International Journal of Evaluation and Research in Education (IJERE)
Vol. 14, No. 6, December 2025, pp. 4276~4294
ISSN: 2252-8822, DOI: 10.11591/ijere.v14i6.32613

Enhancing teachers' digital literacy for security: a systematic review of frameworks and analytical methods in education

Nadirah Othman[1], Nor Aslily Sarkam[1], Norhayati Baharun[1], Teoh Sian Hoon[2], Suraya Masrom[1], Nor Faezah Mohamad Razi[1], Abdullah Sani Abd Rahman[3]
[1]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Perak Branch, Tapah Road, Malaysia
[2]Faculty of Education, Universiti Teknologi MARA Selangor Branch, Puncak Alam, Malaysia
[3]Faculty of Science and Information Technology, Universiti Teknologi PETRONAS, Seri Iskandar, Malaysia

Article Info

Article history:

Received Aug 28, 2024
Revised May 28, 2025
Accepted Jul 25, 2025

Keywords:

Analytical methods
Digital security
Education
Frameworks
Teachers' digital literacy

ABSTRACT

The rising use of digital tools in education emphasizes the crucial need of teachers' digital security, which relies on strong digital literacy. This study assesses teachers' digital literacy on digital security literature to meet the urgent need for safe practices in schools due to increased security breaches. A total of 30 studies were reviewed using preferred reporting items for systematic reviews and meta-analyses (PRISMA) criteria to build frameworks and data analysis methodologies in this field. Five research areas were identified: teacher perspectives, security-related issues, educational impacts, pedagogical approaches, and instrument validation. The predominant framework used was the digital competence framework for citizens (DigComp), however hybrid frameworks that integrate other theoretical perspectives were highly commended for their comprehensive approach. The 30% of the studies focused on security issues, including cyberbullying and data protection, while 70% incorporated security dimensions into digital literacy frameworks. Quantitative approaches comprising 60%, including t-tests, analysis of variance (ANOVA), and regression analysis. Structural equation modeling (SEM) was used in several studies to examine complex relationships. Although current research predominantly emphasizes quantitative methods, future investigations could enhance knowledge of teachers' digital literacy and security by integrating SEM with artificial neural networks (ANN). This review emphasizes the necessity for hybrid frameworks and sophisticated approaches to enhance research.

Corresponding Author:

Nor Aslily Sarkam
Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Perak Branch
35400 Tapah Road, Perak, Malaysia
Email: noraslilysarkam@uitm.edu.my

1. INTRODUCTION

The digital literacy has become a key part of modern education and covers a wide range of skills to navigate the digital world [1], [2]. In education, digital literacy is not just about using digital tools but also about understanding, evaluating and integrating digital resources effectively and ethically [3], [4]. The challenges of digital literacy in education are not novel; however, they have gained prominence and pose a substantial obstacle, particularly due to the shift from traditional to digital learning, exacerbated by the effects of COVID-19.

Existing studies highlighted digital divide [5], [6] and insufficient digital literacy [7]–[9] as a significant issue in 21st-century digital literacy education. The ramifications of inadequate digital literacy are

far-reaching, impacting both educational quality and engendering various safety and security issues. This arises from individuals' incapacity to comprehend and safeguard themselves in digital contexts. This can lead to unintentional sharing sensitive data [10], [11], increasing risk of privacy breaches [10], [12], and cyberbullying [13], [14]. Addressing problems, particularly in security and safety, is crucial for attaining sustainable development goal 4 (SDG 4) concerning excellent education and lifelong learning; it will provide a comprehensive perspective on digital literacy.

This paper presents a novel contribution by systematically reviewing studies that specifically address teachers' digital literacy within the security context, a subdomain that has received limited scholarly attention despite its growing urgency. Unlike prior reviews that broadly assess digital literacy, this study narrows its focus to security-related dimensions such as cyberbullying prevention, data protection, and ethical digital behavior. It uniquely synthesizes findings based on the preferred reporting items for systematic reviews and meta-analyses (PRISMA) method, analyzes the use of theoretical frameworks, e.g., digital competence framework for citizens (DigComp), International Society for Technology in Education (ISTE), National Institute of Educational Technologies and Teacher Training (INTEF), and categorizes analytical methods and research objectives across 30 empirical studies. Moreover, it highlights the need for hybrid frameworks and the integration of advanced techniques such as structural equation modeling (SEM) and artificial neural networks (ANN) to assess complex relationships in digital literacy research. This multidimensional review not only fills a gap in existing literature but also provides actionable insights for researchers, policymakers, and educators aiming to strengthen digital security literacy among teachers.

Security and safety are important components of the digital literacy [15], [16]. Consequently, it is imperative to ensure a secure digital environment within the educational setting, as all educational institutions depend on digital platforms for teaching and learning. Security in the digital literacy context involves protecting information from unauthorized access and cyber threats, while safety means being an ethical user in digital space [17]. These facets of security and safety emphasize the necessity for teachers to possess expertise in these domains to safeguard themselves and their students. The rising cases of cyber-attacks and data breaches in educational institutions highlights the urgency of this issue [18], [19]. Universities, colleges, and schools are primary targets for cybercriminals due to their substantial populations of information and communication technology (ICT) users and valuable data. Therefore, it is crucial to comprehend and mitigate these risks not only for personal and institutional data but also for a secure and conducive learning environment.

Teachers play an important part in the promotion of digital literacy and are seen as key factor in the success of integrating and innovating technology in schools [20], [21]. Teachers need to equip themselves with digital literacy in order to guide students. Granda *et al*. [22] highlighted that teachers play a pivotal role in transforming the classroom into a digital environment, which involves learning new technologies and providing personalized instructions. Yet, the digital literacy of teachers themselves especially in security and safety is frequently neglected [23]. As the development of teachers' digital literacy emerges as a global concern, studies have been conducted to analyze and assess the level of digital literacy among educators, particularly in the context of security. Consequently, it is advisable for educators to consistently enhance and prepare themselves with digital literacy and security to foster professional development and improve educational practices. Various methods of data analysis are employed to assess teachers' digital literacy; however, there remains an opportunity for enhancement, particularly through the application of advanced data analysis techniques.

This review paper examines the present condition of teachers' digital literacy in security, highlighting the importance of improving digital literacy to foster a secure learning environment for pupils. Considering the growing utilization of digital tools in education, it is imperative to evaluate and enhance teachers' digital literacy in security. This analysis seeks to provide thorough insights and actionable recommendations for enhancing teachers' capacity to handle digital security successfully. The subsequent research questions serve as a framework for this review:

i) What are the common research objectives in studies on teachers' digital literacy within the security context?
ii) What frameworks are commonly used in studies on teachers' digital literacy within the security context?
iii) What dimensions are used to evaluate teachers' digital competence in the security context?
iv) What research methods and data analysis techniques are commonly used in studies on teachers' digital literacy within the security context?

2. METHOD

2.1. Database selection

This review involved the collection of data from two prominent journal databases, Scopus and Web of Science (WoS), which are acknowledged as the foremost indexing systems for citations. WoS is a comprehensive database that includes more than 254 fields of study, spanning sciences, transdisciplinary social sciences, arts, and humanities. This database can be organized based on three distinct criteria: citations, papers,

and citations per publication. The collection boasts a wealth of historical records and citation information that spans more than a century. Scopus serves as an extensive database of scholarly works, providing both abstracts and citations. The dataset comprises 27,950 active peer-reviewed journals sourced from 7,000 publishers across the globe. The content encompasses a wide range of academic fields, including the sciences, social sciences, agriculture, and biological sciences. The integration of both databases significantly improves the journal coverage, guaranteeing that the papers examined in this study meet the highest standards of quality.

2.2. Document searching

This systematic review was carried out following the PRISMA, which is a recognized guideline for the execution of systematic reviews. Publication guidelines hold significant importance for authors, as they offer essential information for assessing and scrutinizing the quality and rigor of a review. PRISMA serves as a fundamental basis for systematic review documentation, providing advantages across diverse domains [24]. In addition, PRISMA provides a widely acknowledged and endorsed method that employs a checklist of criteria to improve the quality assurance of the revision process and guarantee its replicability [25], [26]. A comprehensive analysis was carried out following the PRISMA criteria to assess the digital literacy levels of educators in the security subject. This investigation focused on the framework, methodologies, and the instructors' level of literacy, particularly concerning security. The process comprised three distinct procedures, as depicted in Figure 1.

2.2.1. Identification

The first step of the systematic review process involves pinpointing terms that are pertinent to educators' digital literacy concerning security. It is crucial to incorporate all pertinent terms for this subject to guarantee a thorough investigation. We utilize a variety of pertinent sources, such as terms from previous studies, dictionaries, database thesauri, Scopus, wildcards, truncations, and combined Boolean operators, to improve the identification of suitable studies. In June 2024, search queries were generated on the Scopus and WoS databases, as in Table 1. A total of 324 documents were obtained from the Scopus database, alongside 279 items sourced from the WoS database.

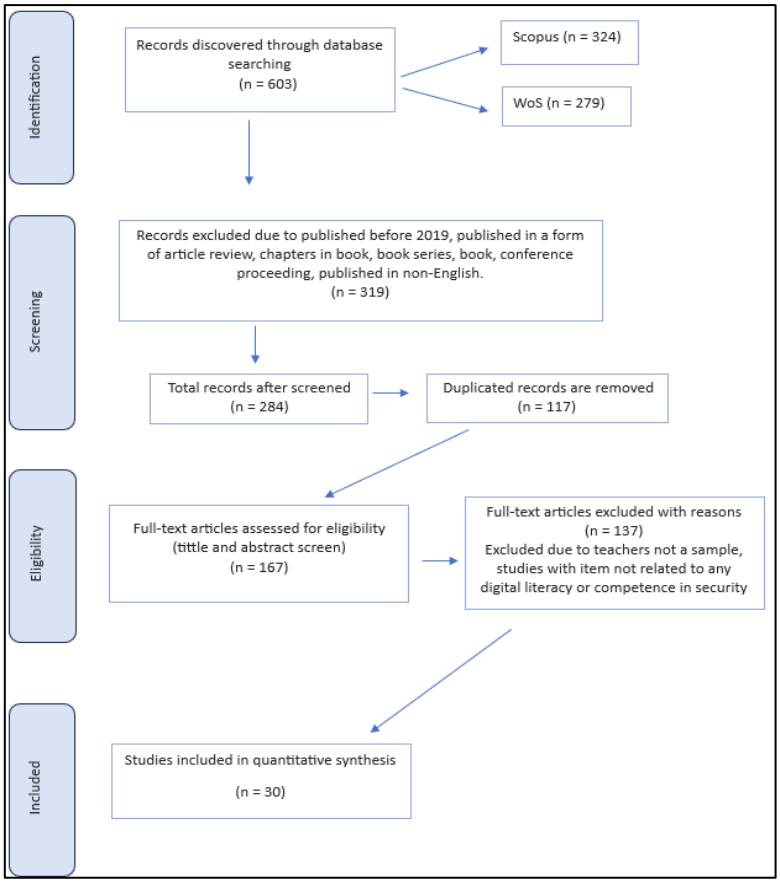

Figure 1. The PRISMA flow diagram of the study

Table 1. The search string

Databases	Keywords used
Scopus	TITLE-ABS-KEY ((“digital literacy*” OR “digital ability*” OR “digital competence*” OR “digital skill*”) AND (“security” OR “cybersecurity*” OR “cyber security*” OR “cybersafety*” OR “safety” OR “cyberbullying”) AND (“primary education” OR “secondary education” OR “early childhood” OR “higher education” OR “teacher*” OR “educator*” OR “lecturer*” OR “professor*” OR “instructor*” OR “coach*”))
	TITLE-ABS-KEY ((“digital security”) AND (“primary education” OR “secondary education” OR “early childhood” OR “Higher education” OR “teacher*” OR “educator*” OR “lecturer*” OR “professor*” OR “instructor*” OR “coach*”))
WoS	TS= ((“digital literacy*” OR “digital ability*” OR “digital competence*” OR “digital skill*”) AND (“security” OR “cybersecurity*” OR “cyber security*” OR “cybersafety*” OR “safety” OR “cyberbullying”) AND (“primary education” OR “secondary education” OR “early childhood” OR “higher education” OR “teacher*” OR “educator*” OR “lecturer*” OR “professor*” OR “instructor*” OR “coach*”))
	TS= ((“digital security”) AND (“primary education” OR “secondary education” OR “early childhood” OR “higher education” OR “teacher*” OR “educator*” OR “lecturer*” OR “professor*” OR “instructor*” OR “coach*”))

2.2.2. Screening

The second element of our systematic review process, screening, consists of three essential stages: first is data merging, followed by duplicate removal, and lastly is data relevancy assessment. Initially, the bibliometric R [27] package was employed to merge the extracted data from the WoS and Scopus databases and to eliminate duplicate documents. Subsequently, we focused on assessing the relevancy of the remaining documents using predefined selection criteria that are crucial for ensuring the articles’ relevance to the study’s focus [28]. The selection criteria outlined in Table 2 involved evaluating articles based on empirical data, their relevance to digital literacy within the security context, publication dates ranging from 2019 to 2024, and a restriction to the English language only. The advanced sorting functionalities of the databases greatly facilitated this process, significantly streamlining the screening phase and ensuring that only papers relevant to teachers’ digital literacy and security were included in the review. Following a comprehensive evaluation, a total of 167 publications fulfilled the specified criteria.

Table 2. Inclusion and exclusion criteria

Criterion	Inclusion	Exclusion
Literature type	Indexed journal (research articles)	Non indexed journals, systematic review journals, chapter in book, conference proceeding
Language	English	Non-English
Time line	Between 2019-2024	<2019

2.2.3. Eligibility

The assessment of eligibility represents the concluding phase in our systematic review technique. During this phase, we assessed the significance of each article to the study by examining their titles, abstracts, findings, and discussions. This thorough examination resulted in the removal of 137 publications that did not fulfil our criteria, as these articles either lacked empirical evidence or did not specifically focus on the aspect of teachers’ digital literacy in relation to security. As a result, 30 papers fulfilled all the criteria and were deemed appropriate for additional assessment.

The final sample size of 30 articles in this systematic review is considered sufficient based on several reasons. First, based on the study maturity concept by Kraus *et al.* [29], research areas that are still developing or not widely explored, such as digital literacy in the context of security, usually have fewer related studies. As a result, the number of eligible articles tends to be lower. Second, Robinson and Lowe [30] mentioned that many systematic literature reviews (SLR) include fewer than 50 articles, and some even have fewer than 10, depending on the research focus and availability of studies. Third, other SLR on similar topics have also used a small number of articles. For example, previous research [31], [32] reviewed only 31 and 14 articles, respectively. These examples show that selecting 30 articles is acceptable and still allows for a meaningful review and analysis. The selected papers are delineated in Figure 1, which depicts the eligibility assessment procedure and the final selection for comprehensive review.

2.3. Data abstraction and analysis

The examination of the remaining 30 articles is thorough, highlighting their correspondence with the research enquiries. The articles underwent a descriptive analysis that included a quantitative summarization and categorization. This quantitative analysis explored different facets of the literature, encompassing research methodology, instruments, data analysis techniques, and frameworks. The results of these methodologies are thoroughly detailed in Tables 3 and 4.

Table 3. The framework

Authors	DC	INTEF	ISTE	OA	NM	DCE	NLT	TPB	UTAUT	PTMT	TPACK	TMI
[33]								/				
[34]					/							
[35]					/							
[36]	/											
[37]						/						
[38]	/											
[39]				/								
[40]			/	/								
[41]					/							
[42]					/							
[43]											/	
[44]					/							
[45]									/			
[46]		/										
[47]					/							
[48]							/					
[49]					/							
[50]					/							
[51]					/							
[52]					/							
[53]	/											/
[54]	/											
[55]		/				/						
[56]					/							
[57]										/		
[58]					/							
[59]					/							
[60]					/							
[61]				/								
[62]					/							

Framework: DC=DigComp; OA=other authors; NM=not mentioned; DCE=DigCompEdu; NLT=network learning theory; TPB=theory planned behavior; UTAUT=the unified theory of acceptance and use of technology; PTMT=parental/teacher mediation theory; TPACK=technology, pedagogy, and content knowledge; TMI=theory of multiple intelligences

Table 4. The research methodology, instruments and data analysis methods

Authors	Methodology			Instrument						Method(s)								
	QN	QL	MX	Q	FG	IN	ON	D	SY	D	IS	FA	SEM	CA	PCA	CNA	DR	TM
[33]		/				/	/	/									/	
[34]	/			/						/	/							
[35]		/			/													/
[36]	/			/						/		/						
[37]	/			/						/								
[38]	/			/						/		/						
[39]	/			/						/		/						
[40]		/				/												/
[41]		/				/												/
[42]		/		/												/		
[43]	/			/						/	/							
[44]	/			/							/							
[45]	/			/						/	/	/	/					
[46]	/			/						/	/							
[47]	/			/						/								
[48]		/				/												/
[49]	/			/						/								
[50]	/			/						/								
[51]			/						/	/	/			/				
[52]	/			/								/	/					
[53]	/			/						/	/				/			
[54]	/			/						/	/							
[55]	/			/						/		/						
[56]			/	/		/				/						/		
[57]		/				/												/
[58]	/			/						/	/							
[59]		/			/													/
[60]	/			/						/	/							
[61]		/			/													/
[62]			/	/						/	/							/

Methodology: QN=quantitative; QL=qualitative; and MX=mixed method. Instrument: Q=questionnaire; FG=focus group; IN=interview; OB=observation; D=diary/document); and SY=survey. Method: CA=cluster analysis; PCA=principal component analysis; DR=data reduction; and TM=thematic analysis

3. RESULTS

This section addresses the research questions by analyzing 30 selected articles through a SLR. The analysis is organized in the same order as the research questions, ensuring a detailed study of common research objectives, frameworks, dimensions, and methodologies related to teachers' digital literacy within the security context. By synthesizing these findings, it provides useful insights for future efforts to improve teachers' digital literacy and securing educational environment.

3.1. What are the common research objectives in the studies on teachers' digital literacy within the security context?

This study categorizes 30 objectives related to teachers' digital literacy in security contexts into five distinct groups. They are: i) understanding educators' views and knowledge regarding digital security; ii) elements that affect digital security; iii) effects of digital security on learning results; iv) teaching strategies to improve digital security; and v) assessment and dependability of digital security tools. Table 5 indicates that a significant portion of the studies concentrate on assessing and evaluating educators' perceptions or levels of digital literacy, accounting for 33% (n=10). The eight studies (27%) closely examine the factors that impact digital security. The total of three studies (10%) assess the influence of digital security on educational outcomes, whereas an additional 13% (n=4) focus on teaching strategies and methods aimed at improving digital security. In conclusion, five studies (17%) assess the validity and reliability of instruments related to digital security.

Table 5. Category of research objectives

Categories of research objectives	Authors(s)	Objective
RO1: teachers' perceptions and awareness of digital security	[33]	Evaluating beliefs and practices of EFL teachers in integrating digital literacy.
	[37]	Analyzing digital competence levels among teachers in Spain.
	[41]	Identifying components of teachers' digital literacy in remote education.
	[53]	Studying the relationship between literacy components, digital skills, and types of intelligence among teachers.
	[60]	Investigating in-service teachers' self-perceptions of digital competence and the impact of gender and teaching experience.
	[46]	Assessing the digital proficiency of teachers and the improvement facilitated by nano-MOOC courses.
	[56]	Assessing perspectives and levels of digital citizenship among preschool and instructional technology teacher candidates.
	[57]	Identifying aspects of responsible online communication promoted by teachers.
	[58]	Assessing knowledge and skills related to digital literacy in the area of e-threats.
	[59]	Determining digital literacy levels in areas related to e-threats and exploring the impact of gender on knowledge and skills.
RO2: factors influencing digital security	[34]	Examining the relationship between information technology and digital competencies in teachers.
	[43]	Examining the correlation between STEM teachers' digital literacy competence and their levels of technology integration.
	[44]	Determining factors influencing strategies for data protection and digital sustainability among teachers.
	[45]	Examining the relationship among teachers' self-efficacy, enabling conditions, and digital proficiency.
	[35]	Recognizing challenges encountered by teachers during the COVID-19 pandemic.
	[48]	Analyzing challenges faced by lecturers during online examinations.
	[47]	Identifying professional deficits of teachers in the context of digital transformation.
	[51]	Analyzing teachers' performance in digital safety areas.
RO3: impact of digital security on educational outcomes	[40]	Identifying concerns and actions related to digital safety among elementary school children.
	[49]	Evaluating the efficacy of the social lab virtual social network as a teaching instrument to augment teacher digital proficiency.
	[50]	Examining the effectiveness of educational video games in developing teachers' digital competence in the e-safety area.
RO4: pedagogical approaches to enhance digital security	[42]	Investigating teachers' perspectives on AR competences, digital skills for integrating AR, and associated safety, security, and ethical issues.
	[59]	Improving pedagogical approaches to enhance students' information security by focusing on educational strategies that address the negative impacts of ICT.
	[61]	Restructuring teaching practices to enhance student motivation, engagement, and interest in cybersecurity.
	[62]	Analyzing teachers' feedback of their students' understanding and application of digital citizenship.
RO5: validation and reliability of digital security instruments	[36]	Validation of a scale to assess digital teaching competence.
	[38]	Analyzing the validity and reliability of the digital competence scale for teachers.
	[39]	Validation of the Turkish version of the 'teachers' basic ICT competence beliefs' instrument.
	[55]	Validation of a scale for eco-responsible use of technologies among teachers.
	[52]	Creation and evaluation of a tool to evaluate teachers' basic concepts regarding ICT competence

3.2. What frameworks are commonly used in studies on teachers' digital literacy within the security context?

A review of 30 studies examining teachers' digital literacy within a security setting identified 11 different frameworks. The frameworks include a range of theoretical perspectives, methodologies, and practical applications, highlighting the interdisciplinary character of this research nature. Table 3 shows that 15 studies did not specify any framework, opting instead for general discussions on digital literacy and security without grounding their work in established theoretical models. lacking a foundation in recognized theoretical models. Nevertheless, these 15 studies utilized distinct frameworks, offering significant insights into the theoretical foundations of digital literacy research.

The DigComp emerged as the most used framework, appearing in four studies [36], [38], [53], [54]. This framework focuses on five areas: information literacy, communication and collaboration, digital content creation, security, and problem solving. Previous studies [36], [38] used DigComp to validate digital competence scale for teachers, whereas other study [54] used it to investigate teachers' awareness of e-safety and data privacy. Sitoy *et al.* [53] took an innovative approach by combining DigComp and theory of multiple intelligences (TMI) in their study to investigate the relationship between digital literacy dimensions and types of intelligence among teachers.

The DigCompEdu and the INTEF were significant in the analysis. DigCompEdu was used in two studies [37], [55], with the other study [55] combining it with INTEF to create a scale for eco-responsible technology usage. INTEF, created in Spain, was utilized in Basantes-Andrade *et al.* [46], to assess teacher training programs and environmentally sustainable practices, showcasing its effectiveness in both technical and ethical issues of digital literacy. The ISTE framework was used in Martin *et al.* [40] to identify the themes of digital safety among elementary school children. These frameworks highlight the importance of innovation and safety in the application of technology, established solid foundation for evaluating digital practices of young learners. Furthermore, study by Martin *et al.* [40] combines ISTE with a framework developed by other authors (OA) to offer a more comprehensive perspective on digital security, demonstrating how ISTE can be used to enhance analysis. Other studies [39], [61] also employed OA framework. These frameworks address specific digital security issues. Nurzhanova *et al.* [61] employ framework developed by previous authors that focusing on pedagogical phenomenology. This methodology establishes hypotheses to investigate the perspectives of teacher-practitioners regarding cyberbullying prevention. Korukluoğlu *et al*. [39] on the other hand, is based on framework proposed by Rubach and Lazarides [52]. This framework emphasizes the evaluation 'teachers' basic ICT competence beliefs.

The analysis also showed behavioral and pedagogical frameworks. In Majola and Mudau [48], the NLT was applied to investigate the problem that lecturers experienced during online examinations, focusing the influence of network environments on digital practices. Similarly, the theory planned behavior (TPB) was implemented in Demirdağ and Taşgın [33] to examine the impact of teachers' attitudes and perceived behavioral control on their decisions regarding safe digital tools. The unified theory of acceptance and use of technology (UTAUT) was employed in Wang and Chu [45] in analyzing the relationship between self-efficacy, facilitating factors and digital competence, offering a behavioral perspective on technology adoption in educational contexts. To investigate how teachers promote responsible online communication practices, the parental/teacher mediation theory (PTMT) was used in Martinez [57]. The PTMT, which focuses on the perceptions and responses of individuals to digital threats, offered valuable insights into teachers' responsibilities in the development of ethical and secure online behaviors. Furthermore, the technology, pedagogy, and content knowledge (TPACK) framework were implemented in Ramli and Arsad [43] to investigate the integration of technology in science, technology, engineering, and mathematics (STEM) education, highlighting the interaction among technological, pedagogical and content knowledge.

Several studies have shown the value of combining framework to answer complicated research questions. For example, Sitoy *et al.* [53] combined DigComp and TMI to investigate the relationship between digital literacy dimensions and intelligence types. Study by Martin *et al.* [40] used ISTE and OA to measure digital safety themes among elementary school children, whereas Barragán-Sánchez *et al.* [55] combined DigCompEdu and INTEF to create comprehensive scale for environmentally responsible technology use.

3.3. What dimensions are used to evaluate teachers' digital competence in security context?

The analysis of all studies indicates that the dimensions employed are associated with the field of security. Examining these dimensions allows us to classify the studies into two distinct categories. The first is the investigations that focus on security aspects including cyberbullying, cybersecurity, device protection, and personal data protection. Secondly are the investigations that explore security or safety in an indirect manner, incorporating these elements as dimensions within wider evaluations of digital literacy. The findings for the two categories are displayed in Tables 6 and 7.

Table 6. Dimensions that used in the studies that directly investigate security and safety

Author(s)	Dimensions
[40]	Issues pertaining to content; issues pertaining to contact; issues pertaining to conduct; issues pertaining to contracts; issues pertaining to home.
[44]	Demographic variables such as safeguarding personal data, encouraging strategies, informing families, school accounts, and sustainability: advising students, utilizing protocols, promoting sustainable practices, educational proposals.
[51]	Demographic; assessment of ICT utilization and proficiency in digital media education: safety perceptions, intellectual property rights, reliability of online content, cyberbullying awareness, and malware defense strategies.
[50]	Digital identity, safeguarding and utilization of personal data, management of privacy, licensing of digital content, awareness of cybersecurity, and ethical application of digital technologies.
[58]	Examining the ergonomics of ICT usage, evaluating the credibility of information, ensuring secure online communication, preserving anonymity in the digital realm, implementing safe login practices, understanding intellectual property.
[59]	Programs aimed at preventing cyberbullying face various implementation challenges, including the need for teachers to enhance their knowledge in this area. Additionally, there are significant obstacles related to teacher training and the necessity for collaboration within the community.
[60]	Ensuring safety while interacting with other online users, protecting images shared on the internet, understanding copyright laws, assessing the credibility of online information, addressing cyberbullying, managing financial transactions securely.
[61]	Teacher training and experience, implementation issues, student needs and expectations, assessment programs, social and emotional intelligence, use of digital media; social and legal repercussions, parental participation, school policies and procedure, technological advancements, cyberbullying directed at teachers.
[62]	Utilization of digital devices, online harassment, proper online etiquette, digital trace, online privacy, virtual identity.

Table 7. Dimension that used in the studies that indirectly investigate security or safety

Author(s)	Dimensions
[33]	Teachers' belief: behavioral beliefs, normative beliefs, control beliefs; digital literacy: functional, finding information, creativity, critical thinking, collaboration, cultural understanding, communication, e-safety.
[34]	Information technology in education: technological, pedagogical, management social, ethical and legal; attitudinal, digital competencies encompass various essential skills, including information and information literacy, effective communication and collaboration, digital content creation, security awareness, and problem-solving abilities.
[35]	The elements concerning the impact of the COVID-19 pandemic on pre-university education are challenges in professional settings, administrative hurdles, psychological obstacles, technical issues, social barriers, digital skills, and concerns regarding online safety and security. Assessment and evaluation.
[36]	Knowledge and understanding of information, effective communication and teamwork, creation of digital content, safety measures, solutions to challenges.
[37]	Professional involvement; digital resources, digital pedagogy, evaluation and feedback, empowering students, enhancing students' digital proficiency.
[38]	Safety; data literacy, problem solving, digital content creation, communication and collaboration, ethics.
[39]	Information and information literacy; communication and cooperation; digital content creation; safety and security; problem-solving; analysis and reflection.
[42]	Digital competencies of teacher's pedagogical methodologies and instructional techniques; accessibility and assessment of educational augmented reality resources; security, safety, privacy, and ethical considerations; advantages and prospects.
[41]	Understanding and utilizing technology tools and digital media, exploring and managing information and data, digital ethics and safety, relationship building, teaching and evaluation.
[43]	Comprehension of digital tools, communication and collaboration, creation of digital content; security, problem-solving, technology integration.
[45]	Demographic variables, self-efficacy, facilitating conditions, digital competence: values, ethics and security, digital resources, teaching and learning, scientific research, continuing professional development, facilitating learners' digital competence.
[46]	Information and information literacy; communication and collaboration; digital content creation; security; problem solving.
[47]	Digital competence; psychological competence; educational competence; communicative competence; organizational competence; ethical competence.
[48]	Student challenges; preparedness; technical and technological education; delivery content; administration of examination.
[49]	Usability; educational efficacy; perceived utility; enjoyment; endorsement and integration; challenge difficulty; digital competency level.
[52]	Data literacy; communication and cooperation; digital content production; safety and security; problem-solving; analysis and reflection.
[53]	Digital literacy includes information processing, communication, content creation, safety, and problem-solving. Multiple intelligences: bodily-kinesthetic, existential, interpersonal, intrapersonal, logical-mathematical, musical, naturalistic, verbal, visual-spatial. Demographics; teachers' self-assessment: information and data literacy, communication and collaboration, digital content production, safety, problem-solving; utilization of ICT tools; teachers' attitude.
[55]	Teachers' understanding of the environmental implications of technology usage in both formal and informal contexts; the practical potential for integrating environmental knowledge into pedagogical practices with students and families; Instructing individuals in the identification of the environmental consequences of technological utilization and methods to mitigate such effects; educating students and families on strategies for preventing this impact.
[56]	Digital security; digital rights and responsibilities; digital law.
[57]	Strategic mediation encompasses active mediation, co-utilization, participatory learning, and instructional simulation, responsible online communication, digital competence, online safety, and privacy.

By examining at the first category, the study by Vázquez-Cano *et al*. [44] focus on investigating teachers' demographics such as gender, age, and years of experience, to determine their influence on strategies for promoting data protection and sustainability in primary schools. This study consists of aspects of personal data protection and sustainability, including strategies for safeguarding data on devices and protocols for identifying risks. Tomczyk [58] and Gabrielli *et al*. [60] focus to investigate teachers' digital literacy level specifically in digital safety. The challenges encountered by teachers regarding digital safety are focal points in both researches, emphasizing concerns such as cyberbullying prevention, implementation obstacles, and safety in online communication.

Conversely, 70% (n=21) of the research belongs to the second category by integrating security or safety components within a broader digital literacy framework. For example, Demirdağ and Taşgın [33] investigate teachers' beliefs and digital literacy by integrating e-safety in the study. Several studies [34], [46], [53] include information literacy, communication and collaboration, digital content creation, security, and problem solving as a dimension that give comprehensive view on how teachers incorporate digital safety in their professional practices.

3.4. What research methods and data analysis techniques are commonly used in studies on teachers' digital literacy within the security context?

The methodologies utilized in 30 studies examining teachers' digital literacy in the context of security are outlined in Table 4. This analysis reveals notable differences in the design, instruments, and data analysis methods utilized across the studies. The primary research design employed in these studies is quantitative methods (n=18), using questionnaires as instruments to gather data on teachers' digital literacy and security. For instance, several studies [37], [43], [45] used these methodologies to measure various aspects of digital literacy and security practices. In addition, nine studies employed qualitative methods and interviews as data collection tools to gain deeper insights into teachers' perceptions and experiences regarding digital security. The remaining studies employed mixed methods to advance the exploration of teachers' digital literacy within a security context, aiming for a thorough understanding by capturing both numerical data and contextual nuances.

Moving forward, the data analysis utilized in quantitative design primarily relied on descriptive and inferential statistics. Common techniques utilized encompass t-test, correlation, analysis of variance (ANOVA), and regression analysis to discern the differences and relationships among variables. It indicates that a limited number of studies have utilized SEM to investigate the complex relationships among the components of digital literacy. Thematic analysis is often employed in qualitative design to identify themes, dimensions, and patterns in teachers' responses regarding digital literacy and security issues. Although the least utilized design in this study is mixed methods, the combination of the quantitative and qualitative data. For example, a study by Elmali *et al.* [56] that combined descriptive and content analysis to examine the elements of digital citizenship.

4. DISCUSSION

4.1. What are the common research objectives in studies on teachers' digital literacy within the security context?

The analysis of the selected studies demonstrates a wide range of study objectives concerning teachers' digital literacy in the context of security. These objectives were divided into five categories: i) teachers' perspectives and awareness of digital security; ii) factors impacting digital security; iii) the impact of digital security on educational results; iv) pedagogical approaches to improving digital security; and v) the validity and reliability on digital security instruments.

Most of the researchers (10 out of 30) focused on analyzing and evaluating teachers' perceptions and awareness of digital security. Identifying gaps in teachers' understanding of digital security concepts and assessing beliefs and practices are the main objectives of these studies. Several studies [33], [37], [60], for instance, look at general knowledge and digital competence, which provides the groundwork for understanding how teachers deal with digital security issues in their work environments. Although this study provides a foundational understanding, many of these studies are descriptive rather than evaluative, often failing to provide actionable insights on how to bridge identified gaps in awareness. This gap emphasizes the importance of conducting additional research on professional development programs and practical interventions targeted at improving knowledge of digital security [63].

The second category, consisting of eight studies, looks into the variables affecting teachers' ability to adopt safe digital practices. For example, previous studies [34], [43] investigate the relationship between teachers' technological integration and level of digital literacy. These studies highlight the importance of self-efficacy [64] and facilitating conditions [65] in encouraging secure practices. However, there is a gap in

addressing external issues like infrastructure, institutional policies, and the socioeconomic environment of schools. For instance, studies [35], [48] highlights issues that were encountered during the COVID-19 pandemic, such as inadequate security measures for online examination and professional deficiencies in digital transition. Even though these studies offer valuable information, a more predictive approach is required to investigate how the pandemic's lessons could influence long-term digital security plans [66].

The research in the third category (3 out of 30) examines the impact of digital security on educational outcomes, specifically on student safety and teacher proficiency. Several studies [40], [49], [50] examine new approaches, including simulated social networks and educational video games, to improve teachers' digital literacy. These methods show promise, but their effectiveness in growing and working across different educational settings has remains underexplored [67], [68]. The lack of real-world conditions highlights the need for future research to investigate the long-term consequences of these interventions in teacher effectiveness and student learning.

Four studies that focus on pedagogical approaches to raise awareness and practices of digital security fall under the fourth category. To engage teachers and students in safe digital activities, previous studies [42], [59], [61] highlight innovative approaches including augmented reality (AR) and cyberbullying prevention initiatives. These results demonstrate the importance of a comprehensive approach to digital security education that includes not just technical skills but also ethical values and social responsibilities [69]. However, these studies sometimes overlook several points of view and experiences, which are essential for meeting various educational needs. For instance, while study by Hawamdeh [62] examines teachers' perceptions of students' understanding of digital citizenship, it neglects to address the influence of cultural or socio-economic factors on these views. Future research should examine how pedagogical approaches might be modified to tackle the unique issues encountered by various groups of teachers and students.

Finally, the fifth category comprises five research focused on the validation and evaluation of instruments designed to measure digital competence and security practices. Studies including [36], [52] offers significant advancements by creating reliable instruments for examining teachers' understanding and implementation of digital security. These instruments are essential for setting benchmarks and monitoring advancements in digital literacy programs. However, several of these studies focus on technical validation without closely analyzing the useful application of these instruments in actual learning environments. The instruments validated by previous studies [38], [55], for example, might not be useful in all educational settings. Future studies should focus on making these instruments adaptable and relevant to ensure they work effectively in different contexts [70].

The significance of these findings lies in their potential to influence both research and practice in digital security education. Current research frequently lacks coordination, underscoring the necessity for a more integrated and comprehensive strategy to address the numerous issues in this field [71]. For instance, investigations into perceptions and awareness should be more effectively integrated with research on pedagogical approaches and learning outcomes. Connecting these areas can help provide a better understanding of how to equip teachers with the skills and knowledge needed to create safe digital environments.

Moreover, the predominance of descriptive studies highlights the need for more evaluative and intervention-based research. Developing and testing comprehensive frameworks that integrate the five categories identified in this review could provide a cohesive understanding of digital security in education. Such an approach would not only advance academic knowledge but also offer practical guidance for policymakers and educators striving to enhance digital literacy and security practices in schools.

4.2. What frameworks are commonly used in studies on teachers' digital literacy within the security context?

The review of frameworks used in studies on teachers' digital literacy in the context of security shows some key insights. These frameworks offer a clear and structured approach to understanding and improving digital literacy, with each presenting its own distinct ideas and applications. The discussion critically evaluates the findings in respect to each framework, highlighting the consequences of their use and combination.

The DigComp framework has been broadly employed in various studies [36], [38], [53], [54]. The popularity of DigComp is due to its comprehensive approach thorough evaluation of digital competence, encompassing technical, cognitive, and socio-emotional skills [72]. Its widespread use highlights its importance in meeting digital literacy needs in education. However, it should be noted that DigComp's broad application may not necessarily address specific security-related aspects of digital literacy. This raises concerns about its suitability for tackling the special issues that teachers encounter in a security setting [73]. The INTEF framework, used in previous studies [46], [55], highlights the importance of competence in digital teaching and learning. INTEF offers a localized and context-specific approach; however, its implementation in security contexts remains underexplored. The few studies utilizing INTEF indicate that

its implementation may be restricted due to its regional emphasis [74] or insufficient alignment with wider security issues [75].

The ISTE framework, as applied in Martin *et al.* [40], emphasizes the integration of technology in pedagogy, fostering innovation and the ethical utilization of digital tools. While this focus aligns with advancements in teaching practices, the limited attention to security issues reveals a significant gap [76]. To address these challenges, it is essential to develop frameworks that integrate comprehensive risk mitigation strategies for ethical digital environments. This highlights the necessity of modifying current frameworks to incorporate strong security protocols.

Several studies [39], [40], [61] referred OA frameworks, highlighting the contributions of researchers to digital literacy. These studies highlight the diversity of theoretical and practical approaches based on frameworks created by other researchers. While this diversity adds valuable perspective, the differences in scope and focus among these modified frameworks might make it challenging to compare findings across studies. Defining clear criteria for categorizing and applying these frameworks may improve their relevance and promote a deeper understanding of their contributions [77], [78].

The DigCompEdu framework, utilized in the studies [37], [55], emphasizes educational context but seems to be inadequately addressed in security related discussions [79]. The limited adoption suggests a potential gap in addressing digital risks comprehensively. Extending its application to security related issues may improve its relevance and effectiveness in equipping teachers for secure digital practices. The use of NLT in Majola and Mudau [48] highlights the need of supporting cooperative, adaptable, and networked teaching approaches as well as the connections between digital learning settings. While NLT provides valuable insights into digital learning processes, as evidenced by its growing application in systems like small and medium-sized enterprises (SMEs) [80] and governance networks [81]. However, its potential to address security-related challenges remains underexplored and requires further research. This emphasizes the importance of investigating how NLT concepts might be applied to successfully manage contemporary digital dangers.

Behavioral frameworks, such as TPB, UTAUT, and PTMT, provide valuable insights into teachers' attitudes regarding secure technology. TPB focuses on how attitudes and perceived social norms influence technology adoption [82], whereas UTAUT stresses performance and effort expectations as crucial behavioral determinants [83]. Similarly, the Teacher Mediation concept emphasizes the role of teachers' own beliefs and environmental circumstances in determining their adoption and pedagogical use of technology [84]. Together, these frameworks improve our knowledge of adoption trends in educational settings. Nonetheless, their limited application in addressing broader security concerns indicates potential for incorporating these models into comprehensive digital literacy frameworks.

The study by Ramli and Arsad [43] utilizes the TPACK framework, which focuses on combining technology, pedagogy, and content knowledge to improve teaching efficacy similar with Deng *et al.* [85]. This makes it ideal for research aimed at improving teachers' skills to use technology meaningfully in their pedagogy. However, its focus on technology integration may overlook specific aspects of digital security, thereby limiting its usefulness in addressing risks in digital education environments. On the other hand, TMI that used in Sitoy *et al.* [53] investigates various intellectual talents such as linguistic, logical, and interpersonal intelligences, in a manner consistent with its use in Gardner and Hatch [86] provides an important foundation for customizing learning. While TMI supports a variety of approaches to teaching and learning, its lack of emphasis on technology or digital competence suggests that it may require modification to stay relevant in research addressing digital literacy in security situations.

The benefits of integrating frameworks were shown in several research. To achieve a balance between broad competence and instructional specialization, for instance, study by Sitoy *et al.* [53] combined DigComp and TMI. In the same way, research by Martin *et al.* [40] integrated accessibility and ethical standards by combining ISTE and OA. Additionally, to bridge local and educational views, the research by Barragán-Sánchez *et al.* [55] connected INTEF and DigCompEdu. These pairings highlight the fact that no singular framework is adequate to handle the complex issues of digital literacy in security contexts. A comprehensive approach that creates a balance between general competencies and individual needs is made possible by the integration of several frameworks.

The conclusions derived from this discussion highlight the importance of addressing the gaps present in existing frameworks. Although strong in many aspects, frameworks such as DigComp and ISTE require improvement to effectively address specific issues of digital security. Behavioral models like TPB, UTAUT, and PTMT emphasize the need to understand teacher attitudes and motives for implementing secure practices. These findings highlight the need of aligning frameworks with two primary goals: developing secure digital literacy and addressing the real-world issues that educators encounter. By adopting these features, the field can better satisfy the various requirements of digital literacy in education.

4.3. What dimensions are used to evaluate teachers' digital literacy in the security context?

The analysis of research question 3 identified two categories of studies regarding dimensions of teachers' digital competence in relation to security. They are those that directly examine security elements and those that indirectly address security or safety aspects. The findings reveal important patterns, opportunities, and challenges in enhancing teachers' digital literacy concerning security.

Research in the first category, including [40], [44], [50], [51], highlights security related competencies such as personal data protection, digital identity management, and safe online communication. For example, previous studies [50], [87] addresses important issues such cybersecurity awareness and ethical usage of digital technologies, which are essential for creating a safe learning environment. Likewise, other studies [58], [60] explore practical concerns such as safe logging-in, intellectual property, and anonymity in digital spaces, proving the need of teachers having a strong understanding of these factors. A recurring theme among these studies emphasizes the importance of addressing cyberbullying, as highlighted in previous studies [59], [61]. Cyberbullying affects students [88] and creates challenges for teachers [89], necessitating the implementation of prevention programs and sufficient training within schools [90]. Additionally, study by Nurzhanova *et al.* [61] indicates the importance of integrating emotional intelligence and parental collaboration to develop a comprehensive strategy for digital security. However, while these studies contribute valuable insights, they often focus on specific aspects of security without providing a comprehensive framework. For example, while the study by Hawamdeh [62] discusses digital privacy, digital netiquette, and cyberbullying, it lacks integration with broader pedagogical practices. This gap indicates the need for frameworks that combine technical skills with pedagogical strategies to ensure effective implementation.

The second category includes several studies [33]–[35], which investigate dimensions of security indirectly through broader digital competencies. For example, study by Vásquez-Pajuelo *et al.* [34] emphasizes areas such as ethical and legal considerations, demonstrating the growing understanding of security as an essential component of digital literacy. Similarly, previous studies [34], [35] highlight safety within data literacy, problem-solving, and teamwork, demonstrating how security intersects with other competencies. This perspective is broadened by the studies [41], [43], which integrate psychological and pedagogical competencies. According to research by Falloon [91], these dimensions highlight the interaction between teachers' technical proficiency and their capacity to establish safe and welcoming learning environments. For instance, controlling online safety while teaching [44] or comprehending digital ethics and safety [37] demonstrate the increasing necessity for educators to strike a balance between ethical considerations and technology integration. While these studies make valuable contributions, many fail to address skills related to digital safety. For example, study by Gordillo *et al.* [49] includes safety as part of a broader digital literacy framework but does not offer practical strategies for building awareness about security. This gap highlights the need to treat security as a separate and essential component within digital literacy frameworks.

The findings reveal a lack of consistent strategies for addressing security in teachers' digital literacy. Some studies focus directly on specific challenges like protecting personal data, managing digital identities, and preventing cyberbullying, highlighting the need for targeted skills in these areas. On the other hand, other studies look at how security connects with broader aspects of digital literacy, such as collaboration, problem-solving, and ethical considerations, showing how security fits into overall teaching practices.

This dual perspective highlights the need for more integrated approaches that incorporate digital security as part of broader teaching frameworks. By addressing both the technical aspects and the real-world context of digital security, teachers can create safer and more successful digital learning environments. These findings emphasize the significance of integrating specific security skills with comprehensive digital literacy training to help teachers comfortably handle digital threats.

4.4. What research methods and data analysis techniques are commonly used in studies on teachers' digital literacy within the security context?

The findings for research question 4 reveal significant differences in research design, instruments, and data analysis methods across the 30 studies reviewed. These differences indicate the diverse methodologies researchers use to investigate teachers' digital literacy in the context of security, while also highlighting potential gaps and opportunities for methodological enhancement. Most of the studies (18 out of 30) used quantitative approaches, with questionnaires as the main instruments for data collection. Studies investigating teachers' digital literacy frequently adopt quantitative research designs, utilizing techniques, such as descriptive and inferential statistics, as well as factor analysis, to analyze their findings [30], [32]–[34]. For example, previous studies [39], [40] used advanced methods such as SEM to explore relationships between variables. Nagy and Dringó-Horváth [92] found that SEM in educational research provides a clearer understanding of the factors influencing teachers' digital literacy, including self-efficacy, training quality, and institutional support. The thorough analytical capabilities of SEM enhance the validity and reliability of findings, making it a valuable tool for future research.

Despite its advantages, the effectiveness of SEM relies heavily on the quality of data collection and the appropriateness of model specifications [93]. By capturing the complexities of digital literacy and security issues, SEM offers significant potential to deepen our understanding of the impact of digital technologies on educational practices and organizational performance [94], [95]. However, the heavy reliance on self-reported data can introduce biases, such as overestimating or underestimating competence levels [96]. Additionally, while quantitative studies provide valuable insights into specific skills, they often fail to fully explore the broader details or real-world aspects of security-related practices.

The nine studies used qualitative approaches, employing interviews, focus groups, and observations as common tools for data collection. For instance, several studies [29], [31], [36] utilized thematic analysis to explore teachers' experiences and perspectives in depth. Other studies [55], [57] used focus groups to gather collective insights on challenges and best practices for addressing digital security in education. Qualitative methods are valuable for providing deep, detailed insights and for uncovering the reasons behind teachers' actions and the challenges they encounter. However, the findings are often difficult to apply widely, making it challenging to apply ideas across different educational contexts.

Only three research utilized mixed methodologies, combining quantitative and qualitative approaches. For instance, research by Galustov *et al.* [47] employed surveys combined with cluster analysis, whereas the work of Tomczyk [58] utilized questionnaires with theme analysis to present a comprehensive perspective on security competencies. This balanced approach allows researchers to combine different methods, helping to confirm findings and gain a more complete understanding of teachers' digital literacy [97]. Despite these benefits, mixed-methods studies remain underrepresented in the reviewed literature.

The methodological diversity observed in the reviewed studies underscores both the strengths and limitations of current research approaches. Quantitative methods provide valuable large-scale insights, while qualitative methods offer rich contextual understanding, yet the limited use of mixed methods remains a gap. These findings highlight the need for a more integrative and balanced methodological approach to effectively address the complexities of teachers' digital literacy in security contexts.

4.5. Recommendation

Based on the findings and discussions presented in this review, the recommendations are proposed to advance research and practice in teachers' digital literacy within security contexts. By addressing these recommendations, future studies can contribute to a more comprehensive and actionable understanding of teachers' digital literacy in security contexts. These efforts will not only enhance academic knowledge but also inform policy and practice, empowering teachers to create secure and effective digital learning environments.

4.5.1. Development of integrated frameworks

Existing frameworks like DigComp, ISTE, and TPACK offer robust foundations but often lack specificity in addressing security-related competencies. Future research should prioritize the development of integrated frameworks that combine technical, pedagogical, and security-focused dimensions to provide a holistic approach to digital literacy. These frameworks should explicitly address emerging challenges such as cybersecurity, ethical technology use, and data privacy.

4.5.2. Enhanced methodological approaches

The review highlights significant methodological diversity but also underscores limitations in the use of quantitative, qualitative, and mixed methods. Future studies should adopt more integrative designs that leverage the strengths of the quantitative and qualitative approaches. For instance, employing mixed-methods designs could provide a balanced understanding of teachers' digital literacy by capturing both large-scale trends and contextual nuances. Additionally, incorporating advanced data analysis methods, such as SEM and ANN, can enhance the depth and accuracy of findings. These methods allow researchers to model complex relationships and identify underlying patterns, making them particularly valuable in understanding multifaceted aspects of digital literacy and security.

4.5.3. Professional development and training

Teachers require continuous professional development to navigate the rapidly evolving digital landscape. Future research should focus on designing and evaluating training programs that address both foundational digital literacy and advanced security competencies. These programs should incorporate practical, hands-on components to enhance teachers' confidence and efficacy in using digital tools securely.

4.5.4. Incorporation of emerging technologies

As digital technologies evolve, future research should examine how emerging technologies such as artificial intelligence, blockchain, and cloud computing impact teachers' digital literacy and security practices. Understanding these technologies' implications will be crucial for preparing teachers to address new challenges in educational settings. Moreover, integrating these innovations into teacher training programs can ensure that teachers remain adaptable and competent in a rapidly changing digital landscape.

4.5.5. Focus on ethical and social implications

Future research should investigate the ethical and social dimensions of teachers' digital literacy, particularly in relation to security. Topics such as digital rights, online behavior, and the social consequences of digital interactions deserve greater attention to prepare teachers for responsible and inclusive digital practices. Addressing these concerns will also promote a culture of accountability and ethical awareness among teachers in their professional and personal use of technology.

5. CONCLUSION

This SLR examined 30 studies related to teachers' digital literacy within a security context. The findings revealed a wide range of research objectives, with many studies aiming to strengthen teachers' competencies in digital security, ethical technology use, and pedagogical integration. Commonly used frameworks such as DigComp, ISTE, and TPACK demonstrated their relevance, although their focus on security-specific skills was often limited. The review also found that essential security dimensions like personal data protection and digital identity management were addressed inconsistently across studies. Quantitative methods were most frequently applied, followed by qualitative and mixed methods, with each offering different strengths and limitations.

Overall, this review shows the evolving but uneven nature of research in this area. While there has been progress, key gaps remain in aligning technical and pedagogical objectives, adopting comprehensive frameworks, and combining diverse research methods. These findings suggest a need for more integrated, security-focused research that better supports teachers in navigating digital environments safely and effectively. The insights from this review provide a valuable foundation for future studies, policy development, and teacher training programs focused on digital literacy and security.

FUNDING INFORMATION

The author thanks the Ministry of Higher Education (MoHE) for supporting this research through the Fundamental Research Grant Scheme (FRGS) (Grant No. FRGS/1/2023/SS10/UITM/02/11) and Universiti Teknologi MARA for the support.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Nadirah Othman	✓	✓	✓			✓	✓		✓	✓				
Nor Aslily Sarkam	✓	✓		✓			✓		✓	✓		✓	✓	✓
Norhayati Baharun	✓				✓	✓		✓		✓		✓		
Teoh Sian Hoon		✓			✓					✓				
Suraya Masrom		✓	✓		✓					✓	✓			
Nor Faezah Mohamad Razi				✓		✓	✓	✓		✓				
Abdullah Sani Abd Rahman		✓	✓							✓	✓		✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

REFERENCES

[1] A. Garcia and R. S. de Roock, "Civic dimensions of critical digital literacies: towards an abolitionist lens," *Pedagogies*, vol. 16, no. 2, pp. 187–201, 2021, doi: 10.1080/1554480X.2021.1914058.

[2] A. Haleem, M. Javaid, M. A. Qadri, and R. Suman, "Understanding the role of digital technologies in education: A review," *Sustainable Operations and Computers*, vol. 3, pp. 275–285, 2022, doi: 10.1016/j.susoc.2022.05.004.

[3] L. A. T. Nguyen and A. Habók, "Tools for assessing teacher digital literacy: a review," *Journal of Computers in Education*, vol. 11, no. 1, pp. 305–346, 2024, doi: 10.1007/s40692-022-00257-5.

[4] E. P. Yildiz, "Opinions of academicians on digital literacy: A phenomenology study," *Cypriot Journal of Educational Sciences*, vol. 15, no. 3, pp. 469–478, 2020, doi: 10.18844/cjes.v15i3.4913.

[5] V. S. Khandagale, "A mixed method study of strategies adopted by postgraduate teachers to mitigate the impact of the digital divide," *Journal of E-Learning and Knowledge Society*, vol. 19, no. 3, pp. 110–118, 2023, doi: 10.20368/1971-8829/1135867.

[6] N. S. M. Ishah, K. L. Lee, and G. Nawanir, "Educational supply chain sustainability," *Asian Education and Development Studies*, vol. 12, no. 2–3, pp. 137–149, 2023, doi: 10.1108/AEDS-09-2022-0123.

[7] L. Momdjian, M. Manegre, and M. Gutiérrez-Colón, "A comparison of perceptions of digital competences of Schoolteachers to school leaders in Lebanon," *Social Sciences and Humanities Open*, vol. 10, p. 100937, 2024, doi: 10.1016/j.ssaho.2024.100937.

[8] Rasimin, A. B. Semma, Zakiyuddin, M. Ali, and M. I. Helmy, "Multi-dimensional challenges in the Indonesian social science information technology-based learning: A systematic literature review," *Heliyon*, vol. 10, no. 7, p. e28706, Apr. 2024, doi: 10.1016/j.heliyon.2024.e28706.

[9] G. Šarníková, "Parents' Approaches to Their Children's Education and Related Issues During the COVID-19 Pandemic in the Slovak and the Czech Republic," *Journal of Family Issues*, vol. 44, no. 8, pp. 2185–2212, 2023, doi: 10.1177/0192513X221075633.

[10] S. Livingstone, M. Stoilova, and R. Nandagiri, "Data and privacy literacy: The role of the school in educating children in a datafied society," in *The Handbook of Media Education Research*, D. Frau-Meigs, S. Kotilainen, M. Pathak-Shelat, M. Hoechsmann, and S. R. Poyntz, Eds., Hoboken, NJ: Wiley, 2020, pp. 413–425, doi: 10.1002/9781119166900.ch38.

[11] L. Göbl, M. R. Jokisch, D. Leopold, and M. Doh, "Understanding the feeling of being overwhelmed by the internet: The role of digital literacy among older adults," *Gerontechnology*, vol. 23, no. 2, p. 1, 2024, doi: 10.4017/GT.2024.23.S.901.OPP.

[12] I. A. Ismail and J. M. Aloshi, "Data Privacy in AI-Driven Education," in *AI Applications and Strategies in Teacher Education*, K. L. Keeley, Ed., Hershey, PA: IGI Global Scientific Publishing, 2024, pp. 223–252, doi: 10.4018/979-8-3693-5443-8.ch008.

[13] R. S. Hirschprung, S. Tayro, and E. Reznik, "Optimising technological literacy acquirement to protect privacy and security," *Behaviour and Information Technology*, vol. 41, no. 5, pp. 922–933, 2022, doi: 10.1080/0144929X.2020.1842907.

[14] A. A. M. C. Dyanggi, N. Islam, and R. Rian, "Digital Literacy as An Effort to Build National Resilience in Defending the Country in the Digital Field," *Journal of Digital Law and Policy*, vol. 1, no. 3, pp. 121–130, 2022, doi: 10.58982/jdlp.v1i3.202.

[15] Ł. Tomczyk and L. Eger, "Online safety as a new component of digital literacy for young people," *Integration of Education*, vol. 24, no. 2, pp. 172–184, 2020, doi: 10.15507/1991-9468.099.024.202002.172-184.

[16] Ł. Tomczyk and K. Potyrała, "Parents' knowledge and skills about the risks of the digital world," *South African Journal of Education*, vol. 41, no. 1, pp. 1–19, 2021, doi: 10.15700/saje.v41n1a1833.

[17] M. J. Latorre-Medina and C. Tnibar-Harrus, "Digital Security in Educational Training Programs: a Study Based on Future Teachers' Perceptions," *Information Technologies and Learning Tools*, vol. 95, no. 3, p. 102, 2023, doi: 10.33407/itlt.v95i3.5204.

[18] S. A. Jawaid, "Cyber Security Threats to Educational Institutes: A Growing Concern for the New Era of Cybersecurity," *International Journal of Data Science and Big Data Analytics*, vol. 2, no. 2, pp. 1–18, 2023, doi: 10.51483/ijdsbda.2.2.2022.11-17.

[19] V. G. Dharmavaram, "Data Privacy in Education Sector–Issues and Measures," *The EDP Audit, Control, and Security Newsletter*, vol. 68, no. 2, pp. 1–12, 2023, doi: 10.1080/07366981.2023.2242130.

[20] E. Ifinedo and M. Kankaanranta, "Understanding the influence of context in technology integration from teacher educators' perspective," *Technology, Pedagogy and Education*, vol. 30, no. 2, pp. 201–215, 2021, doi: 10.1080/1475939X.2020.1867231.

[21] O. Wohlfart and I. Wagner, "Teachers' role in digitalizing education: an umbrella review," *Educational Technology Research and Development*, vol. 71, no. 2, pp. 339–365, 2023, doi: 10.1007/s11423-022-10166-0.

[22] C. J. M. Granda, L. Y. G. Asencio, and W. A. C. Cajamarca, "Teacher's role in digital literacy in the 21st century," (in Spanish), *Sociedad & Tecnología*, vol. 4, no. S2, pp. 350–363, 2021, doi: 10.51247/st.v4is2.156.

[23] R. Zakia and D. Yana, "English Teachers' Perception of Security in Digital Literacy Competence," *Journal on Education*, vol. 5, no. 3, pp. 8873–8882, 2023, doi: 10.31004/joe.v5i3.1685.

[24] Y. Gao *et al.*, "Reporting guideline for systematic review: Comparative analysis of PRISMA 2020 and PRISMA 2009," *Chinese Journal of Evidence-Based Medicine*, vol. 21, no. 5, pp. 606–616, 2021, doi: 10.7507/1672-2531.202104143.

[25] M. J. Page *et al.*, "Updating guidance for reporting systematic reviews: development of the PRISMA 2020 statement," *Journal of Clinical Epidemiology*, vol. 134, pp. 103–112, 2021, doi: 10.1016/j.jclinepi.2021.02.003.

[26] S. Sánchez-Serrano, I. Pedraza-Navarro, and M. Donoso-González, "How to conduct a systematic review under PRISMA protocol? Uses and fundamental strategies for its application in the educational field through a practical case study," *Bordon. Revista de Pedagogía*, vol. 74, no. 3, pp. 51–66, 2022, doi: 10.13042/Bordon.2022.95090.

[27] M. Aria and C. Cuccurullo, "bibliometrix: An R-tool for comprehensive science mapping analysis," *Journal of Informetrics*, vol. 11, no. 4, pp. 959–975, 2017, doi: 10.1016/j.joi.2017.08.007.

[28] M. Gusenbauer and N. R. Haddaway, "Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources," *Research Synthesis Methods*, vol. 11, no. 2, pp. 181–217, 2020, doi: 10.1002/jrsm.1378.

[29] S. Kraus, M. Breier, and S. Dasí-Rodríguez, "The art of crafting a systematic literature review in entrepreneurship research," *International Entrepreneurship and Management Journal*, vol. 16, no. 3, pp. 1023–1042, 2020, doi: 10.1007/s11365-020-00635-4.
[30] P. Robinson and J. Lowe, "Literature reviews vs systematic reviews," *Australian and New Zealand Journal of Public Health*, vol. 39, no. 2, p. 103, 2015, doi: 10.1111/1753-6405.12393.
[31] N. Torres-Hernández and M. J. Gallego-Arrufat, "Indicators to assess preservice teachers' digital competence in security: A systematic review," *Education and Information Technologies*, vol. 27, no. 6, pp. 8583–8602, 2022, doi: 10.1007/s10639-022-10978-w.
[32] P. H. Pradana, K. Agustini, G. R. Dantes, and I. G. W. Sudatha, "The Urgency of Digital Literacy Learning in Educational Units: Systematic Literature Review," *Child Education Journal*, vol. 6, no. 1, pp. 25–33, 2024, doi: 10.33086/cej.v6i1.6100.
[33] M. C. Demirdağ and A. Taşgın, "The Relationship Between Teachers' Digital Literacy Levels and Research Literacy Skills," *Kuramsal Eğitimbilim*, vol. 18, no. 1, pp. 81–105, Jan. 2025, doi: 10.30831/akukeg.1507150.
[34] L. Vásquez-Pajuelo, J. R. Rodriguez-Barboza, K. R. Bartra-Rivero, E. A. Quintanilla-Alarcón, W. Vega-Jaime, and E. F. Chavarri-Joo, "Digital Challenges: The Need to Improve the Use of Information Technologies in Teaching," *Data and Metadata*, vol. 3, p. 216, 2024, doi: 10.56294/dm2024216.
[35] V. Marinescu, A. A. Rodideal, and R. Marinache, "Risks and Opportunities for Education in Romania During the COVID-19 Pandemic," *Anthropological Researches and Studies*, vol. 2024, no. 14, pp. 73–81, 2024, doi: 10.26758/14.1.6.
[36] I. Ballester-Esteve, D. Parra-Camacho, L. Padilla-Bautista, and R. Fernández-Piqueras, "Adaptation and validation of a scale to assess digital teaching competence in soccer coaches," *Journal of Physical Education and Sport*, vol. 23, no. 1, pp. 112–121, 2023, doi: 10.7752/jpes.2023.01014.
[37] M. Á. García-Delgado, S. Rodríguez-Cano, V. Delgado-Benito, and C. Di Giusto-Valle, "Digital Teaching Competence among Teachers of Different Educational Stages in Spain," *Education Sciences*, vol. 13, no. 6, p. 581, 2023, doi: 10.3390/educsci13060581.
[38] M. M. Gümüş and V. Kukul, "Developing a digital competence scale for teachers: validity and reliability study," *Education and Information Technologies*, vol. 28, no. 3, pp. 2747–2765, 2023, doi: 10.1007/s10639-022-11213-2.
[39] P. Korukluoğlu, B. Alci, and C. Rubach, "Reliability and validity of the Turkish version of the teachers' basic ICT competence beliefs scale," *International Journal of Assessment Tools in Education*, vol. 10, no. 1, pp. 29–55, 2023, doi: 10.21449/ijate.995005.
[40] F. Martin, J. Bacak, D. Polly, W. Wang, and L. Ahlgrim-Delzell, "Teacher and School Concerns and Actions on Elementary School Children Digital Safety," *TechTrends*, vol. 67, no. 3, pp. 561–571, 2023, doi: 10.1007/s11528-022-00803-z.
[41] H. Park, "Exploring digital literacy in the context of remote education for Korean elementary school teachers: Challenges, efforts, and demands," *KEDI Journal of Educational Policy*, vol. 20, no. 1, pp. 63–88, 2023.
[42] M. Perifanou, A. A. Economides, and S. A. Nikou, "Teachers' Views on Integrating Augmented Reality in Education: Needs, Opportunities, Challenges and Recommendations," *Future Internet*, vol. 15, no. 1, p. 20, 2023, doi: 10.3390/fi15010020.
[43] F. N. A. Ramli and N. M. Arsad, "STEM Teacher Digital Literacy: Relationship Between Digital Literacy and Technology Integration in Teaching and Learning Post COVID-19," *Journal of Nusantara Studies (JONUS)*, vol. 8, no. 2, pp. 316–333, 2023, doi: 10.24200/jonus.vol8iss2pp316-333.
[44] E. Vázquez-Cano, J. M. Sáez-López, R. Ó. Grimaldo-Santamaría, and M. del P. Quicios-García, "Influence of Age, Gender and Years of Experience on Teachers in Promoting Strategies for Digital Sustainability and Data Protection," *Journal of New Approaches in Educational Research*, vol. 12, no. 2, pp. 307–322, 2023, doi: 10.7821/naer.2023.7.1467.
[45] Z. Wang and Z. Chu, "Examination of Higher Education Teachers' Self-Perception of Digital Competence, Self-Efficacy, and Facilitating Conditions: An Empirical Study in the Context of China," *Sustainability*, vol. 15, no. 14, p. 10945, 2023, doi: 10.3390/su151410945.
[46] A. Basantes-Andrade, M. Cabezas-González, S. Casillas-Martín, M. Naranjo-Toro, and A. Benavides-Piedra, "NANO-MOOCs to train university professors in digital competences," *Heliyon*, vol. 8, no. 6, p. e09456,2022, doi: 10.1016/j.heliyon.2022.e09456.
[47] R. A. Galustov, I. V. Gerlach, M. N. Egizaryants, K. R. Kapieva, and I. A. Tvelova, "Monitoring and analysis of professional deficits of teachers in the field of psychological and pedagogical competencies, manifested in the conditions of digital transformation of education," *Perspektivy Nauki i Obrazovania*, vol. 59, no. 5, pp. 585–599, 2022, doi: 10.32744/pse.2022.5.35.
[48] M. X. Majola and P. K. Mudau, "Lecturers' Experiences of Administering Online Examinations at a South African Open Distance e-Learning University During the COVID-19 Pandemic," *International Journal of Educational Methodology*, vol. 8, no. 2, pp. 275–283, 2022, doi: 10.12973/ijem.8.2.275.
[49] A. Gordillo, E. Barra, P. Garaizar, and S. López-Pernas, "Use of a Simulated Social Network as an Educational Tool to Enhance Teacher Digital Competence," *Revista Iberoamericana de Tecnologias del Aprendizaje*, vol. 16, no. 1, pp. 107–114, 2021, doi: 10.1109/RITA.2021.3052686.
[50] A. Gordillo, E. Barra, S. López-Pernas, and J. Quemada, "Development of teacher digital competence in the area of e-safety through educational video games," *Sustainability*, vol. 13, no. 15, p. 8485, 2021, doi: 10.3390/su13158485.
[51] K. Potyrała and Ł. Tomczyk, "Teachers in the lifelong learning process: examples of digital literacy," *Journal of Education for Teaching*, vol. 47, no. 2, pp. 255–273, 2021, doi: 10.1080/02607476.2021.1876499.
[52] C. Rubach and R. Lazarides, "Addressing 21st-century digital skills in schools – Development and validation of an instrument to measure teachers' basic ICT competence beliefs," *Computers in Human Behavior*, vol. 118, p. 106638, 2021, doi: 10.1016/j.chb.2020.106636.
[53] R. E. Sitoy, P. Ndinga, M. Plaisent, B. Prosper, and E. D. Peteros, "Intelligence style and digital literacy," *Journal of E-Learning and Higher Education*, vol. 2021, p. 234285, 2021, doi: 10.5171/2021.234285.
[54] Y. Zhao, A. M. P. Llorente, M. C. S. Gómez, and L. Zhao, "The impact of gender and years of teaching experience on college teachers' digital competence: an empirical study on teachers in Gansu Agricultural University," *Sustainability*, vol. 13, no. 8, p. 4163, 2021, doi: 10.3390/su13084163.
[55] R. Barragán-Sánchez, M. C. Corujo-Vélez, A. Palacios-Rodríguez, and P. Román-Graván, "Teaching digital competence and eco-responsible use of technologies: Development and validation of a scale," *Sustainability*, vol. 12, no. 18, p. 7721, 2020, doi: 10.3390/su12187721.
[56] D. F. Elmali, D. A. Tekin, and E. Polat, "A Study on Digital Citizenship: Preschool Teacher Candidates Vs. Computer Education and Instructional Technology Teacher Candidates," *Turkish Online Journal of Distance Education*, vol. 21, no. 4, pp. 251–269, 2020, doi: 10.17718/TOJDE.803423.
[57] C. Martinez, "Imagine the Person in Front of You: How Teachers Promote Responsible Online Communication in Swedish Leisure-Time Centers," *Scandinavian Journal of Educational Research*, vol. 65, no. 6, pp. 899–913, Sep. 2021, doi: 10.1080/00313831.2020.1788140.
[58] Ł. Tomczyk, "Skills in the area of digital safety as a key component of digital literacy among teachers," *Education and Information Technologies*, vol. 25, no. 1, pp. 471–486, 2020, doi: 10.1007/s10639-019-09980-6.

[59] J. J. Fayzullayev, "Improving the Pedagogical Aspects of Ensuring the Information Security of Students," *Current Research Journal of Pedagogics*, vol. 5, no. 12, pp. 67–70, 2024, doi: 10.37547/pedagogics-crjp-05-12-13.
[60] S. Gabrielli, S. Rizzi, S. Carbone, and E. M. Piras, "School Interventions for Bullying–Cyberbullying Prevention in Adolescents: Insights from the UPRIGHT and CREEP Projects," *International Journal of Environmental Research and Public Health*, vol. 18, no. 21, p. 11697, Nov. 2021, doi: 10.3390/ijerph182111697.
[61] S. Nurzhanova, A. Stambekova, K. Zhaxylikova, G. Tatarinova, E. Aitenova, and Z. Zhumabayeva, "Investigation of Future Teachers' Digital Literacy and Technology Use Skills," *International Journal of Education in Mathematics, Science and Technology*, vol. 12, no. 2, pp. 387–405, Nov. 2023, doi: 10.46328/ijemst.3826.
[62] M. Hawamdeh, "The Students and Faculty Perception of Digital Citizenship Practices in Distance Learning Environment – The Case Study of Al-Quds Open University," *Qeios*. pp. 1–14, Feb. 15, 2023, doi: 10.32388/WNFPP1.
[63] B. Alkhazi, M. Alshaikh, S. Alkhezi, and H. Labbaci, "Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior," *IEEE Access*, vol. 10, pp. 132132–132143, 2022, doi: 10.1109/ACCESS.2022.3230286.
[64] M. A. Hameed and N. A. G. Arachchilage, "The role of self-efficacy on the adoption of information systems security innovations: a meta-analysis assessment," *Personal and Ubiquitous Computing*, vol. 25, no. 5, 2021, doi: 10.1007/s00779-021-01560-1.
[65] A. Marotta and S. Madnick, "Convergence and divergence of regulatory compliance and cybersecurity," *Issues in Information Systems*, vol. 22, no. 1, pp. 10–50, 2021, doi: 10.48009/1_iis_2021_10-50.
[66] S. Ghosh, G. S. Chauhan, and R. Kotwal, "Sanctity of Digital Privacy and Personal Data during COVID-19: Are Youths Enough Digitally Literate to Deal with it?" *Digital Education Review*, no. 43, pp. 131–150, 2023, doi: 10.1344/der.2023.43.131-150.
[67] M. Temirkhanova, G. Abildinova, and C. Karaca, "Enhancing digital literacy skills among teachers for effective integration of computer science and design education: a case study at Astana International School, Kazakhstan," *Frontiers in Education*, vol. 9, p. 1408512, 2024, doi: 10.3389/feduc.2024.1408512.
[68] M. Máthé, H. Verhagen, and M. Wiklund, "Investigating Social Media Potential for Supporting Teachers' Digital Games Literacy," in *ECGBL 2022 16th European Conference on Game-Based Learning*, pp. 329–338, 2022, doi: 10.34190/ecgbl.16.1.712.
[69] J. Dewitt and C. Cicalese, "Contextual integration: A framework for presenting social, legal, and ethical content across the computer security and information assurance curriculum," in *Proceedings of the 2006 Information Security Curriculum Development Conference, InfoSecCD '06*, 2007, pp. 30–40, doi: 10.1145/1231047.1231054.
[70] M. Montenegro-Rueda and J. M. Fernández-Batanero, "Adaptation and validation of an instrument for assessing the digital competence of special education teachers," *European Journal of Special Needs Education*, vol. 39, no. 3, pp. 367–382, 2024, doi: 10.1080/08856257.2023.2216573.
[71] A. Parveen, F. Bashir, A. Nazir, P. N. Zimik, and S. Jan, "Pedagogical Strategies for Developing Digital Literacy," in *Digital Literacy at the Intersection of Equity, Inclusion, and Technology*, K. B. Prager and N. Bilge, Eds., Hershey, PA: IGI Global Scientific Publishing, 2024, pp. 255–274, doi: 10.4018/979-8-3693-2591-9.ch011.
[72] R. Vuorikari, "DigComp Helping Shape the Education Ecosystem in Europe," in *Annual Conference of European Distance and E-Learning Network*, 2022, pp. 137–143, doi: 10.1007/978-3-031-20518-7_11.
[73] A. R. Trindade, D. Holley, and C. G. Marques, "Skills for Safety, Security, and Well-Being in the DigComp Framework Revision and Their Relevance for a Sustainable Global (Higher) Education," *Technologies for Sustainable Global Higher Education*, M. J. Sousa, A. de B. Machado, and G. A. Dandolini, Eds., New York: Auerbach Publications, 2023, pp. 45–76, doi: 10.1201/9781003424543-4.
[74] V. Betancur-Chicué and A. G.-V. Muñoz-Repiso, "Training Needs around Digital Teaching Competence: a Systematic Review," *Fonseca Journal of Communication*, no. 25, pp. 133–146, 2022, doi: 10.14201/fjc.29603.
[75] A. Palacios-Rodríguez, F. D. Guillén-Gámez, J. Cabero-Almenara, and J. J. Gutiérrez-Castillo, "Teacher Digital Competence in the stages of Compulsory Education according to DigCompEdu: The impact of demographic predictors on its development," *Interaction Design and Architecture(s)*, no. 57, pp. 115–132, Jun. 2023, doi: 10.55612/s-5002-057-007.
[76] H. Crompton, "Evidence of the ISTE Standards for Educators leading to learning gains," *Journal of Digital Learning in Teacher Education*, vol. 39, no. 4, pp. 201–219, 2023, doi: 10.1080/21532974.2023.2244089.
[77] P. A. Pasque and C. Gilbert, "Theoretical and Conceptual Frameworks: Understanding the Role of Theory in Congruent Research Designs," in *A Practical Guide to Teaching Research Methods in Education: Lesson Plans and Advice from Faculty*, A. L. Terosky, V. L. Baker, and J. C. Sun, Eds., London: Routledge, 2023, pp. 52–61, doi: 10.4324/b23320-11.
[78] A. Kandiero, S. Bigirimana, and S. Chizwina, *Theoretical and conceptual frameworks in ICT research*. Hershey, PA: IGI Global Scientific Publishing, 2024.
[79] T. D. Dang, T. T. Phan, T. N. Q. Vu, T. D. La, and V. K. Pham, "Digital competence of lecturers and its impact on student learning value in higher education," *Heliyon*, vol. 10, no. 17, p. e37318, 2024, doi: 10.1016/j.heliyon.2024.e37318.
[80] J. Y. Lee, Y. S. Yang, P. N. Ghauri, and B. Il Park, "The Impact of Social Media and Digital Platforms Experience on SME International Orientation: The Moderating Role of COVID-19 Pandemic," *Journal of International Management*, vol. 28, no. 4, 100950, 2022, doi: 10.1016/j.intman.2022.100950.
[81] B. McAteer and W. Flannery, "Network governance and reflexivity in fisheries management: a case study of Northern Ireland," *Journal of Environmental Policy & Planning*, vol. 27, no. 1, pp. 21–33, Jan. 2024, doi: 10.1080/1523908X.2024.2395860.
[82] M. D. Gurer, "Examining technology acceptance of pre-service mathematics teachers in Turkey: A structural equation modeling approach," *Education and Information Technologies*, vol. 26, no. 4, pp. 4709–4729, 2021, doi: 10.1007/s10639-021-10493-4.
[83] M. J. Mohamed and S. A. Hassan, "Studying the Factors that Influence the Adoption of Educational Technology in Mogadishu Secondary Schools Using UTAUT Model," *International Journal of Information and Education Technology*, vol. 13, no. 7, pp. 1070–1077, 2023, doi: 10.18178/ijiet.2023.13.7.1906.
[84] A. González-Marcos, F. Navaridas-Nalda, and J. Castellano-Latorre, "Design and Validation of an Emerging Educational Technologies Acceptance and Integration Questionnaire for Teachers," in *Proceedings of the 13th International Conference on Computer Supported Education (CSEDU 2021)*, 2021, pp. 525–532, doi: 10.5220/0010526705250532.
[85] F. Deng, W. Lan, D. Sun, and Z. Zheng, "Examining Pre-Service Chemistry Teachers' Technological Pedagogical Content Knowledge (TPACK) of Using Data-Logging in the Chemistry Classroom," *Sustainability*, vol. 15, no. 21, p. 15441, 2023, doi: 10.3390/su152115441.
[86] H. Gardner and T. Hatch, "Educational Implications of the Theory of Multiple Intelligences," *Educational Researcher*, vol. 18, no. 8, pp. 4–10, 1989, doi: 10.3102/0013189X018008004.
[87] M. M. Gümüş, R. Çakır, and Ö. Korkmaz, "Investigation of pre-service teachers' sensitivity to cyberbullying, perceptions of digital ethics and awareness of digital data security," *Education and Information Technologies*, vol. 28, no. 11, pp. 14399–14421, 2023, doi: 10.1007/s10639-023-11785-7.

[88] P. J. R. Macaulay and L. R. Betts, "Cyberbullying in school: The role of teachers," in *Cyberbullying and Values Education: Implications for Family and School Education*, A. N. M. Leung, K. K. S. Chan, C. S. M. Ng, and J. C.-K. Lee, Eds., London: Routledge, 2023, pp. 156–171, doi: 10.4324/9781003314509-13.
[89] J. Rajbhandari and K. Rana, "Cyberbullying on Social Media: an Analysis of Teachers' Unheard Voices and Coping Strategies in Nepal," *International Journal of Bullying Prevention*, vol. 5, no. 2, pp. 95–107, 2023, doi: 10.1007/s42380-022-00121-1.
[90] M. Hess, A. Schultze-Krumbholz, and H. Scheithauer, "Effects of the Preventive Intervention Program 'Media Heroes' on the Association Between Traditional and Cyberbullying and Internalizing Problems," (in German), *Kindheit und Entwicklung*, vol. 29, no. 2, pp. 92–100, Apr. 2020, doi: 10.1026/0942-5403/a000307.
[91] G. Falloon, "From digital literacy to digital competence: the teacher digital competency (TDC) framework," *Educational Technology Research and Development*, vol. 68, no. 5, pp. 2449–2472, 2020, doi: 10.1007/s11423-020-09767-4.
[92] J. T. Nagy and I. Dringó-Horváth, "Factors Influencing University Teachers' Technological Integration," *Education Sciences*, vol. 14, no. 1, p. 55, 2024, doi: 10.3390/educsci14010055.
[93] J. B. Grace, "General guidance for custom-built structural equation models," *One Ecosystem*, vol. 7, p. e72780, 2022, doi: 10.3897/oneeco.7.e72780.
[94] M. Salama and R. Farag, "Factors Affecting Public Adoption of Digital Government Services: Theoretical Perspectives and Model Development," in *2024 International Conference on Decision Aid Sciences and Applications (DASA)*, 2024, pp. 1–8, doi: 10.1109/DASA63652.2024.10836593.
[95] M. Sabol, J. Hair, G. Cepeda, J. L. Roldán, and A. Y. L. Chong, "PLS-SEM in information systems: seizing the opportunity and marching ahead full speed to adopt methodological updates," *Industrial Management and Data Systems*, vol. 123, no. 12, pp. 2997–3017, 2023, doi: 10.1108/IMDS-07-2023-0429.
[96] A. S. Ahmad *et al.*, "A method of correction for heaping error in the variables using validation data," *Statistical Papers*, vol. 65, no. 2, pp. 687–704, 2024, doi: 10.1007/s00362-023-01405-4.
[97] G. B. Sarzhanova, S. T. Abdrakhmanova, G. N. Akbayeva, and G. K. Tleuzhanova, "Digital Learning Environment in Training Future Kazakhstani English Teachers," *Forum for Linguistic Studies*, vol. 6, no. 5, pp. 280–286, 2024, doi: 10.30564/fls.v6i5.7039.

BIOGRAPHIES OF AUTHORS

Nadirah Othman received a B.Sc. in statistics from Universiti Teknologi MARA (UiTM) in 2009 and a M.Sc. in statistics from UiTM in 2012. Currently, she is pursuing a Ph.D. in statistics, focusing on advanced statistical methodologies and their applications in various domains. Her research interests include structural equation modeling and the integration of statistical methods with machine learning techniques. She can be contacted at email: nadirahothman2021@gmail.com.

Nor Aslily Sarkam is a senior lecturer at the Universiti Teknologi MARA (UiTM). She is the coordinator postgraduate of College of Computing, Informatics and Mathematics at Universiti Teknologi MARA (UiTM) Perak Branch. She received her Ph.D. in management from the Tohoku University Japan in 2018. She started her career as a lecturer at UiTM Perak Branch in 2000, specializing in statistics. Other academic qualifications include both master degree and bachelor's degree in statistics from Universiti Teknologi MARA. Among her recent achievements include on-going and complete research grants (leader and members), 17 indexed journal publications. Her research interest is in SEM and educational technology. She can be contacted at email: noraslilysarkam@uitm.edu.my.

Norhayati Baharun is a professor of statistics at Universiti Teknologi MARA Perak Branch, Tapah Campus. She received her Ph.D. in statistics education from the University of Wollongong Australia in 2012. Her career started as an academic from January 2000 to date at the Universiti Teknologi MARA that specialized in statistics. Other academic qualifications include both master degree and bachelor degree in statistics from Universiti Sains Malaysia and diploma in statistics from Institute Teknologi MARA. She is also a certified Professional Technologist (Ts.) (Information and Computing Technology) of the Malaysia Board of Technologist (MBOT), a fellow member of the Royal Statistical Society (RSS), London, United Kingdom, a professional member of Association for Computing Machinery (ACM), New York, USA, and a Certified Neuro Linguistic Program (NLP) Coach of the Malaysia Neuro Linguistic Program Academy. Her research interests continue with current postgraduate students under her supervision in decision science now expanding to a machine learning application. She can be contacted at email: norha603@uitm.edu.my.

Teoh Sian Hoon is a professor at the Faculty of Education, Universiti Teknologi MARA (UiTM). She received her B.Sc. (Hons.) from Universiti Teknologi Malaysia (UTM), M.Sc., and Ph.D. from Universiti Sains Malaysia (USM). She actively engages in mathematics education teaching and supervising thesis students. Her research interests include mathematics and statistics education, with a particular emphasis on the mathematical process, STEM teaching, and modelling in a multidisciplinary context. She actively participates in research initiatives and makes valuable contributions to academic discourse through her papers and conference presentations. She can be contacted at email: teohsian@uitm.edu.my.

Suraya Masrom received her Ph.D. in Information Technology and Quantitative Science from UiTM in 2015. She started her career in the information technology industry as an Associate Network Engineer at Ramgate Systems Sdn. Bhd (a subsidiary of DRB-HICOM) in June 1996 after receiving her bachelor's degree in Computer Science from Universiti Teknologi Malaysia (UTM) in Mac 1996. She started her career as a lecturer at UTM after receiving her master's degree in computer science from Universiti Putra Malaysia in 2001. She transferred to the Universiti Teknologi MARA (UiTM), Seri Iskandar, Perak, Malaysia, in 2004. She is an active researcher in the meta-heuristics search approach, machine learning, and educational technology. She can be contacted at email: suray078@uitm.edu.my.

Nor Faezah Mohamad Razi is a senior lecturer at Universiti Teknologi MARA (UiTM). She is the resource person for fundamentals of research. She received her B.Sc. in Statistics and MSc in Applied Statistics from UiTM in 2009 and 2012 respectively. Currently, she pursues her Ph.D. study in the decision science area. Her research interest is in structural equation modeling (SEM), data envelopment analysis and educational technology. She can be contacted at email: norfa122@uitm.edu.my.

Abdullah Sani Abd Rahman obtained his first degree in Informatique majoring in industrial systems from the University of La Rochelle, France in 1995. He received a master's degree from Universiti Putra Malaysia in computer science, with specialization in Distributed Computing. Currently, he is a lecturer at the Universiti Teknologi PETRONAS, Malaysia and a member of the Institute of Autonomous System at the same university. His research interests are cybersecurity, data analytics and machine learning. He is also a registered Professional Technologist. He can be contacted at email: sani.arahman@utp.edu.my.