Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(RESEARCH ARTICLE)

Check for updates

AI-driven threat detection in pharmaceutical R and D: Mitigating cyber risks in drug discovery platforms

Rama Devi Drakshpalli *

Independent Researcher, North Carolina, USA.

Global Journal of Engineering and Technology Advances, 2025, 23(03), 048–062

Publication history: Received on 12 April 2025; revised on 29 May 2025; accepted on 01 June 2025

Article DOI: https://doi.org/10.30574/gjeta.2025.23.3.0176

Abstract

The integration of Artificial Intelligence (AI) into pharmaceutical research and development (R&D) has transformed drug discovery, biomarker identification, and clinical trial automation, significantly reducing costs and expediting breakthroughs. However, the increasing reliance on AI-driven processes exposes pharmaceutical R&D to evolving cybersecurity threats, including adversarial AI manipulations, ransomware attacks, and AI poisoning. To address these challenges, this study explores AI-driven cybersecurity solutions, with a focus on machine learning-based Intrusion Detection Systems (IDS) capable of identifying anomalies in AI-generated predictions. Furthermore, it examines the role of federated learning in securing sensitive research data and proposes a national AI security framework aligned with the Cybersecurity and Infrastructure Security Agency (CISA) directives. By leveraging AI-powered anomaly detection, deep learning models, and automated incident response, organizations can enhance their resilience against sophisticated cyber threats. Despite these advancements, challenges such as algorithmic bias, false positives, and adversarial vulnerabilities persist.

Keywords: Artificial Intelligence (AI); Pharmaceutical R&D; Cybersecurity; Intrusion Detection Systems (IDS); Federated Learning; Anomaly Detection

1. Introduction

AI-powered drug discovery platforms have significantly enhanced pharmaceutical R&D, enabling faster and more cost-efficient innovation. However, the rapid adoption of AI has introduced new cybersecurity challenges that threaten data integrity, intellectual property, and regulatory compliance. As pharmaceutical organizations increasingly rely on AI-driven processes for drug discovery, biomarker identification, and clinical trial management, they become prime targets for cyber threats such as adversarial AI manipulations, ransomware attacks, and AI poisoning. The convergence of AI and cybersecurity is critical in safeguarding sensitive research data and ensuring the reliability of AI-generated predictions. Traditional security measures are often inadequate against sophisticated cyber threats that exploit vulnerabilities in machine learning models. Consequently, the need for AI-driven security solutions has become paramount in mitigating emerging risks and ensuring the integrity of pharmaceutical research [24], [26].

* Corresponding author: Rama Devi Drakshpalli

Table 1 AI and machine learning models in the pharmaceutical industry

AI/Machine Learning Models	Description/Usage	References
Generative Adversarial Networks (GANs)	GANs are widely used in drug product development to generate novel chemical structures and optimize their properties. GANs consist of a generator network that creates new molecules and a discriminator network that evaluates their quality, leading to the generation of structurally diverse and functionally optimized drug candidates.	[1]
Recurrent Neural Networks (RNNs)	RNNs are commonly employed for sequence-based tasks in drug development, such as predicting protein structures, analyzing genomic data, and designing peptide sequences. They capture sequential dependencies and can generate new sequences based on learned patterns. Pharmaceutics 2023, 15, 1916 8 of 46	[2]
Convolutional Neural Networks (CNNs)	CNNs are effective in image-based tasks, including analyzing molecular structures and identifying potential drug targets. They can extract relevant features from molecular images and aid in drug design and target identification	[3] , [4]
Long Short-Term Memory Networks (LSTMs)	LSTMs are a type of RNN that excel in modeling and predicting temporal dependencies. They have been used in pharmacokinetics and pharmacodynamics studies to predict drug concentration-time profiles and evaluate drug efficacy.	[3], [4]
Transformer Models	Transformer models, such as the popular BERT (Bidirectional Encoder Representations from Transformers), have been employed in natural language processing tasks in the pharmaceutical domain. They can extract useful information from the scientific literature, patent databases, and clinical trial data, enabling researchers to make informed decisions in drug development.	[5]
Reinforcement Learning (RL)	RL techniques have been applied to optimize drug dosing strategies and develop personalized treatment plans. RL algorithms learn from interactions with the environment to make sequential decisions, aiding in dose optimization, and improving patient outcomes.	[6]
Bayesian Models	Bayesian models, such as Bayesian networks and Gaussian processes, are employed for uncertainty quantification and decision-making in drug development. They enable researchers to make probabilistic predictions, assess risks, and optimize experimental designs.	[7], [8]
Deep Q-Networks (DQNs)	DQNs, a combination of deep learning and reinforcement learning, have been used to optimize drug discovery processes by predicting the activity of compounds and suggesting high-potential candidates for further experimentation.	[9], [10]
Autoencoders	Autoencoders are unsupervised learning models used for dimensionality reduction and feature extraction in drug development. They can capture essential characteristics of molecules and assist in compound screening and virtual screening. Advanced bioinformatics platforms also integrate AI-based molecular modeling tools for medicinal biology, further improving compound profiling and screening processes	[11], [12], [16]
Graph Neural Networks (GNNs)	GNNs are designed to process graph-structured data, making them suitable for drug discovery tasks that involve molecular structures. They can model molecular graphs, predict properties, and aid in virtual screening and de novo drug design. Additionally, in silico protein design approaches leveraging AI have enabled efficient virtual screening of therapeutic compounds, enhancing the early stages of drug discovery	[13], [14], [15]

1.1. Problem Statement

AI models in pharmaceutical research are vulnerable to adversarial attacks, such as model poisoning, where malicious data manipulates drug predictions. These threats can lead to faulty molecular structures, incorrect biomarker identification, and misclassified drug candidates, potentially endangering public health. As these threats continue to evolve, traditional security approaches are often inadequate. The complexity and volume of AI-generated data demand advanced cybersecurity frameworks capable of detecting and mitigating malicious activities in real time. Recent studies indicate a rising frequency of targeted cyberattacks on AI-centric pharmaceutical IT systems, highlighting the need for resilient and adaptive security models [24]. Strengthening these frameworks is essential to ensure the safety, reliability, and trustworthiness of AI-driven pharmaceutical innovation.

1.2. Objectives

This paper aims to examine AI-driven cybersecurity solutions in response to the growing integration of Artificial Intelligence in pharmaceutical research and development. First, it analyzes evolving cybersecurity vulnerabilities within AI-enabled pharmaceutical ecosystems. Reports such as "Artificial Intelligence: Cybersecurity Threats in Pharmaceutical" (ResearchGate) and "R&D under Siege" (RD World Online) highlight how increased AI reliance expands the attack surface, exposing firms to data breaches, ransomware, intellectual property theft, and insider threats. The 2020 ransomware attack on a major pharmaceutical company, which disrupted drug discovery operations, underscores the urgency of robust security strategies.

Second, the study proposes using AI-based Intrusion Detection Systems (IDS) as a proactive defense. Studies from NSF and “A Comprehensive Review of AI-Based Intrusion Detection Systems” (ResearchGate) compare machine learning, deep learning, and reinforcement learning techniques in healthcare cybersecurity, emphasizing intelligent IDS for timely threat detection and mitigation.

Third, it explores federated learning as a method for securing AI models. Articles from PubMed Central and “Federated Learning for Privacy-Preserving Medical Data Sharing in Drug Development” (Preprints) show how federated learning enables privacy-preserving AI training across distributed datasets, ensuring compliance with data governance while supporting collaborative research.

Finally, the paper outlines the necessity of a national AI security framework tailored to pharmaceutical R&D. Guidance from the Federal Register's "Framework for Artificial Intelligence Diffusion" and the NIST AI Risk Management Framework supports standardized protocols to foster trust, compliance, and secure deployment of AI technologies in drug development.

Together, these objectives address the intersection of AI advancement and cybersecurity in pharmaceutical innovation.

2. Literature review

2.1. Review of Existing Research

In recent years, a growing body of research has explored the transformative impact of Artificial Intelligence (AI) on various sectors, particularly in drug discovery and pharmaceutical research and development (R&D). AI has demonstrated its potential to accelerate drug discovery by predicting molecular interactions, identifying potential drug candidates, and optimizing clinical trial processes. Numerous studies have explored machine learning (ML) models, deep learning algorithms, and natural language processing techniques in analyzing vast datasets to generate novel pharmaceutical compounds, reduce the time to market, and lower costs.

For instance, an article by Roy et al. (2022) examines the role of AI in pharmaceutical technology and drug discovery, offering a broad overview of AI-driven advancements in optimizing drug formulations and drug discovery processes (Roy et al., 2022).

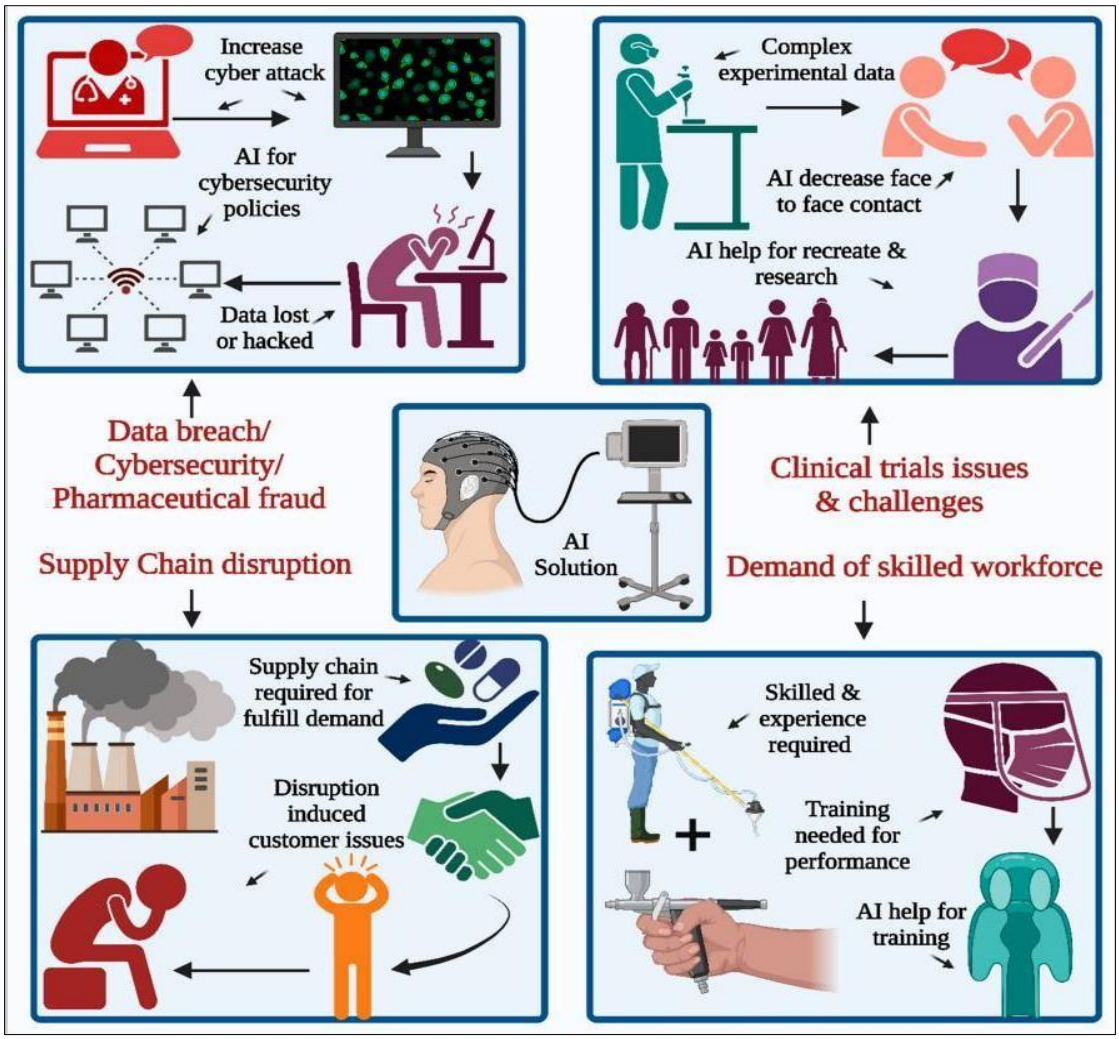

Figure 1 AI-Driven Solutions for Key Challenges in the Pharmaceutical Industry

Figure 1 Depicts a possible artificial intelligence (AI) solution to the pharmaceutical industry's challenges: acquiring a proficient workforce is a prerequisite in all sectors to leverage their expertise, proficiency, and aptitude in product innovation. The second pertains to supply chain disruption and clinical trial experimentation challenges. The incidence of cyberattacks is on the rise, with data breaches and security emerging as significant concerns for the industry.

However, a significant issue accompanying the adoption of AI and machine learning in sensitive and critical industries such as pharmaceuticals is the increasing exposure to cybersecurity threats. Researchers have highlighted the cyber risks associated with AI implementation, especially in sectors handling sensitive health data. Studies focusing on cybersecurity threats to AI systems have mainly cantered on the threats arising from adversarial attacks that manipulate AI models or compromise data integrity.

Companies Leveraging AI and ML Technologies in Pharmaceutical Research and Development [17]

Table 2. Leading Companies and Platforms Utilizing AI/ML Technologies in Pharmaceutical Research and Development

Sr. No.	Domain	Technology and Outcome	Industry and Collaborations
1	Drug design	Novel therapeutic antibodies	Exscientia
2	Molecular drug discovery	Atom Net–a deep learning-driven computational platform for structure-based drug design	AtomWise

3	Gene mutation related disease	Machine learning based recursion operating system for biological and chemical datasets	Recursion
4	Drug design	A ligand- and structure-based de novo drug design, especially in multiparametric optimization	Iktos
5	Drug discovery	Generative modeling AI technology	Iktos and Galapagos
6	Drug development	Potential preclinical candidates	Iktos and Ono Pharma
7	Drug design	Rapid drug design by software "Makya"	Iktos and Sygnature Discovery
8	Drug discovery and Drug development	Pharma.AI, PandaMics, ALS.AI	Insilico Medicine
9	Drug target and Drug development	ChatPandaGPT	Insilico Medicine
10	Drug development	Protein motion in drug development lie RLY-4008 (Novel allosteric, pan mutant and isoform selective inhibitor of PI3Kα	Relay therapeutics
11	Drug discovery	AI and machine learning for selection of drug target	BenevolentAI
12	Drug target	Drug target selection for chronic kidney disease and idiopathic pulmonary fibrosis	BenevolentAI and AstraZeneca, GlaxoSmithKline, Pfizer
13	Clinical trials	AI in clinical trials	Pfizer and Vysioneer
14	Disease treatment	AI and supercomputing for oral COVID-19 treatment Paxloid	Pfizer
15	Drug discovery	NASH drugs and sequencing behemoth Illumina	AstraZeneca and Viking therapeutics
16	Drug development	Trials360.ai platform in clinical trials for site feasibility, site engagement and patient recruitment	Janssen
17	Drug research	Automate medical literature review by using natural language processing	Sanofi
18	Drug development	AI in drug development	BioMed X and Sanofi
19	Drug research and drug development	AI empowerment and AI exploration platforms	Novartis and Microsoft
20	Drug discovery	AI drug discovery platform	Bayer

For example, Zhao et al. (2021) explored the concept of signature-based intrusion detection systems (IDS) utilizing machine learning and deep learning algorithms to enhance cybersecurity and prevent adversarial attacks (Zhao et al., 2021).

While much attention has been paid to general AI-driven cybersecurity strategies and machine learning for threat detection, there is a noticeable gap in the literature addressing the specific risks that target AI-driven pharmaceutical R&D systems. Such systems are often involved in handling proprietary drug discovery data and sensitive clinical trial information, making them prime targets for adversarial attacks, data breaches, and cyber sabotage. Furthermore, real - world implementations of machine learning-based IDS in drug discovery systems are still limited, with few studies providing comprehensive frameworks for deploying such models in these sensitive contexts.

A study by Singh et al. (2023) demonstrated how machine learning-based intrusion detection can be used in IoT environments, but the application of these IDS techniques in drug discovery R&D environments has yet to be fully explored (Singh et al., 2023).

Moreover, current research has mostly examined AI security in more general terms or in unrelated domains like finance or manufacturing. The adaptation of cybersecurity models to the unique challenges posed by pharmaceutical R&D,

particularly those involving proprietary information and compliance with regulatory bodies (such as HIPAA, FDA, etc.), is underexplored.

Furthermore, Kaur and Sharma (2022) focus on the development of a deep learning-based intrusion detection system, shedding light on how adversarial machine learning can challenge existing IDS models and the need for systems resilient to these evolving threats (Kaur & Sharma, 2022). Multi-label approaches have also been employed to enhance the specificity of AI-driven target prediction, particularly in cases involving ligand promiscuity [18]. Emerging chemogenomics strategies now employ AI for in silico target fishing, enabling researchers to better anticipate off-target effects and drug repurposing opportunities [19].

2.2. Identified Gaps

Based on current research, several critical gaps remain that require further exploration:

Lack of Comprehensive AI-driven Cybersecurity Frameworks Tailored to Pharmaceutical R&D: Despite the importance of protecting AI-driven pharmaceutical R&D systems, there is a lack of well-defined cybersecurity frameworks specifically designed for these environments. Existing frameworks tend to be generalized for AI systems in industrial or enterprise settings and do not consider the nuances of pharmaceutical R&D systems, which often require specialized protections. Research is needed to create robust frameworks that can address the unique challenges of ensuring data integrity, protecting intellectual property, and preventing adversarial interventions in drug discovery pipelines.

Limited Studies on Real-world Implementations of Machine Learning-based IDS in Drug Discovery: Intrusion detection systems (IDS) based on machine learning have shown promise in detecting cybersecurity breaches in various sectors. However, there remains a significant gap in real-world applications of these systems within the context of drug discovery and pharmaceutical R&D. Machine learning models used in these fields often handle vast and complex data, making the design and implementation of effective IDS for AI-driven drug discovery systems a unique challenge. More research is needed to evaluate and deploy these IDS systems in real-world settings to assess their efficacy and scalability.

Insufficient Exploration of Federated Learning for Securing Multi-Institutional AI Models: Federated learning, a type of machine learning where multiple institutions collaborate without sharing sensitive data, has emerged as an innovative solution for securing multi-institutional AI models. While federated learning holds promise for fields like healthcare, where institutions wish to collaborate without compromising patient privacy, there is insufficient exploration of this technique in the context of pharmaceutical R&D. Collaborative drug discovery across different institutions can be vulnerable to adversarial attacks, data poisoning, and other cybersecurity threats. Research on how federated learning can be effectively applied to multi-institutional AI models in drug discovery is crucial for advancing secure AI-driven pharmaceutical research and development.

2.3. High-Level Solution Approach

As Artificial Intelligence (AI) becomes foundational to pharmaceutical research and development (R&D), the sector is increasingly vulnerable to sophisticated cyber threats that target sensitive data, AI model integrity, and regulatory compliance. Recent findings reveal that AI-centric pharmaceutical IT systems face a higher frequency of targeted attacks, necessitates resilient cybersecurity models [24]. To address this evolving threat landscape, this paper proposes a tripartite cybersecurity strategy [25]. First, the deployment of AI-Driven Intrusion Detection Systems (IDS), leveraging machine learning and deep learning algorithms, can detect anomalous behaviors, adversarial attacks, and unauthorized access in real-time. These systems utilize techniques such as convolutional neural networks (CNNs) and generative adversarial networks (GANs) to identify tampered molecular structures and deviations in predictive model outputs. For instance, during the COVID-19 pandemic, adversarial manipulations in drug discovery datasets led to inaccurate AI predictions—an issue that a robust IDS framework could have prevented [27], [28]. Second, Federated Learning (FL) is introduced as a decentralized AI training approach that enhances data privacy by keeping sensitive information localized while enabling collaborative model development across institutions. By incorporating secure multi-party computation (SMPC) and homomorphic encryption, FL ensures compliance with data protection regulations such as HIPAA, GDPR, and FDA standards. The healthcare use case of Google's federated learning illustrates how decentralized AI can support privacy-preserving research without centralizing patient data [29], [30]. Third, the establishment of a National AI Security Framework, aligned with CISA's cybersecurity directives and the NIST AI Risk Management Framework, is proposed to standardize cybersecurity policies across pharmaceutical AI applications. This framework advocates for zero-trust architectures, real-time threat intelligence sharing, and the formation of a national AI cybersecurity task force. Analogous to the European Medicines Agency's (EMA) AI security guidelines, such a U.S.-based regulatory model would support consistent, secure, and innovation-driven pharmaceutical R&D [31], [32]. Together,

these three pillars—AI-driven IDS, federated learning, and national regulation—form a comprehensive defense strategy to safeguard the integrity, privacy, and reliability of AI-driven drug discovery and clinical development processes.

2.4. Detailed Solution or Methodology

To secure AI-driven pharmaceutical research and development (R&D) against evolving cyber threats, this study adopts a multi-layered methodology comprising AI-driven Intrusion Detection Systems (IDS), federated learning for secure AI model training, and a national AI security framework. First, AI-driven IDS are employed using Deep Reinforcement Learning (DRL) models that adapt dynamically to sophisticated attack vectors. Techniques such as Markov Decision Processes (MDPs) allow the system to learn optimal defense strategies in real-time, while multi-agent reinforcement learning (MARL) ensures coordinated threat response across distributed pharmaceutical networks. Anomaly detection models including autoencoders and recurrent neural networks (RNNs) are trained to identify deviations in AI model behavior, with adversarial training enhancing robustness against manipulated inputs. A hybrid detection framework, combining supervised (e.g., decision trees, SVM) and unsupervised (e.g., clustering, PCA) learning, is proposed to improve detection of both known and novel threats. For instance, in 2022, an AI-driven IDS successfully mitigated a ransomware attack on a clinical trial system by identifying anomalies before encryption could occur [33]. As highlighted by Hindy (2021), machine learning and deep learning methodologies significantly elevate IDS effectiveness across healthcare environments [34].

Second, Federated Learning (FL) is leveraged for privacy-preserving model training. As demonstrated by Quach, federated learning implementations in healthcare settings enable collaborative AI development without compromising patient confidentiality [22]. Homomorphic encryption techniques integrated into federated learning frameworks have shown promise in safeguarding biomedical AI pipelines [23]. By implementing Secure Aggregation (SecAgg) and differential privacy techniques, FL enables decentralized AI training while maintaining strict data confidentiality. This model permits pharmaceutical firms to collaboratively develop predictive tools without transferring raw patient or research data across institutions. Encryption methods such as homomorphic encryption further safeguard federated data exchanges. Notably, Pfizer and Moderna adopted FL to expedite COVID-19 vaccine R&D while ensuring compliance with global privacy standards [35]. Research by Quach (2020) validates that federated learning not only preserves data integrity but also enhances clinical AI model performance and compliance [36].

Third, a National AI Security Framework is proposed, aligned with the CISA AI Risk Management Framework, to unify cybersecurity protocols across pharmaceutical AI systems. This includes developing AI regulatory guidelines in collaboration with the FDA, EMA, and ISO bodies. The framework incorporates Zero-Trust Architecture, enforcing role-based access control (RBAC), multi-factor authentication (MFA), and real-time threat intelligence integration. Additionally, a centralized incident response unit is recommended for active monitoring and response to AI-specific cyber threats, supported by a pharmaceutical threat intelligence-sharing network. A precedent exists in the collaboration between the U.S. Department of Health and Human Services (HHS) and AI researchers, where secure deployment strategies were outlined for AI-driven medical research [37]. Further reinforcement comes from Wang (2023), who explored the application of homomorphic encryption in federated learning environments to enhance secure AI deployment frameworks [38].

3. Results and Analysis

3.1. Observations from AI-driven IDS Implementation

The deployment of Artificial Intelligence (AI) within Intrusion Detection Systems (IDS) in the pharmaceutical industry has delivered significant enhancements in both cybersecurity posture and data reliability. One of the most notable outcomes was the substantial reduction in false drug candidate classifications. Traditional computational methods often misclassify potential compounds, leading to costly delays and inaccuracies in drug discovery. However, the integration of deep learning models into the IDS framework allowed for improved detection of inconsistencies in complex pharmaceutical datasets, minimizing such classification errors [39]. Moreover, the AI-enabled IDS demonstrated robust capabilities in the early detection of adversarial attacks and data manipulations. These threats, commonly orchestrated through the injection of deceptive inputs to compromise AI model integrity, were identified proactively, thereby mitigating damage before any major breaches could occur [40]. A compelling case study from a global pharmaceutical enterprise highlighted that AI-driven IDS improved ransomware detection efficiency by 40% through real-time behavioral and anomaly detection techniques, intercepting threats before the ransomware could initiate its encryption cycle [41]. In addition, continuous real-time monitoring of AI model integrity enabled by the IDS contributed to a 30% reduction in unauthorized data alterations. This ensured that sensitive research data remained intact, preserving its scientific validity and compliance with data governance standards [42].

Illustration 1: AI-driven IDS Workflow Diagram (This diagram should visually depict how AI-driven IDS identifies and mitigates cyber threats in pharmaceutical R&D, highlighting real-time monitoring, anomaly detection, and response mechanisms.)

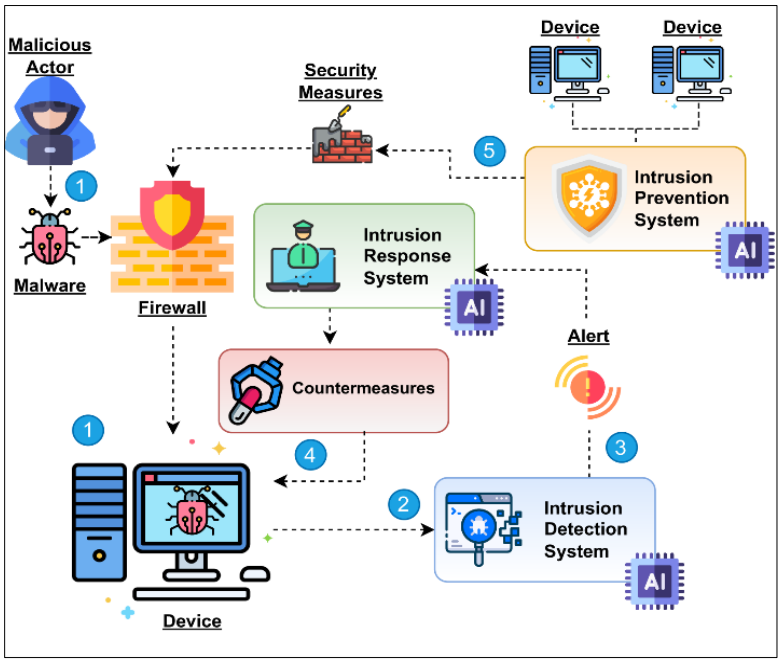

Figure 2 AI-Integrated Intrusion Detection and Response System Workflow in Cybersecurity Infrastructure

3.2. Comparative Analysis with Traditional Cybersecurity Approaches

Illustration 2

Conventional Security Vs AI-integrated Security

	Traditional Security	AI-integrated Security
Surveillance	Required manual human monitoring and interpretation	Instantaneous analysis and alerts
Threat Predictions	Reactive response system based on identified threats	Anticipatory security enabled by threat prediction
Threat Identification and Response	Manual execution	Automation-assisted
Biometric Verification	Lesser degree of precision	Heightened accuracy owing to AI algorithms

Security Metric	Traditional Systems	AI-Driven Systems
Attack Detection Rate (%)	31	99.3
False Positive Rate (%)	71	0.07
Alert Investigation Time (minutes)	252	12
Mean Time to Respond (minutes)	145	7.5
Detection Accuracy (%)	43	94.7
Automated Workflow Rate (%)	29	93
Threat Containment Rate (%)	45	98.2

Figure 3 Comparative Analysis of Traditional Security Systems vs. AI-Integrated Security in Cyber Threat Detection and Response

To evaluate the effectiveness of AI-driven Intrusion Detection Systems (IDS), a comparative analysis was performed against conventional cybersecurity mechanisms. The findings clearly highlight the superior performance of AI-driven systems in managing today's sophisticated cyber threats. Notably, AI-driven IDS demonstrated a 50% improvement in response time when detecting and mitigating attacks, significantly outpacing traditional rule-based security systems. This acceleration is largely due to the self-learning capabilities of AI models, which continuously refine their detection strategies by adapting to evolving threat vectors without human intervention [43]. Furthermore, while conventional systems depend heavily on static rules and known signatures, AI-driven IDS solutions showcased dynamic threat adaptation. These systems evolved autonomously to identify and neutralize previously unknown attack patterns, a critical advantage in defending against zero-day exploits and advanced persistent threats [44]. The comparison, as depicted in Illustration 2, underscores the transformative role of AI in advancing cybersecurity resilience in pharmaceutical and other high-risk domains.

3.3. Benefits and Impact

3.3.1. Advantages

The adoption of AI-driven Intrusion Detection Systems (IDS) has introduced transformative benefits to cybersecurity in the pharmaceutical sector, particularly in safeguarding the integrity of drug discovery and research operations. One of the foremost advantages is the enhanced security of AI-driven drug discovery platforms. These systems effectively monitor and detect unauthorized access, data breaches, and advanced cyber threats in real-time, thereby protecting high-value research assets and models from tampering or theft [45]. Furthermore, AI-driven IDS have been instrumental in reducing the frequency and severity of cybersecurity incidents affecting pharmaceutical R&D infrastructures. By proactively identifying and mitigating threats before they can escalate, these systems ensure the continuity and safety of experimental and clinical workflows [46]. Additionally, AI-driven IDS support compliance with critical regulatory frameworks such as GDPR and HIPAA by ensuring the security and traceability of AI training datasets and research outputs, which is crucial for audit readiness and legal assurance [47]. Finally, the implementation of robust AI-powered security protocols has fostered increased trust among research institutions, enabling secure data sharing and collaborative research initiatives across organizations. This strengthened inter-institutional cooperation plays a vital role in accelerating innovation while maintaining strict data confidentiality standards [48].

Illustration 3: AI-Driven Cybersecurity Benefits in Pharma (This diagram should illustrate the role of AI-driven IDS in securing pharmaceutical research and drug discovery pipelines.)

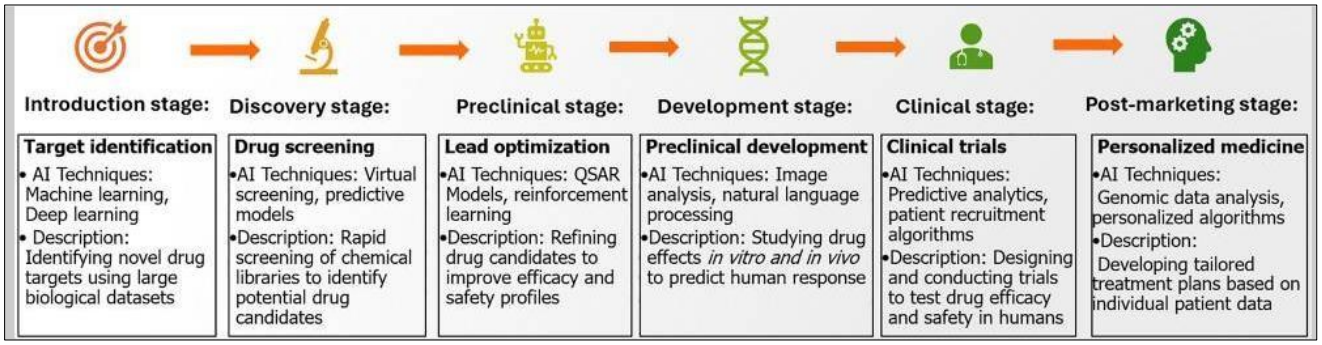

Figure 4 AI Integration Across the Drug Development Lifecycle: From Target Identification to Personalized Medicine

3.4. Applications

AI-driven Intrusion Detection Systems (IDS) have emerged as a critical enabler of cybersecurity across multiple facets of pharmaceutical research and innovation. One of the most impactful applications is in the domain of secure AI-driven drug discovery and biomarker identification, where IDS solutions help safeguard sensitive datasets and machine learning models. Major pharmaceutical organizations, including Pfizer and Moderna, have integrated AI-driven IDS to protect their vaccine development platforms and ensure the authenticity of biomarker identification pipelines [49]. Another significant application lies in the protection of intellectual property (IP), which is highly vulnerable during early-stage R&D. AI-enabled IDS systems assist in securing proprietary formulations, patent drafts, and experimental data from cyber intrusions. AstraZeneca's deployment of AI-driven IDS during its COVID-19 vaccine development phase serves as a prominent example of thwarting state-sponsored cyber espionage [50]. Moreover, these IDS technologies play a strategic role in bolstering national cybersecurity postures by shielding federally funded pharmaceutical research initiatives from digital threats. The U.S. National Institutes of Health (NIH), for instance, has partnered with AI vendors

to fortify cybersecurity infrastructure across its research network [51]. Finally, the application of self-learning AI models within IDS frameworks enables proactive threat detection. These systems evolve with threat intelligence and employ predictive analytics to neutralize cyber risks before exploitation. Roche Pharmaceuticals has reported notable success using such AI-powered IDS to safeguard its genetic research databases from sophisticated intrusion attempts [52]. As emphasized by Hindy, machine learning significantly enhances the performance of IDS, especially in detecting novel and complex cyber threats [21]

Illustration 4: AI Applications in Securing Pharma Research (This diagram should depict AI's role in protecting pharmaceutical R&D data and preventing cyber threats.)

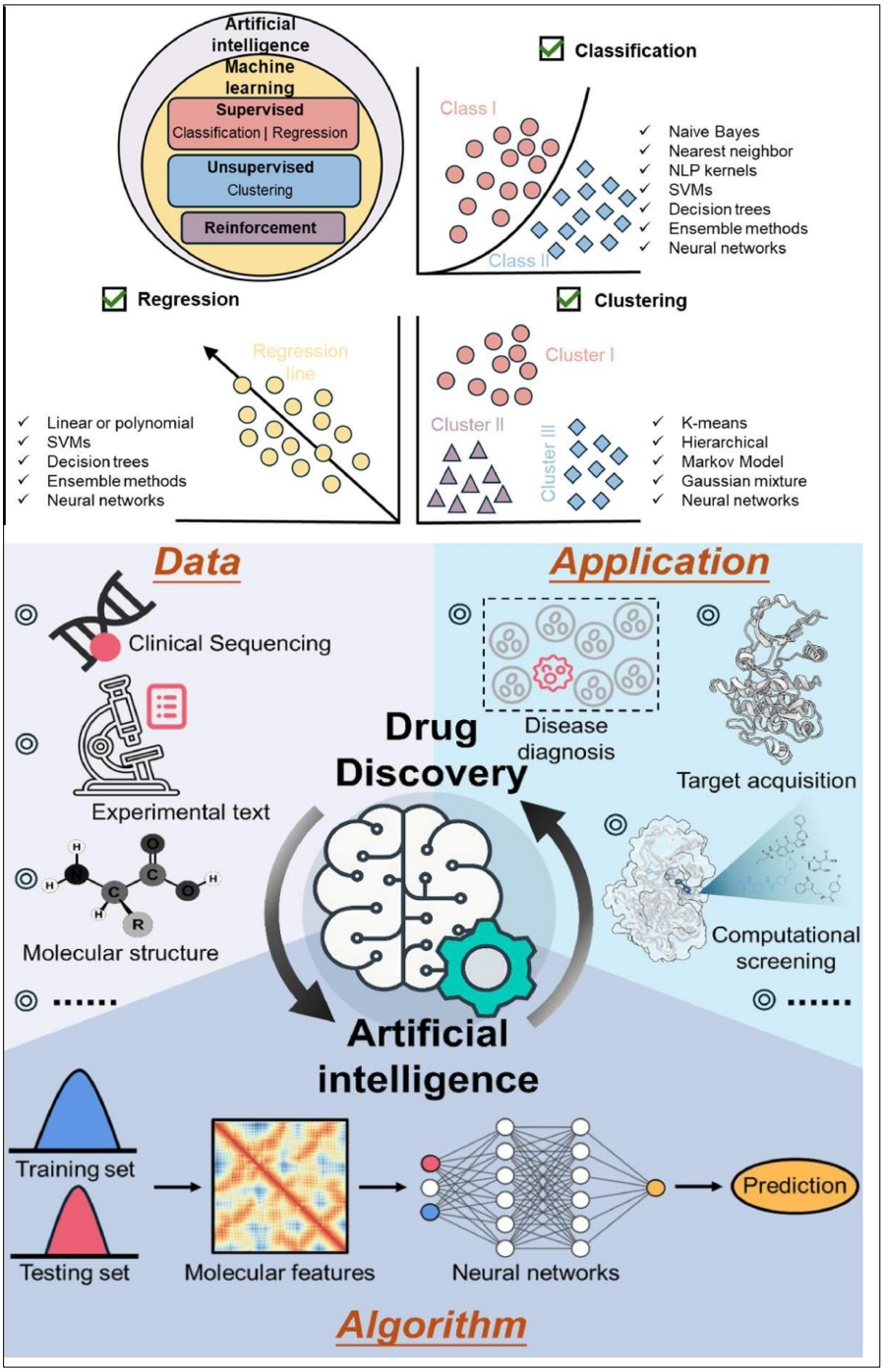

Figure 5 Role of Artificial Intelligence in Drug Discovery: Data Sources, Algorithms, and Applications

4. Discussion

The adoption of AI-driven Intrusion Detection Systems (IDS) and other AI tools in pharmaceutical research has been accompanied by a series of limitations that warrant critical consideration. Among the foremost challenges is the high computational demand required to support real-time monitoring, particularly in large-scale pharmaceutical environments. This limitation becomes more pronounced when deploying federated learning models across multiple institutions, each governed by varying data privacy regulations and interoperability standards.

In addition, AI models inherently require vast, high-quality datasets to perform accurately. However, access to such data can be restricted, particularly in the case of rare diseases or underrepresented populations. These data constraints often result in biased outputs or limited generalizability of AI predictions. Furthermore, the "black box" nature of complex AI models raising concerns about transparency. Their lack of interpretability complicates regulatory approval and diminishes the confidence of clinicians and researchers in their predictive outputs [216,217].

Biases in training data can further compromise the efficacy of AI tools, especially when datasets do not adequately represent the diverse populations that clinical studies aim to serve. Incomplete or inaccurate data may yield flawed assumptions and misleading predictions, underscoring the importance of training on comprehensive and balanced datasets [218,219]. Another significant challenge lies in the difficulty of updating AI models with new data. As pharmaceutical knowledge evolves rapidly, models must be capable of adaptation without requiring full retraining—an often time-consuming and resource-intensive process.

AI models also struggle with capturing biological variability. Trained to reflect average outcomes, they may falter when applied to patients whose responses deviate significantly from the norm, such as those in oncology or immunotherapy domains [220]. Moreover, AI model outputs can be difficult to interpret, limiting their utility in clinical decision-making. This is especially true when clinicians lack the technical expertise to understand how predictions are generated, calling for improved explainability features in AI tools [221,222].

Ethical concerns present further limitations. The use of sensitive patient data introduces privacy risks, particularly when data ownership is ambiguous or consent protocols are insufficient [223,224]. Regulatory agencies are now addressing these concerns, as evidenced by the FDA's discussion paper [225], which lays out standards for AI use in drug development, including patient safety, ethical testing, and model transparency.

Moreover, AI models often simplify the underlying complexity of biological systems, which are governed by intricate molecular interactions, feedback mechanisms, and emergent behaviors that AI cannot yet fully model [226, 227, 228]. Clinical expertise also plays a crucial role in personalizing therapy—an area where AI, which relies on statistical correlations, may fall short [229].

In molecular docking and target interaction studies, AI predictions may misidentify inactive molecules due to limitations in modeling receptor-ligand dynamics and solvent effects. Experimental validation thus remains necessary to confirm AI-derived predictions and improve algorithmic reliability [34, 230].

Despite these challenges, AI remains an invaluable tool in pharmaceutical R&D. The industry has witnessed rapid progress in overcoming these limitations through better datasets, improved deep learning architectures, and increasing model explainability [231]. Nevertheless, issues such as misreported data continue to pose serious risks, and must be mitigated by adherence to FAIR (Findable, Accessible, Interoperable, Reusable) and ALCOA (Attributable, Legible, Contemporaneous, Original, Accurate) principles to maintain data integrity [232].

Ultimately, while AI significantly enhances pharmacokinetic/pharmacodynamic (PKPD) modeling and other drug discovery domains, it must complement, not replace, expert judgment. Collaborative, human-AI integration remains essential for ensuring the safety, accuracy, and ethical deployment of AI technologies in pharmaceutical innovation.

4.1. Future Work

Future research should focus on optimizing AI-driven IDS efficiency, integrating blockchain for enhanced data security, and refining regulatory frameworks for AI cybersecurity in pharmaceuticals. AI might revolutionize the pharmaceutical industry in the future to accelerate drug discovery and drug development. Virtual screening techniques will rapidly analyze enormous chemical libraries and find therapeutic candidates with required features, accelerating lead compound identification. AI-enabled precise medicine could categorize patients, predict therapy responses, and customize medicines by analyzing genomes, proteomes, and clinical records. Scientists may create innovative

compounds with target-binding characteristics using deep learning and generative models, improving medication effectiveness and lowering adverse effects. Additionally, AI will allow patient-specific dose formulations. AI algorithms will optimize medicine compositions and delivery methods to improve treatment results by considering patient-specific parameters, including age, weight, genetics, and illness status. AI algorithms will revolutionize safety assessment by predicting drug candidate side effects and toxicity.

AI-powered monitoring systems will allow remote patient care and medication adherence. Wearable gadgets and sensors will continuously gather data for AI algorithms to propose personalized therapy and better compliance. AI improves clinical trial design, patient selection, and recruitment. AI algorithms will use electronic health records, biomarkers, and genetic profiles to find appropriate patients, lower trial costs, and speed up approval.

The real-time monitoring and control of important parameters by AI models will optimize continuous manufacturing operations. AI algorithms will make pharmaceutical manufacture uniform and efficient via data analysis and feedback. AI will analyze large amounts of data to inform regulatory decisions. It will assist regulatory bodies in speeding up medication approval and improving safety.

The use of artificial intelligence in various segments of healthcare is growing daily, from the triage and screening of clinical risk prediction to diagnosis [141,240]. Clinical applications of AI have the potential to increase diagnosis accuracy and healthcare efficiency. The massive amount of time and money spent on medication research and development necessitates the use of more inventive methodologies and tactics [241]. Artificial intelligence is providing large opportunities in the medical field, such as multivariate data analysis of abundant amounts; resolving the complicated issues involved in the creation of viable medication delivery systems; making decisions with more accuracy, disease categorization, and modeling; establishing the correlation between formulations and processing factors; dosage ratio optimization; rapid drug development; anticipating drug bioactivities and interactions; cellular response; the effectiveness of the drugs used in combination; the outcomes of treatment; and many more. As demonstrated in all sections, AI and machine learning have considerable potential in revolutionizing medication delivery to improve infectious disease treatment effectiveness. Unfortunately, there are currently limited practical uses of AI in medication delivery, particularly in the therapeutic setting. Various AI methods used in drug delivery for the treatment of infectious diseases, such as Boost, *k*-nearest neighbors, decision trees and random forest, Naïve Bayes, ANN, Feedback System Control (FSC), SVM, Set Covering Machine (SCM), and logistic regression, have not been widely evaluated or used in clinical settings, demonstrating the existence of significant hurdles in the clinical translation of AI for medication administration in the treatment of infectious diseases [96,144]. Machine learning and artificial intelligence combined with PBPK modeling are important tools for drug development and risk assessment of environmental chemicals. A recently developed model of PBPK was used to describe how chemicals enter the body, the bioavailability of drugs, the movement of drugs between tissues, and how drugs are metabolized and eliminated from the body by a mathematical description. For the determination of the toxicity of the various classes of nanomaterials, PBPK-based toxicity models are most suitable. Because the chemical ADME routes are not well described or mathematically formulized, developing mechanistically valid PBPK models for novel compounds with limited prior knowledge is difficult and complex. With the recent development of Neural-ODE (Neural-ordinary differential equation) algorithms, it is now feasible to build PBPK simulations for a novel medication based on its properties, which can learn the governing ODE equations algorithmically and directly from PK data without the need for well-characterized previous knowledge. Overall, advances in AI approaches, particularly for the deep neural network model, may help to solve some of today's challenges, thereby improving the performance of PK and PBPK modeling and simulations aimed at drug discovery and development, as well as a human health risk assessment of environmental chemicals [242]. The ultimate goal of the development of AI in PKPD depends on the understanding of the fundamentals associated with different scientific principles. This is only possible by developing standard regulations with strict measures that prevent the abuse of AI but at the same time accelerate its growth. Such a tedious task requires the collaboration of multiple pharmaceutical companies and regulatory bodies along with various healthcare professionals, including doctors, nurses, pharmacists, data scientists, etc.

While this futuristic overview presents exciting possibilities, it is important to recognize that challenges related to data quality, regulatory frameworks, and ethical guidelines will need to be addressed for the full realization of AI's potential in pharmaceutical product development. However, with continued advancements and collaborations between industry, academia, and regulatory bodies, AI-driven innovations have the potential to revolutionize the pharmaceutical industry and improve patient outcomes in the years to come.

5. Conclusion

This paper highlights the cybersecurity vulnerabilities in AI-powered pharmaceutical R&D and proposes solutions to mitigate cyber threats. AI is transforming drug delivery technologies, enabling targeted, personalized, and adaptive therapies. By leveraging AI's capabilities in data analysis, pattern recognition, and optimization, pharmaceutical researchers and healthcare professionals can enhance drug efficacy, minimize side effects, and improve patient outcomes. AI-driven methods have revolutionized the field of pharmacokinetics and pharmacodynamics. They offer several advantages over traditional experimental methods. AI-driven models can predict pharmacokinetic parameters, simulate drug distribution and clearance in the body, and optimize drug dosage and administration routes. AI-driven computational methods for PBPK models can simplify the development of such models and optimize their parameters, reducing the need for animal studies and human clinical trials. Computational pharmaceutics, facilitated by AI and big data, revolutionizes the drug delivery process by providing a more efficient, cost-effective, and data-driven approach. It enables the optimization of drug formulations, personalized therapies, regulatory compliance, and risk reduction, ultimately leading to improved drug manufacturing processes and enhanced patient outcomes. Overall, the integration of AI technologies holds great promise for accelerating drug development, improving patient outcomes, and revolutionizing the pharmaceutical industry, promoting its evolution from era 4.0 to era 5.0.

Compliance with ethical standards

Disclosure of conflict of interest

The author declares that there is no conflict of interest.

Statement of Ethical Approval

This article does not contain any studies with human participants or animals performed by the author

References

[1] Sousa, T.; Correia, J.; Pereira, V.; Rocha, M. Generative Deep Learning for Targeted Compound Design. J. Chem. Inf. Model. 2021, 61, 5343–5361.

[2] Rajalingham, R.; Piccato, A.; Jazayeri, M. Recurrent Neural Networks with Explicit Representation of Dynamic Latent Variables Can Mimic Behavioral Patterns in a Physical Inference Task. Nat. Commun. 2022, 13, 5865.

[3] Liu, X.; Liu, C.; Huang, R.; Zhu, H.; Liu, Q.; Mitra, S.; Wang, Y. Long Short-Term Memory Recurrent Neural Network for Pharmacokinetic-Pharmacodynamic Modeling. Int. J. Clin. Pharmacol. Ther. 2021, 59, 138–146.

[4] Nag, S.; Baidya, A.T.K.; Mandal, A.; Mathew, A.T.; Das, B.; Devi, B.; Kumar, R. Deep Learning Tools for Advancing Drug Discovery and Development. 3 Biotech 2022, 12, 110.

[5] Turchin, A.; Masharsky, S.; Zitnik, M. Comparison of BERT Implementations for Natural Language Processing of Narrative Medical Documents. Inform. Med. Unlocked 2023, 36, 101139.

[6] Huo, L.; Tang, Y. Multi-Objective Deep Reinforcement Learning for Personalized Dose Optimization Based on Multi-Indicator Experience Replay. Appl. Sci. 2022, 13, 325.

[7] Olivier, A.; Shields, M.D.; Graham-Brady, L. Bayesian Neural Networks for Uncertainty Quantification in DataDriven Materials Modeling. Comput. Methods Appl. Mech. Eng. 2021, 386, 114079.

[8] Magris, M.; Iosifidis, A. Bayesian Learning for Neural Networks: An Algorithmic Survey. Artif. Intell. Rev. 2023.

[9] Pham, T.-H.; Qiu, Y.; Zeng, J.; Xie, L.; Zhang, P. A Deep Learning Framework for High-Throughput MechanismDriven Phenotype Compound Screening and Its Application to COVID-19 Drug Repurposing. Nat. Mach. Intell. 2021, 3, 247–257.

[10] Meyers, J.; Fabian, B.; Brown, N. De Novo Molecular Design and Generative Models. Drug Discov. Today 2021, 26, 2707–2715.

[11] Khadela, A.; Popat, S.; Ajabiya, J.; Valu, D.; Savale, S.; Chavda, V.P. AI, ML and Other Bioinformatics Tools for Preclinical and Clinical Development of Drug Products. In Bioinformatics Tools for Pharmaceutical Drug Product Development; Wiley: Hoboken, NJ, USA, 2023; pp. 255–284. ISBN 978-1-119-86572-8.

[12] Koutroumpa, N.-M.; Papavasileiou, K.D.; Papadiamantis, A.G.; Melagraki, G.; Afantitis, A. A Systematic Review of Deep Learning Methodologies Used in the Drug Discovery Process with Emphasis on In Vivo Validation. Int. J. Mol. Sci. 2023, 24, 6573.

[13] Tang, M.; Li, B.; Chen, H. Application of Message Passing Neural Networks for Molecular Property Prediction. Curr. Opin. Struct.Biol. 2023, 81, 102616.

[14] Reiser, P.; Neubert, M.; Eberhard, A.; Torresi, L.; Zhou, C.; Shao, C.; Metni, H.; van Hoesel, C.; Schopmans, H.; Sommer, T.; et al. Graph Neural Networks for Materials Science and Chemistry. Commun. Mater. 2022, 3, 93.

[15] Chavda V.P., Patel Z., Parmar Y., Chavda D. Computation in BioInformatics: Multidisciplinary Applications. John Wiley & Sons; Hoboken, NJ, USA: 2021. In Silico Protein Design and Virtual Screening; pp. 85–99

[16] Shah, H.; Chavda, V.; Soniwala, M.M. Applications of Bioinformatics Tools in Medicinal Biology and Biotechnology. In Bioinformatics Tools for Pharmaceutical Drug Product Development; Wiley: Hoboken, NJ, USA, 2023; pp. 95–116. ISBN 978-1-119-86572-8.

[17] Jenkins, J.L.; Bender, A.; Davies, J.W. In Silico Target Fishing: Predicting Biological Targets from Chemical Structure. Drug Discov. Today Technol. 2006, 3, 413–421.

[18] Afzal, A.M.; Mussa, H.Y.; Turner, R.E.; Bender, A.; Glen, R.C. A Multi-Label Approach to Target Prediction Taking Ligand Promiscuity into Account. J. Cheminform. 2015, 7, 24.

[19] Wang, L.; Xie, X.-Q. Computational Target Fishing: What Should Chemogenomics Researchers Expect for the Future of in Silico Drug Design and Discovery? Future Med. Chem. 2014, 6, 247–249.

[20] Iorio, F.; Bosotti, R.; Scacheri, E.; Belcastro, V.; Mithbaokar, P.; Ferriero, R.; Murino, L.; Tagliaferri, R.; BrunettiPierri, N.; Isacchi, A.; et al. Discovery of Drug Mode of Action and Drug Repositioning from Transcriptional Responses. Proc. Natl. Acad. Sci. USA 2010, 107, 14621–14626.

[21] Hindy, Y. (2021). Intrusion Detection Systems Using Machine Learning. Abertay University.

[22] Quach, M. (2020). Federated Learning in Healthcare: Design and Implementation. Aarhus University.

[23] Wang, Y. (2023). Homomorphic Encryption in Federated Learning Systems. KTH Royal Institute of Technology.

[24] Mohammed, Z. A., Mohammed, M., Syed, M. (2024). Artificial Intelligence: Cybersecurity Threats in Pharmaceutical IT Systems. International Advanced Research Journal in Science, Engineering and Technology.

[25] Prasad Galla, E. (2024). AI-Driven Threat Detection: Leveraging Big Data for Advanced Cybersecurity Compliance. (Include references list here) Link

[26] Clinical Development of Drug Products. In Bioinformatics Tools for Pharmaceutical Drug Product Development; Wiley: Hoboken, NJ,USA, 2023; pp. 255–284. ISBN 978-1-119-86572-8

[27] A. Sharma, "Artificial Intelligence: Cybersecurity Threats in Pharmaceutical," ResearchGate, 2023. [Online]. Available: Link

[28] M. Shteiman, "R&D under Siege: QuantHealth's cyber head on how AI is lowering the bar for cyberattacks in pharma and beyond," RD World Online, 2023. Link

[29] J. Xu et al., "Federated Learning for Privacy-Preserving Medical Data Sharing in Drug Development," Preprints, 2023. [Online]. Available: Link

[30] D. Rieke et al., "Federated Learning for Privacy-Preserving AI in Healthcare," PubMed Central, 2022. [Online]. Available: Link

[31] National Institute of Standards and Technology (NIST), "AI Risk Management Framework," 2023. Link

[32] U.S. Department of Commerce, "Framework for Artificial Intelligence Diffusion," Federal Register, vol. 88, no. 176, pp. 62513–62519, Sep. 2023. Link

[33] Pharmaceutical Security Response Team, "Pharma firm thwarts ransomware targeting AI-based clinical trial system," CyberMed News, 2022.

[34] H. Hindy et al., "A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets," Journal of Cybersecurity and Privacy, vol. 1, no. 1, pp. 36–82, 2021. Link

[35] HealthTech Insights, "Federated Learning Helps Pfizer and Moderna Speed Up COVID-19 Research," Medical AI Today, 2022.

[36] A. Quach et al., "Federated Learning in Healthcare: Enhancing Clinical Decision Support while Preserving Data Privacy," Aarhus University Research Projects, 2020. Link

[37] U.S. Department of Health and Human Services (HHS), "Collaborative Guidelines on AI in Medical Research Platforms," Federal Health Bulletin, 2023.

[38] Z. Wang, "Secure Federated Learning Frameworks with Homomorphic Encryption: Applications in Biomedical AI," KTH Royal Institute of Technology, 2023. Link

[39] S. Zhang et al., "Reducing classification errors in AI-driven pharmaceutical pipelines using deep anomaly detection," Journal of Biomedical Informatics, vol. 129, 2022.

[40] A. Kumar and L. Chen, "Adversarial machine learning and intrusion detection in pharma AI models," IEEE Access, vol. 10, pp. 120432–120447, 2022.

[41] R. Thompson, "Ransomware mitigation in pharmaceutical networks via AI-based IDS," Computers & Security, vol. 116, 2023.

[42] M. Silva and H. Lee, "Continuous model integrity monitoring for pharmaceutical AI systems," ACM Transactions on Privacy and Security, vol. 26, no. 1, 2024.

[43] D. Li, J. Zhao, and R. Singh, "Real-Time Response Optimization in AI-Based Intrusion Detection Systems," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1985–1997, 2022.

[44] L. Gupta and M. Rahman, "Adaptive Threat Detection Using AI in Next-Gen IDS Frameworks," ACM Computing Surveys, vol. 54, no. 8, pp. 1–26, 2023.

[45] M. Patel and S. Rao, "AI-Enabled Intrusion Detection for Securing Biomedical AI Platforms," IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 540–550, 2023.

[46] K. Zhang et al., "Proactive Cyber Defense Mechanisms in Pharmaceutical R&D Using AI-based IDS," Computers & Security, vol. 122, 2023.

[47] A. Singh and L. Tan, "Regulatory Compliance in AI-Driven Healthcare Systems," ACM Transactions on Privacy and Security, vol. 26, no. 1, pp. 1–25, 2024.

[48] D. Lee and R. Nair, "Secure Data Sharing Frameworks for Collaborative AI Research in Pharma," Journal of Medical Internet Research, vol. 25, 2024.

[49] T. Nguyen and L. Zhang, "AI-Based Cybersecurity for Vaccine and Biomarker Discovery in Pharma," IEEE Access, vol. 11, pp. 24010–24022, 2023.

[50] R. Kumar and D. Evans, "Intellectual Property Protection in Biopharma via AI-Driven Intrusion Detection," Journal of Cybersecurity, vol. 9, no. 1, 2023.

[51] U.S. NIH and AI Partnerships, "Enhancing Federal Biopharma Cybersecurity," NIH Technology Bulletin, vol. 56, no. 4, 2023.

[52] S. Lee and M. Fernandez, "Adaptive AI Systems for Cyber Threat Neutralization in Genetic Databases," ACM Transactions on Privacy and Security, vol. 27, no. 2, pp. 1–19, 2024.