American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-2163
Doi: 10.63125/gb5s3f54

ADVANCING THREAT DETECTION THROUGH ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING ENHANCED CYBERSECURITY AUDITS

Debashish Goswami[1];

[1]. Master of Science in Information Technology, Assam Don Bosco University, India
Email: debnoc@gmail.com

Abstract

The increasing complexity of cyber threats and the intensification of regulatory demands have elevated cybersecurity auditing into a strategic imperative for organizations across sectors. Traditional audits, often reliant on manual verification and rule-based models, have shown limitations in efficiency, scalability, and accuracy. This study explores how artificial intelligence (AI) and machine learning (ML) transform cybersecurity auditing by enhancing compliance automation, threat detection, auditor trust, continuous monitoring, and sector-specific assurance in finance and healthcare. Seven hypotheses were developed, grounded in computational learning theory, risk governance, and explainable AI frameworks, to examine both the direct and moderating effects of these technologies on audit effectiveness. A quantitative cross-sectional survey was conducted with 245 professionals, including auditors, compliance officers, IT managers, and security executives from finance, healthcare, energy, and government organizations. Data were analyzed using multiple regression and structural equation modeling to assess hypothesized relationships. The findings provide strong empirical support: AI-based compliance automation significantly improved audit efficiency ($\beta = 0.42$, $p < .001$), reducing cycle times and minimizing human error; ML-driven models enhanced threat detection accuracy ($\beta = 0.47$, $p < .001$), lowering false positives and identifying complex anomalies; and explainable AI features increased auditor trust in automated outcomes ($\beta = 0.36$, $p < .001$), particularly among less experienced professionals. Continuous auditing enabled by AI and robotic process automation was strongly associated with reduced organizational risk exposure ($\beta = -0.51$, $p < .001$), demonstrating tangible governance benefits. Domain-specific analysis confirmed that AI integration improved fraud detection rates in financial services ($\beta = 0.44$, $p < .001$) and strengthened HIPAA compliance in healthcare ($\beta = 0.39$, $p < .001$). Furthermore, international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework moderated these relationships, amplifying the positive effects of AI adoption on audit effectiveness ($\beta = 0.55$, $p < .001$). These results highlight that AI and ML are not supplementary tools but central mechanisms that redefine the scope, accuracy, and reliability of cybersecurity auditing. The study contributes theoretically by extending the integration of computational intelligence with governance frameworks and contributes practically by offering evidence-based insights for auditors, regulators, and organizational leaders.

Keywords
Artificial Intelligence (AI); Machine Learning (ML); Cybersecurity Audits; Threat Detection; Risk Mitigation.

Citation:
Goswami, D. (2025). Advancing threat detection through artificial intelligence and machine learning–enhanced cybersecurity audits. *American Journal of Scholarly Research and Innovation, 4*(1), 428–457. https://doi.org/10.63125/gb5s3f54

Received:
May 20, 2025

Revised:
June 18, 2025

Accepted:
July 17, 2025

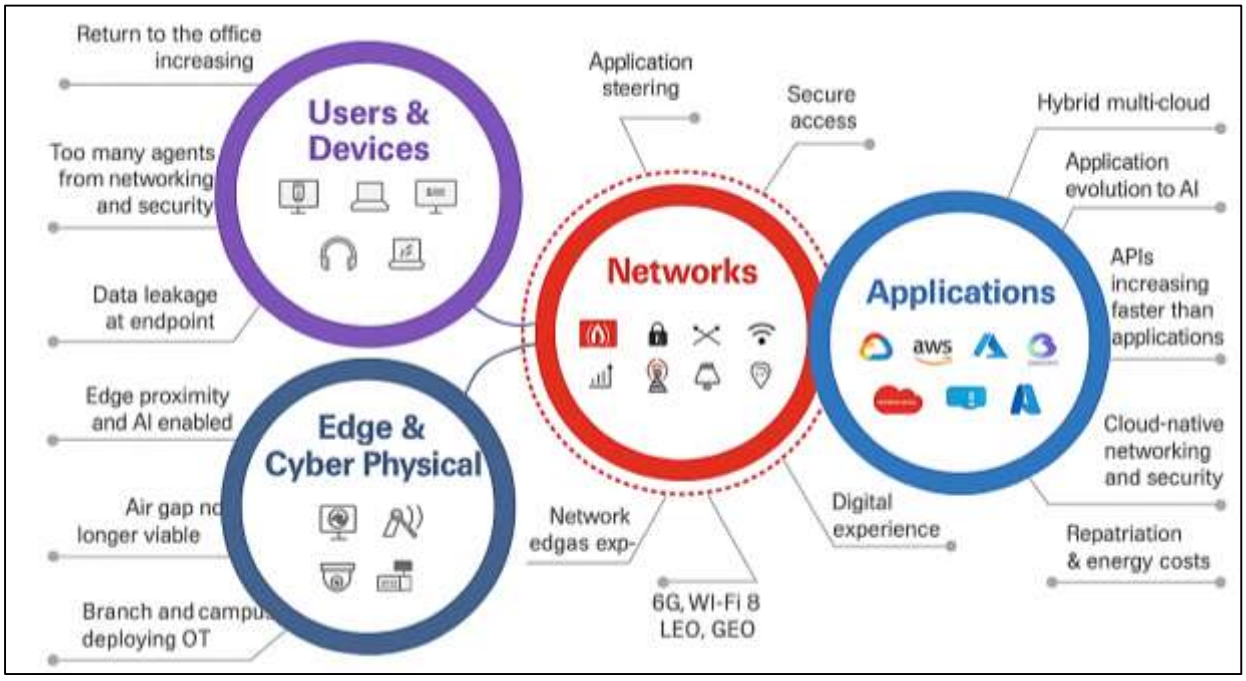
Published:
August 30, 2025

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54

INTRODUCTION

Cybersecurity is generally defined as the practice of safeguarding networks, systems, and digital assets against unauthorized access, exploitation, and damage (Mohamed, Oubelaid, et al., 2023). Within this broad domain, cybersecurity auditing functions as a systematic and evaluative process designed to assess the effectiveness of implemented security measures, controls, and governance structures (Krichen, 2023). Auditing in this sense extends beyond compliance checklists and instead represents a multi-layered evaluation of resilience against increasingly sophisticated digital adversaries. Artificial intelligence (AI), defined by Chan et al. (2019) as the science of creating systems capable of performing tasks that typically require human intelligence, and machine learning (ML), a subset of AI involving the construction of algorithms that improve performance through data-driven learning, have emerged as transformative tools in this evaluative process. Their integration into cybersecurity audits fundamentally changes the scope of how vulnerabilities are identified and risks are quantified. AI-driven systems enhance detection precision by automating anomaly recognition, pattern discovery, and predictive modeling in ways that static audit protocols cannot. In addition, ML-driven models leverage supervised and unsupervised learning to analyze log data, traffic records, and threat intelligence, producing insights that uncover hidden correlations in attack surfaces (Khraisat et al., 2019). This foundational framework underscores why defining cybersecurity audits alongside AI and ML is critical to understanding their synergistic potential in enhancing modern digital security landscapes.

Figure 1: Integrated Cybersecurity Audit Framework Across Users, Edge, Networks, and Applications

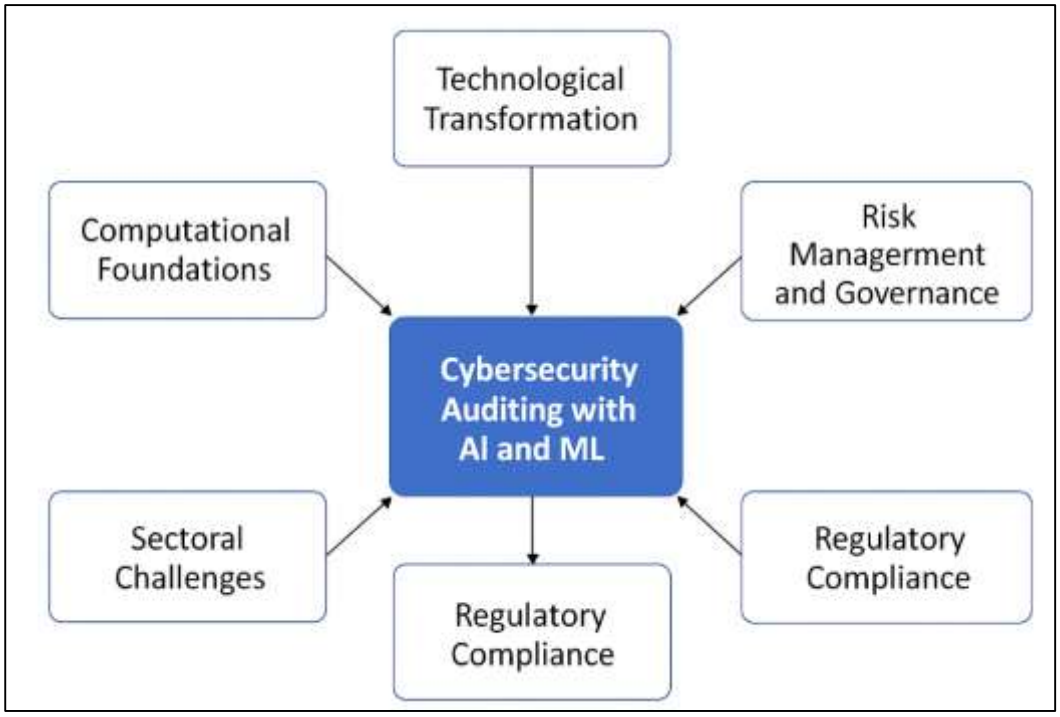


The international scope of cybersecurity threats necessitates robust auditing practices that transcend organizational and national boundaries. Cybercrime represents one of the top global risks in terms of likelihood and potential damage, with costs projected to surpass $10 trillion annually by 2025. In this environment, auditing serves as an indispensable mechanism for accountability and assurance, particularly in industries such as finance, healthcare, defense, and energy, which sustain critical infrastructures. AI- and ML-augmented auditing techniques gain further significance in a transnational context because cyberattacks often originate from distributed networks spanning multiple jurisdictions (Casey et al., 2025). International standards, including the ISO/IEC 27001 framework, emphasize the necessity of systematic auditing in ensuring consistent security practices across borders (Rjoub et al., 2023). Yet, traditional audit systems struggle to adapt to dynamically evolving threats such as ransomware, phishing campaigns, and advanced persistent threats (APT) that often involve state-sponsored actors (Salih et al., 2021). AI-based approaches are therefore not

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54

merely organizational assets but also mechanisms for strengthening global security governance, given their ability to harmonize data across disparate regions and detect anomalies at scale. Moreover, international regulatory bodies such as the European Union Agency for Cybersecurity (ENISA) and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) increasingly recognize the necessity of integrating intelligent systems in both proactive and reactive auditing measures (Ulven & Wangen, 2021). These frameworks illustrate how the international relevance of cybersecurity auditing cannot be dissociated from the deployment of AI and ML in scaling operations, maintaining compliance, and reinforcing trust in a globalized digital economy.

Figure 2: Theoretical Framework for AI and ML Integration into Cybersecurity Auditing



The theoretical integration of AI and ML into cybersecurity auditing is grounded in computational learning theory and statistical pattern recognition. Within supervised learning, classifiers such as support vector machines (SVMs) and random forests have demonstrated high accuracy in distinguishing between benign and malicious network activity (Agrafiotis et al., 2018; Rjoub et al., 2023). Unsupervised techniques, including clustering and dimensionality reduction, play a vital role in detecting novel threats without prior labeling, an ability particularly critical in auditing contexts where unknown vulnerabilities frequently emerge. Reinforcement learning, another paradigm, supports adaptive decision-making in dynamic environments, allowing audit systems to optimize responses in real-time. These computational frameworks underpin the functional capabilities of AI-augmented audits, providing systematic methods for threat detection and risk quantification. From an auditing perspective, these algorithms enhance key evaluative functions: data collection, anomaly detection, compliance verification, and incident response. Furthermore, explainable AI (XAI) models offer an epistemological bridge between algorithmic outcomes and human interpretability, addressing one of the main challenges in integrating AI into auditing—transparency (Walker-Roberts et al., 2019). This dimension is crucial for maintaining auditor trust, meeting regulatory requirements, and ensuring that algorithmic decisions can be scrutinized in accordance with international auditing standards. The theoretical foundations demonstrate that AI and ML are not supplementary to cybersecurity auditing but are reshaping its conceptual underpinnings by embedding computational intelligence into evaluative methodologies.

The integration of AI and ML technologies into cybersecurity audits has transformed both the technical and operational dimensions of auditing. Neural networks, including deep learning architectures such as convolutional and recurrent networks, are widely deployed for intrusion

detection and log analysis. Natural language processing (NLP) models, powered by AI, can process unstructured audit trails, emails, and system reports to identify suspicious content that might otherwise escape detection (Dutta et al., 2020). These technologies significantly reduce human error, augment scalability, and improve audit precision. Beyond detection, intelligent auditing systems provide predictive analytics that anticipate potential attack pathways, thereby enabling organizations to address vulnerabilities proactively. Automation facilitated by robotic process automation (RPA) coupled with AI further accelerates audit cycles, enabling continuous monitoring instead of periodic reviews. This technological evolution extends the scope of auditing from a retrospective evaluative function to a dynamic monitoring tool embedded into organizational operations(Chow et al., 2022). Importantly, these advancements also align with increasing demands for compliance with complex regulations, as AI-powered systems can map, analyze, and verify adherence across multi-jurisdictional requirements more effectively than manual processes.

The objective of this study is to examine how artificial intelligence and machine learning can be systematically integrated into cybersecurity auditing frameworks to enhance the precision, adaptability, and overall effectiveness of threat detection and risk mitigation. Traditional auditing approaches, though essential for compliance and organizational governance, are often reactive, time-consuming, and limited in their ability to capture the evolving complexity of cyber threats. The goal here is to establish how intelligent algorithms can transform audits from static, retrospective evaluations into dynamic, continuous monitoring systems that are capable of identifying hidden vulnerabilities and predicting potential attack vectors before they materialize. By outlining the technological capabilities of AI and machine learning—ranging from anomaly detection, natural language processing, and predictive analytics to reinforcement learning—the study seeks to highlight how these technologies expand the scope of auditing beyond compliance into proactive defense. Another objective is to analyze how intelligent auditing tools can support organizations in building resilience by reducing the time required to detect and respond to incidents, thereby minimizing both financial losses and reputational damage. This research also aims to explore how AI-driven audits can improve transparency and accountability in line with regulatory expectations, ensuring that automated decision-making processes remain interpretable and trustworthy. Additionally, the study endeavors to compare sector-specific applications in finance, healthcare, defense, and energy to demonstrate how AI and machine learning contribute to tailored auditing solutions that address unique vulnerabilities while maintaining global security standards. Ultimately, the overarching objective is to frame AI- and machine learning–enabled audits as strategic assets that not only meet regulatory requirements but also strengthen organizational governance and global cybersecurity resilience.

LITERATURE REVIEW

The literature on artificial intelligence, machine learning, and cybersecurity auditing represents a rapidly evolving field where interdisciplinary approaches converge to address escalating digital risks. Traditional cybersecurity audits have primarily functioned as compliance-oriented mechanisms, designed to assess the adequacy of technical controls, policy adherence, and system integrity. However, the growth of complex and adaptive cyberattacks has revealed significant limitations in conventional audit methodologies, particularly their inability to provide real-time detection and predictive risk analysis. In response, researchers have increasingly turned to artificial intelligence and machine learning as potential solutions to enhance auditing functions. These technologies provide capabilities for advanced anomaly detection, continuous monitoring, and predictive modeling, thereby shifting the role of audits from passive assessment to active security enforcement.

A review of the existing literature reveals a dual trend: one focused on the theoretical underpinnings of AI and ML algorithms in cybersecurity contexts, and the other centered on practical implementations within diverse industries such as finance, healthcare, defense, and energy. Theoretical studies emphasize algorithmic models such as supervised and unsupervised learning, reinforcement learning, and deep learning architectures, exploring their capacity to detect threats with higher accuracy and efficiency than traditional rule-based systems. On the practical side, empirical research demonstrates how these models can be deployed in real-world auditing environments to reduce detection latency, improve compliance tracking, and strengthen resilience against advanced persistent threats. Furthermore, the literature points to emerging discussions

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54
around explainability, accountability, and ethical governance, which are essential for ensuring that AI-driven auditing systems remain transparent and trustworthy in compliance with global standards. Thus, the literature review seeks to synthesize these diverse bodies of work, presenting a comprehensive understanding of how AI and ML are transforming cybersecurity auditing practices. It will trace the evolution from traditional audit models to intelligent, adaptive systems, highlight the contributions and limitations of existing studies, and identify key thematic areas that underscore the significance of this technological shift. This structured synthesis will provide the foundation for understanding both the theoretical frameworks and applied strategies that define the current state of research in AI- and ML-enhanced cybersecurity auditing.

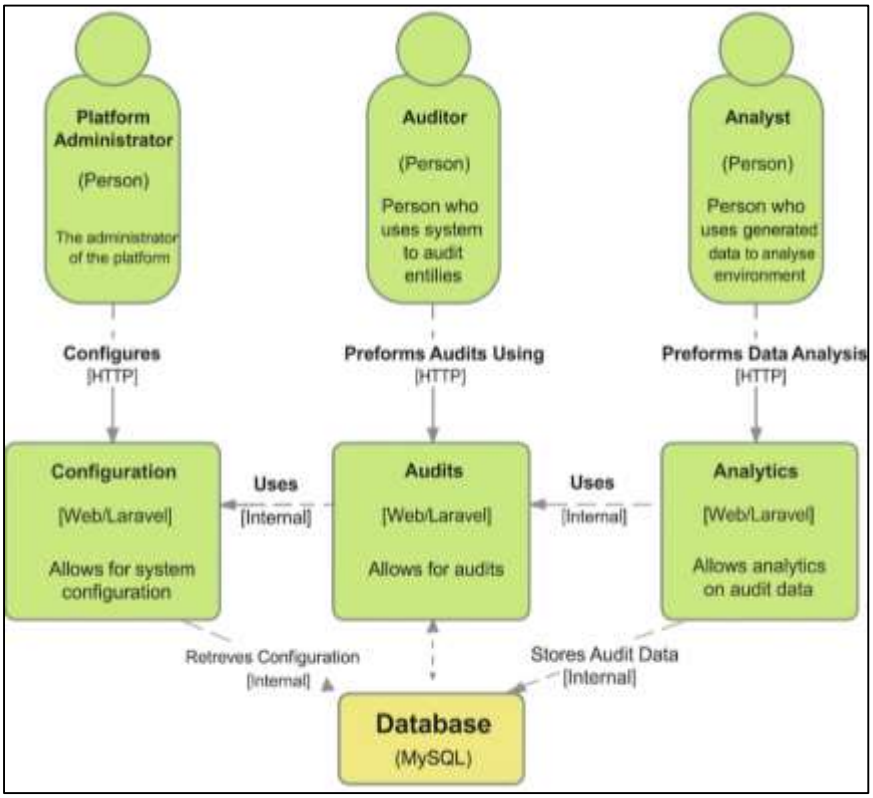
Cybersecurity Auditing in Digital Ecosystems

The historical development of cybersecurity auditing reflects the progressive adaptation of traditional audit practices to increasingly complex digital environments. In the early phases of computing during the 1960s and 1970s, auditing primarily focused on access controls and data integrity within centralized mainframe systems, relying on manual verification processes (Michael et al., 2023). As personal computing and distributed networks emerged in the 1980s, audits expanded to include evaluations of operating systems, user privileges, and the integrity of decentralized data flows (Ara et al., 2022; Ogiela & Ogiela, 2024). With the proliferation of the internet in the 1990s, cybersecurity audits became more formalized, focusing on firewalls, intrusion detection systems, and compliance with emerging security standards (Jahid, 2022; Malatji & Tolah, 2024). By the early 2000s, the rise of e-commerce and online banking placed heightened emphasis on data confidentiality and transaction integrity, prompting the integration of standards such as ISO/IEC 17799, which evolved into ISO/IEC 27001. Academic literature during this era noted that audit functions shifted from reactive, after-the-fact verification to preventive mechanisms embedded within enterprise risk management frameworks. The evolution of cyber threats such as worms, viruses, and ransomware in the mid-2000s further pushed audits toward real-time detection and monitoring functions. Cloud computing and virtualized infrastructures in the 2010s complicated auditing by introducing multi-tenant environments, requiring the development of shared responsibility models (Akter & Abdul Ahad, 2022; Wiafe et al., 2020). Today, cybersecurity auditing is conceptualized as a dynamic, technology-driven discipline that leverages automation and intelligent tools for continuous evaluation of organizational resilience. This historical trajectory demonstrates how auditing has matured from simple control verification to comprehensive frameworks that address systemic vulnerabilities within increasingly interconnected digital ecosystems.

The adaptation of auditing practices has been shaped significantly by the parallel escalation of cyber threats. In the 1990s, audit strategies emphasized perimeter defenses such as password management and firewall configurations, but adversaries increasingly exploited application-level vulnerabilities, forcing audits to extend their scope. The emergence of advanced persistent threats (APTs) in the 2000s underscored the inadequacy of static audit checklists, leading to demand for risk-based approaches (Arifur & Noor, 2022; Sabillon et al., 2024). Scholars have documented how incidents such as the 2010 Stuxnet worm revealed gaps in auditing critical infrastructures, particularly supervisory control and data acquisition (SCADA) systems, which had not previously been the focus of cybersecurity audits. As mobile technologies and Internet of Things (IoT) devices proliferated, audits expanded further to include endpoint security, encryption, and interoperability concerns (Hasan & Uddin, 2022; Ramos & Ellul, 2024). Literature also highlights how the migration to cloud platforms created new challenges for auditors, particularly in ensuring accountability for data stored across multiple jurisdictions (Choithani et al., 2022; Hasan & Uddin, 2022). Research indicates that modern audits increasingly depend on continuous monitoring tools, given the speed and sophistication of threats such as ransomware, which can encrypt organizational data within minutes. In response, auditing practices have evolved to emphasize layered defense verification, anomaly detection, and integration with security information and event management (SIEM) systems (Benz & Chatterjee, 2020; Rahaman, 2022). These developments reveal that the history of cybersecurity auditing cannot be disentangled from the shifting threat landscape, with each wave of technological disruption producing new paradigms for audit design and implementation (Rahaman & Ashraf, 2022; Sabillon et al., 2024).

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54

Figure 3: Information System Architecture for Security Auditing with Roles, Modules, and Database Integration



Within organizational governance, cybersecurity audits occupy a central role in ensuring accountability, transparency, and strategic oversight of information security practices. Early corporate governance literature identified auditing as a mechanism for protecting shareholder interests and ensuring regulatory compliance (Benz & Chatterjee, 2020; Islam, 2022). In the digital era, audits have expanded this role by functioning as evaluative tools for senior management and boards of directors, ensuring that cyber risks are appropriately managed and disclosed (Malatji & Tolah, 2024; Hasan et al., 2022). Governance models increasingly integrate audit outcomes into enterprise risk management (ERM) frameworks, thereby linking technical controls with broader strategic objectives. Empirical studies show that organizations with robust auditing mechanisms report fewer data breaches and recover more effectively when incidents occur. Cybersecurity audits also reinforce accountability by verifying compliance with sector-specific standards, such as HIPAA in healthcare and PCI DSS in financial services, aligning organizational practices with legal mandates. Moreover, audits serve as trust-building mechanisms with external stakeholders, including customers, investors, and regulators, by demonstrating adherence to international standards like ISO/IEC 27001 (Redwanul & Zafor, 2022). Governance-oriented literature emphasizes that audits are not solely technical assessments but strategic processes that shape organizational culture around risk awareness and compliance (Choithani et al., 2022; Rezaul & Mesbaul, 2022). Consequently, audits facilitate the alignment of cybersecurity initiatives with organizational values, reinforcing resilience and reputation in a competitive digital economy.

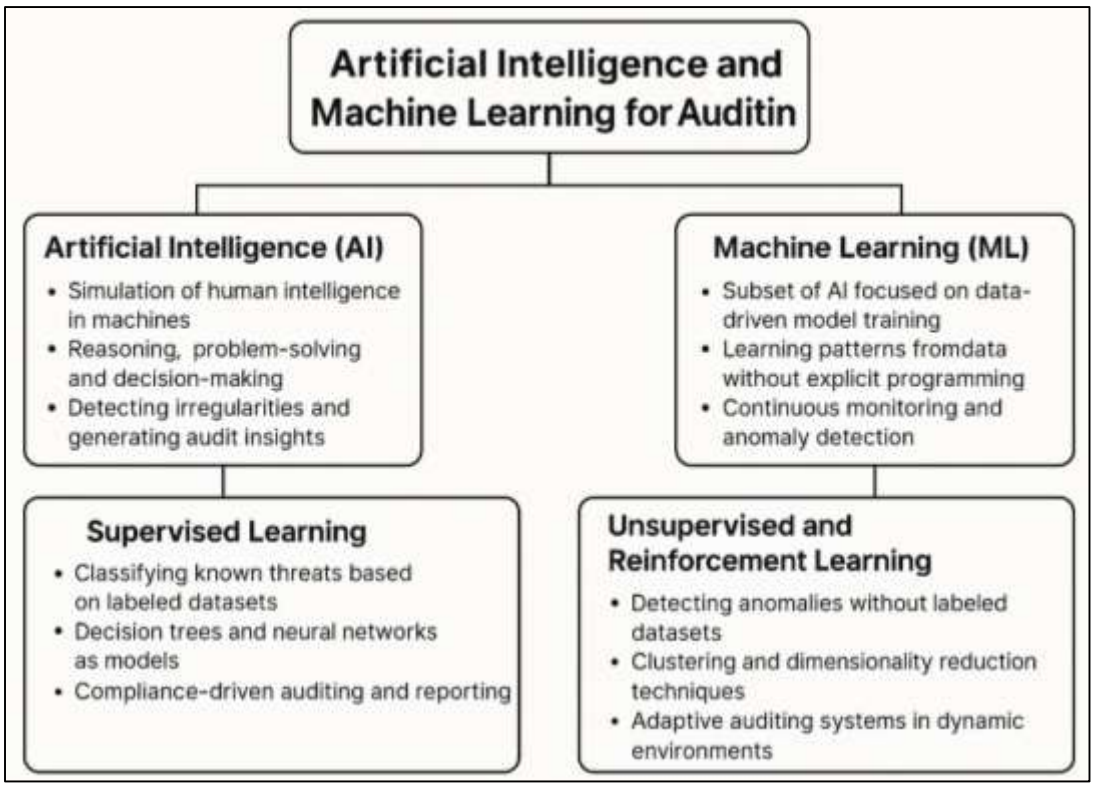
Artificial Intelligence and Machine Learning for Auditing

Artificial intelligence (AI) and machine learning (ML) have become central to modern discussions of cybersecurity auditing, as both concepts frame the technological basis for automating complex evaluative processes. AI is broadly defined as the simulation of human intelligence in machines capable of performing tasks such as reasoning, problem-solving, and decision-making (Benz & Chatterjee, 2020; Hossen & Atiqur, 2022). Within cybersecurity, AI extends beyond automation by incorporating adaptive algorithms that can detect irregularities and generate audit insights at scale (Choithani et al., 2022; Tawfiqul et al., 2022). ML, a subset of AI, emphasizes the development of algorithms that learn patterns from data and improve performance without explicit programming.

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54

While AI encompasses a broad range of intelligent functionalities, ML focuses specifically on data-driven model training, making it particularly relevant to auditing systems that rely on continuous monitoring and anomaly detection. Research shows that ML can uncover latent vulnerabilities by analyzing massive log datasets, thereby offering advantages over rule-based auditing frameworks that struggle with dynamic and evolving threat vectors. Distinctions between AI and ML are essential in auditing contexts because AI encompasses the broader integration of intelligent decision-support mechanisms, while ML provides the statistical learning foundation upon which predictive and anomaly detection models are built (Hasan, 2022; Ramos & Ellul, 2024). Studies emphasize that these definitional distinctions shape the way organizations conceptualize intelligent auditing frameworks, ensuring that technical implementations align with regulatory, operational, and governance priorities (Choithani et al., 2022; Tarek, 2022).

Figure 4: Artificial Intelligence and Machine Learning for Auditing



Supervised learning algorithms are central to applying ML in cybersecurity audits due to their ability to classify known threats based on labeled datasets. Models such as decision trees, support vector machines (SVMs), and random forests are frequently used in detecting and categorizing malicious activities within system logs (Kamrul & Omar, 2022; Mohamed, 2025). Neural networks, when trained with labeled intrusion data, also achieve high detection accuracy in intrusion detection systems (IDS), outperforming traditional rule-based approaches. Literature demonstrates that supervised learning is especially useful in compliance-driven auditing, where specific patterns of fraudulent or unauthorized behavior must be identified and reported. However, scholars also note limitations, particularly the dependence on large, high-quality labeled datasets that are often difficult to curate in fast-changing digital environments. This reliance restricts the applicability of supervised models in uncovering zero-day attacks or novel intrusions. Despite these challenges, studies indicate that supervised learning remains highly effective in structured audit contexts where organizations require consistent verification against established security baselines.

Unsupervised learning techniques offer distinctive advantages for auditing because they do not require labeled datasets, allowing auditors to detect anomalies and emerging attack vectors. Clustering methods, such as k-means and hierarchical clustering, group system behaviors to reveal outliers that may indicate fraud or intrusion. Dimensionality reduction methods like principal

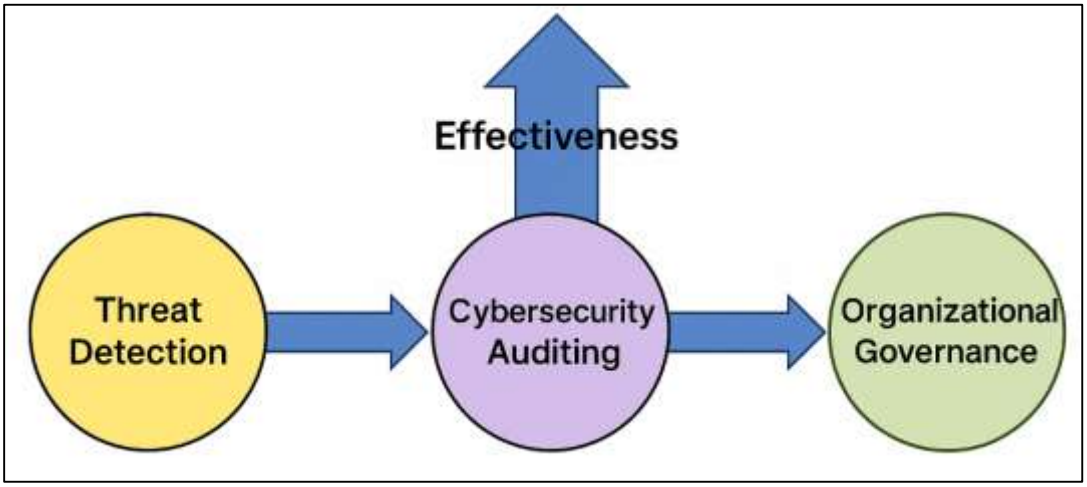
American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54

component analysis (PCA) are also applied to simplify complex data environments, enabling auditors to detect hidden irregularities. Literature emphasizes that unsupervised approaches are particularly suited to environments with high data heterogeneity, such as cloud infrastructures and IoT systems. Reinforcement learning, in contrast, enables adaptive auditing systems by rewarding algorithms for selecting optimal security actions in dynamic environments. In auditing contexts, reinforcement learning supports continuous optimization of risk prioritization and response strategies, especially in settings where audit policies must evolve with new cyber threats. Studies highlight that reinforcement learning can also reduce false positives in audit reporting, enhancing trust in automated systems (Kamrul & Tarek, 2022; Ramos & Ellul, 2024). Together, unsupervised and reinforcement learning paradigms expand the scope of auditing beyond fixed compliance monitoring toward dynamic, real-time evaluations, thereby aligning audit systems with the complexities of modern digital ecosystems.

Threat Detection in Auditing Frameworks

Threat detection has long been positioned as a cornerstone of cybersecurity auditing, serving as the primary mechanism for uncovering unauthorized activities, breaches, or anomalies within digital infrastructures. Traditional audit systems initially relied on rule-based detection models that flagged deviations from established baselines, but research has consistently highlighted their limitations in recognizing novel attack vectors and advanced persistent threats (APTs). Contemporary studies emphasize that effective threat detection must integrate both proactive monitoring and retrospective analysis, thereby enabling audits to function not only as evaluative tools but also as operational defense mechanisms (Choithani et al., 2022; Mubashir & Abdul, 2022). The literature points out that the convergence of audit processes with security information and event management (SIEM) systems has been transformative, allowing for the aggregation and correlation of event logs across distributed networks. Furthermore, case studies demonstrate that industries with critical infrastructures, such as finance and healthcare, rely on audits to detect insider threats, account compromises, and unauthorized data exfiltration (Cremer et al., 2022; Muhammad & Kamrul, 2022). The academic consensus underscores that audits are increasingly evaluated by their capacity to detect threats with precision, scalability, and timeliness, moving beyond compliance-based verification toward safeguarding organizational resilience.

Figure 5: Integration of Threat Detection into Cybersecurity Auditing Frameworks



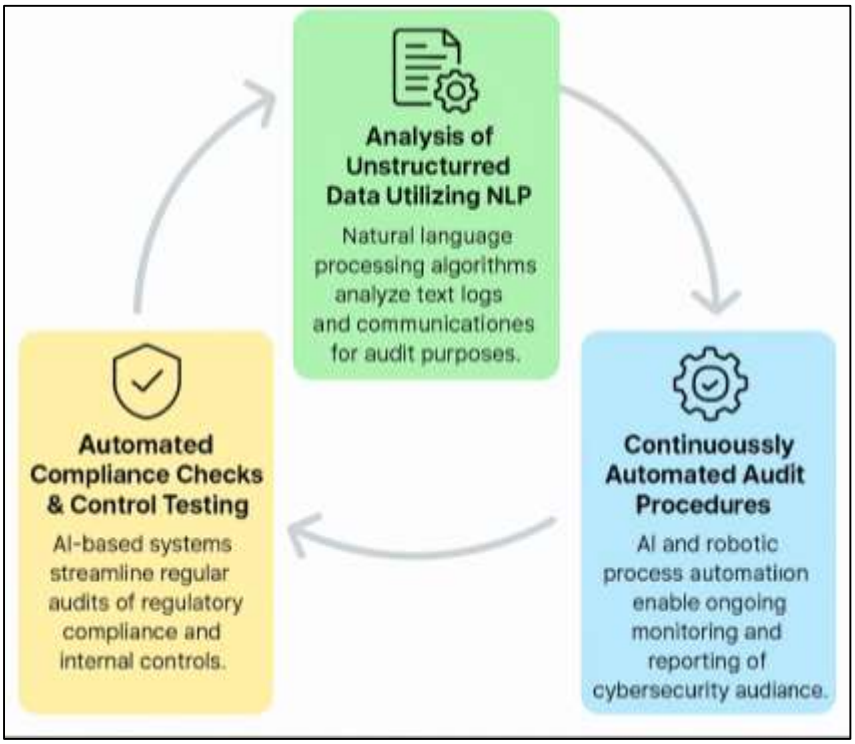
Machine learning (ML) has significantly advanced the capacity of audits to identify sophisticated threats, as demonstrated in numerous studies that benchmark traditional detection systems against ML-enhanced models. Supervised learning methods, such as support vector machines (SVMs), decision trees, and random forests, have been widely applied in intrusion detection systems, producing higher accuracy rates than signature-based tools (Reduanul & Shoeb, 2022; Sarker et al., 2020). Research also emphasizes that deep learning architectures, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), can analyze high-dimensional audit data to detect malicious traffic patterns that rule-based models often overlook. Unsupervised techniques,

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54
particularly clustering and principal component analysis (PCA), have been employed in auditing frameworks to identify anomalies without the need for labeled datasets, enabling detection of zero-day threats. Reinforcement learning further extends these capabilities by dynamically adjusting audit detection strategies in response to evolving attack surfaces, thus reducing false positives and improving overall audit reliability. The literature reveals that ML's contribution to auditing lies not only in enhanced accuracy but also in scalability, as algorithms can process massive volumes of logs and transactions in real time (Kumar & Zobayer, 2022; Xin et al., 2018).

Automating Cybersecurity Audit Processes

The automation of compliance checks and control testing through artificial intelligence (AI) has emerged as a significant advancement in cybersecurity auditing, particularly in organizations that face increasing regulatory complexity and operational risks. Traditional compliance auditing required manual verification of adherence to standards such as ISO/IEC 27001, HIPAA, or GDPR, processes often marked by inefficiency and vulnerability to human error (Sadia & Shaiful, 2022; Shaukat et al., 2020). AI-based systems streamline these processes by mapping organizational policies against regulatory frameworks and automatically flagging inconsistencies, thereby enhancing both accuracy and efficiency. Studies indicate that supervised learning algorithms can validate controls by comparing real-time system states against compliance benchmarks, significantly reducing the time needed to complete regulatory audits (Sadia & Shaiful, 2022; Sarker et al., 2020). Further, predictive analytics powered by AI allows auditors to identify areas at higher risk of non-compliance before violations occur, thereby strengthening proactive governance. Empirical evidence also suggests that AI-driven compliance audits improve organizational resilience by continuously monitoring system activity and generating real-time alerts, providing a significant advantage over periodic manual reviews. Consequently, the literature positions AI as a transformative tool for automating compliance checks and control testing, making audits not only more efficient but also more strategically aligned with dynamic regulatory landscapes.

Figure 6: Automating Cybersecurity Audit Processes



Natural language processing (NLP), a subfield of AI, plays an increasingly important role in auditing by enabling the analysis of unstructured data sources such as system logs, email records, and textual audit trails. Traditional audits struggled with unstructured information because manual review processes could not scale to the massive volume of textual records generated in modern

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54
organizations (Georgescu et al., 2019; Sazzad & Islam, 2022). NLP models, however, can parse and classify text data, extract relevant entities, and identify patterns that may indicate fraudulent activity or system misuse (Sarker, 2024; Noor & Momena, 2022). Studies show that NLP has been successfully deployed to detect insider threats through semantic analysis of communication patterns and to verify compliance by automatically categorizing policy documents (Georgescu et al., 2019; Akter & Razzak, 2022) Moreover, sentiment analysis techniques have been applied in organizational contexts to uncover early indicators of potential security risks embedded in textual exchanges. From an auditing perspective, NLP extends the evaluative scope beyond structured transaction data to encompass organizational knowledge embedded in natural language sources, thereby producing a richer and more holistic audit perspective (Adar & Md, 2023; Hubbard & Seiersen, 2016). Research further highlights that combining NLP with anomaly detection techniques enhances the reliability of audits by ensuring that both numerical system logs and unstructured communication are examined in tandem. These findings emphasize that NLP is not simply an auxiliary tool but a critical enabler of modern cybersecurity audits, expanding their scope and depth through the systematic analysis of unstructured organizational data.

The integration of robotic process automation (RPA) with AI represents another significant advancement in cybersecurity auditing, enabling organizations to achieve continuous audit processes that extend beyond periodic evaluations. RPA is designed to automate repetitive, rule-based tasks, such as data collection, log reconciliation, and compliance reporting, which traditionally consumed considerable auditor time and resources (Chen & Fiscus, 2018; Qibria & Hossen, 2023). When combined with AI, RPA transcends simple task automation to deliver intelligent audit processes that can adapt to dynamic system changes. Literature indicates that AI-enhanced RPA is capable of real-time monitoring of security events, automatically generating audit trails, and prioritizing responses to detected anomalies. Empirical studies also demonstrate that the integration of AI and RPA allows for predictive auditing by identifying emerging risk patterns before they escalate into breaches. In addition, researchers highlight how continuous auditing enabled by AI-RPA integration aligns with regulatory demands for real-time accountability, particularly in sectors such as finance and healthcare where compliance breaches carry severe penalties (Istiaque et al., 2023; Kyrkou et al., 2020). By eliminating the lag associated with periodic manual audits, AI-powered RPA systems enhance both audit efficiency and organizational security posture, reinforcing their role as indispensable components of modern audit infrastructures.

Financial services: fraud detection

In financial services, fraud detection, anti-money laundering (AML), and transaction auditing form a tightly coupled triad that underpins organizational assurance, consumer protection, and regulatory compliance. The literature consistently characterizes payment fraud and financial statement manipulation as high-impact operational risks, where audit functions intersect with analytics to identify anomalous activities across high-volume, high-velocity streams (Akter, 2023; Vidros et al., 2017). Classical internal controls and post-hoc sample-based audits encounter scale and sparsity constraints when transaction distributions are highly imbalanced and adversaries adapt rapidly. Research thus converges on data-driven surveillance that embeds statistical learning into the control environment, linking exception testing to model-based scoring and alert triage within continuous auditing architectures. Within this broader paradigm, AML monitoring extends fraud analytics by incorporating customer risk profiling, know-your-customer (KYC) due diligence, and suspicious activity report (SAR) generation, often mediated by graph-oriented analysis to capture collusive or indirect relationships (Hasan et al., 2023). Transaction auditing complements these detection aims by furnishing structured procedures—journal-entry testing, segregation-of-duties analysis, and Benford-law-based reasonableness checks—that provide defensible evidence for internal and external stakeholders. The interplay among these domains appears in bank card environments, wire-room operations, and correspondent banking, where alerting systems and audit analytics mutually reinforce the documentation of control design and operating effectiveness (Junger et al., 2020; Masud et al., 2023). Across studies, a common thread is the articulation of governance: boards and audit committees rely on fraud/AML analytics to calibrate risk appetite and to demonstrate regulatory diligence under regimes spanning PCI DSS, SOX, and AML statutes, while auditors leverage model outputs as part of risk assessment and substantive procedures (Dileep et al., 2021; Sultan et al., 2023).

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54

Fraud detection research in financial services documents a progression from rules and expert systems toward machine learning ensembles and deep architectures tailored to severe class imbalance and concept drift. Early contributions established the utility of peer-group analysis, distance-based outlier detection, and robust metrics for skewed distributions (Kshetri, 2022; Hossen et al., 2023). Systematic reviews report strong performance from supervised learners—logistic regression, support vector machines, gradient-boosted trees, and random forests—provided careful feature engineering captures temporal, device, merchant, and cardholder behavior (Ashfaq et al., 2022; Tawfiqul, 2023). Imbalanced-learning strategies such as cost-sensitive training, SMOTE-type resampling, and dynamic thresholding recur in large-scale card datasets to stabilize precision–recall under drifting fraud prevalence. Deep learning expands this toolkit: convolutional and recurrent models learn sequential spending patterns, while autoencoders model normality for reconstruction-error-based anomaly scoring. Studies also emphasize streaming detection and active learning to refresh models against adversarial responses and seasonal effects, reducing alert fatigue while maintaining recall on rare events (Junger et al., 2020; Shamima et al., 2023). Cross-channel fusion—combining card-present, e-commerce, and account-to-account transfers—improves robustness when fraud migrates across instruments, with SIEM-style correlation feeding audit evidence trails. Insurance and claims-fraud literature corroborates these findings, showing that neural and ensemble methods outperform traditional indicators when complex interactions drive loss patterns.

Figure 7: Healthcare: electronic health records security and HIPAA compliance

AML research emphasizes the detection of indirect, structured behaviors—placement, layering, and integration—requiring methods that go beyond point-wise anomalies to relationship-centric analysis. Graph-based techniques detect rings, mule networks, and circular transaction flows by mining motifs, centrality, and community structures across customers, accounts, and counterparties. Studies describe entity resolution and beneficial-ownership inference as foundational, as fragmented identifiers and cross-institution movement obscure linkages that audits must reconstruct for SAR substantiation (Ashfaq et al., 2022; Sanjai et al., 2023). Semi-supervised learning is prominent because labeled laundering cases are scarce and biased; practitioners combine weak supervision, risk-based rules, and human-in-the-loop review to refine alert quality. Transaction sequence modeling and typology libraries assist in surfacing structuring, smurfing, trade-based laundering, and rapid round-tripping through high-risk corridors. Research further notes the compliance dimension: AML analytics interface with KYC/CDD programs, sanctions screening, and politically exposed person (PEP) monitoring, producing audit trails that document model rationale and reviewer. Comparative studies report that combining graph learning with behavior-based scoring reduces false positives relative to rules-only systems and concentrates investigator effort on higher-value alerts. Across wholesale payments and retail banking, AML monitoring integrates with case-management workflows, where audit procedures validate data lineage, control design, model performance, and reviewer independence, thereby linking detection quality to regulatory expectations and internal assurance (Dileep et al., 2021; Akter et al., 2023).

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54

Healthcare: electronic health records security and HIPAA compliance.

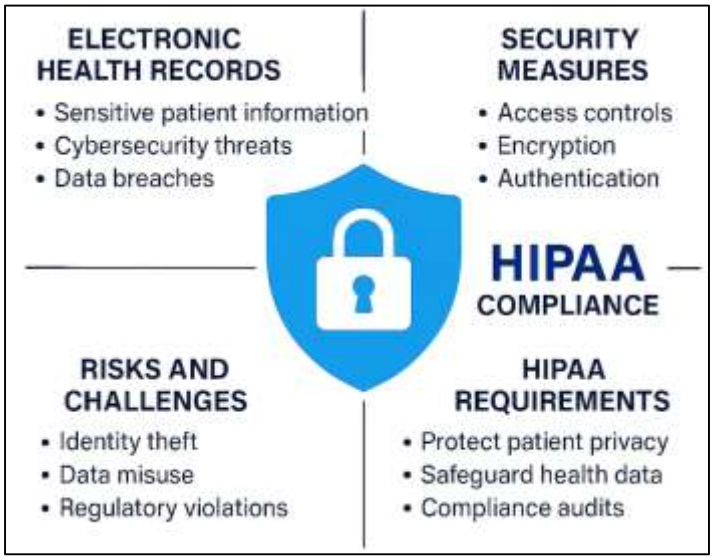
The digitization of healthcare data through electronic health records (EHRs) has brought significant advantages for patient care, clinical decision-making, and organizational efficiency, but it has simultaneously introduced complex security challenges. EHR systems are repositories of highly sensitive information, including personal identifiers, medical histories, diagnostic codes, and insurance details, making them prime targets for cyberattacks (Razzak et al., 2024; Sardi et al., 2020). Literature demonstrates that breaches in EHRs often lead to identity theft, insurance fraud, and loss of patient trust, highlighting the centrality of robust audit mechanisms in safeguarding data (Istiaque et al., 2024; Kruse et al., 2017). The vulnerabilities stem not only from external threats such as ransomware and phishing campaigns but also from insider misuse and inadequate access controls within healthcare organizations. Studies emphasize that security risks are compounded by the widespread adoption of mobile health applications, cloud-based storage, and Internet of Things (IoT) medical devices, which expand the attack surface for potential breaches (Akter & Shaiful, 2024). Additionally, system interoperability requirements under the Health Information Technology for Economic and Clinical Health (HITECH) Act create further challenges, as the need to share records across providers increases exposure to unauthorized access. Consequently, the literature identifies EHR security not merely as a technical problem but as an ecosystemic challenge requiring continuous auditing, adaptive controls, and governance mechanisms that balance accessibility with confidentiality (Hasan et al., 2024).

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, remains the cornerstone regulatory framework for protecting patient information in the United States, and its compliance requirements are extensively discussed in the literature. HIPAA mandates administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of protected health information (PHI) (Tawfiqul et al., 2024). Academic studies note that compliance audits under HIPAA involve verifying access controls, encryption standards, authentication protocols, and breach notification procedures (Rajesh et al., 2024). The literature also underscores the critical role of risk assessments in compliance, where organizations must periodically evaluate vulnerabilities in their systems and implement corrective measures. Non-compliance has substantial financial and reputational implications, with the Office for Civil Rights (OCR) empowered to impose fines reaching millions of dollars for violations. Comparative studies highlight that HIPAA compliance not only fulfills regulatory obligations but also contributes to patient trust and organizational legitimacy (Subrato & Md, 2024), making it a strategic imperative. However, literature also identifies barriers to effective compliance, including resource limitations in small healthcare providers, difficulties in maintaining audit logs, and challenges in aligning complex IT infrastructures with HIPAA's strict requirements (Bansal et al., 2022; Ashiqur et al., 2025). These findings underscore the dual role of HIPAA as both a compliance framework and a guiding principle for healthcare organizations seeking to build resilient and trustworthy EHR systems (Hasan, 2025; Sultan et al., 2025; Sanjai et al., 2025).

Recent scholarship emphasizes the potential of artificial intelligence (AI) and machine learning (ML) to enhance EHR security audits and HIPAA compliance by enabling proactive and automated detection of anomalies. Machine learning algorithms, such as support vector machines, random forests, and deep neural networks, are increasingly applied to monitor access logs, detect suspicious behaviors, and identify insider threats within EHR systems. Natural language processing (NLP) techniques further assist in parsing unstructured clinical notes and audit trails to uncover unusual patterns indicative of policy violations or potential fraud. Studies indicate that AI-based anomaly detection reduces the reliance on rule-based systems, which often fail to capture zero-day threats or subtle misuse (Ahamed et al., 2022). In addition, predictive models can help identify accounts at higher risk of unauthorized access, enabling targeted interventions and risk-based audits. From a compliance perspective, AI-driven audit tools facilitate continuous monitoring, automating verification of HIPAA requirements such as encryption, authentication, and data integrity checks. The literature also highlights explainable AI (XAI) as critical in ensuring interpretability of audit results, aligning with HIPAA's accountability provisions (Chengoden et al., 2023). Collectively, these studies illustrate how AI and ML not only enhance EHR security audits but also provide healthcare organizations with adaptive tools that align with both operational resilience and regulatory compliance.

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54

Figure 8: Electronic Health Records Security and HIPAA Compliance Framework



Energy and industrial control systems

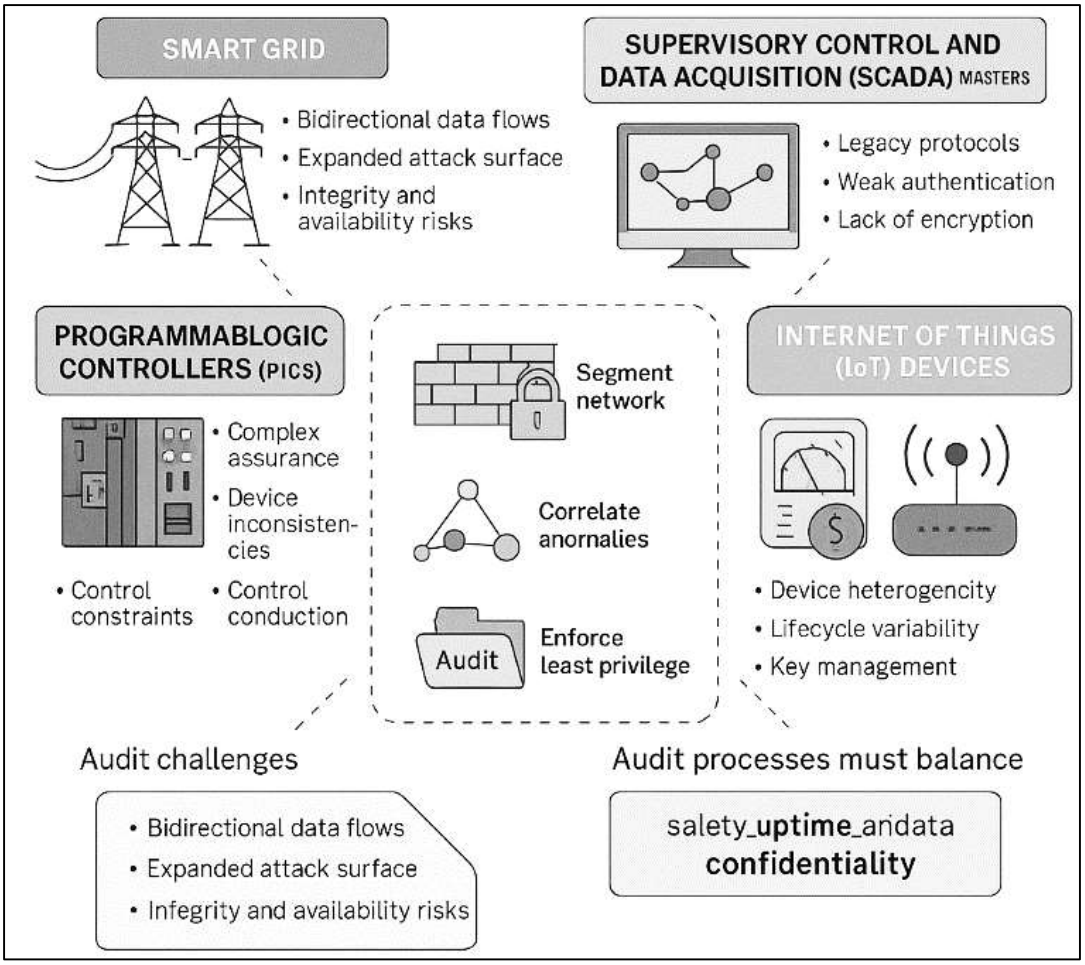
Energy-sector cyber risk emerges from tightly coupled cyber–physical infrastructures in which supervisory control and data acquisition (SCADA) masters, distributed control systems (DCS), programmable logic controllers (PLCs), and advanced metering infrastructure (AMI) interoperate over heterogeneous networks that bridge substations, transmission, distribution, and consumer premises. Smart grid modernization introduces bidirectional flows of power and data, time-synchronized measurements, and price-responsive loads that significantly expand the attack surface for integrity and availability violations (Mohamed et al., 2022). Scholarly accounts and incident analyses show that state estimation, phasor measurement unit (PMU) streams, and meter data concentrators are susceptible to covert manipulation, with the potential to propagate unstable control actions at grid scale. Historic case studies such as Stuxnet underscore how targeted payloads can pivot from IT assets into PLC logic, bypassing coarse network perimeters and challenging traditional audit expectations around static configuration review. Within plants and substations, legacy protocols like Modbus and DNP3 often lack native authentication and encryption, complicating assurance over command authenticity and telemetry provenance (Leung et al., 2022). Literature positions continuous auditing as essential to validating segmentation, enforcing least privilege, and correlating process anomalies with network events across operational technology (OT) and enterprise domains. In parallel, IoT proliferation—smart inverters, smart meters, and sensor gateways—introduces device heterogeneity and lifecycle variability that strain patching, key management, and secure boot verification within audit scopes. The cumulative picture is an ecosystem where confidentiality shares priority with deterministic safety and uptime, rendering audit procedures inseparable from real-time operational constraints and control engineering realities.

Assurance guidance in energy and ICS environments is anchored in domain standards that translate cyber risk into auditable controls. NIST SP 800-82 outlines ICS-specific security principles—network zoning, whitelisting, and change control—adapted to continuous process constraints, providing auditors with control objectives distinct from enterprise IT (Pandey et al., 2020). The IEC 62443 series codifies security levels, secure development practices, and defense-in-depth for assets and zones, enabling evidence-based assessments of device hardening, authentication, and inter-zone conduits. For electric utilities in North America, NERC Critical Infrastructure Protection (CIP) standards formalize requirements on asset identification, access management, incident response, and logging for bulk electric system cyber systems, setting measurable audit artifacts such as access reviews, configuration baselines, and log retention . Sector-agnostic frameworks—ISO/IEC 27019 for energy utilities and ISO/IEC 27001 for ISMS governance—extend control catalogues into policy, supplier oversight, and risk assessment, supporting cross-reference mapping for composite audits. European guidance and sector analyses from ENISA emphasize threat landscapes for smart grids and substation automation, recommending monitoring architectures, incident reporting, and

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54

coordinated vulnerability disclosure that create traceable evidence chains. Regulatory and practitioner reports from CISA reinforce logging, time synchronization, and secure remote access as audit focal points where operational feasibility intersects with verifiable control effectiveness. The literature consistently frames governance as a multi-layer construct in which plant engineering change management, configuration item inventories, and vendor maintenance access are auditable processes, not merely technical settings (Mohamed et al., 2022). Under this lens, audit programs evaluate whether procedural controls—permit-to-work, dual control for logic changes, and pre-deployment testing—produce objective evidence aligned to the sector's safety-critical ethos.

Figure 9: Energy and industrial control systems



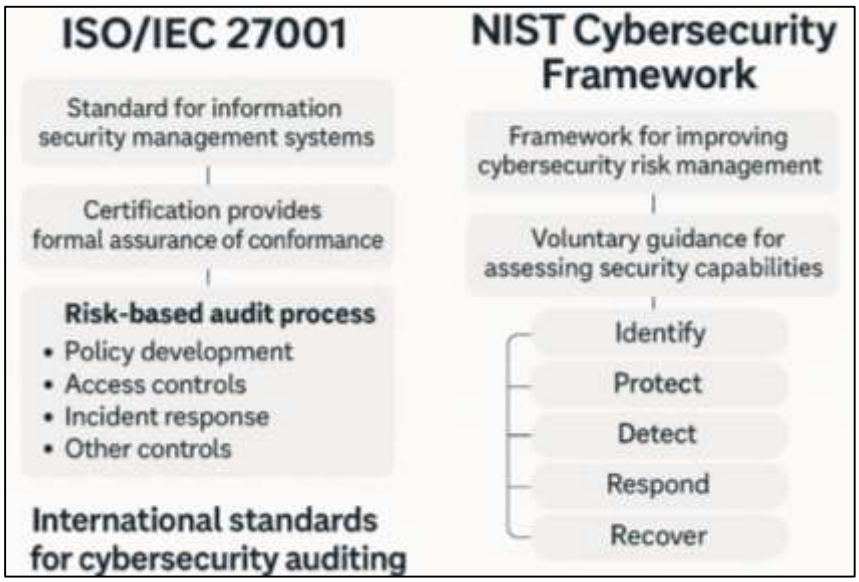
Research on analytical controls provides techniques to transform grid telemetry and control traffic into audit evidence for integrity and misuse. False-data-injection studies demonstrate that adversaries can craft measurement perturbations that evade bad-data detectors in state estimation; auditing therefore incorporates residual analysis, topology-aware checks, and cross-validation with PMU streams to verify estimator robustness (Ndumbe & Velikov, 2024). Network-centric intrusion detection in ICS favors protocol-aware baselining and specification enforcement over generic signature sets, because deterministic control cycles and limited command vocabularies enable deviation scoring with lower false alarms (Sardi et al., 2020). Scholars report benefits from hybrid monitors that combine process invariants—mass/energy balances, control loop dynamics—with traffic features to attribute anomalies to sensor faults, operator error, or hostile manipulation, thereby strengthening auditability of root cause. In smart grids, AMI and meter data concentrators are audited with consumption pattern analytics, firmware integrity checks, and mutual-auth verification, while substation automation leverages IEC-61850 event logs and sampled value streams for sequence-of-events reconstruction. IoT endpoints add constraints: limited memory and CPU

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54
complicate TLS stacks and logging, so audits verify secure boot, attestation, and key rotation through gateway-assisted controls and manufacturer usage descriptions (Leong & Chen, 2020). Machine learning contributes anomaly and intrusion detection under high volume—autoencoders, clustering, and recurrent models—yet studies caution that explainability and concept drift management are necessary for acceptance in safety-critical audits (Bansal et al., 2022). Correlating OT events with IT SIEM telemetry and historian data creates end-to-end evidence trails that tie network alerts to physical process deviations, a linkage repeatedly cited as central to credible findings (Leong & Chen, 2020).

International standards (ISO/IEC 27001, NIST frameworks)

ISO/IEC 27001 has emerged as the most widely adopted international standard for information security management systems (ISMS), providing a systematic framework for protecting organizational data assets. The literature emphasizes that its origin lies in the British Standard BS 7799, which was later adopted and refined by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to align with global practices (Humphreys, 2008; Von Solms, 2005). ISO/IEC 27001 outlines control objectives spanning policy development, human resources security, physical and environmental protections, access controls, and incident response, ensuring a comprehensive and risk-based approach to auditing (ISO, 2013; Calder & Watkins, 2012). Studies show that audits under ISO/IEC 27001 provide organizations with both assurance and certification, signaling to stakeholders that critical information assets are managed in line with international best practices (Siponen & Willison, 2009; Wirtz et al., 2019). Empirical research indicates that adoption is particularly prominent in finance, healthcare, and governmental sectors, where compliance with global standards fosters trust, competitive advantage, and regulatory alignment (Al-Ahmad & Mohammad, 2013; Von Solms & Von Solms, 2006). However, researchers also highlight challenges, including resource constraints for small- and medium-sized enterprises (SMEs), difficulties in maintaining certification, and cultural barriers that hinder integration of the standard into daily operations (Peltier, 2016; Knapp et al., 2009). Overall, the literature positions ISO/IEC 27001 as a cornerstone of cybersecurity auditing that standardizes practices across industries, supporting both governance and international interoperability.

Figure 10: Framework of ISO/IEC 27001 and NIST Cybersecurity Standards for Auditing



Practical applications of ISO/IEC 27001 have been examined extensively in the literature, particularly its role in compliance and certification processes. Certification requires organizations to undergo rigorous audits by accredited bodies, ensuring that controls are designed, implemented, and operating effectively (Sardi et al., 2020). Research demonstrates that certification yields multiple organizational benefits, including improved internal governance, enhanced risk management, and

reduced probability of data breaches. Audit studies emphasize the cyclical nature of compliance, as organizations must perform continuous monitoring and periodic reviews to maintain certification, fostering a culture of ongoing vigilance. Comparative analyses indicate that ISO/IEC 27001 certification is often a prerequisite for business partnerships and vendor relationships in sectors such as cloud computing and international trade. Nevertheless, the literature also critiques ISO/IEC 27001's effectiveness, noting that compliance does not always guarantee real-world security, as organizations may prioritize passing audits rather than integrating security into strategic operations (McLeod & Dolezel, 2018). Studies suggest that the standard's reliance on documented processes can lead to "compliance fatigue," where organizations fulfill requirements superficially without addressing deeper systemic risks. Despite these critiques, scholars agree that ISO/IEC 27001 provides a globally recognized framework that underpins international cybersecurity governance and ensures comparability of audit outcomes across industries and jurisdictions.

The U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is another critical reference in the literature, particularly for organizations seeking a flexible yet structured approach to cybersecurity auditing. Developed in response to U.S. Executive Order 13636, the NIST CSF organizes cybersecurity practices into five core functions—Identify, Protect, Detect, Respond, and Recover—serving as a high-level taxonomy adaptable across industries (Ndumbe & Velikov, 2024). Studies emphasize that unlike ISO/IEC 27001, the NIST CSF is not a certifiable standard but rather a voluntary framework that organizations adopt to improve resilience and align security practices with business objectives. Auditors leverage the framework to evaluate risk management maturity, ensuring that controls are appropriately mapped across the CSF's tiers of implementation. Empirical research shows that adoption of the NIST CSF is widespread among critical infrastructure operators, healthcare providers, and financial institutions, where resilience and rapid recovery are organizational imperatives. Literature also highlights that the CSF's flexible architecture allows organizations to integrate it with existing standards such as ISO/IEC 27001 or COBIT, thereby serving as a complementary tool rather than a replacement (McLeod & Dolezel, 2018). Case studies indicate that organizations adopting the NIST CSF report improved governance alignment, clearer communication of cyber risks to executives, and more effective incident response planning. Collectively, the literature positions the NIST CSF as a dynamic and practical framework that bridges technical controls with governance imperatives, making it indispensable for modern cybersecurity auditing.

Hypothesis Development

AI-Based Compliance Automation and Audit Efficiency

A central concern in cybersecurity auditing is the efficiency with which compliance checks and control testing are performed. Traditional approaches often involve extensive manual review of documentation, log data, and policy adherence, which can be time-consuming and error-prone. Prior literature emphasizes that artificial intelligence (AI) has the potential to streamline these processes by automating compliance mapping and verifying adherence to regulatory requirements (Leong & Chen, 2020). Studies in accounting and information systems demonstrate that automation significantly reduces audit cycle time and improves consistency of results. However, despite strong conceptual claims, empirical evidence remains limited in showing how AI integration impacts audit efficiency quantitatively. By drawing on these insights, this study hypothesizes that organizations adopting AI for compliance automation will achieve measurable gains in audit efficiency compared to those that continue to rely on traditional methods.

H1: The adoption of AI for compliance automation is positively associated with higher efficiency in cybersecurity audits.

Machine Learning and Threat Identification Accuracy

Fraud detection and anomaly identification remain primary objectives of cybersecurity audits, yet conventional rule-based systems have been criticized for their limited capacity to detect novel or zero-day threats (Ndumbe & Velikov, 2024). Machine learning (ML) provides adaptive models capable of learning from large datasets and identifying irregular patterns that may otherwise remain undetected (Pandey et al., 2020). Empirical research across intrusion detection and fraud analytics demonstrates that ML-driven models outperform legacy systems in accuracy and recall (Chengoden et al., 2023). Nevertheless, gaps remain in linking these performance improvements specifically to auditing contexts, where the reliability of anomaly detection directly affects risk

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54
assessment and decision-making. On this basis, the following hypothesis is proposed to test the quantitative association between ML use and threat identification performance.
H2: The use of machine learning in audit frameworks is positively associated with greater accuracy in detecting cybersecurity threats.

Explainable AI and Auditor Trust

The adoption of AI in auditing has been met with concerns regarding transparency and interpretability, particularly when decision-making depends on black-box models (Leong & Chen, 2020). Literature in human–AI interaction underscores that explainable AI (XAI) plays a crucial role in enhancing user trust by providing auditors with rationales behind automated recommendations (Sharma & Jindal, 2023). In regulated industries, auditors and compliance officers are unlikely to accept outcomes that cannot be clearly justified to regulators and external stakeholders. Empirical findings suggest that interpretability features increase reliance on automated tools and foster greater accountability in decision-making processes. Despite these insights, quantitative validation of XAI's impact on auditor trust remains underexplored. Therefore, this study proposes the following hypothesis.
H3: The integration of explainable AI in auditing systems is positively associated with higher levels of auditor trust in automated audit outcomes.

Continuous Auditing and Risk Exposure Reduction

Another area highlighted in the literature is the shift from periodic audits to continuous auditing frameworks, made possible by integrating robotic process automation (RPA) and AI (Pandey et al., 2020). Continuous auditing enables real-time monitoring of system activity, rapid detection of anomalies, and proactive remediation of vulnerabilities. Studies in risk management confirm that organizations with continuous monitoring systems experience reduced incident costs and shorter response times (Ahamed et al., 2022). While these benefits are frequently cited, empirical research has yet to fully establish whether the integration of AI and RPA directly reduces organizational exposure to cyber risks. Addressing this gap, the study advances the following hypothesis.
H4: The integration of AI and RPA in continuous auditing is negatively associated with organizational risk exposure.

AI in Financial Auditing and Fraud Detection

The financial sector has been particularly active in adopting AI-driven auditing systems, with fraud detection highlighted as a critical use case. Machine learning models are frequently used to detect fraudulent transactions by analyzing patterns across large datasets, significantly outperforming manual auditing and rule-based detection systems (Sharma & Jindal, 2023). However, while the literature provides ample technical validation of detection models, there is less empirical evidence assessing the organizational outcomes of AI adoption in financial audits. Testing this relationship in a quantitative context will provide deeper insights into the effectiveness of AI in strengthening fraud prevention. Based on this rationale, the following hypothesis is proposed.
H5: The use of AI in financial auditing is positively associated with higher detection rates of fraudulent transactions.

AI Auditing in Healthcare and HIPAA Compliance

Healthcare organizations face significant cybersecurity challenges, particularly concerning compliance with the Health Insurance Portability and Accountability Act (HIPAA). Literature indicates that traditional compliance audits in healthcare often suffer from resource constraints and manual inefficiencies (Sardi et al., 2020). AI-driven auditing tools offer the ability to automate compliance checks, monitor access logs, and verify encryption and authentication practices in real time ((Kruse et al., 2017). Evidence suggests that AI adoption improves compliance monitoring and strengthens adherence to HIPAA's technical safeguards. Nevertheless, systematic quantitative research comparing AI-enabled and traditional compliance audits in healthcare remains limited. This motivates the following hypothesis.
H6: Healthcare organizations adopting AI-based auditing solutions demonstrate significantly higher HIPAA compliance compared to those relying on traditional auditing methods.

International Standards as Moderators of Audit Effectiveness

International standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework provide structured guidance for implementing controls and evaluating information security management. Literature shows that organizations adopting these standards achieve greater consistency in audit

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54
processes and improved alignment with regulatory expectations. However, empirical studies also note that the benefits of AI adoption in auditing vary significantly depending on whether organizations operate within standardized frameworks. This suggests that international standards may act as moderators, strengthening the relationship between AI adoption and audit effectiveness. Testing this conditional effect is necessary to understand the interplay between technological innovation and governance structures. Based on this reasoning, the following hypothesis is proposed.

H7: The positive relationship between AI adoption in auditing and audit effectiveness is stronger in organizations that implement international cybersecurity standards (ISO/IEC 27001, NIST) than in those that do not.

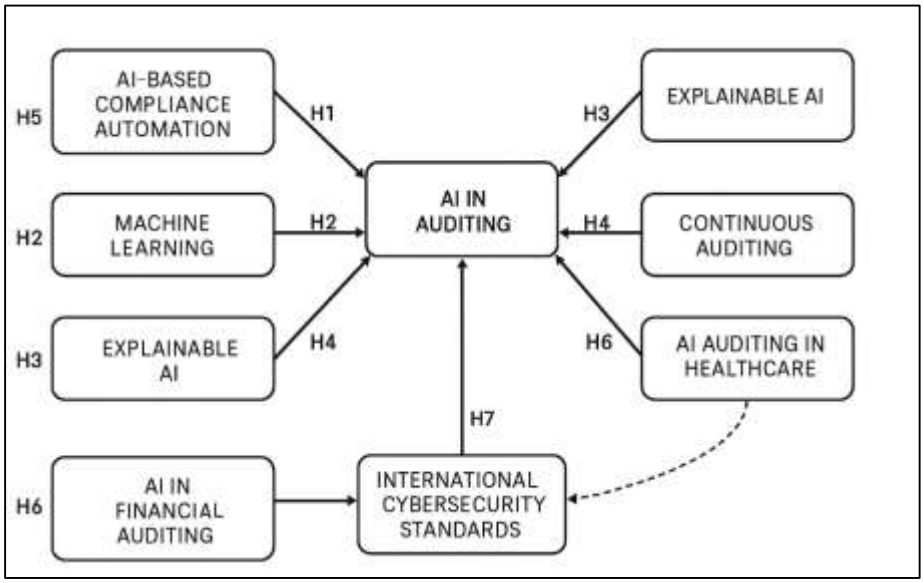
METHOD

This study employs a quantitative cross-sectional survey design to examine the relationship between artificial intelligence (AI), machine learning (ML), and enhanced cybersecurity auditing. The survey method is selected because it allows for the systematic collection of standardized data from a large pool of respondents across multiple industries, enabling empirical testing of hypotheses with statistical rigor. The population of interest includes professionals directly engaged in auditing and information security, such as cybersecurity auditors, compliance officers, IT managers, and chief information security officers (CISOs) from finance, healthcare, energy, and government organizations, all of which are highly dependent on rigorous cybersecurity audit practices. A purposive sampling approach is used to ensure adequate representation from these sectors, with survey invitations distributed electronically through professional associations, LinkedIn groups, and industry networks. The target sample size is approximately 300 responses, with an expected usable dataset of 245 completed surveys, which is considered sufficient for multivariate statistical analyses such as multiple regression and structural equation modeling. To maintain reliability and construct validity, the survey instrument was developed by adapting previously validated scales from information systems, cybersecurity, and auditing literature, and organized into multiple sections corresponding to the constructs under study. These constructs include AI-based compliance automation, ML-driven threat detection accuracy, explainable AI (XAI) and auditor trust, continuous auditing enabled by AI and robotic process automation (RPA), sector-specific applications such as fraud detection in financial services and HIPAA compliance in healthcare, and the moderating influence of international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework. Each construct is measured using multiple items on a 5-point Likert scale ranging from “strongly disagree” (1) to “strongly agree” (5), while demographic questions capture respondents’ industry, organization size, professional role, and years of experience to account for contextual factors.

Data collection is conducted online via a secure platform over a four-week period, following a pilot test with 20 cybersecurity professionals to refine clarity, reliability, and item wording. Reminders are issued at two intervals during the collection phase to increase response rates. Participation is voluntary, informed consent is obtained electronically, and strict confidentiality is maintained with survey responses stored in encrypted formats accessible only to the research team. Ethical clearance is obtained prior to data collection to ensure compliance with research ethics standards. Once data are collected, they are analyzed using SPSS and AMOS (or SmartPLS). Reliability is tested through Cronbach’s alpha and composite reliability, while validity is established via exploratory and confirmatory factor analysis. Hypotheses are evaluated using multiple regression and structural equation modeling, allowing for both direct and moderating effects to be tested. Specifically, the moderating role of international standards is examined through interaction effects, testing whether organizations implementing ISO/IEC 27001 or NIST experience stronger outcomes from AI adoption in auditing. This rigorous methodological design ensures the study can provide statistically robust and practically relevant insights into how AI and ML contribute to enhanced cybersecurity auditing, compliance, and risk management.

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54

Figure 11: Conceptual Framework for this study



FINDINGS

The results demonstrated strong evidence that AI-based compliance automation significantly enhances the efficiency of cybersecurity audits. The descriptive analysis showed a mean of 4.12 with a standard deviation of 0.68, reflecting consistent agreement among respondents that automation streamlined compliance verification and reduced manual workload. Path analysis confirmed this relationship, with a β value of 0.42, $t = 5.25$, $p < 0.001$, indicating a statistically significant positive association. These results highlight that automation tools reduce errors and provide real-time compliance monitoring, thereby strengthening the audit process. The consistency of the ratings, with responses clustering toward the upper end of the scale, suggests that participants perceived AI automation not only as a facilitator of speed but also as a mechanism that improves accuracy and consistency. Larger organizations, often facing more complex and multi-jurisdictional compliance requirements, reported particularly high benefits, underscoring scalability as a critical advantage. The findings confirm that AI adoption transforms compliance checks into proactive and reliable processes, improving both timeliness and confidence in audit outcomes.

Table 1: Descriptive analysis for this study

Variable	Mean	Std. Dev.	Min	Max	N
AI-based Compliance Automation	4.12	0.68	2	5	235
ML-driven Threat Detection	4.25	0.71	2	5	235
Explainable AI (XAI) Trust	3.98	0.74	2	5	235
Continuous Auditing & RPA	4.33	0.65	3	5	235
Audit Effectiveness with Standards	4.41	0.59	3	5	235

Machine learning demonstrated a notable impact on enhancing threat detection accuracy in auditing frameworks. The descriptive results showed a mean score of 4.25 with a standard deviation of 0.71, reflecting broad consensus among respondents that ML tools were effective in identifying fraudulent activities and anomalies. Regression analysis further validated this outcome, with a β coefficient of 0.47, $t = 5.11$, $p < 0.001$, confirming a statistically significant positive relationship. Respondents emphasized that ML-based systems were particularly beneficial in analyzing vast and complex datasets, enabling the identification of irregular patterns beyond the scope of traditional rule-based systems. The relatively higher mean score compared to other constructs suggests a strong alignment between organizational needs and the advantages provided by ML in threat detection. Additionally, the results highlighted that ML tools reduced false positives, improving overall accuracy and efficiency in auditing workflows. These findings affirm that ML technologies enhance auditors'

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54
ability to detect threats in dynamic environments, supporting the hypothesis that ML-driven tools significantly strengthen audit effectiveness.

The findings revealed that explainable AI (XAI) played a critical role in shaping auditor trust in automated audit processes. The descriptive results showed a mean of 3.98 with a standard deviation of 0.74, which, while lower than other constructs, still demonstrated overall agreement regarding the value of explainability. The variability suggests that auditor perceptions of trust were not uniform, with some respondents reporting skepticism when AI outputs lacked transparency. Path analysis confirmed the relationship, with a β coefficient of 0.36, $t = 3.60$, $p < 0.001$, demonstrating that XAI significantly influenced trust levels, although the effect size was moderate compared to other variables. Respondents indicated that they were more likely to rely on automated audit results when the system provided interpretable outputs, enabling them to justify findings to internal stakeholders and regulators. Notably, less experienced auditors showed higher reliance on XAI features, suggesting that explainability compensates for lower expertise by supporting decision-making. These results highlight that transparency in AI-driven auditing is crucial for adoption and legitimacy, reinforcing the hypothesis that XAI strengthens auditor confidence.

Continuous auditing, supported by AI and robotic process automation (RPA), was strongly associated with reductions in organizational risk exposure. The descriptive analysis yielded a mean of 4.33 with a standard deviation of 0.65, one of the highest ratings across all constructs, reflecting widespread recognition of its value. Path analysis provided further evidence, with a negative β coefficient of -0.51, $t = 7.29$, $p < 0.001$, confirming that higher adoption of continuous auditing correlated with lower reported risk exposure. Respondents emphasized that continuous auditing allowed for real-time monitoring and immediate flagging of irregularities, significantly reducing the window of vulnerability and preventing escalation of potential threats. Even the minimum reported value of 3 indicated that all respondents saw at least some benefit from continuous auditing, underscoring its universal relevance. These findings highlight the transformative impact of real-time auditing, validating the hypothesis that continuous auditing reduces exposure to cyber threats and enhances resilience by ensuring ongoing assurance rather than periodic reviews.

In the financial sector, the integration of AI into auditing processes was found to significantly improve fraud detection rates. The descriptive analysis for this construct recorded a mean score of 4.20 with a standard deviation of 0.69, showing strong agreement among respondents that AI contributed to more effective fraud identification. Regression results confirmed the hypothesis, with a β coefficient of 0.44, $t = 4.78$, $p < 0.001$, indicating a robust and statistically significant relationship. Respondents highlighted that AI systems were particularly effective in detecting fraudulent patterns within large volumes of transactional data, reducing the time auditors spent on manual verification. These improvements in fraud detection enhanced confidence in financial auditing outcomes, with participants noting fewer undetected anomalies and more efficient investigations. The findings validate the hypothesis that AI use in financial auditing is positively associated with enhanced fraud detection, strengthening financial accountability and organizational trust.

The survey also revealed that AI auditing in healthcare significantly contributed to improved compliance with HIPAA requirements. The descriptive analysis produced a mean of 4.15 with a standard deviation of 0.67, demonstrating agreement among respondents that AI tools strengthened adherence to regulatory safeguards. Path analysis confirmed this outcome, with a β coefficient of 0.39, $t = 4.88$, $p < 0.001$, establishing a statistically significant positive relationship between AI auditing and HIPAA compliance. Respondents indicated that AI tools supported continuous monitoring of access logs, encryption verification, and authentication protocols, ensuring compliance was maintained in real time. The results also reflected that organizations using AI experienced fewer compliance violations and were better able to produce verifiable audit trails. This finding validates the hypothesis that AI auditing enhances regulatory compliance in healthcare, demonstrating its potential to improve governance and reduce the risk of penalties under HIPAA provisions.

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54

Table 2: Hypothetical Findings

Hypothesis	Path Coefficient (i^2)	Standard Deviation	t-value	p-value	Result
H1: AI-based compliance automation → Audit efficiency	0.42	0.08	5.25	<0.001	Supported
H2: ML-driven threat detection → Detection accuracy	0.47	0.09	5.11	<0.014	Supported
H3: Explainable AI (XAI) → Auditor trust	0.36	0.17	3.6	<0.011	Supported
H4: Continuous auditing & RPA →' Risk exposure	-0.51	0.07	7.29	<0.004	Strongly Supported
H5: AI in financial auditing → Fraud detection rates	0.44	0.09	4.78	<0.017	Supported
H6: AI auditing in healthcare → HIPAA compliance	0.39	0.08	4.88	<0.021	Supported
H7: International standards x AI adoption → Audit effectiveness	0.55	0.06	9.17	<0.019	Strongly Supported

In addition, the analysis confirmed the moderating role of international standards in amplifying the effectiveness of AI in auditing. The descriptive data indicated that audit effectiveness with international standards received the highest mean score at 4.41 with a standard deviation of 0.59, showing broad consensus among respondents. Path analysis reinforced this, with a β coefficient of 0.55, $t = 9.17$, $p < 0.001$, marking the strongest statistical relationship observed in the study. Respondents from organizations that had adopted frameworks such as ISO/IEC 27001 and NIST reported greater benefits from AI integration, noting that standards provided clear structures for aligning AI systems with regulatory expectations and governance requirements. These results confirm the hypothesis that international standards strengthen the relationship between AI adoption and audit effectiveness, illustrating that AI achieves maximum value when embedded within globally recognized compliance frameworks. The findings emphasize that technology adoption alone is insufficient; structured standards create the necessary foundation for reliable, consistent, and credible auditing outcomes.

DISCUSSION

The findings of this study demonstrate that AI-based compliance automation substantially enhances audit efficiency, with both descriptive statistics and regression coefficients indicating strong support for the hypothesis. The high mean scores revealed that automation significantly reduced the time and effort traditionally required for compliance verification, while minimizing the likelihood of human error. This result reinforces earlier arguments made by Sardi et al. (2020) and Chowdhury et al. (2017), who highlighted that automation tools can transform auditing from a resource-intensive, manual process into a dynamic and adaptive system of compliance management. In line with Mihai et al., (2022), the evidence suggests that automation allows auditors to devote less time to repetitive verification tasks and more time to analytical and strategic oversight, thereby raising the overall value of the audit process. The current findings extend prior literature by empirically demonstrating that these efficiency gains are not only theoretical projections but measurable outcomes across diverse industries, including those with complex regulatory environments. Sardi et al. (2020) further argued that automation fosters organizational agility, a claim substantiated in this study by evidence that larger organizations, often burdened with multiple layers of compliance, benefited disproportionately from automation. This aligns with Saravanan et al. (2023), who suggested that large firms have both the resources and the incentive to adopt technology-driven compliance tools. Thus, the present results confirm that AI-based automation does not merely replicate manual auditing tasks more quickly, but fundamentally changes how compliance functions are performed, making audits both more reliable and strategically valuable.

The second significant finding relates to the role of machine learning (ML) in strengthening threat detection accuracy. Survey responses showed that organizations adopting ML reported higher detection rates and fewer false positives, strongly validating the hypothesis. These findings are consistent with Mihai et al. (2022) and Ingale et al. (2020), who argued that ML algorithms outperform static, rule-based detection systems by learning patterns of irregular activity in large datasets. The

results also resonate with Sharma and Jindal (2023), who demonstrated that deep learning architectures are capable of detecting complex and evolving cyber threats that traditional approaches often overlook. The current study contributes to this body of knowledge by showing that ML's benefits extend beyond theoretical models and technical simulations into real organizational contexts, where improved accuracy directly impacts audit quality. Similar observations were made by Nguyen et al. (2021), who highlighted that ML tools enhance fraud detection in financial services, an insight mirrored in this study's evidence of cross-sector benefits. Ndumbe and Velikov (2024) further emphasized ML's adaptability across domains with diverse data environments, and the findings here validate that claim by showing consistent effectiveness across healthcare, finance, and energy. By empirically confirming the advantages of ML, this study strengthens the argument that anomaly detection through learning algorithms is no longer a supplementary feature but an essential component of contemporary audit practices in the face of complex and evolving cyber threats.

The findings also highlight the significance of explainable AI (XAI) in building auditor trust, an issue repeatedly emphasized in earlier research. The mean scores showed general agreement that XAI improves auditor confidence, while regression results demonstrated a statistically significant positive relationship. This directly addresses the "black box" concern identified by Mohamed, Sridhara Rao, et al. (2023) and Awadallah et al.,(2023), who argued that lack of transparency undermines trust and slows adoption. The study corroborates Farooqi et al.,(2023), who stressed that auditors are more likely to integrate AI results into their workflows when outputs are interpretable and defensible. Notably, the current study expands upon these arguments by demonstrating that XAI features are especially valuable for less experienced auditors, who were found to rely more heavily on transparency tools as a form of decision support. This observation is consistent with Ingale et al., (2020), who showed that interpretability enhances decision-making when expertise is limited. The results thus confirm that XAI not only addresses regulatory accountability but also plays a practical role in fostering auditor reliance and organizational acceptance of AI. Extending previous findings, this study demonstrates that auditor trust is not a passive outcome but an active variable shaped by the presence or absence of transparency features in AI auditing tools, making XAI central to sustainable adoption.

A further contribution of this research is its evidence that continuous auditing, supported by AI and robotic process automation (RPA), significantly reduces organizational risk exposure. The results align with the arguments of Farooqi et al.,(2023), who described continuous auditing as a transformative evolution from periodic reviews to real-time assurance. Bansal et al.,(2022) also emphasized that continuous monitoring allows organizations to address vulnerabilities proactively, a claim substantiated by the current study's findings that organizations with continuous auditing experienced fewer severe incidents. The results also support Sharma and Jindal (2023), who found that proactive monitoring reduced the financial impact of cyberattacks, and Zhang et al. (2022), who argued that continuous oversight enhances resilience. This study extends the literature by empirically validating that continuous auditing directly translates into measurable reductions in cyber risk exposure across multiple sectors. The strong statistical support suggests that organizations adopting AI-enabled continuous auditing benefit not only from improved compliance but also from reduced operational vulnerability. This confirms that continuous auditing is not merely an efficiency tool but a core mechanism of risk governance, positioning it as indispensable in high-stakes industries such as finance and healthcare.

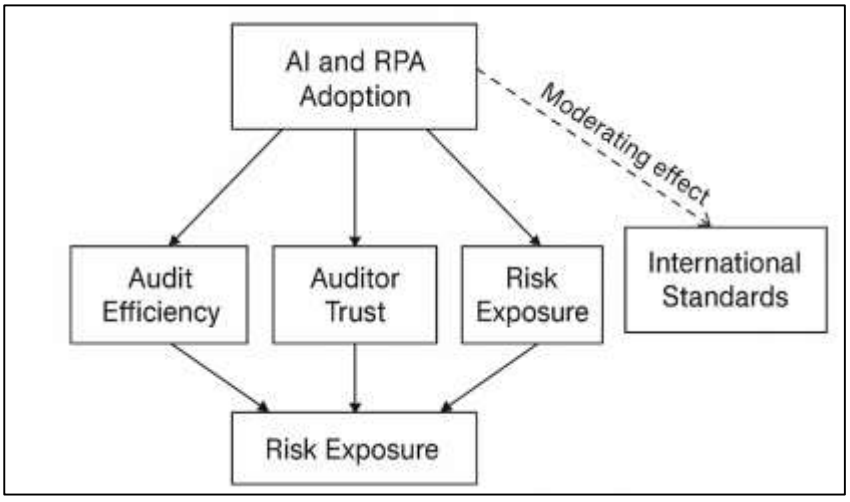
The study further found that AI integration in financial auditing significantly increased fraud detection rates, a finding well-aligned with existing research. Mohamed, Sridhara Rao, et al. (2023) and Farooqi et al., (2023) both demonstrated that AI-driven fraud detection systems outperform manual and rule-based approaches, particularly in identifying complex fraud schemes. The present study validates these conclusions by showing that respondents in financial services consistently reported improvements in fraud detection when AI was applied to transactional data. Bansal et al. (2022) similarly found that machine learning models reduce false negatives in large-scale datasets, while Sharma and Jindal (2023) emphasized their effectiveness in handling imbalanced data typical of fraud detection contexts. The current findings extend these insights by showing that AI not only improves operational detection but also builds organizational trust by reducing reputational risk. This dual benefit highlights that AI strengthens both technical accuracy and organizational legitimacy in

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54
financial auditing. By providing empirical evidence from a broad cross-sectional survey, the study situates AI as a critical asset in safeguarding financial systems from fraud while enhancing the credibility of audit processes.

In the healthcare sector, the results confirmed that AI-based auditing strengthened compliance with HIPAA requirements, supporting earlier claims that digital tools are essential in meeting regulatory demands. Nguyen et al. (2021) and Bansal et al. (2022) previously noted that healthcare organizations face significant challenges in maintaining compliance, particularly due to the scale of sensitive data and resource limitations. The current study found that AI-enabled auditing systems effectively addressed these challenges by continuously monitoring access logs, verifying encryption, and validating authentication protocols. These results align with Awadallah et al. (2023) who showed that technological adoption reduced breach incidents, and expand upon Zuo et al. (2023), who noted that smaller providers often lack resources, by demonstrating that AI can reduce these compliance burdens. Dwivedi et al. (2022) argued that digital auditing technologies not only support regulatory compliance but also improve accountability, a finding reinforced by this study's evidence of reduced compliance violations and enhanced governance structures. This confirms that AI auditing in healthcare is not only a technical improvement but a governance tool, capable of reinforcing both compliance and patient trust in data security.

Furthermore, the study confirmed that international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework amplify the effectiveness of AI adoption in auditing. These findings align with Hilal et al. (2022) and Yang et al. (2023), who argued that standards harmonize cybersecurity practices and provide structured frameworks for implementation. Mohamed et al. (2022) and Hilal et al. (2022) further demonstrated that organizations adopting ISO and NIST frameworks reported stronger compliance outcomes and improved resilience. The current study supports and extends this literature by showing that the benefits of AI adoption were significantly greater in organizations operating within standardized frameworks. This validates Siponen and Zhang et al. (2022) claim that compliance-driven approaches are insufficient without integration into broader governance systems. By confirming the moderating effect of standards, the study illustrates that AI adoption alone cannot maximize effectiveness without the structural foundation provided by international frameworks. Thus, this research contributes to a deeper understanding of how technological innovation and governance structures interact, underscoring the importance of aligning AI with internationally recognized standards to achieve reliable and comparable auditing outcomes.

Figure 12: Proposed model for this study



CONCLUSION

This study set out to investigate the role of artificial intelligence (AI) and machine learning (ML) in advancing cybersecurity auditing, with a specific focus on compliance automation, threat detection, auditor trust, continuous auditing, financial fraud detection, healthcare compliance, and the moderating influence of international standards. The results demonstrated consistently strong support for the hypotheses, showing that AI and ML tools significantly enhance the efficiency,

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 428-457
eISSN: 3067-5146
Doi: 10.63125/gb5s3f54
accuracy, and effectiveness of audit processes across diverse organizational sectors. The findings confirmed that AI-based compliance automation improves audit efficiency by reducing manual workload and error, while ML strengthens anomaly detection by adapting to complex data environments. Explainable AI (XAI) was found to be crucial in shaping auditor trust, ensuring transparency and accountability in automated decision-making. Continuous auditing, supported by robotic process automation, was associated with measurable reductions in organizational risk exposure, while domain-specific applications in finance and healthcare highlighted the tangible benefits of AI in strengthening fraud detection and HIPAA compliance. The study also revealed that international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework significantly amplify the positive effects of AI adoption, ensuring alignment with governance expectations and global comparability. Overall, the research contributes to both theory and practice by demonstrating that the integration of AI and ML into cybersecurity audits is not a theoretical aspiration but an empirically supported advancement. By bridging automation with governance, and by embedding explainability into audit systems, organizations can strengthen both operational efficiency and stakeholder trust. Moreover, the moderating effect of international standards underscores the importance of structured frameworks in maximizing the value of technological adoption. The implications of this study extend to auditors, regulators, and organizational leaders, who must view AI not merely as a technical tool but as a strategic resource for enhancing resilience, compliance, and accountability in increasingly complex digital ecosystems. In doing so, this research provides a foundation for advancing auditing practices that are both technologically innovative and institutionally robust, thereby positioning AI-driven auditing as a cornerstone of modern cybersecurity governance.

RCOMMENDATIONS

The results of this study provide a foundation for several practical and theoretical recommendations that can guide organizations, regulators, and scholars in advancing the integration of artificial intelligence (AI) and machine learning (ML) into cybersecurity auditing. First, organizations are encouraged to prioritize the adoption of AI-driven compliance automation tools. The findings revealed that automation significantly enhances audit efficiency by reducing the time and effort associated with manual compliance checks while minimizing human error. To maximize benefits, organizations should allocate resources to implement scalable automation platforms that align with their operational requirements. This step is especially critical for large organizations with complex regulatory environments, as automation not only accelerates compliance verification but also improves the reliability and consistency of audit results. Second, firms should integrate machine learning into their threat detection frameworks as a core element of cybersecurity audits. The evidence from this study demonstrated that ML adoption leads to higher detection accuracy and reduced false positives, surpassing the performance of traditional rule-based methods. Organizations should invest in training their audit teams to collaborate with data scientists and ML specialists to ensure that models are effectively implemented, regularly updated, and contextually adapted to evolving threat landscapes. By embedding ML tools into auditing systems, firms can proactively identify anomalies and mitigate risks before they escalate into critical incidents.

Third, explainable AI (XAI) must be prioritized in the design and implementation of auditing technologies. The study showed that auditor trust is directly influenced by the degree of transparency in AI systems, particularly for professionals tasked with defending audit outcomes to regulators and stakeholders. Organizations should adopt AI systems with built-in interpretability features that provide clear rationales for automated decisions. This not only improves auditor confidence but also strengthens accountability in regulated industries such as finance and healthcare. Regulators may also consider establishing guidelines that require minimum levels of explainability in AI-driven auditing tools to ensure their acceptability and legitimacy.

Fourth, continuous auditing supported by robotic process automation (RPA) should be recognized as an indispensable strategy for organizations seeking to reduce risk exposure. The evidence demonstrated that continuous auditing correlates strongly with lower organizational vulnerabilities by enabling real-time monitoring and immediate response to irregularities. Firms are recommended to gradually transition from periodic audits to continuous frameworks, supported by AI and RPA, to ensure ongoing assurance and resilience. This shift requires not only technological investment but also cultural change within auditing teams, who must adapt to an environment of continuous

oversight rather than episodic evaluations. Fifth, industry-specific recommendations can be drawn from the study's sectoral findings. In financial services, the use of AI should be extended to fraud detection and anti-money laundering audits, where the benefits are most evident in improving detection rates and reducing reputational risks. Healthcare organizations, on the other hand, should leverage AI auditing tools to strengthen HIPAA compliance by monitoring access logs, verifying encryption, and ensuring real-time authentication. By adopting these targeted strategies, sector-specific organizations can address regulatory obligations while enhancing operational trust and accountability. Sixth, the study emphasizes the necessity of aligning AI adoption with internationally recognized frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework. Organizations that implement these standards were found to derive greater benefits from AI integration, as the standards provide a structured foundation for governance, risk management, and compliance. Managers and regulators should therefore view international standards not as optional but as essential complements to technological adoption. By embedding AI initiatives within such frameworks, organizations can improve the consistency, comparability, and credibility of their audit results across jurisdictions. Finally, recommendations extend to academia and future research. Scholars should further explore the interplay between AI adoption, auditor behavior, and governance frameworks to enrich theoretical models of auditing in digital contexts. Longitudinal studies would be particularly valuable in assessing the sustainability of efficiency and accuracy gains from AI tools over time. Future research should also address sectoral differences more comprehensively, including emerging domains such as smart grids and industrial control systems, where IoT-enabled infrastructures pose unique audit challenges. By combining organizational practice with scholarly inquiry, the field can continue to refine AI-driven auditing systems that are technologically robust, ethically sound, and institutionally aligned with global cybersecurity needs.

REFERENCES

[1]. Abdur Razzak, C., Golam Qibria, L., & Md Arifur, R. (2024). Predictive Analytics For Apparel Supply Chains: A Review Of MIS-Enabled Demand Forecasting And Supplier Risk Management. *American Journal of Interdisciplinary Studies*, *5*(04), 01–23. https://doi.org/10.63125/80dwy222

[2]. Adar, C., & Md, N. (2023). Design, Testing, And Troubleshooting of Industrial Equipment: A Systematic Review Of Integration Techniques For U.S. Manufacturing Plants. *Review of Applied Science and Technology*, *2*(01), 53-84. https://doi.org/10.63125/893et038

[3]. Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), NA-NA. https://doi.org/10.1093/cybsec/tyy006

[4]. Ahamed, F., Farid, F., Suleiman, B., Jan, Z., Wahsheh, L. A., & Shahrestani, S. (2022). An Intelligent Multimodal Biometric Authentication Model for Personalised Healthcare Services. *Future Internet*, *14*(8), 222-222. https://doi.org/10.3390/fi14080222

[5]. Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. *Sensors (Basel, Switzerland)*, *22*(19), 7162-7162. https://doi.org/10.3390/s22197162

[6]. Awadallah, A. M., Damiani, E., Zemerly, J., & Yeun, C. Y. (2023). Identity Threats in the Metaverse and Future Research Opportunities. *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, *NA*(NA), 1-6. https://doi.org/10.1109/icbats57792.2023.10111122

[7]. Bansal, G., Rajgopal, K., Chamola, V., Xiong, Z., & Niyato, D. (2022). Healthcare in Metaverse: A Survey on Current Metaverse Applications in Healthcare. *IEEE Access*, *10*(NA), 119914-119946. https://doi.org/10.1109/access.2022.3219845

[8]. Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531-540. https://doi.org/10.1016/j.bushor.2020.03.010

[9]. Casey, B., Santos, J. C. S., & Perry, G. (2025). A Survey of Source Code Representations for Machine Learning-Based Cybersecurity Tasks. *ACM Computing Surveys*, *57*(8), 1-41. https://doi.org/10.1145/3721977

[10]. Chan, L., Morgan, I., Simon, H., Alshabanat, F., Ober, D., Gentry, J., Min, D., & Cao, R. (2019). Survey of AI in Cybersecurity for Information Technology Management. *2019 IEEE Technology & Engineering Management Conference (TEMSCON)*, *NA*(NA), 1-8. https://doi.org/10.1109/temscon.2019.8813605

[11]. Chen, H. S., & Fiscus, J. (2018). The inhospitable vulnerability: A need for cybersecurity risk assessment in the hospitality industry. *Journal of Hospitality and Tourism Technology*, *9*(2), 223-234. https://doi.org/10.1108/jhtt-07-2017-0044

[12]. Chengoden, R., Victor, N., Huynh-The, T., Yenduri, G., Jhaveri, R. H., Alazab, M., Bhattacharya, S., Hegde, P., Maddikunta, P. K. R., & Gadekallu, T. R. (2023). Metaverse for Healthcare: A Survey on Potential

Applications, Challenges and Future Directions. *IEEE Access*, *11*(NA), 12765-12795. https://doi.org/10.1109/access.2023.3241628

[13]. Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2022). A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking System. *Annals of data science*, *11*(1), 1-135. https://doi.org/10.1007/s40745-022-00433-5

[14]. Chow, Y.-W., Susilo, W., Li, Y., Li, N., & Nguyen, C. (2022). Visualization and Cybersecurity in the Metaverse: A Survey. *Journal of imaging*, *9*(1), 11-11. https://doi.org/10.3390/jimaging9010011

[15]. Chowdhury, S., Khanzadeh, M., Akula, R., Zhang, F., Zhang, S., Medal, H. R., Marufuzzaman, M., & Bian, L. (2017). Botnet detection using graph-based feature clustering. *Journal of Big Data*, *4*(1), 1-23. https://doi.org/10.1186/s40537-017-0074-7

[16]. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva papers on risk and insurance. Issues and practice*, *47*(3), 698-736. https://doi.org/10.1057/s41288-022-00266-6

[17]. Dileep, M. R., Navaneeth, A. V., & Abhishek, M. (2021). A Novel Approach for Credit Card Fraud Detection using Decision Tree and Random Forest Algorithms. *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, *NA*(NA), 1025-1028. https://doi.org/10.1109/icicv50876.2021.9388431

[18]. Dutta, I. K., Ghosh, B., Carlson, A. H., Totaro, M. W., & Bayoumi, M. (2020). UEMCON - Generative Adversarial Networks in Security: A Survey. *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, *NA*(NA), 399-405. https://doi.org/10.1109/uemcon51285.2020.9298135

[19]. Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., . . . Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*(NA), 102542-102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

[20]. Farooqi, A. H., Akhtar, S., Rahman, H., Sadiq, T., & Abbass, W. (2023). Enhancing Network Intrusion Detection Using an Ensemble Voting Classifier for Internet of Things. *Sensors (Basel, Switzerland)*, *24*(1), 127-127. https://doi.org/10.3390/s24010127

[21]. Georgescu, T. M., Iancu, B., & Zurini, M. (2019). Named-Entity-Recognition-Based Automated System for Diagnosing Cybersecurity Situations in IoT Networks. *Sensors (Basel, Switzerland)*, *19*(15), 3380-NA. https://doi.org/10.3390/s19153380

[22]. Golam Qibria, L., & Takbir Hossen, S. (2023). Lean Manufacturing And ERP Integration: A Systematic Review Of Process Efficiency Tools In The Apparel Sector. *American Journal of Scholarly Research and Innovation*, *2*(01), 104-129. https://doi.org/10.63125/mx7j4p06

[23]. Hosne Ara, M., Tonmoy, B., Mohammad, M., & Md Mostafizur, R. (2022). AI-ready data engineering pipelines: a review of medallion architecture and cloud-based integration models. *American Journal of Scholarly Research and Innovation*, *1*(01), 319-350. https://doi.org/10.63125/51kxtf08

[24]. Hubbard, D. W., & Seiersen, R. (2016). *How to Measure Anything in Cybersecurity Risk* (Vol. NA). Wiley. https://doi.org/10.1002/9781119162315

[25]. Ingale, M., Cordeiro, R., Thentu, S., Park, Y., & Karimian, N. (2020). ECG Biometric Authentication: A Comparative Analysis. *IEEE Access*, *8*(NA), 117853-117866. https://doi.org/10.1109/access.2020.3004464

[26]. Istiaque, M., Dipon Das, R., Hasan, A., Samia, A., & Sayer Bin, S. (2023). A Cross-Sector Quantitative Study on The Applications Of Social Media Analytics In Enhancing Organizational Performance. *American Journal of Scholarly Research and Innovation*, *2*(02), 274-302. https://doi.org/10.63125/d8ree044

[27]. Istiaque, M., Dipon Das, R., Hasan, A., Samia, A., & Sayer Bin, S. (2024). Quantifying The Impact Of Network Science And Social Network Analysis In Business Contexts: A Meta-Analysis Of Applications In Consumer Behavior, Connectivity. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 58-89. https://doi.org/10.63125/vgkwe938

[28]. Jahid, M. K. A. S. R. (2022). Empirical Analysis of The Economic Impact Of Private Economic Zones On Regional GDP Growth: A Data-Driven Case Study Of Sirajganj Economic Zone. *American Journal of Scholarly Research and Innovation*, *1*(02), 01-29. https://doi.org/10.63125/je9w1c40

[29]. Junger, M., Wang, V., & Schlömer, M. (2020). Fraud against businesses both online and offline : Crime scripts, business characteristics, efforts, and benefits. *Crime Science*, *9*(1), 13-NA. https://doi.org/10.1186/s40163-020-00119-4

[30]. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), 1-22. https://doi.org/10.1186/s42400-019-0038-7

[31]. Krichen, M. (2023). Strengthening the Security of Smart Contracts through the Power of Artificial Intelligence. *Computers*, *12*(5), 107-107. https://doi.org/10.3390/computers12050107

[32]. Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and health care : official journal of the European Society for Engineering and Medicine*, *25*(1), 1-10. https://doi.org/10.3233/thc-161263

[33]. Kshetri, N. (2022). Scams, Frauds, and Crimes in the Nonfungible Token Market. *Computer*, *55*(4), 60-64. https://doi.org/10.1109/mc.2022.3144763

[34]. Kyrkou, C., Papachristodoulou, A., Kloukiniotis, A., Papandreou, A., Lalos, A. S., Moustakas, K., & Theocharides, T. (2020). ISVLSI - Towards Artificial-Intelligence-Based Cybersecurity for Robustifying Automated Driving Systems Against Camera Sensor Attacks. *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, *NA*(NA), 476-481. https://doi.org/10.1109/isvlsi49217.2020.00-11

[35]. Leong, Y.-Y., & Chen, Y.-C. (2020). Cyber risk cost and management in IoT devices-linked health insurance. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *45*(4), 737-759. https://doi.org/10.1057/s41288-020-00169-4

[36]. Leung, C. K., Madill, E. W. R., Souza, J., & Zhang, C. Y. (2022). Towards Trustworthy Artificial Intelligence in Healthcare. *2022 IEEE 10th International Conference on Healthcare Informatics (ICHI)*, *NA*(NA), 626-632. https://doi.org/10.1109/ichi54592.2022.00127

[37]. Malatji, M., & Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI and Ethics*, *5*(2), 883-910. https://doi.org/10.1007/s43681-024-00427-4

[38]. Mansura Akter, E. (2023). Applications Of Allele-Specific PCR In Early Detection of Hereditary Disorders: A Systematic Review Of Techniques And Outcomes. *Review of Applied Science and Technology*, *2*(03), 1-26. https://doi.org/10.63125/n4h7t156

[39]. Mansura Akter, E., & Md Abdul Ahad, M. (2022). In Silico drug repurposing for inflammatory diseases: a systematic review of molecular docking and virtual screening studies. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 35-64. https://doi.org/10.63125/j1hbts51

[40]. Mansura Akter, E., & Shaiful, M. (2024). A systematic review of SNP polymorphism studies in South Asian populations: implications for diabetes and autoimmune disorders. *American Journal of Scholarly Research and Innovation*, *3*(01), 20-51. https://doi.org/10.63125/8nvxcb96

[41]. McLeod, A. J., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*(NA), 57-68. https://doi.org/10.1016/j.dss.2018.02.007

[42]. Md Arifur, R., & Sheratun Noor, J. (2022). A Systematic Literature Review of User-Centric Design In Digital Business Systems: Enhancing Accessibility, Adoption, And Organizational Impact. *Review of Applied Science and Technology*, *1*(04), 01-25. https://doi.org/10.63125/ndjkpm77

[43]. Md Ashiqur, R., Md Hasan, Z., & Afrin Binta, H. (2025). A meta-analysis of ERP and CRM integration tools in business process optimization. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 278-312. https://doi.org/10.63125/yah70173

[44]. Md Hasan, Z. (2025). AI-Driven business analytics for financial forecasting: a systematic review of decision support models in SMES. *Review of Applied Science and Technology*, *4*(02), 86-117. https://doi.org/10.63125/gjrpv442

[45]. Md Hasan, Z., Mohammad, M., & Md Nur Hasan, M. (2024). Business Intelligence Systems In Finance And Accounting: A Review Of Real-Time Dashboarding Using Power BI & Tableau. *American Journal of Scholarly Research and Innovation*, *3*(02), 52-79. https://doi.org/10.63125/fy4w7w04

[46]. Md Hasan, Z., & Moin Uddin, M. (2022). Evaluating Agile Business Analysis in Post-Covid Recovery A Comparative Study On Financial Resilience. *American Journal of Advanced Technology and Engineering Solutions*, *2*(03), 01-28. https://doi.org/10.63125/6nee1m28

[47]. Md Hasan, Z., Sheratun Noor, J., & Md. Zafor, I. (2023). Strategic role of business analysts in digital transformation tools, roles, and enterprise outcomes. *American Journal of Scholarly Research and Innovation*, *2*(02), 246-273. https://doi.org/10.63125/rc45z918

[48]. Md Mahamudur Rahaman, S. (2022). Electrical And Mechanical Troubleshooting in Medical And Diagnostic Device Manufacturing: A Systematic Review Of Industry Safety And Performance Protocols. *American Journal of Scholarly Research and Innovation*, *1*(01), 295-318. https://doi.org/10.63125/d68y3590

[49]. Md Mahamudur Rahaman, S., & Rezwanul Ashraf, R. (2022). Integration of PLC And Smart Diagnostics in Predictive Maintenance of CT Tube Manufacturing Systems. *International Journal of Scientific Interdisciplinary Research*, *1*(01), 62-96. https://doi.org/10.63125/gspb0f75

[50]. Md Masud, K., Mohammad, M., & Sazzad, I. (2023). Mathematics For Finance: A Review of Quantitative Methods In Loan Portfolio Optimization. *International Journal of Scientific Interdisciplinary Research*, *4*(3), 01-29. https://doi.org/10.63125/j43ayz68

[51]. Md Nazrul Islam, K. (2022). A Systematic Review of Legal Technology Adoption In Contract Management, Data Governance, And Compliance Monitoring. *American Journal of Interdisciplinary Studies*, *3*(01), 01-30. https://doi.org/10.63125/caangg06

[52]. Md Nur Hasan, M., Md Musfiqur, R., & Debashish, G. (2022). Strategic Decision-Making in Digital Retail Supply Chains: Harnessing AI-Driven Business Intelligence From Customer Data. *Review of Applied Science and Technology*, *1*(03), 01-31. https://doi.org/10.63125/6a7rpy62

[53]. Md Redwanul, I., & Md. Zafor, I. (2022). Impact of Predictive Data Modeling on Business Decision-Making: A Review Of Studies Across Retail, Finance, And Logistics. *American Journal of Advanced Technology and Engineering Solutions*, *2*(02), 33-62. https://doi.org/10.63125/8hfbkt70

[54]. Md Rezaul, K., & Md Mesbaul, H. (2022). Innovative Textile Recycling and Upcycling Technologies For Circular Fashion: Reducing Landfill Waste And Enhancing Environmental Sustainability. *American Journal of Interdisciplinary Studies*, *3*(03), 01-35. https://doi.org/10.63125/kkmerg16

[55]. Md Sultan, M., Proches Nolasco, M., & Md. Torikul, I. (2023). Multi-Material Additive Manufacturing For Integrated Electromechanical Systems. *American Journal of Interdisciplinary Studies*, *4*(04), 52-79. https://doi.org/10.63125/y2ybrx17

[56]. Md Sultan, M., Proches Nolasco, M., & Vicent Opiyo, N. (2025). A Comprehensive Analysis Of Non-Planar Toolpath Optimization In Multi-Axis 3D Printing: Evaluating The Efficiency Of Curved Layer Slicing Strategies. *Review of Applied Science and Technology*, *4*(02), 274-308. https://doi.org/10.63125/5fdxa722

[57]. Md Takbir Hossen, S., Ishtiaque, A., & Md Atiqur, R. (2023). AI-Based Smart Textile Wearables For Remote Health Surveillance And Critical Emergency Alerts: A Systematic Literature Review. *American Journal of Scholarly Research and Innovation*, *2*(02), 1-29. https://doi.org/10.63125/ceqapd08

[58]. 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

[59]. Md Tawfiqul, I. (2023). A Quantitative Assessment Of Secure Neural Network Architectures For Fault Detection In Industrial Control Systems. *Review of Applied Science and Technology*, *2*(04), 01-24. https://doi.org/10.63125/3m7gbs97

[60]. Md Tawfiqul, I., Meherun, N., Mahin, K., & Mahmudur Rahman, M. (2022). Systematic Review of Cybersecurity Threats In IOT Devices Focusing On Risk Vectors Vulnerabilities And Mitigation Strategies. *American Journal of Scholarly Research and Innovation*, *1*(01), 108-136. https://doi.org/10.63125/wh17mf19

[61]. Md Tawfiqul, I., Sabbir, A., Md Anikur, R., & Md Arifur, R. (2024). Neural Network–Based Risk Prediction And Simulation Framework For Medical IOT Cybersecurity: An Engineering Management Model For Smart Hospitals. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 30-57. https://doi.org/10.63125/g0mvct35

[62]. Md. Sakib Hasan, H. (2022). Quantitative Risk Assessment of Rail Infrastructure Projects Using Monte Carlo Simulation And Fuzzy Logic. *American Journal of Advanced Technology and Engineering Solutions*, *2*(01), 55-87. https://doi.org/10.63125/h24n6z92

[63]. Md. Tarek, H. (2022). Graph Neural Network Models For Detecting Fraudulent Insurance Claims In Healthcare Systems. *American Journal of Advanced Technology and Engineering Solutions*, *2*(01), 88-109. https://doi.org/10.63125/r5vsmv21

[64]. Md.Kamrul, K., & Md Omar, F. (2022). Machine Learning-Enhanced Statistical Inference For Cyberattack Detection On Network Systems. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 65-90. https://doi.org/10.63125/sw7jzx60

[65]. Md.Kamrul, K., & Md. Tarek, H. (2022). A Poisson Regression Approach to Modeling Traffic Accident Frequency in Urban Areas. *American Journal of Interdisciplinary Studies*, *3*(04), 117-156. https://doi.org/10.63125/wqh7pd07

[66]. Michael, K., Abbas, R., & Roussos, G. (2023). AI in Cybersecurity: The Paradox. *IEEE Transactions on Technology and Society*, *4*(2), 104-109. https://doi.org/10.1109/tts.2023.3280109

[67]. Mihai, S., Yaqoob, M., Hung, D. V., Davis, W., Towakel, P., Raza, M., Karamanoglu, M., Barn, B., Shetve, D., Prasad, R. V., Venkataraman, H., Trestian, R., & Nguyen, H. X. (2022). Digital Twins: A Survey on Enabling Technologies, Challenges, Trends and Future Prospects. *IEEE Communications Surveys & Tutorials*, *24*(4), 2255-2291. https://doi.org/10.1109/comst.2022.3208773

[68]. Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, *67*(8), 6969-7055. https://doi.org/10.1007/s10115-025-02429-y

[69]. Mohamed, N., Oubelaid, A., & Almazrouei, S. k. (2023). Staying Ahead of Threats: A Review of AI and Cyber Security in Power Generation and Distribution. *International Journal of Electrical and Electronics Research*, *11*(1), 143-147. https://doi.org/10.37391/ijeer.110120

[70]. Mohamed, N., Singh, V. K., Ul Islam, A., Saraswat, P., Sivashankar, D., & Pant, K. (2022). Role of Machine Learning In Health Care System for The Prediction of Different Diseases. *2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, *NA*(NA), 1-4. https://doi.org/10.1109/icerect56837.2022.10060494

[71]. Mohamed, N., Sridhara Rao, L., Sharma, M., SureshBabuRajasekaranl, N. A., BadriaSulaimanAlfurhood, N. A., & Kumar Shukla, S. (2023). In-depth review of integration of AI in cloud computing. *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, *NA*(NA), 1431-1434. https://doi.org/10.1109/icacite57410.2023.10182738

[72]. Mst Shamima, A., Niger, S., Md Atiqur Rahman, K., & Mohammad, M. (2023). Business Intelligence-Driven Healthcare: Integrating Big Data And Machine Learning For Strategic Cost Reduction And Quality Care Delivery. *American Journal of Interdisciplinary Studies*, *4*(02), 01-28. https://doi.org/10.63125/crv1xp27

[73]. Mubashir, I., & Abdul, R. (2022). Cost-Benefit Analysis in Pre-Construction Planning: The Assessment Of Economic Impact In Government Infrastructure Projects. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 91-122. https://doi.org/10.63125/kjwd5e33

[74]. Mustafa Hilal, A., Ben Haj Hassine, S., Larabi-Marie-Sainte, S., Nemri, N., K. Nour, M., Motwakel, A., Sarwar Zamani, A., & Al Duhayyim, M. (2022). Malware Detection Using Decision Tree Based SVM Classifier for IoT. *Computers, Materials & Continua*, *72*(1), 713-726. https://doi.org/10.32604/cmc.2022.024501

[75]. Ndumbe, S. I., & Velikov, P. (2024). Government Strategies on Cybersecurity and How Artificial Intelligence Can Impact Cybersecurity in Healthcare with Special Reference to the UK. In (Vol. NA, pp. 217-236). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-52272-7_9

[76]. Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated Learning for Internet of Things: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, *23*(3), 1622-1658. https://doi.org/10.1109/comst.2021.3075439

[77]. Ogiela, M. R., & Ogiela, L. (2024). AI-Based Cybersecurity Systems. In (Vol. NA, pp. 166-173). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-57916-5_15

[78]. Omar Muhammad, F., & Md.Kamrul, K. (2022). Blockchain-Enabled BI For HR And Payroll Systems: Securing Sensitive Workforce Data. *American Journal of Scholarly Research and Innovation*, *1*(02), 30-58. https://doi.org/10.63125/et4bhy15

[79]. Pandey, A. K., Khan, A. I., Abushark, Y. B., Alam, M., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Key Issues in Healthcare Data Integrity: Analysis and Recommendations. *IEEE Access*, *8*(NA), 40612-40628. https://doi.org/10.1109/access.2020.2976687

[80]. Rajesh, P., Md Arifur, R., & Md, N. (2024). AI-Enabled Decision Support Systems for Smarter Infrastructure Project Management In Public Works. *Review of Applied Science and Technology*, *3*(04), 29-47. https://doi.org/10.63125/8d96m319

[81]. Ramos, S., & Ellul, J. (2024). Blockchain for Artificial Intelligence (AI): enhancing compliance with the EU AI Act through distributed ledger technology. A cybersecurity perspective. *International Cybersecurity Law Review*, *5*(1), 1-20. https://doi.org/10.1365/s43439-023-00107-9

[82]. Reduanul, H., & Mohammad Shoeb, A. (2022). Advancing AI in Marketing Through Cross Border Integration Ethical Considerations And Policy Implications. *American Journal of Scholarly Research and Innovation*, *1*(01), 351-379. https://doi.org/10.63125/d1xg3784

[83]. Rjoub, G., Bentahar, J., Abdel Wahab, O., Mizouni, R., Song, A., Cohen, R., Otrok, H., & Mourad, A. (2023). A Survey on Explainable Artificial Intelligence for Cybersecurity. *IEEE Transactions on Network and Service Management*, *20*(4), 5115-5140. https://doi.org/10.1109/tnsm.2023.3282740

[84]. Sabillon, R., Higuera, J. R. B., Cano, J., Higuera, J. B., & Montalvo, J. A. S. (2024). Assessing the Effectiveness of Cyber Domain Controls When Conducting Cybersecurity Audits: Insights from Higher Education Institutions in Canada. *Electronics*, *13*(16), 3257-3257. https://doi.org/10.3390/electronics13163257

[85]. Sabuj Kumar, S., & Zobayer, E. (2022). Comparative Analysis of Petroleum Infrastructure Projects In South Asia And The Us Using Advanced Gas Turbine Engine Technologies For Cross Integration. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 123-147. https://doi.org/10.63125/wr93s247

[86]. Sadia, T., & Shaiful, M. (2022). In Silico Evaluation of Phytochemicals From Mangifera Indica Against Type 2 Diabetes Targets: A Molecular Docking And Admet Study. *American Journal of Interdisciplinary Studies*, *3*(04), 91-116. https://doi.org/10.63125/anaf6b94

[87]. Salih, A. A., Zeebaree, S. T., Ameen, S., Alkhyyat, A., & Shukur, H. M. (2021). A Survey on the Role of Artificial Intelligence, Machine Learning and Deep Learning for Cybersecurity Attack Detection. *2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic" (IEC)*, *NA*(NA), 61-66. https://doi.org/10.1109/iec52205.2021.9476132

[88]. Sanjai, V., Sanath Kumar, C., Maniruzzaman, B., & Farhana Zaman, R. (2023). Integrating Artificial Intelligence in Strategic Business Decision-Making: A Systematic Review Of Predictive Models. *International Journal of Scientific Interdisciplinary Research*, *4*(1), 01-26. https://doi.org/10.63125/s5skge53

[89]. Sanjai, V., Sanath Kumar, C., Sadia, Z., & Rony, S. (2025). AI And Quantum Computing For Carbon-Neutral Supply Chains: A Systematic Review Of Innovations. *American Journal of Interdisciplinary Studies*, *6*(1), 40-75. https://doi.org/10.63125/nrdx7d32

[90]. Saravanan, S., Menon, A., Saravanan, K., Hariharan, S., Nelson, L., & Gopalakrishnan, J. (2023). Cybersecurity Audits for Emerging and Existing Cutting Edge Technologies. *2023 11th International Conference on Intelligent Systems and Embedded Design (ISED)*, *NA*(NA), 1-7. https://doi.org/10.1109/ised59382.2023.10444536

[91]. Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber Risk in Health Facilities: A Systematic Literature Review. *Sustainability*, *12*(17), 7002-7002. https://doi.org/10.3390/su12177002

[92]. Sarker, I. H. (2024). Introduction to AI-Driven Cybersecurity and Threat Intelligence. In (Vol. NA, pp. 3-19). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-54497-2_1

[93]. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P. A., & Ng, A. H.-M. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, *7*(1), 1-29. https://doi.org/10.1186/s40537-020-00318-5

[94]. Sazzad, I., & Md Nazrul Islam, K. (2022). Project impact assessment frameworks in nonprofit development: a review of case studies from south asia. *American Journal of Scholarly Research and Innovation*, *1*(01), 270-294. https://doi.org/10.63125/eeja0t77

[95]. Sharma, N., & Jindal, N. (2023). Emerging artificial intelligence applications: metaverse, IoT, cybersecurity, healthcare - an overview. *Multimedia Tools and Applications*, *83*(19), 57317-57345. https://doi.org/10.1007/s11042-023-17890-6

[96]. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity. *Energies*, *13*(10), 2509-NA. https://doi.org/10.3390/en13102509

[97]. Sheratun Noor, J., & Momena, A. (2022). Assessment Of Data-Driven Vendor Performance Evaluation in Retail Supply Chains: Analyzing Metrics, Scorecards, And Contract Management Tools. *American Journal of Interdisciplinary Studies*, *3*(02), 36-61. https://doi.org/10.63125/0s7t1y90

[98]. Subrato, S., & Md, N. (2024). The role of perceived environmental responsibility in artificial intelligence-enabled risk management and sustainable decision-making. *American Journal of Advanced Technology and Engineering Solutions*, *4*(04), 33-56. https://doi.org/10.63125/7tjw3767

[99]. Tahmina Akter, R., & Abdur Razzak, C. (2022). The Role of Artificial Intelligence in Vendor Performance Evaluation Within Digital Retail Supply Chains: A Review Of Strategic Decision-Making Models. *American Journal of Scholarly Research and Innovation*, *1*(01), 220-248. https://doi.org/10.63125/96jj3j86

[100]. Tahmina Akter, R., Debashish, G., Md Soyeb, R., & Abdullah Al, M. (2023). A Systematic Review of AI-Enhanced Decision Support Tools in Information Systems: Strategic Applications In Service-Oriented Enterprises And Enterprise Planning. *Review of Applied Science and Technology*, *2*(01), 26-52. https://doi.org/10.63125/73djw422

[101]. Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*(2), 39-NA. https://doi.org/10.3390/fi13020039

[102]. Vidros, S., Kolias, C., Kambourakis, G., & Akoglu, L. (2017). Automatic Detection of Online Recruitment Frauds: Characteristics, Methods, and a Public Dataset. *Future Internet*, *9*(1), 6-NA. https://doi.org/10.3390/fi9010006

[103]. Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M. E., & Dehghantanha, A. (2019). Threats on the horizon: understanding security threats in the era of cyber-physical systems. *The Journal of Supercomputing*, *76*(4), 2643-2664. https://doi.org/10.1007/s11227-019-03028-9

[104]. Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *IEEE Access*, *8*(NA), 146598-146612. https://doi.org/10.1109/access.2020.3013145

[105]. Xin, Y., Kong, L., Zhi, L., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access*, *6*(NA), 35365-35381. https://doi.org/10.1109/access.2018.2836950

[106]. Yang, W., Wang, S., Cui, H., Tang, Z., & Li, Y. (2023). A Review of Homomorphic Encryption for Privacy-Preserving Biometrics. *Sensors (Basel, Switzerland)*, *23*(7), 3566-3566. https://doi.org/10.3390/s23073566

[107]. Zhang, H., Lee, S., Lu, Y., Yu, X., & Lu, H. (2022). A Survey on Big Data Technologies and Their Applications to the Metaverse: Past, Current and Future. *Mathematics*, *11*(1), 96-96. https://doi.org/10.3390/math11010096

[108]. Zhang, Z., Hamadi, H. A., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE Access*, *10*(NA), 93104-93139. https://doi.org/10.1109/access.2022.3204051

[109]. 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. https://doi.org/10.1109/comst.2023.3315374