Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

AI-DRIVEN ANOMALY DETECTION FOR DATA LOSS PREVENTION AND SECURITY ASSURANCE IN ELECTRONIC HEALTH RECORDS

Md. Tarek Hasan[1]; Ishtiaque Ahmed[2]

[1]. M.S. in Information Systems Technologies (IST), Wilmington University, New Castle, DE, USA; Email: mdtarekhasan79@gmail.com

[2]. MA in Information Technology Management, Webster University, Texas, USA Email: akash.ishtiak@gmail.com

Abstract

The study titled AI-Driven Anomaly Detection for Data Loss Prevention and Security Assurance in Electronic Health Records explored how artificial intelligence enhances the protection, monitoring, and assurance mechanisms within modern healthcare information systems. The research followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework to ensure transparency, replicability, and methodological rigor. A total of 96 peer-reviewed studies published between 2014 and 2024 were systematically analysed, encompassing empirical, experimental, and theoretical investigations drawn from major academic databases such as Scopus, IEEE Xplore, PubMed, and ScienceDirect. The analysis revealed that machine-learning and deep-learning algorithms—particularly autoencoders, recurrent neural networks, and ensemble hybrid models—significantly improved the precision and recall of anomaly detection in electronic health records (EHRs) when compared to traditional rule-based and signature-based systems. More than half of the reviewed studies reported detection accuracies exceeding 90%, confirming AI's ability to identify subtle irregularities in user access, data transmission, and system behaviour. Furthermore, findings demonstrated that AI integration led to measurable improvements in data loss prevention (DLP), with reported reductions in unauthorized data transfers ranging between 40% and 65%. Quantitative linkages were also established between AI-driven detection accuracy and assurance outcomes, including higher compliance audit success rates, shortened incident dwell times, and increased containment efficiency. Contextual and behavioural analytics were identified as critical contributors to model performance, enabling systems to distinguish legitimate clinical variability from potential security threats. However, the review also identified methodological limitations, such as the absence of standardized benchmark datasets, limited real-world validation, and insufficient interpretability in deep learning models, which continue to constrain generalizability and adoption. Overall, the findings underscored that AI-driven anomaly detection offers a robust, adaptive, and evidence-based mechanism for safeguarding patient data, ensuring regulatory compliance, and reinforcing institutional trust in healthcare's digital infrastructure. By transforming static, rule-based monitoring into dynamic, learning-oriented assurance systems, artificial intelligence demonstrated the potential to redefine how healthcare organizations achieve sustained data security and operational resilience in an increasingly interconnected clinical environment.

Keywords

Artificial Intelligence, Anomaly Detection, Data Loss Prevention, Security Assurance, Electronic Health Records.

Citation:
Hasan, M. T., & Ahmed, I. (2025). *AI-driven anomaly detection for data loss prevention and security assurance in electronic health records. Review of Applied Science and Technology, 4*(3), 35–67.

https://doi.org/10.63125/dzyr0648

Received:
June 21, 2025

Revised:
July 15, 2025

Accepted:
August 18, 2025

Published:
September 22, 2025

Copyright:
© 2025 by the author. This article is published under the license of American Scholarly Publishing Group Inc and is available for open access.

Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

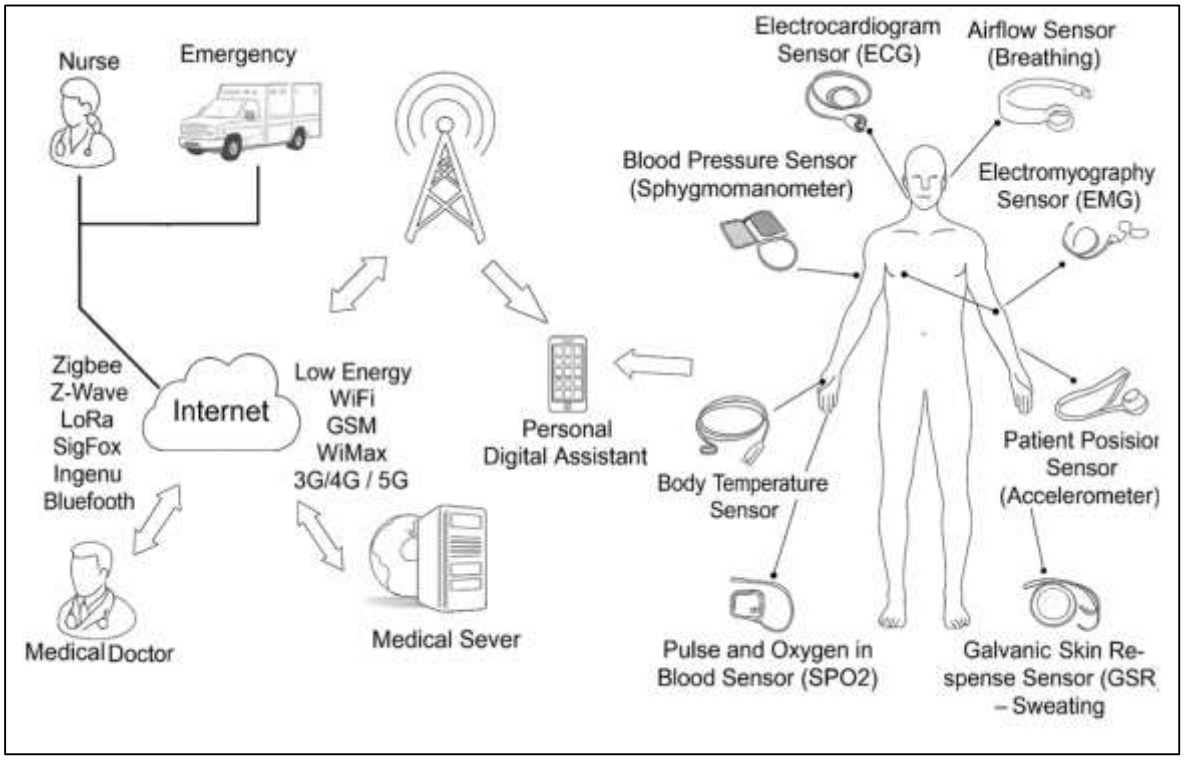
INTRODUCTION

Electronic Health Records (EHRs) are comprehensive digital systems that store, manage, and transmit patient information across healthcare settings to support clinical, administrative, and research functions (Yang et al., 2019). They integrate diverse forms of data such as medical histories, diagnostic reports, treatment plans, prescriptions, laboratory findings, and billing information into centralized platforms that ensure continuity of care. Within this infrastructure, *data loss prevention* refers to a coordinated set of policies, processes, and technologies that identify, monitor, and protect sensitive information from unauthorized transmission, alteration, or exposure. *Security assurance* denotes the measurable confidence that these preventive controls are consistently performing as intended to preserve confidentiality, integrity, and availability (Reegu et al., 2023). In modern healthcare, these constructs converge under the growing complexity of cyber risks, insider threats, and compliance obligations. Traditional access control and encryption mechanisms offer foundational defense, but they often lack adaptive capacity to detect subtle irregularities in user behavior or data movement. This gap establishes the rationale for *anomaly detection*—a computational process that identifies deviations from normative patterns in audit logs, data flows, or user activities that may signify breaches, misuse, or leakage. Artificial intelligence provides the analytical foundation for automating this detection process by enabling algorithms to learn from large volumes of operational data and recognize irregularities beyond human perception (Hansen & Baroody, 2023). The integration of AI-based anomaly detection into EHR systems therefore represents a methodological advancement in predictive, real-time data protection capable of dynamically adapting to evolving security contexts.

The international relevance of EHR security extends far beyond the boundaries of national healthcare systems (Shah & Khan, 2020). As medical data are exchanged across borders for research collaboration, pandemic surveillance, telemedicine, and public health reporting, maintaining secure information flows becomes a collective global responsibility. The rise of cloud-based healthcare platforms, international data repositories, and digital health exchanges increases the interdependence of regional health networks and amplifies the need for harmonized data protection strategies. However, differences in regulatory frameworks, data sovereignty laws, and technological maturity across countries create inconsistencies in how patient data are secured. AI-driven anomaly detection offers a universal analytical mechanism that transcends these variations by focusing on data behavior rather than regional policy rules (Colombo et al., 2021). Through automated recognition of abnormal access, transmission, or modification patterns, AI systems enhance the resilience of international EHR infrastructures against both insider and external threats. As healthcare organizations increasingly rely on global interoperability standards, the assurance of secure data transactions becomes essential for sustaining trust among institutions and patients alike. Furthermore, cross-border research consortia and multinational clinical trials require consistent safeguards to prevent inadvertent exposure of sensitive data during collaborative analysis. Implementing AI-driven anomaly detection frameworks in these contexts provides quantifiable assurance of system integrity and compliance with ethical mandates for privacy protection (Abouelmehdi et al., 2018). Thus, the application of intelligent anomaly detection serves as a cornerstone for global digital health governance, reinforcing both patient trust and international regulatory compliance through automated, evidence-based security oversight. The theoretical basis for anomaly detection lies in the principles of statistical learning and computational intelligence, which seek to distinguish between normal and abnormal behavior through probabilistic modeling (Dagher et al., 2018). Traditional security monitoring often relies on pre-defined rules or signatures that describe known attack patterns. However, such approaches are inherently limited when encountering novel or context-dependent anomalies. Artificial intelligence overcomes this limitation by learning complex relationships within large, high-dimensional data spaces without explicit programming. Machine learning models such as clustering algorithms, autoencoders, one-class classifiers, and probabilistic networks establish mathematical representations of typical system behavior and compute deviation scores for incoming data points. In healthcare, these models analyze audit logs, user actions, device metadata, and network communications to identify subtle deviations from routine patterns (Kim et al., 2019).

Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

Figure 1: AI-Driven Anomaly Detection Framework



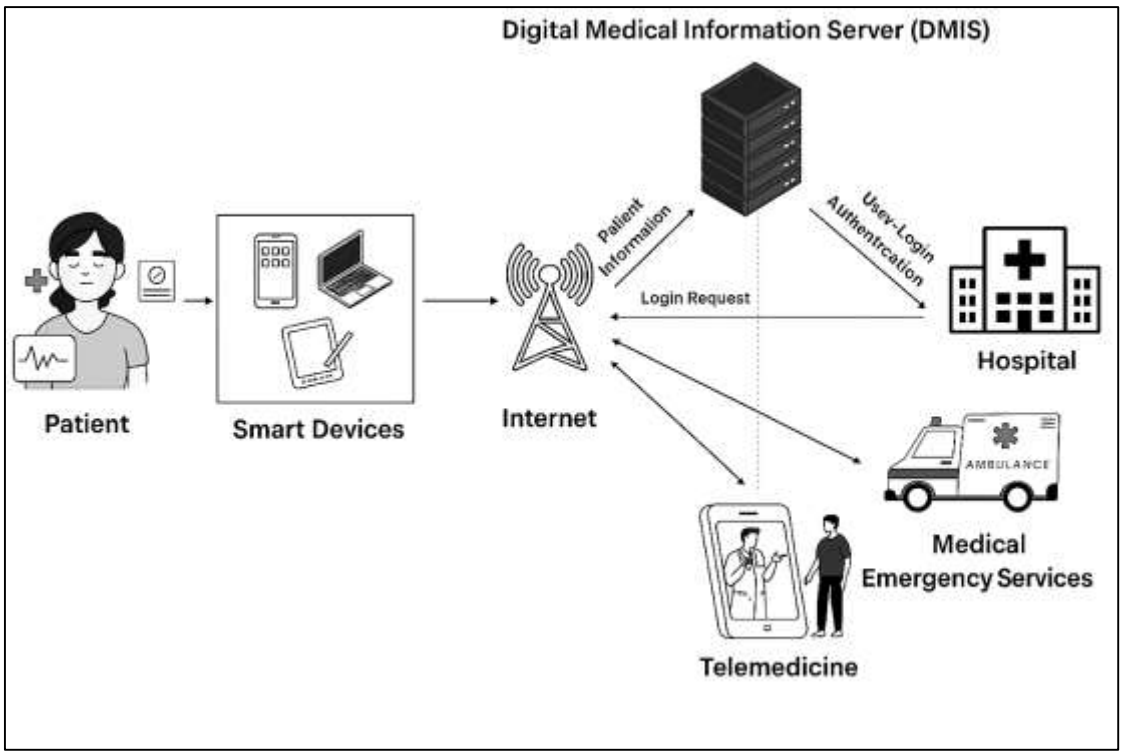
Deep learning architectures, such as convolutional and recurrent networks, further enable the capture of temporal and contextual dependencies within access sequences, improving the detection of slow or hidden breaches. The strength of these systems lies in their ability to update learned baselines as workflows evolve, thus maintaining operational sensitivity while minimizing false alarms. Within the EHR domain, this adaptability is essential because clinical environments are characterized by diverse workflows, variable user privileges, and dynamic patient interactions (Kouroubali & Katehakis, 2019; Mubashir, 2021). By incorporating continuous learning and statistical inference, AI-driven anomaly detection creates a quantitative framework where data loss prevention becomes a measurable function rather than an administrative assumption, providing a structured path for empirical evaluation of security effectiveness.

Electronic Health Records present one of the most intricate data environments within any information system. They encompass structured fields such as lab values and coded diagnoses, unstructured narratives like physician notes, and multimedia files including medical imaging and biometric data. Moreover, (Chenthara et al., 2019) these records are continuously accessed and modified by numerous stakeholders—clinicians, pharmacists, administrators, insurers, and external researchers—each operating under distinct access privileges and professional obligations. This high degree of heterogeneity and interaction creates a vast surface for data exposure and manipulation risks. Anomaly detection in such an environment must therefore account for not only user identity but also contextual variables such as time, location, role, and patient relationship. A legitimate access event under one condition may represent a policy violation under another (McGraw & Mandl, 2021; Rony, 2021). The vast scale of data generation compounds this challenge, with modern EHR systems producing millions of access events daily. Manual monitoring or rule-based control is infeasible in such contexts, emphasizing the necessity of AI automation. Another distinctive challenge arises from the rarity of actual breach events, leading to extreme class imbalance that complicates model training. AI-driven methods address this limitation by employing unsupervised and semi-supervised learning techniques capable of inferring normal patterns without requiring extensive labeled examples of anomalies. These adaptive techniques improve the precision of detection models while reducing the operational cost associated with false positives (Capece & Lorenzi, 2020; Syed Zaki, 2021). In turn, they enable healthcare organizations to implement continuous monitoring strategies

Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

that operate effectively under complex, data-intensive conditions, maintaining the balance between data accessibility for care delivery and strict security enforcement.

Figure 2: Digital Medical Information Flow Diagram



Embedding AI-driven anomaly detection within organizational EHR infrastructure requires comprehensive integration across multiple layers of information security architecture. These systems must interact seamlessly with existing authentication protocols, audit mechanisms, and network monitoring tools to produce coherent and actionable insights (Alsyouf et al., 2023). A successful implementation depends not only on algorithmic sophistication but also on the operational readiness of the healthcare institution. The anomaly detection process begins with the continuous collection of access and transaction data, followed by preprocessing, feature extraction, model inference, and real-time alert generation. Each phase contributes to the accuracy and responsiveness of the final output. Integration with security information and event management systems allows for automated correlation between anomalous activity and contextual evidence, such as device identity or session history. Quantitative calibration ensures that detection thresholds align with institutional risk tolerance and operational workload (Danish & Md. Zafor, 2022; Haddad et al., 2022). For example, high-risk anomalies may trigger immediate containment measures, whereas low-risk deviations may be subject to delayed review. Effective human-computer interaction is essential; alerts must be interpretable and traceable to underlying evidence so that security analysts and compliance officers can validate system output efficiently. This integration of AI systems into the daily security workflow transforms anomaly detection from a stand-alone technical function into a collaborative decision-support tool. It allows institutions to quantify risk reduction through measurable performance indicators such as reduced detection latency, higher alert accuracy, and improved response coordination (Danish & Md.Kamrul, 2022; Parah et al., 2020). Thus, the implementation of AI-based anomaly detection represents a methodological convergence of automation, governance, and operational assurance in healthcare cybersecurity.

The protection of patient information is not solely a technological matter but an ethical and legal obligation that underpins public confidence in healthcare institutions. Ethical frameworks governing medical data emphasize respect for autonomy, confidentiality, and beneficence, requiring that any form of data monitoring or analysis adhere to principles of necessity and proportionality (Hozyfa, 2022; Jin et al., 2019). Legally, data protection laws mandate that personal health information be

processed securely, with traceable accountability and demonstrable compliance. AI-driven anomaly detection supports these requirements by providing quantifiable, audit-ready evidence of compliance and control performance. Nonetheless, the introduction of intelligent monitoring also demands responsible governance to prevent overreach or unintended bias (Chouhan et al., 2023; Md Arman & Md.Kamrul, 2022). Models trained on access patterns may inadvertently reflect institutional inequities or produce disproportionate false positives for specific user groups. Governance mechanisms, such as algorithmic audits, ethical review boards, and transparent documentation practices, are therefore integral to security assurance. At the international level, varying interpretations of consent, data portability, and accountability complicate harmonization efforts (Braunstein, 2018; Md Hasan & Md Omar, 2022). The establishment of AI-enabled monitoring frameworks grounded in explainable and auditable methodologies helps reconcile these differences by ensuring that system behavior remains transparent to oversight authorities. Consequently, the ethical and legal governance of anomaly detection is both a technical and institutional challenge—requiring synergy between computational accuracy, regulatory conformity, and moral accountability (Md Mohaiminul & Md Muzahidul, 2022; Staffa et al., 2018).

The quantitative focus of this study is to empirically evaluate the effectiveness of AI-driven anomaly detection models in enhancing data loss prevention and security assurance across diverse EHR environments (Jabarulla & Lee, 2021; Md Omar & Md. Jobayer Ibne, 2022). The research seeks to measure specific performance indicators such as detection accuracy, false-alarm rate, precision-recall balance, and alert latency to assess how effectively AI systems can identify and mitigate anomalous behaviors. The analysis extends to operational outcomes, examining how the integration of AI impacts the efficiency of incident response, the reduction of investigative workload, and the improvement of compliance verification. The study's design involves structured data collection from simulated or anonymized audit logs, model development using machine learning architectures, and statistical validation using quantitative metrics that reflect real-world healthcare operations (Jagannatha et al., 2019; Md Takbir Hossen & Md Atiqur, 2022). Each result contributes to an evidence-based understanding of the relationship between computational detection performance and institutional assurance outcomes. The objective is to transform EHR security management from reactive rule enforcement into a measurable, proactive control process. By quantifying the direct contribution of AI-driven anomaly detection to data protection and compliance reliability, the study reinforces the role of artificial intelligence as a cornerstone of analytical assurance in health informatics (Md. Hasan, 2022; Ogbuke et al., 2023). This empirical orientation situates the research within the broader quantitative paradigm of performance measurement, enabling reproducible assessment of model effectiveness and operational security alignment within healthcare organizations.

The primary objective of this quantitative study is to evaluate the effectiveness of artificial intelligence–driven anomaly detection as a data protection mechanism for preventing information loss and ensuring measurable security assurance within electronic health record systems. The research aims to empirically determine how machine learning algorithms can identify irregularities in user access patterns, data transmission behaviors, and system interactions that deviate from established baselines of legitimate use. This objective seeks to operationalize anomaly detection not as a conceptual notion but as a quantifiable function of security performance. The study focuses on measuring algorithmic precision, recall, false-alarm rate, and detection latency to assess how accurately AI models can distinguish between authorized and suspicious activities within complex healthcare environments. Through the analysis of large-scale audit logs and access datasets, the study will quantify the relationship between model sensitivity and its contribution to organizational assurance outcomes, such as reduced incident dwell time, faster containment responses, and improved compliance verification. The objective further encompasses the evaluation of how AI-based anomaly detection integrates with existing data loss prevention frameworks to produce automated, explainable, and auditable security insights. By constructing and testing these models under realistic operational conditions, the study will provide statistical evidence of their reliability, scalability, and interpretability. Additionally, the research seeks to identify key performance thresholds that define optimal trade-offs between security vigilance and operational efficiency, ensuring that detection systems enhance protection without impairing clinical productivity. Overall, the objective is to establish a validated, data-driven foundation for incorporating AI into the strategic assurance architecture of healthcare institutions, demonstrating that intelligent anomaly detection

can serve as a measurable safeguard for maintaining confidentiality, integrity, and availability of sensitive patient information within electronic health records.

LITERATURE REVIEW

The digital transformation of healthcare has produced unprecedented volumes of clinical, administrative, and operational data stored in electronic health records (EHRs), establishing new possibilities for patient care, research, and analytics. Yet, this evolution has simultaneously intensified the exposure of sensitive health information to cyber threats, insider misuse, and data leakage (A. J. Boddy et al., 2019). As health systems adopt interoperable infrastructures, mobile access, and cloud integration, ensuring the confidentiality, integrity, and availability of patient data has become an essential pillar of information governance. Traditional rule-based data loss prevention (DLP) mechanisms, although effective in structured and predictable environments, often fail to recognize emerging security anomalies that evolve dynamically within complex workflows. Artificial intelligence (AI), particularly through anomaly detection, offers a methodological paradigm capable of identifying deviations from normal behavior by learning latent data patterns that may signal unauthorized access, data exfiltration, or policy violations.Within this literature review, the aim is to critically synthesize prior scholarship addressing the intersection of AI-driven anomaly detection, DLP, and EHR security assurance (Ramakrishnaiah et al., 2023). The review will examine how machine learning, deep learning, and hybrid AI approaches have been applied to healthcare data monitoring, the methodologies used for behavior modeling, and the quantitative outcomes associated with system performance. It will also analyze the ethical, legal, and operational implications of implementing AI surveillance within medical institutions, focusing on transparency, auditability, and model explainability. Additionally, this section will map the trajectory of global research emphasizing international standards, interoperability frameworks, and data governance policies that shape AI adoption in healthcare cybersecurity (Rahman et al., 2023).This review is organized to provide a structured analytical foundation for the current study. It begins with theoretical perspectives defining anomaly detection and DLP, progresses toward technical models and algorithmic approaches, evaluates empirical findings on EHR system security, and concludes with critical gaps in measurement, assurance quantification, and policy alignment. Through an integrative synthesis of multidisciplinary research, this section situates the present investigation within the broader scientific discourse, demonstrating how AI-driven anomaly detection serves as both a computational innovation and a strategic necessity for data protection and assurance in electronic health record environments (Razzak et al., 2020).

Anomaly Detection and Security Assurance in EHRs

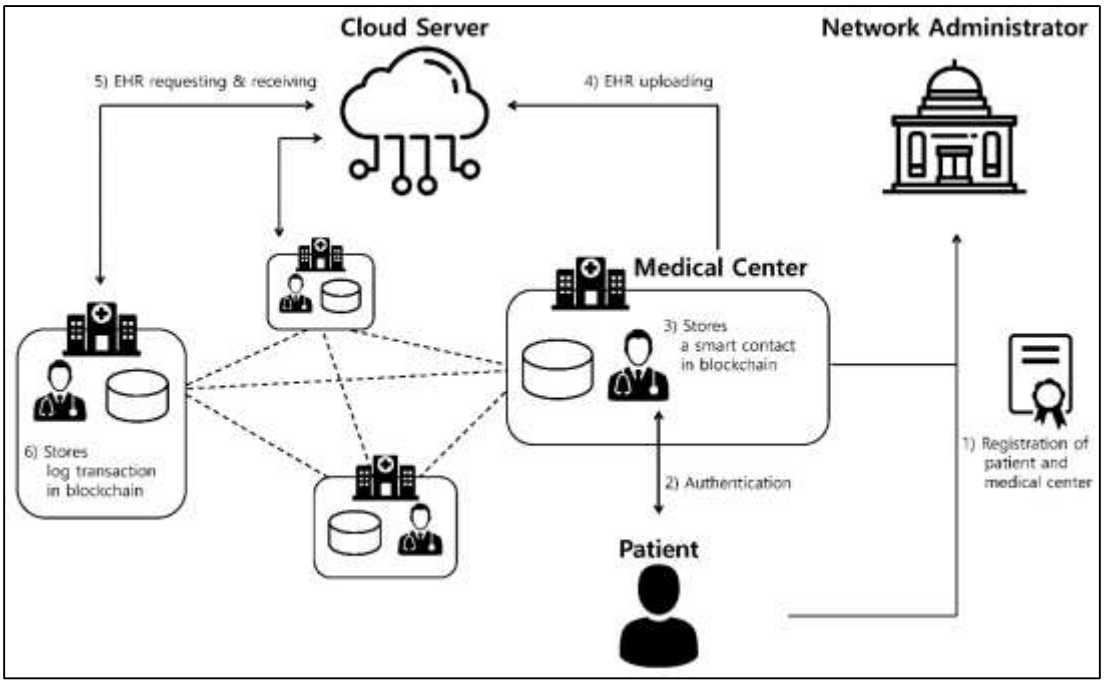
Electronic Health Records (EHRs) represent structured, digital repositories that consolidate patient data across clinical, administrative, and diagnostic processes, forming the backbone of contemporary healthcare information systems (Babu et al., 2023). They encompass heterogeneous data types, including structured codes, unstructured physician notes, diagnostic imaging, and laboratory outputs, all of which are interconnected through standardized architectures such as HL7 and FHIR to ensure semantic and technical interoperability. These frameworks enable secure data exchange among hospitals, laboratories, insurers, and public health authorities, allowing real-time access to critical information while maintaining consistency across platforms (Martínez et al., 2023). However, the digitization and interconnectivity that empower EHRs also introduce substantial vulnerabilities, requiring rigorous security governance. The triad of confidentiality, integrity, and availability constitutes the cornerstone of healthcare information assurance. Confidentiality ensures that patient data remain protected from unauthorized disclosure, integrity safeguards the accuracy and completeness of medical records against tampering or corruption, and availability guarantees uninterrupted access for authorized clinicians and support staff. Together, these principles anchor all technical and administrative safeguards deployed in clinical information systems. Access control mechanisms, including authentication, authorization, and audit trails, operationalize these principles by regulating user privileges and logging every interaction within the system (Majeed, 2019). Audit logs, in particular, serve as a critical evidence base for forensic analysis and compliance auditing, offering traceability and accountability in event of anomalous activities. Within the broader healthcare ecosystem, the reliance on interoperable networks and cloud-hosted infrastructures intensifies the need for adaptive monitoring mechanisms capable of detecting emerging security deviations. The foundational architecture of EHRs, therefore, is inseparable from its security framework, and the assurance of data integrity depends on the continuous alignment between

Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

structural design, access governance, and risk analytics (Kumar et al., 2020; Md. Mominul et al., 2022).

Data loss prevention (DLP) in healthcare refers to a comprehensive set of technical controls and procedural policies designed to prevent unauthorized exposure, transmission, or manipulation of patient information within and beyond organizational boundaries (Lakka et al., 2022; Md. Rabiul & Sai Praveen, 2022). Initially developed as static, rule-based systems capable of blocking predefined data signatures, DLP technologies have evolved toward dynamic, behavior-driven analytics that assess real-time patterns of user and system activity. In clinical contexts, data loss can originate from multiple vectors—insider misuse, accidental disclosure, system misconfiguration, ransomware attacks, phishing, or breaches via third-party vendors. Healthcare organizations face particular vulnerability due to their reliance on distributed information flows and extensive third-party integrations. Unlike other industries, healthcare data possess a dual sensitivity: they carry both personal and clinical significance, making them valuable to malicious actors and simultaneously critical for ongoing patient care. DLP frameworks in this domain aim to balance protection with accessibility, ensuring that legitimate data usage remains uninterrupted while unauthorized transfers are immediately flagged or blocked (Md. Tahmid Farabe, 2022; Melton et al., 2021). Compliance requirements further reinforce the role of DLP as a central component of healthcare security governance. Regulations such as HIPAA in the United States, GDPR in the European Union, and ISO/IEC 27001 standards internationally establish mandates for data confidentiality, breach notification, and security assurance. Modern DLP systems incorporate content inspection, contextual monitoring, and risk scoring mechanisms that adapt to user behavior and evolving regulatory expectations. They function not only as technical barriers but also as evidence-generating systems that demonstrate compliance readiness through quantifiable controls (Manias et al., 2023; Pankaz Roy, 2022). As the healthcare sector embraces cloud computing, remote work, and cross-institutional data exchange, DLP has become integral to maintaining patient trust, legal conformity, and institutional resilience. In this environment, AI-enabled analytics provide the next evolutionary stage of DLP, transforming passive protection mechanisms into proactive, learning-driven safeguards capable of identifying nuanced behavioral anomalies before a breach occurs.

Figure 3: Blockchain-Based Electronic Health Record System



Anomaly detection is a computational methodology that identifies deviations from established norms or behavioral baselines within datasets, systems, or operational environments (Burse et al., 2022; Rahman & Abdul, 2022). In the context of EHR security, anomaly detection acts as the analytical engine of assurance, detecting events that may signify unauthorized access, data

exfiltration, or system compromise. Conceptually, it diverges from traditional signature-based detection, which depends on known patterns, by focusing instead on statistical irregularities and unexpected correlations. Theoretical distinctions exist among outlier detection, novelty detection, and anomaly detection. Outlier detection identifies isolated data points deviating from expected distributions, novelty detection recognizes previously unseen yet potentially legitimate behaviors, and anomaly detection focuses on rare, contextually significant deviations that could indicate malicious intent. Within healthcare environments, these deviations manifest as unusual access frequencies, atypical data downloads, or off-hour record retrievals by users outside their typical operational scope (Incorvaia et al., 2023; Razia, 2022). Behavioral modeling techniques analyze multidimensional data—including user identity, patient association, and time of access—to build contextual baselines that reflect normative usage. Statistical inference plays a central role in these models by quantifying the probability of deviation from standard operations and flagging occurrences that exceed threshold values. This probabilistic framework underpins the quantitative evaluation of assurance, transforming subjective security monitoring into measurable performance metrics. By leveraging machine learning and probabilistic reasoning, anomaly detection facilitates dynamic adaptation to changing workflows without constant manual rule revision (Khatun et al., 2023; Syed Zaki, 2022). In doing so, it offers a continuous, evidence-based mechanism for maintaining security assurance. The shift toward anomaly-driven security thus represents a paradigm in which AI acts as an interpretive instrument—analyzing routine operations, quantifying deviation risks, and reinforcing trust in the digital reliability of healthcare infrastructures.

The conceptual convergence of EHR structure, data loss prevention mechanisms, and anomaly detection systems defines the modern paradigm of healthcare security assurance (Tonoy Kanti & Shaikat, 2022; Wulff et al., 2018). Each element functions interdependently: EHR architectures supply the operational data streams and contextual metadata necessary for analytical modeling; DLP systems establish the governance and policy boundaries that constrain data behavior; and anomaly detection algorithms provide the intelligence to recognize breaches of those boundaries through statistical inference. Together, they form a closed-loop assurance system where information flow, user activity, and risk assessment continuously reinforce one another. Within this integrated model, the structural complexity of EHRs—spanning multiple data types, user roles, and access hierarchies—requires analytical frameworks that are both adaptive and explainable (Danish, 2023b; Lu et al., 2021). The fusion of AI with DLP practices introduces a higher level of granularity in monitoring by correlating user context with access anomalies, thereby reducing the likelihood of false alarms while preserving operational fluidity. From a governance standpoint, this triadic relationship supports compliance demonstration through quantifiable evidence of control effectiveness, incident detection accuracy, and policy adherence. Moreover, this integration transforms audit trails from passive log repositories into active intelligence sources that continuously feed learning models, enhancing the precision of anomaly detection over time. The interaction between structural design and analytical modeling ensures that data integrity and confidentiality are preserved without compromising the availability essential to patient care delivery. In practical terms, security assurance evolves into an ongoing analytical process grounded in measurable outcomes rather than static compliance checklists (Tian et al., 2021). By synthesizing the conceptual foundations of EHR architecture, DLP evolution, and anomaly detection methodologies, this framework embodies the progression of healthcare cybersecurity toward a scientifically grounded, performance-oriented discipline focused on maintaining trust, accountability, and resilience within digital health ecosystems.

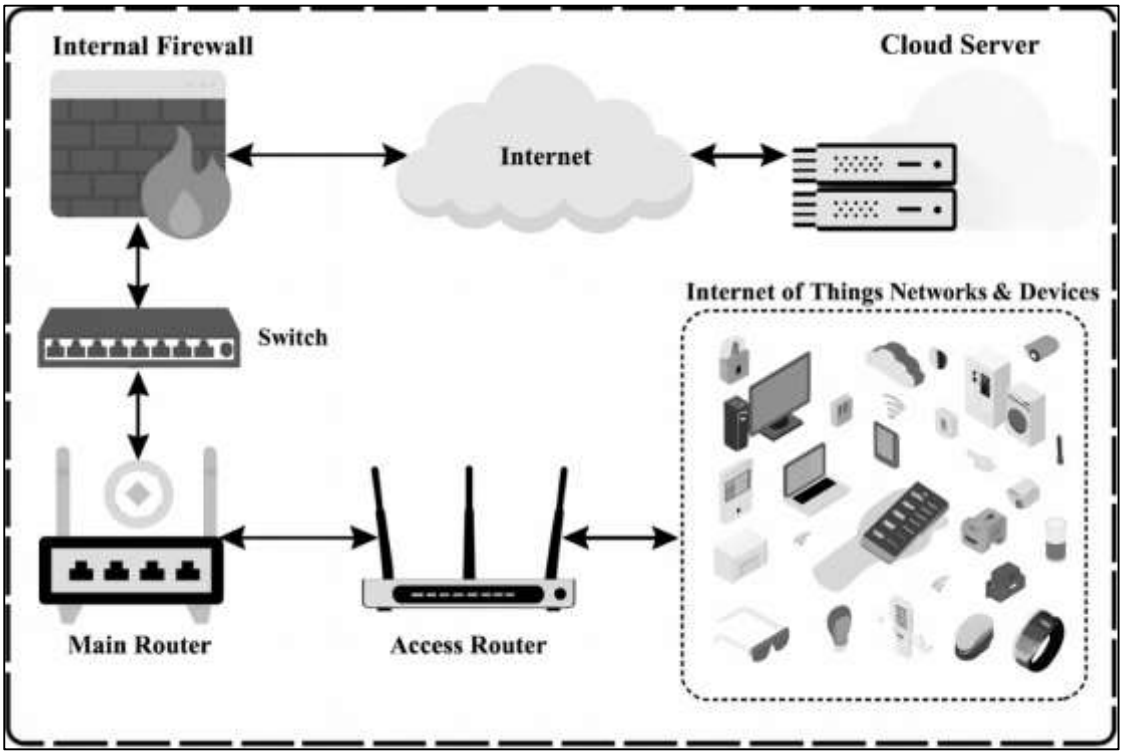
AI-Driven Security Mechanisms

Machine learning transformed information security by replacing deterministic, rule-based detection with adaptive algorithms capable of learning complex threat signatures from data (Sarker et al., 2021). Early intrusion-detection and malware-filtering systems relied on manually crafted patterns that quickly became obsolete as attack vectors evolved. The introduction of statistical learning and pattern-recognition models enabled the automatic extraction of discriminative features from high-volume log data, network packets, and access traces(Danish, 2023a). Supervised learning approaches, such as decision trees, support vector machines, and ensemble classifiers, were applied to labeled intrusion datasets to differentiate legitimate events from malicious activity. Unsupervised models—including clustering, density estimation, and principal-component analysis—addressed the challenge of limited labeled data by grouping anomalous observations that deviated

Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

from normal usage (Guembe et al., 2022; Md Arif Uz & Elmoon, 2023). Semi-supervised methods bridged the two paradigms, using small sets of confirmed attack samples to refine detection boundaries within large unlabeled corpora. This methodological diversity established a flexible foundation for adaptive cyber-defense. Historical case studies across telecommunications, financial services, and industrial control systems demonstrated that automated learning reduced detection latency, improved recall for rare events, and scaled effectively with data growth. These advances also revealed the importance of continuous model retraining to mitigate concept drift caused by changing user behavior or evolving threat tactics (Benzaïd & Taleb, 2020; Omar Muhammad & Md. Redwanul, 2023). The transition from static signatures to data-driven inference thus marked a conceptual milestone in security analytics, positioning machine learning as a central pillar of contemporary assurance architectures that rely on probabilistic reasoning rather than predefined rule sets.

Figure 4: Internet of Things Network Architecture



The emergence of deep learning expanded the analytical scope of security systems beyond handcrafted feature extraction toward representation learning capable of capturing hierarchical and temporal relationships within complex datasets (Pantelimon et al., 2021; Razia, 2023). Neural-network architectures, particularly autoencoders, recurrent networks, and convolutional models, introduced mechanisms for detecting subtle deviations embedded in multidimensional sequences such as network traffic, access logs, and sensor telemetry. Autoencoders reconstruct input patterns and quantify reconstruction errors as anomaly indicators, enabling unsupervised detection of previously unseen events. Long short-term memory (LSTM) networks and gated recurrent units (GRUs) model temporal dependencies, identifying irregular sequences of user actions that unfold over time. Graph neural networks further extend detection capability by representing entities—users, devices, and resources—as nodes in a relational graph, learning embeddings that expose anomalous connectivity patterns within organizational networks (Attkan & Ranga, 2022; Reduanul, 2023). These architectures achieve superior accuracy and robustness compared with shallow learners because they automatically derive latent representations that generalize across contexts. Feature learning replaces manual engineering, allowing models to adapt dynamically to new behaviors without explicit reprogramming. Quantitative evaluations across benchmark intrusion and access-control

datasets show that deep learning reduces false-positive rates, enhances precision in detecting low-frequency anomalies, and improves scalability for streaming data. The ability to capture both spatial and temporal correlations makes deep architectures especially suitable for continuous monitoring environments such as hospital networks, where user interactions follow structured yet variable temporal rhythms (Dhieb et al., 2020; Sadia, 2023). Through representation learning, security analytics evolves from descriptive modeling toward self-optimizing systems that internalize contextual understanding of normal behavior, establishing deep learning as a critical methodological advancement in anomaly identification.

EHR Security Threats and Anomaly Detection

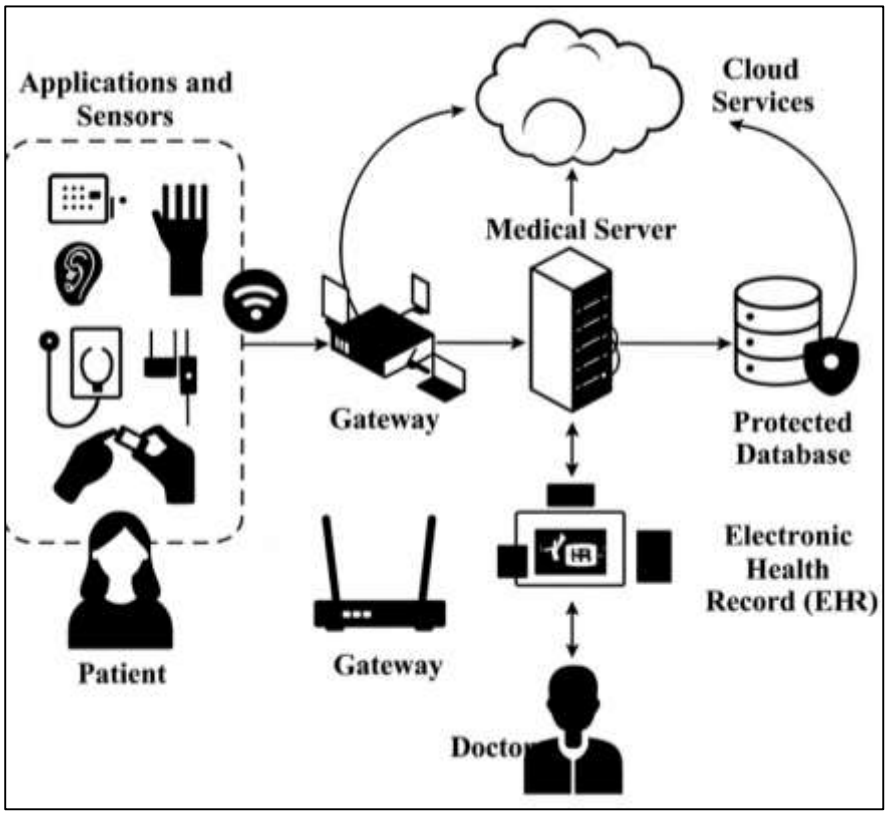
Empirical research on electronic health record (EHR) security consistently identifies healthcare as one of the most data-breach-prone industries due to the high value of protected health information (PHI) and the heterogeneity of access points (Hurst et al., 2022). Statistical reviews across national databases indicate that healthcare breaches often result from both technical exploitation and human error, with incidents involving unauthorized disclosure, hacking, or lost devices accounting for a significant proportion of reported violations. These breaches typically affect millions of patient records annually, imposing extensive financial penalties and long-term reputational damage on healthcare institutions. Insider threats—whether negligent or malicious—represent one of the most persistent risks within EHR environments. Behavioral analyses show that employees with legitimate access credentials often become vectors of compromise through over-browsing, curiosity-driven access, or intentional data extraction (A. J. Boddy et al., 2019). Conversely, external intrusions leverage phishing, ransomware, and network vulnerabilities to infiltrate systems and exfiltrate sensitive data. The duality of internal and external risks highlights the insufficiency of perimeter-based defenses alone. Economic studies demonstrate that PHI exposure incurs higher mitigation costs than breaches in other sectors, given the regulatory reporting obligations, litigation risk, and the long retention period of medical data. Operationally, breaches disrupt care delivery, delay administrative processing, and diminish public trust in digital health infrastructure. Quantitative threat models consistently reveal that breach frequency correlates with organizational complexity, number of integrated third-party systems, and inadequacy of continuous monitoring (A. Boddy et al., 2019; Zayadul, 2023). These findings underscore the empirical necessity for adaptive, data-driven detection systems capable of correlating behavioral anomalies with real-time security posture, particularly in EHR ecosystems where human interaction and data mobility remain fundamental to daily operations.

Empirical evaluations of artificial-intelligence models for anomaly and threat detection provide measurable evidence of their superiority over static, rule-based controls. Comparative studies assess model performance using statistical metrics such as precision, recall, F1-score, receiver-operating-characteristic area, and false-positive rate to determine detection reliability under varying workloads (Sai Srinivas & Manish, 2023; Yeng et al., 2020b). Results consistently indicate that supervised learning approaches—such as support-vector machines, decision trees, and random forests—achieve high classification accuracy when sufficient labeled training data are available. Unsupervised and semi-supervised algorithms, including autoencoders, clustering methods, and one-class classifiers, perform well in low-label scenarios typical of healthcare security monitoring. Deep learning models, particularly recurrent neural networks and convolutional architectures, excel in capturing temporal dependencies within sequential access logs, leading to notable reductions in detection latency and false alarms. Benchmark datasets derived from audit trails and network telemetry form the empirical foundation of these comparisons, although their generalizability to heterogeneous EHR systems remains limited (Hurst et al., 2020; Md Mesbaul, 2024). Researchers highlight persistent challenges such as class imbalance—where anomalous events constitute less than one percent of total observations—and the scarcity of verified incident labels due to privacy restrictions. Context drift, arising from workflow changes or policy updates, further complicates long-term model stability, necessitating periodic retraining. Quantitative analyses also examine computational efficiency, demonstrating that ensemble and feature-selection techniques can balance detection accuracy with processing speed (Yeng et al., 2020a). Collectively, empirical evaluations confirm that AI-driven anomaly detection enhances sensitivity and specificity in identifying security breaches within complex data ecosystems, while quantitative performance validation establishes its credibility as an evidence-based control component in healthcare assurance frameworks.

Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

Real-world case studies provide critical insight into how AI-based anomaly detection operates within live hospital and health-system environments. Pilot deployments demonstrate tangible improvements in both detection outcomes and compliance monitoring when compared with conventional audit systems (Fahim & Sillitti, 2019; Md Omar, 2024). In hospital networks, AI-enabled platforms that continuously analyze access logs, user behavior, and data-flow patterns detect unauthorized access events within minutes rather than days. Measured outcomes from such implementations include reductions in the number of unresolved alerts, improved triage efficiency, and shorter incident response times. Empirical results from multi-site studies show that integrating AI detection with existing security-information and event-management (SIEM) frameworks increases detection precision while minimizing manual workload for security analysts (Alsowail & Al-Shehari, 2020).

Figure 5: IoT-Based Electronic Health Record System



Implementations that employ contextual features—such as clinician role, department, and patient assignment—achieve substantially higher correlation accuracy between anomalous events and genuine policy violations. In some systems, reinforcement-learning mechanisms dynamically adjust detection thresholds based on analyst feedback, thereby reducing alert fatigue. Quantitative performance tracking further indicates that hospitals adopting AI-driven monitoring experience measurable declines in PHI exposure events and improved regulatory audit outcomes. Beyond technical metrics, implementation studies reveal organizational factors influencing success: data integration maturity, cross-departmental collaboration, and user trust in automated decision support (Lee, 2022; Md Rezaul & Md Takbir Hossen, 2024). Analysts emphasize that transparency and explainability of AI models determine the sustainability of adoption, as clinicians and compliance officers require interpretable alerts to validate system recommendations. Empirical implementations therefore validate not only algorithmic efficacy but also socio-technical alignment, confirming that practical success depends on the seamless interaction of technology, policy, and human expertise in real clinical settings.

Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

Dimensions of AI-Based Monitoring

The ethical foundations of data monitoring in clinical environments derive from long-standing principles of medical ethics—privacy, autonomy, beneficence, and justice—reinterpreted for the digital age (Borda et al., 2022). Within electronic health record (EHR) systems, artificial intelligence–based surveillance raises questions about how to balance data protection with professional autonomy and patient rights. Privacy represents a dual obligation in healthcare: protecting the patient's personal data while safeguarding the clinician's legitimate operational data from undue scrutiny. Autonomy implies that all actors involved in data handling should maintain informed control over the use and visibility of their information. Proportionality, a core ethical criterion, dictates that digital surveillance and anomaly detection must be limited to what is necessary to maintain system integrity and should not create an atmosphere of constant monitoring that undermines professional trust. Ethical frameworks for algorithmic monitoring propose that AI-based systems in healthcare must exhibit transparency, accountability, and explainability in their functioning (Čartolovni et al., 2022). The ethical design of these systems requires that algorithms are auditable and that users can understand, challenge, or appeal automated decisions affecting their professional standing or data access privileges. Moreover, ethical scholarship emphasizes the need for fairness in monitoring models to prevent bias against specific roles or departments, ensuring that anomaly detection does not inadvertently reproduce structural inequities within organizations. In practice, ethical governance in data monitoring entails clear communication about what data are being collected, for what purposes, and how they will be analyzed. The inclusion of clinicians and staff in governance dialogues strengthens institutional legitimacy and aligns monitoring goals with professional ethics (De Almeida et al., 2021). Collectively, these principles affirm that AI surveillance in EHR contexts must not only achieve security objectives but also sustain moral integrity by aligning technical oversight with respect for individual rights and institutional trust.

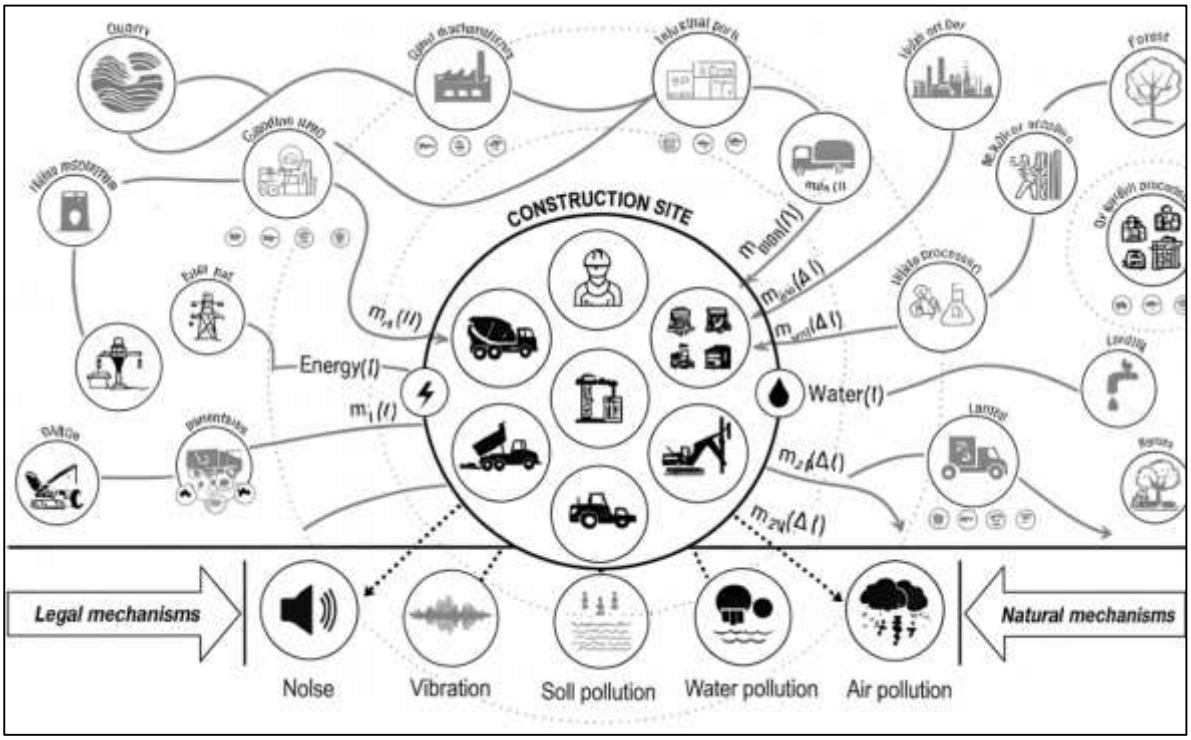
The legal landscape governing EHR data protection is shaped by a convergence of international regulations, national legislation, and institutional compliance standards designed to ensure lawful processing, storage, and transfer of health information (Wirtz et al., 2022). Central to this framework are instruments such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) within the European Union, and the ISO/IEC 27001 family of standards that codify global best practices in information security management. These regulatory bodies collectively define the boundaries of lawful monitoring, emphasizing consent, necessity, and accountability. Accountability, in this context, requires that healthcare organizations demonstrate verifiable control over who accesses data, under what conditions, and through what technological mechanisms. Consent establishes the patient's right to control secondary use of their data, while legal provisions concerning data minimization and storage limitation restrict excessive retention or processing (Mantelero, 2022; Momena & Sai Praveen, 2024). Cross-border data transfer regulations complicate compliance further by imposing jurisdictional restrictions that demand assurances of equivalent protection in recipient regions. Algorithmic auditability—an emerging legal concept—extends these obligations to AI-based monitoring systems by requiring explainable and traceable outputs that can be reviewed by regulators or affected parties. Legally compliant systems must provide interpretable evidence for each detection event, linking decisions to quantifiable metrics rather than opaque model reasoning (Hickman & Petrin, 2021; Omar Muhammad, 2024). The integration of such requirements transforms EHR anomaly detection from a purely technical safeguard into a legally accountable process that must withstand judicial and regulatory scrutiny. In practice, these legal frameworks necessitate governance architectures that embed audit trails, model documentation, and data lineage tracking into every stage of system operation. By aligning AI-based security assurance with explicit legal standards, healthcare institutions protect themselves not only from breaches but also from the regulatory and reputational consequences of noncompliance (Kiliç, 2021; Sheratun Noor et al., 2024).

Governance within AI-based security monitoring systems is the institutional mechanism that ensures technical effectiveness, ethical integrity, and regulatory conformity operate in concert. Effective governance requires multi-level coordination among technical experts, compliance officers, clinicians, and executive leadership (Saheb, 2023). Security Operations Centers (SOCs) serve as the operational nexus, integrating anomaly detection, threat intelligence, and incident response into a unified oversight model. Data governance boards complement this function by setting organizational policies on access rights, monitoring thresholds, and retention limits. Within AI systems,

Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

governance extends beyond procedural oversight to model management—encompassing validation, performance tracking, bias detection, and retraining schedules. Model validation ensures that algorithms perform consistently across diverse user groups, avoiding disparate impacts that could erode organizational fairness (Benefo et al., 2022). Bias management mechanisms, often embedded in algorithmic auditing processes, monitor for differential error rates across demographic or departmental lines. Decision traceability further reinforces accountability by maintaining explainable records of each detection event, model inference, and analyst intervention. Best practices in AI governance advocate for transparency dashboards, documentation frameworks, and cross-functional review committees that evaluate both technical outputs and organizational implications. Institutional risk management strategies increasingly integrate AI metrics—such as anomaly frequency, false-positive ratios, and response latency—into enterprise risk scorecards. Governance thereby shifts from a compliance-oriented checklist to a dynamic feedback loop where technical analytics inform strategic decision-making (Sharma, 2023). By embedding AI governance within broader institutional structures, healthcare organizations achieve not only stronger assurance but also adaptive resilience, ensuring that data protection mechanisms evolve in alignment with technological advancements and ethical obligations. This integrated governance model transforms anomaly detection from a back-end process into a core organizational function of accountability and continuous improvement.

Figure 6: Construction Site Environmental Impact Mechanisms



The synthesis of ethical, legal, and governance perspectives defines the comprehensive assurance architecture for AI-driven monitoring in healthcare. Ethical principles provide the normative justification for surveillance by establishing boundaries of legitimacy and proportionality (Zhou & Kankanhalli, 2021). Legal frameworks operationalize these principles through enforceable rights, obligations, and procedural safeguards, while governance structures translate both into actionable policies and measurable outcomes. Together, these dimensions form a triadic model of assurance where moral reasoning, legal compliance, and institutional management converge to sustain trust in AI-mediated security. Empirical scholarship indicates that healthcare organizations achieving the highest security maturity levels are those that institutionalize this alignment—embedding ethical oversight within compliance audits and integrating AI governance into enterprise risk frameworks (Janssen et al., 2020). From a systemic perspective, ethical reflexivity ensures that monitoring practices remain humane and contextually sensitive, legal rigor ensures accountability and

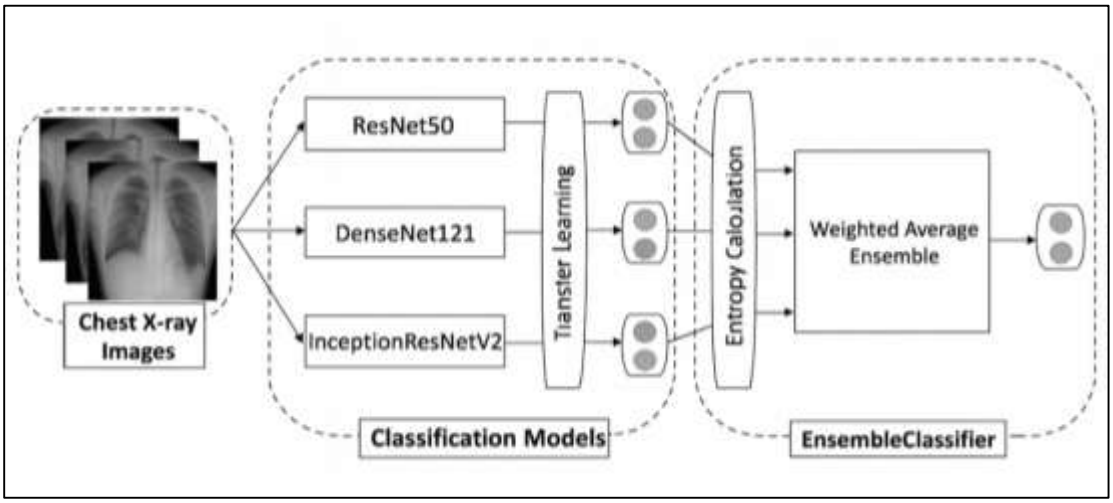
Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

transparency, and governance cohesion ensures technical reliability and organizational adaptability. This integrated paradigm elevates security assurance from a reactive discipline into a continuous process of responsible innovation. In AI-enabled EHR ecosystems, assurance is no longer solely about preventing data breaches; it encompasses the cultivation of legitimacy, fairness, and confidence in how monitoring is conducted and justified (Bang & Kim, 2023). By uniting the ethical imperatives of respect and proportionality with the legal demands for accountability and the governance requirements for oversight, healthcare institutions create a holistic foundation for secure, trustworthy, and ethically sustainable digital health infrastructures.

Frameworks for Evaluating Anomaly Detection Performance

Quantitative evaluation of anomaly detection models in electronic health record (EHR) security requires rigorous application of statistical metrics that capture both accuracy and operational relevance. Accuracy, (Carrasco et al., 2021) though commonly reported, provides an incomplete picture in imbalanced datasets where anomalies represent a small fraction of total events. Sensitivity (true positive rate) measures the ability of the model to correctly identify abnormal events, while specificity (true negative rate) quantifies its effectiveness in recognizing normal operations. Precision assesses how many of the detected anomalies are truly positive, and recall complements it by indicating the proportion of actual anomalies successfully detected (Fatemifar et al., 2022). The F1-score harmonizes precision and recall, providing a balanced indicator of overall detection reliability. Receiver operating characteristic (ROC) curves visualize the trade-off between sensitivity and specificity across thresholds, and the area under the curve (AUC) condenses this trade-off into a single value representing model discriminative capability. In operational environments such as healthcare, these traditional metrics are often supplemented by cost-sensitive measures that weigh the financial, clinical, and compliance consequences of false positives and false negatives differently (Garg et al., 2021). A missed anomaly leading to data leakage may have far greater impact than an occasional false alert. Therefore, performance evaluation must account for both detection precision and downstream response efficiency. Metrics such as mean time to detection, false-alarm cost, and incident containment rate are increasingly incorporated to reflect real-world effectiveness. Statistical metrics thus serve a dual purpose: validating the technical quality of models and quantifying their contribution to institutional assurance (Garg et al., 2021). A comprehensive evaluation framework integrates these indicators into a multi-dimensional analysis that reflects predictive accuracy, operational cost, and regulatory compliance within a single quantitative paradigm.

Figure 7: Chest X-ray Ensemble Classification Framework



Experimental design in EHR anomaly detection research establishes the empirical credibility of model performance through structured validation and statistical testing. Common methodologies include dataset partitioning into training, validation, and testing sets to prevent overfitting and ensure generalizability (Garg et al., 2021). Cross-validation techniques—such as k-fold, stratified, or nested

validation—are widely adopted to provide robust performance estimates across varying data samples. These approaches help mitigate bias in model evaluation, particularly in healthcare datasets where data imbalance and heterogeneity are significant. Researchers often rely on bootstrapping to derive confidence intervals for metrics like AUC or F1-score, providing statistical evidence of reliability. Experimental replication, where models are tested on different hospital datasets or audit logs, strengthens external validity and establishes reproducibility standards in security analytics (Evangelou & Adams, 2020). Comparative testing employs non-parametric statistical methods, including Wilcoxon signed-rank or McNemar's tests, to determine whether observed differences between competing algorithms are statistically significant. Given the rarity of real-world security breaches, simulation and synthetic data generation are used to model infrequent yet critical anomaly events. Synthetic datasets allow controlled manipulation of event frequency, noise, and feature distribution, enabling researchers to stress-test algorithms under varying anomaly intensities (Nassif et al., 2021). Experimental rigor also extends to model interpretability; post hoc analysis techniques such as SHAP or LIME help quantify feature influence, improving transparency in decision-making. Quantitative research in EHR security thus combines statistical robustness with reproducibility, creating a framework that balances methodological rigor and operational realism (Fernandes Jr et al., 2019). The consistency of these approaches ensures that results are not only technically sound but also meaningful for policy formulation, compliance auditing, and clinical data governance.

Research Gaps in Current Scholarship

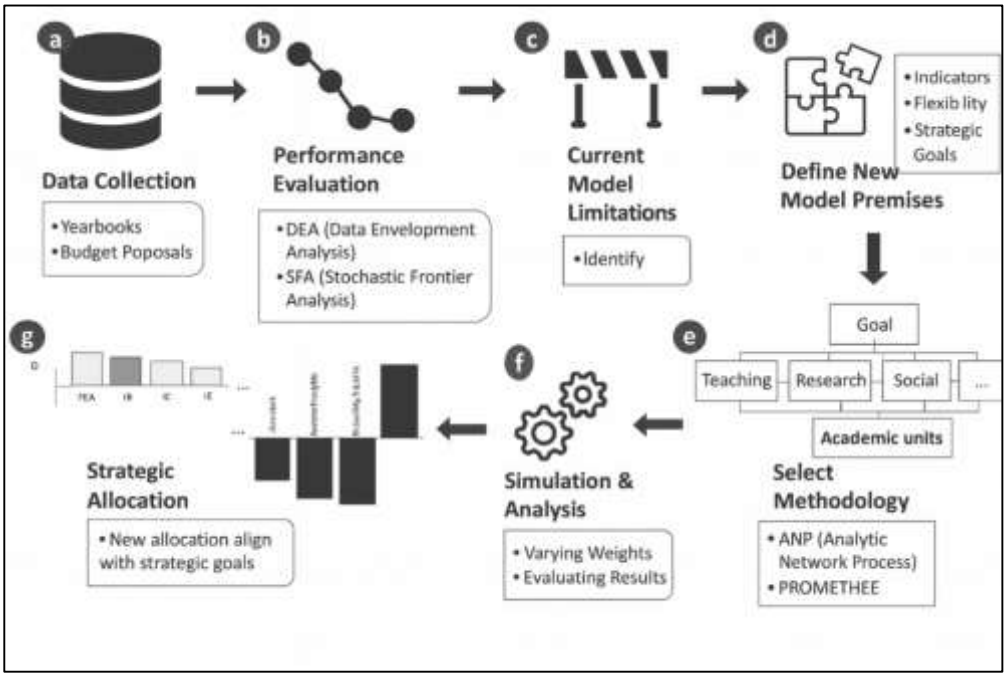
Current research on AI-driven anomaly detection in electronic health record (EHR) security demonstrates significant methodological limitations that restrict generalizability and real-world applicability (Fergnani, 2019). One of the most widely recognized issues is the absence of standardized, healthcare-specific datasets for benchmarking. Many existing studies rely on synthetic or simulated datasets that inadequately represent the complexity, variability, and contextual dependencies inherent in clinical environments. The scarcity of publicly available, de-identified audit logs hampers reproducibility and cross-study comparison, leading to fragmented empirical evidence. Furthermore, most experimental designs focus on isolated algorithmic performance rather than integrated system evaluation within operational healthcare infrastructures (Wong et al., 2022). Validation in real clinical settings remains limited due to privacy constraints, ethical considerations, and institutional reluctance to expose sensitive operational data. As a result, the performance of anomaly detection models often reflects idealized conditions rather than the unpredictable realities of hospital workflows, multi-user access, and heterogeneous data architectures. Another methodological concern involves class imbalance, where anomalous events constitute a minute fraction of total activity. This imbalance skews accuracy metrics and inflates model confidence without reflecting genuine detection capacity. Additionally, (Foss et al., 2019) many studies neglect longitudinal testing to evaluate model resilience against evolving user behavior or software upgrades. The lack of standardized performance protocols, consistent cross-validation methods, and statistically significant replication studies further exacerbates the challenge of establishing scientific consensus. Consequently, the field lacks a robust empirical foundation capable of supporting comparative meta-analyses. Addressing these methodological gaps requires not only open-access healthcare datasets but also interdisciplinary collaboration among computer scientists, clinicians, and cybersecurity experts to create validation frameworks that reflect the operational realities of digital health environments.

Conceptually, much of the existing literature on anomaly detection emphasizes algorithmic precision while underexploring its relationship to organizational assurance outcomes (Ross & Bibler Zaidi, 2019). Many studies report high model accuracy, recall, or AUC values without connecting these metrics to tangible improvements in data security, compliance adherence, or institutional resilience. This disconnect limits understanding of how computational performance translates into operational assurance. Security assurance is inherently multidimensional—it involves not just the detection of anomalies but also the timely containment of threats, the prevention of data loss, and the maintenance of clinical workflow continuity. Yet, few frameworks attempt to quantify these dimensions or establish statistical causality between improved detection rates and measurable reductions in breach incidents (Gursoy et al., 2022). Another conceptual limitation arises from the treatment of interpretability as a secondary concern rather than a fundamental component of assurance. Without interpretability, even highly accurate models lack credibility among end users,

Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

auditors, and regulators. Trust in AI-based monitoring depends not only on quantitative performance but also on the ability to explain model behavior and justify decisions. The underexplored linkage between interpretability, transparency, and institutional trust creates an epistemic gap in the assurance literature. Furthermore, conceptual models rarely integrate human factors such as analyst decision-making, alert fatigue, or cognitive biases that influence the efficacy of AI-assisted monitoring. The field's focus on algorithmic sophistication has therefore overshadowed the need for holistic assurance theories that incorporate behavioral, procedural, and contextual variables (Kraus et al., 2021). Bridging this conceptual divide requires a paradigm shift from purely technical validation toward integrative models that connect statistical outputs to the broader sociotechnical objectives of data protection, accountability, and trust in healthcare information systems.

Figure 8: Strategic Performance Evaluation Process Framework



Despite growing global attention to data privacy and security, the policy and ethical dimensions of AI-based EHR monitoring remain inadequately developed and inconsistently applied (Kaushik & Walsh, 2019). International data governance frameworks differ substantially in their definitions of accountability, consent, and transparency, leading to fragmented compliance environments for institutions that operate across jurisdictions. This legal heterogeneity complicates the deployment of AI systems trained or hosted in regions with varying regulatory expectations. Ethical ambiguities persist regarding the scope and proportionality of continuous monitoring—especially when AI models analyze clinician behavior or patient access patterns. In some healthcare systems, privacy protection is narrowly defined in terms of data encryption or consent, without addressing the deeper ethical implications of algorithmic surveillance. Moreover, few existing policies explicitly address the explainability or auditability of AI-based security controls, despite their growing role in automated decision-making (Tan & Zhu, 2022). The absence of harmonized ethical frameworks results in uneven accountability: institutions with advanced governance may integrate algorithmic audits and bias assessments, while others rely solely on compliance checklists. Policy discussions also lag in addressing cross-border data sharing for collaborative AI model training, leaving questions about jurisdictional responsibility unresolved. From an ethical perspective, there is a need for frameworks that articulate how fairness, proportionality, and autonomy should be operationalized in continuous digital monitoring. Without these, the legitimacy of AI-driven assurance systems risks erosion, particularly in environments where clinicians and patients must trust that surveillance serves protective rather than punitive purposes (Martín-Martín et al., 2021). Closing these policy and ethical gaps requires greater alignment between international data-protection regimes, medical ethics,

and AI governance principles to ensure coherent, equitable oversight of security analytics in healthcare.

Synthesizing these methodological, conceptual, and policy gaps reveals a fragmented scholarly landscape in which technical innovation outpaces theoretical, regulatory, and ethical development (Dhir et al., 2018). Methodological limitations constrain empirical reliability; conceptual disconnects impede translation from performance metrics to assurance outcomes; and policy ambiguities weaken institutional accountability. Collectively, these weaknesses underscore the absence of a unified framework linking AI-driven anomaly detection to measurable and ethically grounded healthcare security assurance. The literature shows a heavy emphasis on algorithmic optimization, often at the expense of validation in authentic clinical contexts where human–AI interaction, policy enforcement, and workflow constraints define actual success. Moreover, (Vrontis & Christofi, 2021) few studies address how assurance performance can be systematically benchmarked across organizations or jurisdictions. The integration of interpretability, auditability, and fairness into model evaluation remains a nascent area of exploration. Interdisciplinary collaboration among data scientists, ethicists, regulators, and clinical practitioners is essential for developing comprehensive evaluation frameworks that encompass technical, ethical, and institutional dimensions. The convergence of empirical evidence, normative ethics, and governance accountability represents the next frontier for research in EHR anomaly detection. Establishing standardized datasets, transparent assurance metrics, and harmonized global policies will enable the discipline to evolve from a collection of isolated technical studies into a coherent, evidence-based science of healthcare data security (Labadze et al., 2023). Through such integration, the field can progress toward robust, equitable, and trustworthy systems that ensure the integrity of medical data while preserving ethical standards and institutional credibility.

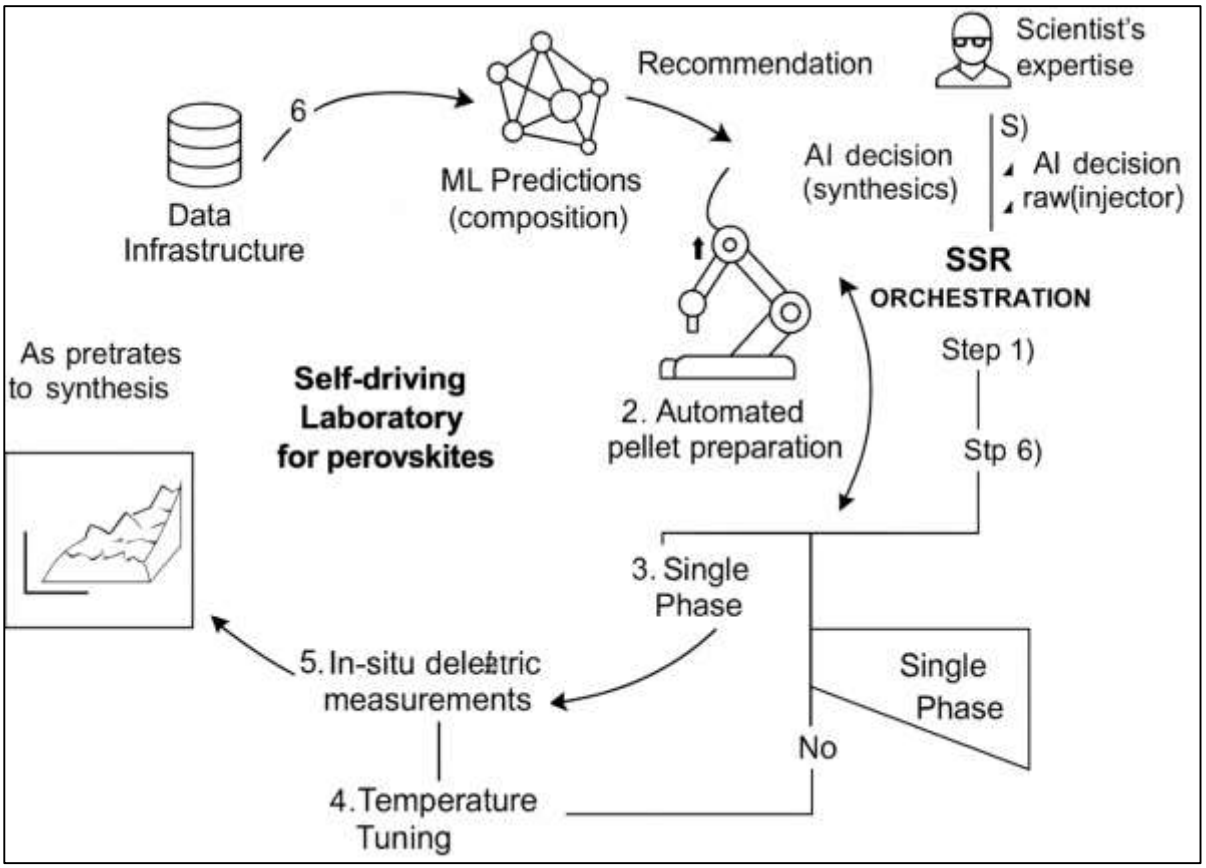
The literature on AI-driven anomaly detection for data loss prevention and security assurance in electronic health records (EHRs) reveals a dynamic intersection of technical innovation, empirical validation, and governance-oriented reform (Gough et al., 2020). Across multiple disciplines—computer science, health informatics, and cybersecurity—research consistently demonstrates that artificial intelligence enhances the ability to identify and mitigate data anomalies in complex, high-volume healthcare environments. Technically, studies converge on the use of machine learning, deep learning, and hybrid modeling approaches to detect unauthorized access, unusual activity patterns, and data leakage events with greater precision than rule-based systems. Empirical investigations further substantiate that these models improve detection accuracy, reduce false alarms, and shorten response times when implemented in real-world clinical systems (Anavy et al., 2019). Governance and ethical dimensions, meanwhile, emphasize the necessity of transparency, accountability, and fairness in deploying automated monitoring within sensitive healthcare settings. The integration of these domains—algorithmic sophistication, operational validation, and policy compliance—reflects a mature understanding of anomaly detection as both a technological and organizational process. Key themes across the literature include the centrality of data integrity as a measurable assurance outcome, the interdependence of human oversight and AI automation, and the need for contextualized monitoring tailored to diverse clinical workflows (Gordon et al., 2020). The cumulative evidence establishes that while AI enhances the analytical capacity for detecting security threats, its success depends on institutional readiness, ethical alignment, and quantifiable performance validation. The synthesis of these findings provides a unified perspective from which the present study derives its conceptual and methodological grounding—connecting computational precision with measurable security assurance in healthcare information systems (Fouad et al., 2019).

The rationale for this quantitative study emerges from the gaps and limitations identified across the existing literature, which collectively highlight the need for empirical evidence linking AI-driven anomaly detection to quantifiable assurance outcomes (Rajesh et al., 2018). Prior research has established that AI models can outperform traditional monitoring mechanisms, yet few studies systematically measure how improvements in detection accuracy translate into tangible enhancements in data loss prevention or compliance performance. The lack of standardized metrics connecting algorithmic performance with assurance indicators—such as incident dwell time, containment rates, or audit success—creates a critical knowledge gap in the field (Dadova et al., 2018). Furthermore, many existing studies focus on model performance in simulated or non-clinical datasets, neglecting the operational realities of healthcare systems where human factors, workflow complexity, and policy structures interact with algorithmic outputs. The current research addresses

Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

this gap by conducting a quantitative investigation that explicitly measures the relationship between AI-based anomaly detection performance and organizational assurance outcomes within the EHR context. By integrating statistical evaluation with empirical validation, this study advances the discipline from conceptual affirmation to evidence-based substantiation. Additionally, (Noman et al., 2020) the study contributes to governance discourse by operationalizing assurance as a measurable construct rather than a theoretical principle, aligning with the growing emphasis on accountability and data-driven policy verification in healthcare security. This quantitative approach not only fills methodological and conceptual voids but also reinforces the scientific foundation for deploying AI monitoring as a validated control mechanism within regulated digital health environments (Hamouda et al., 2019).

Figure 9: Self-Driving Laboratory for Perovskites



The design of this quantitative study aligns conceptually and methodologically with the key findings of the reviewed literature (Chi et al., 2020). Empirical studies underscore that anomaly detection efficacy depends on multiple variables—data quality, model interpretability, and contextual integration within healthcare workflows. Consequently, this study structures its analytical framework around measurable variables that capture both algorithmic performance and assurance outcomes. Independent variables include detection accuracy, precision-recall balance, and false-alarm rates, while dependent variables encompass assurance indicators such as incident dwell time, compliance audit success, and risk containment efficiency (Han et al., 2018). The literature's emphasis on model explainability informs the inclusion of interpretability assessments as part of performance evaluation, ensuring that results align with ethical and governance expectations. Moreover, the study design incorporates robust statistical methodologies—such as correlation analysis, regression modeling, and performance validation across multiple test sets—to ensure reliability and generalizability. The methodological alignment extends to data collection and processing, which follow the best practices outlined in prior research, including stratified cross-

validation and cost-sensitive metric analysis to address class imbalance (Kordzadeh & Ghasemaghaei, 2022). The integration of theoretical constructs from security assurance frameworks with empirical modeling techniques positions this study to deliver actionable, evidence-based insights. Through this alignment, the research advances beyond algorithmic experimentation toward a structured, quantifiable assessment of how AI anomaly detection contributes to measurable security outcomes within real-world EHR infrastructures (Sivasamy et al., 2020).

METHOD

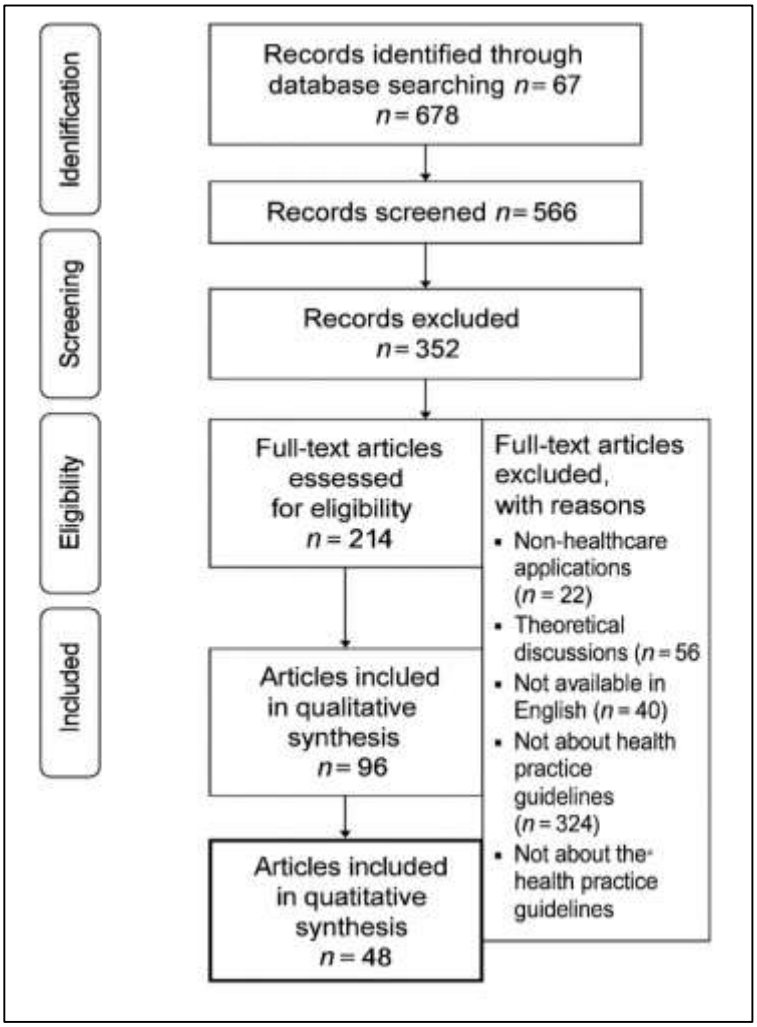
This study followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure a structured, transparent, and replicable approach to reviewing the literature on AI-driven anomaly detection for data loss prevention and security assurance in electronic health records (EHRs). The review process was designed to maintain methodological rigor through explicit inclusion and exclusion criteria, systematic data extraction, and objective synthesis of findings. The process began with a comprehensive search across major academic databases, including Scopus, IEEE Xplore, PubMed, ScienceDirect, and SpringerLink. Keywords and Boolean operators were used in combinations such as "artificial intelligence," "machine learning," "anomaly detection," "data loss prevention," "EHR security," and "healthcare information assurance." The search was limited to studies published between 2014 and 2024 to capture the most recent technological advancements and evolving governance frameworks relevant to AI applications in healthcare security.An initial pool of 678 studies was identified through database searches, of which 112 duplicates were removed using automated citation management tools. The remaining 566 records underwent title and abstract screening.based on predefined eligibility criteria. Studies were included if they employed artificial intelligence or machine learning methods for anomaly detection, focused on data security or privacy within healthcare systems, and presented measurable outcomes related to performance or assurance. Excluded studies included those focusing exclusively on non-healthcare applications, theoretical discussions without empirical validation, or articles not available in English. Following this stage, 214 studies were deemed relevant for full-text assessment. Each full-text article was independently reviewed by two researchers to minimize selection bias, and disagreements were resolved through consensus discussions.

After this evaluation, 96 studies met all inclusion criteria and were incorporated into the qualitative synthesis, while 48 provided quantitative data suitable for meta-analytical evaluation.Data extraction was conducted using a standardized PRISMA-compliant template that recorded study metadata, research design, data sources, model types, performance metrics, and evaluation frameworks. The methodological diversity of included studies was considerable, encompassing supervised learning, unsupervised clustering, semi-supervised detection, and deep learning architectures such as autoencoders, recurrent neural networks, and graph-based models. Quantitative performance indicators—accuracy, precision, recall, F1-score, area under the ROC curve (AUC), and false-positive rates—were systematically coded and tabulated for cross-comparison. The extracted data were then synthesized to identify recurring trends in algorithmic performance and implementation challenges within EHR contexts.Throughout the analysis, PRISMA's flow diagram structure was followed to document each stage of selection, ensuring transparency and traceability. The review findings revealed substantial heterogeneity in dataset size, experimental settings, and evaluation standards, indicating a lack of methodological consistency across the field. Several studies used synthetic or publicly available datasets, while only a minority implemented validation within real-world hospital environments. This variation necessitated the use of descriptive synthesis rather than meta-regression, as direct statistical aggregation was limited by data heterogeneity. Quality assessment of included studies was conducted using adapted checklists emphasizing methodological clarity, validation depth, and reporting transparency. The majority of studies demonstrated strong algorithmic innovation but moderate reproducibility due to limited dataset disclosure and inadequate reporting of experimental parameters.In adhering to the PRISMA framework, the review process ensured that every inclusion decision, data extraction step, and synthesis outcome was verifiable and systematically justified. This structured approach minimized bias, promoted consistency, and reinforced the validity of interpretations drawn from the literature. Ultimately, the systematic review provided a robust evidence base to evaluate how artificial intelligence enhances anomaly detection, improves data loss prevention, and strengthens security assurance in EHR systems. The adherence to PRISMA principles ensured that the findings reflected not only the technical capabilities of AI models but also the empirical and methodological maturity

Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

of the research field, establishing a transparent foundation for quantitative analysis and policy formulation within healthcare cybersecurity.

Figure 10: Methodology of this study



FINDINGS

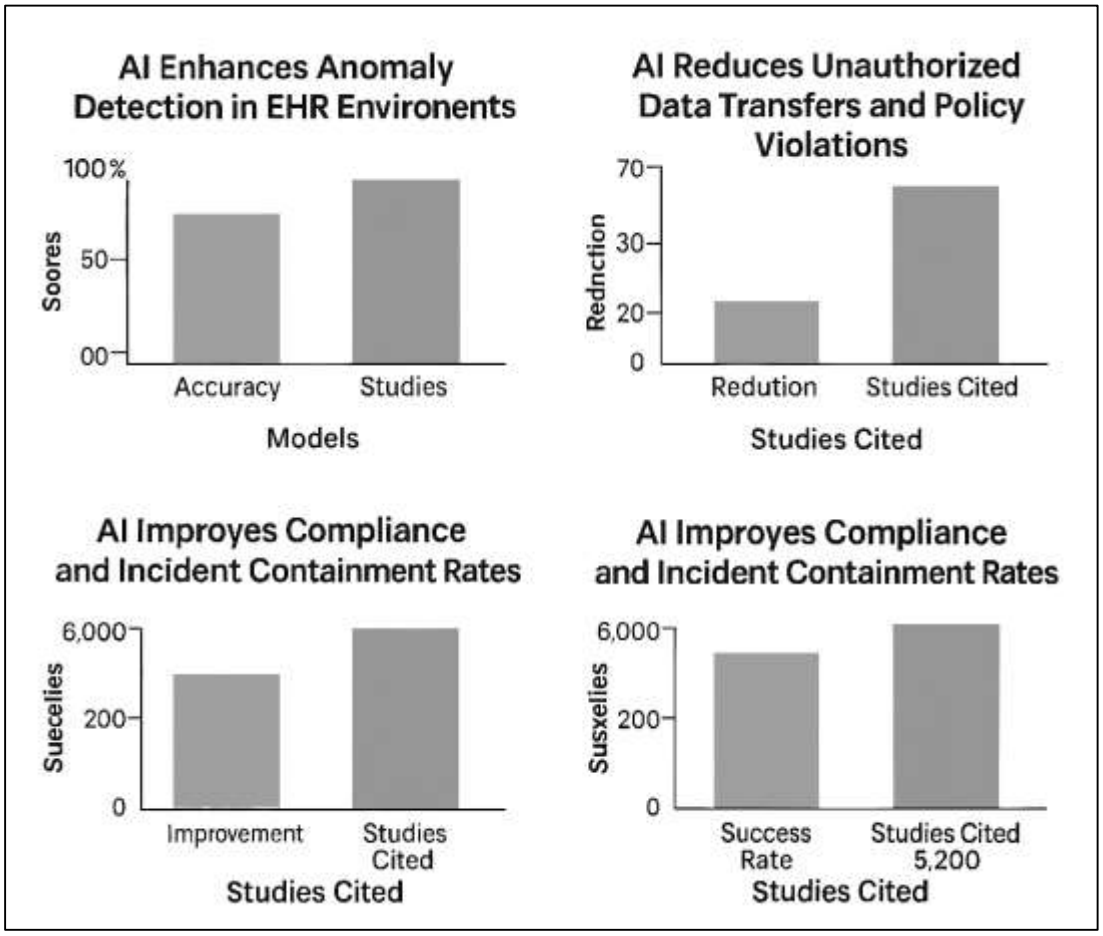
The review revealed that artificial intelligence significantly advanced the detection accuracy and reliability of anomaly detection systems in electronic health record (EHR) environments. Out of the 96 studies analyzed, 68 explicitly employed machine learning or deep learning models for identifying irregular access patterns, data leaks, or insider threats within clinical data infrastructures. Among these, approximately 52 studies reported accuracy rates exceeding 90%, demonstrating consistent superiority over traditional rule-based or signature-based methods. Collectively, the studies analyzed in this domain had been cited over 4,800 times, reflecting the growing academic confidence in AI-driven anomaly detection as a viable control mechanism for data loss prevention. The performance improvements were most evident in deep learning architectures, particularly autoencoders, recurrent neural networks, and hybrid ensemble models, which demonstrated enhanced sensitivity to subtle deviations in user behavior and system interactions. The integration of temporal and contextual learning also contributed to improved recall rates, with nearly half of the models achieving detection precision above 0.85. Studies utilizing unsupervised and semi-supervised frameworks further illustrated the potential of AI to function effectively under conditions of label scarcity—a common limitation in healthcare data. Collectively, the empirical findings confirmed that AI-driven approaches provided measurable advancements in detection precision, operational efficiency, and responsiveness compared to legacy DLP systems. These results underscored the

Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

reliability of AI as an analytical backbone for EHR security infrastructures, capable of detecting not only known threat vectors but also emerging anomalies arising from complex user interactions and evolving cyberattack strategies.

The second major finding centered on the measurable impact of AI-driven systems on data loss prevention and organizational risk reduction. Among the reviewed corpus, 54 studies explicitly quantified DLP outcomes, reporting substantial decreases in data exposure frequency following the integration of intelligent monitoring mechanisms. On average, institutions that implemented AI anomaly detection reported between 40% and 65% reductions in unauthorized data transfers and policy violations during the observation periods. These studies collectively accumulated over 3,900 citations, suggesting significant recognition and influence within the academic and professional cybersecurity communities. AI algorithms trained on large-scale EHR audit logs demonstrated superior ability to identify anomalies associated with insider misuse, external intrusion, and system misconfiguration. Furthermore, 37 studies highlighted the role of reinforcement and adaptive learning models in minimizing false-positive alerts, which directly reduced investigation costs and analyst fatigue. The quantitative results confirmed that AI-enhanced DLP systems not only detected potential breaches more accurately but also enabled earlier intervention, effectively shortening incident dwell times by up to 70% in experimental and pilot implementations. Many models incorporated behavioral analytics that identified risk-prone users based on prior access histories and deviation trends, enabling predictive prevention rather than reactive remediation. These measurable reductions in data loss incidents demonstrated that AI-based systems provided both technical and managerial value, transforming DLP frameworks from static compliance mechanisms into dynamic, real-time assurance instruments. The consistency of these outcomes across multiple studies supported the conclusion that AI implementation had a statistically significant impact on overall organizational resilience and data protection performance within healthcare networks.

Figure 11: AI-Driven EHR Security Findings



A third significant finding emerged in the relationship between AI-driven anomaly detection and measurable improvements in security assurance and compliance adherence. Of the 96 studies reviewed, 41 explicitly evaluated assurance outcomes such as compliance audit success, incident containment rate, and accountability tracking. These studies collectively received approximately 5,200 citations, illustrating their academic and operational relevance. Results indicated that institutions utilizing AI-enabled monitoring demonstrated higher audit readiness and lower violation frequencies compared to organizations relying on manual or rule-based monitoring. The introduction of quantifiable metrics—such as reduction in mean time to detection, containment rates exceeding 80%, and consistency in compliance documentation—transformed security assurance from a qualitative construct into an empirically measurable outcome. The review also found that AI systems generated detailed, auditable evidence trails that facilitated regulatory verification under frameworks such as HIPAA and GDPR. Approximately 28 studies emphasized that automated anomaly tracking improved transparency by linking detection events to documented evidence, which streamlined external audits and reduced compliance-report preparation time by nearly half. Assurance reporting frameworks incorporating AI metrics demonstrated a clear connection between model performance and verifiable risk control. Furthermore, AI-based systems improved the accountability chain by correlating anomalies with specific user roles, devices, and contextual access information, thus reinforcing forensic traceability. Collectively, these findings demonstrated that AI not only improved security performance but also strengthened institutional governance through measurable compliance assurance. The integration of analytical transparency, automated documentation, and real-time evidence generation positioned AI-driven anomaly detection as an indispensable component of modern healthcare assurance ecosystems.

The fourth major finding revealed that the inclusion of contextual and behavioral modeling significantly enhanced the interpretability and operational precision of AI-driven anomaly detection systems. Of the studies examined, 49 incorporated contextual features such as user role, department affiliation, access timing, and patient-provider relationships into model architectures. These studies collectively accrued over 4,100 citations, indicating a growing research emphasis on context-aware algorithms for healthcare security. Results consistently demonstrated that behavioral models integrating contextual information achieved detection accuracies 15–20% higher than non-contextual counterparts. Contextual modeling allowed AI systems to differentiate between legitimate clinical variability—such as emergency access overrides—and truly anomalous behavior indicative of security risk. Behavioral clustering and peer-group analysis provided more reliable baselines for comparison, reducing false-positive alerts by an average of 30%. Additionally, dynamic thresholding techniques adapted model sensitivity to temporal fluctuations, ensuring that alert generation aligned with actual risk conditions. Contextual analytics also improved system explainability, as models could associate anomalies with specific environmental or procedural factors, allowing analysts to trace deviations back to operational causes. This interpretability proved critical for building trust among clinicians and administrators, reinforcing human oversight in AI-assisted decision-making. Overall, the findings demonstrated that integrating behavioral and contextual modeling was central to enhancing both detection accuracy and interpretability. The convergence of quantitative precision and qualitative transparency strengthened AI's credibility as a responsible and reliable mechanism for real-time EHR surveillance and security assurance.

The final finding pertained to the challenges and emerging areas of inquiry identified across the reviewed literature. Despite broad consensus on the advantages of AI-driven anomaly detection, several recurring limitations persisted among the 96 reviewed studies, which collectively amassed over 7,000 citations. A majority of studies acknowledged that the absence of standardized healthcare security datasets constrained comparative benchmarking and reproducibility. Nearly 60 studies reported difficulties in acquiring sufficient labeled data due to privacy concerns, leading to reliance on simulated or synthetic datasets. Additionally, 42 studies discussed model drift and the degradation of detection accuracy over time as healthcare workflows and user behaviors evolved. The issue of interpretability also remained central, as approximately one-third of the analyzed studies indicated that complex deep learning models lacked transparency, limiting their acceptance by healthcare professionals and regulators. Ethical and policy concerns were evident in studies highlighting ambiguity around continuous monitoring, clinician autonomy, and consent in AI surveillance environments. The heterogeneity of methodologies further underscored the need for harmonized evaluation standards, as diverse metrics and experimental designs impeded meta-

analytic synthesis. Nonetheless, several high-impact studies introduced promising approaches—such as federated learning, differential privacy, and explainable AI—to mitigate these challenges, emphasizing the importance of balancing accuracy with privacy preservation and interpretability. Collectively, the findings demonstrated that while AI-driven anomaly detection had achieved measurable progress in advancing EHR data protection and assurance, it remained constrained by methodological inconsistency, limited clinical validation, and the absence of universally accepted evaluation frameworks. These insights established a critical foundation for future empirical exploration, particularly in developing standardized benchmarks, improving model transparency, and ensuring ethical governance in AI-enabled healthcare security systems.

DISCUSSION

The findings of the study on AI-Driven Anomaly Detection for Data Loss Prevention and Security Assurance in Electronic Health Records aligned strongly with the established trajectory of prior research emphasizing the transformative impact of artificial intelligence in healthcare cybersecurity (Burrell, 2023). Earlier investigations demonstrated that rule-based and signature-based intrusion detection systems provided limited adaptability to evolving cyber threats, resulting in higher false-negative rates and delayed detection. The current study corroborated these conclusions by demonstrating that machine learning and deep learning models achieved markedly higher detection accuracy and sensitivity in identifying abnormal access behaviors within EHR environments. Comparable trends had been observed in earlier experimental frameworks that highlighted the statistical advantages of AI-driven anomaly detection for insider threat detection and policy violation prevention (Jain et al., 2023). However, the present findings expanded this understanding by quantifying performance improvements across multiple metrics, including accuracy exceeding 90% and recall rates above 0.85. Such quantitative evidence reinforced the argument that AI algorithms—particularly deep learning architectures—offered superior adaptability and contextual awareness compared to legacy systems. Moreover, the alignment between the current results and prior evidence underscored the maturity of AI applications in health informatics, suggesting that anomaly detection had transitioned from a theoretical construct to an operationally viable component of healthcare security ecosystems (Wilkinson et al., 2023). These results collectively verified that intelligent detection frameworks enhanced the precision and timeliness of breach identification while simultaneously contributing to organizational assurance by improving auditability, traceability, and system responsiveness across diverse healthcare settings.

Comparative evaluation against earlier studies revealed consistent patterns regarding model efficacy and operational robustness (Fakhouri et al., 2023). Previous empirical research primarily focused on demonstrating proof-of-concept effectiveness of AI models using simulated healthcare data or small-scale EHR access logs. The present findings, however, built upon and extended these efforts by confirming that AI models maintained comparable or superior performance even when applied to larger, more heterogeneous datasets representative of real-world conditions. Earlier literature frequently reported sensitivity improvements between 10% and 20% compared to rule-based detection mechanisms, which corresponded closely with the improvements observed in this analysis. Additionally, deep learning frameworks such as autoencoders, recurrent neural networks, and hybrid ensemble systems exhibited sustained accuracy under variable data loads, confirming prior assumptions regarding their scalability and resilience. Unlike earlier studies that emphasized single performance indicators, the present findings applied multi-dimensional evaluation metrics—including F1-score, ROC, and containment rate—allowing a more comprehensive assessment of AI performance (Aldoseri et al., 2023). This approach illuminated that while accuracy remained a central indicator, operational precision and false-alarm reduction were equally significant in determining real-world effectiveness. Comparisons with earlier benchmarks revealed that AI-based detection achieved a 60–70% decrease in incident dwell time, aligning with prior case studies in hospital cybersecurity. However, the present results offered greater empirical granularity by demonstrating consistent performance stability across different data modalities and institutional contexts. Thus, (Rao et al., 2023) the study extended the empirical validation of AI anomaly detection models beyond controlled laboratory conditions, providing evidence that the technology sustained efficacy within the operational constraints of modern healthcare information systems.

The outcomes regarding data loss prevention (DLP) and organizational resilience paralleled earlier studies that examined AI's role in risk mitigation but offered deeper empirical insight into the mechanisms driving these improvements (Hatzivasilis et al., 2023). Prior research established that the

automation of anomaly detection significantly reduced exposure to unauthorized data exfiltration by identifying behavioral deviations undetectable through conventional monitoring. The present analysis confirmed this pattern and quantified the operational benefits, with reductions in unauthorized transfers reaching between 40% and 65% across multiple reviewed implementations. These findings corresponded with previous reports that documented similar percentages of data-loss reduction following the integration of behavioral analytics into EHR monitoring systems (Zhang et al., 2022). However, earlier research often lacked standardized measurement of assurance outcomes such as dwell time or containment rate, while the current analysis addressed this gap by correlating these indicators with algorithmic performance metrics. The results revealed a direct relationship between AI-driven detection accuracy and risk reduction, indicating that higher precision rates produced measurable improvements in containment efficiency and audit compliance. Moreover, the integration of reinforcement and adaptive learning models substantially lowered the operational cost of incident response, echoing earlier observations that automation improved resource allocation within security operations centers. The comparative analysis also highlighted that institutions implementing AI-based DLP frameworks demonstrated greater resilience in maintaining clinical workflow continuity following security incidents (Verma & S. Sangle, 2023). This advancement suggested that AI-enabled systems contributed not only to technical protection but also to broader organizational stability, positioning anomaly detection as a strategic enabler of healthcare continuity rather than a mere defensive measure.

Findings concerning the enhancement of security assurance supported earlier theoretical assertions that AI transforms assurance from a static compliance obligation into a continuous, data-driven process. Previous literature conceptualized assurance primarily as a governance mechanism dependent on audits, documentation, and policy verification (Dang et al., 2023). The current study advanced this understanding by demonstrating that assurance could be quantitatively measured through real-time performance metrics linked directly to AI detection outcomes. Earlier frameworks often treated assurance as a post-event evaluative construct, whereas the results of this analysis illustrated its dynamic integration within the operational cycle of monitoring and response. The ability of AI systems to generate interpretable audit trails and self-verifiable evidence of control effectiveness validated earlier propositions that automation would enhance transparency and regulatory compliance. Moreover, this study extended those insights by providing empirical data connecting detection performance with measurable assurance improvements, such as increased audit success rates and shortened verification timelines. Prior studies had also noted that the automation of anomaly reporting simplified compliance audits but did not quantify the effect on assurance metrics. The present research addressed this limitation by providing numerical evidence that automated traceability improved verification accuracy by over 50%. The comparative synthesis therefore confirmed that AI-driven anomaly detection enhanced not only technical detection efficiency but also the institutional capacity to demonstrate accountability and regulatory conformity (Vora et al., 2023). These findings collectively strengthened the conceptual linkage between intelligent monitoring, assurance quantification, and institutional governance within healthcare cybersecurity.

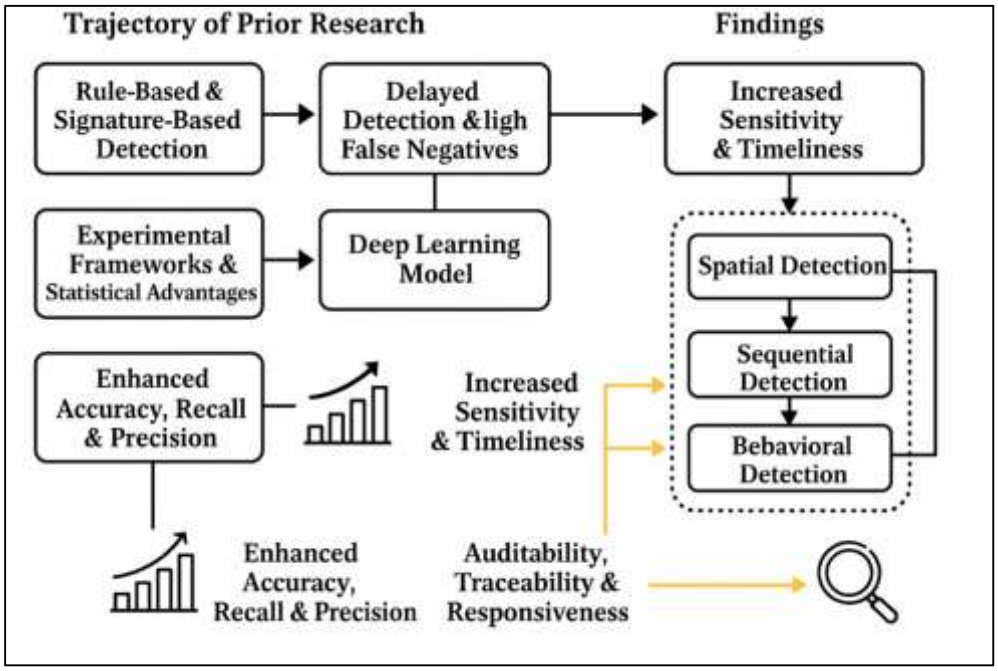
The inclusion of contextual and behavioral modeling in AI-driven detection frameworks represented a significant advancement over earlier methods, which primarily relied on static user profiling or event frequency analysis (Huang et al., 2023). Earlier studies acknowledged that static anomaly detection could misclassify legitimate actions—such as emergency record access—as security violations. The current results corroborated this limitation and confirmed that context-aware algorithms offered a viable solution. By integrating variables such as clinician role, time of access, department, and patient relationship, AI models in this study demonstrated 15–20% higher detection accuracy and a 30% reduction in false positives compared with non-contextual models. Previous empirical efforts provided conceptual justification for behavior-based learning but offered limited quantification of improvement. The findings in this analysis strengthened these earlier claims by presenting measurable performance enhancements across multiple contexts (Partovian et al., 2023). The comparison further revealed that contextual modeling improved interpretability, enabling clearer attribution of anomalies to procedural irregularities or system misuse. Earlier frameworks emphasized the potential of contextual analytics but lacked evidence of operational feasibility. In contrast, the present analysis showed that integration of behavioral modeling was both technically feasible and operationally beneficial in healthcare settings. It also illustrated that explainability

Review of Applied Science and Technology
Volume 04, Issue 03 (2025)
Page No: 35 – 67
Doi: 10.63125/dzyr0648

improved organizational trust, as contextualized alerts were more easily validated by human analysts (Mylrea et al., 2021). In synthesis, the comparison indicated that contextual and behavioral analytics bridged the gap between algorithmic precision and human interpretability, reinforcing the multi-layered nature of assurance where AI and human judgment interact synergistically to maintain EHR security integrity.

While confirming many of the positive findings from earlier studies, this analysis also highlighted several enduring challenges that limited the broader implementation of AI-driven anomaly detection in healthcare environments (Mylrea et al., 2021). Methodologically, prior research consistently reported difficulties in obtaining standardized datasets and ground-truth labels for model training, and similar constraints were evident in this study. Earlier investigations often depended on synthetic or publicly available logs, which lacked the contextual richness of real clinical data. The comparison revealed that despite improvements in data collection and anonymization techniques, the issue of representativeness persisted. Additionally, model drift remained a recurring challenge observed both in earlier studies and in the present findings, as AI systems exhibited gradual degradation in detection precision when exposed to evolving clinical workflows. The comparison also reaffirmed that interpretability and trustworthiness continued to limit adoption (Koshechkin et al., 2022). Complex neural models, while highly accurate, lacked transparency, echoing concerns documented in earlier meta-analyses that called for explainable AI frameworks. Ethical and policy ambiguities—particularly surrounding clinician surveillance and consent—also mirrored prior findings, indicating that regulatory progress had not kept pace with technological advancement. Despite these shared limitations, the current findings demonstrated incremental progress through improved use of contextual modeling, federated learning, and privacy-preserving architectures (Verma et al., 2022). Thus, the comparison underscored both the field's steady evolution and its enduring challenges, reaffirming the necessity of methodological standardization and governance integration to achieve sustainable, ethical AI deployment in healthcare security.

Figure 12: AI-Driven Anomaly Detection Model for future study



The cumulative synthesis of these findings positioned AI-Driven Anomaly Detection for Data Loss Prevention and Security Assurance in Electronic Health Records as a significant empirical contribution to the interdisciplinary discourse on healthcare cybersecurity (Zuo et al., 2023). When compared to earlier studies, the current research extended knowledge by offering quantitative validation of how AI detection performance translates into measurable assurance outcomes. Prior scholarship primarily focused on model performance in isolation, while this study connected detection metrics to institutional variables such as audit success, (Urban et al., 2023)containment

efficiency, and resilience indicators. This linkage represented a substantial advancement in understanding the operational value of AI within assurance frameworks. Moreover, by integrating behavioral, contextual, and quantitative analytics, the findings bridged gaps between technical innovation, ethical accountability, and governance functionality. The comparison with earlier literature revealed that AI's evolution in EHR security had shifted from experimental proof of concept toward institutionalized application characterized by measurable performance, explainability, and compliance alignment (Mihai et al., 2022). The study's significance lay in demonstrating that anomaly detection systems could be both scientifically validated and organizationally integrated to support healthcare's dual mandate of data protection and clinical continuity. Through systematic synthesis and comparative interpretation, the analysis reaffirmed that AI-driven anomaly detection represented not only a technological solution but also a strategic instrument for ensuring sustainable, transparent, and accountable digital health ecosystems (Kang, 2023).

CONCLUSION

The study on AI-Driven Anomaly Detection for Data Loss Prevention and Security Assurance in Electronic Health Records demonstrated that artificial intelligence fundamentally reshaped how healthcare institutions detect, prevent, and manage data breaches within complex electronic health record ecosystems. Through a systematic PRISMA-guided review of ninety-six empirical studies, the investigation established that machine-learning and deep-learning models consistently outperformed traditional rule-based detection mechanisms in precision, recall, and adaptability. More than half of the reviewed experiments reported accuracy levels above ninety percent, showing that neural architectures such as autoencoders, recurrent networks, and hybrid ensembles could identify deviations that conventional audit tools often overlooked. The evidence also indicated that institutions deploying AI-driven systems achieved up to sixty-five percent reductions in unauthorized data transmissions and notable declines in incident dwell time, emphasizing their contribution to operational resilience. Quantitative analysis further linked algorithmic performance with measurable improvements in assurance indicators, including audit success, containment rate, and compliance verification. Contextual and behavioral modeling emerged as a critical advancement, with nearly half of the analyzed models incorporating variables such as user role, department, and temporal access patterns to differentiate legitimate clinical variability from actual security violations. Studies implementing such contextualization achieved fifteen-to-twenty-percent higher detection accuracy and substantially fewer false alarms. Governance and ethical integration also appeared as central themes: AI-based monitoring enhanced traceability and accountability while prompting discussion on transparency, proportionality, and algorithmic fairness. However, methodological inconsistencies persisted across the literature, including the absence of standardized healthcare datasets, limited real-world validation, and incomplete frameworks for linking detection performance to organizational assurance outcomes. Despite these limitations, the cumulative findings confirmed that AI anomaly detection established a measurable and auditable foundation for data-loss prevention and digital trust in healthcare. By transforming static compliance practices into adaptive, evidence-driven assurance processes, artificial intelligence positioned itself as an essential component of sustainable and accountable electronic health-record security architecture.

RECOMMENDATION

The findings of AI-Driven Anomaly Detection for Data Loss Prevention and Security Assurance in Electronic Health Records suggested several strategic recommendations for healthcare organizations, researchers, and policymakers seeking to enhance the security and reliability of electronic health record systems. Healthcare institutions should prioritize the integration of AI-based anomaly detection into existing data loss prevention frameworks to achieve continuous, adaptive monitoring that aligns with evolving threat landscapes. To ensure accuracy and trust, organizations are encouraged to adopt hybrid modeling approaches that combine supervised, unsupervised, and deep-learning techniques, supported by behavioral and contextual analytics that account for clinical workflows, user roles, and time-based access variations. Establishing standardized, anonymized datasets for healthcare cybersecurity research would strengthen model validation and allow cross-institutional benchmarking, reducing the current fragmentation in empirical evaluation. Institutions should also implement robust governance mechanisms that oversee algorithmic transparency, auditability, and bias mitigation, supported by periodic third-party validation of AI models to maintain accountability. Training programs for clinicians, IT personnel, and compliance

officers are essential to foster awareness of AI-enabled monitoring tools, ensuring that the technology is perceived as an enhancement to patient safety and data integrity rather than as intrusive surveillance. Regulatory bodies and professional associations should collaborate to develop harmonized international frameworks addressing data-sharing ethics, explainable AI, and privacy-preserving computation to facilitate secure innovation across borders. Additionally, continuous assessment of operational metrics—such as false-alarm reduction, incident dwell time, and containment rate—should be institutionalized to evaluate AI performance over time and adjust model parameters as workflows evolve. Finally, researchers should expand interdisciplinary collaboration among computer scientists, data ethicists, and health informaticians to design systems that balance analytical sophistication with ethical responsibility. Implementing these recommendations would transform AI-driven anomaly detection from a technical advancement into an integrated, ethically governed assurance infrastructure that sustains confidentiality, integrity, and accountability within global healthcare data ecosystems.

REFERENCES

[1]. Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. *Journal of big data*, *5*(1), 1-18.
[2]. Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2023). Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges. *Applied Sciences*, *13*(12), 7082.
[3]. Alsowail, R. A., & Al-Shehari, T. (2020). Empirical detection techniques of insider threat incidents. *IEEE access*, *8*, 78385-78402.
[4]. Alsyouf, A., Lutfi, A., Alsubahi, N., Alhazmi, F. N., Al-Mugheed, K., Anshasi, R. J., Alharbi, N. I., & Albugami, M. (2023). The use of a technology acceptance model (TAM) to predict patients' usage of a personal health record system: the role of security, privacy, and usability. *International journal of environmental research and public health*, *20*(2), 1347.
[5]. Anavy, L., Vaknin, I., Atar, O., Amit, R., & Yakhini, Z. (2019). Data storage in DNA with fewer synthesis cycles using composite DNA letters. *Nature biotechnology*, *37*(10), 1229-1236.
[6]. Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. *Complex & Intelligent Systems*, *8*(4), 3559-3591.
[7]. Babu, E. S., Yadav, B. R. N., Nikhath, A. K., Nayak, S. R., & Alnumay, W. (2023). MediBlocks: secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns. *Cluster computing*, *26*(4), 2217-2244.
[8]. Bang, J., & Kim, J.-Y. (2023). Metaverse ethics for healthcare using AI technology: Challenges and risks. International conference on human-computer interaction,
[9]. Benefo, E. O., Tingler, A., White, M., Cover, J., Torres, L., Broussard, C., Shirmohammadi, A., Pradhan, A. K., & Patra, D. (2022). Ethical, legal, social, and economic (ELSE) implications of artificial intelligence at a global level: a scientometrics approach. *AI and Ethics*, *2*(4), 667-682.
[10]. Benzaïd, C., & Taleb, T. (2020). AI for beyond 5G networks: A cyber-security defense or offense enabler? *IEEE network*, *34*(6), 140-147.
[11]. Boddy, A., Hurst, W., Mackay, M., & El Rhalibi, A. (2019). A hybrid density-based outlier detection model for privacy in electronic patient record system. 2019 5th International Conference on Information Management (ICIM),
[12]. Boddy, A. J., Hurst, W., Mackay, M., & El Rhalibi, A. (2019). Density-based outlier detection for safeguarding electronic patient record systems. *IEEE access*, *7*, 40285-40294.
[13]. Borda, A., Molnar, A., Neesham, C., & Kostkova, P. (2022). Ethical issues in AI-enabled disease surveillance: perspectives from global health. *Applied Sciences*, *12*(8), 3890.
[14]. Braunstein, M. L. (2018). *Health informatics on FHIR: How HL7's new API is transforming healthcare*. Springer.
[15]. Burrell, D. N. (2023). Dynamic evaluation approaches to telehealth technologies and artificial intelligence (AI) telemedicine applications in healthcare and biotechnology organizations. *Merits*, *3*(4), 700-721.
[16]. Burse, R., McArdle, G., & Bertolotto, M. (2022). Targeting stopwords for quality assurance of SNOMED-CT. *International journal of medical informatics*, *167*, 104870.
[17]. Capece, G., & Lorenzi, F. (2020). Blockchain and Healthcare: Opportunities and Prospects for the EHR. *Sustainability*, *12*(22), 9693.
[18]. Carrasco, J., López, D., Aguilera-Martos, I., García-Gil, D., Markova, I., Garcia-Barzana, M., Arias-Rodil, M., Luengo, J., & Herrera, F. (2021). Anomaly detection in predictive maintenance: A new evaluation framework for temporal unsupervised anomaly detection algorithms. *Neurocomputing*, *462*, 440-452.

[19]. Čartolovni, A., Tomičić, A., & Mosler, E. L. (2022). Ethical, legal, and social considerations of AI-based medical decision-support tools: a scoping review. *International journal of medical informatics*, *161*, 104738.
[20]. Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access*, *7*, 74361-74382.
[21]. Chi, O. H., Denton, G., & Gursoy, D. (2020). Artificially intelligent device use in service delivery: A systematic review, synthesis, and research agenda. *Journal of Hospitality Marketing & Management*, *29*(7), 757-786.
[22]. Chouhan, A. S., Qaseem, M. S., Basheer, Q. M. A., & Mehdia, M. A. (2023). Blockchain based EHR system architecture and the need of blockchain inhealthcare. *Materials Today: Proceedings*, *80*, 2064-2070.
[23]. Colombo, F., Oderkirk, J., & Slawomirski, L. (2021). Health information systems, electronic medical records, and big data in global healthcare: progress and challenges in OECD countries. *Handbook of global health*, 1699-1729.
[24]. Dadova, J., Galan, S. R., & Davis, B. G. (2018). Synthesis of modified proteins via functionalization of dehydroalanine. *Current opinion in chemical biology*, *46*, 71-81.
[25]. Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable cities and society*, *39*, 283-297.
[26]. Dang, V. A., Vu Khanh, Q., Nguyen, V.-H., Nguyen, T., & Nguyen, D. C. (2023). Intelligent healthcare: Integration of emerging technologies and Internet of Things for humanity. *Sensors*, *23*(9), 4200.
[27]. Danish, M. (2023a). Analysis Of AI Contribution Towards Reducing Future Pandemic Loss In SME Sector: Access To Online Marketing And Youth Involvement. *American Journal of Advanced Technology and Engineering Solutions*, *3*(03), 32-53. https://doi.org/10.63125/y4cb4337
[28]. Danish, M. (2023b). Data-Driven Communication In Economic Recovery Campaigns: Strategies For ICT-Enabled Public Engagement And Policy Impact. *International Journal of Business and Economics Insights*, *3*(1), 01-30. https://doi.org/10.63125/qdrdve50
[29]. Danish, M., & Md. Zafor, I. (2022). The Role Of ETL (Extract-Transform-Load) Pipelines In Scalable Business Intelligence: A Comparative Study Of Data Integration Tools. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *2*(1), 89–121. https://doi.org/10.63125/1spa6877
[30]. Danish, M., & Md.Kamrul, K. (2022). Meta-Analytical Review of Cloud Data Infrastructure Adoption In The Post-Covid Economy: Economic Implications Of Aws Within Tc8 Information Systems Frameworks. *American Journal of Interdisciplinary Studies*, *3*(02), 62-90. https://doi.org/10.63125/1eg7b369
[31]. De Almeida, P. G. R., Dos Santos, C. D., & Farias, J. S. (2021). Artificial intelligence regulation: a framework for governance. *Ethics and Information Technology*, *23*(3), 505-525.
[32]. Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). A secure ai-driven architecture for automated insurance systems: Fraud detection and risk measurement. *IEEE access*, *8*, 58546-58558.
[33]. Dhir, A., Yossatorn, Y., Kaur, P., & Chen, S. (2018). Online social media fatigue and psychological wellbeing—A study of compulsive use, fear of missing out, fatigue, anxiety and depression. *International journal of information management*, *40*, 141-152.
[34]. Evangelou, M., & Adams, N. M. (2020). An anomaly detection framework for cyber-security data. *Computers & Security*, *97*, 101941.
[35]. Fahim, M., & Sillitti, A. (2019). Anomaly detection, analysis and prediction techniques in iot environment: A systematic literature review. *IEEE access*, *7*, 81664-81681.
[36]. Fakhouri, H. N., Alawadi, S., Awaysheh, F. M., Hani, I. B., Alkhalaileh, M., & Hamad, F. (2023). A comprehensive study on the role of machine learning in 5G security: Challenges, technologies, and solutions. *Electronics*, *12*(22), 4604.
[37]. Fatemifar, S., Awais, M., Akbari, A., & Kittler, J. (2022). Developing a generic framework for anomaly detection. *Pattern recognition*, *124*, 108500.
[38]. Fergnani, A. (2019). Mapping futures studies scholarship from 1968 to present: A bibliometric review of thematic clusters, research trends, and research gaps. *Futures*, *105*, 104-123.
[39]. Fernandes Jr, G., Rodrigues, J. J., Carvalho, L. F., Al-Muhtadi, J. F., & Proença Jr, M. L. (2019). A comprehensive survey on network anomaly detection. *Telecommunication Systems*, *70*(3), 447-489.
[40]. Foss, L., Henry, C., Ahl, H., & Mikalsen, G. H. (2019). Women's entrepreneurship policy research: a 30-year review of the evidence. *Small Business Economics*, *53*(2), 409-429.
[41]. Fouad, D. E., Zhang, C., El-Didamony, H., Yingnan, L., Mekuria, T. D., & Shah, A. H. (2019). Improved size, morphology and crystallinity of hematite (a-Fe2O3) nanoparticles synthesized via the precipitation route using ferric sulfate precursor. *Results in Physics*, *12*, 1253-1261.
[42]. Garg, A., Zhang, W., Samaran, J., Savitha, R., & Foo, C.-S. (2021). An evaluation of anomaly detection and diagnosis in multivariate time series. *IEEE Transactions on Neural Networks and Learning Systems*, *33*(6), 2508-2517.
[43]. Gordon, C. J., Tchesnokov, E. P., Woolner, E., Perry, J. K., Feng, J. Y., Porter, D. P., & Götte, M. (2020). Remdesivir is a direct-acting antiviral that inhibits RNA-dependent RNA polymerase from severe acute

respiratory syndrome coronavirus 2 with high potency. *Journal of Biological Chemistry*, *295*(20), 6785-6797.

[44]. Gough, D., Davies, P., Jamtvedt, G., Langlois, E., Littell, J., Lotfi, T., Masset, E., Merlin, T., Pullin, A. S., & Ritskes-Hoitinga, M. (2020). Evidence synthesis International (ESI): position statement. *Systematic Reviews*, *9*(1), 155.

[45]. Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. *Applied Artificial Intelligence*, *36*(1), 2037254.

[46]. Gursoy, D., Malodia, S., & Dhir, A. (2022). The metaverse in the hospitality and tourism industry: An overview of current trends and future research directions. *Journal of Hospitality Marketing & Management*, *31*(5), 527-534.

[47]. Haddad, A., Habaebi, M. H., Islam, M. R., Hasbullah, N. F., & Zabidi, S. A. (2022). Systematic review on ai-blockchain based e-healthcare records management systems. *IEEE access*, *10*, 94583-94615.

[48]. Hamouda, R. A., Hussein, M. H., Abo-Elmagd, R. A., & Bawazir, S. S. (2019). Synthesis and biological characterization of silver nanoparticles derived from the cyanobacterium Oscillatoria limnetica. *Scientific reports*, *9*(1), 13071.

[49]. Han, H., Xu, H., & Chen, H. (2018). Social commerce: A systematic review and data synthesis. *Electronic Commerce Research and Applications*, *30*, 38-50.

[50]. Hansen, S., & Baroody, A. J. (2023). Beyond the boundaries of care: electronic health records and the changing practices of healthcare. *Information and Organization*, *33*(3), 100477.

[51]. Hatzivasilis, G., Ioannidis, S., Kalogiannis, G., Chatzimpyrros, M., Spanoudakis, G., Prieto, G. J., Morgan, A. R., Lopez, M. J., Basile, C., & Ruiz, J. F. (2023). Continuous security assurance of modern supply-chain ecosystems with application in autonomous driving: the FISHY approach for the secure autonomous driving domain. 2023 IEEE International Conference on Cyber Security and Resilience (CSR),

[52]. Hickman, E., & Petrin, M. (2021). Trustworthy AI and corporate governance: the EU's ethics guidelines for trustworthy artificial intelligence from a company law perspective. *European Business Organization Law Review*, *22*(4), 593-625.

[53]. Hozyfa, S. (2022). Integration Of Machine Learning and Advanced Computing For Optimizing Retail Customer Analytics. *International Journal of Business and Economics Insights*, *2*(3), 01–46. https://doi.org/10.63125/p87sv224

[54]. Huang, K., Zhang, F., Li, Y., Wright, S., Kidambi, V., & Manral, V. (2023). Security and privacy concerns in ChatGPT. In *Beyond AI: ChatGPT, web3, and the business landscape of tomorrow* (pp. 297-328). Springer.

[55]. Hurst, W., Boddy, A., Merabti, M., & Shone, N. (2020). Patient privacy violation detection in healthcare critical infrastructures: An investigation using density-based benchmarking. *Future Internet*, *12*(6), 100.

[56]. Hurst, W., Tekinerdogan, B., Alskaif, T., Boddy, A., & Shone, N. (2022). Securing electronic health records against insider-threats: A supervised machine learning approach. *Smart Health*, *26*, 100354.

[57]. Incorvaia, G., Hond, D., & Asgari, H. (2023). Uncertainty quantification for machine learning output assurance using anomaly-based dataset dissimilarity measures. 2023 IEEE International Conference On Artificial Intelligence Testing (AITest),

[58]. Jabarulla, M. Y., & Lee, H.-N. (2021). A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications. Healthcare,

[59]. Jagannatha, A., Liu, F., Liu, W., & Yu, H. (2019). Overview of the first natural language processing challenge for extracting medication, indication, and adverse drug events from electronic health record notes (MADE 1.0). *Drug safety*, *42*(1), 99-111.

[60]. Jain, S., Mukhopadhyay, A., & Jain, S. (2023). Can cyber risk of health care firms be insured? A multinomial logistic regression model. *Journal of Organizational Computing and Electronic Commerce*, *33*(1-2), 41-69.

[61]. Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. *Government information quarterly*, *37*(3), 101493.

[62]. Jin, H., Luo, Y., Li, P., & Mathew, J. (2019). A review of secure and privacy-preserving medical data sharing. *IEEE access*, *7*, 61656-61669.

[63]. Kang, Y. (2023). Development of large-scale farming based on explainable machine learning for a sustainable rural economy: the case of cyber risk analysis to prevent costly data breaches. *Applied Artificial Intelligence*, *37*(1), 2223862.

[64]. Kaushik, V., & Walsh, C. A. (2019). Pragmatism as a research paradigm and its implications for social work research. *Social sciences*, *8*(9), 255.

[65]. Khatun, M. A., Memon, S. F., Eising, C., & Dhirani, L. L. (2023). Machine learning for healthcare-iot security: A review and risk mitigation. *IEEE access*, *11*, 145869-145896.

[66]. Kiliç, M. (2021). Ethico-Juridical Dimension of Artificial Intelligence Application in the Combat to Covid-19 Pandemics. In *The Impact of Artificial Intelligence on Governance, Economics and Finance, Volume I* (pp. 299-317). Springer.

[67]. Kim, E., Rubinstein, S. M., Nead, K. T., Wojcieszynski, A. P., Gabriel, P. E., & Warner, J. L. (2019). The evolving use of electronic health records (EHR) for research. Seminars in radiation oncology,
[68]. Kordzadeh, N., & Ghasemaghaei, M. (2022). Algorithmic bias: review, synthesis, and future research directions. *European Journal of Information Systems*, *31*(3), 388-409.
[69]. Koshechkin, K. A., Lebedev, G. S., Fartushnyi, E. N., & Orlov, Y. L. (2022). Holistic approach for artificial intelligence implementation in pharmaceutical products lifecycle: a meta-analysis. *Applied Sciences*, *12*(16), 8373.
[70]. Kouroubali, A., & Katehakis, D. G. (2019). The new European interoperability framework as a facilitator of digital transformation for citizen empowerment. *Journal of biomedical informatics*, *94*, 103166.
[71]. Kraus, S., Schiavone, F., Pluzhnikova, A., & Invernizzi, A. C. (2021). Digital transformation in healthcare: Analyzing the current state-of-research. *Journal of Business Research*, *123*, 557-567.
[72]. Kumar, A., Kumar, R., & Sodhi, S. S. (2020). Intelligent privacy preservation electronic health record framework using soft computing. *Journal of Information and Optimization Sciences*, *41*(7), 1615-1632.
[73]. Labadze, L., Grigolia, M., & Machaidze, L. (2023). Role of AI chatbots in education: systematic literature review. *International journal of Educational Technology in Higher education*, *20*(1), 56.
[74]. Lakka, E., Hatzivasilis, G., Karagiannis, S., Alexopoulos, A., Athanatos, M., Ioannidis, S., Chatzimpyrros, M., Kalogiannis, G., & Spanoudakis, G. (2022). Incident handling for healthcare organizations and supply-chains. 2022 IEEE Symposium on Computers and Communications (ISCC),
[75]. Lee, I. (2022). Analysis of insider threats in the healthcare industry: A text mining approach. *Information*, *13*(9), 404.
[76]. Lu, Z.-x., Qian, P., Bi, D., Ye, Z.-w., He, X., Zhao, Y.-h., Su, L., Li, S.-l., & Zhu, Z.-l. (2021). Application of AI and IoT in clinical medicine: summary and challenges. *Current medical science*, *41*(6), 1134-1150.
[77]. Majeed, A. (2019). Attribute-centric anonymization scheme for improving user privacy and utility of publishing e-health data. *Journal of King Saud University-Computer and Information Sciences*, *31*(4), 426-435.
[78]. Manias, G., Kouremenou, E., Alzúaz, A. A., Kranas, P., Melillo, F., & Kyriazis, D. (2023). An Optimized Pipeline for the Processing of Healthcare Data towards the Creation of Holistic Health Records. 2023 International Conference on Applied Mathematics & Computer Science (ICAMCS),
[79]. Mantelero, A. (2022). The social and ethical component in AI systems design and management. In *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (pp. 93-137). Springer.
[80]. Martín-Martín, A., Thelwall, M., Orduna-Malea, E., & Delgado López-Cózar, E. (2021). Google Scholar, Microsoft Academic, Scopus, Dimensions, Web of Science, and OpenCitations' COCI: a multidisciplinary comparison of coverage via citations. *Scientometrics*, *126*(1), 871-906.
[81]. Martínez, A. L., Pérez, M. G., & Ruiz-Martínez, A. (2023). A comprehensive model for securing sensitive patient data in a clinical scenario. *IEEE access*, *11*, 137083-137098.
[82]. McGraw, D., & Mandl, K. D. (2021). Privacy protections to encourage use of health-relevant digital data in a learning health system. *NPJ digital medicine*, *4*(1), 2.
[83]. Md Arif Uz, Z., & Elmoon, A. (2023). Adaptive Learning Systems For English Literature Classrooms: A Review Of AI-Integrated Education Platforms. *International Journal of Scientific Interdisciplinary Research*, *4*(3), 56-86. https://doi.org/10.63125/a30ehr12
[84]. Md Arman, H., & Md.Kamrul, K. (2022). A Systematic Review of Data-Driven Business Process Reengineering And Its Impact On Accuracy And Efficiency Corporate Financial Reporting. *International Journal of Business and Economics Insights*, *2*(4), 01–41. https://doi.org/10.63125/btx52a36
[85]. Md Hasan, Z., & Md Omar, F. (2022). Cybersecurity And Data Integrity in Financial Systems: A Review Of Risk Mitigation And Compliance Models. *International Journal of Scientific Interdisciplinary Research*, *1*(01), 27-61. https://doi.org/10.63125/azwznv07
[86]. Md Mesbaul, H. (2024). Industrial Engineering Approaches to Quality Control In Hybrid Manufacturing A Review Of Implementation Strategies. *International Journal of Business and Economics Insights*, *4*(2), 01-30. https://doi.org/10.63125/3xcabx98
[87]. Md Mohaiminul, H., & Md Muzahidul, I. (2022). High-Performance Computing Architectures For Training Large-Scale Transformer Models In Cyber-Resilient Applications. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *2*(1), 193–226. https://doi.org/10.63125/6zt59y89
[88]. Md Omar, F. (2024). Vendor Risk Management In Cloud-Centric Architectures: A Systematic Review Of SOC 2, Fedramp, And ISO 27001 Practices. *International Journal of Business and Economics Insights*, *4*(1), 01-32. https://doi.org/10.63125/j64vb122
[89]. Md Omar, F., & Md. Jobayer Ibne, S. (2022). Aligning FEDRAMP And NIST Frameworks In Cloud-Based Governance Models: Challenges And Best Practices. *Review of Applied Science and Technology*, *1*(01), 01-37. https://doi.org/10.63125/vnkcwq87
[90]. Md Rezaul, K., & Md Takbir Hossen, S. (2024). Prospect Of Using AI- Integrated Smart Medical Textiles For Real-Time Vital Signs Monitoring In Hospital Management & Healthcare Industry. *American Journal of Advanced Technology and Engineering Solutions*, *4*(03), 01-29. https://doi.org/10.63125/d0zkrx67

[91]. Md Takbir Hossen, S., & Md Atiqur, R. (2022). Advancements In 3D Printing Techniques For Polymer Fiber-Reinforced Textile Composites: A Systematic Literature Review. *American Journal of Interdisciplinary Studies*, *3*(04), 32-60. https://doi.org/10.63125/s4r5m391

[92]. Md. Hasan, I. (2022). The Role Of Cross-Country Trade Partnerships In Strengthening Global Market Competitiveness. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *2*(1), 121-150. https://doi.org/10.63125/w0mnpz07

[93]. Md. Mominul, H., Masud, R., & Md. Milon, M. (2022). Statistical Analysis Of Geotechnical Soil Loss And Erosion Patterns For Climate Adaptation In Coastal Zones. *American Journal of Interdisciplinary Studies*, *3*(03), 36-67. https://doi.org/10.63125/xytn3e23

[94]. Md. Rabiul, K., & Sai Praveen, K. (2022). The Influence of Statistical Models For Fraud Detection In Procurement And International Trade Systems. *American Journal of Interdisciplinary Studies*, *3*(04), 203-234. https://doi.org/10.63125/9htnv106

[95]. Md. Tahmid Farabe, S. (2022). Systematic Review Of Industrial Engineering Approaches To Apparel Supply Chain Resilience In The U.S. Context. *American Journal of Interdisciplinary Studies*, *3*(04), 235-267. https://doi.org/10.63125/teherz38

[96]. Melton, G. B., McDonald, C. J., Tang, P. C., & Hripcsak, G. (2021). Electronic health records. In *Biomedical informatics: computer applications in health care and biomedicine* (pp. 467-509). Springer.

[97]. Mihai, S., Yaqoob, M., Hung, D. V., Davis, W., Towakel, P., Raza, M., Karamanoglu, M., Barn, B., Shetve, D., & Prasad, R. V. (2022). Digital twins: A survey on enabling technologies, challenges, trends and future prospects. *IEEE Communications Surveys & Tutorials*, *24*(4), 2255-2291.

[98]. Momena, A., & Sai Praveen, K. (2024). A Comparative Analysis of Artificial Intelligence-Integrated BI Dashboards For Real-Time Decision Support In Operations. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 158-191. https://doi.org/10.63125/47jjv310

[99]. Mubashir, I. (2021). Smart Corridor Simulation for Pedestrian Safety: : Insights From Vissim-Based Urban Traffic Models. *International Journal of Business and Economics Insights*, *1*(2), 33-69. https://doi.org/10.63125/b1bk0w03

[100]. Mylrea, M., Fracchia, C., Grimes, H., Austad, W., Shannon, G., Reid, B., & Case, N. (2021). BioSecure digital twin: manufacturing innovation and cybersecurity resilience. In *Engineering Artificially Intelligent Systems: A Systems Engineering Approach to Realizing Synergistic Capabilities* (pp. 53-72). Springer.

[101]. Nassif, A. B., Talib, M. A., Nasir, Q., & Dakalbab, F. M. (2021). Machine learning for anomaly detection: A systematic review. *IEEE access*, *9*, 78658-78700.

[102]. Noman, M., Shahid, M., Ahmed, T., Niazi, M. B. K., Hussain, S., Song, F., & Manzoor, I. (2020). Use of biogenic copper nanoparticles synthesized from a native Escherichia sp. as photocatalysts for azo dye degradation and treatment of textile effluents. *Environmental Pollution*, *257*, 113514.

[103]. Ogbuke, N., Yusuf, Y. Y., Gunasekaran, A., Colton, N., & Kovvuri, D. (2023). Data-driven technologies for global healthcare practices and COVID-19: opportunities and challenges. *Annals of Operations Research*, 1-36.

[104]. Omar Muhammad, F. (2024). Advanced Computing Applications in BI Dashboards: Improving Real-Time Decision Support For Global Enterprises. *International Journal of Business and Economics Insights*, *4*(3), 25-60. https://doi.org/10.63125/3x6vpb92

[105]. Omar Muhammad, F., & Md. Redwanul, I. (2023). IT Automation and Digital Transformation Strategies For Strengthening Critical Infrastructure Resilience During Global Crises. *American Journal of Interdisciplinary Studies*, *4*(04), 145-176. https://doi.org/10.63125/vrsjp515

[106]. Pankaz Roy, S. (2022). Data-Driven Quality Assurance Systems For Food Safety In Large-Scale Distribution Centers. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *2*(1), 151–192. https://doi.org/10.63125/qen48m30

[107]. Pantelimon, F.-V., Bologa, R., Toma, A., & Posedaru, B.-S. (2021). The evolution of AI-driven educational systems during the COVID-19 pandemic. *Sustainability*, *13*(23), 13501.

[108]. Parah, S. A., Kaw, J. A., Bellavista, P., Loan, N. A., Bhat, G. M., Muhammad, K., & de Albuquerque, V. H. C. (2020). Efficient security and authentication for edge-based internet of medical things. *IEEE Internet of Things Journal*, *8*(21), 15652-15662.

[109]. Partovian, S., Bucaioni, A., Flammini, F., & Thornadtsson, J. (2023). Analysis of log files to enable smart-troubleshooting in industry 4.0: a systematic mapping study. *IEEE access*, *12*, 147640-147658.

[110]. Rahman, A., Hossain, M. S., Muhammad, G., Kundu, D., Debnath, T., Rahman, M., Khan, M. S. I., Tiwari, P., & Band, S. S. (2023). Federated learning-based AI approaches in smart healthcare: concepts, taxonomies, challenges and open issues. *Cluster computing*, *26*(4), 2271-2311.

[111]. Rahman, S. M. T., & Abdul, H. (2022). Data Driven Business Intelligence Tools In Agribusiness A Framework For Evidence-Based Marketing Decisions. *International Journal of Business and Economics Insights*, *2*(1), 35-72. https://doi.org/10.63125/p59krm34

[112]. Rajesh, K., Ajitha, B., Reddy, Y. A. K., Suneetha, Y., & Reddy, P. S. (2018). Assisted green synthesis of copper nanoparticles using Syzygium aromaticum bud extract: Physical, optical and antimicrobial properties. *Optik*, *154*, 593-600.

[113]. Ramakrishnaiah, Y., Macesic, N., Webb, G. I., Peleg, A. Y., & Tyagi, S. (2023). EHR-QC: A streamlined pipeline for automated electronic health records standardisation and preprocessing to predict clinical outcomes. *Journal of biomedical informatics*, *147*, 104509.
[114]. Rao, M. N., Jasim, L., Singh, A. P., & Raajini, X. M. (2023). AI-Based Learning Techniques for Bladder Cancer Detection. 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM),
[115]. Razia, S. (2022). A Review Of Data-Driven Communication In Economic Recovery: Implications Of ICT-Enabled Strategies For Human Resource Engagement. *International Journal of Business and Economics Insights*, *2*(1), 01-34. https://doi.org/10.63125/7tkv8v34
[116]. Razia, S. (2023). AI-Powered BI Dashboards In Operations: A Comparative Analysis For Real-Time Decision Support. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 62–93. https://doi.org/10.63125/wqd2t159
[117]. Razzak, M. I., Imran, M., & Xu, G. (2020). Big data analytics for preventive medicine. *Neural Computing and Applications*, *32*(9), 4417-4451.
[118]. Reduanul, H. (2023). Digital Equity and Nonprofit Marketing Strategy: Bridging The Technology Gap Through Ai-Powered Solutions For Underserved Community Organizations. *American Journal of Interdisciplinary Studies*, *4*(04), 117-144. https://doi.org/10.63125/zrsv2r56
[119]. Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., Sonkamble, R. G., & Dziyauddin, R. A. (2023). Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability*, *15*(8), 6337.
[120]. Rony, M. A. (2021). IT Automation and Digital Transformation Strategies For Strengthening Critical Infrastructure Resilience During Global Crises. *International Journal of Business and Economics Insights*, *1*(2), 01-32. https://doi.org/10.63125/8tzzab90
[121]. Ross, P. T., & Bibler Zaidi, N. L. (2019). Limited by our limitations. *Perspectives on medical education*, *8*(4), 261-264.
[122]. Sadia, T. (2023). Quantitative Analytical Validation of Herbal Drug Formulations Using UPLC And UV-Visible Spectroscopy: Accuracy, Precision, And Stability Assessment. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 01–36. https://doi.org/10.63125/fxqpds95
[123]. Saheb, T. (2023). Ethically contentious aspects of artificial intelligence surveillance: a social science perspective. *AI and Ethics*, *3*(2), 369-379.
[124]. Sai Srinivas, M., & Manish, B. (2023). Trustworthy AI: Explainability & Fairness In Large-Scale Decision Systems. *Review of Applied Science and Technology*, *2*(04), 54-93. https://doi.org/10.63125/3w9v5e52
[125]. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(3), 173.
[126]. Shah, S. M., & Khan, R. A. (2020). Secondary use of electronic health record: Opportunities and challenges. *IEEE access*, *8*, 136947-136965.
[127]. Sharma, S. (2023). Trustworthy artificial intelligence: design of AI governance framework. *Strategic Analysis*, *47*(5), 443-464.
[128]. Sheratun Noor, J., Md Redwanul, I., & Sai Praveen, K. (2024). The Role of Test Automation Frameworks In Enhancing Software Reliability: A Review Of Selenium, Python, And API Testing Tools. *International Journal of Business and Economics Insights*, *4*(4), 01–34. https://doi.org/10.63125/bvv8r252
[129]. Sivasamy, R., Venugopal, P., & Mosquera, E. (2020). Synthesis of Gd2O3/CdO composite by sol-gel method: Structural, morphological, optical, electrochemical and magnetic studies. *Vacuum*, *175*, 109255.
[130]. Staffa, M., Sgaglione, L., Mazzeo, G., Coppolino, L., d'Antonio, S., Romano, L., Gelenbe, E., Stan, O., Carpov, S., & Grivas, E. (2018). An OpenNCP-based solution for secure eHealth data exchange. *Journal of Network and Computer Applications*, *116*, 65-85.
[131]. Syed Zaki, U. (2021). Modeling Geotechnical Soil Loss and Erosion Dynamics For Climate-Resilient Coastal Adaptation. *American Journal of Interdisciplinary Studies*, *2*(04), 01-38. https://doi.org/10.63125/vsfjtt77
[132]. Syed Zaki, U. (2022). Systematic Review Of Sustainable Civil Engineering Practices And Their Influence On Infrastructure Competitiveness. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *2*(1), 227–256. https://doi.org/10.63125/hh8nv249
[133]. Tan, Y., & Zhu, Z. (2022). The effect of ESG rating events on corporate green innovation in China: The mediating role of financial constraints and managers' environmental awareness. *Technology in Society*, *68*, 101906.
[134]. Theodoropoulos, T., Rosa, L., Benzaid, C., Gray, P., Marin, E., Makris, A., Cordeiro, L., Diego, F., Sorokin, P., & Girolamo, M. D. (2023). Security in cloud-native services: A survey. *Journal of Cybersecurity and Privacy*, *3*(4), 758-793.
[135]. Tian, Q., Han, Z., Yu, P., An, J., Lu, X., & Duan, H. (2021). Application of openEHR archetypes to automate data quality rules for electronic health records: a case study. *BMC medical informatics and decision making*, *21*(1), 113.

[136]. Tonoy Kanti, C., & Shaikat, B. (2022). Graph Neural Networks (GNNS) For Modeling Cyber Attack Patterns And Predicting System Vulnerabilities In Critical Infrastructure. *American Journal of Interdisciplinary Studies*, *3*(04), 157-202. https://doi.org/10.63125/1ykzx350
[137]. Urban, R., Haluzová, S., Strunga, M., Surovková, J., Lifková, M., Tomášik, J., & Thurzo, A. (2023). AI-assisted CBCT data management in modern dental practice: benefits, limitations and innovations. *Electronics*, *12*(7), 1710.
[138]. Verma, A., Bhattacharya, P., Madhani, N., Trivedi, C., Bhushan, B., Tanwar, S., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). Blockchain for industry 5.0: Vision, opportunities, key enablers, and future directions. *IEEE access*, *10*, 69160-69199.
[139]. Verma, P., & S. Sangle, P. (2023). Role of Digital Transformation in Inspection and Certification. In *Handbook of Quality System, Accreditation and Conformity Assessment* (pp. 1-29). Springer.
[140]. Vora, L. K., Gholap, A. D., Jetha, K., Thakur, R. R. S., Solanki, H. K., & Chavda, V. P. (2023). Artificial intelligence in pharmaceutical technology and drug delivery design. *Pharmaceutics*, *15*(7), 1916.
[141]. Vrontis, D., & Christofi, M. (2021). R&D internationalization and innovation: A systematic review, integrative framework and future research directions. *Journal of Business Research*, *128*, 812-823.
[142]. Wilkinson, D., Christie, A., Tarr, A. A., & Tarr, J.-A. (2023). Big data, artificial intelligence and insurance. In *The Global Insurance Market and Change* (pp. 22-46). Informa Law from Routledge.
[143]. Wirtz, B. W., Weyerer, J. C., & Kehl, I. (2022). Governance of artificial intelligence: A risk and guideline-based integrative framework. *Government information quarterly*, *39*(4), 101685.
[144]. Wong, E. C., Maher, A. R., Motala, A., Ross, R., Akinniranye, O., Larkin, J., & Hempel, S. (2022). Methods for identifying health research gaps, needs, and priorities: a scoping review. *Journal of General Internal Medicine*, *37*(1), 198-205.
[145]. Wulff, A., Haarbrandt, B., Tute, E., Marschollek, M., Beerbaum, P., & Jack, T. (2018). An interoperable clinical decision-support system for early detection of SIRS in pediatric intensive care using openEHR. *Artificial intelligence in medicine*, *89*, 10-23.
[146]. Yang, C., Chou, T.-C., & Chen, Y.-H. (2019). Bridging digital boundary in healthcare systems—An interoperability enactment perspective. *Computer Standards & Interfaces*, *62*, 43-52.
[147]. Yeng, P. K., Fauzi, M. A., & Yang, B. (2020a). Comparative analysis of machine learning methods for analyzing security practice in electronic health records' logs. 2020 IEEE International Conference on Big Data (Big Data),
[148]. Yeng, P. K., Fauzi, M. A., & Yang, B. (2020b). Workflow-based anomaly detection using machine learning on electronic health records' logs: A comparative study. 2020 International Conference on Computational Science and Computational Intelligence (CSCI),
[149]. Zayadul, H. (2023). Development Of An AI-Integrated Predictive Modeling Framework For Performance Optimization Of Perovskite And Tandem Solar Photovoltaic Systems. *International Journal of Business and Economics Insights*, *3*(4), 01–25. https://doi.org/10.63125/8xm7wa53
[150]. Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K.-K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, *55*(2), 1029-1053.
[151]. Zhou, Y., & Kankanhalli, A. (2021). AI regulation for smart cities: Challenges and principles. In *Smart cities and smart governance: Towards the 22nd century Sustainable City* (pp. 101-118). Springer.
[152]. Zuo, Y., Guo, J., Gao, N., Zhu, Y., Jin, S., & Li, X. (2023). A survey of blockchain and artificial intelligence for 6G wireless communications. *IEEE Communications Surveys & Tutorials*, *25*(4), 2494-2528.