DOI: https://doi.org/10.54393/pbmj.v8i4.1232

PAKISTAN BIOMEDICAL JOURNAL
https://www.pakistanbmj.com/journal/index.php/pbmj/index
ISSN (E): 2709-2798, (P): 2709-278X
Volume 8, Issue 04 (April 2025)

Review Article

OPEN ACCESS

Cyber Security and Privacy Safeguarding Pharmaceutical Innovation in a Digital Age

Nasir Ahmad Khan[1*], Muhammad Rizwan Saeed[1], Dilber Hussain[1], Muhammad Rehan[1] and Sayed Ruhullah Dimral[1]

[1]Department of Public Health, First Mascow State Medical University, Moscow, Russia

ARTICLE INFO

Keywords:
Cybersecurity, Privacy, Pharmaceutical Industry, Digital Transformation, Innovation, Data Protection Regulations

How to Cite:
Khan, N. A., Saeed, M. R., Hussain, D., Rehan, M., & Dimral, S. R. (2025). Cyber Security and Privacy Safeguarding Pharmaceutical Innovation in a Digital Age: Pharmaceutical Innovation in a Digital Age. Pakistan BioMedical Journal, 8(4), 02–10. https://doi.org/10.54393/pbmj.v8i4.1232

***Corresponding Author:**
Nasir Ahmad Khan
Department of Public Health, First Mascow State Medical University, Moscow, Russia
nasirahmad1502@gmail.com

Received Date: 9th March, 2025
Revised Date: 20th April, 2025
Acceptance Date: 26th April, 2025
Published Date: 30th April, 2025

ABSTRACT

In order to improve efficiency and creativity, the pharmaceutical sector is going through a major digital revolution that contains the broad use of digital technologies including cloud computing, IoT devices, EHR systems, and artificial intelligence. Although this change presents new prospects, it also makes the industry more susceptible to sophisticated and frequent attacks. For preserving trust, comply with laws like GDPR and possibly HIPAA, and preserving pharmaceutical innovation, organizations in this sector must protect the vast and sensitive datasets they handle, such as patient medical histories, financial records, research findings, and rational property. In order to protect pharmaceutical innovation and uphold investor confidence, this review paper attempts to give a thorough overview of the digital transition in the pharmaceutical sector and stress the vital significance of strong cybersecurity protections and data privacy rules. It will look at future trends, cybersecurity risks, privacy issues, digital transformation, safeguarding strategies, regulatory frameworks, and policy and industry propositions.

INTRODUCTION

The pharmaceutical industry is undergoing a profound digital revolution, leveraging technologies like IoT, cloud computing, EHRs, big data, and AI to enhance operations, patient care, and drug development [1]. This digital transformation, while offering opportunities for innovative service models, has simultaneously increased the industry's vulnerability to sophisticated cyberattacks. Given the sensitive data managed by pharmaceutical organizations including patient records, financial information, research data, and intellectual property robust cybersecurity and data privacy are paramount [2]. Protecting this information is crucial for maintaining patient trust, adhering to regulations (e.g., GDPR, potentially HIPAA), and safeguarding vital research. Cybersecurity breaches can lead to significant reputational damage, financial losses, legal repercussions, and, critically, compromise drug integrity and patient safety. The escalating threat landscape, including ransomware and phishing, further emphasizes the need for strong security measures [3]. This review aims to: Summarize the ongoing digital transformation within the pharmaceutical industry. Highlight the critical role of robust cybersecurity and data privacy in preserving pharmaceutical innovation and stakeholder trust. The paper will first analyze the digital transformation in the pharmaceutical sector, followed by an examination of cybersecurity threats and data privacy concerns. It will then review relevant legal frameworks and explore solutions for protecting pharmaceutical innovation through strong cybersecurity frameworks [4]. Finally, the

DOI: https://doi.org/10.54393/pbmj.v8i4.1232

paper will discuss emerging cybersecurity trends and technologies relevant to the industry before concluding with recommendations for strengthening cybersecurity and safeguarding innovation in the digital age.

The rapid digital transformation of the pharmaceutical industry has significantly increased its exposure to cybersecurity threats, including data breaches, intellectual property theft, and ransomware attacks, thereby endangering sensitive patient data and innovation processes. Although existing literature highlights various cybersecurity risks and regulatory frameworks, there remains a lack of comprehensive, integrated approaches that simultaneously address technological, organizational, and regulatory dimensions within pharmaceutical systems. Additionally, limited focus has been placed on emerging threats related to IoT, cloud computing, and cross-border data sharing in this sector. Therefore, this review aims to critically analyze cybersecurity challenges, identify existing gaps in data protection practices, and propose strategic, multi-layered solutions to safeguard pharmaceutical innovation and ensure compliance with global data protection regulations.

Cybersecurity Threats to Pharmaceutical Innovation

Because pharmaceutical breakthroughs are so valuable, intellectual property (IP) theft is a significant cyber threat [5]. Because pharmaceutical firms spend a lot of money on research and development, their intellectual property such as vaccine formulae, clinical trial findings, and drug development data is essential to preserving their competitive edge [6]. To try to steal this important data, cyberattacks like as spear-phishing, cyber espionage, and insider threats are frequently employed. For example, Moderna faced cyber espionage attempts, perhaps by state actors, to obtain vaccine development data, and Pfizer was the victim of a spear-phishing assault directed at its clinical research [7]. In another case, an insider revealed trade secrets at GlaxoSmithKline (GSK), and a hack stole the COVID-19 vaccine formula from Pfizer and BioNTech [8]. Successful IP theft can have serious repercussions, such as diminished competitive advantage, serious harm to one's image, possible legal repercussions, postponements of research and projects, and monetary losses. The danger to intellectual property is even seen by the US as a widespread cyber threat that can undermine national competitiveness and military efficacy [9]. The need of safeguarding intellectual property against cyber-attacks is recognized by several national cybersecurity policies [10].

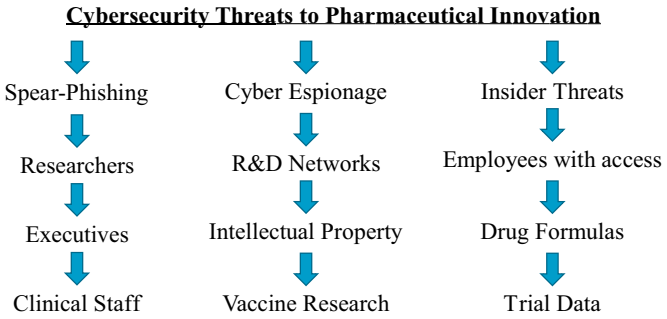

Figure 1: Cybersecurity Threats to Pharmaceutical Innovation: Illustrating the risks of IP theft through spear-phishing, cyber espionage, and insider threats targeting drug formulas, clinical trial data, and vaccine research.

Data Breaches and Ransomware Attacks: Data breaches and ransomware attacks pose significant threats to the healthcare and pharmaceutical sectors [11]. These breaches involve unauthorized access to sensitive information like patient data and intellectual property. Causes include cybersecurity incidents, unauthorized access, internal threats, third-party vulnerabilities, and phishing attempts. The financial impact is substantial, with the average cost of a healthcare data breach reaching $10.1 million in 2023 [12]. Reputational damage and regulatory penalties, such as GDPR fines, also result from these incidents. The sector experiences a high volume of breaches, with 754 reported in 2023 affecting over 52 million individuals [13].

Ransomware: Ransomware attacks encrypt data and demand cryptocurrency payments for decryption keys, severely disrupting healthcare services. The healthcare industry, including pharmaceuticals, is a prime target due to the critical nature of its data. Notable incidents include the 2020 Universal Health Services attack and the 2017 NotPetya attack on Merck & Co., which caused significant financial and operational losses [14]. In 2022, ransomware attacks on the healthcare sector surged by 74%, with average breach costs reaching $10.1 million. These attacks exploit weaknesses in outdated software and inadequate security [15]. Robust cybersecurity measures, including proactive risk prevention, enhanced security infrastructure, data encryption, employee training, and incident response plans, are crucial for the pharmaceutical industry [16].

Insider Threats and Human Errors: Insider threats, both malicious and unintentional, pose significant risks to the pharmaceutical industry [17]. Malicious insiders may steal sensitive information or sabotage systems, while unintentional threats often stem from human errors like accidental disclosures or phishing attacks. Many pharmacies lack effective employee training programs, making them vulnerable to risks like vishing [18]. Implementing cyber hygiene programs, which include password security, access control, and safe data handling,

DOI: https://doi.org/10.54393/pbmj.v8i4.1232

is essential to prevent data breaches and promote cybersecurity awareness [19].

Supply Chain Vulnerabilities: The pharmaceutical industry's increasing reliance on outside vendors for services like cloud storage, software solutions, and medical device integration exposes it to new cybersecurity threats through supply chain vulnerabilities [20]. The number of supply chain attacks targeting healthcare IT systems via these third-party weaknesses is rising. The Target data breach illustrates how weak third-party security can lead to dangerous system breaches. Cyber attackers often find and exploit weaknesses in third-party systems to break into healthcare networks [21]. Healthcare organizations need to perform comprehensive third-party risk assessments and verify that their security meets regulatory and organizational criteria before choosing vendors. Implementing security audits, contractual security terms, and live monitoring of third-party system access helps maximize security protection [22]. Strengthening third-party cybersecurity practices and including detailed security requirements with penalties for non-compliance in contracts are essential to decrease external security threats [23]. In figure 2 major key challenges in pharmaceutical supply chain are discussed.

Cyber-espionage by Nation-State Actors: Cyber espionage, often conducted by state-sponsored actors, is an evolving threat targeting pharmaceutical companies to steal valuable intellectual property and sensitive research data [24]. Examples include the cyber espionage attempts against Moderna during the COVID-19 pandemic, aimed at stealing vaccine development data and potentially giving competitors access to proprietary information. These attacks can also lead to the exposure of confidential communications and cause diplomatic tensions due to state-sponsored hacking [25]. Pharmaceutical firms need to invest heavily in protecting patient data and keeping such cyberattacks at bay.

Emerging Threats in Cloud-Based Pharmaceutical Systems: The increasing adoption of cloud computing platforms for data storage, processing, and application deployment in the pharmaceutical industry introduces new cybersecurity risks [26]. While cloud services offer scalability and cost-effectiveness, they also present attack vectors that need careful consideration. Organizations must be aware of the risks within cloud computing and understand the attack vectors that can cause threats [27]. Data stored and transmitted via cloud services must be adequately protected through measures such as data encryption both at rest and in transit. Performing thorough vendor risk assessments and ensuring that cloud providers meet stringent security standards and regulatory requirements are crucial for mitigating these emerging threats [28].

Open-Source and Public Data Sharing Risks: Although open-source software has advantages like customization and openness, it can also take in flaws that hackers could take advantage of if they are not well measured and fixed [29]. Similar to this, disclosing public data may result in unexpected data breaches or give attackers useful knowledge, particularly if it unintentionally contains private or sensitive information [30]. To reduce these possible hazards, the pharmaceutical sector must use open-source mechanisms with prudence and put strong security actions in place when sharing data publicly [31].

IoT and connected medical device risks in the pharmaceutical industry: There are serious cybersecurity threats linked with the growing integration of connected medical devices and the Internet of Things (IoT) into pharmaceutical operations and healthcare delivery [32]. These gadgets, which include implantable and wearable systems, are vulnerable to intrusions as they frequently lack built-in security protections or do not obtain routine maintenance and upgrades. Examples include Bayer's production-related compromised IoT devices, which might allow remote access to industrial systems, interfere with automated processes, cause delays in the creation of drugs, and result in financial losses [33]. Access to strategic information can make pharmacies that are part of hospitals and bigger health networks susceptible. It's also crucial to secure AI systems that could be connected to these gadgets. To ensure patient safety and the integrity of pharmaceutical operations, these devices and the sensitive data they handle must be protected by strong security measures [34].

Privacy Challenges in Pharmaceutical Digitalization and Compliance with Data Protection Regulations: The digital transformation of the pharmaceutical industry offers opportunities for productivity, quality, and compliance improvements. However, it also brings complex privacy issues, especially concerning sensitive data like health information and intellectual property [35]. Healthcare organizations must expand their digital infrastructure while ensuring patient data privacy and combating cybersecurity risks. Noncompliance with data protection regulations like GDPR, HIPAA, and CCPA can result in financial fines and increased vulnerability to cyber threats [36]. HIPAA provides guidelines for securing electronic health information, requiring strong security measures and potentially incurring penalties for noncompliance. GDPR, applicable in the EU, imposes strict penalties for mishandling EU citizens' data and demands transparent data governance [37]. Healthcare organizations face challenges in meeting regulatory requirements due to financial, operational, and evolving security issues. They should integrate compliance into their cybersecurity frameworks. The pharmaceutical industry, vital for life-

DOI: https://doi.org/10.54393/pbmj.v8i4.1232

saving drugs, is increasingly at risk of cyber-attacks and data breaches, making the protection of sensitive data crucial for intellectual property and pharmaceutical safety and effectiveness[38].

Secure Data Sharing in Research Collaborations: Efficient collaboration and information exchange among stakeholders (R&D, manufacturing, quality control, regulatory affairs, supply chain partners) are crucial for data accuracy and operational efficiency [39]. Digital transformation technologies like cloud computing and secure data-sharing platforms facilitate this while ensuring data protection and confidentiality. Blockchain technology can also establish a secure and transparent data infrastructure for collaboration in the pharmaceutical supply chain, enhancing data integrity and minimizing conflicts [40]. However, data privacy, security, and governance concerns must be addressed for ethical and secure blockchain use. Sharing clinical trial data also requires careful consideration of patient privacy, including informed consent and legal aspects of Data Sharing Agreements(DSAs)[40].

Anonymization and Data Integrity: Maintaining data integrity (accuracy, consistency, and reliability throughout its lifecycle) is critical for drug safety and regulatory decision-making. Anonymization or de-identification of patient-level data is a key recommendation for sharing clinical trial data for third-party research. Data holders employ strategies to minimize the risk of patient re-identification when sharing de-identified data, considering relevant legislation and data security controls. However, 100% confidentiality cannot be guaranteed, especially with increasing data availability in the public domain. Digital transformation initiatives, including electronic data capture systems and automated data validation, can significantly enhance data precision and dependability, bolstering data integrity by reducing manual errors and unauthorized modifications. Block chain can also contribute to data originality in pharma manufacturing[41] Ethical Issues with the Use of Patient Data: Using sophisticated analytics in pharmaceutical research and development presents ethical issues with regard to protecting patient privacy. It's critical to strike a balance between upholding strict ethical standards, patient privacy, and technical innovation. To guarantee that innovation supports the larger healthcare purpose without jeopardizing individual privacy rights, a persistent dedication to both technological excellence and ethical monitoring is necessary. A patient-centered strategy that gives patients authority over their medical records via cryptographic keys in blockchain systems is consistent with the moral precepts of informed consent and autonomy[42].

Risks to Privacy in Remote and Telemedicine Services: As IoT is used more and more to create innovative healthcare applications, privacy (access control), confidentiality, and integrity especially with regard to patient records are the main issues. Security and privacy issues are brought up by remote and telemedicine services, even if they save costs and enhance patient satisfaction[43].

International Difficulties with Cross-Border Data Transfers: Pharmaceutical businesses that operate internationally have to manage and abide by a number of legal obligations in several jurisdictions, each of which has specific standards for data integrity. Establishing uniform and harmonized data integrity procedures across the global supply chain may be made more difficult by national variations in laws, norms, and expectations. To ensure smooth market access and speed up approval procedures, it is essential to harmonize international regulatory standards. Establishing global rules to streamline regulatory submissions across borders is a critical function of organizations such as the International Council for Harmonization(ICH)[44].

Risks to Privacy and Third-Party Data Processing: Healthcare organizations frequently depend on outside suppliers when looking to expand their digital infrastructure, which might pose privacy problems if these partners fail to sufficiently secure patient data. In accordance with HIPAA, organizations must make sure business associates set up strong security measures for ePHI[45].

Strategies for Enhancing Cybersecurity in Pharmaceutical Innovation: The pharmaceutical industry, undergoing rapid digital transformation, faces increasing and sophisticated cyber threats that can jeopardize sensitive data, intellectual property, and patient safety. Enhancing cybersecurity is therefore crucial to protect the innovation pipeline, maintain regulatory compliance, and foster trust. A multi-layered and proactive approach, incorporating advanced technologies, robust practices, and a strong security culture, is essential to build resilience against evolving cyber risks[46].

Implementing Robust Encryption and Access Controls: Implementing robust encryption is a fundamental policy for protecting sensitive pharmaceutical data both in transit and at rest. This comprises using advanced encryption algorithms like AES and ensuring secure key managing. Strong access controls, based on the belief of least privilege, are vital to limit data access only to official personnel. This involves multi-factor verification, role-based access control, and regular reviews of user permissions. Cyber hygiene programs that syndicate password security training with access control methodology education are also crucial to defend against employee-caused data breaks[47].

AI and Machine Learning for Threat Detection: Artificial

DOI: https://doi.org/10.54393/pbmj.v8i4.1232

intelligence (AI) and machine learning (ML) are developing as powerful tools for improving threat detection in the pharmaceutical industry. AI/ML can analyze vast amounts of data to identify patterns and anomalies that may specify security breaches, enabling real-time threat detection and response. AI-driven systems can learn from historical data and adapt to emerging threats, cultivating risk management. Integrating AI with mathematical optimization techniques can further enhance the detection and neutralization of threats [48].

Zero Trust Architecture in Pharmaceutical Security: The sources do not explicitly detail the implementation of a Zero Trust architecture in pharmaceutical security. However, the principles of Zero Trust, which assume no user or device is inherently trustworthy and require continuous verification, align with the need for stringent access controls and monitoring discussed within the sources. Applying Zero Trust principles would necessitate strict identity verification, micro-segmentation of networks, and continuous monitoring of all activity within the pharmaceutical IT ecosystem [49].

Cybersecurity Training and Awareness for Employees: Cybersecurity training and awareness programs for employees are critical in creating a security-conscious culture and mitigating insider threats and employee-caused data breaches. Every employee needs to develop a cybersecurity awareness culture that understands their responsibility to guard sensitive data. Training should cover password security, phishing awareness, safe data handling procedures, and the importance of reporting suspicious activities. Regular updates and cybersecurity drills for handling IP breaches can further enhance employee preparedness [50].

Regulatory Compliance and Risk Management: Pharmaceutical cybersecurity relies heavily on proactive risk management and regulatory compliance. Strict laws like GDPR and HIPAA, which need strong security requirements, govern how the sector functions. Detecting, evaluating, and reducing cyber threats at every stage of the supply chain and research and development process is part of a proactive approach to risk management. Regular penetration tests, vulnerability scans, and security assessments are all part of this [51].

Enhancing Plans for Incident Response and Recovery: To lessen the effects of cyberattacks and guarantee company continuity, incident response and recovery plans must be strengthened. Procedures for identifying, evaluating, containing, eliminating, and recovering from security issues should be described in these plans. To guarantee the efficacy of these programs, regular testing and updating are necessary. A proactive approach to cybersecurity also includes developing operational continuity plans to minimize disruptions [52].

Regulatory Frameworks and Compliance in Cybersecurity: A key component of cybersecurity, especially in the pharmaceutical and healthcare industries, is regulatory compliance. Strict regulatory frameworks are in place for pharmaceutical businesses and healthcare institutions to secure sensitive patient data and maintain the integrity of their operations. The National Institute of Standards and Technology (NIST) Cybersecurity Framework, the General Data Protection Regulation (GDPR) in the European Union, and the Health Insurance Portability and Accountability Act (HIPAA) in the United States are among the important laws cited in the sources. Organizations are required by these frameworks to set up technological, administrative, and physical security measures for sensitive data, including electronic health records. Compliance is not merely a checklist exercise but a fundamental aspect of ensuring data privacy, maintaining patient trust, and avoiding significant financial penalties and reputational damage. For example, GDPR allows EU citizens to receive compensation equivalent to 4% of an organization's global annual turnover for non-compliance. Similarly, HIPAA non-compliance can lead to millions of dollars in fines [53].

Case Study in Pharmaceutical Cybersecurity The Incident: In 2017, pharmaceutical giant Merck & Co. was hit by a significant ransomware attack. This attack caused substantial operational disruptions across the company.

Impact: The ransomware attack led to a total IT outage for Merck. The attack caused significant operational disruptions for the company. Merck experienced delays and impacted production quality due to the cyberattack on IoT devices in its production systems. The company faced financial losses from production downtime as a consequence of the attack. Interestingly, Merck's insurance initially denied their claim for the losses, citing a war exclusion clause.

Type of Attack: The Merck incident is identified as a ransomware attack. Ransomware is a type of malware that encrypts a victim's files and demands a ransom payment to restore access.

Remediation and Lessons Learned: The instance highlights how important it is for the pharmaceutical industry to have a thorough and proactive tactic to cybersecurity in order to reduce risks and lessen the effect of potential attacks. As established by the insurance dispute, it draws attention to the possibility of serious financial consequences that go beyond the expense of recovery. The assault highlights how vulnerable IoT devices and production systems are to cyberattacks in the pharmaceutical manufacturing industry. This calls for particular security protocols for situations including operational technology (OT). Finally, the ransomware assault on Merck is a clear reminder of the serious financial

DOI: https://doi.org/10.54393/pbmj.v8i4.1232

and operational repercussions that cyberattacks may have on large pharmaceutical firms. It emphasizes how significant it is to have strong cybersecurity measures, such as proactive risk management, preparing for operational continuity, and paying close attention to protecting production systems [54].

Future Directions and Emerging Trends in Cybersecurity for Pharmaceutical and Healthcare Industries

Digital transformation and evolving threats are shaping cybersecurity trends in the pharmaceutical and healthcare sectors. Key developments include:

Machine Learning and AI: These technologies enhance threat detection by analyzing large datasets and identifying anomalies, leading to more precise and proactive threat mitigation.

Blockchain: Provides robust data security and integrity, particularly for pharmaceutical supply chains, to ensure transparency and prevent counterfeiting.

Medical Device Security: Focus on securing connected devices (IoMT) to protect patient safety and healthcare system integrity.

Emerging Trends: Integrating security into the Software Development Lifecycle (SDLC) for secure medical device design. Developing quantum-resistant encryption methods to safeguard against future threats. Strengthening regulatory frameworks and compliance requirements. Adopting proactive and adaptive security systems that evolve with new threats. Incorporating cybersecurity into Industry 5.0, emphasizing human-machine collaboration and resilience. Converging AI and blockchain for advanced cybersecurity solutions. These trends reflect a proactive and technology-driven approach to enhance resilience against evolving threats and protect sensitive data and critical operations [55].

This study is limited by its reliance on secondary data and previously published literature, which may not fully capture real-time or region-specific cybersecurity challenges. Additionally, the absence of empirical validation restricts the generalizability of the findings. Future research should incorporate primary data, case-based analyses, and quantitative assessments to evaluate cybersecurity interventions. Moreover, exploring advanced technologies such as AI-driven security systems and blockchain in practical pharmaceutical settings is recommended.

CONCLUSIONS

The digital transformation of the pharmaceutical industry, while offering significant opportunities for innovation and efficiency, has also exposed it to a range of cybersecurity threats and privacy challenges. Intellectual property theft, data breaches, ransomware attacks, insider threats, supply chain vulnerabilities, and cyber-espionage are among the critical issues that necessitate robust cybersecurity measures. Compliance with data protection regulations like GDPR and HIPAA is essential to protect sensitive data and maintain stakeholder trust. Strategies such as implementing strong encryption, adopting AI and machine learning for threat detection, enforcing zero trust architecture, and enhancing employee training are crucial for safeguarding pharmaceutical innovation. Future trends, including the integration of AI and blockchain, the security of IoT devices, and the development of quantum-resistant encryption, will shape the industry's cybersecurity landscape. A proactive and adaptive approach, combined with stringent regulatory compliance, is vital to ensure the integrity and safety of pharmaceutical operations in the digital age.

Authors' Contribution

Conceptualization: NAK
Methodology: MRS
Formal analysis: DH
Writing and Drafting: NAK, MRS, DH, MR, SRD
Review and Editing: NAK, MRS, DH, MR, SRD

All authors approved the final manuscript and take responsibility for the integrity of the work.

Conflicts of Interest

The authors declare no conflict of interest.

Source of Funding

The author received no financial support for the research, authorship and/or publication of this article.

REFERENCES

[1] Snigdha EZ, Jalil MS, Dahwal FM, Saeed M, Mehedy MT, Hasan SK. Cybersecurity in Healthcare IT Systems: Business Risk Management and Data Privacy Strategies. The American Journal of Engineering and Technology. 2025 Mar; 7(03): 163-84. doi: 10.37547/tajet/Volume07Issue03-15.

[2] Arden NS, Fisher AC, Tyner K, Yu LX, Lee SL, Kopcha M. Industry 4.0 for pharmaceutical manufacturing: Preparing for the smart factories of the future. International Journal of Pharmaceutics. 2021 Jun; 602: 120554. doi: 10.1016/j.ijpharm.2021.120554.

[3] Bag S, Pretorius JH, Gupta S, Dwivedi YK. Role of institutional pressures and resources in the adoption of big data analytics powered artificial intelligence, sustainable manufacturing practices and circular economy capabilities. Technological Forecasting and Social Change. 2021 Feb; 163: 120420. doi: 10.1016/j.techfore.2020.120420.

[4] Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care. 2017 Jan; 25(1): 1-0. doi: 10.3233/THC-161263.

DOI: https://doi.org/10.54393/pbmj.v8i4.1232

[5] Parihar A, Prajapati JB, Prajapati BG, Trambadiya B, Thakkar A, Engineer P. Role of IOT in healthcare: Applications, security & privacy concerns. Intelligent Pharmacy. 2024 Oct; 2(5): 707-14. doi: 10.1016/j.ipha.2024.01.003.

[6] Jadav NK, Kakkar R, Mankodiya H, Gupta R, Tanwar S, Agrawal S *et al.* GRADE: Deep learning and garlic routing-based secure data sharing framework for IIoT beyond 5G. Digital Communications and Networks. 2023 Apr; 9(2): 422-35. doi: 10.1016/j.dcan.2022.11.004.

[7] Rust-Nguyen N, Sharma S, Stamp M. Darknet traffic classification and adversarial attacks using machine learning. Computers & Security. 2023 Apr; 127: 103098. doi: 10.1016/j.cose.2023.103098.

[8] Aamir M and Zaidi SM. DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation. International Journal of Information Security. 2019 Dec; 18: 761-85. doi: 10.1007/s10207-019-00434-1.

[9] Benmalek M. Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. Internet of Things and Cyber-Physical Systems. 2024 Jan; 4: 186-202. doi: 10.1016/j.iotcps.2023.12.001.

[10] Check Point Research. A continuing cyber-storm with increasing ransomware threats and a surge in healthcare and APAC region. [Cited on: 10th May 2025]. Available at: https://blog.checkpoint.com/security/a-continuing-cyber-storm-with-increasing-ransomware-threats-and-a-surge-in-healthcare-and-apac-region/.

[11] Shaki F, Amirkhanloo M, Jahani D, Chahardori M. Artificial intelligence in pharmaceuticals: Exploring applications and legal challenges. Pharmaceutical and Biomedical Research. 2024 Dec; 10(1): 1-0. doi: 10.32598/PBR.10.1.1257.1.

[12] Shackelford SJ. Protecting intellectual property and privacy in the digital age: the use of national cybersecurity strategies to mitigate cyber risk. Chapman Law Review. 2016; 19: 445.

[13] Ramezan G and Leung C. A blockchain-based contractual routing protocol for the internet of things using smart contracts. Wireless Communications and Mobile Computing. 2018 Nov; 2018(1): 4029591. doi: 10.1155/2018/4029591.

[14] He Y, Aliyu A, Evans M, Luo C. Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review. Journal of Medical Internet Research. 2021 Apr; 23(4): e21747. doi: 10.2196/21747.

[15] Weber GM, Adams WG, Bernstam EV, Bickel JP, Fox KP, Marsolo K et al. Biases introduced by filtering electronic health records for patients with "complete data". Journal of the American Medical Informatics Association. 2017 Nov; 24(6): 1134-41. doi: 10.1093/jamia/ocx071.

[16] Singh, H. (2024). Ethical considerations in pharmaceutical analytics: Balancing innovation and patient privacy. International Journal of Research in Computer Applications and Information Technology. 2024 Nov; 7(2): 955-972. doi: 10.5281/zenodo.14054904.

[17] Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy. Journal of big data. 2018 Dec; 5(1): 1-8. doi: 10.1186/s40537-017-0110-7.

[18] Chen Y, Yang O, Sampat C, Bhalode P, Ramachandran R, Ierapetritou M. Digital twins in pharmaceutical and biopharmaceutical manufacturing: a literature review. Processes. 2020 Sep; 8(9): 1088. doi: 10.3390/pr8091088.

[19] Demyanenko VG, Demyanenko DV, Breusova SV, Baranova II, Karpenko LA. Effect of the material of primary packaging containers on providing of visual inspection of pharmaceutical products. Scripta Scientifica Pharmaceutica. 2016 Jul; 3(1): 60-72. doi: 10.14748/ssp.v1i1.1685.

[20] Abrar I, Ayub Z, Masoodi F. Current trends and future scope for the internet of things. Internet of Things in Business Transformation: Developing an Engineering and Business Strategy for Industry 5.0. 2021 Jan: 185-209. doi: 10.1002/9781119711148.ch11.

[21] Buese, A. M., & Setterlund, E. Rise in Healthcare Data Breaches & the Impact for Healthcare Providers in 2024. Journal of Healthcare Information Management. 2024 Mar; 38(2): 225-241.

[22] AL-Dosari K, Fetais N, Kucukvar M. Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. Cybernetics and systems. 2024 Feb; 55(2): 302-30. doi: 10.1080/01969722.2022.2112539.

[23] Gupta V. IoT enabled air pollution monitoring in smart cities. Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's. 2020: 569-91. doi: 10.1007/978-3-030-40305-8_27.

[24] Sufian MA, Haque S, Al-Samad K, Faruq O, Hossain MA, Talukder T et al. IoT and Data Science Integration for Smart City Solutions. AIJMR-Advanced International Journal of Multidisciplinary Research. 2024 Sep 18;2(5). doi: 10.62127/aijmr.2024.v02i05.1086.

[25] Elali W. The importance of strategic agility to business survival during corona crisis and beyond. International Journal of Business Ethics and Governance (IJBEG). 2021 May: 1-8. doi: 10.51325/ijbeg.v4i2.64.

DOI: https://doi.org/10.54393/pbmj.v8i4.1232

[26] Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F *et al.* Cyber risk and cybersecurity: a systematic review of data availability. The Geneva papers on risk and insurance. Issues and Practice. 2022 Feb; 47(3): 698. doi: 10.1057/s41288-022-00266-6.

[27] Khan N, Hossain S, Khadka U, Sarkar S. Optimizing Business Operations through Edge Computing: Advancements in Real-Time Data Processing for the Big Data Era. AIJMR-Advanced International Journal of Multidisciplinary Research. 2024 Oct; 2(5). doi: 10.62127/aijmr.2024.v02i05.1108.

[28] Akram PS, Ramesha M, Valiveti SA, Sohail S, Rao KT. IoT based remote patient health monitoring system. In2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS) 2021 Mar; 1: 1519-1524. doi: 10.1109/ICACCS51430.2021.9441874.

[29] Buliga O, Scheiner CW, Voigt KI. Business model innovation and organizational resilience: towards an integrated conceptual framework. Journal of Business Economics. 2016 Aug; 86: 647-70. doi: 10.1007/s11573-015-0796-y.

[30] Rouhani S, Ashrafi A, Zare Ravasan A, Afshari S. The impact model of business intelligence on decision support and organizational benefits. Journal of Enterprise Information Management. 2016 Feb; 29(1): 19-50. doi: 10.1108/JEIM-12-2014-0126.

[31] Almalawi A, Khan AI, Alsolami F, Abushark YB, Alfakeeh AS. Managing security of healthcare data for a modern healthcare system. Sensors. 2023 Mar; 23(7): 3612. doi: 10.3390/s23073612.

[32] Arif H, Kumar A, Fahad M, Hussain HK. Future horizons: AI-enhanced threat detection in cloud environments: Unveiling opportunities for research. International Journal of Multidisciplinary Sciences and Arts. 2024 Jan; 3(1): 242-51. doi: 10.47709/ijmdsa.v2i2.3452.

[33] Dedzins R, James M. Biopharmaceutical technical resource guide. Emerson; 2015 [Cited On: 10th May 2025]. Available at: https://www.lakesidecontrols.com/getattachment/7846bd01-541d-4b2d-a70017a37c651f76/article.

[34] Biasin E, Kamenjašević E, Ludvigsen KR. Cybersecurity of AI medical devices: risks, legislation, and challenges. Research Handbook on Health, AI and the Law. 2024 Jul: 57-74. doi: 10.4337/9781802205657.ch04.

[35] Attkan A, Ranga V, Ahlawat P. A Rubik's Cube Cryptosystem-based Authentication and Session Key Generation Model Driven in Blockchain Environment for IoT Security. Association for Computing Machinery Transactions on Internet of Things. 2023 May; 4(2): 1-39. doi: 10.1145/3586578.

[36] Patil RS, Kulkarni SB, Gaikwad VL. Artificial intelligence in pharmaceutical regulatory affairs. Drug Discovery Today. 2023 Sep; 28(9): 103700. doi: 10.1016/j.drudis.2023.103700.

[37] Mohammed ZA, Mohammed M, Mohammed S, Syed M. Artificial Intelligence: Cybersecurity Threats in Pharmaceutical IT Systems. 2024 Aug: 11(8). doi: 10.17148/IARJSET.2024.11801.

[38] Michael K, Abbas R, Roussos G. AI in cybersecurity: The paradox. Institute of Electrical and Electronics Engineers Transactions on Technology and Society. 2023 Jun; 4(2): 104-9. doi: 10.1109/TTS.2023.3280109.

[39] Abd Elazeem NE. Effect of cybercrime on the pharmaceutical industry. Journal of Intellectual Property and Innovation Management. 2020 Jul; 3(5): 91-121. doi: 10.21608/jipim.2021.181274.

[40] Kazim AK and Shanshul NR. The impact of cyber-attacks on companies and organisations in developed countries. Edelweiss Applied Science and Technology. 2024 Dec; 8(6): 9245-52. doi: 10.55214/25768484.v8i6.3980.

[41] Eisenhardt KM and Graebner ME. Theory building from cases: Opportunities and challenges. Academy of Management Journal. 2007 Feb; 50(1): 25-32. doi: 10.5465/amj.2007.24160888.

[42] Khan MN, Haque S, Azim KS, Al-Samad K, Jafor AH, Aziz M *et al.* Analyzing the Impact of Data Analytics on Performance Metrics in SMEs. AIJMR-Advanced International Journal of Multidisciplinary Research. 2024 Sep; 2(5). doi: 10.62127/aijmr.2024.v02i05.1081.

[43] Haque S, Azim KS, Al-Samad K, Jafor AH, Aziz M, Faruq O *et al.* The Evolution of Artificial Intelligence and its Impact on Economic Paradigms in the USA and Globally. AIJMR-Advanced International Journal of Multidisciplinary Research. 2024 Sep; 2(5). doi: 10.62127/aijmr.2024.v02i05.1083.

[44] Khasawneh O and Alzghoul A. The real effects of Fintech on the global financial system. International Journal of Professional Business Review: International Journal of Professional Business Review. 2023 Mar; 8(3): e01725. doi: 10.26668/businessreview/2023.v8i3.1725.

[45] Hossain Z, Chowdhury SS, Rana MS, Hossain A, Faisal MH, Al Wahid SA *et al.* Business Innovations in Healthcare: Emerging Models for Sustainable Growth. AIJMR-Advanced International Journal of Multidisciplinary Research. 2024 Sep; 2(5). doi: 10.62127/aijmr.2024.v02i05.1093.

[46] Punia V and Aggarwal G. Impact of Artificial Intelligence (AI) in Cybersecurity. InRecent Advances in Computational Intelligence and Cyber Security. 2024 Apr; 13(5): 183-193. doi: 10.1201/9781003518587-18.

DOI: https://doi.org/10.54393/pbmj.v8i4.1232

[47] Salama R and Al-Turjman F. Future uses of AI and blockchain technology in the global value chain and cybersecurity. InSmart Global Value Chain 2024 Aug: 257-269. doi: 10.1201/9781003461432-17.

[48] Field M. WannaCry cyber-attack cost the NHS£ 92m as 19,000 appointments cancelled. The telegraph. 2018 Oct; 11. doi: 10.1016/S1361-3723(18)30102-7.

[49] Pharmaceutical Technology. Five pharma cybersecurity breaches to know and learn from: the transition to digital, expedited by the Covid-19 pandemic, has opened up new cybersecurity concerns. [Cite On: 10th May 2025]. Available at: https://www.pharmaceutical-technology.com/comment/pharma-cybersecurity-breaches/.

[50] Alexandra P, Camelia C, Elena CC, Bogdan P, Răzvan dc. Cyber risk assessment in the pharmaceutical industry: vulnerabilities, threats, and global response strategies. Annals of'Constantin Brancusi'University of Targu-Jiu. Economy Series/Analele Universităţii'Constantin Brâncuşi'din Târgu-Jiu Seria Economie. 2024 Oct: 1(5): 307–319.

[51] Shafik W. Blockchain-based internet of things (B-IoT): Challenges, solutions, opportunities, open research questions, and future trends. Blockchain-based Internet of Things. 2024 Feb: 35-58. doi: 10.1201/9781003407096-3.

[52] Mathkor DM, Mathkor N, Bassfar Z, Bantun F, Slama P, Ahmad F *et al.* Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends. Journal of Infection and Public Health. 2024 Apr; 17(4): 559-72. doi: 10.1016/j.jiph.2024.01.013.

[53] Ramos-Cruz B, Andreu-Perez J, Martínez L. The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research. Neurocomputing. 2024 Feb: 127427. doi: 10.1016/j.neucom.2024.127427.

[54] Iqbal Z, Khan S, Mehmood A, Lloret J, Alrajeh NA. Adaptive Cross-Layer Multipath Routing Protocol for Mobile Ad Hoc Networks. Journal of Sensors. 2016; 2016(1): 5486437. doi: 10.1155/2016/5486437.

[55] Li C, Li F, Yin L, Luo T, Wang B. A Blockchain-Based IoT Cross-Domain Delegation Access Control Method. Security and Communication Networks. 2021 Sep; 2021(1): 3091104. doi: 10.1155/2021/3091104.