Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

A Systematic Literature Review of AI-Driven Security Assessment and Regulatory Compliance in Cloud-Edge Environments

Rasha Almarshood[1*], Abdullah Albuali[1*]

[1]*Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia*

ARTICLE INFO

Article History

Received: 25-03-2026
Revised: 30-06-2026
Accepted: 15-07-2026
Published: 29-07-2026

Vol.2026, No.3

DOI:

***Corresponding author. Email:** 224108485@student.kfu.edu.sa and aabuali@kfu.edu.sa

Orcid: https://orcid.org/0009-0003-8600-7499

ABSTRACT

Cloud and edge systems increasingly depend on AI to address evolving security threats. This reliance underscores the importance of regulatory compliance. Although global regulations such as GDPR and HIPAA have been widely examined, national regulatory frameworks remain insufficiently explored. This paper systematically reviews AI-driven approaches for security assessments in cloud-edge environments, focusing on their adherence to regulatory compliance requirements. The review followed the PRISMA 2020 guidelines to identify, screen, and analyze 30 studies published between 2020 to 2025 from databases such as IEEE Xplore and SpringerLink. Approximately 40% of the studies use Federated Learning (FL), while 30% use NLP techniques. The analysis reveals that 80% of the studies examined GDPR, while HIPAA and the EU AI Act received minimal attention. As a result, the review highlights a lack of unified frameworks integrating security with compliance. This limitation reduces applicability for non-EU regulations such as Saudi Arabia's NCA and PDPL. To address these gaps, this paper presents the E-EDGE-GRC framework. It uses a multi-level architecture and a maturity scoring system to automate compliance with Saudi national requirements and global standards. These findings and the proposed framework offer a basis for unified, multi-regulatory AI security assessments.

Keywords: Artificial Intelligence, Security Assessment, Cloud Computing, Edge Computing, Regulatory Compliance, GDPR, EU AI Act, Federated Learning.

How to cite the article

1. Introduction

Cloud and edge computing are foundational architectures of modern digital infrastructure. These technologies enable scalability and real-time services across various industries, including finance, healthcare, and smart city infrastructure. However, the increasing reliance on distributed data processing introduces significant security challenges. Additionally, the pressure to comply with governance regulations is increasing. Therefore, ensuring efficient security assessments and maintaining regulatory compliance are crucial. Frameworks such as GDPR and HIPAA represent legal regulations, and security assessments verify compliance with them [1, 2].

Artificial Intelligence (AI) is used to address a variety of challenges by providing advanced methods for enhancing security capabilities. AI can provide privacy-preserving analytics, compliance verification, and risk monitoring. Knowledge graphs are used to automate GDPR compliance [3]. Federated learning (FL) is increasingly applied in cloud-edge scenarios. This approach can enhance privacy and enable security assessments without centralized data collection [4]. Additionally, Natural Language Processing (NLP) and hybrid rule-based and machine learning models are employed for contract analysis. Prior studies highlight the importance of AI-based compliance systems. These include healthcare data governance and AI Act-aligned risk monitoring [5, 6].

Despite these advantages, the integration of legal frameworks and technical performance remains limited. Many studies focus solely on privacy-preserving methods or the security of distributed systems. However, these studies have not specifically demonstrated compliance with regulatory requirements [7]. Many AI-based cloud-edge security models lack measurable evidence of compliance with regulations. Additionally, legal and governance studies often lack detailed technical information on AI. There is a lack of understanding of how AI techniques can ensure robust security and comply with formal regulatory standards. This gap motivates this review to analyze AI-based cloud-edge security assessments focusing on regulatory compliance. The objective is to explore existing models, identify relevant frameworks, and address open challenges for AI adoption.

This review systematically analyzes research from 2020 to 2025. It investigates the role of AI in supporting cloud and edge security assessments. Moreover, the review identifies the main methods associated with regulatory compliance while also highlighting the limitations and research opportunities. To address the identified gap, this review is guided by the following research questions (RQs):

• RQ1: Which AI techniques are currently applied to assess security in cloud-edge environments?

• RQ2: How do these techniques support or automate compliance with major regulations and national frameworks?

• RQ3: What are the key limitations and open challenges in designing AI-driven systems for multi-regulation security compliance?

This paper contributes to the current field by providing:

• A clear taxonomy of AI techniques currently applied to security and regulatory compliance in cloud-edge environments.

• A comparative mapping of these techniques against major global regulations and emerging national frameworks with particular attention to gaps in coverage related to Saudi Arabia's National Cybersecurity Authority (NCA) controls and Personal Data Protection Law (PDPL).

• Identification of the main research gaps and directions, emphasizing the necessity of unified compliance frameworks that can address multiple regulations.

This paper is structured as follows: Section 2 outlines the methodology for selecting related studies. Section 3 provides background on AI, cloud-edge computing, and their connection to regulatory compliance. Section 4 reviews the related studies and compares previous research to identify key findings, limitations, and contributions. Section 5 presents a comparative analysis of AI techniques based on compliance automation and risk assessment systems. Section 6 presents the results. Section 7 discusses the findings. Section 8 provides recommendations and future directions. Section 9 concludes the paper.

2. Methodology

This study applied a systematic literature review (SLR) methodology. The methodology was based on PRISMA to ensure transparency and reproducibility. The review is derived from the following objectives: (1) to identify and classify AI approaches applied for cloud and edge security assessments, (2) to investigate the approaches that address regulatory compliance frameworks such as GDPR, HIPAA, and the EU AI Act, and (3) to analyze the strengths, limitations, and gaps of AI-based compliance systems. Based on these objectives, this paper will address the following research questions. This paper will examine the application of AI models and techniques in cloud and edge security assessments. Privacy-preserving and federated methods were examined as key mechanisms for AI-based compliance support.

2.1 Search String

The search for related studies was conducted across high-ranking databases such as IEEE Xplore, SpringerLink, MDPI, and the Saudi Digital Library. We used keywords including "AI" OR "ML" AND "Cloud Security Assessment"; "Edge Computing" AND "Federated Learning" OR "HIPAA" OR "AI Act" AND "AI security". Studies published between 2020 and 2025 were included. The inclusion criteria specifically required studies to address AI-based cloud or edge security assessment with a link to regulatory compliance. Table 1 presents the search strategy used across the databases.

Table 1 Search Strategy

Database	Search String
IEEE Xplore	("AI" OR "ML") AND ("Cloud" OR "Edge") AND ("Security" AND "Compliance") OR ("GDPR" OR "AI Act")
SpringerLink	("Artificial Intelligence" OR "Machine Learning") AND ("Security Assessment") AND ("Regulatory Compliance")
MDPI	("AI" OR "Federated Learning") AND ("Cloud Computing" OR "Edge Computing") AND ("GDPR")
ScienceDirect	"AI" OR "NLP" AND "Security" AND "Compliance" AND "Cloud"
Saudi Digital Library	("AI" OR "Machine Learning") AND ("Cyber security") AND ("NCA" OR "Compliance")

2.2 Study Selection and PRISMA Flow

This paper follows the PRISMA guidance to ensure reproducibility and transparency. It provides a standardized framework for reporting the identification, screening, eligibility, and inclusion of studies. This helps reduce bias and enhance precision. The final review included 30 studies published between 2020 and 2025. Table 2 outlines the inclusion and exclusion criteria applied during study selection. Figure 1 illustrates the paper selection process for the literature review using the PRISMA 2020 flow diagram.

Table 2 Inclusion and Exclusion Criteria

Criterion	Inclusion	Exclusion
Time Period	2020–2025	Published before 2020
Language	English	Non-English
Publication Type	Peer-reviewed Journals, Conferences	Posters, Abstracts, purely legal essays without technical validation
Focus	Explicit use of AI for security/compliance in Cloud/Edge environments	Non-AI solutions, or papers lacking specific Cloud/Edge context
Content	Addressed both security assessment and regulatory compliance	Focused solely on theoretical law or purely technical security without compliance links

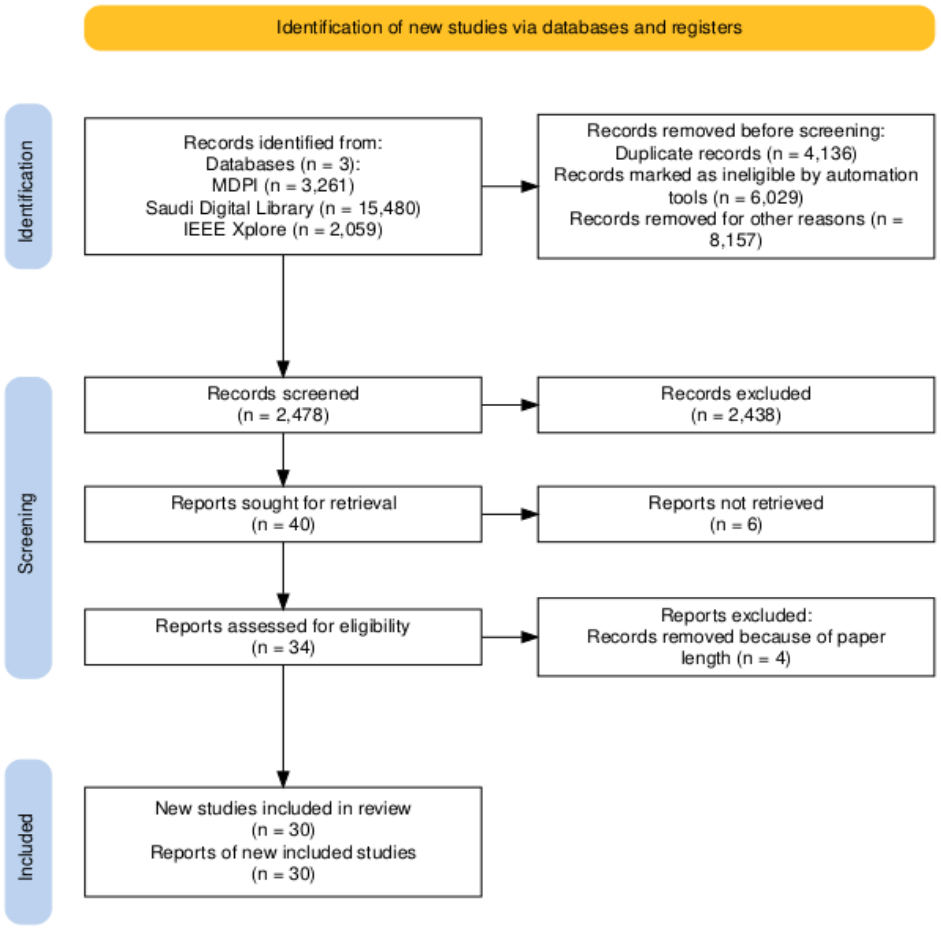


Figure 1 Papers selection for literature review using PRISMA 2020

2.3 Quality Assessment of Included Studies

We conducted a quality assessment of the final set of included studies using predefined criteria. A binary scoring scheme (Yes = 1, No = 0) was applied. The results show that most studies address regulatory compliance at a conceptual level with limited empirical validation. Moreover, large-scale cloud and edge deployment remains an unexplored research gap. Table 3 presents the quality assessment criteria and questions, and Table 4 summarizes the corresponding results for the included studies.

Table 3 Quality Assessment Criteria and Questions

QA ID	Assessment Criterion	Assessment Question
QA1	Research Clarity	Is the research objective or problem clearly stated and well-defined?
QA2	Methodological Rigor	Does the study clearly describe the AI-driven security or assessment methodology used?
QA3	Regulatory Compliance Coverage	Does the study explicitly address regulatory or compliance frameworks such as GDPR, HIPAA, EU AI Act, NCA?
QA4	Evaluation and Validation	Does the study provide experimental evaluation, case studies, or real-world validation?
QA5	Applicability to Cloud– Edge Environments	Is the proposed approach applicable to cloud, edge, or hybrid computing environments?

Table 4 Quality Assessment Results of Included Studies

Ref	QA1	QA2	QA3	QA4	QA5	TOTAL
[4]	**1**	**1**	**1**	**0**	1	4/5
[8]	**1**	**1**	**0**	**1**	1	4/5
[9]	**1**	**1**	**0**	**1**	1	4/5
[10]	**1**	**1**	**0**	**0**	1	3/5
[11]	**1**	**1**	**1**	**0**	1	4/5
[12]	**1**	**1**	**1**	**0**	0	3/5
[13]	**1**	**1**	**1**	**0**	0	3/5
[14]	**1**	**1**	**1**	**0**	0	3/5
[15]	**1**	**1**	**1**	**0**	0	3/5
[16]	**1**	**1**	**1**	**0**	1	4/5
[1]	**1**	**1**	**1**	**0**	0	3/5
[2]	**1**	**0**	**1**	**0**	0	2/5
[17]	**1**	**1**	**1**	**0**	1	4/5
[18]	**1**	**1**	**1**	**0**	0	3/5
[19]	**1**	**1**	**0**	**0**	1	3/5
[20]	**1**	**1**	**1**	**0**	1	4/5

2.4 Data Extraction

To ensure consistency, we used a standardized format to extract data from the 30 studies. We collected bibliographic details, including the authors, year, and publication source. This step ensures that the studies were recent, relevant, and traceable. We also identified the computing context, such as cloud, edge, or hybrid systems. By including the relevant studies within our scope and excluding unrelated studies, we mapped specific AI techniques, including FL and NLP. We included regulatory frameworks such as GDPR, HIPAA, and the EU AI Act. This helps in making our study more specific to emerging techniques. Lastly, we recorded the validation methods and key research limitations. This process formed the basis for the taxonomy and comparative analysis in Sections 4 and 5.

2.5 Overview of Included Studies

The 30 studies selected for this review were published between 2020 and 2025. The selected studies reflect increasing interest in AI-enabled cloud-edge security, particularly in healthcare, multi-cloud enterprise environments, and smart cities.

3. Background

3.1 Cloud and Edge Computing Overview

Modern distributed systems rely on cloud and edge computing. These systems provide scalable storage and flexible computational resources for large-scale data processing. Organizations can efficiently process data across different sectors [21]. A key advantage of edge computing is that computation can be performed close to data sources. These systems reduce latency and improve data privacy. Some papers highlight the importance of these systems for sensitive applications, such as the role of FL in enhancing performance without centralizing sensitive data [22].

Recent cloud outages, such as the 2021 AWS disruption and the 2022 Cloudflare failures, expose the heavy reliance on few cloud providers [23, 24]. These incidents may affect multiple services and disrupt authentication, data availability, and logging. Such incidents can disrupt service availability, authentication, logging, and data access. This emphasizes the necessity to design cloud-edge architectures that ensure security and compliance during such occurrences. Therefore, many organizations are considering adopting distributed and edge-based AI systems. These systems aim to sustain operations in the event of significant failures.

AI plays a crucial role in securing these environments. For instance, FL promotes privacy-preserving models. Models are trained across different IoT and edge devices. Moreover, FL has been integrated into real-time monitoring and IDS [25]. As systems become more complex, privacy-preserving and distributed AI architectures are essential. Regulatory compliance is another requirement that shapes cloud and edge integration. Examples of such compliance frameworks include EU regulations such as the GDPR [6].

While existing studies present AI integration in smart city system designs [21, 26], the increasing reliance on generative AI raises legal and privacy concerns. Furthermore, literature such as [7, 27] highlights compliance challenges for large language models. Despite these challenges, smart city systems require AI techniques to ensure strong security. Additionally, these AI-driven models maintain compliance with evolving regulatory frameworks and protect sensitive data in these environments.

3.2 AI Techniques for Security and Compliance

AI has emerged as an important element for securing systems and meeting regulatory requirements. This review identifies three main categories of AI techniques applied in this field:

- Federated Learning (FL): FL is the main approach used in approximately 40% of the reviewed studies. It ensures privacy in security assessments by training models locally without sharing sensitive data [4, 12]. This makes FL particularly suitable for healthcare and IoT contexts, where GDPR and HIPAA compliance is critical [20, 21, 28]. To reduce data leakage risks, recent developments combine FL with zero-trust architecture [13, 14].
- Natural Language Processing (NLP): NLP techniques are used to automate legal text interpretation in about 30% of the reviewed studies. These models extract requirements from privacy policies to verify GDPR compliance [3, 8]. Moreover, the impact of Large Language Models (LLMs) has been explored in recent studies on compliance challenges [11, 12].
- Knowledge Graphs and Semantic Models: These approaches provide an organized view of compliance rules. They reduce the need for human interaction by enabling automated reasoning and compliance verification [1, 2]. Furthermore, hybrid models combine rule-based logic and ML to enhance compliance verification accuracy.

3.3 Regulatory and Governance Background

Cloud and edge systems produce and process large amounts of sensitive data. This makes regulatory compliance a crucial requirement to secure and lawful operation. GDPR is an example of such a regulatory framework for data collection, storage, and usage. This framework highlights accountability, transparency, and security in cloud-edge architecture. It also promotes analytics and learning systems, as shown in [21, 26]. Furthermore, it helps organizations to design privacy-preserving data models.

Another example of regulations is the EU AI Act. It imposes additional obligations on high-risk AI systems, including requirements related to robustness, fairness, transparency, and human oversight. The effect of these rules on real-world AI integrations is highlighted in [6]. LLMs are modern AI models that raise new privacy and compliance issues. Some of these concerns include data leakage and lack of transparency [7, 27]. From an ethical perspective, the existing studies emphasize the need for responsible and reliable systems in such environments [26]. Overall, these regulations require careful design and monitoring of secure AI systems.

3.4 Global and National Regulatory Frameworks

Global regulations such as GDPR are widely discussed in the literature. However, national frameworks play a crucial role in compliant cloud environments. GDPR, which enforces strict requirements on data minimization and user consent, remains the global baseline for data privacy [4, 21]. HIPAA requires specific controls for protected health information (PHI), which is specifically relevant for edge-based medical diagnostics [17]. Recently, the EU AI Act has introduced a risk-based categorization for AI systems by imposing transparency and accountability requirements on high-risk AI models [1, 2].

National regulations define specific cybersecurity controls that cloud-edge systems must adhere to within their respective jurisdictions. The NCA enforces the ECC as a national baseline and the CCC specifically for cloud service providers [28]. Moreover, PDPL governs the processing and cross-border transfer of personal data. Current research shows a clear gap, as no documented AI system implements the requirements of Saudi Arabia's NCA ECC/CCC or PDPL.

3.5. Conceptual Mapping of AI, Infrastructure, and Compliance

We propose a conceptual model to explain the interaction between legal requirements and security measures. The infrastructure layer includes data creation and processing within distributed systems. The AI security layer uses advanced methods such as FL, NLP, and Knowledge graphs. The top regulatory layer represents legal frameworks
such as GDPR, Saudi Arabia's NCA, ECC, CCC, and PDPL. This layer specifies the compliance requirements for the underlying layers. Most of the existing studies focus on aligning AI security with GDPR, while technical implementations rarely address the specific obligations of Saudi regulations. Figure 2 presents the conceptual model of AI-driven security assessments across the infrastructure, AI, and regulatory layers.

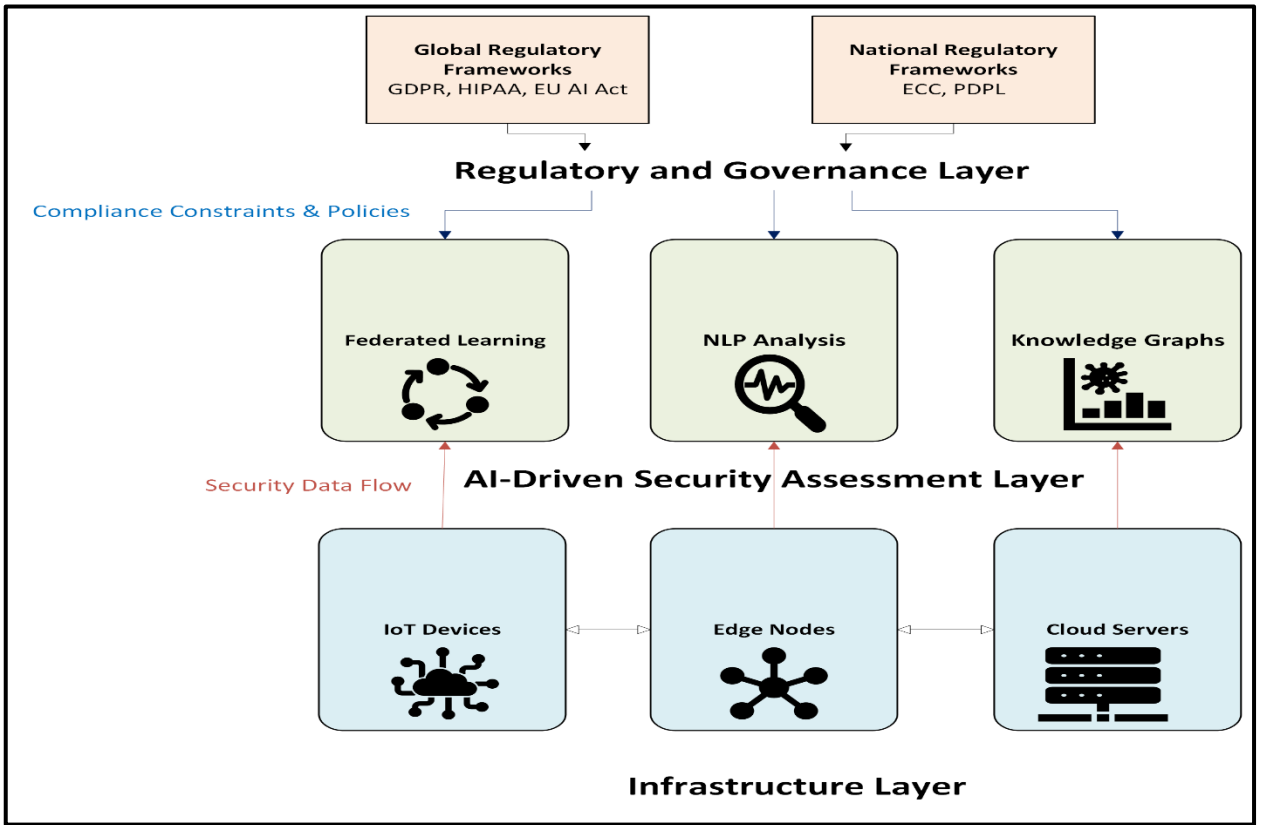


Figure 2 AI-driven Security Assessment Across Infrastructure, AI, and Regulatory Layers.

4. Literature Review

4.1 Overview of Selected Studies

Studies published between 2020 and 2025 highlight the increasing interest in AI-based cloud-edge security. The review shows that AI is increasingly adopted to support security and compliance. Among the 30 studies, FL represents 40%, NLP and other approaches represent 30% of the applied AI techniques. For regulations, GDPR was used in 80% of the studies, while HIPAA and the EU AI Act appeared in 10-13% of the reviewed studies.

4.2 FL-Based Security and Privacy Frameworks

FL is widely used in healthcare and IoT systems. It allows models to be trained without data centralization. FL and privacy-preserving methods enhance data protection in cloud-edge systems. For instance, prior work in [8] showed secure FL

utilization in medical imaging. Similarly, [9] discussed local differential privacy techniques for IoT networks. Robustness and resilience in FL are explored in [10]. To address compliance challenges, the authors of [11] proposed a GDPR-compliant zero-trust FL framework. Additionally, the authors of [17] reviewed PETs in federated medical research that links to GDPR standards. These studies identify the critical role of AI-based distributed systems.

4.3 NLP and Semantic-Based Compliance Automation

The study in [15] explored NLP techniques for automating legal-text and contract-compliance analysis. Other studies, such as [14], have used NLP to assess privacy policies for GDPR compliance. These systems enhance cloud service compliance by identifying data roles and regulations. However, the lack of multi-language support remains a challenge for these systems. This limitation restricts the application of these approaches in non-English systems.

4.4 Knowledge Graphs and Rule-Based Compliance

Knowledge graphs and rule-based systems provide a clear organization of compliance rules for automating compliance verification [1, 2]. The authors of [12] proposed a semantic model to automate GDPR compliance verification. Moreover, the study in [13] proposed using KG with hybrid rule-based and ML models to improve compliance accuracy. Other studies, such as [16], explore static compliance checking in distributed systems. The aim of these techniques is to reduce manual compliance-checking effort. However, there are challenges to scalability and generalization across different domains.

4.5 Emerging Challenges: EU AI Act and National Frameworks

Recent studies have explored the readiness for the EU AI Act. For instance, the authors in [1] addressed compliance risks, while the authors of [2] discussed risk-based regulations. Additionally, the study in [18] mapped GDPR compliance to standard security controls such as NIST SP-800-53. However, despite this advancement, current research shows a gap in national frameworks. The study in [28] highlights the governance challenges of Saudi NCA ECC for SMEs. This limitation reduces the applicability of these approaches to non-EU regulations. It also highlights the need to align national regulations with AI-driven compliance frameworks.Table 5 Summary of Selected Related Works Table 5 summarizes the key characteristics, evaluation metrics, and limitations of the reviewed studies.

Table 5 Summary of Selected Related Works

Ref	Year	Domain	AI Technique	Regulation	Eval. Metrics	Validation	Limitation/ Research Gap
[4]	**2021**	General / IoT	FL	GDPR	N/A	Survey	FL is not evaluated in real operational environments.
[8]	**2020**	Healthcare	FL	GDPR, HIPAA	N/A	Review	Focused only in medical imaging, limited applicability across scenarios.
[9]	**2020**	IoT	FL + Differential Privacy	Privacy	Accuracy, Convergence	Simulation	Noise injection reduces the accuracy of FL models.
[10]	**2021**	General	FL	Security	N/A	Survey	No specific benchmark to compare defense approaches.
[11]	**2025**	Cloud-Edge	FL + Zero Trust	GDPR	N/A	Formal	No real-world testing on regulated environments.
[12]	**2022**	General	Semantic Modeling	GDPR	Completeness	Proof of Concept	Only discusses specific GDPR consent rules.
[13]	**2021**	Legal	Hybrid (Rule+ML)	GDPR	Precision, Recall	Experiment	Existing rules still need manual updates.
[14]	**2021**	Web Policies	NLP / Semantic	GDPR	Accuracy	Experiment	Complex policy language; lacks multi-lingual support
[15]	**2023**	Contracts	NLP Analysis	GDPR	Precision, Recall	Experiment	Runtime compliance cannot be detected during static analysis.

[16]	**2021**	Dist. Systems	Static Analysis	GDPR	N/A	Formal	Cannot detect runtime violations during static analysis.
[1]	**2025**	Insurance	Algorithmic Bias	EU AI Act	Fairness	Simulation	Focused mostly on insurance applications.
[2]	**2024**	General	AI Risk Assessment	EU AI Act	N/A	Theoretical	No technical solutions, only theoretical analysis.
[17]	**2023**	Medical	FL + PETs	GDPR	N/A (Review)	Scoping Review	Not implemented in real clinical environments.
[18]	**2024**	Cloud Sec.	Auto-Mapping	GDPR, NIST	N/A	Case Study	Automation for verification is not included.
[19]	**2022**	General	FL	Privacy	N/A	Survey	No links of determined challenges to regulatory obligations.
[20]	**2024**	Cloud Comp.	Unified Framework	GDPR	N/A	Framework	Lacks performance and scalability evaluation

5. Integration of AI and Compliance Frameworks

5.1 Technical Effectiveness of AI Approaches

The reviewed studies explore several AI techniques for evaluating security and compliance in cloud and edge environments. For instance, privacy policies and agreements are analyzed using NLP techniques [4, 11]. Semantic modeling and knowledge graph-based approaches enable the automation of GDPR requirements assessments [12]. Furthermore, FL and differential privacy methods improve security, ensuring sensitive data remains distributed across edge systems [8, 29]. Such approaches show strong potential for scalability and privacy preservation. However, these approaches lack standardized regulatory evaluation measures, with evaluation varying across accuracy and qualitative analysis [17].

5.2. Compliance Integration Across Frameworks

Most studies highlight GDPR as the main regulatory standard [13, 14, 16]. Additionally, other studies also address HIPAA in the context of healthcare [17, 29, 30]. Some studies utilized the AI Act in a broader governance context. For instance, the study in [18] linked GDPR controls to NIST SP-800-53. The study helps bridge the gap between technical security and regulatory standards. Other papers, such as [1, 2], highlight the conceptual risks and limitations of the EU AI Act. This paper highlights the need for measurable compliance indicators. Despite these advantages, application remains fragmented.

There is minimal cross-regulatory alignment in AI-based frameworks. Across the 30 studies reviewed, FL represents around 40% of the applied AI techniques. While NLP, semantic, and knowledge approaches represent 30%. GDPR appears in approximately 80% of the reviewed studies. HIPAA appears in approximately 10-13% of the studies, mainly in healthcare-based FL systems. The EU AI Act appears in approximately 10% of the reviewed studies. For multi-cloud and cross-border, none of the reviewed studies implement non-EU laws such as Saudi NCA or PDPL. This study [28] highlights governance and policy challenges related to Saudi NCA Essential Cybersecurity Controls (ECC) for SMEs. This highlights the importance of aligning AI-driven compliance frameworks with national regulation. Table 6 maps AI techniques to the regulatory compliance frameworks identified in the literature.

Table 6 Mapping of AI Techniques to Regulatory Compliance Frameworks based on Literature Review

AI Techniques	GDPR	HIPAA	EU AI Act	Saudi NCA
Federated Learning (FL)	✓	✓	✓	×
Natural Language Processing (NLP)	✓	×	×	×
Knowledge Graphs	✓	×	×	×

5.3. Strengths and Weaknesses between Studies

The compliance automation strength lies in reducing manual auditing. This is particularly achieved through semantic and NLP-driven approaches [12, 15]. FL privacy-preserving methods offer strong potential for distributed systems. However, these methods often struggle to balance accuracy with privacy budgets. Studies that focus on governance contribute valuable conceptual frameworks. However, they often lack practical validation. The key weakness among all categories is the absence of evaluation metrics for unified compliance. This limits cross-comparison of technical and regulatory performance [7, 31].

5.4. Emerging Technology Challenges

Several factors limit the integration of AI with compliance frameworks. The diverse regulatory context (GDPR, HIPAA, AI Act) lacks standardized customization [1, 5]. Scalability issues also remain in real-time cloud-edge deployments [8, 30]. Compliance-checking systems have insufficient explanation [15]. To address these challenges, it is important to have benchmarking datasets. Cross-regulation taxonomies and explainable AI tools are essential for effective compliance monitoring.

6. Results

The analysis of the related studies reveals three research trends, as illustrated in Figure 3. The first trend is the increasing use of AI-driven automation for regulatory compliance, particularly through hybrid rule-based models, NLP, and semantic reasoning [12, 13, 15, 16]. In addition, the focus on privacy-preserving and FL has been explored in distributed cloud-edge environments [4, 8, 11, 17]. Recent research highlights the importance of governance and policy alignment with emerging frameworks. This area includes frameworks such as the EU AI Act and updated GDPR interpretations [2, 18].

The most studied domains are healthcare and IoT [29, 30]. Multi-cloud deployments have also received increasing attention [10]. The findings indicate a gradual shift from isolated technical compliance checks toward governance-aware AI systems that integrate security assessments with legal accountability. Out of the 30 reviewed studies, as shown in Figure 4, GDPR was referenced in 80% of the studies, while HIPAA and the EU AI Act were referenced in 10-13% of the studies. As shown in Figure 5, approximately 40% used FL and 30% relied on NLP and semantic models, while the remaining studies applied hybrid knowledge-based or privacy-preserving methods.

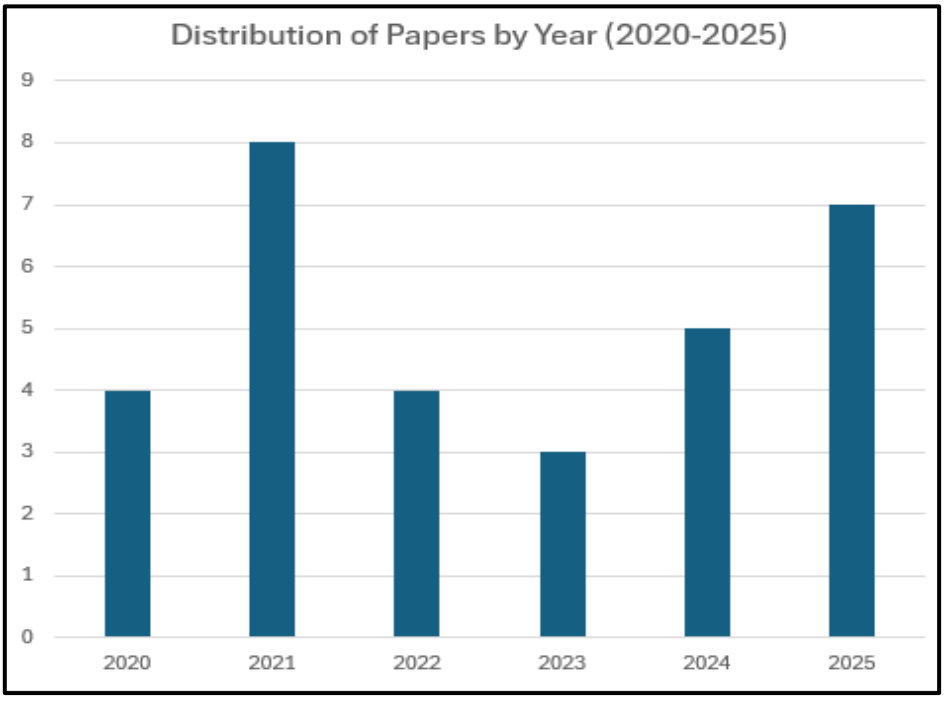


Figure 3 Distribution of Papers by Year 2020-2025.

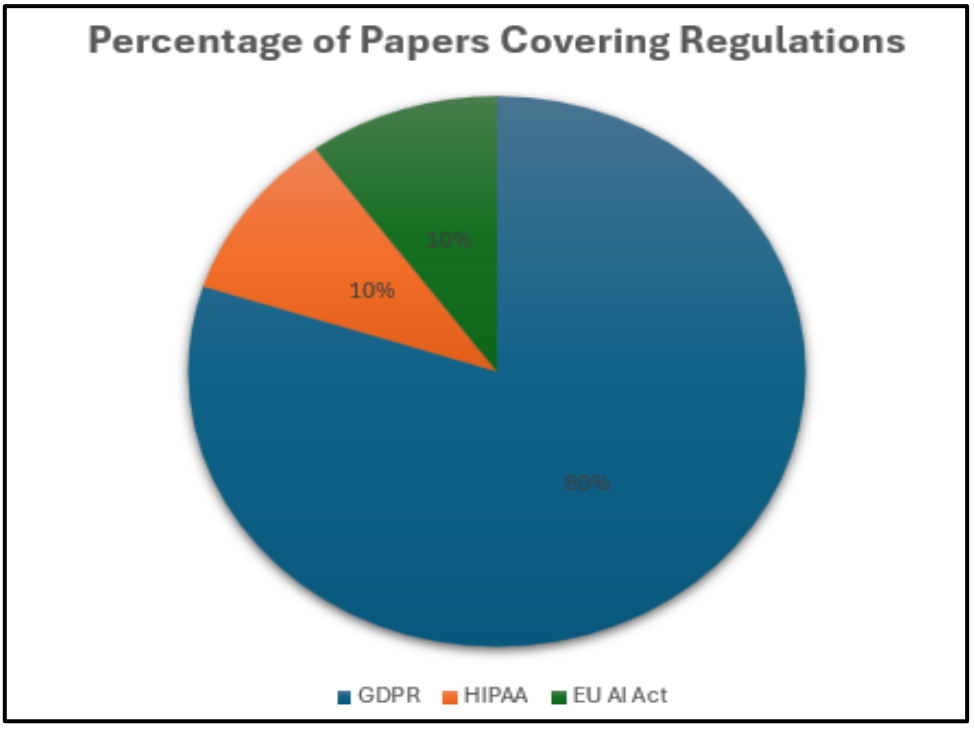


Figure 4 Percentage of Papers Covering Regulations.

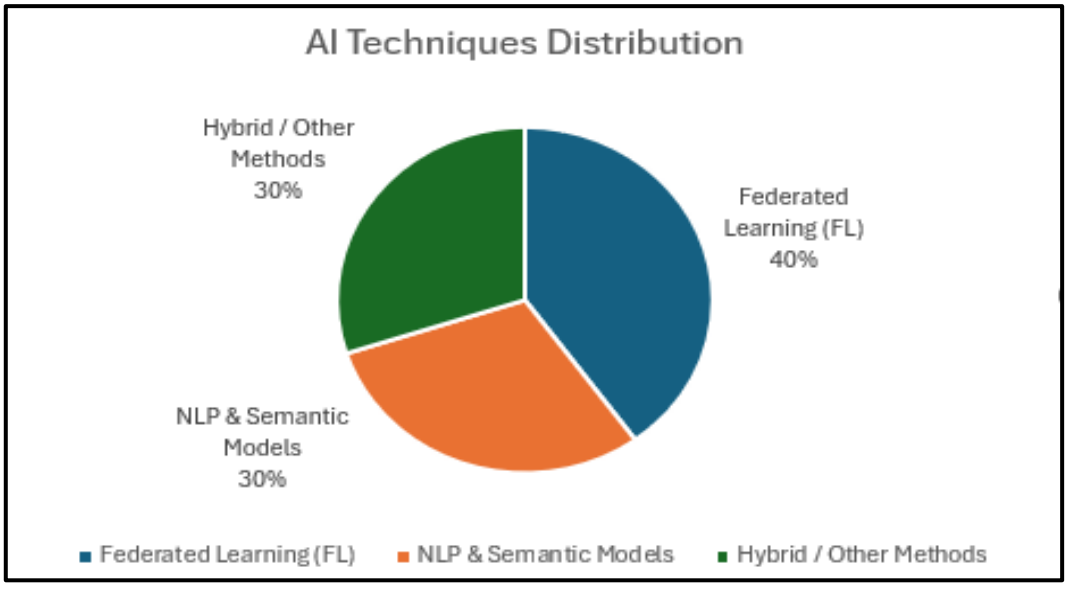


Figure 5 AI Techniques Distribution

6.1. AI Techniques Used for Security and Compliance Assessment

Security and compliance assessments have been addressed using different AI techniques. For instance, several systems use Natural Language Processing (NLP), to analyze regulatory and contractual documents. Data-processing agreements are essential for improving transparency in cloud service compliance [14, 15]. Federated learning (FL) approaches allow

collaborative model training without sharing original data [11, 17]. Semantic and knowledge graph models are effective for formalizing GDPR clauses. Furthermore, this approach allows automated verification of consent and processing activities [3, 12]. Some works assess the AI behavior by using risk-assessment frameworks and rule-based governance. These assessments are mapped against standards such as the EU AI Act and NIST SP-800-53 [1, 2]. Zero-trust models enforce security by isolating local data, and strictly enforced privacy budgets are met [7, 11]. These patterns indicate a merging of technical AI innovation and formal compliance representation.

6.2. Analysis of Applied Regulatory Frameworks

The distribution of regulations across studies indicates that GDPR is the most used framework in most of the reviewed works [17]. HIPAA is primarily addressed in healthcare-related FL and governance studies. It emphasizes patient data protection in edge-based diagnosis systems [30]. Some papers specifically examine the EU AI Act, highlighting its risk classification design. Furthermore, there are challenges in implementing measurable AI risk indicators on cloud platforms. Papers such as [18] that focus on cross-framework integration remain limited. However, it represents an opportunity to unify compliance frameworks. These findings confirm the regulation-bound nature of an AI-driven compliance system. This limitation restricts the applicability of these systems.

7. Discussion

The results of this review provide an overview of AI deployment in cloud-edge security systems. This information is particularly relevant in the implementation of compliance regulations. Previous studies have largely focused on individual technical approaches, including FL, robustness enhancement, and differential privacy [4, 8–10]. Most of the reviewed studies focus heavily on GDPR (80%), with less focus on HIPAA and the EU AI Act (10%). This demonstrates that current AI-driven compliance systems remain heavily EU-centered. Furthermore, there is frequent use of FL (40%) and NLP-based models (30%), emphasizing the importance of privacy-preserving techniques. These approaches strengthen data protection. However, most of them did not address compliance requirements. Recent studies propose frameworks that combine security assessments with compliance needs. An example of these frameworks is a GDPR-based access control model. These frameworks also incorporate automated contract verification, which is part of their design [12–14, 16]. This study indicates the role of AI in supporting legal and regulatory requirements.

Research on regulatory compliance is evolving rapidly. Earlier studies focused on GDPR automation. Additionally, the research also focused on legal text analysis using NLP and knowledge graphs [3, 15, 21]. Recent studies have expanded to include broader governance concerns. This includes AI Act risk categories and algorithmic bias [1, 2, 19]. These studies indicate the rising awareness of compliance. These studies increasingly frame compliance as a technical, ethical, and organizational requirement. However, it still lacks a standardized evaluation framework. This lack of a standardized evaluation framework makes it difficult to measure the effectiveness of compliance-based AI systems. Although AI is improving security assessments, system resilience remains a challenge. Outage scenarios such as Cloudflare illustrate how failures can delay compliance verification and security assessments processes [23, 24]. Most reviewed studies have not tested their models on such incidents.

This indicates an important gap in the behavior of AI during real-world scenarios. Several limitations among reviewed studies have been defined. For instance, many models were simulated in controlled environments. Moreover, none of the reviewed models has been validated in a large-scale operational environment. These models lack legal analysis, which reduces transparency and limits the trustworthiness of AI-driven assessments. Cross-border compliance adds another challenge. This requirement indicates different operations and procedures. However, most studies are using only GDPR frameworks. Moreover, few studies investigate compliance with frequent changes in cloud-edge systems.

Overall, the findings indicate clear gaps in current research. Existing studies investigate individual elements including security models and privacy techniques. However, the existing studies lack unified AI-based assessments and distributed edge architectures. Future work should be on the integration of technical and regulatory requirements for real-world systems.

7.1. Comparison with Related Studies

This study investigates the role of AI in improving security and regulatory compliance in cloud-edge environments. Existing works mainly discuss technical and legal aspects. This review considers both technical security and legal requirements, highlighting AI models such as privacy-preserving methods. Additionally, it explores emerging technologies that can address existing gaps. This paper outlines the benefits and limitations of existing studies. It also discusses the AI roles in enhancing the overall security and regulatory posture of cloud-edge systems. Few papers demonstrate partial alignment with this review's goals. For instance, the study in [12] connects AI methods with regulatory compliance. However, it is only limited to the GDPR framework. It also does not extend to the cloud-edge environment. The study in [17] discusses privacy-enhancing technologies and the GDPR requirements. The paper offers a useful legal and technical approach. However, it does not address broader multi-regulations. The study in [20] provides a structured GDPR framework for cloud systems. However, their work only focused on cloud settings. Such an approach limits the exploration of wider regulatory frameworks. Table 7 summarizes the alignment of the three selected studies with the main criteria of this review.

Table 7 Comparison of Research Focus Areas Among Related Works

Criterion	[12]	[17]	[20]
Scope	GDPR consent verification using semantic modeling	Privacy-enhancing technologies (PETs) in federated medical research	Unified GDPR compliance framework for cloud computing
AI Technique	Semantic modeling and knowledge graphs	Federated Learning with PETs	Structured framework with GDPR mapping
Regulation Coverage	GDPR only	GDPR and HIPAA	GDPR only
Cloud-Edge Relevance	Limited, no cloud or edge deployment	Partial, applicable to distributed medical environments	Moderate, focused on cloud settings only
Validation Method	Proof of concept	Scoping review	Framework design
Key Limitation	Covers only specific GDPR consent rules, does not extend to broader regulatory frameworks	Does not address multi-regulation environments beyond GDPR and HIPAA	Focused solely on cloud, does not extend to edge or hybrid environments
Alignment with This Review	Partial, addresses AI-compliance integration but limited to GDPR and excludes cloud-edge context	Partial, provides useful legal-technical perspectives but lacks multi-regulatory scope	Partial, structured compliance approaches but restricted to cloud single regulation

7.2. Limitations of This Review

This review reveals several limitations in this field. This review analyzed only published English-language studies. This may have excluded relevant industry reports and region-specific research. Another limitation is database coverage, where relevant publications may have been missing. Because this paper specifically focused on AI-based solutions, traditional compliance methods were excluded. Finally, the rapid evolution of regulatory frameworks may limit the ability of this review to reflect the most recent developments.

8. Recommendations and Future Directions

This review shows that AI can support security assessment and regulatory compliance in cloud-edge systems. However, several areas need to be investigated. Future work should focus on developing an integrated framework that combines privacy, security, and regulatory requirements. Additionally, a comprehensive security evaluation should be included within a single model. Existing studies explore them individually. This results in a limitation of real-world utilization.

Another main aspect is the need for transparency and interpretability. A clear explanation of AI decisions is required for regulatory compliance. The results produced by existing models are often difficult to explain. This study indicates the need to design AI systems that support explanation methods. Organizations would meet accountability for global compliance regulations.

Many reviewed approaches were tested in controlled environments. This limitation affects the large-scale implementation results of distributed-edge environments. These models do not account for the complexity of distributed-edge environments. This limitation necessitates that future work focuses on AI behavior in these complex environments. AI-driven threat intelligence is another promising direction. It supports compliance monitoring. Existing studies explored AI roles in healthcare remote monitoring [33]. The system identifies abnormal behaviors and real-time security risks. Using these techniques would help organizations detect compliance violations and security risks in real time.

Future research should focus on the role of AI-based cloud-edge systems during outage scenarios. Studies and incident reports discuss the failures of control functions. Future studies must explore practical solutions. Examples of practical solutions include cloud redundancy and offline compliance tracking. This will ensure that critical functions are available during major failures.

Finally, multi-regulation compatibility should be explored. Organizations must comply with an increasing number of regulations. Most reviewed papers focused on individual frameworks. While other regions require different regulations. The future work should explore the adaptation of AI systems and examine regulatory changes and supporting jurisdiction compliance.

9. Conclusion

This paper investigated the existing integration of AI-based security assessments and regulatory compliance in cloud-edge systems. The review followed the PRISMA 2020 guidelines to identify, screen, and analyze 30 studies published between 2020 to 2025. The findings show that FL is used in 40%, while NLP is used in 30%. Knowledge graphs are increasingly applied for compliance automation. GDPR was the focus of approximately 80% of the reviewed studies, while the EU AI Act has received limited attention.

National frameworks such as Saudi Arabia's NCA ECC/CCC and PDPL are rarely addressed. These findings demonstrate the absence of a unified framework that integrates both security assessment and regulatory compliance requirements. Future work should focus on developing AI-driven solutions that jointly address legal and technical requirements. These solutions must support national regulations to enable cross-border deployment.

Acknowledgements
Not applicable.

Funding
This research will be supported by the Deanship of Scientific Research, King Faisal University.

Contributions
Conceptualization, R.A. and A.A.; methodology, R.A.; validation, R.A. and A.A.; formal analysis, R.A.; investigation, R.A.; resources, R.A.; data curation, R.A.; writing-original draft preparation, R.A.; writing-review and editing, A.A.; supervision, A.A. All authors have read and agreed to the published version of the manuscript.

Ethics declarations
This article does not contain any studies involving human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests.

The use of generative AI

Generative AI tool was used only to improve the language and readability of this manuscript. The authors reviewed the content and take full responsibility for the final manuscript.

References

[1] Mahajan, S., Agarwal, R., & Gupta, M. (2025). Algorithmic bias under the EU AI Act: Compliance risk, capital strain, and pricing distortions in life and health insurance underwriting. Risks, 13, Article 160. https://doi.org/10.3390/risks13090160

[2] Kusche, I. (2024). Possible harms of artificial intelligence and the EU AI act: Fundamental rights and risk. Journal of Risk Research, 1-14. https://doi.org/10.1080/13669877.2024.2350720

[3] Tauqeer, A., Kurteva, A., Chhetri, T. R., Ahmeti, A., & Fensel, A. (2022). Automated GDPR contract compliance verification using knowledge graphs. Information, 13, Article 447. https://doi.org/10.3390/info13100447

[4] Truong, N., Sun, K., Wang, S., Guitton, F., & Guo, Y. (2021). Privacy preservation in federated learning: An insightful survey from the GDPR perspective. Computers & Security, 110, Article 102402. https://doi.org/10.1016/j.cose.2021.102402

[5] Kalodanis, K., Feretzakis, G., Anastasiou, A., Rizomiliotis, P., Anagnostopoulos, D., & Koumpouros, Y. (2025). A privacy-preserving and attack-aware AI approach for high-risk healthcare systems under the EU AI Act. Electronics, 14, Article 1385. https://doi.org/10.3390/electronics14071385

[6] Jørgensen, B. N., & Ma, Z. G. (2025). Impact of EU regulations on AI adoption in smart city solutions: A review of regulatory barriers, technological challenges, and societal benefits. Information, 16, Article 568. https://doi.org/10.3390/info16070568

[7] Feretzakis, G., Vagena, E., Kalodanis, K., Peristera, P., Kalles, D., & Anastasiou, A. (2025). GDPR and large language models: Technical and legal obstacles. Future Internet, 17, Article 151. https://doi.org/10.3390/fi17040151

[8] Kaissis, G. A., Makowski, M. R., Rückert, D., & Braren, R. F. (2020). Secure, privacy-preserving and federated machine learning in medical imaging. Nature Machine Intelligence, 2, 305-311. https://doi.org/10.1038/s42256-020-0186-1

[9] Zhao, Y., Zhao, J., Yang, M., Wang, T., Wang, N., Lyu, L., Niyato, D., & Lam, K. Y. (2020). Local differential privacy-based federated learning for internet of things. IEEE Internet of Things Journal, 8, 8836-8853. https://doi.org/10.1109/jiot.2020.3037194

[10] Blanco-Justicia, A., Domingo-Ferrer, J., Martínez, S., Sánchez, D., Flanagan, A., & Tan, K. E. (2021). Achieving security and privacy in federated learning systems: Survey, research challenges and future directions. Engineering Applications of Artificial Intelligence, 106, Article 104468. https://doi.org/10.1016/j.engappai.2021.104468

[11] Abbas, Z., Ahmad, S. F., Anjum, A., Syed, M. H., Malik, S. U. R., & Rehman, S. (2025). Ensuring zero-trust in GDPR-compliant deep federated learning architecture. Computers, 14, Article 317. https://doi.org/10.3390/computers14080317

[12] Chhetri, T. R., Kurteva, A., DeLong, R. J., Hilscher, R., Korte, K., & Fensel, A. (2022). Data protection by design tool for automated GDPR compliance verification based on semantically modeled informed consent. Sensors, 22, Article 2763. https://doi.org/10.3390/s22072763

[13] Hamdani, R. E., Mustapha, M., Amariles, D. R., Troussel, A., Meeùs, S., & Krasnashchok, K. (2021). A combined rule-based and machine learning approach for automated GDPR compliance checking. ACM, 40-49. https://doi.org/10.1145/3462757.3466081

[14] Sánchez, D., Viejo, A., & Batet, M. (2021). Automatic assessment of privacy policies under the GDPR. Applied Sciences, 11, Article 1762. https://doi.org/10.3390/app11041762

[15] Cejas, O. A., Azeem, M. I., Abualhaija, S., & Briand, L. C. (2023). NLP-based automated compliance checking of data processing agreements against GDPR. IEEE Transactions on Software Engineering, 49, 4282-4303. https://doi.org/10.1109/tse.2023.3288901

[16] Tokas, S., Owe, O., & Ramezanifarkhani, T. (2021). Static checking of GDPR-related privacy compliance for object-oriented distributed systems. Journal of Logical and Algebraic Methods in Programming, 125, Article 100733. https://doi.org/10.1016/j.jlamp.2021.100733

[17] Brauneck, A., Schmalhorst, L., Majdabadi, M. M. K., Bakhtiari, M., Völker, U., Baumbach, J., Baumbach, L., & Buchholtz, G. (2023). Federated machine learning, privacy-enhancing technologies, and data protection laws in medical research: Scoping review. Journal of Medical Internet Research, 25, Article e41588. https://doi.org/10.2196/41588

[18] Granata, D., Mastroianni, M., Rak, M., Cantiello, P., & Salzillo, G. (2024). GDPR compliance through standard security controls: An automated approach. Journal of High Speed Networks, 30, 147-174. https://doi.org/10.3233/jhs-230080

[19] Lyu, L., Yu, H., Ma, X., Chen, C., Sun, L., Zhao, J., Yang, Q., & Yu, P. S. (2022). Privacy and robustness in federated learning: Attacks and defenses. IEEE Transactions on Neural Networks and Learning Systems, 35, 8726-8746. https://doi.org/10.1109/tnnls.2022.3216981

[20] Pattakou, A., Diamantopoulou, V., Kalloniatis, C., & Gritzalis, S. (2024). A unified framework for GDPR compliance in cloud computing. ACM, 1-9. https://doi.org/10.1145/3664476.3670918

[21] Karunaratne, T. (2021). For learning analytics to be sustainable under GDPR—Consequences and way forward. Sustainability, 13, Article 11524. https://doi.org/10.3390/su132011524

[22] Lee, G. H., & Shin, S. Y. (2020). Federated learning on clinical benchmark data: Performance assessment. Journal of Medical Internet Research, 22, Article e20891. https://doi.org/10.2196/20891

[23] Luo, L., Meng, S., Qiu, X., & Dai, Y. (2019). Improving failure tolerance in large-scale cloud computing systems. IEEE Transactions on Reliability, 68, 620-632. https://doi.org/10.1109/TR.2019.2901194

[24] Strickx, T., & Hartman, J. (2022). Cloudflare outage on June 21, 2022. In *The Cloudflare Blog*. https://blog.cloudflare.com/cloudflare-outage-on-june-21-2022/

[25] Campos, E. M., Saura, P. F., González-Vidal, A., Hernández-Ramos, J. L., Bernabé, J. B., Baldini, G., & Skarmeta, A. (2021). Evaluating federated learning for intrusion detection in internet of things: Review and challenges. Computer Networks, 203, Article 108661. https://doi.org/10.1016/j.comnet.2021.108661

[26] Korányi, R., Mancera, J. A., & Kaufmann, M. (2022). GDPR-compliant social network link prediction in a graph DBMS: The case of know-how development at Beekeeper. Knowledge, 2, 286-309. https://doi.org/10.3390/knowledge2020017

[27] Feretzakis, G., Papaspyridis, K., Gkoulalas-Divanis, A., & Verykios, V. S. (2024). Privacy-preserving techniques in generative AI and large language models: A narrative review. Information, 15, Article 697. https://doi.org/10.3390/info15110697

[28] Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., & Hewage, C. (2023). Enhancing cyber security governance and policy for SMEs in industry 5.0: A comparative study between Saudi Arabia and the United Kingdom. Digital, 3, 200-231. https://doi.org/10.3390/digital3030014

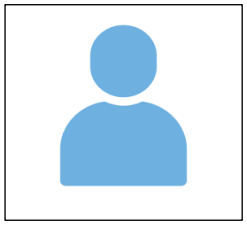
[29] Lepri, B., Oliver, N., & Pentland, A. (2021). Ethical machines: The human-centric use of artificial intelligence. iScience, 24, Article 102249. https://doi.org/10.1016/j.isci.2021.102249

[30] Choudhury, A., Volmer, L., Martin, F., Fijten, R., Wee, L., Dekker, A., & Van Soest, J. (2024). Advancing privacy-preserving health care analytics and implementation of the Personal Health Train: Federated deep learning study. JMIR AI, 4, Article e60847. https://doi.org/10.2196/60847

[31] Khan, L. U., Pandey, S. R., Tran, N. H., Saad, W., Han, Z., Nguyen, M. N. H., & Hong, C. S. (2020). Federated learning for edge networks: Resource optimization and incentive mechanism. IEEE Communications Magazine, 58, 88-93. https://doi.org/10.1109/MCOM.001.1900649

[32] J. Trivedi, M. Tahir and J. Isoaho, "AI-Enhanced Threat Intelligence in Remote Patient Monitoring Systems: A Survey on Recent Advances, Challenges and Future Research Directions," in IEEE Access, vol. 13, pp. 106465-106488, 2025, doi: 10.1109/ACCESS.2025.3572626.

Biographies



RASHA ALMARSHOOD. received the B.Sc. degree from Qassim Private Colleges, now Mustaqbal University, Saudi Arabia, in 2014. She is currently pursuing a master's degree in cybersecurity at King Faisal University. Her current research interests in cybersecurity and IoT. *224108485@student.kfu.edu.sa*

ABDULLAH ALBUALI. (Member, IEEE) received the B.S. degree in computer science from King Faisal University, Saudi Arabia, in 2009, and the M.S. and Ph.D. degrees in computer science, with specialization in security and networking, from Southern Illinois University, USA, in 2014 and 2021, respectively. He is currently an Assistant Professor with the College of Computer Science and Information Technology, King Faisal University. His research interests include zero trust architecture, AI-enabled cybersecurity, cloud and edge computing security, Internet of Things (IoT) systems, drone and autonomous networks, digital forensics, volunteer and distributed computing, and blockchain-based security. **aabuali@kfu.edu.sa**