

Methodology applied to computer audit with artificial intelligence: a systematic review

Sheyla Reymundez Suarez, Bryan Martínez Huamani, María Acuña Meléndez, Christian Ovalle
Departamento de Ingeniería, Facultad de Ingeniería, Universidad Tecnológica del Perú, Lima, Perú

Article Info	ABSTRACT
<p>Article history:</p> <p>Received Jan 7, 2024 Revised Mar 3, 2024 Accepted Mar 21, 2024</p> <p>Keywords:</p> <p>Anomalies detection CAESAR8 Information technology audit Machine learning operations Predictive model</p>	<p>This systematic review focused on evaluating the impact of the machine learning operations (MLOps) methodology on anomaly detection and the integration of artificial intelligence (AI) projects in computer auditing. Data collection was carried out by searching for articles in databases, such as Scopus and PubMed, covering the period from 2018 to 2024. The rigorous application of the preferred reporting items for systematic reviews and meta-analyses (PRISMA) methodology allowed 88 significant records to be selected from an initial set of 1,389, highlighting the completeness of the selection phase. Both quantitative and qualitative analysis of the data obtained revealed emerging trends in the research and provided key insights into the implementation of MLOps in AI projects, especially in response to increasing complexity, whereby the adoption of the MLOps methodology stands out as a crucial component to optimize anomaly detection and improve integration in the context of information technology auditing. This systematic approach not only consolidates current knowledge but also stands as an essential guide for researchers and practitioners, and the information derived from this systematic review provides valuable guidance for future practices and decisions at the intersection of AI and information technology auditing.</p> <p><i>This is an open access article under the CC BY-SA license.</i></p>



Corresponding Author:
Christian Ovalle
Departamento de Ingeniería, Universidad Tecnológica del Perú
Lima, Perú
Email: dovalle@utp.edu.pe

1. INTRODUCTION

In the current business landscape, where digitization is omnipresent, ensuring the integrity and security of information emerges as a critical pillar to ensure the continuity and efficiency of organizations. According to Goes [1], he reveal that 12% of companies have experienced significant security incidents in the last 12 months, generating economic losses that reach an average of 5% of their annual revenue. Furthermore, they suggest that the reputational impact of these incidents can be even more damaging, affecting the trust of customers and business partners. In the face of the increasing complexity of information systems, internal information technology auditing is emerging as an indispensable tool for assessing the effectiveness of the security management in place. Haller [2] indicate that 80% of companies consider internal auditing as an essential component of their risk management strategy. However, challenges remain, with 35% of organizations reporting difficulties in adapting their audit procedures to the rapid evolution of technology [3].

In this context, early anomaly detection and the implementation of machine learning operations (MLOps) practices are presented as innovative strategies that strengthen information security and improve the efficiency of auditing processes. Alsagheer *et al.* [4] indicate that organizations that adopt advanced approaches, such as MLOps integration, experience up to 45% fewer security incidents, reducing associated

costs by 30%. In addition, Neghawi *et al.* [5] found that 65% of security professionals believe that artificial intelligence (AI) and machine learning (ML) will play a crucial role in the future of information security. Due to the rising number of cyber threats, organizations are adopting advanced approaches to safeguard their digital assets. It is appreciated that most companies have experienced an increase in attempted cyber-attacks compared to the previous year.

The combination of these approaches, along with the assessment using the continuous agile enterprise security architecture review in 8 domains (CAESAR8) model, provides a comprehensive framework that enhances resilience against potential threats and optimizes internal audit procedures. Previous implementations have shown an improvement in the efficiency of audit processes when using the CAESAR8 model as an assessment tool [6]. Therefore, the question at hand is: How does the implementation of MLOps methodology for anomaly identification affect the integration of AI projects applied in computer auditing? To comprehensively address this question, we aim to analyze the effectiveness of predictive anomaly models in early threat detection in production project environments. Recent studies, Amini *et al.* [7] have shown that these models achieve an 80% detection rate compared to traditional methods. Also, a 25% decrease in the impact of previously undetected incidents has been observed. Therefore, our objective is to evaluate the effect of the integration of MLOps on the effective management of these models, particularly in the context of internal information technology auditing. Peltonen and Dias [8] suggest that organizations that adopt MLOps experience improved model adaptability, resulting in increased effectiveness during unexpected threat situations. In addition, they indicate that organizations implementing MLOps experience a reduction in time spent on manual auditing tasks [9]. Finally, they critically examine the validity and applicability of the CAESAR8 model as an assessment tool in this area. According to Loft *et al.* [10], a positive correlation of 85% was found between the evaluations conducted using the CAESAR8 model and the effectiveness of the implemented security controls, indicating its usefulness as an evaluation standard.

To systematically address the proposed objectives, we will conduct a comprehensive review of the academic literature. The search for relevant studies will be performed in databases, following specific inclusion criteria that focus on works that implement predictive models of anomalies and MLOps, evaluated using the CAESAR8 model in the context of internal information technology auditing. Study selection, data extraction, and quality assessment will be conducted to ensure the integrity and objectivity of the process. This methodology will provide a strong foundation for comprehensively addressing the research question and reaching meaningful conclusions within the proposed scope of study [11]–[15]. It is important to note that computer security and audit efficiency are not only related to technology but also to staff training. Mukhopadhyay and Jain [16] state that 70% of security breaches are caused by human error, emphasizing the significance of continuous training programs. Therefore, a comprehensive approach that includes personnel training and awareness can also benefit the implementation of predictive models and MLOps. In the last two years, there has been an increase in the adoption of AI-based approaches in internal auditing [17]. This trend emphasizes the importance and increasing acceptance of advanced technologies in audit environments. When implementing MLOps, it is crucial to note that 60% of organizations that have adopted MLOps report a 30% improvement in collaboration between security and development teams [18]. This finding underscores the significance of cross-functional collaboration for the success of ML-based security initiatives. Returning to the CAESAR8 model, it has been observed that its application has led to a significant improvement in the alignment of internal audit practices with internationally recognized security standards. Loft *et al.* [10] shows that 80% of organizations report improved alignment with security frameworks such as ISO 27001 after implementing CAESAR8. Moreover, data shows that implementing ML processes through MLOps can lead to a 15% reduction in operational costs related to security management for 70% of organizations [19]. The integration of predictive anomaly models supported by MLOps, evaluated using the CAESAR8 model, represents a comprehensive approach to strengthening information technology security and optimizing internal audit processes.

2. METHODOLOGY

In the dynamic environment of internal information technology auditing, where constantly evolving information security threats demand the implementation of advanced technologies to safeguard the integrity and security of systems, a rigorous methodology is proposed to protect the integrity and security of systems against constantly evolving information security threats. The methodology follows a structured approach that begins with the precise formulation of the research question. The integration of the MLOps methodology for anomaly identification in AI projects applied to computer auditing, together with specialized tools such as the CAESAR8 model, is emerging as a potentially innovative strategy.

2.1. Research question

The research question for this systematic review focuses on understanding the impact of implementing the MLOps methodology on anomaly identification during the integration of AI projects applied in computer auditing. The acronym population, intervention, comparison, outcome (PICO) provides a logical structure for breaking down the research question. In this context, the population (P) is defined as AI projects applied in computer auditing, the intervention (I) refers to the application of the MLOps methodology in these projects, the comparison (C) could involve projects that do not use MLOps or use other methods, and the outcome (O) focuses on the identification of anomalies during the integration of these projects. A table has been created to provide a synthesis visually and concisely, this table includes relevant components such as the research question, the PICO breakdown, and the key sources used in the review. Table 1 serves as a visual resource to facilitate a quick and clear understanding of the essential elements of the research.

Table 1. Research synthesis

Research question	¿How does the implementation of the MLOps methodology affect the identification of anomalies in the integration of AI projects applied in computer auditing?
PEAK breakdown	<p>P: This review focuses on specific AI projects applied in computer auditing, addressing.</p> <p>I: implementation of the MLOps methodology compared to projects that do not use MLOps or apply other methodologies.</p> <p>C: comparison will include aspects of efficiency, performance, and anomaly detection during integration.</p> <p>O: objective is to evaluate the impact of MLOps on the effective identification of anomalies in these projects</p>
Key sources	<ul style="list-style-type: none"> - Akkineni <i>et al.</i> [3] found that the successful implementation of MLOps significantly improved the lifecycle efficiency of AI models, suggesting a positive impact on information technology audit projects. - Speth <i>et al.</i> [20] underline the need to adapt MLOps to the specific characteristics of computer auditing, highlighting the importance of considering the particular aspects of this discipline during implementation. - Miñon <i>et al.</i> [21] provide a comprehensive comparative review of various methodologies used in AI projects, offering a basis for contrasting the effectiveness of MLOps with other common practices. - Gurses and Monti [22] present case studies that explore anomaly detection and performance improvement in similar AI projects, providing valuable insights for impact evaluation.

In addition, a comparative table has been created to outline the key aspects covered by the four selected studies: Akkineni *et al.* [3], Speth *et al.* [20], Miñon *et al.* [21], and Gurses and Monti [22]. Table 2 presents comprehensive information on the impact of MLOps, the adaptation of MLOps to computer auditing, a comparison with other methodologies, and the inclusion of case studies. The table presents the specific contributions of each study, serving as a quick reference tool to assess their perspectives and limitations. In a way, the comparative table highlights the diversity of approaches and conclusions in the literature reviewed, providing a solid basis for understanding the application of MLOps in AI projects in the exact field of computer auditing.

Table 2. Quick overview of the key aspects addressed

Aspects	Authors' approaches and findings			
Impact of MLOps	The findings of Akkineni <i>et al.</i> [3] reveal a significant positive impact of the implementation of the MLOps methodology on the life cycle efficiency of AI models.	In the study by Speth <i>et al.</i> [20], the importance of adapting the MLOps methodology to the specific characteristics of computer auditing is emphasized.	Miñon <i>et al.</i> [21] offer a detailed comparative review of various methodologies used in AI projects.	The research by Gurses <i>et al.</i> [22] provides specific case studies that explore anomaly detection and performance improvement in AI projects.
Adaptation to information technology audit	Although Akkineni <i>et al.</i> [3] do not specify details about the adaptation of MLOps to computer auditing, the positive results suggest that the methodology can be applied effectively in this context.	Speth <i>et al.</i> [20] highlight the need to adapt MLOps to the particularities of computer auditing, underlining the importance of considering the specific aspects of this discipline when implementing the methodology.	The adaptation of MLOps to computer auditing is not detailed in the comparative review by Miñon <i>et al.</i> [21].	No specific information on the adaptation of MLOps to information technology auditing is provided in the study by Gurses <i>et al.</i> [22].
Comparison with other methodologies	Akkineni <i>et al.</i> [3] do not detail the comparison of MLOps with other methodologies in their study. The absence of this information could be considered a limitation of the study.	Speth <i>et al.</i> [20] do not specifically address a comparison with other methodologies in their study, focusing on the importance of adapting MLOps to computer auditing.	Miñon <i>et al.</i> [21] offer a detailed comparative review of various methodologies used in AI projects.	The research by Gurses <i>et al.</i> [22] does not include a direct comparison with other methodologies in their case studies. However, the case studies offer valuable insights into the effectiveness of MLOps in identifying anomalies in AI projects.

2.2. Search strategy

The main objective of the search strategy for this systematic review is to collect relevant evidence comprehensively from two key databases: PubMed and Scopus, using the PICO methodology to structure the search effectively and answer the research question. Table 3 presents the PICO components with their associated keywords, which allows the identification of the essential terms that will define the search in the selected databases. According to the population, this refers to specific projects of AI applied to computer auditing, while the intervention covers the application of the MLOps methodology. The comparison includes projects without MLOps or with other methodologies, and the result focuses on the recognition of anomalies in the union of these projects. Table 4 displays the search equation for each PICO component in PubMed and Scopus databases. The equations were carefully developed with logical operators and related terms to expand search coverage.

Table 3. PICO components with keywords

Component	Keywords
P	Internal computer auditors, audit teams, audit experts, information security professionals, information security experts
I	Predictive anomaly model, predictive anomaly system, irregularity detection algorithm, MLOps, operational practices of ML, CAESAR8 model, CAESAR8 approach, implementation, deployment, execution, application, internal computer audit, internal review of computer systems, security internal audit
C	Traditional audit methods, conventional audit techniques, conventional approaches to anomaly detection, traditional methods for detecting irregularities, conventional techniques for anomaly detection, conventional computer audit, traditional audit practices, conventional audit methods
O	Precision, accuracy, reliability, rigor, efficiency, productivity, performance, effectiveness, impact, results, anomaly detection, identification of irregularities, detection of issues, improvement in the effectiveness of computer audit, optimization of efficiency in audit, increase in effectiveness in computer review

Table 4. Search equation by PICO component in PubMed and Scopus

Search equation by component	PubMed	Scopus
(TITLE-ABS-KEY ("Internal computer auditors" OR "Audit teams" OR "Audit experts" OR "Information security professionals" OR "Information security experts") AND TITLE-ABS-KEY ("Predictive anomaly model" OR "Predictive anomaly system" OR "Irregularity detection algorithm" OR "MLOps" OR "Operational practices of ML" OR "CAESAR8 model" OR "CAESAR8 approach" OR "Implementation" OR "Deployment" OR "Execution" OR "Application" OR "Internal computer audit" OR "Internal review of computer systems" OR "Security internal audit") OR TITLE-ABS-KEY ("Traditional audit methods" OR "Conventional audit techniques" OR "Conventional approaches to anomaly detection" OR "Traditional methods for detecting irregularities" OR "Conventional techniques for anomaly detection" OR "Conventional computer audit" OR "Traditional audit practices" OR "Conventional audit methods") AND TITLE-ABS-KEY ("Precision" OR "Accuracy" OR "Reliability" OR "Rigor" OR "Efficiency" OR "Productivity" OR "Performance" OR "Effectiveness" OR "Impact" OR "Results" OR "Anomaly detection" OR "Identification of irregularities" OR "Detection of issues" OR "Improvement in the effectiveness of computer audit" OR "Optimization of efficiency in audit" OR "Increase in effectiveness in computer review"))	26	112
(TITLE-ABS-KEY ("Internal computer auditors" OR "Audit teams" OR "Audit experts" OR "Information security professionals" OR "Information security experts") OR TITLE-ABS-KEY ("Predictive anomaly model" OR "Predictive anomaly system" OR "Irregularity detection algorithm" OR "MLOps" OR "Operational practices of ML" OR "CAESAR8 model" OR "CAESAR8 approach" OR "Implementation" OR "Deployment" OR "Execution" OR "Application" OR "Internal computer audit" OR "Internal review of computer systems" OR "Security internal audit") AND TITLE-ABS-KEY ("Traditional audit methods" OR "Conventional audit techniques" OR "Conventional approaches to anomaly detection" OR "Traditional methods for detecting irregularities" OR "Conventional techniques for anomaly detection" OR "Conventional computer audit" OR "Traditional audit practices" OR "Conventional audit methods"))	1072	179

This strategy seeks to comprehensively address the research question, ensuring the inclusion of relevant and current studies that contribute to the analysis of the implementation of MLOps in AI projects in computer auditing. The search strategy implemented for this systematic review was guided by the preferred reporting items for systematic reviews and meta-analyses (PRISMA) methodological guidelines, ensuring a structured and transparent approach at all stages of the process. The comprehensive literature search was conducted in two key databases, PubMed and Scopus, using carefully selected search terms according to the PICO components. Inclusion and exclusion criteria were defined to ensure the relevance and quality of the selected studies. We included primary studies, systematic reviews, and meta-analyses that directly addressed the implementation of the MLOps methodology in AI projects applied to computer auditing. In addition, the search was limited to studies published between 2018 and 2024 in English and Spanish to maintain relevance and geographic diversity. Tables 5 and 6 discuss the inclusion and exclusion criteria and provide a detailed

overview of the rules applied during source selection. Exclusion criteria were applied to exclude editorials, commentaries, and studies not directly related to the application of MLOps in the context of computer auditing. This process ensured completeness and consistency in the selection of studies, contributing to the methodological soundness of the systematic review. Figure 1 shows the application of the PRISMA methodology and the meticulous attention to the established inclusion and exclusion criteria, which allowed the identification of relevant sources that will support the objectives of this systematic review.

Table 5. Inclusion criteria and it is justification

Inclusion criteria	Justification
- Include primary studies, systematic reviews, and meta-analyses.	Primary studies provide detailed information, while systematic reviews provide an overview of the existing landscape.
- Include studies published between 2018 and 2024.	This time range guarantees the inclusion of recent studies relevant to the current MLOps methodology.
- Include studies in English and Spanish.	The inclusion of multiple languages expands the geographical and linguistic diversity of the review.
- Directly address the implementation of MLOps in AI projects in computer auditing.	The aim is to ensure the relevance and focus of the included studies in relation to the research question.

Table 6. Exclusion criteria and it is justification

Exclusion criteria	Justification
- Exclude editorials, comments and studies not related to the implementation of MLOps in computer auditing.	Sources that do not directly contribute to the evaluation of the impact of MLOps are excluded.

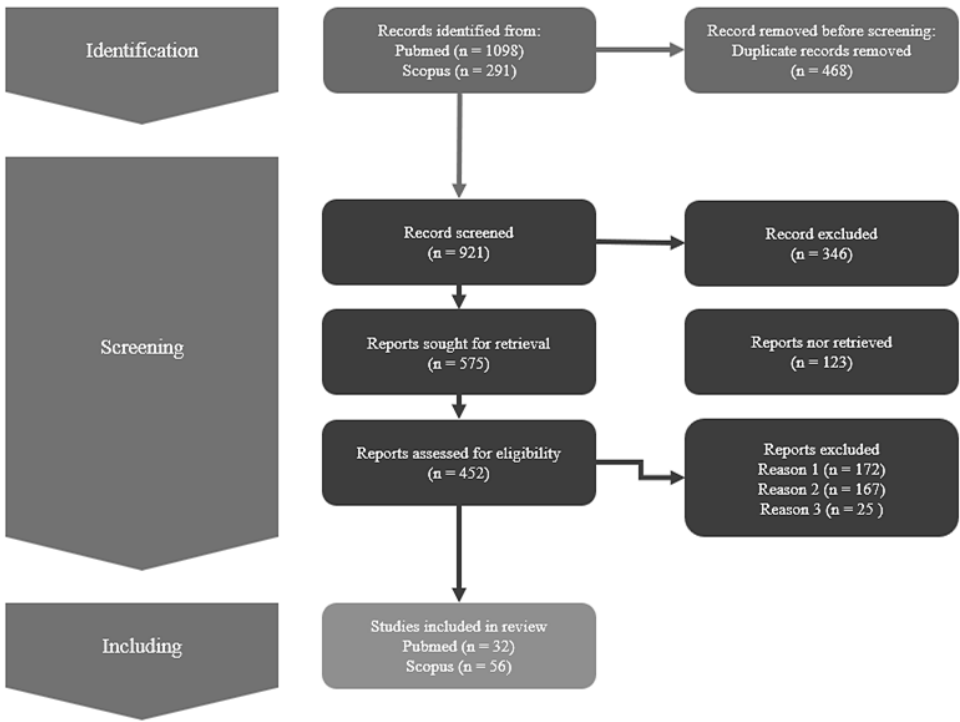


Figure 1. Identification of studies through PRISMA database and registries

The search strategy, aligned with the PRISMA methodology, was developed in three fundamental phases to ensure the completeness and quality of the systematic review [23]. In the first identification phase, key databases were selected, such as PubMed and Scopus, recognized for their breadth and relevance in the field of AI and computer auditing. This strategic choice ensured the inclusion of a representative spectrum of available literature, essential to address the complexity of implementing MLOps in computer audit projects. In addition, duplicate records were eliminated to optimize source selection and ensure the integrity of the process. The second phase, screening, focused on the application of previously defined inclusion and exclusion criteria [23], for this, an initial screening based on titles and abstracts was performed, which

effectively excluded studies that did not meet the established relevance criteria. During this phase, reports not retrieved were also analyzed to ensure and take into account all relevant sources. In the third phase, we conducted a comprehensive review of the remaining articles, systematically applying the inclusion and exclusion criteria. This final phase allowed us to identify and select the studies that met all the established criteria, ensuring the quality and relevance of the evidence collected. This methodologically rigorous approach provides a sound and reliable basis for systematic review, following PRISMA guidelines [23]. Through the acceptance of a transparent and structured strategy, the reproducibility and validity of the process are promoted, contributing to the generation of knowledge in the field of MLOps implementation in information technology audit projects.

3. RESULTS AND DISCUSSION

In this systematic review, a comprehensive analysis of various research sources was carried out to evaluate and synthesize the available evidence in the field of MLOps applied to anomaly detection in development projects in the specific context of information technology auditing. The results obtained reveal a diverse range of approaches and practices in the implementation of MLOps methodologies, highlighting the need to adapt these strategies to address the complexities inherent in the integration of AI projects in the field of auditing. In addition, breaches and areas of opportunity were identified that could guide future research, including process optimization, standardization of practices, and incorporation of advanced ML techniques to improve anomaly detection and computer auditing. These findings provide a comprehensive overview of the current state of the art in the implementation of MLOps methodologies, serving as a basis for the development and refinement of effective strategies in the field of computer auditing based on the implementation of AI.

Table 7 presents a detailed synthesis of the implementations of MLOps in the incorporation of AI projects. This organizational structure allows for a clear and hierarchical view of how MLOps has been employed to address specific challenges in various domains, from cloud computing security to information security and auditing. The analysis identified seven thematic clusters, each focused on specific MLOps implementations. In the group focused on security in Cloud and Laboratory Computing, valuable insights on how MLOps is applied to ensure technical and organizational security in cloud-based laboratory environments are provided [24]. In the enterprise IT governance group, the PubMed study [25] highlighted the importance of MLOps in the efficient management of AI models in the IT governance framework. For the ML model development and deployment group, multiple registries such as [26]–[55] contributed to a comprehensive view of how MLOps optimizes the entire lifecycle of models, from initial development to deployment in production environments. In the context of drug discovery, Yadav and Thakkar [56] highlighted the specific application of MLOps in the neural oscillation attention long short-term memory (NOA-LSTM) architecture for time series forecasting. However, multiple records [4], [17], [56]–[67] highlight that the implementation focuses on effective time series data management, optimization, and implementation of deployment pipelines that enable seamless integration in the discovery domain. The group focused on applications in Information security and policy compliance, in [60] detailed the creation of deepchecks, a library that uses MLOps to test and validate ML models and data likewise, the other records as [67]–[82] show that this type of implementation addresses critical security and compliance concerns by providing automated tools to assess the integrity and ethics of AI models used in different applications. The DevOps-related group on software engineering and anomaly detection showed how the paper [83] outlined a complete AI lifecycle, integrating MLOps for efficient anomaly detection throughout the development and production process. Finally, the group linked to cybersecurity and auditing revealed the specific application of MLOps in the cybersecurity decision support model [84], providing tools for risk identification and management in cyber environments. This systematic analysis provides a comprehensive overview of the various implementations of MLOps in specific contexts, highlighting their crucial role in the optimization and security of AI projects applied in computer auditing.

Table 7. Specific implementations of MLOps in the integration of AI projects

#	Implementations	Reference
1	Cloud Computing and Laboratory Security	[24]
2	Governance of Information Technologies in Colombian Companies	[25]
3	Development and Deployment of ML Models	[26]–[55]
4	MLOps Methodology in Drug Discovery	[4], [17], [56]–[66]
5	Applications in Information Security and Policy Compliance	[67]–[82]
6	DevOps in Software Engineering and Anomaly Detection	[83], [85]–[89]
7	Cybersecurity and Audit	[10], [84], [90]–[104]

The table highlights the diversity of applications of MLOps in various AI-related contexts. The specific implementation for each group presents unique approaches, demonstrating the adaptability of the MLOps methodology to diverse problems. This diversity reveals the richness of MLOps implementation in current research on AI project integration. Consequently, Table 8 presents a synthesis of alternative methodologies and efficiency differences in AI projects in computer auditing, each of them characterized. In the first group, composed of records such as the development and deployment of ML models, the implementation of a specific MLOps architecture is proposed to efficiently coordinate the development and deployment of models, optimizing operational efficiency in the management of computer audit projects [26], [60]. The second group, which includes registries such as patient-level explainable ML to predict major adverse cardiovascular events from single photon emission computed tomography (SPECT) myocardial perfusion imaging (MPI) and coronary computed tomography angiography (CCTA) images, highlights the application of an interpretable ML approach, improving efficiency in the identification of cardiovascular events at the patient level [30], [36], [56]. The third group, presenting radiological images and ML in trends, perspectives, and projections, proposes the application of advanced ML techniques to medical images to improve the identification of pathologies, thus optimizing the detection of anomalies in computer auditing [34], [43], [60]. The fourth group, which includes logs as iterative processes in a review of semi-supervised ML in rehabilitation science, highlights the implementation of iterative and semi-supervised processes in ML to improve efficiency in computer auditing projects with limited data sets [38], [44], [63]. The fifth group sees the comparison of different supervised ML algorithms for anomaly or disease prediction and suggests the comparison of supervised algorithms to optimize efficiency in computer audit projects related to prediction [31], [39], [59]. In the sixth group, the application of decentralized governance of ML, as evidenced in logs such as MLOps, is presented to improve efficiency in computer audit project management [4], [33], [66]. Finally, the seventh group, [24], [67], [81], presents technical and organizational security considerations for laboratory cloud computing, addresses security and compliance in MLOps projects, and optimizes efficiency in computer audit security in laboratory cloud environments. This detailed classification and analysis provides a comprehensive view of alternative methodologies and observed differences in efficiency.

Table 8. Matrix of alternative methodologies and difference in efficiency in MLOps projects

#	Alternative methodology	Difference in efficiency	Reference
1	Implement a specific MLOps architecture to efficiently coordinate the development and deployment of ML models in information technology audit projects.	Optimize laboratory cloud security by applying MLOps, thereby improving operational efficiency in project management.	[26], [60]
2	Use an interpretable ML approach to predict cardiovascular events from SPECT MPI and CCTA images, providing a clear understanding of model decisions.	Improve efficiency in the identification of adverse cardiovascular events at the patient level, thus optimizing decision making in health-related computer audits.	[30], [36], [56]
3	Apply advanced ML techniques to radiological and pathological images to improve pathology identification in the context of pathology.	Optimize the detection of anomalies in computer auditing through more accurate interpretation of medical images.	[34], [43], [60]
4	Implement iterative and semi-supervised processes in ML to optimize efficiency in rehabilitation science, especially in limited data sets.	Improve efficiency in computer audit projects where data sets are limited, through iterative and semi-supervised processes.	[38], [44], [63]
5	Carry out the comparison of different supervised ML algorithms for disease prediction, selecting the most effective one.	Optimize efficiency in computer audit projects related to medical evaluation through careful selection of disease prediction algorithms.	[31], [39], [59]
6	Implement decentralized governance of ML, providing an overview and overcoming challenges to improve efficiency in managing information technology audit projects.	Optimize information technology audit project management by decentralizing MLOps and addressing specific challenges.	[4], [33], [66]
7	Address technical and organizational security considerations for laboratory cloud computing in MLOps projects.	Improve the security efficiency of information technology audit projects in laboratory cloud environments through a detailed focus on technical and organizational security.	[24], [67], [81]

Upon examining the table, it becomes apparent that each group of registries has adopted a diverse range of approaches and strategies. Each alternative methodology is tailored to the specific nature of the analyzed projects, emphasizing crucial aspects such as interpretability in ML, the application of advanced techniques in medical imaging, and decentralized governance in MLOps. The efficiency difference is evident in how each approach enhances operational efficiency and security in various information technology audit contexts. The variety of approaches highlights the significance of tailoring the methodology to the specifics of each project, enabling efficient optimization of anomaly identification.

Table 9 presents a classification of 88 articles selected from PubMed and Scopus databases into 6 groups that allow a structured analysis of impact measurement in projects with and without MLOps, focusing on efficiency, performance, and anomaly detection. The first group, composed of articles [4], [26], [29], [32], [34], [43], [51], [60], [63], [66], [72], [77], [83], [86], efficiency in projects with MLOps was explored,

evaluating development time, resource utilization and adaptability in these contexts. In the second group, composed of articles [17], [27], [28], [30], [33], [35], [37], [39], [41], [42], [45], [48]–[50], [52], [53], [55], [56], [58]–[61], [68], [69], [71], [73]–[75], [78]–[82], [85], [86], [88], [90], [92]–[94], [105], [106], examined the performance in projects with MLOps, analyzing accuracy, processing speed, and scalability. The third group, composed of papers [10], [24], [25], [31], [36], [38], [40], [44], [46], [47], [54], [57], [62], [64], [65], [67], [70], [76], [84], [91], [95]–[104], focused on anomaly detection in projects with MLOps, evaluating the ability of the models to identify unconventional behaviors. Groups 4, 5, and 6 performed similar measurements but on projects without MLOps, analyzing efficiency, performance, and anomaly detection, respectively. The resulting table will provide a detailed and comparative analysis of impact measurement in different key aspects, providing a solid basis for the discussion and conclusions of this systematic review.

The table presents a comprehensive overview of how the implementation of MLOps affects efficiency, performance, and anomaly detection in AI projects applied to computer auditing. The results demonstrate the positive impact of MLOps on key aspects of project development, emphasizing its importance in enhancing operational efficiency, model performance, and the ability to identify and manage anomalies. In addition, the comparison between projects with and without MLOps highlights the potential limitations associated with the absence of this methodology. These findings provide a solid basis for the discussion and conclusions of the systematic review, emphasizing the importance of implementing MLOps in the context of computer auditing and AI.

Table 9. Measuring the impact of MLOps in AI projects for computer audit: efficiency, performance, and anomaly detection

#	Impact measurement	Reference
1	Efficiency in projects with MLOps	[4], [26], [29], [32], [34], [43], [51], [60], [63], [66], [72], [77], [83], [86]
2	Performance in projects with MLOps	[17], [27], [28], [30], [33], [35], [37], [39], [41], [42], [45], [48]–[50], [52], [53], [55], [56], [58]–[61], [68], [69], [71], [73]–[75], [78]–[82], [85], [87], [88], [90], [92]–[94], [105], [106]
3	Detection of anomalies in projects with MLOps	[10], [24], [25], [31], [36], [38], [40], [44], [46], [47], [54], [57], [62], [64], [65], [67], [70], [76], [84], [91], [95] – [104]
4	Efficiency in projects without MLOps	[10], [25], [28], [29], [33], [34], [37], [43], [44], [51], [54], [56], [59], [60], [61], [63], [65], [67], [72], [75], [78], [80], [83], [85], [88], [89], [91]–[93], [95]–[105]
5	Performance in projects without MLOps	[4], [17], [24], [26], [27], [30]–[32], [35], [36], [38]–[42], [45]–[50], [52], [53], [55], [57], [58], [60], [64], [66], [68]–[71], [73], [74], [76], [77], [79], [81], [82], [86], [87], [90], [106]
6	Anomaly detection in projects without MLOps	[10], [87], [92], [94]–[104]

4. CONCLUSIONS

This systematic review follows a sound methodology that includes formulating the research question using the PICO approach and applying the PRISMA methodology. The results significantly contribute to understanding the implementation of the MLOps methodology in identifying anomalies in integrating AI projects in computer auditing. The initial search strategy, which covered 1098 PubMed and 291 Scopus records, was refined by inclusion and exclusion criteria, resulting in a final sample of 88 relevant records. This selection process resulted in a retention rate of 8%, highlighting the rigor applied to ensure the relevance of the data analyzed. The bibliometric analysis revealed key trends in the literature reviewed. In recent years, there has been a steady increase in the publication of research on MLOps and AI projects applied in computer auditing. In addition, we identified specific topic areas that have received increased attention, providing a quantitative view of the most prominent areas of focus. At the level of handwritten results, each of the 88 selected logs contributed essential qualitative data. In this context, the quantitative figures support the robustness of the findings and provide a solid basis for conclusions. Also, the diversity and depth of the qualitative data extracted from the logs contribute to a more complete understanding of the impact of MLOps on anomaly identification in the integration of AI projects in computer auditing. These results support the importance of considering MLOps methodology as a crucial component in AI projects in computer auditing, providing tangible data and qualitative insights to inform future research and practical decisions in this dynamic field.

ACKNOWLEDGMENTS

Our deepest gratitude to the Technological University of Peru for being a fundamental pillar in the development of this research since their assistance, both in terms of literature and laboratory facilities, has been crucial to achieving the proposed objectives, and their management and support has made possible the significant progress of this research.

REFERENCES

- [1] M. V. D. Goes, "Scaling enterprise recommender systems for decentralization," in *Fifteenth ACM Conference on Recommender Systems*, New York, USA: ACM, Sep. 2021, pp. 592–594, doi: 10.1145/3460231.3474616.
- [2] K. Haller, *Managing AI in the Enterprise*. Berkeley, CA: Apress, 2022, doi: 10.1007/978-1-4842-7824-6.
- [3] A. Akkineni, S. Koohborfardhaghighi, and S. Singh, "Centrality of AI quality in MLOPs lifecycle and its impact on the adoption of AI/ML solutions," in *Intelligent Systems Design and Applications*, 2023, pp. 436–448, doi: 10.1007/978-3-031-35510-3_42.
- [4] D. Alsagheer, L. Xu, and W. Shi, "Decentralized machine learning governance: overview, opportunities, and challenges," *IEEE Access*, vol. 11, pp. 96718–96732, 2023, doi: 10.1109/ACCESS.2023.3311713.
- [5] E. Neghaw, Z. Wang, J. Huang, and Y. Liu, "Linking team-level and organization-level governance in machine learning operations through explainable AI and responsible AI connector," in *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, IEEE, Jun. 2023, pp. 1223–1230, doi: 10.1109/COMPSAC57700.2023.00185.
- [6] S. S. Sounchio, L. Geneste, B. K. -Foguem, C. Béler, S. N. Araghi, and M. R. Naqvi, "An enterprise architecture for interpersonal activity knowledge management," in *Knowledge Graphs and Semantic Web*, 2023, pp. 66–81, doi: 10.1007/978-3-031-47745-4_6.
- [7] L. Amini, E. H. E. Karni, M. Oubenal, H. E. Ouafy, M. Mbarki, and B. E. Ouadi, "Predictive study, using density functional theory and time dependent functional theory, on the structure-property quantification of methylene blue and methyl red dyes for the application in organic solar cells," *Current Chemistry Letters*, vol. 13, no. 1, pp. 187–198, 2024, doi: 10.5267/j.ccl.2023.7.002.
- [8] E. Peltonen and S. Dias, "LinkEdge: open-sourced MLOps integration with IoT edge," in *The 3rd Eclipse Security, AI, Architecture and Modelling Conference on Cloud to Edge Continuum*, New York, USA: ACM, 2023, pp. 67–76, doi: 10.1145/3624486.3624496.
- [9] E. D. Canedo *et al.*, "Information and communication technology (ICT) governance processes: a case study," *Information*, vol. 11, no. 10, Sep. 2020, doi: 10.3390/info11100462.
- [10] P. Loft, Y. He, I. Yevseyeva, and I. Wagner, "CAESAR8: An agile enterprise architecture approach to managing information security risks," *Computers and Security*, vol. 122, Nov. 2022, doi: 10.1016/j.cose.2022.102877.
- [11] R. Cohen, "Digital strategy, machine learning, and industry survey of MLOps," in *Digital Strategies and Organizational Transformation*, 2023, pp. 137–150, doi: 10.1142/9789811271984_0008.
- [12] S. Bhutad and K. Patil, "A novel system for potential mosquito breeding hotspot intimation and monitoring using MLOps and improved YoloV3," *Instrumentation Mesure Métrologie*, vol. 22, no. 1, pp. 35–40, Feb. 2023, doi: 10.18280/i2m.220105.
- [13] J. Pool, S. Akhlaghpour, F. Fatehi, and A. B. -Jones, "A systematic analysis of failures in protecting personal health data: A scoping review," *International Journal of Information Management*, vol. 74, Feb. 2024, doi: 10.1016/j.ijinfomgt.2023.102719.
- [14] M. Safdar *et al.*, "Fundamental requirements of a machine learning operations platform for industrial metal additive manufacturing," *Computers in Industry*, vol. 154, Jan. 2024, doi: 10.1016/j.compind.2023.104037.
- [15] J. D. -Arcaya, A. I. T. -Bastida, R. Miñón, and A. Almeida, "Orfeon: an AIOps framework for the goal-driven operationalization of distributed analytical pipelines," *Future Generation Computer Systems*, vol. 140, pp. 18–35, 2023, doi: 10.1016/j.future.2022.10.008.
- [16] A. Mukhopadhyay and S. Jain, "A framework for cyber-risk insurance against ransomware: A mixed-method approach," *International Journal of Information Management*, vol. 74, Feb. 2024, doi: 10.1016/j.ijinfomgt.2023.102724.
- [17] L. Sundberg and J. Holmström, "Democratizing artificial intelligence: How no-code AI can leverage machine learning operations," *Business Horizons*, vol. 66, no. 6, pp. 777–788, Nov. 2023, doi: 10.1016/j.bushor.2023.04.003.
- [18] S. Moreschini, D. Hästbacka, and D. Taibi, "MLOps pipeline development," in *Proceedings of the International Conference on Research in Adaptive and Convergent Systems*, New York, USA: ACM, Aug. 2023, pp. 1–8, doi: 10.1145/3599957.3606211.
- [19] A. Kathole, S. Shinde, and L. Wadhwa, "Integrating MLOps and EEG techniques for enhanced crime detection and prevention," *Multidisciplinary Science Journal*, vol. 6, no. 1, Jul. 2023, doi: 10.31893/multiscience.2024009.
- [20] F. Speth, C. Hartmann, U. Keschull, D. Sabath, and F. Sellmaier, "Towards transparent AI-systems: benefits of MLOps pipelines for space system development," in *Proceedings of the International Astronautical Congress, IAC*, 2022.
- [21] R. -Miñón, J. D. D. -Arcaya, A. I. T. -Bastida, and P. Hartlieb, "Pangea: An mlops tool for automatically generating infrastructure and deploying analytic pipelines in edge, fog and cloud layers," *Sensors*, vol. 22, no. 12, Jun. 2022, doi: 10.3390/s22124425.
- [22] G. G. -Tran and A. Monti, "Advances in time series forecasting development for power systems' operation with MLOps," *Forecasting*, vol. 4, no. 2, pp. 501–524, May 2022, doi: 10.3390/forecast4020028.
- [23] D. V. -Cruz, J. P. M. -Chávez, and R. G. G. -Contreras, "Towards the understanding of consumer behavior in the metaverse," in *IGI Global*, 2023, pp. 1–21, doi: 10.4018/978-1-6684-7029-9.ch001.
- [24] N. Krumm, "Organizational and technical security considerations for laboratory cloud computing," *The Journal of Applied Laboratory Medicine*, vol. 8, no. 1, pp. 180–193, Jan. 2023, doi: 10.1093/jalm/jfac118.
- [25] G. M. -Góngora and D. Aponte, "Dataset about information technology governance: A survey in Colombian enterprises," *Data in Brief*, vol. 50, Oct. 2023, doi: 10.1016/j.dib.2023.109480.
- [26] J. A. Pruneski *et al.*, "The development and deployment of machine learning models," *Knee Surgery, Sports Traumatology, Arthroscopy*, vol. 30, no. 12, pp. 3917–3923, Dec. 2022, doi: 10.1007/s00167-022-07155-4.
- [27] J. R. Verbiest, B. Bonnechère, W. Saeys, P. Van de Walle, S. Truijen, and P. Meyns, "Gait stride length estimation using embedded machine learning," *Sensors*, vol. 23, no. 16, Aug. 2023, doi: 10.3390/s23167166.
- [28] A. Ranjbar, F. Montazeri, M. V. Farashah, V. Mehrnosh, F. Darsareh, and N. Roozbeh, "Machine learning-based approach for predicting low birth weight," *BMC Pregnancy and Childbirth*, vol. 23, no. 1, Nov. 2023, doi: 10.1186/s12884-023-06128-w.
- [29] D. Wolf *et al.*, "Self-supervised pre-training with contrastive and masked autoencoder methods for dealing with small datasets in deep learning for medical imaging," *Scientific Reports*, vol. 13, no. 1, Nov. 2023, doi: 10.1038/s41598-023-46433-0.
- [30] F. Alahdab, R. El Shawi, A. I. Ahmed, Y. Han, and M. Al-Mallah, "Patient-level explainable machine learning to predict major adverse cardiovascular events from SPECT MPI and CCTA imaging," *PLOS ONE*, vol. 18, no. 11, Nov. 2023, doi: 10.1371/journal.pone.0291451.
- [31] S. Uddin, A. Khan, M. E. Hossain, and M. A. Moni, "Comparing different supervised machine learning algorithms for disease prediction," *BMC Medical Informatics and Decision Making*, vol. 19, no. 1, Dec. 2019, doi: 10.1186/s12911-019-1004-8.
- [32] O. Spjuth, J. Frid, and A. Hellander, "The machine learning life cycle and the cloud: implications for drug discovery," *Expert Opinion on Drug Discovery*, vol. 16, no. 9, pp. 1071–1079, Sep. 2021, doi: 10.1080/17460441.2021.1932812.
- [33] H. Park and J.-H. Son, "Machine learning techniques for THz imaging and time-domain spectroscopy," *Sensors*, vol. 21, no. 4, Feb. 2021, doi: 10.3390/s21041186.
- [34] Z. Zhang and E. Sejdíć, "Radiological images and machine learning: Trends, perspectives, and prospects," *Computers in Biology and Medicine*, vol. 108, pp. 354–370, May 2019, doi: 10.1016/j.compbiomed.2019.02.017.
- [35] V. Zinchuk and O. G. -Zinchuk, "Machine learning for analysis of microscopy images: a practical guide and latest trends," *Current Protocols*, vol. 3, no. 7, Jul. 2023, doi: 10.1002/cpz1.819.




- [36] S. A. Z. -Fregoso *et al.*, “Using artificial intelligence to develop a multivariate model with a machine learning model to predict complications in Mexican diabetic patients without arterial hypertension (national nested case-control study): metformin and elevated normal blood press,” *Journal of Diabetes Research*, pp. 1–11, Feb. 2023, doi: 10.1155/2023/8898958.
- [37] M. Romanowicz *et al.*, “Machine learning identifies smartwatch-based physiological biomarker for predicting disruptive behavior in children: a feasibility study,” *Journal of Child and Adolescent Psychopharmacology*, vol. 33, no. 9, pp. 387–392, Nov. 2023, doi: 10.1089/cap.2023.0038.
- [38] E. A. Kringle, E. C. Knutson, C. Engstrom, and L. Terhorst, “Iterative processes: a review of semi-supervised machine learning in rehabilitation science,” *Disability and Rehabilitation: Assistive Technology*, vol. 15, no. 5, pp. 515–520, Jul. 2020, doi: 10.1080/17483107.2019.1604831.
- [39] A. Z. Woldaregay *et al.*, “Data-driven modeling and prediction of blood glucose dynamics: Machine learning applications in type 1 diabetes,” *Artificial Intelligence in Medicine*, vol. 98, pp. 109–134, Jul. 2019, doi: 10.1016/j.artmed.2019.07.007.
- [40] R. Castaldo, C. Cavaliere, A. Soricelli, M. Salvatore, L. Pecchia, and M. Franzese, “Radiomic and genomic machine learning method performance for prostate cancer diagnosis: systematic literature review,” *Journal of Medical Internet Research*, vol. 23, no. 4, Apr. 2021, doi: 10.2196/22394.
- [41] S. Kaddoura, D. E. Popescu, and J. D. Hemanth, “A systematic review on machine learning models for online learning and examination systems,” *PeerJ Computer Science*, vol. 8, 2022, doi: 10.7717/peerj-cs.986.
- [42] R. Cuocolo *et al.*, “Machine learning for the identification of clinically significant prostate cancer on MRI: a meta-analysis,” *European Radiology*, vol. 30, no. 12, pp. 6877–6887, Dec. 2020, doi: 10.1007/s00330-020-07027-w.
- [43] J. H. Harrison *et al.*, “Introduction to artificial intelligence and machine learning for pathology,” *Archives of Pathology and Laboratory Medicine*, vol. 145, no. 10, pp. 1228–1254, Oct. 2021, doi: 10.5858/arpa.2020-0541-CP.
- [44] F. Fabris, J. P. D. Magalhães, and A. A. Freitas, “A review of supervised machine learning applied to ageing research,” *Biogerontology*, vol. 18, no. 2, pp. 171–188, Apr. 2017, doi: 10.1007/s10522-017-9683-y.
- [45] S. Kistkins *et al.*, “Comparative analysis of predictive interstitial glucose level classification models,” *Sensors*, vol. 23, no. 19, Oct. 2023, doi: 10.3390/s23198269.
- [46] K. Cao, K. Verspoor, S. Sahebjada, and P. N. Baird, “Accuracy of machine learning assisted detection of keratoconus: a systematic review and meta-analysis,” *Journal of Clinical Medicine*, vol. 11, no. 3, Jan. 2022, doi: 10.3390/jcm11030478.
- [47] F. V. D. Sommen *et al.*, “Machine learning in GI endoscopy: practical guidance in how to interpret a novel field,” *Gut*, vol. 69, no. 11, pp. 2035–2045, Nov. 2020, doi: 10.1136/gutjnl-2019-320466.
- [48] C. Caruso, “Machine learning models ID cancer drivers,” *Cancer Discovery*, vol. 11, no. 10, pp. 2361–2362, Oct. 2021, doi: 10.1158/2159-8290.CD-NB2021-0376.
- [49] F. Mohr, M. Wever, A. Tornede, and E. Hullermeier, “Predicting machine learning pipeline runtimes in the context of automated machine learning,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 43, no. 9, pp. 3055–3066, Sep. 2021, doi: 10.1109/TPAMI.2021.3056950.
- [50] D. Falla, V. Devecchi, D. J. -Grande, D. Rügamer, and B. X. W. Liew, “Machine learning approaches applied in spinal pain research,” *Journal of Electromyography and Kinesiology*, vol. 61, Dec. 2021, doi: 10.1016/j.jelekin.2021.102599.
- [51] D. Ledesma, S. Symes, and S. Richards, “Advancements within modern machine learning methodology: impacts and prospects in biomarker discovery,” *Current Medicinal Chemistry*, vol. 28, no. 32, pp. 6512–6531, Oct. 2021, doi: 10.2174/0929867328666210208111821.
- [52] R. R. Gupta, “Application of artificial intelligence and machine learning in drug discovery,” in *Artificial Intelligence in Drug Design*, 2022, pp. 113–124, doi: 10.1007/978-1-0716-1787-8_4.
- [53] J. Raman, S. Venkatesh, and R. Bellomo, “Machine learning in risk prediction for cardiac surgery-an emerging trend?” *Heart, Lung and Circulation*, vol. 30, no. 12, pp. 1790–1791, Dec. 2021, doi: 10.1016/j.hlc.2021.09.007.
- [54] D. Jancarczyk, M. Bernaś, and T. Boczar, “Classification of low frequency signals emitted by power transformers using sensors and machine learning methods,” *Sensors*, vol. 19, no. 22, Nov. 2019, doi: 10.3390/s19224909.
- [55] J. D. Elhai and C. Montag, “The compatibility of theoretical frameworks with machine learning analyses in psychological research,” *Current Opinion in Psychology*, vol. 36, pp. 83–88, Dec. 2020, doi: 10.1016/j.copsyc.2020.05.002.
- [56] H. Yadav and A. Thakkar, “NOA-LSTM: An efficient LSTM cell architecture for time series forecasting,” *Expert Systems with Applications*, vol. 238, Mar. 2024, doi: 10.1016/j.eswa.2023.122333.
- [57] J. C. G. Mejia, F. A. V. Agudelo, M. M. Rivas, and I. A. Delgado, “Method to manage the security of information assets (in Spanish: método para gestionar la seguridad de activos de Información),” *Revista Iberica de Sistemas e Tecnologias de Informacao*, pp. 252–266, 2023.
- [58] Y. Ai *et al.*, “A deep learning approach on short-term spatiotemporal distribution forecasting of dockless bike-sharing system,” *Neural Computing and Applications*, vol. 31, no. 5, pp. 1665–1677, May 2019, doi: 10.1007/s00521-018-3470-9.
- [59] D. Kreuzberger, N. Kühn, and S. Hirschl, “Machine learning operations (MLOps): overview, definition, and architecture,” *IEEE Access*, vol. 11, pp. 31866–31879, 2023, doi: 10.1109/ACCESS.2023.3262138.
- [60] S. Chorev *et al.*, “Deepchecks: a library for testing and validating machine learning models and data,” *Journal of Machine Learning Research*, vol. 23, 2022.
- [61] P. Ruf, M. Madan, C. Reich, and D. O. -Abdeslam, “Demystifying MLOps and presenting a recipe for the selection of open-source tools,” *Applied Sciences*, vol. 11, no. 19, Sep. 2021, doi: 10.3390/app11198861.
- [62] A. M. D. Río, I. S. Ramirez, M. Papaelias, and F. P. G. Márquez, “Pattern recognition based on statistical methods combined with machine learning in railway switches,” *Expert Systems with Applications*, vol. 238, Mar. 2024, doi: 10.1016/j.eswa.2023.122214.
- [63] D. J. Kedziora, T.-D. Nguyen, K. Musial, and B. Gabrys, “On taking advantage of opportunistic meta-knowledge to reduce configuration spaces for automated machine learning,” *Expert Systems with Applications*, vol. 239, Apr. 2024, doi: 10.1016/j.eswa.2023.122359.
- [64] Z. Zhang, Y. Li, S. Yang, Z. Zhang, and Y. Lei, “Code-aware fault localization with pre-training and interpretable machine learning,” *Expert Systems with Applications*, vol. 238, Mar. 2024, doi: 10.1016/j.eswa.2023.121689.
- [65] K. Filippou, G. Aifantis, G. A. Papakostas, and G. E. Tsekouras, “Structure learning and hyperparameter optimization using an automated machine learning (AutoML) pipeline,” *Information*, vol. 14, no. 4, Apr. 2023, doi: 10.3390/info14040232.
- [66] K. Lefevre *et al.*, “ModelOps for enhanced decision-making and governance in emergency control rooms,” *Environment Systems and Decisions*, vol. 42, no. 3, pp. 402–416, Sep. 2022, doi: 10.1007/s10669-022-09855-1.
- [67] N. Fong and S. B. -Ore, “Considerations for compliance with the information security policy (in Spanish: Consideraciones para el cumplimiento de la política de seguridad de la información),” *Revista Iberica de Sistemas e Tecnologias de Informacao*, pp. 528–539, 2022.

- [68] R. Grande, A. Vizcaino, and F. O. García, "Is it worth adopting DevOps practices in global software engineering? Possible challenges and benefits," *Computer Standards and Interfaces*, vol. 87, Jan. 2024, doi: 10.1016/j.csi.2023.103767.
- [69] O. H. Plant, J. V. Hillegersberg, and A. Aldea, "Rethinking IT governance: Designing a framework for mitigating risk and fostering internal control in a DevOps environment," *International Journal of Accounting Information Systems*, vol. 45, Jun. 2022, doi: 10.1016/j.accinf.2022.100560.
- [70] J. Nord, C. S. Sargent, A. Koohang, and A. Marotta, "Predictors of success in information security policy compliance," *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 863–873, Jul. 2022, doi: 10.1080/08874417.2022.2067795.
- [71] S. B. -Oré and N. F. Ochoa, "Information security policy compliance: usefulness and ease of use," in *International Congress on Information and Communication Technology*, 2024, pp. 413–419, doi: 10.1007/978-981-99-3236-8_32.
- [72] M. Dieguez and C. Cares, "Comparison of two quantitative approaches to selecting information security controls (in Spanish: Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información)," *Revista Iberica de Sistemas e Tecnologias de Informacao*, no. 32, pp. 113–128, 2019.
- [73] L. Almeida and A. Respicio, "Decision support for selecting information security controls," *Journal of Decision Systems*, vol. 27, pp. 173–180, May 2018, doi: 10.1080/12460125.2018.1468177.
- [74] G. Ugunbayar, A. Yautsiukhin, F. Martinelli, and F. Massacci, "Optimisation of cyber insurance coverage with selection of cost-effective security controls," *Computers and Security*, vol. 101, Feb. 2021, doi: 10.1016/j.cose.2020.102121.
- [75] M. D. -Dorado, D. C. -Polo, J. C. -Murillo, F. J. R. -Pérez, and J. G. -Brajones, "Fast, lightweight, and efficient cybersecurity optimization for tactical-operational management," *Applied Sciences*, vol. 13, no. 10, May 2023, doi: 10.3390/app13106327.
- [76] C. R. S. Guaman, S. A. M. Vivar, D. P. P. Rivera, and F. A. C. Calderon, "Perception of information security in small and medium-sized businesses in Santo Domingo (in Spanish: Percepción de seguridad de la información en las pequeñas y medianas empresas en santo domingo)," *Investigacion Operacional*, vol. 40, no. 3, pp. 421–428, 2019.
- [77] A. H. Fawzy, K. Wassif, and H. Moussa, "Framework for automatic detection of anomalies in DevOps," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 3, pp. 8–19, Mar. 2023, doi: 10.1016/j.jksuci.2023.02.010.
- [78] D. Korać, B. Damjanović, D. Simić, and K.-K. R. Choo, "A hybrid XSS attack (H XSS) based on fusion approach: Challenges, threats and implications in cybersecurity," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 9284–9300, Nov. 2022, doi: 10.1016/j.jksuci.2022.09.008.
- [79] S. Henning and W. Hasselbring, "The titan control center for industrial DevOps analytics research," *Software Impacts*, vol. 7, Feb. 2021, doi: 10.1016/j.simpa.2020.100050.
- [80] B. Wang *et al.*, "Research on anomaly detection and real-time reliability evaluation with the log of cloud platform," *Alexandria Engineering Journal*, vol. 61, no. 9, pp. 7183–7193, Sep. 2022, doi: 10.1016/j.aej.2021.12.061.
- [81] S. Almuairfi and M. Alenezi, "Security controls in infrastructure as code," *Computer Fraud and Security*, vol. 2020, no. 10, pp. 13–19, Jan. 2020, doi: 10.1016/S1361-3723(20)30109-3.
- [82] H.-L. Truong and P. Klein, "DevOps contract for assuring execution of IoT microservices in the edge," *Internet of Things*, vol. 9, Mar. 2020, doi: 10.1016/j.iot.2019.100150.
- [83] D. D. Silva and D. Alahakoon, "An artificial intelligence life cycle: From conception to production," *Patterns*, vol. 3, no. 6, Jun. 2022, doi: 10.1016/j.patter.2022.100489.
- [84] K. Razikin and B. Soewito, "Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework," *Egyptian Informatics Journal*, vol. 23, no. 3, pp. 383–404, Sep. 2022, doi: 10.1016/j.eij.2022.03.001.
- [85] W. Li, W. Hu, T. Chen, N. Chen, and C. Feng, "StackVAE-G: An efficient and interpretable model for time series anomaly detection," *AI Open*, vol. 3, pp. 101–110, 2022, doi: 10.1016/j.aiopen.2022.07.001.
- [86] M. Steidl, M. Felderer, and R. Ramler, "The pipeline for the continuous development of artificial intelligence models-current state of research and practice," *Journal of Systems and Software*, vol. 199, May 2023, doi: 10.1016/j.jss.2023.111615.
- [87] J. Xu *et al.*, "StreamAD: A cloud platform metrics-oriented benchmark for unsupervised online anomaly detection," *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, vol. 3, no. 2, Jun. 2023, doi: 10.1016/j.bench.2023.100121.
- [88] J. Henriques, F. Caldeira, T. Cruz, and P. Simões, "An automated closed-loop framework to enforce security policies from anomaly detection," *Computers and Security*, vol. 123, Dec. 2022, doi: 10.1016/j.cose.2022.102949.
- [89] P. Singh, "Systematic review of data-centric approaches in artificial intelligence and machine learning," *Data Science and Management*, vol. 6, no. 3, pp. 144–157, Sep. 2023, doi: 10.1016/j.dsm.2023.06.001.
- [90] N. D. -Rodríguez, J. D. Ser, M. Coeckelbergh, M. L. D. Prado, E. H. -Viedma, and F. Herrera, "Connecting the dots in trustworthy artificial intelligence: from AI principles, ethics, and key requirements to responsible AI systems and regulation," *Information Fusion*, vol. 99, Nov. 2023, doi: 10.1016/j.inffus.2023.101896.
- [91] J. N. Al-Karaki, A. Gawanmeh, and S. El-Yassami, "GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 6, pp. 3079–3095, Jun. 2022, doi: 10.1016/j.jksuci.2020.09.011.
- [92] N. Ebert, T. Schaltegger, B. Ambuehl, L. Schöni, V. Zimmermann, and M. Knieps, "Learning from safety science: A way forward for studying cybersecurity incidents in organizations," *Computers and Security*, vol. 134, Nov. 2023, doi: 10.1016/j.cose.2023.103435.
- [93] F. Abdullayeva, "Cyber resilience and cyber security issues of intelligent cloud computing systems," *Results in Control and Optimization*, vol. 12, Sep. 2023, doi: 10.1016/j.rico.2023.100268.
- [94] I. D. S. -García, T. S. F. Gilabert, and J. A. C. -Manzano, "Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review," *Computers and Security*, vol. 128, May 2023, doi: 10.1016/j.cose.2023.103170.
- [95] A. Paya, A. Cotarelo, and J. M. Redondo, "Egida: Automated security configuration deployment systems with early error detection," *Computers and Security*, vol. 116, May 2022, doi: 10.1016/j.cose.2022.102638.
- [96] N. Mäurer, T. Guggemos, T. Ewert, T. Gräupl, C. Schmitt, and S. Grundner-Culemann, "Security in digital aeronautical communications a comprehensive gap analysis," *International Journal of Critical Infrastructure Protection*, vol. 38, Sep. 2022, doi: 10.1016/j.ijcip.2022.100549.
- [97] S. Pawar and D. H. Palivela, "LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)," *International Journal of Information Management Data Insights*, vol. 2, no. 1, Apr. 2022, doi: 10.1016/j.jjime.2022.100080.
- [98] I. F. D. Arroyabe, C. F. A. Arranz, M. F. Arroyabe, and J. C. F. D. Arroyabe, "Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019," *Computers and Security*, vol. 124, Jan. 2023, doi: 10.1016/j.cose.2022.102954.
- [99] S. Slapničar, T. Vuko, M. Čular, and M. Drašček, "Effectiveness of cybersecurity audit," *International Journal of Accounting Information Systems*, vol. 44, Mar. 2022, doi: 10.1016/j.accinf.2021.100548.




- [100] N. Rawindaran, A. Jayal, E. Prakash, and C. Hewage, "Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales," *International Journal of Information Management Data Insights*, vol. 3, no. 2, Nov. 2023, doi: 10.1016/j.ijime.2023.100191.
- [101] M.-C. Alejandro, G.-H. Andrés, and V.-F. Ricardo, "Constructing an architecture-based cybersecurity solution for a system," *MethodsX*, vol. 10, 2023, doi: 10.1016/j.mex.2023.102010.
- [102] Ž. Turk, B. García de Soto, B. R. K. Mantha, A. Maciel, and A. Georgescu, "A systemic framework for addressing cybersecurity in construction," *Automation in Construction*, vol. 133, Jan. 2022, doi: 10.1016/j.autcon.2021.103988.
- [103] S. Slapničar, M. Axelsen, I. Bongiovanni, and D. Stockdale, "A pathway model to five lines of accountability in cybersecurity governance," *International Journal of Accounting Information Systems*, vol. 51, Dec. 2023, doi: 10.1016/j.accinf.2023.100642.
- [104] A. R. -González, P. A. -Cabarcos, and J. P. -Arnau, "Privacy-centered authentication: A new framework and analysis," *Computers and Security*, vol. 132, Sep. 2023, doi: 10.1016/j.cose.2023.103353.
- [105] P. Sha, S. Chen, L. Zheng, X. Liu, H. Tang, and Y. Li, "Design and implement of microservice system for edge computing," *IFAC-PapersOnLine*, vol. 53, no. 5, pp. 507–511, 2020, doi: 10.1016/j.ifacol.2021.04.137.
- [106] M. A. Akbar, K. Smolander, S. Mahmood, and A. Alsanad, "Toward successful DevSecOps in software development organizations: A decision-making framework," *Information and Software Technology*, vol. 147, Jul. 2022, doi: 10.1016/j.infsof.2022.106894.

BIOGRAPHIES OF AUTHORS






Sheyla Reymundez Suarez    student passionate about computing and technology, currently studying Systems Engineering at the Technological University of Peru. Her interest in this field is reflected in her constant search for knowledge and experiences that enrich her academic training. Her dedication has allowed me to stand out in academic projects, actively participating in multidisciplinary teams to solve technological challenges. She opens to internship opportunities, research projects, and collaborations that allow me to expand her experience and contribute to the constantly evolving technological world. She can be contacted at email: u18310845@utp.edu.pe.






Bryan Martínez Huamani    student passionate about computing and technology, currently embarking on his academic journey in the Systems Engineering degree at the Technological University of Peru. Beyond achievements in the academic field, he seeks to broaden my horizons by actively participating in events and conferences related to technology. As a committed student, he constantly looking for opportunities to apply his knowledge in practical and collaborative projects, with the aim of contributing to the advancement of technology and facing the challenges inherent to systems engineering. He can be contacted at email: u18304453@utp.edu.pe.



María Acuña Meléndez    is professor at the Faculty of Engineering of Engineering of the Technological University of Peru, Lima-Peru. She holds a Ph.D. in Systems Engineering. Her research areas are Information Systems and Communications, as well as Systems Auditing and Information Security. She has participated in several research projects, as well as in thesis advising. She has registered several patents on software copyrights. Her research interests include information systems, data science, information security, data mining, artificial intelligence, and knowledge management among other related lines of research. She can be contacted at email: c21584@utp.edu.pe.



Christian Ovalle    is an associate professor at the Faculty of Engineering of the Technological University of Peru, Lima-Peru. He has a Ph.D. in Systems Engineering with a specialization in artificial intelligence. His research areas are process mining, business data analysis, and pattern recognition. He is the CEO of the 7D consultancy dedicated to the investigation of intelligent solutions. He has participated in different research projects, receiving awards from the Peruvian Ministry of Defense and the Armed Forces Army for the best general researcher, which is a technology-based company and his innovative products received national and international recognition. He has filed a number of patents and industrial designs on his innovative ideas. His research interests include data mining, artificial intelligence, image/signal processing, bibliometrics, and pattern recognition. He can be contacted at email: dovalle@utp.edu.pe.