EDITOR
Prof. Dr. Nezih ÖNAL

Research and
Evaluations in the Field of

COMPUTER AND EDUCATIONAL TECHNOLOGIES EDUCATION

June 2025

Privilege Holder • Yaşar Hız
Editor-in-chief • Eda Altunel
Prepared for Publication • Gece Kitaplığı
Editor • Prof. Dr. Nezih ÖNAL

First Edition • June 2025 / ANKARA

ISBN • 978-625-388-436-9

Gece Kitaplığı
Adress: Kızılay Mah. Fevzi Çakmak 1. Sokak Ümit Apt
No: 22/A Çankaya/ANKARA Tel: 0312 384 80 40

www.gecekitapligi.com
gecekitapligi@gmail.com

Printing and Binding
Bizim Buro
Certificate No: 42488

Research And Evaluations In The Field Of Computer And Educational Technologies Education

June 2025

Editor:
Prof. Dr. Nezih ÖNAL

CONTENTS

CHAPTER 1

SMART CLASSROOMS: THE MEETING POINT OF TECHNOLOGY AND TEACHING IN THE DIGITAL AGE

Mehmet Can ŞAHİN[1]

1 Dr. Mehmet Can ŞAHİN, (Çukurova University, Faculty of Education, Department of Computer Education and Instructional Technology), mcsahin@cu.edu.tr, ORCID: 0000-0002-3687-600X

1. Introduction

The rapid advancement of digital technologies has irrevocably transformed numerous sectors, with education standing as a prominent domain undergoing profound metamorphosis. At the heart of this educational revolution lies the concept of the 'smart classroom,' an environment where the confluence of technology and pedagogy aims to create more engaging, personalized, and effective learning experiences (Al-Emran et al., 2018; Hwang et al., 2017; Saini & Goel, 2019; Timms, 2016; Zhu et al., 2016). Smart classrooms are typically characterized by the integration of various advanced technologies, including the Internet of Things (IoT), artificial intelligence (AI), interactive displays, mobile devices, and sophisticated learning management systems. These technologies are not merely augmentations to traditional teaching methods but are intended to foster a dynamic learning ecosystem that is responsive to the diverse needs of 21st-century learners. The core premise of a smart classroom revolves around leveraging these technological affordances to move beyond conventional didactic approaches towards more student-centric, interactive, and data-driven instructional strategies (Al-Emran et al., 2018; Saini & Goel, 2019; Timms, 2016; Zhu et al., 2016).

The significance of smart classrooms in the contemporary educational landscape cannot be overstated, particularly as institutions grapple with the demands of preparing students for a future increasingly shaped by digital innovation and complex global challenges. These technologically enriched environments hold the promise of revolutionizing teaching methodologies by enabling personalized learning pathways, fostering greater student engagement and motivation, and facilitating collaborative knowledge construction (Gros, 2016; Li et al., 2015; Mircea & Andreescu, 2011; Peng et al., 2019; Wanner & Palmer, 2015). For instance, adaptive learning systems can tailor educational content to individual student paces and preferences, while interactive tools can transform passive information consumption into active exploration and critical thinking. However, the proliferation of smart classrooms is not without its complexities. The journey towards realizing their full potential is paved with a spectrum of emerging challenges that span technological, pedagogical, ethical, and financial domains. These include issues such as ensuring equitable access, addressing data privacy and security concerns, the imperative for robust teacher training and professional development, and the substantial investment required for infrastructure and maintenance (Gros, 2016; Li et al., 2015; Peng et al., 2019; Wanner & Palmer, 2015). Therefore, a critical examination of both the opportunities and the attendant challenges is essential for navigating the evolving terrain of smart education effectively.

This chapter aims to provide a comprehensive theoretical review of the emerging challenges and opportunities associated with smart classrooms. It seeks to synthesize existing literature to offer a nuanced understanding of how these technologically advanced learning environments are reshaping the educational landscape. The central thesis of this chapter posits that while smart classrooms offer transformative potential for enhancing teaching and learning, their successful and ethical implementation hinges upon a proactive and holistic approach that addresses the multifaceted challenges they present. By critically evaluating these dimensions, this chapter endeavors to contribute to a more informed discourse on the future trajectory of smart education.

The subsequent sections of this chapter are structured to systematically explore this topic. Section two, the Theoretical Framework, will delve into the relevant theories and conceptual models that underpin the understanding of smart classrooms, their adoption, and their impact on educational processes. This will include discussions on foundational learning theories, technology acceptance models, and frameworks specific to smart learning environments. Section three will present an in-depth Literature Review, analyzing and synthesizing existing research on the specific opportunities—such as personalized learning and enhanced engagement—and the diverse challenges—including technological hurdles, pedagogical shifts, and ethical considerations—related to smart classrooms. This section will also identify key debates and gaps within the current body of literature. Following this, section four, Future Directions, will propose areas for future research and discuss potential methodological approaches to address the identified gaps and emerging trends in the field. Finally, the Conclusion will summarize the key arguments and findings of the chapter, reiterating the significance of a balanced perspective on the challenges and opportunities of smart classrooms and offering insights into the path forward for educators, policymakers, and researchers in harnessing the potential of these innovative learning environments (Ally & Prieto-Blázquez, 2014; Bond et al., 2020; Major et al., 2021; Sailer & Homner, 2020; Tawalbeh et al., 2016).

2. Theoretical Framework

The emergence and evolution of smart classrooms are not isolated technological phenomena but are deeply intertwined with various theoretical underpinnings that seek to explain how learning occurs, how technology is adopted, and how educational environments can be optimally designed. Understanding these theoretical frameworks is crucial for critically analyzing the opportunities and challenges presented by smart classrooms and for guiding their effective implementation. This section will explore foundational learning theories, models of technology acceptance, and conceptual frameworks specific to smart learning environments, illustrating how they collectively inform the discourse on technology-enhanced education.

2.1. Foundational Learning Theories in the Context of Smart Classrooms

Several learning theories provide a lens through which the pedagogical potential of smart classrooms can be understood. **Constructivism**, for instance, posits that learners actively construct their own knowledge and understanding through experiences and interactions rather than passively receiving information (Wanner & Palmer, 2015). Smart classrooms, with their interactive tools and collaborative platforms, can create rich environments for constructivist learning by enabling students to explore, experiment, and co-create knowledge (Peng et al., 2019). Features like virtual laboratories, simulation software, and project-based learning modules facilitated by smart technologies align well with constructivist principles, encouraging active student participation and deeper conceptual understanding (Vesin et al., 2018; Yadav & Oyelere, 2021). For example, the flipped classroom model, often implemented in smart settings, requires students to engage with instructional content independently before class, using class time for interactive problem-solving and discussion, a practice rooted in constructivist ideals (Wanner & Palmer, 2015).

Connectivism, a more recent theory, emphasizes the importance of connections and networks in the learning process, particularly in a digital age where knowledge is distributed and constantly evolving (Chen et al., 2014). Smart classrooms can embody connectivist principles by providing access to vast networks of information and facilitating communication and collaboration among learners and with external experts (Bower, 2016). Learning analytics, a key component of many smart classroom systems, can help map and understand these connections, providing insights into how students navigate and utilize networked resources (Chen et al., 2014; Peng et al., 2019). The ability to personalize learning paths based on these connections and interactions is a hallmark of connectivist-informed smart learning environments.

Socio-cultural learning theories, stemming from Vygotsky's work, highlight the social nature of learning and the role of cultural context and interaction in cognitive development (Dimitriadou et al., 2023). Smart classrooms can support socio-cultural learning by providing tools for collaborative projects, peer-to-peer learning, and communication that transcends geographical boundaries (Yadav & Oyelere, 2021). However, the design and implementation of these tools must be sensitive to diverse socio-cultural contexts to ensure equitable participation and avoid reinforcing existing inequalities, a particular concern in regions like Sub-Saharan Africa where infrastructure and pedagogical adaptation present unique challenges (Dimitriadou et al., 2023). The integration of technologies like augmented reality (AR) can also offer situated learning experiences that are culturally relevant and promote shared understanding within a community of learners (Vesin et al., 2018).

2.2. Technology Acceptance Models (TAM) and Unified Theory of Acceptance and Use of Technology (UTAUT)

The successful integration of smart classroom technologies depends significantly on their acceptance and use by both educators and students. The **Technology Acceptance Model (TAM)** and its extensions, such as the **Unified Theory of Acceptance and Use of Technology (UTAUT)**, provide valuable frameworks for understanding the factors that influence this adoption process (Almaiah et al., 2020; Yu et al., 2022). TAM posits that perceived usefulness (PU) and perceived ease of use (PEOU) are primary determinants of an individual's intention to use a technology. In the context of smart classrooms, teachers are more likely to adopt new tools if they believe these tools will genuinely enhance their teaching effectiveness (PU) and are not overly complex to learn and operate (PEOU) (Wang et al., 2022). Similarly, student adoption is influenced by whether they perceive the technologies as beneficial to their learning and user-friendly (Yu et al., 2022).

UTAUT expands on TAM by incorporating additional constructs such as social influence (the extent to which an individual perceives that important others believe they should use the system) and facilitating conditions (the availability of organizational and technical infrastructure to support use) (Almaiah et al., 2020). These factors are particularly relevant for smart classrooms, where institutional support, availability of technical assistance, and a collaborative school culture can significantly impact technology adoption (Mircea & Andreescu, 2011;). Challenges such as increased workload, lack of adequate training, and insufficient institutional support, as highlighted during the rapid shift to online teaching during the COVID-19 pandemic, underscore the importance of these facilitating conditions (Watermeyer et al., 2021). Therefore, strategies for implementing smart classrooms must go beyond merely providing technology; they must also address user perceptions, provide comprehensive training, and ensure a supportive ecosystem (Wang et al., 2022).

2.3. Frameworks for Smart Learning Environments

Beyond general learning theories and technology acceptance models, specific conceptual frameworks have been developed to define the architecture, components, and functionalities of smart learning environments (SLEs). These frameworks aim to guide the design and evaluation of smart classrooms. Hwang et al. (2017) proposed criteria for SLEs, emphasizing that they should be **context-aware** (able to sense the learner's situation and environment), **adaptive** (able to adjust to the learner's needs), and **seamless** (able to support learning across different devices and locations). This framework highlights the dynamic and responsive nature expected of smart classrooms, moving beyond static technological setups.

Other frameworks focus on the integration of specific technologies. For instance, Timms (2016) conceptualized smart classrooms incorporating **AIED (Artificial Intelligence in Education)**, educational cobots (collaborative robots), and sensor networks to create more interactive and supportive learning spaces. Peng et al. (2019) developed a framework for **personalized adaptive learning** within SLEs, emphasizing components like learner profiles, competency-based progression, personal learning paths, and flexible learning environments, all orchestrated through real-time monitoring and adaptive adjustments. The systematic review by Al-Emran et al. (2020) also contributes a conceptual model that outlines the benefits (e.g., personalized learning, enhanced engagement), challenges (e.g., technical, pedagogical, security), and enabling conditions for smart classroom adoption. Saini and Goel (2019) provided a taxonomy of smart classroom technologies, which helps in understanding the diverse technological landscape, while Li et al. (2021) reviewed AI in education, outlining frameworks for intelligent tutoring, assessment, and educational management. More recent frameworks explore AI-human collaboration in education (Pratama et al., 2023) and the role of IoT (Badshah et al., 2023; Huertas Celdrán et al., 2020) and blockchain (Ahmad et al., 2021) in creating secure, efficient, and interconnected smart learning ecosystems.

2.4. Conceptualizing Challenges and Opportunities through Theoretical Lenses

These diverse theoretical frameworks not only help in understanding the operational aspects of smart classrooms but also provide a basis for conceptualizing their inherent challenges and opportunities. For example, while constructivist and connectivist theories highlight the opportunities for student-centered and networked learning, they also implicitly point to the challenge of designing pedagogical approaches that effectively leverage these technologies without overwhelming students or neglecting foundational skills (Gros, 2016; Wanner & Palmer, 2015). Technology acceptance models underscore the opportunity presented by user-friendly and demonstrably useful technologies but also highlight the challenge of overcoming resistance to change and ensuring adequate teacher preparedness (Watermeyer et al., 2021).

Frameworks for SLEs showcase the potential for highly adaptive and personalized learning experiences (Hwang et al., 2017; Peng et al., 2019) but simultaneously bring to the fore significant challenges related to data privacy, algorithmic bias, and the digital divide (Alfoudari, 2021; Gros, 2016; Tawalbeh et al., 2016). The ethical implications of pervasive data collection and AI-driven decision-making in education are critical concerns that these frameworks help to articulate (Li et al., 2015; Oyelere et al., 2018). Furthermore, the socio-cultural perspective reminds us that the opportunities of smart classrooms may not be universally accessible or equally beneficial across different contexts, emphasizing the challenge of ensuring equity and inclusivity (Ifinedo et al., 2020; Dimitriadou et al., 2023). The financial and infrastructural challenges associated with implementing and sustaining these complex technological environments are also significant hurdles that need to be addressed through robust policy and institutional commitment (Lorenzo et al., 2021; Saini & Goel, 2019). Thus, a theoretically informed approach is indispensable for navigating the multifaceted landscape of smart classrooms, maximizing their benefits while mitigating their risks.

3. Literature Review

The discourse surrounding smart classrooms is rich with explorations of their potential to revolutionize education, alongside critical examinations of the hurdles that impede their widespread and effective adoption. This literature review synthesizes existing research to delineate the key emerging opportunities and challenges associated with smart classrooms, focusing on their impact on pedagogical practices, student experiences, and the broader educational ecosystem. The analysis is structured around the primary benefits offered by these technologically advanced environments and the significant obstacles that must be navigated to realize their full promise.

3.1. Opportunities Presented by Smart Classrooms

The integration of advanced technologies within smart classrooms opens up a plethora of opportunities to enhance teaching and learning. These range from highly individualized educational experiences to more engaging and collaborative learning environments, supported by access to a wealth of digital resources and data-driven pedagogical insights.

3.1.1. Enhanced Personalized and Adaptive Learning

One of the most significant opportunities afforded by smart classrooms is the capacity to deliver enhanced personalized and adaptive learning experiences. By leveraging technologies such as AI, learning analytics, and IoT sensors, smart environments can gather real-time data on individual student progress, learning styles, and engagement levels, subsequently tailoring instructional content, pace, and feedback accordingly (Al-Emran et al., 2018; Li et al., 2015; Peng et al., 2019). Wanner and Palmer (2015) highlight how flexible pedagogies like the flipped classroom, often facilitated by smart technologies, allow for greater personalization of the learning journey. Peng et al. (2019) further elaborate on this by proposing a framework for personalized adaptive learning that utilizes real-time monitoring to adjust teaching strategies, incorporating learner profiles and competency-based progression. AI-driven intelligent tutoring systems can provide individualized support and adaptive feedback, catering to diverse learner needs (Li et al., 2015; Pratama et al., 2023), while learning analytics can offer insights for personalized interventions and identify students requiring additional support (Xie et al., 2019). Even technologies like blockchain are being explored for creating personalized lifelong learning records and tracking skill development (Ahmad et al., 2021), and IoT sensors contribute data that enables dynamic adaptation of the learning environment (Badshah et al., 2023; Zhu et al., 2016).

3.1.2. Improved Student Engagement and Motivation

Smart classrooms offer numerous avenues for improving student engagement and motivation, moving beyond traditional passive learning models. Interactive technologies, multimedia content, and gamified learning experiences can capture students' attention and foster active participation (Sailer & Homner, 2020; Vesin et al., 2018). The flipped classroom model, as noted by Wanner and Palmer (2015), has been shown to increase student engagement. Augmented reality (AR) applications can create immersive and experiential learning opportunities that enhance motivation (Vesin et al., 2018), while well-designed adaptive learning systems can boost intrinsic motivation by providing appropriate levels of challenge and support (Bower, 2016). Smart learning environments in various contexts, such as India, are reported to foster active participation through their learner-centric design (Yadav & Oyelere, 2021). Gamification elements, including points, badges, and leaderboards, are increasingly used to make learning more enjoyable and to encourage sustained effort (Sailer & Homner, 2020). However, it is crucial to note, as Gros (2016) cautions, that technology alone does not guarantee engagement; the pedagogical design and the quality of content remain paramount (Singh & Thurman, 2019).

3.1.3. Facilitation of Collaborative Learning and Interaction

Smart classrooms can significantly enhance opportunities for collaborative learning and interaction among students, and between students and educators. Digital tools can support group projects, peer-to-peer learning, and communication that transcends physical classroom boundaries (Al-Samarraie et al., 2020; Chen et al., 2014; Timms, 2016). Timms (2016) suggests that educational cobots (collaborative robots) could facilitate group work, while smart classroom platforms can provide shared digital workspaces and tools for collaborative tasks. Learning analytics can be employed to identify collaboration patterns and even support the formation of effective learning groups (Chen et al., 2014). In contexts like Sub-Saharan Africa, mobile technologies are being used to enable collaborative projects and peer learning, despite infrastructural challenges (Dimitriadou et al., 2023). Smart environments, as described by Hwang et al. (2017), are designed to enable seamless interaction and resource sharing. Virtual reality (VR) technologies are also emerging as powerful tools for creating collaborative simulations and training environments, allowing students to learn by doing in shared virtual spaces (Al-Samarraie et al., 2020). While the shift to online learning during the pandemic sometimes hindered collaboration due to various issues (Watermeyer et al., 2021), the potential of well-designed smart environments to foster rich interaction remains a key opportunity.

3.1.4. Access to Richer Educational Resources and Tools

Smart classrooms provide students and teachers with access to an unprecedented array of rich educational resources and sophisticated learning tools (Ally & Prieto-Blázquez, 2014; Saini & Goel, 2019; Tawalbeh et al., 2016). These include digital libraries, multimedia content, interactive simulations, virtual laboratories, and specialized software that can cater to diverse subject areas and learning objectives. Mobile learning, a component of many smart classroom strategies, allows access to resources anytime and anywhere, promoting ubiquitous learning (Ally & Prieto-Blázquez, 2014). IoT technologies can enable access to real-time data streams and remote experimental setups, expanding learning possibilities beyond the traditional classroom (Tawalbeh et al., 2016). Gamified platforms often offer a diverse range of learning activities and resources embedded within engaging narratives (Sailer & Homner, 2020). The COVID-19 pandemic, despite its challenges, spurred the rapid development and curation of online educational resources (Major et al., 2021). However, ensuring equitable access to these resources remains a critical concern, as highlighted by experiences during emergency remote teaching (Bond et al., 2020).

3.1.5. Data-Driven Insights for Pedagogical Improvement

Smart classrooms generate vast amounts of data about student learning processes, interactions, and performance, which can be harnessed through learning analytics to provide valuable insights for pedagogical improvement (Chen et al., 2014; Li et al., 2015; Timms, 2016; Xie et al., 2019). This data-driven approach allows educators to monitor student progress in real-time, identify learning difficulties early, and adapt their teaching strategies to better meet student needs (Al-Emran et al., 2018; Timms, 2016). Learning analytics can reveal patterns in student engagement, help in identifying at-risk students for timely interventions, and inform the design of more effective learning activities and assessments (Chen et al., 2014; Xie et al., 2019). AI systems can analyze this data to provide automated feedback and even suggest personalized learning paths (Li et al., 2015). For teachers, data literacy—the ability to interpret and use this data effectively—is becoming an increasingly important competency (Wang et al., 2022). At an institutional level, data on system usage and student performance can inform strategic decisions regarding e-learning support and resource allocation (Almaiah et al., 2020; Huertas Celdrán et al., 2020).

4. Challenges in Implementing and Sustaining Smart Classrooms

Despite the compelling opportunities, the path to successful implementation and sustainability of smart classrooms is fraught with challenges. These obstacles are multifaceted, encompassing technological, pedagogical, ethical, social, financial, and administrative dimensions.

4.1. Technological Challenges

Technological challenges are often the most immediate and visible hurdles. These include the need for robust and reliable ICT infrastructure, including high-speed internet connectivity, adequate devices for students and teachers, and appropriate software platforms (Al-Emran et al., 2018; Gros, 2016; Ifinedo et al., 2020). Interoperability between different systems and technologies, and the integration of disparate hardware and software components, can be complex and costly (Saini & Goel, 2019). Ensuring the security and privacy of the vast amounts of sensitive student data collected by smart classroom systems is a paramount concern, with threats ranging from data breaches to unauthorized access (Badshah et al., 2023; Al-Emran et al., 2018; Oyelere et al., 2018; Tawalbeh et al., 2016). The maintenance and regular updating of both hardware and software also pose ongoing logistical and financial burdens (Saini & Goel, 2019). Furthermore, technical glitches, system failures, and the digital divide—unequal access to technology and connectivity—can exacerbate existing inequalities and hinder the learning process (Ally & Prieto-Blázquez, 2014; Gros, 2016; Dimitriadou et al., 2023; Lorenzo et al., 2021; Sailer & Homner, 2020).

4.2. Pedagogical Challenges

The integration of technology into classrooms necessitates significant pedagogical shifts, which present a distinct set of challenges. Teachers require adequate training and ongoing professional development to effectively utilize new technologies and adapt their teaching methods to suit smart learning environments (Bower, 2016; Dimitriadou et al., 2023; Wang et al., 2022). This involves not just technical skills but also pedagogical content knowledge (TPACK) – understanding how to integrate technology, pedagogy, and content effectively (). Designing engaging and effective learning experiences within smart environments, redesigning curricula to leverage technological affordances, and developing appropriate assessment methods are complex tasks that demand considerable time and expertise (Bower, 2016; Singh & Thurman, 2019). There is often a concern about teacher workload associated with implementing new pedagogies like the flipped classroom or personalized learning (Wanner & Palmer, 2015). Moreover, fostering critical digital literacy among students, rather than just passive technology consumption, is a crucial pedagogical challenge (Gros, 2016). The rapid shift to online learning during the COVID-19 pandemic highlighted the difficulties many educators faced in adapting their teaching methods and maintaining student engagement and pedagogical quality without adequate preparation or support (Bond et al., 2020; Major et al., 2021; Watermeyer et al., 2021).

4.3. Ethical and Social Challenges

The pervasive data collection and analysis inherent in smart classrooms raise significant ethical and social concerns. Data privacy and security are paramount, as student data is highly sensitive and vulnerable to misuse or breaches (Badshah et al., 2023; Al-Emran et al., 2018; Li et al., 2015; Oyelere et al., 2018; Timms, 2016). The potential for algorithmic bias in AI-driven systems, where historical biases in data could lead to discriminatory outcomes in terms of student assessment or learning path recommendations, is a serious ethical consideration (Li et al., 2015; Pratama et al., 2023). The digital divide, encompassing disparities in access to technology, internet connectivity, and digital skills, can exacerbate existing social inequalities, potentially leaving disadvantaged students further behind (Alfoudari, 2021; Gros, 2016; Hwang et al., 2017; Ifinedo et al., 2020). Issues of data ownership, transparency in how data is used, and student consent are also critical ethical dilemmas that need careful consideration (Ahmad et al., 2021; Huertas Celdrán et al., 2020). Furthermore, concerns about increased screen time, potential for student isolation in highly individualized learning paths, and the impact on overall student well-being must be addressed.

4.4. Financial and Administrative Challenges

The implementation and long-term sustainability of smart classrooms entail substantial financial investment and pose administrative challenges. The initial costs of acquiring hardware, software, and developing necessary infrastructure can be prohibitive for many institutions, particularly in resource-constrained settings (Dimitriadou et al., 2023; Saini & Goel, 2019; Tawalbeh et al., 2016). Ongoing expenses for maintenance, upgrades, software licenses, technical support, and teacher training add to the financial burden (Oyelere et al., 2018; Saini & Goel, 2019). Securing adequate and sustained funding, along with strong institutional support and clear policies, is crucial for the success of smart classroom initiatives (Ifinedo et al., 2020; ; Wanner & Palmer, 2015). Administrative challenges include developing effective policies for technology integration, data governance, and ethical oversight, as well as managing the complex logistics of large-scale technology deployment and support (Huertas Celdrán et al., 2020; Yu et al., 2022). The lack of institutional support was a frequently cited concern by teachers regarding the adoption of innovative pedagogies (Wanner & Palmer, 2015), and the financial strain on both institutions and students for remote learning technologies became evident during the pandemic (Lorenzo et al., 2021).

5. Key Debates in the Field

The literature on smart classrooms is characterized by several ongoing debates. A central debate revolves around whether smart classroom initiatives should be **technology-driven or pedagogy-driven**. Critics argue that an overemphasis on acquiring the latest technology without a clear pedagogical vision can lead to ineffective implementation and underutilization (Gros, 2016; Wanner & Palmer, 2015). Conversely, a pedagogy-first approach emphasizes identifying educational goals and then selecting appropriate technologies to support them (Bower, 2016). Another debate concerns the **actual effectiveness versus the perceived hype** surrounding smart classrooms. While proponents highlight transformative potential, skeptics call for more rigorous empirical evidence to substantiate claims of improved learning outcomes and caution against techno-solutionism (Al-Emran et al., 2018; Saini & Goel, 2019). The issue of **standardization versus customization** is also prominent. While some argue for standardized platforms and tools to ensure interoperability and ease of use, others advocate for highly customizable solutions that can cater to specific institutional and learner needs (Hwang et al., 2017; Peng et al., 2019). Finally, the balance between **data-driven personalization and student privacy/ autonomy** remains a contentious issue, with ongoing discussions about how to leverage data ethically and empower students in their learning journeys (Li et al., 2015; Pratama et al., 2023; Timms, 2016).

6. Gaps in Current Literature

Despite a growing body of research, several gaps persist in the literature on smart classrooms. There is a need for more **longitudinal studies** that track the long-term impacts of smart classroom interventions on student learning outcomes, engagement, and skill development (Al-Emran et al., 2018; Vesin et al., 2018; Xie et al., 2019). More research is required on **effective pedagogical strategies** specifically designed for smart learning environments across diverse disciplines and age groups (Bower, 2016; Wanner & Palmer, 2015). The **ethical implications of AI and learning analytics** in education, particularly concerning bias, transparency, and student agency, warrant deeper investigation (Li et al., 2015; Pratama et al., 2023). Studies focusing on **teacher professional development models** that effectively prepare educators for the complexities of teaching in smart classrooms are also crucial (Wang et al., 2022). Furthermore, there is a need for more research on the **scalability and sustainability** of smart classroom initiatives, especially in resource-limited contexts and developing countries (Badshah et al., 2023; Ifinedo et al., 2020; Dimitriadou et al., 2023). Finally, comparative studies that evaluate different models of smart classrooms and their cost-effectiveness would provide valuable insights for policymakers and institutional leaders (Saini & Goel, 2019; Zhu et al., 2016).

7. Future Directions

The rapidly evolving landscape of smart classrooms, characterized by continuous technological advancements and shifting pedagogical paradigms, necessitates a forward-looking perspective to guide future research and development. Building upon the opportunities and challenges identified in the preceding literature review, this section proposes key areas for future inquiry and discusses potential methodological approaches to deepen our understanding and optimize the impact of smart learning environments. The aim is to chart a course for research that is not only innovative but also ethically responsible and contextually relevant, ensuring that smart classrooms effectively serve the diverse needs of learners and educators in the digital age.

7.1. Advancing Pedagogical Models for Smart Classrooms

While technology provides the infrastructure for smart classrooms, pedagogy remains the cornerstone of effective learning. Future research should focus on developing and validating innovative pedagogical models specifically tailored for these technologically rich environments (Bower, 2016; Wang et al., 2022; ; Wanner & Palmer, 2015). This includes investigating how to best integrate emerging technologies to support active learning, critical thinking, and collaborative problem-solving across various disciplines (Peng et al., 2019; Wanner & Palmer, 2015). There is a need for more studies on the long-term impact of flexible learning models, such as the flipped classroom and personalized adaptive learning, on student outcomes and engagement, particularly across different educational levels and cultural contexts (Peng et al., 2019; Singh & Thurman, 2019; Wanner & Palmer, 2015). Research should also explore effective strategies for curriculum redesign to fully leverage the capabilities of smart classrooms, moving beyond mere content delivery to foster deeper conceptual understanding and 21st-century skills (Bower, 2016). Furthermore, developing and evaluating robust and authentic assessment methods that align with the dynamic and interactive nature of smart learning environments is a critical area for future investigation (Wanner & Palmer, 2015).

7.2. Exploring Emerging Technologies and Their Educational Applications

The relentless pace of technological innovation continues to present new possibilities for smart classrooms. Future research should proactively explore the educational potential and implications of emerging technologies (Al-Emran et al., 2018; Li et al., 2015; Saini & Goel, 2019; Timms, 2016). Artificial intelligence, particularly advancements in explainable AI (XAI), generative AI, and AI-driven adaptive systems, warrants significant attention to understand how these tools can create more personalized, responsive, and supportive learning experiences (Li et al., 2015; Pratama et al., 2023; Timms, 2016). The integration of immersive technologies like augmented reality (AR), virtual reality (VR), and mixed reality (MR) into various subject areas should be further investigated to assess their impact on student engagement, conceptual understanding, and skill development (Al-Samarraie et al., 2020; Hwang et al., 2017; Vesin et al., 2018). Affective computing, which aims to recognize and respond to learners' emotional states, presents another frontier for creating more empathetic and effective smart learning environments (Timms, 2016). Additionally, the application of technologies like blockchain for secure credentialing, managing lifelong learning records, and ensuring data integrity in educational settings deserves continued exploration (Ahmad et al., 2021). Research should focus not only on the technical capabilities of these emerging technologies but also on their pedagogical affordances and the challenges associated with their integration (Saini & Goel, 2019; Tawalbeh et al., 2016).

7.3. Addressing Ethical, Equity, and Inclusivity Concerns

As smart classrooms become increasingly data-intensive and reliant on AI, addressing the associated ethical, equity, and inclusivity concerns is paramount. Future research must prioritize the development of frameworks and guidelines for the responsible and ethical use of student data and AI in education (Badshah et al., 2023; Li et al., 2015; Oyelere et al., 2018; Timms, 2016). This includes investigating methods to mitigate algorithmic bias, ensure transparency and accountability in AI-driven decision-making, and protect student privacy (Li et al., 2015; Pratama et al., 2023). A significant research focus should be on understanding and addressing the digital divide to ensure that smart classroom initiatives promote equity rather than exacerbate existing inequalities (Alfoudari, 2021; Gros, 2016; Hwang et al., 2017; Ifinedo et al., 2020). This involves exploring strategies for providing equitable access to technology, developing culturally relevant digital content, and supporting learners with diverse needs and backgrounds (Dimitriadou et al., 2023). Research is also needed on how to foster critical digital literacy and responsible digital citizenship among students to empower them to navigate the complexities of smart learning environments safely and effectively (Gros, 2016; Oyelere et al., 2018).

7.4. Methodological Innovations for Smart Classroom Research

The complexity and dynamism of smart classrooms call for innovative methodological approaches to effectively study their impact and inform their design. While traditional quantitative and qualitative methods remain valuable, future research could benefit from the increased adoption of **mixed-methods research designs** that can provide a more holistic understanding of the interplay between technology, pedagogy, and learning outcomes (Wanner & Palmer, 2015). **Longitudinal studies** are crucial for tracking the long-term effects of smart classroom interventions and understanding how student learning and engagement evolve over time (Al-Emran et al., 2018; Vesin et al., 2018; Xie et al., 2019). **Design-based research (DBR)** offers a powerful methodology for iteratively developing and refining smart classroom innovations in authentic educational settings, bridging the gap between theory and practice (Peng et al., 2019). The field of **learning analytics** itself requires further methodological advancement to move beyond descriptive analytics towards predictive and prescriptive analytics that can offer actionable insights for educators and learners (Chen et al., 2014; Xie et al., 2019). Exploring new data collection techniques, such as multimodal data capture (e.g., eye-tracking, physiological sensors), could provide richer insights into student engagement and cognitive processes within smart environments (Timms, 2016).

7.5. Policy, Scalability, and Sustainability Research

For smart classrooms to move beyond isolated pilot projects and achieve widespread, sustainable impact, research into effective policies, scalability strategies, and sustainability models is essential. Future studies should investigate the role of **educational policies** at institutional, regional, and national levels in fostering or hindering the adoption and effective use of smart classroom technologies (Ifinedo et al., 2020; ; Wanner & Palmer, 2015). This includes examining policies related to funding, infrastructure development, teacher training, curriculum standards, and data governance (Huertas Celdrán et al., 2020). Research on **scalability** should focus on identifying factors that enable the successful expansion of smart classroom initiatives from small-scale implementations to broader systemic adoption, particularly in diverse and resource-constrained contexts (Badshah et al., 2023; Dimitriadou et al., 2023; Saini & Goel, 2019). This involves understanding the organizational changes, leadership commitment, and stakeholder collaboration required for scaling up. Finally, **sustainability research** needs to explore financial models, resource allocation strategies, and continuous improvement processes that can ensure the long-term viability and relevance of smart classroom investments, preventing them from becoming obsolete or underutilized (Saini & Goel, 2019; Yu et al., 2022).

In conclusion, the future of smart classrooms hinges on a concerted research effort that is interdisciplinary, critically reflective, and focused on practical impact. By addressing these future directions, the research community can play a vital role in shaping smart learning environments that are not only technologically advanced but also pedagogically sound, ethically responsible, and equitably accessible to all learners.

8. Conclusion

The journey through the landscape of smart classrooms reveals a domain rich with transformative potential yet fraught with complex challenges. This chapter has endeavored to provide a comprehensive theoretical review of these emerging opportunities and obstacles, synthesizing existing literature to illuminate the multifaceted nature of technology-enhanced education in the digital age. The central argument maintained throughout this exploration is that while smart classrooms offer unprecedented avenues for personalizing learning, enhancing student engagement, fostering collaboration, and providing access to vast educational resources, their successful and ethical implementation is contingent upon a proactive, critical, and holistic approach that diligently addresses the technological, pedagogical, ethical, social, financial, and administrative hurdles they present.

The exploration began by defining smart classrooms as technologically enriched environments where the integration of tools like IoT, AI, and interactive systems aims to create dynamic and responsive learning ecosystems. The significance of these environments in preparing students for a digitally driven future was underscored, alongside an acknowledgment of the complexities inherent in their adoption. The theoretical framework section grounded the discussion in foundational learning theories such as constructivism, connectivism, and socio-cultural perspectives, illustrating how smart classrooms can align with or challenge these established pedagogical principles. Furthermore, technology acceptance models like TAM and UTAUT provided insights into the factors influencing the adoption of these technologies by educators and students, while specific frameworks for smart learning environments helped to conceptualize their architecture and functionalities. This theoretical lens was crucial for framing the subsequent discussion of both the affordances and the impediments associated with smart classrooms.

The literature review systematically cataloged the key opportunities, including the capacity for enhanced personalized and adaptive learning, improved student engagement and motivation, facilitation of collaborative learning, access to richer educational resources, and the generation of data-driven insights for pedagogical improvement. Simultaneously, it detailed the significant challenges that must be overcome. These encompass technological hurdles such as infrastructure and security; pedagogical challenges related to teacher training and curriculum adaptation; profound ethical and social concerns regarding data privacy, algorithmic bias, and the digital divide; and substantial financial and administrative challenges concerning cost and institutional support. Key debates in the field, such as technology-driven versus pedagogy-driven approaches and concerns about effectiveness versus hype, were also highlighted, alongside identified gaps in the current literature that call for further scholarly inquiry.

Looking towards the future, this chapter proposed several critical directions for research. These include advancing pedagogical models tailored for smart environments, exploring the educational applications of emerging technologies like advanced AI and immersive realities, rigorously addressing ethical and equity concerns, innovating research methodologies to better capture the complexities of smart learning, and investigating effective policies for scalability and sustainability. The overarching goal of these future endeavors should be to ensure that smart classrooms evolve in a manner that is not only technologically sophisticated but also pedagogically sound, ethically responsible, and equitably accessible to all learners.

In conclusion, smart classrooms represent a significant meeting point of technology and teaching in the digital age, holding the promise of a more adaptive, engaging, and effective educational future. However, this promise can only be fully realized if stakeholders—educators, policymakers, researchers, and technology developers—work collaboratively and critically. A balanced perspective, one that embraces the innovative potential of smart technologies while vigilantly addressing their inherent complexities and risks, is essential. By fostering a culture of continuous inquiry, ethical reflection, and pedagogical innovation, the educational community can navigate the evolving terrain of smart classrooms and harness their power to genuinely transform learning for the better, ensuring that technology serves as a potent enabler of human potential and equitable educational opportunity.

References

Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Omar, M., & Ellahham, S. (2021). The role of blockchain technology in telehealth and telemedicine. International Journal of Medical Informatics, 148, 104399. https://doi.org/10.1016/j.ijmedinf.2021.104399

Al-Emran, M., Mezhuyev, V., Kamaludin, A., & ALSinani, M. (2018). Development of M-learning application based on knowledge management processes. In *Proceedings of the 2018 7th international conference on software and computer applications* (pp. 248-253). https://doi.org/10.1145/3185089.3185120

Alfoudari, A. M., Durugbo, C. M., & Aldhmour, F. M. (2021). Understanding socio-technological challenges of smart classrooms using a systematic review. *Computers & Education*, *173*, 104282. https://doi.org/10.1016/j.compedu.2021.104282

Almaiah, M. A., Al-Khasawneh, A., & Althunibat, A. (2020). Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic. Education and Information Technologies, 25, 5261-5280. https://doi.org/10.1007/s10639-020-10219-y

Ally, M., & Prieto-Blázquez, J. (2014). What is the future of mobile learning in education? The International Journal of Educational Technology in Higher Education, 11(1), 142-151. https://doi.org/10.7238/rusc.v11i1.2033

Al-Samarraie, H., Shamsuddin, A., & Alzahrani, A. I. (2020). A flipped classroom model in higher education: A review of the evidence across disciplines. Educational Technology Research and Development, 68, 1017-1051. https://doi.org/10.1007/s11423-019-09718-8

Badshah, A., Ghani, A., Daud, A., Jalal, A., Bilal, M., & Crowcroft, J. (2023). Towards smart education through internet of things: A survey. *ACM Computing Surveys*, *56*(2), 1-33. https://doi.org/10.48550/arXiv.2304.12851

Bond, M., Buntins, K., Bedenlier, S., Zawacki-Richter, O., & Kerres, M. (2020). Mapping research in student engagement and educational technology in higher education: A systematic evidence map. International Journal of Educational Technology in Higher Education, 17(1), 1-30. https://doi.org/10.1186/s41239-019-0176-8

Bower, M. (2016). A framework for adaptive learning design in a web-conferencing environment. Journal of Interactive Media in Education, 2016(1), 11. https://doi.org/10.5334/jime.406

Chen, C. M., Wang, J. Y., & Chen, Y. C. (2014). Facilitating English-language reading performance by a digital reading annotation system with self-regulated learning mechanisms. *Journal of Educational Technology & Society*, *17*(1), 102-114.

Dimitriadou, E., & Lanitis, A. (2023). A critical evaluation, challenges, and future perspectives of using artificial intelligence and emerging technologies in smart classrooms. *Smart Learning Environments*, *10*(1), 12. https://doi.org/10.1186/s40561-023-00231-3

Gros, B. (2016). The design of smart educational environments. Smart Learning Environments, 3(1), 15. https://doi.org/10.1186/s40561-016-0039-x

Hwang, G. J., Chu, H. C., & Yin, C. (2017). Objectives, methodologies and research issues of learning analytics. *Interactive Learning Environments*, *25*(2), 143-146.

Huertas Celdrán, A., Ruipérez-Valiente, J. A., García Clemente, F. J., Rodríguez-Triana, M. J., Shankar, S. K., & Martínez Pérez, G. (2020). A Scalable Architecture for the Dynamic Deployment of Multimodal Learning Analytics Applications in Smart Classrooms. *Sensors*, *20*(10), 2923. https://doi.org/10.3390/s20102923

Ifinedo, E., Rikala, J., & Hämäläinen, T. (2020). Factors affecting Nigerian teacher educators' technology integration: Considering characteristics, knowledge constructs, ICT practices and beliefs. Computers &

Li, B., Kong, S. C., & Chen, G. (2015). Development and validation of the smart classroom inventory. Smart Learning Environments, 2(1), 3. https://doi.org/10.1186/s40561-015-0012-0

Lorenzo, N., Gallon, R., Palau, R., & Mogas, J. (2021). New objectives for smart classrooms from industry 4.0. *Technology, Knowledge and Learning*, *26*(4), 719-731. https://doi.org/10.1007/s10758-021-09527-0

Major, L., Francis, G. A., & Tsapali, M. (2021). The effectiveness of technology-supported personalised learning in low-and middle-income countries: A meta-analysis. *British Journal of Educational Technology*, *52*(5), 1935-1964. https://doi.org/10.1111/bjet.13116

Mircea, M., & Andreescu, A. I. (2011). Using cloud computing in higher education: A strategy to improve agility in the current financial crisis. *Communications of the IBIMA*. https://doi.org/10.5171/2011.875547

Oyelere, S. S., Suhonen, J., Wajiga, G. M., & Sutinen, E. (2018). Design, development, and evaluation of a mobile learning application for computing education. *Education and Information Technologies*, *23*, 467-495. https://doi.org/10.1007/s10639-017-9613-2

Peng, H., Ma, S., & Spector, J. M. (2019). Personalized adaptive learning: an emerging pedagogical approach enabled by a smart learning environment. *Smart Learning Environments*, *6*(1), 1-14. https://doi.org/10.1186/s40561-019-0089-y

Pratama, M. P., Sampelolo, R., & Lura, H. (2023). Revolutionizing education: harnessing the power of artificial intelligence for personalized learning. *Klasikal: Journal of education, language teaching and science*, *5*(2), 350-357. https://doi.org/10.52208/klasikal.v5i2.877

Sailer, M., & Homner, L. (2020). The gamification of learning: A meta-analysis. Educational Psychology Review, 32, 77-112. https://doi.org/10.1007/s10648-019-09498-w

Saini, M., & Goel, N. (2019). How smart are smart classrooms? A review of smart classroom technologies. ACM Computing Surveys, 52(6), 130. https://doi.org/10.1145/3365757

Singh, V., & Thurman, A. (2019). How many ways can we define online learning? A systematic literature review of definitions of online learning (1988-2018). American Journal of Distance Education, 33(4), 289-306. https://doi.org/10.1080/08923647.2019.1663082

Tawalbeh, M., Eardley, A., & Tawalbeh, L. (2016). Studying the energy consumption in mobile devices. Procedia Computer Science, 94, 183-189. https://doi.org/10.1016/j.procs.2016.08.028

Timms, M. J. (2016). Letting artificial intelligence in education out of the box: Educational cobots and smart classrooms. International Journal of Artificial Intelligence in Education, 26(2), 701-712. https://doi.org/10.1007/s40593-016-0095-y

Vesin, B., Mangaroska, K., & Giannakos, M. (2018). Learning in smart environments: user-centered design and analytics of an adaptive learning system. *Smart Learning Environments*, *5*(1), 24. https://doi.org/10.1186/s40561-018-0071-0

Wang, J., Tigelaar, D. E., Luo, J., & Admiraal, W. (2022). Teacher beliefs, classroom process quality, and student engagement in the smart classroom learning environment: A multilevel analysis. *Computers & Education*, *183*, 104501. https://doi.org/10.1016/j.compedu.2022.104501

Wanner, T., & Palmer, E. (2015). Personalising learning: Exploring student and teacher perceptions about flexible learning and assessment in a flipped university course. Computers & Education, 88, 354-369. https://doi.org/10.1016/j.compedu.2015.07.008

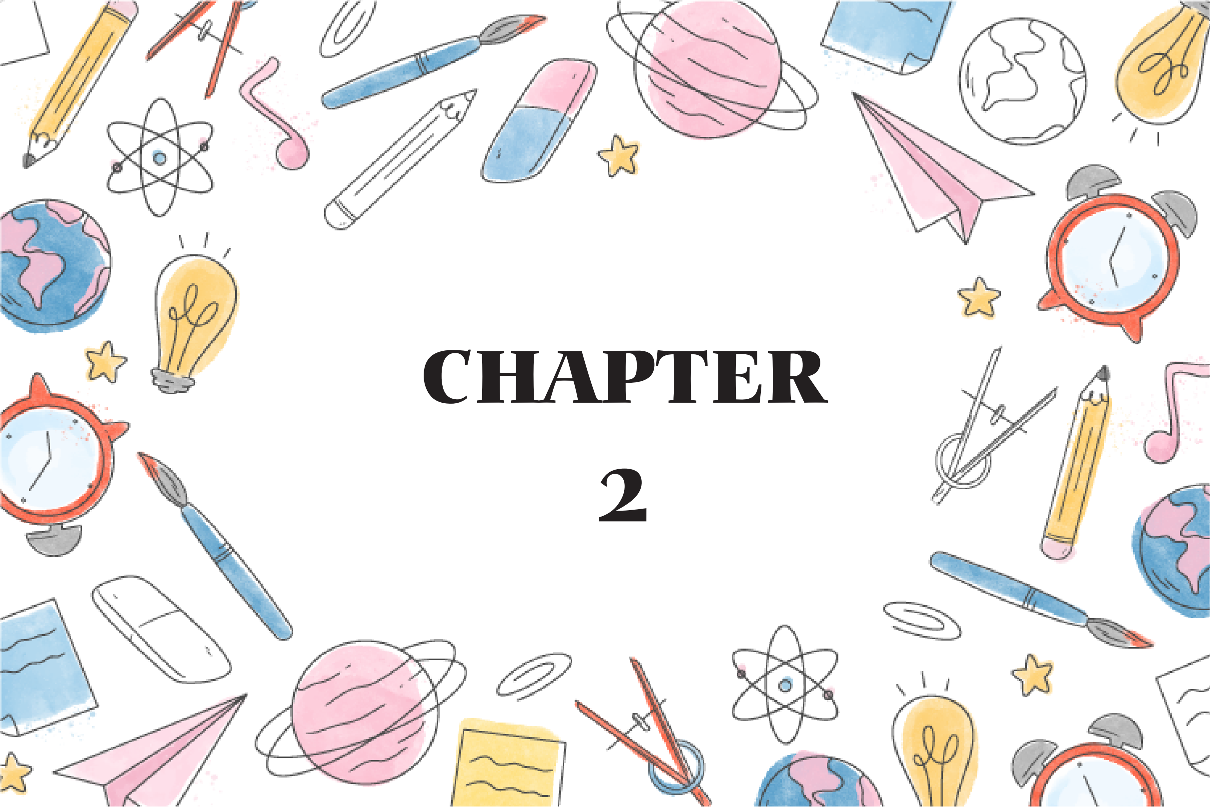
Watermeyer, R., Crick, T., Knight, C., & Goodall, J. (2021). COVID-19 and digital disruption in UK universities: Afflictions and affordances of emergency online migration. Higher Education, 81, 623-641. https://doi.org/10.1007/s10734-020-00561-y

Xie, H., Chu, H. C., Hwang, G. J., & Wang, C. C. (2019). Trends and development in technology-enhanced adaptive/personalized learning: A systematic review of journal publications from 2007 to 2017. Computers & Education, 140, 103599. https://doi.org/10.1016/j.compedu.2019.103599

Yadav, D. K., & Oyelere, S. S. (2021). Contextualized mobile game-based learning application for computing education. Education and Information Technologies, 26, 2539-2562. https://doi.org/10.1007/s10639-020-10373-3

Yu, L., Wu, D., Yang, H. H., & Zhu, S. (2022). Smart classroom preferences and information literacy among college students. *Australasian Journal of Educational Technology*, *38*(2), 142-161. https://doi.org/10.14742/ajet.7081

Zhu, Z. T., Yu, M. H., & Riezebos, P. (2016). A research framework of smart education. Smart Learning Environments, 3(1), 4. https://doi.org/10.1186/s40561-016-0026-2



CHAPTER 2

HIGHER EDUCATION STUDENTS' ETHICAL ATTITUDES TOWARDS INFORMATION TECHNOLOGIES: A DEMOGRAPHIC ANALYSIS

Recep ÖZ[1]

Nusrettin YILMAZ[2]

1 Assoc. Prof. Dr. Recep ÖZ, Erzincan Binali Yıldırım University, Faculty of Education, Department of Computer Education and Instructional Technology, E-mail:recepoz@erzincan.edu.tr, ORCID: 0000-0001-9974-0022
2 Assistant Professor Dr. Nusrettin YILMAZ, Erzincan Binali Yıldırım University, Faculty of Education, Department of Basic Education, Division of Primary Education, E-mail: nyilmaz@erzincan.edu.tr, ORCID: 0000-0002-9019-2602

1. Introduction

The word "ethics" is derived from the Greek word "ethos," which encompasses meanings such as customs, morals, traditions, habits, character, temperament, among others. Similarly, the word "morality," originating from Latin, carries meanings related to customs, habits, traditions, character, nature, among others. Likewise, the Turkish term "ahlak," which is the plural of the Arabic word "hulk," is used to denote customs, habits, traditions, character, nature. Hence, it can be said that etymologically, these terms generally convey similar meanings. However, their philosophical meanings in context differ from the meanings derived from their etymology, and therefore, these concepts should be addressed within the philosophical context (Pieper, 1999; Akarsu, 1984; Özlem, 2017; Tepe, 2007).

In philosophy, the term "ethics" refers to the science of morals or moral philosophy. Ethics, as a branch of philosophy, encompasses the pursuit of a good life, contemplation of good and evil, defining correct behavior, making morally correct choices, and the doctrine of making correct decisions (Cevizci, 2008).

The complexity of modern life has brought ethical studies into the realm of applied ethics. While fundamental ethical issues remain unchanged, new ethical dilemmas constantly arise, and there are also changes in how these issues are addressed. In our age, applied ethics deals with new ethical domains such as racism, gender discrimination, issues related to sexual orientation, violence and capital punishment, suicide, abortion, cloning, war and terrorism, animal rights, match-fixing, gambling, doping, environmental concerns, and other emerging ethical areas. In this context, applied ethics has been subdivided into subcategories such as biomedical ethics, business ethics, and environmental ethics (Cevizci, 2008; Tepe, 2016; Yılmaz, 2009).

Information and Communication Technologies (ICT) refer to digital tools and systems used in processes of information gathering, storing, processing, transmission, and sharing. These technologies encompass computers, smartphones, internet infrastructure, software applications, data storage systems, networks, and other electronic devices. ICT has become an indispensable part of modern life, affecting a range of fields and facilitating business processes, easing communication, and accelerating access to information. Analyses of the frequency of ICT usage paint a striking picture. With the proliferation of computers and smartphones, the average technology usage time increased from 6 hours per day in 1999 to 7.5 hours in 2005, 10 hours and 45 minutes in 2009, and up to 13 hours per day in 2013 (Raven, 2018). In 2016, the number of internet users in Turkey was reported as 46,196,720, which accounted for 58% of the population at that time (Internet Users by Country, 2016). According to the Household Information Technologies (IT) Usage Survey conducted by the Turkish Statistical Institute (TUIK) in 2022, the percentage of individuals using the internet is 85% (TUIK, 2022).

The integration of the internet and computers into the daily lives of society has brought with it ethical challenges alongside the advantages these technologies offer. One of these challenges is ethical issues, which extend to computer crimes. Particularly with the widespread use of the internet, unethical behaviors such as misuse of personal information, verbal attacks, copyright infringement, dissemination of misleading information, unauthorized access, and fraud have come to the forefront (Dedeoğlu, 2006).

Information technologies are important because they provide great convenience in terms of information and access. However, to prevent the negative impacts of these technologies on human life, a field such as computer ethics has been developed. Computer ethics aims to prevent harmful integration of these technologies into human life (Moor, 1985).

Computer ethics is a branch of philosophy that examines the use of computer and communication technologies and discusses the application of general ethical principles to the use of these technologies (TBD, 2010). Moor (1985) defines computer ethics as a field that encompasses principles and rules regarding the development and use of computer technologies. Tıngöy (2009) describes computer ethics as the written and unwritten rules we should adhere to when using information technologies. According to Sevindik (2011), these rules ensure that users utilize the electronic environment with minimal harm and maximum benefit in information and communication environments. Computer ethics is based on determining and implementing these principles and rules and seeks ethically based solutions to problems encountered in the computing environment. According to Cerrah (2002), failure to use technology properly and regulate it regularly can have negative effects not only on individuals' physical and psychological health but also on social peace and integrity.

According to the Turkey Informatics Association Report, issues related to computer ethics include the right to access electronic data and digital inequality, the reliability, accuracy, and currency of electronic data, distortion of reality, system security, intellectual property rights, privacy violations, protection of personal data, protection of corporate data, internet usage issues, problems on websites, electronic mailing lists, and social media debates (TBD, 2010). In the literature of computer ethics, ethical issues related to information technologies are classified as follows:

- Privacy,

- Intellectual property, copyright, license agreements, patents,
- Security and quality,
- Accuracy,
- Freedom of expression,
- Digital divide,
- Cyberbullying

(Mason, 1986; Johnson, 2009; Dedeoğlu, 2006; Duymaz, 2013; Himma and Tavani, 2008; Reynolds, 2009; Uysal and Odabaşı, 2006).

The principles of computer ethics were first formulated by the Computer Ethics Institute (CEI) in 1972 under the name "Ten Commandments of Computer Ethics" and are considered a significant step in the field of computer ethics (Kallman and Grillo, 1996). These principles were developed to regulate the ethical use and misuse of information technologies.

Internationally, the Computer Ethics Institute (CEI) and the British Computer Society (BCS) are among the influential organizations in the field of computer ethics. In Turkey, the Turkey Informatics Foundation (TBV), the Turkey Informatics Association (TBD), and the Turkey Informatics Industry Association (TÜBİDER) are important organizations working in this field (Dedeoğlu, 2006).

The 10 fundamental principles of computer ethics developed by the CEI are important values that should be instilled in students in education. These principles aim to prevent the misuse of computers and provide ethical guidance. Particularly, providing education on computer ethics from an early age helps students develop ethical awareness. In Turkey, this education is included in the Computer Technologies and Software course at the middle school level.

This approach emphasizes the importance of developing social awareness and responsibility regarding the ethical use of information technologies. The ethical use of computers and information technologies is an important issue that individuals need to learn consciously from an early age. The imparting of this ethical awareness and consciousness, especially at a young age, is of great importance for internalizing ethical values among students (Çelen, 2012; Duymaz, 2013).

In Turkey, education on computer ethics is currently provided within the Computer Technologies and Software course at the middle school level. This approach emphasizes that directly and comprehensively conveying the concept of computer ethics to students is effective in the development of ethical awareness.

Studies such as those by Beyhan and Tunç (2012), Duymaz (2013), Ghazali (2003), Genç, Kazez, and Fidan (2013), Haines and Leonard (2007), Kuzu (2009), Masrom et al. (2010), Namlu and Odabaşı (2007), Uysal (2006), and Uysal and Odabaşı (2007) have provided important data on students' unethical behaviors. However, it is observed that the issue of computer ethics in higher education curricula is inadequately addressed in these studies.

Therefore, there is a need to more accurately define the knowledge and skills that higher education students need to develop regarding computer ethics and to redesign the curriculum to meet these needs. The findings of such research can provide important guidance for improving curricula and making computer ethics education more effective.

The main objective of this study is to examine the ethical views and attitudes of higher education students towards the use of information technologies in terms of various demographic characteristics. In line with this aim, we aim to answer the following questions:

1. How are the ethical views and attitudes scores of participants according to four different scenarios?
2. Is there a significant relationship among them?
3. Does it show a significant difference according to gender?
4. Does it show a significant difference according to income perception?
5. Does it show a significant difference according to class level?
6. Does it show a significant difference according to the enrolled undergraduate program?

2. Method

2.1 Research Design

In this study, a general survey model was used as the quantitative research design. This model aims to achieve a general understanding in a broad research universe. The general survey model is used especially to obtain general information about a specific topic or to understand a phenomenon. This model aims to provide a general overview rather than searching for specific or detailed answers. The events, situations, objects, or individuals examined in the research were attempted to be described in detail within their own conditions. The researcher proceeded by observing and determining the current situation without interventions such as influencing or changing it (McMillan and Schumacher, 2010; Karasar, 2004). The method and principles specified by Karasar (2004) were adopted in this study.

2.2 Study Group

While the population of the study consists of students of Erzincan Binali Yıldırım University Faculty of Education, the sample group consists of university students studying in various fields of the Faculty of Education during the Spring semester of the 2022-2023 Academic Year. Of these students, 106 are female and 250 are male, and they participated in the research voluntarily.

2.3 Data Collection Tools

For the purpose of data collection, a information form created by the researchers and the Scenarios of Real Life Situations with Information Ethics (RLSSIE) Scale were used. The information form includes questions about the student's gender, Faculty/School, Department/Main Discipline, class, internet access, and economic situation perception. RLSSIE, developed by Yoon (2011), was adapted into Turkish by Arıkan and Duymaz (2014). The original scale consists of 17 items and is a seven-point Likert-type scale. The items in the scale are structured in a five-point Likert type. Table 1 provides the internal consistency coefficients of the adapted scale with the original.

Tablo 1. *Internal Consistency Coefficients for RLSSIE Scale Scenarios*

Scenarios	Item Count	Cronbach's Alpha		
		Current Implementation	Turkish Adaptation (Arıkan & Duymaz, 2014)	Original Scale (Yoon, 2011)
Scenario 1	17	.949	.919	.773 - .939
Scenario 2	17	.950	.815	.722 - .940
Scenario 3	17	.937	.884	.824 - .968
Scenario 4	17	.959	.965	.787 - .954

The internal consistency coefficients (Cronbach's Alpha) found in the original scale and the current application are shown in Table 1. The calculated internal consistency coefficients for the current application were found to be .937 for Scenario 1, .952 for Scenario 2, .948 for Scenario 3, and .987 for Scenario 4. It is understood that the obtained internal consistency coefficients are at an acceptable level (Murphy & Davidshofer, 1988), indicating their usability in answering the research questions.

Four different scenarios were utilized, each representing ethical dilemmas encountered in the real-world context of the Internet. In creating these scenarios, initially, scenarios used in IS ethics studies were analyzed (Banerjee et al., 1998; Chow, 2001; Leonard & Cronan, 2001). Subsequently, visits to newspaper websites and obtaining education from Internet ethics websites were conducted to gather ideas and data. Based on these ideas and data, four separate scenarios were developed. The created scenarios were reviewed by ethics professors and subjected to adjustments based on their recommendations.

Scenario 1 addresses privacy violation.

Scenario 2 involves the spread of unhealthy materials, particularly explicit content. This scenario was adapted from scenarios used by Zippy (2024) for teaching Internet ethics.

Scenario 3 deals with the situation of software piracy as an infringement of intellectual property.

Scenario 4 focuses on the dissemination of false information over the Internet.

2.4. Statistical Analysis

During the data analysis process, independent samples t-test was employed for comparing binary groups. Additionally, one-way ANOVA test was applied to assess the mean differences among three or more groups. Upon detecting significant differences from these statistical analyses, Tukey test was utilized to determine which groups the differences were statistically significant between.

3. Findings

Descriptive statistics regarding the demographic characteristics of the participants are presented in Table 2.

Table 2. *Descriptive statistics on participants' characteristics*

Measurement	Value	Frequency (%)
Gender	Female	106 (29.8)
	Male	250 (70.2)
Income Perception	Very Good + Good	64 (18.0)
	Medium	247 (69.4)
	Very Poor + Poor	45 (12.6)

Class Level	1st Year	136 (38.2)
	2nd Year	64 (18.0)
	3rd Year	69 (19.4)
	4th Year	87 (24.4)
Undergraduate Program	Classroom Teaching	150 (42.1)
	Primary Mathematics Teacher Education	77 (21.6)
	Turkish Language Teaching	16 (4.5)
	Preschool Education	79 (22.2)
	Social Studies Teacher Education	26 (7.3)
	Science Teacher Education	8 (2.2)

A total of 356 students participated in the study, with 250 being male and 106 being female. Participants' income perceptions were categorized as follows: those perceiving their income as "Very Good" or "Good" (18.0%), those perceiving it as "Average" (69.4%), and those perceiving it as "Very Poor" or "Poor" (12.6%). Regarding class levels, participants were distributed as follows: 1st-year students (38.2%), 2nd-year students (18.0%), 3rd-year students (19.4%), and 4th-year students (24.4%). The distribution of participants according to their registered undergraduate programs is as follows: Class Teaching program (42.1%), Elementary Mathematics Teaching program (21.6%), Turkish Language Teaching program (4.5%), Preschool Education program (22.2%), Social Studies Teaching program (7.3%), and Science Education program (2.2%).

Table 3. *Descriptive statistics for participants' ethical views and attitude scores for the four different scenarios*

	N	**Minimum**	**Maximum**	**$\bar{X}$**	**Sd**
Scenario 1	356	37	85	75.51	9.018
Scenario 2	356	21	85	71.29	11.666
Scenario 3	356	41	85	70.47	11.456
Scenario 4	356	17	85	72.90	18.053

Descriptive statistics regarding participants' ethical views and attitude scores for the four different scenarios are presented in Table 3. Scores ranging from 17 to 85 were assigned for the 17 items on the scale. Participant scores are distributed as follows: for Scenario 1, they range from 37 to 85, for Scenario 2, they range from 21 to 85. Scenario 3 scores range from 41 to 85, while Scenario 4 scores vary between 17 and 85. The mean scores are as follows: 75.51 for Scenario 1, 71.29 for Scenario 2, 70.47 for Scenario 3, and 72.90 for Scenario 4. These scores being close to the highest score of 85 indicate that participants generally possess high ethical views and attitudes.

Table 4. *Correlation Between Ethical Views and Scenario-Based Attitude Scores*

		Scenario 1	Scenario 2	Scenario 3	Scenario 4
Scenario 1	Correlation	1			
	Significance				
	N	356			
Scenario 2	Correlation	.224**	1		
	Significance	.000			
	N	356	356		
Scenario 3	Correlation	.395**	.516**	1	
	Significance	.000	.000		
	N	356	356	356	
Scenario 4	Correlation	.027	.087	.091	1
	Significance	.611	.099	.088	
	N	356	356	356	356

** Correlation is significant at the 0.01 level.

The results of the simple correlation analysis conducted to assess the relationship between participants' ethical views and attitude scores for different scenarios are presented in Table 4. According to these results, a positive correlation is observed between Scenario 1 and Scenario 2, although this correlation is found to be weak. There is also a positive correlation between Scenario 1 and Scenario 3; however, this relationship is at a low level. On the other hand, a positive correlation is identified between Scenario 2 and Scenario 3, which is at a moderate level.

Table 5. *Results of independent samples t-test for participants' ethical views and attitude scores according to gender*

	Gender	N	$\bar{X}$	Sd	df	t	p
Scenario 1	Female	106	73.17	10.667	354	-3.228	.001*
	Male	250	76.50	8.041			
Scenario 2	Female	106	67.64	11.979	354	-3.918	.000*
	Male	250	72.84	11.201			
Scenario 3	Female	106	66.13	11.150	354	-4.793	.000*
	Male	250	72.31	11.103			
Scenario 4	Female	106	83.45	24.259	354	-0.119	.905
	Male	250	83.79	24.655			

*p<0.01

The independent samples t-test results for ethical views and attitudes scores according to gender are presented in Table 5. For Scenario 1, it was found that the ethical views and attitudes scores of male participants (76.50) were significantly higher than those of female participants (73.17) ($t_{(354)} = -3.228$, $p < 0.01$). Similarly, for Scenario 2, the ethical views and attitudes scores of male participants (72.84) were significantly higher than those of female participants (67.64) ($t_{(354)} = -3.918$, $p < 0.01$). Likewise, for Scenario 3, the ethical views and attitudes scores of male participants (72.31) were significantly higher than those of female participants (66.13) ($t_{(354)} = -4.793$, $p < 0.01$).

However, for Scenario 4, there was no significant difference between the ethical views and attitudes scores of male participants (83.79) and female participants (83.45) ($t_{(354)} = -0.119$, $p > 0.05$). Based on this result, it can be said that gender is a variable influencing ethical views and attitudes scores in all scenarios except Scenario 4.

Table 6. *One-Way ANOVA Results for Ethical Views and Attitude Scores by Perceived Income Status.*

	Source	Sum of Squares	df	Mean Square	F	p	Tukey
Scenario 1	Between Groups	432.15	2	216.075	2.682	0.070	
	Within Groups	28438.82	353	80.563			
	Total	28870.98	355				
Scenario 2	Between Groups	875.07	2	437.533	3.256	0.040*	Good-Very Poor
	Within Groups	47442.13	353	134.397			
	Total	48317.2	355				
Scenario 3	Between Groups	703.54	2	351.770	2.706	0.068	
	Within Groups	45883.12	353	129.981			
	Total	46586.66	355				
Scenario 4	Between Groups	539.76	2	269.878	0.448	0.639	
	Within Groups	212618.26	353	602.318			
	Total	213158.01					

*p<.05

The one-way ANOVA test results regarding ethical views and attitudes scores according to participants' perceived income status are presented in Table 6. No significant difference was found between participants' perceived income status and ethical views and attitudes scores for Scenarios 1, 3, and 4. However, a significant difference was observed between participants' perceived income status and ethical views and attitudes scores for Scenario 2 [$F_{(2, 353)} = 3.256$, $p < 0.05$].

According to the Tukey test results, participants' perceived income status was significantly higher between "good" and "very poor-poor".

Table 7. *One-Way ANOVA Results for Ethical Views and Attitude Scores by Class Level*

	Source	Sum of Squares	df	Mean Square	F	p	Tukey
Scenario 1	Between Groups	957.455	3	319.152	4.025	0.008*	1st -4th Year, 3rd-4th Year
	Within Groups	27913.519	352	79.300			
	Total	28870.975	355				
Scenario 2	Between Groups	1194.542	3	398.181	2.974	0.032*	1st -3rd Year, 3rd-4th Year
	Within Groups	47122.657	352	133.871			
	Total	48317.199	355				
Scenario 3	Between Groups	604.534	3	201.511	1.543	0.203	
	Within Groups	45982.126	352	130.631			
	Total	46586.660	355				
Scenario 4	Between Groups	600.196	3	200.065	0.331	0.803	
	Within Groups	212557.815	352	603.857			
	Total	213158.011	355				

*p<.05

Table 7 presents the results of the one-way ANOVA test regarding ethical views and attitudes scores according to participants' class levels. For Scenario 1, a significant difference was found between participants' class levels and ethical views and attitudes scores [$F_{(2, 353)} = 4.025$, $p < 0.05$]. According to the Tukey test results, participants' class levels were significantly higher between "1st Year" and "4th Year" and between "3rd Year" and "4th Year".

For Scenario 2, a significant difference was observed between participants' class levels and ethical views and attitudes scores [$F_{(2, 353)} = 2.974$, $p < 0.05$]. According to the Tukey test results, participants' class levels were significantly higher between "1st Year" and "3rd Year" and between "3rd Year" and "4th Year".

However, no significant difference was found between participants' class levels and ethical views and attitudes scores for Scenario 3 and Scenario 4.

Table 8. *One-Way ANOVA Results for Ethical Views and Attitude Scores by Undergraduate Program*

	Source	Sum of Squares	df	Mean Square	F	p	Tukey
Scenario 1	Between Groups	630.362	5	126.072	1.562	0.170	
	Within Groups	28240.613	350	80.687			
	Total	28870.975	355				
Scenario 2	Between Groups	935.839	5	187.168	1.383	0.230	
	Within Groups	47381.361	350	135.375			
	Total	48317.199	355				
Scenario 3	Between Groups	361.959	5	72.392	0.548	0.740	
	Within Groups	46224.701	350	132.071			
	Total	46586.660	355				
Scenario 4	Between Groups	4683.194	5	936.639	1.572	0.167	
	Within Groups	208474.817	350	595.642			
	Total	213158.011	355				

$p>.05$

The results of the one-way ANOVA test regarding ethical views and attitudes scores according to participants' enrolled undergraduate programs are presented in Table 8. For all scenarios (Scenario 1 [$F_{(2, 353)} = 1.562$, $p > 0.05$], Scenario 2 [$F_{(2, 353)} = 1.383$, $p > 0.05$], Scenario 3 [$F_{(2, 353)} = 0.548$, $p > 0.05$], and Scenario 4 [$F_{(2, 353)} = 1.572$, $p > 0.05$]), it was observed that the difference in ethical views and attitudes scores according to participants' enrolled undergraduate programs was not statistically significant. Based on these results, it can be concluded that participants' enrolled undergraduate programs are not a significant variable affecting their ethical views and attitudes.

4. Results, Discussion, and Recommendations

Information technologies have altered the way individuals, organizations, and society interact and exchange information. The topic of ethics is often either absent or underrepresented in discussions at various national and international conferences on Information Systems and Technologies (IST). This study aims to examine undergraduate students' ethical views and attitudes regarding the use of information technologies from various demographic perspectives.

The level of ethical views and attitudes among participants is found to be high according to the research findings. These results parallel previous studies (Erdem, 2008; Morgan & Neal, 2011; Çelen, 2012; Duymaz, 2013; Çelen & Seferoğlu, 2016; Bayra & Baysan, 2022).

Additionally, participants' ethical views and attitudes levels were found to be high across all scenarios used in the research (Scenario 1 "privacy breach", Scenario 2 "Dissemination of unhealthy materials - sexual content", Scenario 3 "Intellectual property violation", and Scenario 4 "Dissemination of false information") (Bayra & Baysan, 2022).

Based on the gender-based result analysis, a significant difference in favor of male participants was observed for Scenario 1, Scenario 2, and Scenario 3. These results indicate that male participants have higher ethical views and attitudes levels compared to female participants, which is consistent with previous studies (Uysal, 2006; Akbulut et al., 2008; Morgan & Neal, 2011; Cavalcante, 2021).

Demographic variables—particularly gender—appear to play a notable role in shaping perceptions of computer ethics. Several studies have identified gender-based differences in ethical evaluations, with some suggesting that male students tend to score higher in certain computer ethics scenarios. Contrarily, Tozdan and Keleş (2022) reported that female students in the 7th and 8th grades demonstrated significantly higher ethical attitude levels than their male counterparts. Similarly, Borkowski and Ugras (1992) observed that male participants tended to adopt more neutral stances on specific ethical issues compared to females. However, findings in the literature are not uniform. For instance, Fritzsche (1988) and McNichols and Zimmerer (1985) found no statistically significant differences based on gender. Chonko and Hunt (1985), on the other hand, noted that while women appeared to be more aware of ethical concerns, this did not necessarily translate into more ethical behavior. Further, Miesling and Preble (1985), along with Betz et al. (1989), concluded that women generally exhibited more ethically inclined judgments than men.

Furthermore, Bayra and Baysan's (2022) study indicates that the level of information technology education among secondary school students is higher for females. On the other hand, Duymaz (2013) suggests that students demonstrate a positive attitude towards information technology ethics, and no significant difference is found between genders in this regard. In this context, references to studies in the literature indicating that female participants' ethical views and attitudes towards information technology are high have also been made (Ünlü & Öz, 2024; Erdem, 2008; Söylemez & Balaman, 2015; Gökçearslan et al., 2015; Murugesan & Woodcock, 2006; Schinzel, 2018; Adam, 2001; Nachouki, Ammar & Naaj, 2019; Adam, 2000; Spake, Crown & Franke, 1997).

In conclusion, gender factors could be considered in the planning stage of course activities based on ethical views and attitudes. When examining ethical views and attitudes scores according to participants' perceived income status, a significant difference was only found for Scenario 2. This difference was determined to be between the perceived income statuses of "good" and "very poor-poor". No significant difference was found between perceived income status and ethical views and attitudes scores for other scenarios (Scenario 1, Scenario 3, and Scenario 4). This result indicates that there is no significant relationship between perceived income status and information technology ethics.

This issue is also addressed in Erdem's (2008) thesis titled "evaluation of teacher candidates' use of information technologies from an ethical perspective". Erdem's study suggests that perceived income status is not a determining factor in teacher candidates' views on computer ethics.

The relationship between information technology ethics and perceived income status is a complex issue involving multiple factors. Among these factors are income level, education, unequal opportunities, and awareness. Particularly, individuals from low-income backgrounds may have limited financial resources for accessing technological resources. This could negatively impact children's access to computers, internet, and other technological resources.

Education and awareness are crucial for understanding and implementing information technology ethics. However, a lack of awareness about ethical issues is more common among low-income families. Therefore, information technology ethics education programs should focus on the specific needs of low-income communities. Further research and analysis in this area could help us better understand the relationship between information technology ethics and perceived income status. Understanding the role of income level, education level, and awareness of ethical issues in this relationship is important for social equity and justice.

When considering ethical views and attitudes scores according to participants' class levels, a significant difference was found for Scenario 1 and Scenario 2. Specifically, for Scenario 1 (Privacy breach), a relationship was observed between the 1st and 4th grades and between the 3rd and 4th grades. Similarly, for Scenario 2 (Dissemination of unhealthy materials - sexual content), a relationship was found between the 1st and 3rd grades and between the 3rd and 4th grades.

It is observed that as the class level increases, the ethical views and attitudes scores increase. Especially, participants in higher grades have higher ethical views and attitudes scores compared to other class levels. Similar results have been found in previous studies. For example, in a study by Masrom and Ismail (2008), a significant difference was found between the 8th grade and the 5th grade and between the 8th grade and the 7th grade among middle school students. This difference could be associated with differences in educational content between classes.

On the other hand, in a study conducted by Erdem (2008), no significant difference was found between class levels and internet ethics attitudes. Similarly, Tosun, Geçer, and Kaşıkçı (2016) did not find a significant difference between class levels and internet ethics. These different results may be related to variables such as the age range of the research samples or differences in course content. In this context, it is considered beneficial to further investigate and analyze this variable. Future studies should examine the relationship between class level and ethical views and attitudes in more detail.

No significant difference was found in ethical views and attitudes scores according to participants' enrolled undergraduate programs, similar to the findings of Tosun, Geçer, and Kaşıkçı (2016). However, Erdem (2008) found that the behaviors of teacher candidates in using information technologies differed significantly according to their departments, especially in terms of Intellectual Property and Security and Quality factors. Erdem's study found that Computer and Instructional Technologies Education (CITE) and Social Studies teacher candidates exhibited more unethical behaviors than other participating teacher candidates in both factors.

The results of the four different scenarios examined in the study indicate problems related to "lack of sufficient knowledge about ethical issues" and "lack of sufficient knowledge about legal responsibilities". In this context, it is recommended that every individual receives education on ethical issues from elementary school onwards. This way, potential disadvantages such as security threats and ethical dilemmas that individuals may encounter during the use of computer and internet technologies can be minimized.

Providing training to teachers in schools on how to use computer and internet technologies ethically, efficiently, and ethically could be an important step. Additionally, in higher education institutions where computer teacher candidates are trained, it is recommended to emphasize ethics and related topics more in the content of courses related to Information and Communication Technologies (ICT). This way, individuals can be encouraged to be more conscious and respectful of ethical values during technology use.

References

Adam, A. (2000). Gender and computer ethics. *SIGCAS Comput. Soc.*, 30, 17-24. https://doi.org/10.1145/572260.572265.

Adam, A. (2001). Computer ethics in a different voice. *Inf. Organ.*, 11, 235-261. https://doi.org/10.1016/S1471-7727(01)00006-9.

Akarsu. B. (1970). *Ahlak Öğretileri-I Mutluluk Ahlakı* (Eudaimonism). İÜEF Yay.. İstanbul.

Akbulut Y., Uysal Ö., Odabasi H.F., Kuzu A. (2008). Influence of gender, program of studyand PC experience on unethical computer using behaviors of Turkish undergraduatestudents. Computers & Education, 51 (2), pp. 485–492.

Arıkan. Y.D.. Duymaz. S.H. (2014). Gerçek Yaşam Durum Senaryolarıyla Bilişim Etiği Ölçeği'ni Türkçeye Uyarlama Çalışması. *Ege Eğitim Dergisi. 15*(1) . 318-337. https://doi.org/10.12984/eed.55518

Banerjee. D.. Cronan. T. P.. & Jones. T. W. (1998). Modeling IT Ethics: A Study in Situational Ethics. *MIS Quarterly. 22*(1). 31–60. https://doi.org/10.2307/249677

Bayra, E., & Baysan, E. (2022). Gerçek yaşam durumu senaryolarıyla ortaöğretim öğrencilerinin bilişim etiği düzeylerinin bazı değişkenler açısından incelenmesi. *Gazi Eğitim Bilimleri Dergisi, 8*(1), 82-107. https://doi.org/10.30855/gjes.2022.08.01.006.

Betz, M., O'Connell, L., & Shepard, J. M. (1989). Gender differences in proclivity for unethical behavior. Journal of business ethics, 8, 321-324. https://doi.org/10.1007/BF00381722

Beyhan, Ö. ve Tunç, H. S. (2012). Öğretmen adayı öğrencilerin bilişim teknolojilerini etik kullanımlarının incelenmesi. *Yükseköğretim Dergisi, 2*(2), 85-94.

Borkowski, S.C. & Ugras, Y.J. (1992). The ethical attitudes of students as a function of age, sex and experience. *J Bus Ethics, 11*, 961–979. https://doi.org/10.1007/BF00871962

Cavalcante, M. F. B. (2021). Tomada de Decisão Ética Em Tecnologias e Sistemas de Informação (Order No. 30228803). Available from ProQuest Dissertations & Theses Global. (2778644525). https://www.proquest.com/dissertations-theses/tomada-de-decisão-ética-em-tecnologias-e-sistemas/docview/2778644525/se-2

Çelen, F. K. (2012). *Bilgi ve iletişim teknolojilerinin kullanımında ilköğretim öğrencilerinin etik olmayan davranışlara ilişkin görüşlerinin incelenmesi.* Yayınlanmamış Yüksek Lisans Tezi, Hacettepe Üniversitesi, Ankara.

Çelen, F. K., & Seferoğlu, S. S. (2016). Bilgi ve iletişim teknolojilerinin kullanımı ve etik olmayan davranışlar: Sorunlar, araştırmalar ve değerlendirmeler. *Journal of Computer and Education Research, 4*(8), 124-153. Cevizci. A.(2008). *Etiğe Giriş*. İstanbul: Engin Yayıncılık.

Cerrah, İ. (2002). Bilişim teknolojileri ve etik: Bilişim teknolojilerinin güvenlik hizmetlerinde kullanımının ”etik boyutu” ve “sosyal sonuçları”. *Polis Bilimleri Dergisi, 4*(1-2), 137-155.

Cevizci, A. (2008). *Etiğe Giriş.* İstanbul: Paradigma Yayıncılık.

Chonko, L. B., & Hunt, S. D. (1985). Ethics and Marketing Management: An Empirical Examination. *Journal of Business Research, 13*, 339-359. https://doi.org/10.1016/0148- 2963(85)90006-2

Chow, W. S. (2001). Ethical belief and behavior of managers using information technology for decision making in Hong Kong. *Journal of Managerial Psychology, 16*(4), 258–267.

Dedeoğlu, G. (2006). *Bilişim Toplumu ve Etik Sorunlar*. Bursa: Alfa Aktüel Yayınları.

Duymaz, S. H. (2013). *Ortaokul öğrencilerine yönelik “Bilişim Etiği Öğretim Programı” uygulaması.* Yayınlanmamış Yüksek Lisans Tezi, Ege Üniversitesi, İzmir.

Erdem, Z. (2008). *Öğretmen adaylarının bilişim teknolojilerini kullanımlarının etik açıdan değerlendirilmesi.* Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, İzmir.

Fritzsche, D. J. (1988). An examination of marketing ethics: Role of the decision maker, consequences of the decision, management position, and sex of the respondent. Journal of Macromarketing, 8(2), 29-39. https://doi.org/10.1177/027614678800800205

Genç, Z., Kazez, H. ve Fidan, A. (2013). Üniversite öğrencilerinin etik dışı davranışlarının belirlenmesi. Akademik Bilişim Konferansları, 23-25 Ocak 2013 Akdeniz Üniversitesi.

Ghazali, H. (2003). *Examining high-school student’s views on computer and information ethics.* Unpublished doctoral thesis. Manhattan Kansas State University College of Education.

Gökçearslan, Ş., Günbatar, M. S., & Berikan, B. (2015). Ortaokul öğrencilerinde bilişim etiği: gerçek yaşam durumu senaryolarıyla bir değerlendirme. *Ege Eğitim Dergisi, 16*(2), 254-273.

Haines, R.P., & Leonard, L.N. (2007). Individual characteristics and ethical decision-making in an IT context. *Ind. Manag. Data Syst., 107*, 5-20.

Himma K. E. ve Tavani, H. T. (2008). *The handbook of information and computer ethics.* New Jersey: Wiley Sonc Inc.

Internet Users by Country (2016), *Internet Live Stats*, https://www.internetlivestats.com/internet-users-by-country/

Johnson, D. G. (2009). *Computer Ethics (4th edition),* New Jersey: Pearson Education

Kallman, E. A. ve Grillo, J. P. (1996) *Ethical decision making and information technology (2nd edition)* Boston, Massachusetts: Irwin/McGraw-Hill.

Karasar. N. (2004). *Bilimsel Araştırma Yöntemi* (15. Baskı). Ankara: Nobel Yayın Dağıtım.

Kuzu, A. (2009). Problems telated to computer ethics: Origins of the problems and suggested solutions. *The Turkish Online Journal of Educational Technology, 8*(2), 91-110.

Leonard, L. N. K., & Cronan, T. P. (2001). Illegal, inappropriate, and unethical behavior in an information technology context: A study to explain influences. *Journal of the Association for Information Systems, 1*(12), 1–31.

Mason, R. O. (1986). Four ethical issues of information age. *MIS Quarterly, 10* (1), 5-12.

Masrom, M., & Ismail, Z. (2008). *Computer ethics awareness among undergraduate students in Malaysian higher education institutions*. ACIS 2008 Proceedings, 41.Christchurch, Australia.

Masrom, M., Ismail, Z., Anuar, R. N., Hussein, R. ve Mohamed, N. (2010). Analyzing accuracy and accessibility in information and communication technology ethical scenario context. *American Journal of Economics and Business Administration, 3*(2), 370-376.

McMillan, J. H. & Schumacher, S. (2010). *Research in education: Evidence-based inquiry (7th ed.).* New York, NY: Pearson.

McNichols, C. W., & Zimmerer, T. W. (1985). Situational ethics: An empirical study of differentiators of student attitudes. Journal of business ethics, 4, 175-180. https://doi.org/10.1007/bf00705616

Miesing, P., & Preble, J. F. (1985). A comparison of five business philosophies. Journal of business ethics, 4, 465-476. https://doi.org/10.1007/bf00382609

Moor. J. H. (1985). What is computer ethics?. *Journal of Metaphilosopy. 16* (4). 266-275.

Morgan, J., & Neal, G. (2011). Student assessments of information systems related ethical situations: Do gender and class level matter? *Journal of Legal, Ethical and Regulatory Issues, 14*(1), 113–130.

Murphy, K.R., & Davidshofer, C.O. (1988). *Psychological Testing: Principles and Applications.* Prentice-Hall, Englewood Cliffs, N.J.

Murugesan, S., & Woodcock, L. (2006). Gender Differences in Ethics Perceptions in Information Technology. , 543-549. https://doi.org/10.4018/978-1-59140-815-4.CH084.

Nachouki, M., Ammar, K., & Naaj, M. (2019). Factors Influencing Plagiarism and Collusion in Programming Assignments. *2019 18th International Conference on Information Technology Based Higher Education and Training (ITHET)*, 1-7. https://doi.org/10.1109/ithet46829.2019.8937362.

Namlu, A. G. ve Odabaşı, H. F. (2007). Unethical computer using behavior scale: A study of reliability and validity on Turkish university students. *Computers & Education, 48*, 205–215.

Özlem. D. (2017). *Etik*. İstanbul. Notos Yayınları.

Pieper. A. (1999). *Etiğe Giriş*. V.Atayman ve G. Sezer (Çev.). İstanbul: Ayrıntı Yayınları.

Raven. M. (2018). *Our Rapidly Increasing Consumption of Technology and Data. Medium.* https://medium.com/@micrv/our-rapidly-increasing-consumption-of-technology-and-data-ab363ed71b23

Reynolds, G. W. (2009). *Ethics in information technology (3rd Edition).* Boston: CourseTechnology

Reynolds, R., & Ninomiya, A. (2019). The Digital Divide: A Comparative Analysis of Online Privacy Concerns and the Moderating Role of Social Media Use between Low and High Income Groups. Proceedings of the 52nd Hawaii International Conference on System Sciences.

Schinzel, B. (2018). Gendered Views on the Ethics of Computer Professionals. , 121-134. https://doi.org/10.30965/9783846742006_010.

Sevindik, T. (2011). *Bilişim ve etik ders notları.* http://www.yarbis.yildiz.edu.tr/web/userAnnouncementsFiles/dosya2f00c8b17de373c9f729e1440b895329.pdf

Söylemez, M., & Balaman, F. (2015). Bilişimin etik olarak kullanımının çeşitli değişkenler açısından incelenmesi. *Elektronik Sosyal Bilimler Dergisi, 14*(54), 115-128.

Spake, D., Crown, D., & Franke, G. (1997). Gender differences in ethical perceptions of business practices: a social role theory perspective.. *The Journal of applied psychology*, 82 6, 920-34 . https://doi.org/10.1037/0021-9010.82.6.920.

TBD. Türkiye Bilişim Derneği, (2010). *Bilişim etiği nihai rapor*, https://eski.tbd.org.tr/usr_img/kamu_bib/CG2%20Rapor-28.04.2011.pdf

Tepe. H. (2007). "Bir Felsefe Dalı Olarak Etik". *Doğu Batı* **(**Ağustos. Eylül. Ekim 1998**)**. Yıl.1.S.4. s. 11-28.

Tepe. H. (2016). *Pratik Etik*. Ankara. Bilgesu Yayınları.

Tıngöy, Ö. (2009). *Bilişim Çağında Etik.* İstanbul: Avcıol Basım Yayın.

Tosun, N., Geçer, A. ve Kaşıkcı, D. N. (2016). Öğretmen adaylarının internet etiği algıları ve kontrol odağı algıları arasındaki ilişkinin incelenmesi. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi, 2*(4), 82-103.

Tozdan, N., & Keleş, Ö. (2022). Investigation of 7th and 8th Grade Middle School Students' Environmental Ethics Attitude Levels in Relation to Different Variables. *Science Insights Education Frontiers, 13*(1), 1763–1775. https://doi.org/10.15354/sief.22.or064

TUIK. Türkiye İstatistik Kurumu (2022). *Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması.* https://data.tuik.gov.tr/Bulten/Index?p=Survey-on-Information-and-Communication-Technology-(ICT)-Usage-in-Households-and-by-Individuals-2022-45587

Ünlü, L., & Öz, R. (2024). Behind the Computer Screen: Perspectives on Information Ethics among Music Education Students. *Advanced Education*, *24*, 130-150.Warschauer, M. (2004). *Technology and Social Inclusion: Rethinking the Digital Divide*. The MIT Press.

Uysal, Ö. (2006). *Öğretmen Adaylarının Bilgisayar Etiğine İlişkin Görüşleri.* Yayımlanmamış Yüksek Lisans Tezi. Anadolu Üniversitesi, Eğitim Bilimleri Enstitüsü.

Uysal, Ö. ve Odabaşı, F. (2006). Bilgisayar etiği öğretimde kullanılan yöntemler. VI. International Education Technology Conference, 1639-1652.

Uysal, Ö. ve Odabaşı, F. (2007). Computer ethics issues. VII. International Education Technology Conference. 03-05 Mayıs 2007, Yakın Doğu Üniversitesi.

Yılmaz. A. (2009). Felsefenin Sunduğu Bir İmkân Olarak Uygulamalı Etik, *Gelenekten Geleceğe*, *5*(19-20), 67-78.

Yoon. C. (2011). Ethical decision-making in the Internet context: Development and test of an initial model based on moral philosophy. *Computers in Human Behavior.* (27). 2401–2409. https://doi.org/10.1016/j.chb.2011.08.007

Zippy Scenarios for Teaching Internet Ethics (2024). Illinois University High School Library. https://www.library.illinois.edu/uni/computerlit/scenarios/

CHAPTER

3

AN EXAMINATION OF UNIVERSITY STUDENTS' CYBERSECURITY ATTITUDES IN RELATION TO DEMOGRAPHIC VARIABLES

Recep ÖZ[1]

Murat Tolga KAYALAR[2]

1 Assoc. Prof. Dr. Recep ÖZ, Erzincan Binali Yıldırım University, Faculty of Education, Department of Computer Education and Instructional Technology, E-mail:recepoz@erzincan.edu.tr, ORCID: 0000-0001-9974-0022

2 Assistant Professor Dr. Murat Tolga KAYALAR, Erzincan Binali Yıldırım University, Faculty of Education, Department of Computer Education and Instructional Technology. E-mail: mtkayalar@erzincan.edu.tr | ORCID: 0000-0003-2442-9330

1. Introduction

The emergence of new technologies, and particularly information technologies (IT), has led to profound transformations in both organizational business processes and individuals' ways of working (Valcour & Hunter, 2005). The era in which documents were manually filed and data were stored in physical filing cabinets has been replaced by the dominance of digital systems. With the widespread adoption of personal computers, local area networks, and the Internet, employee productivity levels have increased, and the transition to digital environments has become an increasingly rapid transformation.

One of the most notable milestones in this digital transformation is the concept of the "Internet of Things (IoT)," introduced by Kevin Ashton in 1999 within the context of supply chain management (Ashton, 2009). Ashton predicted that not only computers but also many physical objects around us could be connected to the Internet. Although this perspective was visionary, it is likely that even Ashton could not have anticipated the magnitude of the number of devices that would eventually be connected to the Internet (Allmendinger, 2020; Dorsey, Martin, Howard & Coovert, 2017; Ramaswamy, Madakam & Tripathi, 2015). Indeed, by 2011, the number of Internet-connected devices worldwide had surpassed the global population, and it was projected that this number would reach 24 billion by 2020 (Nordrum, 2016; Gubbi, Buyya, Marusic & Palaniswami, 2013). The Internet of Things (IoT) is a rapidly growing global phenomenon, with 25 billion connected devices and a projected triple by 2025.

The rapid and widespread nature of technological advancements necessitates that individuals become more aware of security risks in cyberspace. Information security has become a critical domain not only for organizations but also for individuals to sustain their digital lives. Particularly, young individuals such as university students, despite actively using technology, may lack sufficient knowledge and awareness regarding cybersecurity. This situation may expose them to threats such as personal data breaches, identity theft, and online fraud.

Cybersecurity is classified among the new category of technologies known as "exponential technologies" (Aldhaheri, Battah, Tihanyi, Alwahedi, & Ferrag, 2024). Until recently, the pace of technological advancement was explained by Moore's Law, which posits that the processing power of technologies such as personal computing doubles approximately every two years while costs are halved (Schaller, 1997). Alongside technologies like artificial intelligence, robotics, and industrial biology, cybersecurity is also considered an exponential technology whose rate of progress far exceeds the predictions of Moore's Law (Briggs & Shingles, 2015; Dorsey et al., 2017). While exponential technologies enable organizations to achieve their goals faster and increase productivity, they can simultaneously have disruptive effects on the workforce (Arena, 2014; Briggs & Shingles, 2015). Globally, the total cost of cybersecurity breaches to organizations exceeded 315 billion US dollars in 2014 and this figure has been increasing in recent years(Tahmasebi, 2024; Dias, Quaglietta, Nguyen, Dixit, & Nathan, 2023). Considering the potentially devastating financial impacts of cybersecurity on organizations and employees, the need for research in this field has become more important than ever.

In behavioral research on cybersecurity, it is important to clearly distinguish between information security and cybersecurity. As the term implies, the concept of information security primarily focuses on the protection of an organization's information and assets. Von Solms and van Niekerk (2013) provide a very clear distinction between information security and cybersecurity. According to them, cybersecurity encompasses information security while also including the protection of organizational employees. The human factor in cybersecurity should be considered not only because of its role in safeguarding organizational data and intellectual property but also due to the fact that individuals are often the direct targets of cyberattacks.

Social engineering is a fundamental component of the human factor in cybersecurity and is defined as the process of gaining unauthorized access to computer networks through psychological deception, misdirection, or manipulation (Erbschloe, 2005; Abraham & Chengalur-Smith, 2010; Dorsey et al., 2017). Employees of organizations are primary targets of social engineering tactics because they represent the most vulnerable element within cybersecurity systems. Furthermore, for hackers, infiltrating a system via employees is significantly easier and less time-consuming than attempting to bypass an organization's established breach prevention measures (Krombholz, Hovel, Huber, & Weippl, 2014).

In this context, it is essential to examine university students' attitudes towards cybersecurity and to determine the relationship of these attitudes with demographic variables such as gender, age, academic year, daily internet usage, receiving cybersecurity training, and use of Wi-Fi on campus. This study is expected to contribute to enhancing the digital security awareness of the student population and to the development of relevant educational policies.

Purpose of the Study

The purpose of this study is to measure university students' attitudes toward cybersecurity and to determine whether these attitudes differ significantly according to demographic variables such as gender, age, academic year, daily internet usage duration, receiving cybersecurity training, and use of Wi-Fi on campus.

Research Questions / Hypotheses

- What are the general attitudes of university students toward cybersecurity?
- Do cybersecurity attitudes differ significantly by gender?
- Are there differences in cybersecurity attitudes across different age groups?
- Do students' attitudes vary according to their academic year?
- Is there a significant relationship between daily internet usage duration and cybersecurity attitudes?
- Does having received cybersecurity training affect attitudes?
- Does the use of Wi-Fi on campus influence students' attitudes?

2. Method

2.1 Research Design

This study employs a general survey model aimed at achieving a comprehensive understanding of a large data set. Rather than focusing on detailed questions, this model is designed to obtain general information on a specific topic from a broad perspective. The research seeks to describe events and situations within their contexts and to analyze the current state through observation without intervention or manipulation (McMillan & Schumacher, 2010; Karasar, 2004). The study was conducted in accordance with the methods and principles proposed by Karasar (2004).

2.2 Study Group

The population of the study consists of students from the Faculty of Education at Erzincan Binali Yıldırım University, while the sample group includes university students enrolled in various departments of the Faculty of Education during the Spring semester of the 2023-2024 academic year. Among these participants, 666 are female and 210 are male, all of whom took part voluntarily.

2.3 Data Collection Tools

For data collection, an information form prepared by the researchers and the Cybersecurity Attitude Scale (CSAS) were used. The information form includes questions regarding students' gender, age, academic year, daily internet usage duration, and whether they have received cybersecurity training. Developed by Howard (2018), the CSAS consists of 10 items and employs a five-point Likert-type scale. The scale comprises two sub-dimensions: Policy Compliance (5 items) and Perceived Vulnerability (5 items).

2.4 Statistical Analysis

In the data analysis phase, the independent samples t-test was conducted to compare two groups. For comparisons involving three or more groups, a one-way ANOVA was performed. Following the detection of significant differences, the Tukey post hoc test was utilized to identify which specific group differences were statistically significant.

3. Findings

Table 1 provides the internal consistency coefficients of the adapted scale with the original.

Table 1. Internal Consistency Coefficients of CSAS

CSAS	Number of Items (N)	Original Scale	Current Implementation
Policy Compliance	5	0.80	0.945
Perceived Vulnerability	5	0.86	0.905
Total	10	0.85	0.931

The internal consistency (Cronbach's Alpha) was very high for all subscales and the total scale. This indicates that the reliability of the scale is excellent. The obtained value of .931 in the current application demonstrates that the items of the scale are highly consistent with each other and effectively measure the intended construct.

Table 2. Independent Samples Test Results for CSAS Scores by Gender

Gender	N	$\bar{X}$	Ss	df	t	p
Female	666	32.733	9.761	874	2.802	.000*
Male	210	30.467	11.555			
*p < .01						

Table 2 presents the results of the independent samples test for CSAS scores according to participants' gender. Female students' cybersecurity attitude scores were statistically significantly higher than those of male students ($p < .01$). It can be stated that females have higher cybersecurity awareness and compliance compared to males.

Table 3. Descriptive Statistics of Participants' CSAS Scores by Age

Eğitim	**N**	$\bar{X}$	**Ss**
I- 18-20 years	539	31.4267	9.84545
II- 21-23 years	274	32.7007	10.61643
III- 24-27 years	37	33.5405	12.86596
IV- 28 years and above	26	40.6923	5.90437
Total	876	32.1895	10.25852

Table 3 presents the descriptive statistics of participants' Cybersecurity Attitude Scale (CSAS) scores by age groups. The data indicate an increasing trend in average cybersecurity attitude scores with age. The highest score was observed in the group aged 28 years and above (M = 40.69). The mean scores for the other age groups were 18-20 years (M = 31.43), 21-23 years (M = 32.70), and 24-27 years (M = 33.54), respectively. These findings suggest that older participants tend to have more positive attitudes toward cybersecurity.

Table 4. One-Way ANOVA Results for CSAS Scores by Age

Source	**Sum of Squares**	**df**	**Mean Square**	**F**	**p**	**Tukey Post Hoc Test**
Between Groups	2332.501	3	777,500	7,554	.000*	I-IV, II-IV, III-IV
Within Groups	89750.043	872	102,924			
Total	92082.543	875				
*p < .001						

The one-way ANOVA results indicate a statistically significant difference in cybersecurity attitude scores across the different age groups ($F_{(3, 872)} = 7.554$, $p < .01$). Post hoc Tukey tests revealed that the significant differences exist between groups I (18-20 years) and IV (28 years and above), II (21-23 years) and IV, as well as III (24-27 years) and IV. This suggests that participants aged 28 and above have significantly higher cybersecurity attitude scores compared to the younger age groups.

Table 5. Descriptive Statistics of Participants' CSAS Scores by Academic Year

Academic Year	**N**	**$\bar{X}$**	**Ss**
I- 1st Year	553	31.6311	10.09545
II- 2nd Year	236	30.8008	10.52891
III- 3rd Year	43	40.2558	6.74746
IV- 4th Year	25	36.9200	8.51919
V- Graduate (Pedagogical Formation)	19	41.2105	5.71138
Total	876	32.1895	10.25852

Table 5 presents the descriptive statistics of participants' Cybersecurity Attitude Scale (CSAS) scores according to academic year. The results reveal that CSAS scores vary across academic levels. While first- and second-year students have lower mean scores (M = 31.63 and M = 30.80, respectively), third-year students (M = 40.26), fourth-year students (M = 36.92), and graduates in pedagogical formation programs (M = 41.21) exhibit notably higher cybersecurity attitude scores. This suggests that as students progress through their academic careers—or gain additional professional training—their awareness and attitudes toward cybersecurity tend to improve.

Table 6. One-Way ANOVA Results for CSAS Scores by Academic Year

Source	**Sum of Squares**	**df**	**Mean Square**	**F**	**p**	**Tukey Post Hoc Test**
Between Groups	5530,975	4	1382,744	13,915	.000*	I-III,I-V, II-III, II-IV, II-V
Within Groups	86551,569	871	99,370			
Total	92082,543	875				
*p < .001						

The results of the one-way ANOVA revealed a statistically significant difference in CSAS (Cybersecurity Attitude Scale) scores based on academic year ($F_{(4, 871)} = 13.915$, $p < .001$). According to the Tukey post hoc test, significant differences were observed between several groups: first-year students scored significantly lower than third-year and graduate (formation) students; second-year students scored significantly lower than third-year, fourth-year, and graduate students. These findings indicate that students in more advanced academic years tend to have more positive attitudes toward cybersecurity, potentially due to increased exposure to academic or practical experiences over time.

Table 7. Descriptive Statistics of Participants' CSAS Scores by Daily Internet Usage Duration

Daily Internet Usage Duration	**N**	$\bar{X}$	**Ss**
I- 0-1 hour	47	27.9362	11.76103
II- 2-3 hour	226	32.0841	10.13540
III- 4-5 hour	356	32.3427	9.56228
IV- 6 hour and more	247	32.8745	10.88915
Total	876	32.1895	10.25852

Table 7 presents the descriptive statistics of Cybersecurity Attitude Scale (CSAS) scores based on participants' daily internet usage duration. The results suggest that students who spend more time online tend to have higher average scores in cybersecurity attitudes. Participants using the internet for 0–1 hour daily reported the lowest average score (M = 27.94), while those using it for 6 or more hours had the highest average score (M = 32.87). This may indicate that increased exposure to digital environments is associated with greater cybersecurity awareness and attitudes.

Table 8. One-Way ANOVA Results for CSAS Scores by Daily Internet Usage Duration

Source	**Sum of Squares**	**df**	**Mean Square**	**F**	**p**	**Tukey Post Hoc Test**
Between Groups	977,032	3	325,677	3,117	.025*	I-III, I-V
Within Groups	91105,511	872	104,479			
Total	92082,543	875				
*p < .05						

The one-way ANOVA results reveal a statistically significant difference in CSAS (Cybersecurity Attitude Scale) scores according to participants' daily internet usage durations ($F_{(3,\ 872)} = 3.117$, $p < .05$). According to the Tukey post hoc analysis, significant differences were found between participants who use the internet for 0–1 hour daily and those who use it for 4–5 hours (I–III), as well as those who use it for 6 or more hours (I–IV). These findings suggest that students who spend more time online tend to have significantly more positive attitudes toward cybersecurity than those who use the internet less frequently.

Table 9. Independent Samples Test Results for CSAS Scores by Cybersecurity Training

Cybersecurity Training	N	$\bar{X}$	Ss	df	t	p
Yes	106	34,7736	10,72272	874	2.777	.555
No	770	31,8338	10,14875			
p > .05						

As shown in Table 9, an independent samples t-test was conducted to examine whether CSAS scores differed based on whether participants had received cybersecurity training. Although the mean score of those who received training (M = 34.77) was higher than those who did not (M = 31.83), the difference was not statistically significant (t(874) = 2.777, p > .05). This suggests that participation in cybersecurity training did not result in a significant difference in students' cybersecurity attitudes.

Table 10. Independent Samples Test Results for CSAS Scores by School WiFi Usage

School WiFi Usage	N	$\bar{X}$	Ss	df	t	p
Yes	574	32,7526	9,97106	874	2.245	.062
No	302	31,1192	10,71927			
p > .05						

As shown in Table 10, an independent samples t-test was conducted to examine whether participants' CSAS (Cybersecurity Attitude Scale) scores differed based on their use of school WiFi. The results indicate that students who use school WiFi (M = 32.75) had slightly higher cybersecurity attitude scores than those who do not (M = 31.12); however, this difference was not statistically significant (t(874) = 2.245, p > .05). Therefore, the use of school WiFi does not appear to have a meaningful effect on students' cybersecurity attitudes.

4. Discussion and Conclusion

The primary aim of this study was to examine university students' attitudes toward cybersecurity and to determine whether these attitudes vary significantly based on demographic variables such as gender, age, academic year, daily internet usage, prior cybersecurity training, and use of school WiFi. The findings yielded meaningful insights across several variables.

Empirical evidence suggests that female students tend to demonstrate more favorable attitudes and behaviors regarding cybersecurity compared to their male peers. For example, a study conducted among university students in Saudi Arabia indicated that women exhibited stronger cyber hygiene practices and more positive perceptions toward online learning than men. Notably, this gender disparity became more pronounced following the implementation of a cybersecurity education program(Salem & Sobaih, 2023). Comparable trends have been observed in intervention-based studies involving secondary and high school students, where female participants showed greater improvements in cybersecurity self-efficacy relative to their male counterparts(Rao, Amo, Frank, Upadhyaya & Liao, 2019).

Nevertheless, gender-based differences in cybersecurity awareness and knowledge are not uniform across all contexts. In certain national settings, male students have been reported to outperform females in specific cybersecurity competencies. For instance, research involving university students in Sudan revealed that male students had slightly higher levels of cybersecurity awareness(Ahmed & Eltahir, 2023). Similarly, a study conducted in China found that male students were more adept in device and internet usage habits, whereas female students demonstrated greater proficiency in securing their social media presence(Guo & Tınmaz, 2023).

Overall, while female students are generally more cautious and inclined toward secure digital practices, gender-related differences in cybersecurity attitudes and behaviors appear to be influenced by a combination of cultural, educational, and national factors. This variability underscores the need for context-sensitive approaches when developing and implementing cybersecurity education programs(Salem & Sobaih, 2023; Rao, Amo, Frank, Upadhyaya & Liao, 2019; Ahmed & Eltahir, 2023; Guo & Tınmaz, 2023).

Age and academic experience have a significant influence on individuals' attitudes and behaviors toward cybersecurity. Research indicates that older individuals (e.g., those aged 28 and above) tend to exhibit higher levels of awareness and risk perception regarding cyber threats and, consequently, demonstrate more secure online behaviors (Fatokun, Norman, Fatokun & Hamid, 2019; Debb, Schaffer & Colson, 2020; Dixon, Joinson, Briggs, Branley-Bell & Coventry, 2022). This can be attributed to the accumulation of digital experiences and increased risk consciousness over time. Similarly, students in higher academic years or those enrolled in additional educational programs such as pedagogical formation display higher levels of knowledge, attitude, and behavior concerning cybersecurity (An, Kolletar-Zhu, Xu, Zhang & Hong, 2022; Fatokun, Norman, Fatokun & Hamid, 2019). Educational level appears to be a key factor in the development of cybersecurity competence; individuals with higher levels of education generally feel more secure in online environments and engage in more informed digital practices (Bukovec & Antoliš, 2024; Chi, Xu, Liu, Lei, Zhang & Hong, 2022; An, Kolletar-Zhu, Xu, Zhang & Hong, 2022). However, some studies suggest that age alone may not always enhance the sense of online security and, in some cases, perceptions of security may even decline with age (Bukovec & Antoliš, 2024; Dixon, Joinson, Briggs, Branley-Bell & Coventry, 2022). Both academic and professional experiences emerge as critical social determinants that shape individuals' cybersecurity attitudes and behaviors. Indeed, significant changes have also been observed among those who enter the workforce (Chi, Xu, Liu, Lei, Zhang & Hong, 2022; An, Kolletar-Zhu, Xu, Zhang & Hong, 2022). In conclusion, demographic and experiential factors such as age, academic year, and level of education play a crucial role in the development of cybersecurity awareness and secure digital behaviors (Fatokun, Norman, Fatokun & Hamid, 2019; Chi, Xu, Liu, Lei, Zhang & Hong, 2022; Dixon, Joinson, Briggs, Branley-Bell & Coventry, 2022; An, Kolletar-Zhu, Xu, Zhang & Hong, 2022; Debb, Schaffer & Colson, 2020).

Students who reported low levels of daily internet use (0–1 hour) were found to have significantly lower cybersecurity attitude scores. This suggests that limited exposure to online environments may lead to lower awareness of cybersecurity threats and practices. Studies have consistently shown that cybersecurity awareness among students is generally low, and this awareness is especially limited among younger age groups (e.g., ages 8–12), who often lack sufficient knowledge of cybersecurity terminology and common online threats (Tirumala, Pang & Sarrafzadeh, 2016; Erendor & Yildirim, 2022; Altarawneh, Alazzam, Althunibat, Alzriqat & Almajali, 2025). Furthermore, as internet usage increases, the risk of exposure to cyber threats also rises; however, individuals with limited internet use may remain inadequately informed about these risks (Tirumala, Pang & Sarrafzadeh, 2016; Çetin, Klein, Wiechetek, Lesjak, Basım & Zwilling, 2020; Erendor & Yildirim, 2022). Educational programs and practical workshops have been shown to be effective in increasing awareness, helping students recognize cybersecurity risks and develop safer internet practices (Hsiung, Jalil, Ali, Almaayah, Yunus & Zaki, 2024; Altarawneh, Alazzam, Althunibat, Alzriqat & Almajali, 2025). In conclusion, limited internet use can be associated with lower levels of cybersecurity knowledge and awareness. Therefore, it is crucial to implement targeted educational and awareness-raising interventions for groups with low internet engagement (Tirumala, Pang & Sarrafzadeh, 2016; Çetin, Klein, Wiechetek, Lesjak, Basım & Zwilling, 2020; Altarawneh, Alazzam, Althunibat, Alzriqat & Almajali, 2025).

Research shows that cybersecurity education is generally effective in increasing students' knowledge and awareness. However, this improvement does not always translate into statistically significant changes in attitudes and behaviors (Prümmer, van Steen & van den Berg, 2024; Van Den Berg, Prümmer & Van Steen, 2024; Ahmad Zukarnain, Hashim, Muhammad, Mansor & Wan Azib, 2020). Meta-analyses particularly indicate that while educational interventions have strong effects on knowledge and attitudes, their influence on actual behavioral change tends to be more limited (Van Den Berg, Prümmer & Van Steen, 2024). In this regard, game-based and hands-on training methods have been reported to generate more favorable outcomes compared to traditional approaches, by enhancing student engagement and participation (Steen v& Deeleman, 2021; Kim, Tu, Jin, White & Heffron, 2018). Nonetheless, some studies emphasize that current cybersecurity programs may not produce significant shifts in student attitudes due to a lack of practical application (Alruwaili, 2019; Antunes, Silva & Marques, 2021). Furthermore, it has been found that the use of school WiFi does not have a notable effect on students' cybersecurity attitudes; rather, awareness levels are shaped primarily by the individual's knowledge and educational exposure (Altarawneh, Alazzam, Althunibat, Alzriqat & Almajali, 2025; Alanazi, Tootell & Freeman, 2022). In conclusion, to enhance the effectiveness of cybersecurity training, it is recommended that educational content be updated to reflect current threats, interactive and practice-oriented methods be employed, and training programs be made continuous and sustainable (Altarawneh, Alazzam, Althunibat, Alzriqat & Almajali, 2025; Fattah, Wagimin & Nurlia, 2023; Ahmad Zukarnain, Hashim, Muhammad, Mansor & Wan Azib, 2020).

University students' attitudes toward cybersecurity are significantly influenced by various demographic factors, including gender, age, academic level, and internet usage habits. Existing research reveals statistically significant differences in cybersecurity awareness and behaviors between male and female students. Furthermore, variables such as age and level of education also play a critical role in shaping individuals' perceptions of risk and their cybersecurity practices. It has been particularly noted that younger students or those with limited digital skills tend to have lower levels of cybersecurity awareness and are more prone to engaging in unsafe online behaviors (Parikh & Nimbekar, 2023; Bottyán & Bognár, 2024).

Digital habits such as frequency of internet use, social media engagement, and password management directly influence students' cybersecurity awareness and behavioral patterns. For instance, students who are more informed about social media security and password safety tend to demonstrate higher levels of cybersecurity awareness (Alqahtani, 2022; Polas, Sohel-Uz-Zaman, Dey, Chowdhury, Kabir, Ahamed & Fahad, 2024). Additionally, individuals' knowledge, attitudes, and behaviors related to cybersecurity are also shaped by broader social factors such as educational background and work experience (Chi, Xu, Liu, Lei, Zhang & Hong, 2022). Those with prior professional exposure tend to adopt more cautious cybersecurity practices, likely due to increased responsibility and awareness in workplace settings.

On the other hand, university students' perception of cybersecurity risks is often shaped by their self-confidence and belief in their digital competencies. However, this confidence is not always proportional to their actual level of knowledge, potentially leading to overconfidence in managing cyber threats (Debb & McClellan, 2021; Haltinner, Sarathchandra & Lichtenberg, 2016). This highlights the importance of incorporating not only informational content but also self-assessment and risk evaluation components into cybersecurity training programs.

In conclusion, to enhance cybersecurity awareness among university students, it is essential to design and implement tailored training and awareness programs that consider students' demographic characteristics and internet usage behaviors (Bottyán & Bognár, 2024; Adeshola & Oluwajana, 2024; Parikh & Nimbekar, 2023).

In today's digital era, it is increasingly recommended that cybersecurity education be integrated not only as an elective course but also as a fundamental component of the core curriculum across all academic disciplines. As digitalization permeates all aspects of life, cybersecurity has evolved beyond a purely technical concern. It has become a societal necessity requiring all individuals—regardless of their field—to acquire essential knowledge and skills to recognize online threats, protect their digital rights, and adopt secure behaviors. Therefore, cybersecurity curricula should extend beyond technical content to include ethical, psychological, sociological, and especially human-centered elements such as social engineering.

Furthermore, the development of demographic-sensitive cybersecurity awareness strategies—particularly those that are gender- and age-aware—is crucial for tailoring content to meet the diverse needs of student populations. Digital literacy and safe online behaviors should be promoted through a comprehensive approach, beginning at the early stages of academic education, to strengthen students' resilience against digital risks.

Research has shown that incorporating cybersecurity topics into core courses not only increases student engagement and knowledge retention but also enhances the development of digital competencies required by today's job market. Additionally, interdisciplinary and practice-based teaching models contribute to the acquisition of both technical skills and essential soft skills such as communication, teamwork, ethical reasoning, and problem-solving.

In conclusion, integrating cybersecurity education into the foundational curriculum of universities through a holistic and inclusive approach is a vital step toward equipping individuals—and society as a whole—with greater resilience to digital threats.

Ultimately, cybersecurity should not be regarded merely as an individual responsibility but as a crucial component of institutional and societal safety culture. Research and educational efforts in this area are essential for the sustainability of digital societies. Thus, the findings of this study are expected to inform educators, policymakers, and curriculum developers, contributing to the development of more effective and inclusive cybersecurity strategies in higher education.

References

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society, 32*(3), 183-196.

Adeshola, I., & Oluwajana, D. (2024). Assessing cybersecurity awareness among university students: implications for educational interventions. *Journal of Computers in Education*. https://doi.org/10.1007/s40692-024-00346-7.

Ahmad Zukarnain, Z., Hashim, M. Z., Muhammad, N., Mansor, F. A., & Wan Azib, W. N. H. (2020). Impact of training on cybersecurity awareness. *Gading Journal for Science and Technology, 3*(1), 114-120.

Ahmed, O., & Eltahir, M. (2023). Cybersecurity Awareness in African Higher Education Institutions: A Case Study of Sudan. *Information Sciences Letters, 12*(1), 171-183. https://doi.org/10.18576/isl/120113.

Alanazi, M., Tootell, H., & Freeman, M. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Comput. Hum. Behav.*, 136, 107376. https://doi.org/10.1016/j.chb.2022.107376.

Aldhaheri, A., Battah, A., Tihanyi, N., Alwahedi, F., & Ferrag, M. (2024). Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. *Internet of Things and Cyber-Physical Systems.* https://doi.org/10.1016/j.iotcps.2023.12.003.

Allmendinger, G. (2020). The Internet of Things (IoT). *Energy and Analytics*. https://doi.org/10.1201/9781003151944-17.

Alqahtani, M. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences*. https://doi.org/10.3390/app12052589.

Alruwaili, A. (2019). A Review Of The Impact Of Training On Cybersecurity Awareness. *International Journal of Advanced Research in Computer Science*. https://doi.org/10.26483/ijarcs.v10i5.6476.

Altarawneh, M., Alazzam, S., Althunibat, A., Alzriqat, N., & Almajali, M. (2025). Cybersecurity awareness among school students: Exploring influencing factors, legal implications, and knowledge gaps.*International Journal of Innovative Research and Scientific Studies*. https://doi.org/10.53894/ijirss.v8i1.4696.

An, Q., Kolletar-Zhu, K., Xu, X., Zhang, Y., & Hong, W. (2022). How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates. *International Journal of Information Security*, 22, 305 - 317. https://doi.org/10.1007/s10207-022-00637-z.

Antunes, M., Silva, C., & Marques, F. (2021). An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context. *Applied Sciences*. https://doi.org/10.3390/app112311269.

Arena, C. (2014, August 13). 4 Reasons Why Exponential Technologies Are Taking Off. Retrieved March 19, 2025.

Ashton, K. (2009). That 'internet of things' thing. *RFiD Journal, 22*(7), 97-114.

Bottyán, L., & Bognár, L. (2024). Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students. *Education Sciences*. https://doi.org/10.3390/educsci14060588.

Bukovec, M., & Antoliš, K. (2024). The Impact of Age and Education on Cyber Security in Digital Banking. *Medijska istraživanja*. https://doi.org/10.22572/mi.30.2.6.

Çetin, F., Klein, G., Wiechetek, L., Lesjak, D., Basım, H., & Zwilling, M. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 62, 82 - 97. https://doi.org/10.1080/08874417.2020.1712269.

Chi, C., Xu, X., Liu, J., Lei, V., Zhang, Y., & Hong, W. (2022). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Education and Information Technologies*, 28, 439 - 470. https://doi.org/10.1007/s10639-022-11121-5.

Debb, S., & McClellan, M. (2021). Perceived Vulnerability As a Determinant of Increased Risk for Cybersecurity Risk Behavior. *Cyberpsychology, behavior and social networking*, *24*(9), 605-611. https://doi.org/10.1089/cyber.2021.0043.

Debb, S., Schaffer, D., & Colson, D. (2020). A Reverse Digital Divide: Comparing Information Security Behaviors of Generation Y and Generation Z Adults. *International Journal of Cybersecurity Intelligence and Cybercrime*. https://doi.org/10.52306/03010420GXUV5876.

Dias, L., Quaglietta, J., Nguyen, D., Dixit, A., & Nathan, K. (2023). Cybersecurity: Guiding Principles and Risk Management Advice for Healthcare Boards, Senior Leaders and Risk Managers.. Healthcare quarterly, 25 4, 35-40. https://doi.org/10.12927/hcq.2023.27019

Dixon, M., Joinson, A., Briggs, P., Branley-Bell, D., & Coventry, L. (2022). Exploring Age and Gender Differences in ICT Cybersecurity Behaviour. *Human Behavior and Emerging Technologies*. https://doi.org/10.1155/2022/2693080.

Dorsey, D. W., Martin, J., Howard, D. J., & Coovert, M. D. (2017). Cybersecurity issues in selection. In *Handbook of employee selection* (pp. 913-930). Routledge.

Erbschloe, M. (2005). Trojans, worms and spyware. A computer security professional's guide to malicious code, 212.

Erendor, M., & Yildirim, M. (2022). Cybersecurity Awareness in Online Educaton: a Case Study Analysis.*IEEE Access*, PP, 1-1.https://doi.org/10.1109/ACCESS.2022.3171829.

Fatokun, J., Norman, A., Fatokun, F., & Hamid, S. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *Journal of Physics: Conference Series*, 1339. https://doi.org/10.1088/1742-6596/1339/1/012098.

Fattah, A., Wagimin, W., & Nurlia, N. (2023). Enhancing Cybersecurity Awareness among University Students: A Study on the Relationship between Knowledge, Attitude, Behavior, and Training. *JSI: Jurnal Sistem Informasi (E-Journal)*. https://doi.org/10.18495/jsi.v15i1.21812.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.

Guo, H., & Tınmaz, H. (2023). A survey on college students' cybersecurity awareness and education from the perspective of China. *Journal for the Education of Gifted Young Scientists*, *11*(3), 351-367. https://doi.org/10.17478/jegys.1323423.

Haltinner, K., Sarathchandra, D., & Lichtenberg, N. (2016). College Students' Cybersecurity Risk Perceptions, Awareness, and Practices. *2016 Cybersecurity Symposium (CYBERSEC)*, 68-73. https://doi.org/10.1109/CYBERSEC.2016.018.

Howard, D. J. (2018).*Development of the cybersecurity attitudes scale and modeling cybersecurity behavior and its antecedents* (Order No. 10838509). Available from ProQuest Dissertations & Theses Global. (2093821450). Retrieved from https://www.proquest.com/dissertations-theses/development-cybersecurity-attitudes-scale/docview/2093821450/se-2

Hsiung, L., Jalil, M., Ali, N., Almaayah, M., Yunus, F., & Zaki, F. (2024). Cybersecurity Awareness among Secondary School Students Post Covid-19 Pandemic.*Journal of Advanced Research in Applied Sciences and Engineering Technology*. https://doi.org/10.37934/araset.37.1.115127.

Karasar. N. (2004). *Bilimsel Araştırma Yöntemi* (15. Baskı). Ankara: Nobel Yayın Dağıtım.

Kim, T., Tu, M., Jin, G., White, J., & Heffron, J. (2018). Game based Cybersecurity Training for High School Students. *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*. https://doi.org/10.1145/3159450.3159591.

Köse, S., & Ayvacı, H. Ş. (2019). Dijital okuryazarlık düzeyinin akademik başarıya etkisi. *Eğitim Teknolojisi Kuram ve Uygulama, 9*(1), 12-29.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications, 22*, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

McMillan, J. H. & Schumacher, S. (2010). *Research in education: Evidence-based inquiry (7th ed.).* New York, NY: Pearson.

Nordrum, A. (2016). The internet of fewer things [News].*IEEE Spectrum, 53*, 12-13. https://doi.org/10.1109/MSPEC.2016.7572524.

Özgür, H., & Aytekin, G. (2020). Cinsiyet değişkenine göre siber güvenlik farkındalığı. Bilgi Güvenliği Dergisi, 3(2), 45-55.

Parikh, V., & Nimbekar, M. (2023). Socializing the Impact: An Analysis of the Theory of Planned Behavior's Influence on Increasing University Students' Cybersecurity Awareness. *Journal of Community Development. 4*(2), 139-156. https://doi.org/10.47134/comdev.v4i2.162.

Polas, M., Sohel-Uz-Zaman, A., Dey, M., Chowdhury, S., Kabir, A., Ahamed, B., & Fahad, A. (2024). Empowering Students for Cybersecurity Awareness Management in the Emerging Digital Era: The Role of Cybersecurity Attitude in the 4.0 Industrial Revolution Era. *SAGE Open*, 14. https://doi.org/10.1177/21582440241228920.

Prümmer, J., Van Steen, T., & Van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security, 136*, 103585. https://doi.org/10.1016/j.cose.2023.103585.

Ramaswamy, R., Madakam, S., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computational Chemistry*, 3, 164-173. https://doi.org/10.4236/JCC.2015.35021.

Rao, R., Amo, L., Frank, E., Upadhyaya, S., & Liao, R. (2019). Cybersecurity Interventions for Teens: Two Time-Based Approaches. *IEEE Transactions on Education, 62*, 134-140. https://doi.org/10.1109/TE.2018.2877182.

Salem, M., & Sobaih, A. (2023). A Quadruple "E" Approach for Effective Cyber-Hygiene Behaviour and Attitude toward Online Learning among Higher-Education Students in Saudi Arabia amid COVID-19 Pandemic. *Electronics. 12*(10), 2268. https://doi.org/10.3390/electronics12102268.

Schaller, R. R. (2002). Moore's law: past, present and future. *IEEE spectrum, 34*(6), 52-59.

Steen, T., & Deeleman, J. (2021). Successful Gamification of Cybersecurity Training. *Cyberpsychology, behavior and social networking*. https://doi.org/10.1089/cyber.2020.0526.

Tahmasebi, M. (2024). Cyberattack Ramifications, The Hidden Cost of a Security Breach. *Journal of Information Security*, *15*(2), 87-105.https://doi.org/10.4236/jis.2024.152007

Tirumala, S., Pang, P., & Sarrafzadeh, A. (2016). A survey on internet usage and cybersecurity awareness in students.*2016 14th Annual Conference* *on Privacy, Security and Trust (PST)*, 223-228. https://doi.org/10.1109/PST.2016.7906931.

Tütüncü, B., & Yıldırım, M. (2021). Üniversite öğrencilerinde siber güvenlik bilinci: Cinsiyetin rolü. *Siber Güvenlik ve Savunma Dergisi, 6*(1), 85-98.

Valcour, P. M., & Hunter, L. W. (2004). Technology, organizations, and work-life integration. In *Work and life integratio* (pp. 76-98). Psychology Press.

Van Den Berg, B., Prümmer, J., & Van Steen, T. (2024). Assessing the effect of cybersecurity training on End-users: A Meta-analysis. *Comput. Secur.*, 150, 104206. https://doi.org/10.1016/j.cose.2024.104206.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Yıldırım, E. (2022). Üniversitelerde siber güvenlik eğitimi: Etkililik değerlendirmesi. Yükseköğretim ve Bilim Dergisi, 12(3), 213-227.