture temporal dependencies and relational structures within educational data. Incorporating CV to interpret visual contexts, such as classroom activities or user gestures, can further strengthen situational awareness. Researchers must also address challenges related to data privacy, real-time processing, and scalability by employing privacy-preserving learning methods, edge computing, and lightweight model architectures. Advancing these context-aware mechanisms will enable adaptive, intelligent security solutions that keep pace with the evolving demands of smart education, fostering a safer and more resilient digital learning ecosystem capable of detecting sophisticated threats, such as context-specific phishing or unauthorized access.

### 6.4. Adversarial Robustness and Explainability

Despite their promising role in enhancing cybersecurity within smart education systems, DL, and CV models remain inherently susceptible to adversarial attacks and often lack interpretability. Malicious actors can exploit subtle input manipulations to bypass authentication, tamper with surveillance, or compromise content moderation undetected. To address these risks, researchers should focus on developing robust architectures that withstand adversarial inputs by implementing defense mechanisms such as adversarial training, input preprocessing, certified defenses, robust optimization, and uncertainty estimation. Tailoring and benchmarking these defenses using datasets that reflect student behaviors, classroom settings, and online learning platforms will help adapt solutions to the specific threats faced in educational contexts. Equally important, researchers should advance XAI techniques that make model predictions transparent and understandable to educators, administrators, and students without sacrificing performance. Combining post-hoc explanations, inherently interpretable designs, and user-centered explainability will foster trust, enhance accountability, and support the adoption of ethical, responsible AI in smart education environments.

### 6.5. Real-Time Visual Surveillance for Insider Threats

A key direction for future research to strengthen cybersecurity in smart education environments is the development of real-time visual surveillance systems that harness advanced DL and CV techniques to detect and mitigate insider threats. Unlike external attacks, insider threats originate from authorized users who exploit legitimate access, making them challenging to detect with traditional security measures. By embedding real-time video analytics into smart campus infrastructure, institutions can continuously monitor user behaviors and physical interactions with critical systems, adding a vital layer of protection. Cutting-edge object detection, facial recognition, and human action recognition models can help identify unauthorized access, suspicious movements, or behavioral anomalies that signal potential misuse. Researchers should design lightweight yet robust DL models capable of processing high-resolution video streams in real-time while maintaining low computational demands for scalability across multiple surveillance nodes. They must also address privacy concerns by ensuring compliance with data protection laws and ethical standards through the use of privacy-preserving analytics, federated learning, and anonymization techniques. Combining visual surveillance with multimodal data, such as biometric signals, access logs, and environmental context, can further enhance the accuracy of detection. Developing adaptive threat models that learn from contextual cues and historical patterns will improve the system's ability to distinguish between benign anomalies and genuine threats. Expanding these CV applications to physical learning spaces, utilizing facial recognition, gait analysis, or behavior monitoring in smart classrooms and labs, can further safeguard sensitive resources and uphold trust within the academic community.

### 6.6. Privacy-Preserving CV Techniques

As smart education systems increasingly utilize DL and CV to enhance cybersecurity through identity verification, behavior monitoring, and anomaly detection, they inevitably collect sensitive visual data, including facial images, gestures, and environmental contexts. This extensive reliance on visual surveillance and biometric cues raises serious privacy concerns that can erode user trust and challenge regulatory compliance. To address these issues, future research should focus on developing robust privacy-preserving CV techniques tailored for smart educational settings. Promising solutions include federated learning, which enables collaborative training of visual models across edge devices without centralizing raw images, and differential privacy, which injects calibrated noise into features or outputs to protect individual identities. Cryptographic methods, such as secure multi-party computation and homomorphic encryption, can further ensure that encrypted visual data remains private during processing, supporting secure facial recognition and activity monitoring without exposing raw images. Adversarial obfuscation methods, such as face de-identification, silhouette extraction, and privacy filters, can also obscure identifiable features in real time, allowing for context-aware monitoring while upholding privacy. Researchers should explore the balance between computational demands and privacy guarantees, design lightweight, privacy-enhanced models suitable for resource-constrained edge devices, and establish frameworks to assess and mitigate privacy risks. Advancing these privacy-preserving vision techniques is crucial for maintaining trust, ensuring regulatory compliance, and promoting ethical surveillance in smart education, which demands interdisciplinary collaboration among machine learning experts, cryptographers, and educational policymakers.

### 6.7. Cross-Domain Transfer Learning

As smart education systems increasingly integrate diverse digital platforms, they face complex cybersecurity challenges due to the variety of data types, devices, and user behaviors involved. Deep learning models often underperform when applied to different but related domains due to domain shift; however, cross-domain transfer learning offers a promising solution by enabling models to leverage knowledge from one domain and adapt it effectively to another. In smart education, this approach can enhance the robustness and generalizability of DL and CV techniques. For instance, models trained to detect phishing attacks or unauthorized access on one platform can be transferred and fine-tuned to identify similar threats in other contexts, even with limited labeled data, reducing the need for costly retraining and large-scale data annotation. By transferring representations of normal and abnormal behaviors across different user groups, devices, or network conditions,

cross-domain transfer learning can also improve anomaly detection and uncover subtle or evolving threats that traditional methods might miss. Future research should develop novel transfer learning architectures and domain adaptation strategies that minimize distribution discrepancies between domains. It should also explore multi-source transfer learning to integrate knowledge from various educational contexts and incorporate explainability to build trust and transparency in these models. Advancing these methodologies will help create adaptive, scalable, and effective cybersecurity solutions that meet the dynamic needs of smart education, enabling institutions to secure diverse digital environments with minimal labeled data and efficient fine-tuning techniques.

### 6.8. Integration With Iot Security Frameworks

As smart education environments increasingly rely on interconnected devices, such as smartboards, IoT-enabled sensors, cameras, wearables, and networked educational tools, their cybersecurity landscape becomes more complex and demanding. To address this, future research should integrate DL and CV techniques with existing and emerging IoT security frameworks to develop robust, adaptive defenses tailored for smart educational ecosystems. The diverse IoT devices in these settings constantly generate vast data streams, enabling seamless interactions among students, educators, and content. However, they also expand the attack surface, exposing systems to threats such as unauthorized access, data breaches, device tampering, and privacy violations. Traditional IoT security frameworks often struggle with scalability, real-time detection, and adapting to evolving threats. The heterogeneity and limited resources of devices further hinder conventional approaches. Researchers should, therefore, focus on DL-enhanced anomaly detection to monitor network traffic and behavior in real time, apply CV for secure authentication and physical security, deploy lightweight models on edge devices for timely threat response, and develop context-aware security policies that adapt dynamically to specific educational scenarios. Additionally, they should incorporate privacy-preserving techniques, such as federated learning, and ensure that new solutions align with existing IoT security standards to guarantee interoperability across diverse educational technologies. By embedding DL and CV into IoT security protocols, smart education systems can become more resilient, proactive, scalable, and privacy-conscious, ultimately safeguarding trust, safety, and continuity in digital learning spaces.

### 6.9. Automated Threat Intelligence and Response Systems

As smart education environments increasingly integrate connected devices, cloud platforms, and AI-driven tools, they face a more complex and vulnerable cybersecurity landscape. Automated Threat Intelligence and Response Systems (ATIRS) provide a vital solution by leveraging DL and CV to detect, analyze, and mitigate cyberattacks in real-time. Future research should focus on developing advanced DL models that process diverse data sources, such as network traffic, user behavior, and system logs, to identify emerging threats—including zero-day vulnerabilities and polymorphic malware—that traditional systems often miss. Additionally, applying CV techniques to visual data from cameras and IoT devices can enable automated detection of anomalous behaviors or unauthorized access, triggering immediate security responses without human intervention. Researchers must also design ATIRS to execute automated, context-aware mitigation actions, such as isolating compromised devices and blocking malicious traffic, while optimizing strategies through reinforcement learning to balance security with operational continuity. Establishing secure, privacy-compliant frameworks for federated threat intelligence sharing among educational institutions will enhance collective defense without compromising sensitive information. Ethical AI frameworks are crucial to ensure that these systems respect privacy, avoid bias, and maintain transparency, thereby fostering trust among educators, students, and cybersecurity staff. Ultimately, scalable, hybrid cloud-edge architectures tailored to the diverse needs and resource constraints of educational institutions will enable efficient deployment and rapid response to threats. By integrating these elements, ATIRS can provide autonomous, adaptive cybersecurity solutions that reduce manual intervention, deliver real-time alerts, and dynamically update defenses to protect smart education environments proactively.

### 6.10. Comprehensive Ethical and Regulatory Frameworks

As smart education increasingly integrates advanced technologies like DL and CV, future research must develop comprehensive ethical and regulatory frameworks to address the unique challenges posed by AI-driven cybersecurity solutions in educational settings. Researchers should establish clear ethical guidelines that protect student privacy by minimizing data exposure, ensuring informed consent, promoting transparency in AI decision-making, and mitigating algorithmic biases to prevent discrimination. They must also clarify accountability for AI-related errors or breaches. Aligning these solutions with existing data protection laws, such as GDPR and FERPA, and establishing standardized protocols and certification processes will enhance regulatory compliance and foster trust among institutions, students, and parents. Effective frameworks require interdisciplinary collaboration among ethicists, legal experts, educators, technologists, and policymakers to ensure adaptability across diverse educational contexts. Moreover, research should design dynamic governance models that enable continuous monitoring and updating of standards, leveraging AI-driven auditing tools to detect risks and non-compliance in real-time. Finally, raising awareness and training stakeholders, including educators, administrators, and students, on ethical principles and data rights will promote responsible AI use and foster a culture of ethical cybersecurity. By proactively addressing these dimensions, future work can ensure that advances in AI-powered

cybersecurity not only strengthen system resilience but also uphold privacy, fairness, and accountability, ultimately creating safer, more trustworthy learning environments.

### 6.11. Collaborative Systems

Collaborative systems in cybersecurity strengthen joint research initiatives by uniting educational institutions, cybersecurity experts, and AI researchers to develop innovative security solutions. By establishing data-sharing and threat intelligence platforms, these systems enable institutions to exchange critical threat information and best practices, enhancing cooperation. Developing open-source security tools and frameworks further accelerates the adoption of AI-driven security measures. Additionally, cross-disciplinary training programs that combine cybersecurity expertise with AI knowledge help build a more skilled workforce. Implementing standardized security protocols across multiple educational institutions ensures consistent and effective cybersecurity practices.

## 7. CONCLUSION

This survey has thoroughly explored the critical role that DL and CV play in strengthening cybersecurity within smart education environments. As educational institutions increasingly adopt smart technologies and IoT-enabled systems, they face a more complex and evolving threat landscape. By integrating advanced DL algorithms, such as CNNs and RNNs, with CV techniques, institutions can implement robust, adaptive, and automated security measures tailored to the unique demands of smart education.

These technologies significantly enhance threat detection accuracy, enable real-time monitoring, and support proactive defenses against threats such as unauthorized access, identity spoofing, and content manipulation. However, despite these promising capabilities, challenges persist. Data privacy concerns, limited model interpretability, high computational requirements, and the scarcity of domain-specific datasets remain pressing issues. Furthermore, the dynamic and diverse nature of smart education systems calls for scalable and flexible cybersecurity frameworks that can adapt to changing conditions.

Future research must address these challenges by developing privacy-preserving approaches such as federated learning and differential privacy, improving model explainability, and strengthening resilience against adversarial attacks. Efforts should also focus on building trustworthy, explainable AI models that foster transparency and user confidence. Close collaboration among cybersecurity experts, educators, and AI researchers will be crucial in designing user-centric, privacy-conscious solutions that align with educational objectives. Ultimately, the continued advancement and integration of DL and CV will play a transformative role in protecting educational data, preserving system integrity, and creating secure digital learning environments that promote innovation and academic excellence.

## Conflicts of Interest

The authors declare that they have no conflict of interest.

## Funding

This research received no external funding.

## Acknowledgment

The authors would like to thank their respective universities for their support. They also acknowledge the contributions of colleagues and reviewers whose feedback helped improve the quality of this manuscript.

## References

[1] S. Wu, H. Qian, B. O. Jiang, W. Zhang, Y. Cao, J. Cui, R. Li, B. Jiang, and W. Zhang, "A Comprehensive Exploration of Personalized Learning in Smart Education: From Student Modeling to Personalized Recommendations," *Journal of the ACM*, vol. 37, no. 4, pp. 1-82, 2024. https://doi.org/https://doi.org/10.48550/arXiv.2402.01666

[2] E. G. Rincon-Flores, L. Castano, S. L. Guerrero Solis, O. Olmos Lopez, C. F. Rodríguez Hernández, L. A. Castillo Lara, and L. P. Aldape Valdés, "Improving the learning-teaching process through adaptive learning strategy," *Smart Learning Environments*, vol. 11, no. 1, pp. 1–27, 2024. https://doi.org/10.1186/S40561-024-00314-9/FIGURES/9

[3] X. Shu, and X. Gu, "An Empirical Study of A Smart Education Model Enabled by the Edu-Metaverse to Enhance Better Learning Outcomes for Students," *Systems*, vol. 11, no. 2, pp. 1-20, 2023. https://doi.org/10.3390/SYSTEMS11020075

[4] A. Badshah, A. Ghani, A. Daud, A. Jalal, M. Bilal, and J. Crowcroft, "Towards Smart Education through Internet of Things: A Survey," *ACM Computing Surveys*, vol. 56, no. 2, pp. 1–33, 2023. https://doi.org/10.1145/3610401.

[5] D. Aggarwal, D. Sharma, and A. B. Saxena, "Smart Education: An Emerging Teaching Pedagogy for Interactive and Adaptive Learning Methods," *Journal of Learning and Educational Policy*, vol. 44, pp. 1–9, 2024. https://doi.org/10.55529/jlep.44.1.9

[6] M. Liu, and D. Yu, "Towards intelligent E-learning systems," *Education and Information Technologies*, vol. 28, no. 7, pp. 7845–7876, 2023. https://doi.org/10.1007/S10639-022-11479-6/TABLES/5

[7] K. Jangjarat, P. Klayklung, P. Chocksathaporn, and P. Maskran, "The Impact of Smart Education on Learning Outcomes in the Digital Era: A Systematic Review," *Advance Knowledge for Executives*, vol. 2, no. 2, pp. 1-9, 2023. https://papers.ssrn.com/abstract=4424676

[8] B. Omonayajo, F. Al-Turjman, and N. Cavus, "Interactive and innovative technologies for smart education," *Computer Science and Information Systems,* vol. 19, no. 3, pp. 1549–1564, 2022. https://doi.org/10.2298/csis210817027o.

[9] A. Adel, "The Convergence of Intelligent Tutoring, Robotics, and IoT in Smart Education for the Transition from Industry 4.0 to 5.0," *Smart Cities*, vol. 7, no. 1, pp. 325–369, 2024. https://doi.org/10.3390/smartcities7010014

[10] Y. Supriya, D. Bhulakshmi, S. Bhattacharya, T. R. Gadekallu, P. Vyas, R. Kaluri, S. Sumathy, S. Koppu, D. J. Brown, and M. Mahmud, "Industry 5.0 in Smart Education: Concepts, applications, challenges, opportunities, and future directions," *IEEE Access*, vol. 12, pp. 81938–81967, 2024. https://doi.org/10.1109/access.2024.3401473

[11] L. Nguyen, S. Tomy, and E. Pardede, "Enhancing Collaborative Learning and E-Mentoring in a Smart Education System in Higher Education," *Computers*, vol. 13, no. 1, pp. 1-29, 2024. https://doi.org/10.3390/computers13010028

[12] E.J. Chukwuemeka, "Smart education: opportunities, challenges and future of traditional education," *International Journal of Smart Technology and Learning,* vol. 4, no. 3, pp. 191–202, 2025. 10.1504/IJSMARTTL.2025.146286

[13] M. Clavel-Maqueda, L. E. Guzmán-Escorza, E. Cornejo-Velázquez, and M. Á. Torres-González, "Smart Education as a tool for sustainable development, equity, and social justice," In *Advances in Computational Intelligence and Robotics book series* (pp. 79–104), IGI Global, 2025. https://doi.org/10.4018/979-8-3693-8161-8.ch005

[14] A. Badshah, M. Nasralla, A. Jalal, and H. Farman, "Smart Education in Smart Cities: Challenges and Solution," *2023 IEEE International Smart Cities Conference (ISC2),* Bucharest, Romania, 24-27 September 2023, pp. 01-08. https://doi.org/10.1109/ISC257844.2023.10293615.

[15] J. Chen, and H. Liu, "Effects of Smart Classroom on Students' Learning Outcomes," *International Journal of Web-Based Learning and Teaching Technologies*, vol. 19, no. 1, pp. 1-3, 2024. https://doi.org/10.4018/ijwltt.356509.

[16] N. Firdausi, N. Fithriyah, R. Ummah, M. Abidin, R. Nirwana, W. Achmad, and F. Kuswanto, "Integrating Smart Education in Basic Education: A Systematic Review of Roles and Challenges," *2024 International Conference on ICT for Smart Society (ICISS),* Bandung, Indonesia, 04-05 September 2024, pp. 1-6. https://doi.org/10.1109/ICISS62896.2024.10751462.

[17] J. Yang, Y. Sun, R. Lin, and H. Zhu, "Strategic Framework and Global Trends in National Smart Education Policies," *Humanities and Social Sciences Communications,* vol. 11, no. 1, pp. 1–13, 2024. https://doi.org/10.1057/s41599-024-03668-0

[18] M. Mahmood, and J. Abdul-Jabbar, "Securing Industrial Internet of Things (Industrial IoT)- A Reviewof Challenges and Solutions," *Al-Rafidain Engineering Journal (AREJ),* vol. 28, no. 1, pp. 312–320, 2023. https://doi.org/10.33899/RENGJ.2022.135292.1196

[19] I. Shakhina, O. Podzygun, A. Petrova, and G. Gordiichuk, "Smart Education in the Transformation Digital Society," *Modern Information Technologies and Innovation Methodologies of Education in Professional Training Methodology Theory Experience Problems*, vol. 67, no. 1, pp. 51–64, 2023. https://doi.org/10.31652/2412-1142-2023-67-51-64

[20] A. Kumar, M. Rani, D. Raje Sisodia, Y. Perwej, A. C. Kakde, F. Makhbuba Rakhimjonovna, and A. Professor, "Transforming Education Through IoT and AI: Opportunities And Challenges," *Educational Administration: Theory and Practice.* Vol. 2024, no. 5, pp. 11610–11622, 2024. https://doi.org/10.53555/kuey.v30i5.4982

[21] A. S. Almogren, W. M. Al-Rahmi, and N. A. Dahri, "Exploring factors influencing the acceptance of ChatGPT in higher education: A smart education perspective," *Heliyon*, vol. 10, no. 11, pp. 1–19, 2024. https://doi.org/10.1016/j.heliyon.2024.e31887

[22] Y. Cheng, "Research on data security and privacy protection in smart Campus," *International Journal of New Developments in Education*, vol. 5, no. 14, pp. 7–10, 2023. https://doi.org/10.25236/ijnde.2023.051402

[23] U. Butt, Y. Dauda, and B. Shaheer, "Ransomware Attack on the Educational Sector," *Advanced Sciences and Technologies for Security Applications*, Part F15, pp. 279–313, 2023. https://doi.org/10.1007/978-3-031-33627-0_11

[24] M. Venturini, F. Freda, E. Miotto, A. Giaretta, and M. Conti, "Differential Area Analysis for Ransomware: Attacks, Countermeasures, and Limitations," *IEEE Transactions on Dependable and Secure Computing,* pp. 1-16, 2023. https://doi.org/10.1109/TDSC.2025.3532324

[25] C. I. Eke, A. A. Norman, and M. Mulenga, "Machine learning approach for detecting and combating bring your own device (BYOD) security threats and attacks: a systematic mapping review," *Artificial Intelligence Review,* vol. 56, no. 8, pp. 8815–8858, 2023. https://doi.org/10.1007/S10462-022-10382-3/METRICS

[26] Z. Othman, "Sustainability of higher education institutions: Case study on cyber attacks," *Global Business Management Review (GBMR),* vol. 15, no. 1, pp. 24–38, 2023. https://doi.org/10.32890/GBMR2023.15.1.2

[27] L. Li, C. P. Chen, L. Wang, K. Liang, and W. Bao, "Exploring Artificial Intelligence in Smart Education: Real-Time Classroom Behavior Analysis with Embedded Devices," *Sustainability*, vol. 15, no. 10, pp. 1–24, 2023. https://doi.org/10.3390/su15107940

[28] D. Magetos, S. Mitropoulos, and C. Douligeris, "Cybersecurity of Distance Education," *2024 9th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM),* Athens, Greece, 20-22 September 2024, pp. 115–120. https://doi.org/10.1109/SEEDA-CECNSM63478.2024.00029

[29] M. Akese, O. Hussein, and M. A. K. Abbasi, "Exploring Vulnerabilities and Mitigation Strategies Among High School Students: A Qualitative Analysis Study," *University of Skovdo,* vol. 1, no. 1, pp. 1–54, 2024. https://www.diva-portal.org/smash/get/diva2:1878459/FULLTEXT01.pdf

[30] G. Alotibi, "A Cybersecurity Awareness Model for the Protection of Saudi Students from Social Media Attacks," *Engineering, Technology and Applied Science Research,* vol. 14, no. 2, pp. 13787–13795, 2024. https://doi.org/10.48084/etasr.7123

[31] R. Tanti, "Study of Phishing Attack and their Prevention Techniques," *International Journal of Scientific Research in Engineering and Management,* vol. 08, no. 10, pp. 1–8, 2024. https://doi.org/10.55041/IJSREM38042

[32] Q. Ismail, S. Almutairi, and H. Kurdi, "Trust-Enabled Framework for Smart Classroom Ransomware Detection: Advancing Educational Cybersecurity Through Crowdsourcing," *Information*, vol. 16, no. 4, pp. 1-16, 2025. https://doi.org/10.3390/info16040312

[33] H. S. Lallie, A. Thompson, E. Titis, and P. Stephens, "Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector," *Computers*, vol. 14, no. 2, pp. 1-28, 2025. https://doi.org/10.3390/COMPUTERS14020049

[34] I. I. Abdul Halim, A. G. Buja, J. Mohamad Zain, A. H. Ngah, and R. Bansal, "BYOD Security Policy Model: A Systematic Literature Review," *Journal of Advanced Research in Applied Sciences and Engineering Technology,* vol. 60, no. 4, pp. 87–103, 2024. https://doi.org/10.37934/araset.60.4.87103

[35] A. Miranda-García, A. Rego, I. Pastor-López, B. Sanz, A. Tellaeche, J. Gaviria, and P. Bringas, "Deep learning applications on cybersecurity: A practical approach," *Neurocomputing*, vol. 563, pp. 126904, 2023. https://doi.org/10.1016/j.neucom.2023.126904.

[36] J. Ruan, G. Liang, J. Zhao, H. Zhao, J. Qiu, F. Wen, and Z. Y. Dong, "Deep learning for cybersecurity in smart grids: Review and perspectives," *Energy Conversion and Economics,* vol. 4, no. 4, pp. 233–251, 2023. https://doi.org/10.1049/enc2.12091

[37] A. Aldhaheri, F. Alwahedi, M. A. Ferrag, and A. Battah, "Deep learning for cyber threat detection in IoT networks: A review," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 110–128, 2024. https://doi.org/10.1016/j.iotcps.2023.09.003

[38] M. M. A. Parambil, L. Ali, F. Alnajjar and M. Gochoo, "Smart Classroom: A Deep Learning Approach towards Attention Assessment through Class Behavior Detection," *2022 Advances in Science and Engineering Technology International Conferences (ASET)*, Dubai, United Arab Emirates, 2022, pp. 1-6, doi: 10.1109/ASET53988.2022.9735018.

[39] G. Takács, J. Mihalík, M. Gulan, A. Vargová, E. Mikuláš, and Š. Ožana, "MagnetoShield: A Novel Open-Source Magnetic Levitation Benchmark Device for Mechatronics Education and Research," *Sensors*, vol. 24, no. 2, pp. 1-33, 2024. https://doi.org/10.3390/S24020538

[40] K. Achuthan, S. Ramanathan, S. Srinivas, and R. Raman, "Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions," *Frontiers in Big Data*, vol. 7, pp. 1–18, 2024. https://doi.org/10.3389/fdata.2024.1497535

[41] I. Ortiz-Garcés, J. Govea, S. Sánchez-Viteri, and W. Villegas-Ch, "CyberEduPlatform: an educational tool to improve cybersecurity through anomaly detection with Artificial Intelligence," *PeerJ. Computer science*, vol. 10, pp. 1-33, 2024. https://doi.org/10.7717/peerj-cs.2041

[42] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," *Journal of Big Data*, vol. 11, no. 1, pp. 1–38, 2024. https://doi.org/10.1186/s40537-024-00957-y

[43] N. M. O. Okafor, "Deep learning in cybersecurity: Enhancing threat detection and response," *World Journal of Advanced Research and Reviews*, vol. 24, no. 3, pp. 1116–1132, 2024. https://doi.org/10.30574/wjarr.2024.24.3.3819

[44] O. Milov, I. Rahimova, A. Havrylova, S. Golovashych, I. Aksonova, and D. Pecherytsia, "Cybersecurity of SMART Technologies Using Deep Learning Methods," *2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT),* Ankara, Turkiye, 07-09 November 2024, pp. 1-6, doi: 10.1109/ISMSIT63511.2024.10757295.

[45] N. Abdi, A. Albaseer, and M. Abdallah, "The role of deep learning in advancing proactive cybersecurity measures for smart grid networks: a survey," *arXiv (Cornell University)*, pp. 1–25, 2024. https://doi.org/10.48550/arxiv.2401.05896

[46] S. Ouf, S. Ahmed, and Y. Helmy, "A blockchain based deep learning framework for a smart learning environment," *Scientific Reports,* vol. 15, no. 1, pp. 1–28, 2025. https://doi.org/10.1038/s41598-025-03688-z

[47] R. Chinnasamy, M. Subramanian, S. V. Easwaramoorthy, and J. Cho, "Deep learning-driven Methods for Network-based Intrusion Detection Systems: A Systematic review," *ICT Express,* vol. 11, no. 1, pp. 181–215, 2025. https://doi.org/10.1016/j.icte.2025.01.005

[48] M. L. Ali, K. Thakur, S. Schmeelk, J. Debello, and D. Dragos, "Deep Learning vs. Machine Learning for Intrusion Detection in Computer Networks: A Comparative Study," *Applied Sciences,* vol. 15, no. 4, pp. 1-19, 2025. https://doi.org/10.3390/app15041903

[49] U. Ahmed, M. Nazir, A. Sarwar, T. Ali, E. M. Aggoune, T. Shahzad, and M. A. Khan, "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering," *Scientific Reports,* vol. 15, no. 1, pp. 1–33, 2025. https://doi.org/10.1038/s41598-025-85866-7

[50] K. Verma, D. Ghosh, and A. Kumar, "Visual tracking in unstabilized real time videos using SURF," *Journal of Ambient Intelligence and Humanized Computing,* vol. 15, no. 1, pp. 809–827, 2024. https://doi.org/10.1007/S12652-019-01249-7/METRICS

[51] M. Ragab, B. M. Alghamdi, R. Alakhtar, H. Alsobhi, L. A. Maghrabi, G. Alghamdi, S. Nooh, and A. A. M. AL-Ghamdi, "Enhancing cybersecurity in higher education institutions using optimal deep learning-based biometric verification," *Alexandria Engineering Journal,* vol. 117, pp. 340–351, 2025. https://doi.org/10.1016/J.AEJ.2025.01.012

[52] I. Hamid, and M. M. H. Rahman, "AI, machine learning and deep learning in cyber risk management," *Discover Sustainability,* vol. 6, no. 1, pp. 1–21, 2025. https://doi.org/10.1007/s43621-025-01012-3

[53] M. Roshanaei, and M.G. Jachura, "Integrating AI in Cybersecurity Higher Education: A Path to Workforce Readiness," *Journal of Intelligent Learning Systems and Applications,* vol. 17, pp. 45-67, 2025. https://doi.org/10.4236/jilsa.2025.172005

[54] A. Kamenskih, "The analysis of security and privacy risks in smart education environments," *Journal of Smart Cities and Society*, vol. 1, no. 1, pp. 17–29, 2022. https://doi.org/10.3233/scs-210114

[55] J. Vykopal, P. Seda, V. Švábenský, and P. Čeleda, "Smart environment for adaptive learning of cybersecurity skills," *IEEE Transactions on Learning Technologies,* vol. 16, no. 3, pp. 443–456, 2022. https://doi.org/10.1109/tlt.2022.3216345

[56] A. A. Abd El-Latif, Y. Maleh, M. A. El-Affendi, and S. Ahmad, "Cybersecurity Management in Education Technologies: Risks and Countermeasures for Advancements in E-learning," In A. A. Abd El-Latif, Y. Maleh, M. A. El-Affendi, & S. Ahmad (Eds.), *Cybersecurity Management in Education Technologies: Risks and Countermeasures for Advancements in E-learning* (1st Edition). CRC Press, 2023. https://doi.org/10.1201/9781003369042/

[57] A. Absadyk, and Y. Absattar, "Using a Virtual Twin of a Building to Ensure Security in Educational Institutions," *Scientific Journal of Astana IT University,* vol. 14, no. 14, pp. 127–140, 2023. https://doi.org/10.37943/14luqf6985.

[58] A. Guesmi, M. A. Hanif, B. Ouni, and M. Shafique, "Physical adversarial attacks for camera-based smart systems: current trends, categorization, applications, research challenges, and future outlook," *arXiv (Cornell University),* pp. 1–54, 2023. https://doi.org/10.48550/arxiv.2308.06173

[59] N. D. Jagli, "The role of artificial intelligence in cyber security," *Journal of Electrical Systems,* vol. 20, no. 3, pp. 5283-5291, 2024. https://doi.org/10.52783/jes.6327

[60] E. Paolini, L. Valcarenghi, L. Maggiani, and N. Andriolli, "Real-Time Network Packet Classification Exploiting Computer Vision Architectures," *IEEE Open Journal of the Communications Society,* vol. 5, pp. 1155-1166, 2024. https://doi.org/10.1109/OJCOMS.2024.3363082.

[61] I. D. Mienye, and T. G. Swart, "A Comprehensive Review of Deep Learning: Architectures, Recent Advances, and Applications," *Information*, vol. 15, no. 12, pp. 1-45, 2024. https://doi.org/10.3390/INFO15120755

[62] B. T. M. Wong, K. C. Li, and M. Liu, "Smart Education across Academic Disciplines: A Systematic Literature Review," *Journal of Educational Technology Development and Exchange (JETDE),* vol. 18, no. 1, pp. 85–108, 2025. https://doi.org/10.18785/jetde.1801.06

[63] X. Zhang, Y. Ding, X. Huang, W. Li, L. Long, and S. Ding, "Smart Classrooms: How Sensors and AI Are Shaping Educational Paradigms," *Sensors*, vol. 24, no. 17, pp. 1-33, 2024. https://doi.org/10.3390/S24175487

[64] N. Y. Dmitrenko, O. V. Voloshyna, S. S. Kizim, K. V. Mnyshenko, and S. V. Nahorniak, "Smart education in the prospective teachers' training," *CTE Workshop Proceedings,* vol. 10, pp. 414–429, 2023. https://doi.org/10.55056/cte.568

[65] L. Hirsto, S. Väisänen, E. Sointu, and T. Valtonen, "Learning Analytics in Supporting Teaching and Learning: Pedagogical Perspectives," In: Sampson, D.G., Ifenthaler, D., Isaias, P. (eds) *Smart Learning Environments in the Post Pandemic Era* (pp 3–17). Springer, 2024. https://doi.org/10.1007/978-3-031-54207-7_1

[66] M. Bellaj, A. Bendahmane, A. Younes, S. Boudra, and M. Ennakra, "A systematic review of smart campus technologies to improve students' educational experiences," *2024 Mediterranean Smart Cities Conference (MSCC),* Martil - Tetuan, Morocco, 02-04 May 2024, pp. 1-7. https://doi.org/10.1109/MSCC62288.2024.10697051

[67] A. E. Koshiry, and M. A. A. Tony, "Enabling smart education: An overview of innovations and challenges in modern learning," *International Journal of Innovative Research and Scientific Studies*, vol. 8, no. 2, pp. 3184–3200, 2025. https://doi.org/10.53894/ijirss.v8i2.5962

[68] P. Selvakumar, C. Hemalatha, I. Indumathy, S. Gandhimathi, and Mujra, P. "Smart education and sustainable learning environments," In *Advances in educational technologies and instructional design book series* (pp. 381–402), IGI Global, 2024. https://doi.org/10.4018/979-8-3693-7723-9.ch023

[69] J. M. Spector, and H. Kim, "Emerging Technologies in Education: A Review," *Journal of Educational Technology & Society*, vol. 22, no. 1, pp. 56–68, 2024. https://doi.org/10.13140/RG.2.2.32845.45285

[70] M. F. Contrino, M. Reyes-Millán, P. Vázquez-Villegas, and J. Membrillo-Hernández, "Using an adaptive learning tool to improve student performance and satisfaction in online and face-to-face education for a more personalized approach," *Smart Learning Environments*, vol. 11, no. 1, pp. 1–24, 2024. https://doi.org/10.1186/S40561-024-00292-Y/FIGURES/7

[71] E. Oskarita, and H. N. Arasy, "The Role of Digital Tools in Enhancing Collaborative Learning in Secondary Education," *International Journal of Educational Research*, vol. 1, no. 1, pp. 26–32, 2024. https://doi.org/10.62951/IJER.V1I1.15

[72] Tirado-Olivares, S., Cózar-Gutiérrez, R., González-Calero, J. A., and N. Dorotea, "Evaluating the Impact of Learning Management Systems in Geographical Education in Primary School: An Experimental Study on the Importance of Learning Analytics-Based Feedback," *Sustainability*, vol. 16, no. 7, pp. 1-16, 2024. https://doi.org/10.3390/SU16072616

[73] I. Nesterenko, "Major benefits of using smart technologies in education," *Scientific Bulletin of Mukachevo State University Series Pedagogy and Psychology,* vol. 9, no. 1, pp. 31-38, 2023. https://doi.org/10.52534/MSU-PP1.2023.31

[74] H. Uzunboylu, and N. Azhar, "Mobile learning as a new technology in education," *Global Journal of Information Technology: Emerging Technologies*, vol. 13, no. 1, pp. 07–16, 2023. https://doi.org/10.18844/GJIT.V13I1.8459

[75] D. Mhlanga, "Digital transformation of education, the limitations and prospects of introducing the fourth industrial revolution asynchronous online learning in emerging markets," *Discover Education*, vol. 3, no. 1, pp. 1–18, 2024. https://doi.org/10.1007/S44217-024-00115-9/FIGURES/9

[76] M. Bhatia, N. Meenakshi, P. Kaur, and A. Dhir, "Digital technologies and carbon neutrality goals: An in-depth investigation of drivers, barriers, and risk mitigation strategies," *Journal of Cleaner Production*, vol. 451, pp. 1-19, 2024. https://doi.org/10.1016/J.JCLEPRO.2024.141946

[77] F. Giannakas, C. Troussas, A. Krouska, I. Voyiatzis, and C. Sgouropoulou, "Blending cybersecurity education with IoT devices: A u-Learning scenario for introducing the man-in-the-middle attack," *Information Security Journal a Global Perspective,* vol. 32, no. 5, pp. 371–382, 2022. https://doi.org/10.1080/19393555.2022.2100297

[78] A. F. Otoom, W. Eleisah, and E. E. Abdallah, "Deep Learning for Accurate Detection of Brute Force attacks on IoT Networks," *Procedia Computer Science*, vol. 220, pp. 291–298, 2023. https://doi.org/10.1016/j.procs.2023.03.038

[79] H. El-Taj, D. Hamedah, and R. Saeed, "Artificial Intelligence and Advanced Cybersecurity to Mitigate Credential-Stuffing Attacks in the Banking Industry," *International Journal of Computational and Experimental Science and Engineering*, vol. 11, no. 1, pp. 935-948, 2025. https://doi.org/10.22399/ijcesen.754

[80] A. B. de Neira, B. Kantarci, and M. Nogueira, "Distributed denial of service attack prediction: Challenges, open issues and opportunities," *Computer Networks*, vol. 222, pp. 109553, 2023. https://doi.org/10.1016/J.COMNET.2022.109553

[81] R. A. de Souza, V. de C. Silva, S. B. Junior, and B. B. Zarpelão, "Forecasting Malware Incident Rates in Higher Education Institutions," *Lecture Notes on Data Engineering and Communications Technologies,* vol. 202, pp. 226–237, 2024. https://doi.org/10.1007/978-3-031-57916-5_20

[82] M. Sayduzzaman, J. T. Tamanna, D. Kundu, and T. Rahman, "Interoperability and explicable AI-based Zero-Day attacks detection process in Smart Community," *arXiv (Cornell University)*, pp. 1–7, 2024. https://doi.org/10.48550/arxiv.2408.02921

[83] F. A. Julianah, K. A. Boniface, O. Olumide, O. Otasowie, and I. O. Ayorinde, "Online Change of Grade Attack Using SQL Injection Case Study: FUTA Cyber Security Department," *The International Journal of Science & Technoledge*, vol. 1, no. 4, pp. 25-32, 2023. https://doi.org/10.24940/THEIJST/2023/V11/I4/ST2304-002

[84] D. Greco, "Security in E-Learning: A Systematic Review," *Lecture Notes in Electrical Engineering*, vol. 1369, pp. 457–465, 2025. https://doi.org/10.1007/978-3-031-84100-2_54

[85] G. Ali, M. M. Mijwil, I. Adamopoulos, B. A. Buruga, M. Gök, and M. Sallam, "Harnessing the Potential of Artificial Intelligence in Managing Viral Hepatitis," *Mesopotamian Journal of Big Data*, vol. 2024, pp. 128–163, 2024. https://doi.org/10.58496/MJBD/2024/010

[86] G. Ali, M. M. Mijwil, B. A. Buruga, M. Abotaleb, and I. Adamopoulos, "A Survey on Artificial Intelligence in Cybersecurity for Smart Agriculture: State-of-the-Art, Cyber Threats, Artificial Intelligence Applications, and Ethical Concerns," *Mesopotamian Journal of Computer Science*, vol. 2024, pp. 71–121, 2024. https://doi.org/10.58496/MJCSC/2024/007

[87] G. Ali, R. Wamusi, M. M. Mijwil, M. Sallam, J. Ayad, and I. Adamopoulos, "Securing the Internet of Wetland Things (IoWT) Using Machine and Deep Learning Methods: A Survey," *Mesopotamian Journal of Computer Science*, vol. 2025, pp. 17–63, 2025. https://doi.org/10.58496/mjcsc

[88] M. Ali, Y. Chen, and Q. Li, "Intelligent surveillance systems for smart campus security using deep learning," *IEEE Access*, vol. 12, pp. 108231–108245, 2024. https://doi.org/10.1109/ACCESS.2024.3306542

[89] G. Ali, M. M. Mijwil, I. Adamopoulos, and J. Ayad, "Leveraging the Internet of Things, Remote Sensing, and Artificial Intelligence for Sustainable Forest Management," *Babylonian Journal of Internet of Things*, vol. 2025, pp. 1–65, 2025. https://doi.org/10.58496/BJIoT/2025/001

[90] F. Naseer, M. N. Khan, M. Tahir, A. Addas, and S. H. Aejaz, "Integrating deep learning techniques for personalized learning pathways in higher education," *Heliyon*, vol. 10, no. 11, pp. 1–18, 2024. https://doi.org/10.1016/j.heliyon.2024.e32628

[91] T. Talaei Khoei, H. Ould Slimane, and N. Kaabouch, "Deep learning: systematic review, models, challenges, and research directions," *Neural Computing and Applications,* vol. 35, no. 31, pp. 23103–23124, 2023. https://doi.org/10.1007/s00521-023-08957-4

[92] W.-H. Choi, and J. Kim, "Unsupervised Learning Approach for Anomaly Detection in Industrial Control Systems," *Applied System Innovation,* vol. 7, no. 2, pp. 1-16, 2024. https://doi.org/10.3390/asi7020018

[93] P. Mavaie, L. Holder, and M. K. Skinner, "Hybrid deep learning approach to improve classification of low-volume high-dimensional data," *BMC Bioinformatics,* vol. 24, no. 1, pp. 1–20, 2023. https://doi.org/10.1186/S12859-023-05557-W/FIGURES/8

[94] G. Ali, S. Aziku, S. P. Kabiito, M. Zaward, T. Adebo, R. Wamusi, D. Asiku, M. Sallam, M. M. Mijwil, J. Ayad, A. O. Salau, and K. Dhoska, "Integration of Artificial Intelligence, Blockchain, and Quantum Cryptography for Securing the Industrial Internet of Things (IIoT): Recent Advancements and Future Trends," *Applied Data Science and Analysis*, vol. 2025, pp. 19–82, 2025. https://doi.org/10.58496/ADSA/2025/004

[95] M. M. Mijwil, I. E. Salem, and M. M. Ismaeel, "The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review," *Iraqi Journal for Computer Science and Mathematics,* vol. 4, no. 1, pp. 87-101, 2023. https://doi.org/10.52866/ijcsm.2023.01.01.008

[96] M. M. Taye, "Understanding of Machine Learning with Deep Learning: Architectures, Workflow, Applications and Future Directions," *Computers*, vol. 12, no. 5, pp. 1-26, 2023. https://doi.org/10.3390/COMPUTERS12050091

[97] A. Saberironaghi, J. Ren, and M. El-Gindy, "Defect Detection Methods for Industrial Products Using Deep Learning Techniques: A Review," *Algorithms*, vol. 16, no. 2, pp. 1-30, 2023. https://doi.org/10.3390/A16020095

[98] S. Vijayalakshmi, B. Madhavi, J. N, G. Bansode, N. Sharma, and S. KG, "Smart Education with IoT and AI: Revolutionizing Learning in the Digital Age," *2024 2nd International Conference on Disruptive Technologies (ICDT),* Greater Noida, India, 15-16 March 2024, pp. 1282–1286. https://doi.org/10.1109/icdt61202.2024.10489741

[99] Y. Pei, and G. Lu, "Design of an Intelligent Educational Evaluation System Using Deep Learning," *IEEE Access*, vol. 11, pp. 29790-29799, 2023. https://doi.org/10.1109/ACCESS.2023.3260979.

[100] L. Zheng, C. Wang, X. Chen, Y. Song, Z. Meng, and R. Zhang, "Evolutionary machine learning builds smart education big data platform: Data-driven higher education," *Applied Soft Computing*, vol. 136, pp. 110114, 2023. https://doi.org/10.1016/j.asoc.2023.110114.

[101] J. D. Pinto, and L. Paquette, "Deep learning for educational data science," *arXiv (Cornell University),* pp. 1–18, 2024. https://doi.org/10.48550/arxiv.2404.19675

[102] Y. Sun, W. Huang, Z. Wang, X. Xu, M. Wen, and P. Wu, "Smart Teaching Systems: A Hybrid Framework of Reinforced Learning and Deep Learning," *International Journal of Emerging Technologies in Learning (iJET),* vol. 18, no. 20, pp. 37–50, 2023. https://doi.org/10.3991/ijet.v18i20.44217

[103] C. H. Le, H. P. Ly, T. D. Nguyen, H. Dang-Ngoc, T. T. Vu, and D. N. M. Dang, "Deep Learning Based Attendance Check System At FPT University," *ICIIT '24: Proceedings of the 2024 9th International Conference on Intelligent Information Technology,* Ho Chi Minh, Vietnam, 23-25 February 2024, pp. 272–281. https://doi.org/10.1145/3654522.3654584

[104] X. Hu, "The role of deep learning in the innovation of smart classroom teaching mode under the background of internet of things and fuzzy control," *Heliyon*, vol. 9, no. 8, pp. 1–9, 2023. https://doi.org/10.1016/j.heliyon.2023.e18594

[105] M. Ozkan-Okay, S. Kosunalp, Ö. Aslan, I. Beloev, E. Akin, I. Stoyanov, and T. Iliev, "A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions," *IEEE Access*, vol. 12, pp. 12229-12256, 2024. https://doi.org/10.1109/ACCESS.2024.3355547.

[106] M. A. Al-Absi, H. R'Bigui, and A. A. Al-Absi, "Deep Learning and Machine Learning Algorithms Methods in Cyber Security," *Proceedings of 3rd International Conference on Smart Computing and Cyber Security,* Kyungdong University, Global Campus, South Korea, 5-6 December 2023, pp. 271–279. https://doi.org/10.1007/978-981-97-0573-3_22

[107] A. Deshmukh, and K. Ravulakollu, "An Efficient CNN-Based Intrusion Detection System for IoT: Use Case Towards Cybersecurity," *Technologies*, vol. 12, no. 10, pp. 1-21, 2024. https://doi.org/10.3390/TECHNOLOGIES12100203

[108] J. M. Kizza, "System Intrusion Detection and Prevention," In: *Guide to Computer Network Security. Texts in Computer Science* (pp 295–323). Springer, 2024. https://doi.org/10.1007/978-3-031-47549-8_13

[109] A. Mahboubi, K. Luong, H. Aboutorab, H. T. Bui, G. Jarrad, M. Bahutair, S. Camtepe, G. Pogrebna, E. Ahmed, B. Barry, and H. Gately, "Evolving techniques in cyber threat hunting: A systematic review," *Journal of Network and Computer Applications,* vol. 232, pp. 1-34, 2024. https://doi.org/10.1016/J.JNCA.2024.104004

[110] D. R. Ojha, "Use of Artificial Neural Networks to Detect and Prevent Cybersecurity Threats," *NPRC Journal of Multidisciplinary Research,* vol. 1, no. 6, pp. 132–141, 2024. https://doi.org/10.3126/NPRCJMR.V1I6.71754

[111] R. Singh, and R.L. Ujjwal, "Intrusion Detection and Prevention System for Smart IoT Network," In: Hasteer, N., McLoone, S., Sharma, P., Nallamalli, R. (eds) *Adaptive Intelligence. InCITe 2024. Lecture Notes in Electrical Engineering* (vol 1280, pp. 135–147). Springer, 2025. https://doi.org/10.1007/978-981-97-9045-6_12

[112] M. Nakıp, and E. Gelenbe, "Online Self-Supervised Deep Learning for Intrusion Detection Systems," *IEEE Transactions on Information Forensics and Security,* vol. 19, pp. 5668–5683, 2024. https://doi.org/10.1109/tifs.2024.3402148

[113] P. S. Nguyen, T. N. Huy, T. A. Tuan, P. D. Trung, and H. V. Long, "Hybrid feature extraction and integrated deep learning for cloud-based malware detection," *Computers & Security*, vol. 150, pp. 104233, 2025. https://doi.org/10.1016/J.COSE.2024.104233

[114] A. Bensaoud, J. Kalita, and M. Bensaoud, "A survey of malware detection using deep learning. Machine Learning with Applications," *Machine Learning with Applications,* vol. 16, pp. 1-16, 2024. https://doi.org/10.1016/J.MLWA.2024.100546

[115] Z. Çıplak, K. Yıldız, and Ş. Altınkaya, "FEDetect: A Federated Learning-Based Malware Detection and Classification Using Deep Neural Network Algorithms," *Arabian Journal for Science and Engineering,* pp. 1–28, 2025. https://doi.org/10.1007/S13369-025-10043-X/TABLES/11

[116] A. Alzahrani, "An Optimized Approach to Deep Learning for Botnet Detection and Classification for Cybersecurity in Internet of Things Environment," *Computers, Materials and Continua,* vol. 80, no, 2, pp. 2331–2349, 2024. https://doi.org/10.32604/CMC.2024.052804

[117] R. Jain, and N. Nihalani, "Botnet Detection in Distributed Network Using Machine Learning- A Detailed Review," *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE),* Gautam Buddha Nagar, India, 09-11 May 2024, pp. 888–895. https://doi.org/10.1109/IC3SE62002.2024.10593476

[118] E. H. Tusher, M. A. Ismail, M. A. Rahman, A. H. Alenezi, and M. Uddin, "Email Spam: A Comprehensive Review of Optimize Detection Methods, Challenges, and Open Research Problems," *IEEE Access,* vol. 12, pp. 143627-143657, 2024. https://doi.org/10.1109/ACCESS.2024.3467996

[119] D. Denysiuk, T. Sochor, M. Kapustian, A. Kashtalian, and A. Drozd, "A method for detecting botnets in IT infrastructure using a neural network," *CEUR Workshop Proceedings*, vol. 3736, pp. 282–292, 2024.

[120] G. Suchetha, and K. Pushpalatha, "A GRU-based approach for botnet detection using deep learning technique," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 38, no. 2, pp. 1098-1105, 2025. https://doi.org/10.11591/IJEECS.V38.I2.PP1098-1105

[121] S. Komakula, and M. Jagadeeshwar, "An Exploration of Deep Learning Algorithm for Fraud Detection using Spark Platform," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 18s, pp. 324–332, 2024. https://www.ijisae.org/index.php/IJISAE/article/view/4976

[122] H. Wang, J. Zheng, I. E. Carvajal-Roca, L. Chen, and M. Bai, "Financial Fraud Detection Based on Deep Learning: Towards Large-Scale Pre-training Transformer Models," *Communications in Computer and Information Science,* vol. 1923 CCIS, pp. 163–177, 2023. https://doi.org/10.1007/978-981-99-7224-1_13

[123] F. A. Nama, and A. J. Obaid, "Financial Fraud Identification Using Deep Learning Techniques," *Al-Salam Journal for Engineering and Technology,* vol. 3, no. 1, pp. 141–147, 2024. https://doi.org/10.55145/ajest.2024.03.01.012

[124] A. Gandhar, K. Gupta, A. K. Pandey, and D. Raj, "Fraud Detection Using Machine Learning and Deep Learning," *SN Computer Science,* vol. 5, no. 5, pp. 1–10, 2024. https://doi.org/10.1007/S42979-024-02772-X/METRICS

[125] J. S. Shyam Mohan, M. Thirunavukkarasu, N. Kumaran, and D. Thamaraiselvi, "Deep learning with blockchain based cyber security threat intelligence and situational awareness system for intrusion alert prediction," *Sustainable Computing: Informatics and Systems,* vol. 42, pp. 100955, 2024. https://doi.org/10.1016/J.SUSCOM.2023.100955

[126] A. Imeri, and O. Rysavy, "Deep learning for predictive alerting and cyber-attack mitigation," *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC),* Las Vegas, NV, USA, 08-11 March 2023, pp. 476–481. https://doi.org/10.1109/CCWC57344.2023.10099209

[127] P. Abichandani, C. Iaboni, D. Lobo, and T. Kelly, "Artificial intelligence and computer vision education: Codifying student learning gains and attitudes," *Computers and Education Artificial Intelligence*, vol. 5, pp. 1–11, 2023. https://doi.org/10.1016/j.caeai.2023.100159

[128] C. Che, H. Zheng, Z. Huang, W. Jiang, and B. Liu, "Intelligent robotic control system based on computer vision technology," *Applied and Computational Engineering,* vol. 64, no. 1, pp. 142–147, 2024. https://doi.org/10.54254/2755-2721/64/20241373

[129] J. D. Blair, K. M. Gaynor, M. S. Palmer, and K. E. Marshall, "A gentle introduction to computer vision-based specimen classification in ecological datasets," *Journal of Animal Ecology,* vol. 93, no. 2, pp. 147–158, 2024. https://doi.org/10.1111/1365-2656.14042

[130] A. Upadhyay, N. S. Chandel, K. P. Singh, S. K. Chakraborty, B. M. Nandede, M. Kumar, A. Subeesh, K. Upendar, A. Salem, and A. Elbeltagi, "Deep learning and computer vision in plant disease detection: a comprehensive review of techniques, models, and trends in precision agriculture," *Artificial Intelligence Review,* vol. 58, no. 3, pp. 1–64, 2025. https://doi.org/10.1007/S10462-024-11100-X

[131] C. Li, L. Wang, Q. Li, and D. Wang, "Intelligent Analysis System for Teaching and Learning Cognitive Engagement Based on Computer Vision in an Immersive Virtual Reality Environment," *Applied Sciences,* vol. 14, no. 8, pp. 1-20, 2024. https://doi.org/10.3390/app14083149.

[132] P. Yadav, N. Gupta, and P. K. Sharma, "A comprehensive study towards high-level approaches for weapon detection using classical machine learning and deep learning methods," *Expert Systems with Applications,* vol. 212, pp. 118698, 2023. https://doi.org/10.1016/j.eswa.2022.118698

[133] L. Zou, "Meta-learning for computer vision," *Meta-Learning,* pp. 91–208, 2023. https://doi.org/10.1016/B978-0-323-89931-4.00012-2

[134] Y. Cong, "The Application of Improved Scale Invariant Feature Transformation Algorithm in Facial Recognition," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 3, pp. 490-499, 2024. https://doi.org/10.14569/IJACSA.2024.0150350

[135] T. J. Nandhini, and K. Thinakaran, "SIFT algorithm-based Object detection and tracking in the video image," *2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT),* Erode, India, 22-24 February 2023, pp. 1-4. https://doi.org/10.1109/ICECCT56650.2023.10179720

[136] S. Verma, and A. Rao, "A short report on deep learning synergy for decentralized smart grid cybersecurity," *Frontiers in artificial intelligence,* vol. 8, pp. 1-4, 2025. https://doi.org/10.3389/frai.2025.1557960

[137] H. Anzid, G. le Goic, A. Bekkari, A. Mansouri, and D. Mammass, "A new SURF-based algorithm for robust registration of multimodal images data," *Visual Computer,* vol. 39, no. 4, pp. 1667–1681, 2023. https://doi.org/10.1007/S00371-022-02435-Z/METRICS

[138] J. Fan, X. Yang, R. Lu, W. Li, and Y. Huang, "Long-term visual tracking algorithm for UAVs based on kernel correlation filtering and SURF features," *Visual Computer,* vol. 39, no. 1, pp. 319–333, 2023. https://doi.org/10.1007/S00371-021-02331-Y/METRICS

[139] J. Gu, G. Liu, Q. Yang, and S. S. Law, "Improved SURF method in digital image correlation for estimation of large rotation angle," *Measurement,* vol. 207, pp. 112372, 2023. https://doi.org/10.1016/J.MEASUREMENT.2022.112372

[140] C. H. Choi, J. Han, J. Cha, J. Shin, and H. W. Oh, "Fast Object Detection Algorithm using Edge-based Operation Skip Scheme with Viola-Jones Method," *2024 IEEE 6th International Conference on AI Circuits and Systems (AICAS),* Abu Dhabi, United Arab, 22-25 April 2024, pp. 199–203. https://doi.org/10.1109/AICAS59952.2024.10595932

[141] Q. Abbas, T. S. Albalawi, G. Perumal, and M. E. Celebi, "Automatic Face Recognition System Using Deep Convolutional Mixer Architecture and AdaBoost Classifier," *Applied Sciences,* vol. 13, no. 17, pp. 1-31, 2023. https://doi.org/10.3390/APP13179880

[142] J. Bian, J. Wang, and Q. Yece, "A novel study on power consumption of an HVAC system using CatBoost and AdaBoost algorithms combined with the metaheuristic algorithms," *Energy*, vol. 302, pp. 131841, 2024. https://doi.org/10.1016/J.ENERGY.2024.131841

[143] A. Sinha, and S. Barde, "Multi invariant face detection via Viola Jones algorithm," *European Chemical Bulletin,* vol. 12, no. 1, pp. 24-32, 2023. https://doi.org/10.31838/ecb/2023.12.s1.003

[144] B. Siregar, I. Setiawan, S. Efendi, and J. Susilo, "Identity recognition of people through face image using principal component analysis," *AIP Conference Proceedings,* vol. 2623, no. 1, pp. 050008, 2023. https://doi.org/10.1063/5.0130970/2907840

[145] P. B. Khatkale, "Iris Recognition Using Principal Component Analysis," *AIP Conference Proceedings*, vol. 3175, no. 1, pp. 020088, 2025. https://doi.org/10.1063/5.0254223/3339038

[146] J. Huang, and D. Zhou, "A scalable real-time computer vision system for student posture detection in smart classrooms," *Education and Information Technologies,* vol. 29, pp. 917-937, 2023. https://doi.org/10.1007/s10639-023-12365-5.

[147] Y. Yang, "Design and Integration of Intelligent Classroom for Preschool Education Majors Based on Computer Visual Recognition Technology Computer," *Journal of Electrical Systems,* vol. 20, no. 6, pp. 638-649, 2024. https://doi.org/10.52783/jes.2718.

[148] A. Asma, R. Mohammed, A. Ahmed, and M. Jaber, "Artificial Intelligence based Computer Vision Analysis for Smart Education Interactive Visualization," *Fusion: Practice and Applications,* vol. 15, no. 2, pp. 245-260, 2024. https://doi.org/10.54216/fpa.150221.

[149] I. Abbo, and N. D. Tchomte, "Feature engineering and computer vision for cybersecurity," In *Advances in information security, privacy, and ethics book series* (pp. 155–174). IGI Global, 2024. https://doi.org/10.4018/978-1-6684-8127-1.ch006

[150] V. Upadhyaya, "Advancements in Computer Vision for Biometrics Enhancing Security and Identification," *Leveraging Computer Vision to Biometric Applications*, pp. 260–292, 2024. https://doi.org/10.1201/9781032614663-14/advancements-computer-vision-biometrics-enhancing-security-identification-vivek-upadhyaya

[151] M. Leo, Z.-M. Lu, M. Trigka, and E. Dritsas, "A Comprehensive Survey of Machine Learning Techniques and Models for Object Detection, *Sensors*, vol. 25, no. 1, pp. 1-32, 2025. https://doi.org/10.3390/S25010214

[152] C. C. Lin, A. Y. Q. Huang, and O. H. T. Lu, "Artificial intelligence in intelligent tutoring systems toward sustainable education: a systematic review," *Smart Learning Environments,* vol. 10, no. 1, pp. 1-22, 2023. https://doi.org/10.1186/S40561-023-00260-Y

[153] H. Jiang, and W. Fu, "Computer vision recognition in the teaching classroom: A Review," *EAI Endorsed Transactions on AI and Robotics,* vol. 3, pp. 1–8, 2024. https://doi.org/10.4108/airo.4079

[154] A. Letaifa, T. Abar, and E. Asmi, "QOE-based intelligent intrusion detection Use case: University video surveillance," *2022 IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT),* pp. 7-11, 2022. https://doi.org/10.1109/SETIT54465.2022.9875657.

[155] I. Kandhro, S. Alanazi, S. Karuppayah, M. Uddin, F. Ali, A. Kehar, and K. Fatima, "Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures," *IEEE Access,* vol. 11, pp. 9136-9148, 2023. https://doi.org/10.1109/ACCESS.2023.3238664.

[156] M. Gu, T. Zhou, H. Zhang, M. Yuan, Y. Liu, and F. Zhou, "Niect: A Model for Intrusion Security Detection Applied to Campus Video Surveillance Edge Networks," *2024 IEEE 11th International Conference on Cyber Security and Cloud Computing (CSCloud),* Shanghai, China, 28-30 June 2024, pp. 24-29. https://doi.org/10.1109/CSCloud62866.2024.00012.

[157] M. Meghana, C. Sivakumar, Y. Sukumar, P. Reddy, and T. Vali, "AI-Powered Video Surveillance for Enhanced Intrusion Detection," *2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS),* Bengaluru, India, 17-18 December 2024, pp. 1630-1634. https://doi.org/10.1109/ICICNIS64247.2024.10823272.

[158] K. Guleria, A. Kumar, D. Upadhyay, and R. Chauhan, "Real-time Threat Monitoring: Utilizing IoT Data for Intrusion Detection in Smart Environments," *2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT),* Kollam, India, 08-09 August 2024, pp. 1566-1570. https://doi.org/10.1109/ICCPCT61902.2024.10673332.

[159] K. Roshan, and A. Zafar, "Ensemble adaptive online machine learning in data stream: a case study in cyber intrusion detection system," *International Journal of Information Technology,* vol. 16, no. 8, pp. 5099–5112, 2024. https://doi.org/10.1007/s41870-024-01727-y

[160] S. Gode, J. Nikhal, A. Singh, R. Khandekar, and D. Athawle, "Facial Recognition & Authentication in E-Learning Portal," *International Journal of Scientific Research in Engineering and Management (IJSREM),* vol. 9, no. 4, pp. 1-8, 2025. https://doi.org/10.55041/ijsrem43915.

[161] R. Juanatas, and X. Jing, "Intelligent campus access management system using facial recognition technology," *2023 2nd International Conference on Image Processing and Media Computing (ICIPMC),* Xi'an, China, 26-28 May 2023, pp. 52-57. https://doi.org/10.1109/ICIPMC58929.2023.00016.

[162] K. Liu, and Y. Zhu, "An Intelligent Access Control Recognition Framework Based on Asian Face Data Augmentation and Edge Computing Optimization in Private University Campuses," *2024 4th International Signal Processing, Communications and Engineering Management Conference (ISPCEM),* Montreal, QC, Canada, 28-30 November 2024, pp. 518-522. https://doi.org/10.1109/ISPCEM64498.2024.00093.

[163] D. Faiza, G. Farell, V. I. Delianti, Thamrin, S. Anori and R. Wahyudi, "Implementation and Evaluation of a Biometric Face Recognition System for Authentication in Digital Learning," *2024 International Conference on ICT for Smart Society (ICISS),* Bandung, Indonesia, 04-05 September 2024, pp. 1-5, doi: 10.1109/ICISS62896.2024.10751544.

[164] Q. Liu, X. Jiang, and R. Jiang, "Classroom Behavior Recognition Using Computer Vision: A Systematic Review," *Sensors*, vol. 25, no. 2, pp. 1-22, 2025. https://doi.org/10.3390/s25020373

[165] N. S. Auti, N. P. Darade, N. A. Munje, N. N. Patil, and N. P. A. Khushwaha, "Deep Learning Approach For Suspicious Activity Detection from Surveillance Video in Examination Hall," *International Journal of Advanced Research in Science Communication and Technology*, vol. 5, no. 2, pp. 627–635, 2025. https://doi.org/10.48175/ijarsct-23073

[166] L. Ren, S. Li and C. Chen, "Student Classroom Behavior Detection Method Based on Deep Learning," *2024 4th International Symposium on Computer Technology and Information Science (ISCTIS),* Xi'an, China, 12-14 July 2024, pp. 104-109, doi: 10.1109/ISCTIS63324.2024.10699088.

[167] R. Golande, R. Bhapkar, A. Nalawade, A. Rashinkar, and S. Mane, "Weapon Detection System: Real-Time object recognition for threat detection," *International Journal for Research in Applied Science and Engineering Technology,* vol. 13, no. 3, pp. 3514–3521, 2025. https://doi.org/10.22214/ijraset.2025.68105

[168] M. Talib, and J. H. Saud, "A Multi-Weapon detection using deep learning," *Iraqi Journal of Information & Communications Technology,* vol. 7, no. 1, pp. 11–22, 2024. https://doi.org/10.31987/ijict.7.1.242

[169] T. Santos, H. Oliveira, and A. Cunha, "Systematic review on weapon detection in surveillance footage through deep learning," *Computer Science Review*, vol. 51, pp. 100612, 2023. https://doi.org/10.1016/j.cosrev.2023.100612

[170] S. Hemavathi, and R. Chakravarthi, "AI-Powered Security and Attendance Management System Using Deep Learning and Facial Recognition," *Journal of Information Systems Engineering and Management,* vol. 10, no. 35s, pp. 372-381, 2025. https://doi.org/10.52783/jisem.v10i35s.6013.

[171] A. Z. Lari, F. Khan, A. Ahmad, A. A. Raza, and M. Suaib, "An Efficient Attendance Management System for College Environments Using Machine Learning Facial Recognition Technology", *International Journal of Innovative Research in Engineering & Management (IJIRCST),* vol. 13, no. 3, pp. 8-12, 2025. https://doi.org/10.55524/ijircst.2025.13.3.2

[172] G. A. Senthil, S. Geerthik, R. Karthikeyan and G. Keerthana, "Face Recognition based Automated Smart Attendance using Hybrid Machine Learning Algorithms and Computer Vision," *2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC),* Salem, India, 05-07 June 2024, pp. 606-611, doi: 10.1109/ICAAIC60222.2024.10574896.

[173] M. Thalor, and O. Gaikwad, "Facial Recognition Attendance Monitoring System using Deep Learning Techniques," *International Journal of Integrated Science and Technology,* vol. 2, no. 1, pp. 45-52, 2024. https://doi.org/10.59890/ijist.v1i6.685.

[174] A. Singh, A. Kalra, R. Teotia, and S. Mamgain, "Smart Campus: Smart Attendance Management System using Face Recognition," *International Journal for Multidisciplinary Research (IJFMR),* vol. 6, no. 2, pp. 1-11, 2024. https://doi.org/10.36948/ijfmr.2024.v06i02.17655.

[175] S. Ali, Q. Xu, and T. Yue, "Digital Twin-based Anomaly Detection with Curriculum Learning in Cyber-physical Systems," *ACM Transactions on Software Engineering and Methodology,* vol. 32, pp. 1 – 32, 2023. https://doi.org/10.1145/3582571.

[176] Lv, Z., Chen, D., Song, H., Cao, B., & Lv, H. "Secure Deep Learning in Defense in Deep-Learning-as-a-Service Computing Systems in Digital Twins," *IEEE Transactions on Computers,* vol. 73, pp. 656-668, 2024. https://doi.org/10.1109/TC.2021.3077687.

[177] C. Lo, T. Y. Win, Z. Rezaeifar, Z. Khan, and P. Legg, "Digital Twins of Cyber Physical Systems in Smart Manufacturing for Threat Simulation and Detection with Deep Learning for Time Series Classification," *2024 27th International Conference on Automation and Computing (ICAC),* Sunderland, United Kingdom, 28-30 August 2024, pp. 1–6. https://doi.org/10.1109/icac61394.2024.10718749

[178] S. Martha, V. Kumar, S. Gaba, M. Abouhawwash, I. Budhiraja, J. Khurmi, A. Singh, S. Askar, and K. Singh, "A Systematic Analysis of Enhancing Cyber Security Using Deep Learning for Cyber Physical Systems," *IEEE Access,* vol. 12, pp. 6017-6035, 2024. https://doi.org/10.1109/ACCESS.2023.3349022.

[179] Q. Liu, and T. Zhang, "Deep learning technology of computer network security detection based on artificial intelligence," *Computers and Electrical Engineering,* vol. 110, pp. 108813, 2023. https://doi.org/10.1016/j.compeleceng.2023.108813.

[180] A.V. Geetha, T. Mala, D. Priyanka, and E. Uma, "Multimodal Emotion Recognition with Deep Learning: Advancements, challenges, and future directions," *Information Fusion*, vol. 105, pp. 102218, 2023. https://doi.org/10.1016/j.inffus.2023.102218.

[181] S. Zhang, Y. Yang, C. Chen, X. Zhang, Q. Leng, and X. Zhao, "Deep learning-based multimodal emotion recognition from audio, visual, and text modalities: A systematic review of recent advancements and future prospects," *Expert Systems with Applications,* vol. 237, pp. 121692, 2023. https://doi.org/10.1016/j.eswa.2023.121692.

[182] R. Pereira, C. Mendes, J. Ribeiro, R. Ribeiro, R. Miragaia, N. Rodrigues, N. Costa, and A. Pereira, "Systematic Review of Emotion Detection with Computer Vision and Deep Learning," *Sensors,* vol. 24, no. 11, pp. 1-29, 2024. https://doi.org/10.3390/s24113484

[183] S. Wang, Z. Pu, Q. Li, and Y. Wang, "Estimating crowd density with edge intelligence based on lightweight convolutional neural networks," *Expert Systems with Applications,* vol. 206, pp. 117823, 2022. https://doi.org/10.1016/j.eswa.2022.117823.

[184] S. R. Alotaibi, H. A. Mengash, M. Maray, F. A. Alotaibi, A. Alkharashi, A. A. Alzahrani, M. Alotaibi, and M. M. Alnfiai, "Integrating Explainable Artificial Intelligence with Advanced Deep Learning Model for Crowd Density Estimation in Real-world Surveillance Systems," *IEEE Access,* vol. 13, pp. 20750–20762, 2025. https://doi.org/10.1109/access.2025.3529843

[185] S. Huang, J. Ji, Y. Wang, W. Li, and Y. Zheng, "A machine vision-based method for crowd density estimation and evacuation simulation," *Safety Science,* vol. 167, pp. 106285, 2023. https://doi.org/10.1016/j.ssci.2023.106285

[186] C. Yi and J. Cho, "Robust Estimation of Crowd Density Using Vision Transformers," *International Journal on Advanced Science, Engineering and Information Technology,* vol. 14, no. 5, pp. 1528–1533, 2024. https://doi.org/10.18517/ijaseit.14.5.11267.

[187] J. H. Lee, and S. J. You, "Balancing Privacy and accuracy: Exploring the impact of data anonymization on deep learning models in computer vision," *IEEE Access*, vol. 12, pp. 8346–8358, 2024. https://doi.org/10.1109/access.2024.3352146

[188] N. J. N. Chukwunweike, N. M. Yussuf, N. O. Okusi, N. T. O. Bakare, and N. A. J. Abisola, "The role of deep learning in ensuring privacy integrity and security: Applications in AI-driven cybersecurity solutions," *World Journal of Advanced Research and Reviews*, vol. 23, no. 2, pp. 1778–1790, 2024. https://doi.org/10.30574/wjarr.2024.23.2.2550

[189] M. R. Naeem, R. Amin, M. Farhan, F. A. Alotaibi, M. M. Alnfiai, G. A. Sampedro, and V. Karovič, "Harnessing AI and analytics to enhance cybersecurity and privacy for collective intelligence systems," *PeerJ Computer Science*, vol. 10, pp. e2264, 2024. https://doi.org/10.7717/peerj-cs.2264

[190] Y. Zhang, L. Zhou, and J. Li, "Biometric authentication using deep learning for secure smart campus access," *Sensors*, vol. 22, no. 18, pp. 6813, 2022. https://doi.org/10.3390/s22186813

[191] L. Chen, and Z. Wang, "A deep learning approach for anomaly detection in educational network traffic," *Computers & Security*, vol. 131, pp. 103284, 2023. https://doi.org/10.1016/j.cose.2023.103284

[192] M. A. Hossain, and S. Roy, "Continuous authentication in smart learning environments using behavioral biometrics and deep learning," *Journal of Network and Computer Applications,* vol. 235, pp. 103763, 2024. https://doi.org/10.1016/j.jnca.2024.103763

[193] F. Rahman, S. Ahmed, and N. Jahan, "Deepfake detection using hybrid deep learning models: A case study for educational cybersecurity," *IEEE Access,* vol. 11, pp. 93721–93733, 2023. https://doi.org/10.1109/ACCESS.2023.3303455

[194] V. Patel, and A. Gupta, "PhishNet: A deep learning-based phishing email detection framework for educational institutions," *Future Generation Computer Systems,* vol. 134, pp. 149–160, 2022. https://doi.org/10.1016/j.future.2022.04.003

[195] T. T. Nguyen, N. H. Vo, and M. N. Tran, "Privacy-preserving edge AI for smart classroom video analytics," *IEEE Transactions on Industrial Informatics,* vol. 19, no. 2, pp. 1673–1681, 2023. https://doi.org/10.1109/TII.2023.3245568

[196] J. Lee, H. Park, and D. Kim, "Access control in IoT-enabled smart classrooms using computer vision and deep learning," *IEEE Internet of Things Journal,* vol. 12, no. 6, pp. 4567–4576, 2025. https://doi.org/10.1109/JIOT.2025.3337105

[197] P. Singh, V. Sharma, and J. Kaur, "Defense against adversarial attacks in smart education systems using robust deep learning models," *Neural Computing and Applications,* vol. 35, no. 15, pp. 11457–11470, 2023. https://doi.org/10.1007/s00521-022-07736-9

[198] L. Huang, "Ethics of Artificial Intelligence in Education: Student Privacy and Data Protection," *Science Insights Education Frontiers,* vol. 16, no. 2, pp. 2577–2587, 2023. https://doi.org/10.15354/sief.23.re202

[199] L. Alzubaidi, J. Bai, A. Al-Sabaawi, J. Santamaría, A. S. Albahri, B. S. N. Al-dabbagh, M. A. Fadhel, M. Manoufali, J. Zhang, A. H. Al-Timemy, Y. Duan, A. Abdullah, L. Farhan, Y. Lu, A. Gupta, F. Albu, A. Abbosh, and Y. Gu, "A survey on deep learning tools dealing with data scarcity: definitions, challenges, solutions, tips, and applications," *Journal of Big Data,* vol. 10, no. 1, pp. 1–82, 2023. https://doi.org/10.1186/S40537-023-00727-2

[200] Z. Zhao, L. Alzubaidi, J. Zhang, Y. Duan, and Y. Gu, "A comparison review of transfer learning and self-supervised learning: Definitions, applications, advantages and limitations," *Expert Systems with Applications,* vol. 242, pp. 122807, 2024. https://doi.org/10.1016/J.ESWA.2023.122807

[201] L. Tukaram, "Deep Learning in Cybersecurity: Applications, Challenges, and Future Prospects," *International Journal of Innovations in Science Engineering and Management,* vol. 4, no. 2, pp. 27–33, 2025. https://doi.org/10.69968/ijisem.2025v4i227-33.

[202] N. Kumar, B. Muniandi, E. Sibonghanoy Groenewald, P. Gawande, S. Dhar, G. Chandra Saha, and A. Professor, "Enhancing Robustness and Generalization in Deep Learning Models for Image Processing," *Power System Technology,* vol. 47, no. 4, pp. 278–293, 2023. https://doi.org/10.52783/PST.193