

Artificial Intelligence: Cybersecurity Threats in Pharmaceutical IT Systems

**Zeeshan Ahmed Mohammed¹, Muneeruddin Mohammed², Shanavaz Mohammed³,
Mujahedullah Syed⁴**

University of the Cumberland, Williamsburg, KY. ¹⁻³

Athenahealth Inc. ⁴

Abstract: Artificial Intelligence (AI) has significantly transformed various industries, including the pharmaceutical sector. As of 2023, the US AI market is valued at \$123 billion, with a projection of \$594 billion by 2032. Industries such as technology, automotive, finance, and healthcare have seen substantial AI adoption. In healthcare, AI optimizes routine tasks, accelerates drug discovery, and enhances clinical trials and manufacturing processes. However, the increased reliance on AI exposes pharmaceutical companies to cybersecurity threats, including data breaches, intellectual property theft, ransomware, and insider threats. Robust cybersecurity measures, such as strong access controls, securing AI systems, incident response plans, regular security audits, data encryption, employee training, and industry collaboration, are critical. Future trends indicate growing AI investment in healthcare, necessitating continuous advancements in cybersecurity to protect sensitive data and ensure regulatory compliance.

Keywords: Data encryption, AI optimization, Incident response, Cybersecurity, Intellectual property

I. INTRODUCTION

Artificial Intelligence (AI) has taken the 21st century industrialization to a whole another level elevating how businesses conduct business. The market size of the US artificial intelligence as of 2023 stood at \$123 billion with a projected market size of \$594 billion by the year 2032 [15]. This projection is at least 500 percent of the current capitalization which means that the use of AI is taking over at a very fast rate. The technology and communications industry has seen the most AI adoption by 32% followed by the automotive and assembly industry with 29% adoption. The third and fourth industries in the list are the financial and energy resources industry with 28% and 27% respectively [11]. Other industries that have led in adopting the use of AI in their day to day activities include the media and entertainment industry, transportation and logistics, consumer packaged goods and the retail industry. Health care industry has not been left behind with the industry coming in the ninth position with 17% AI adoption rate [4]. This is to signify that the rate at which the industries are adopting the use of artificial intelligence is quite high and growing given that it has only been a decade of existence.

Adoption Rate of Artificial Intelligence by Industry

% firms in an industry that are adopting AI

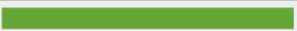











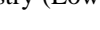
| Rank | Industry | Adoption % | |
|------|-------------------------------|------------|---|
| 1 | Technology and communications | 32% |  |
| 2 | Automotive and assembly | 29% |  |
| 3 | Financial services | 28% |  |
| 4 | Energy and resources | 27% |  |
| 5 | Media and entertainment | 22% |  |
| 6 | Transportation and logistics | 21% |  |
| 7 | Consumer packaged goods | 20% |  |
| 8 | Retail | 19% |  |
| 9 | Health care | 17% |  |
| 10 | Education | 17% |  |
| 11 | Construction | 16% |  |
| 12 | Professional services | 13% |  |
| 13 | Travel and tourism | 11% |  |

Figure 1: Adoption rate of artificial Intelligence by industry (Low, 2018)

Healthcare industry has been one of the most critical industry employing the highest number of employees while still serving the largest number of customers. For instance, in 2021, the US education and healthcare industries had the highest total employed personnel at about 36.378 million people followed by wholesale and retail industry with 19.79 million employees [14]. The healthcare industry is the third largest industry in the world by value after manufacturing and retail industries [2]. This is to show how important the healthcare industry is and its significant contribution to the overall economy. It also means that the industry processes large data sets of employees as well as clients which makes the routine functions and overall tasks to be cumbersome.

Artificial intelligence has been a major force in a majority of the industries. It has been used to optimize and manage routine tasks by increasing accuracy, reducing time and labor as well as managing large data sets easily. AI has also been able to manage repetitive tasks by automation which leaves employees to focus on the more strategic works and decision making process [3]. AI technology has been able to facilitate advancement of the problem solving especially in industries with large numbers of customers. This aspect of AI has been influential in the adoption of the same in the healthcare and pharmaceutical industry. The most significant contribution of AI in the pharmaceutical industry has been the ability to process and analyze large volumes of data which the industry possesses and is shared among various institutions. AI technologies, such as machine learning, natural language processing, and predictive analytics, are increasingly integrated into drug discovery, development, and personalized medicine [19]. The pharmaceutical industry, driven by the promise of AI, continues to invest heavily in these technologies to stay competitive and innovative.

Artificial intelligence in the pharmaceutical industry has been instrumental in drug discovery and development by facilitating repurposing of existing drugs, optimizing the whole drug development process, increased accuracy in data analysis, as well as development of personalized medicine [21]. The process of drug development was hectic and lengthy using the traditional methods which proved to be ineffective. With the help of machine learning and algorithm, the process of drug development has been shortened, and made more accurate. AI has also found use in clinical trials by having accurate and speedy screening of candidates as well as real time monitoring of outcomes in the lab settings. It has been able to expedite the trial design process, streamlined the data collection and analysis of electronic records which has been able to facilitate better results in the clinical trials [27]. AI has also come in handy in the manufacturing and supply chain process of pharmaceuticals by utilizing predictive modelling to forecast sales and demand, supply chain automation as well as facilitating regulatory compliance of audited records. It has also helped in improving efficiency and reducing costs by predicting maintenance needs, minimizing downtime, and ensuring consistent product quality.

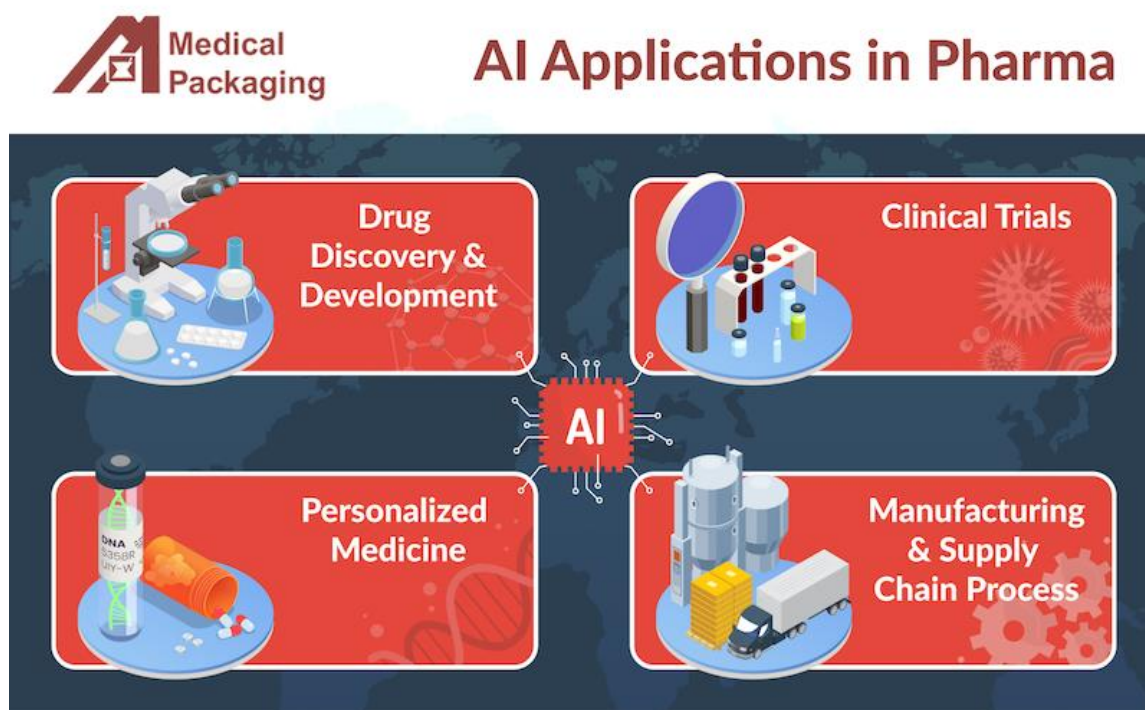


Figure 2: Diagram in AI applications in pharma (Medical packaging, 2023)

With such critical data and information being processed by the pharmaceutical industry, it has been prone to digital and cyber-attacks with an aim to steal the crucial patient data. According to reports of the 2021 analysis of cyberattacks recorded, it was clear that the healthcare and public health industry was the most prone to attacks with 148 cases recorded in the single year while financial services industry was second with almost half the number of attacks at 89 recorded attacks [8]. Emergency services and defense industrial base industries experienced the least attacks with 2 and 1 attacks respectively. Previous cases of cyberattacks have led to loss of crucial data, loss of finances and loss of intellectual property which has been quite detrimental to most companies. For instance, Pfizer and BioNTech experienced a cyberattack in 2020 where their formula for the COVID-19 vaccine was stolen [19]. This led to loss of revenue for the company as the perpetrators could make the vaccine illegally. Such cases necessitate security measures with an aim of putting away the attackers. Besides the theft of their intellectual properties, the companies need to ensure that they do not break any of the regulatory framework put in place to protect the customer data which attracts hefty punitive penalties [1]. Therefore, there is a need to ensure that pharmaceutical companies secure the patients data so as to comply with regulations as well as maintain trust and confidence of their customers.

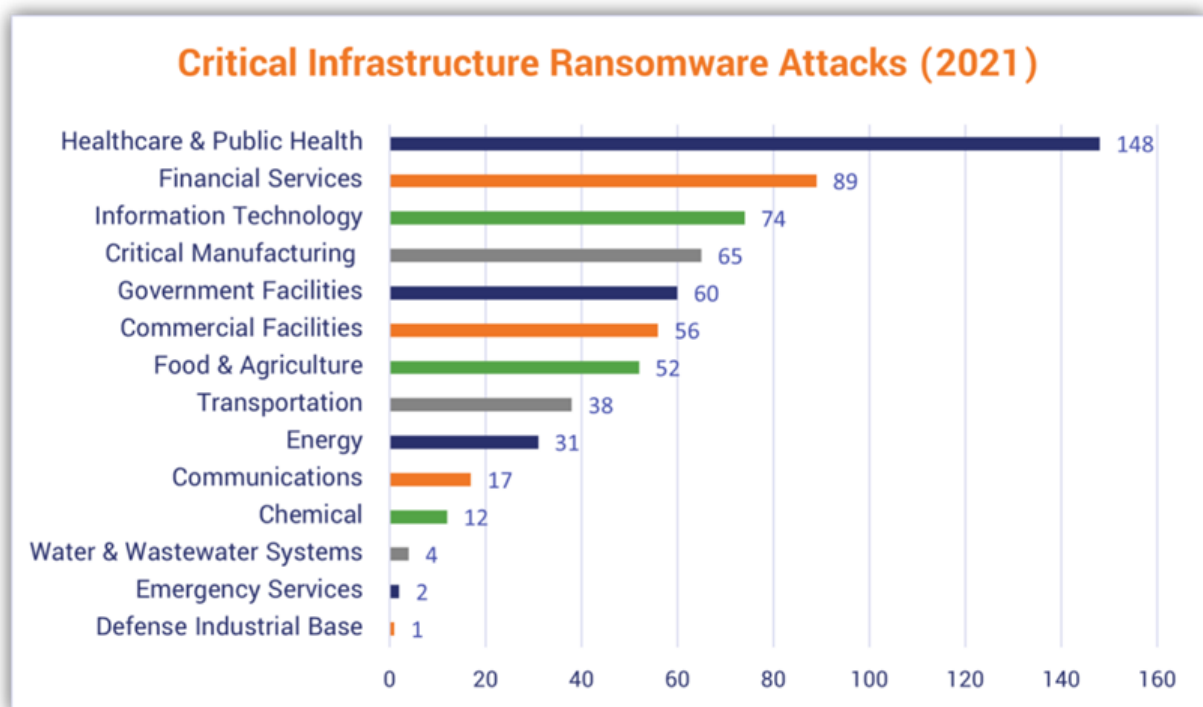


Figure 3: Bar graph on critical infrastructure ransomware attacks 2021 (Crane, 2022).

II. CYBERSECURITY THREATS TO PHARMACEUTICAL IT SYSTEMS

Despite the overwhelming advantages that the adoption of artificial intelligence has in the pharmaceutical industry, cyberattacks threaten to cut short the dominance of the same. Cybersecurity threats, including ransomware, phishing, and data breaches, pose significant risks to the integrity and confidentiality of pharmaceutical IT systems [22]. These threats have been known to cause data breaches, disruption of operations as well as hinder maximum utility of the systems in the industry. These cyberattacks effects highlight the need for robust cybersecurity measures that will ensure that the data and systems are secure from any external exposure. There are several examples of cybersecurity threats including data theft and breaches.

a. Data Breaches and Theft

As earlier noted, the pharmaceutical industry handled a wide variety of data that is processed on a regular basis. For instance, they handle patient information, proprietary data for ongoing research, as well as clinical trial data. These types of data are a cornerstone to all their operations such that without this data, they cannot operate as usual. Some of this data, for instance patient information, should only be utilized by the authorized persons only without divulging the information to any third party [16]. Given the high value of the sensitive data, cybercriminals target the pharmaceutical companies to steal this data.

They can gain access to this data by exploiting the available vulnerabilities in the system by use of malware or even phishing attacks. Unauthorized access to the secure data results in patient data compromise or even intellectual property theft.

Theft of sensitive information leads to several issues such as financial losses, damage to company's credibility and reputation as well as incurring legal liabilities. Patient data compromise can result in identity theft and financial frauds. Intellectual property theft on the other hand can result in loss of competitive advantage for companies as the attackers steal information about proprietary drug development and data related to clinical trials [13]. Competitors or malicious entities may exploit stolen information to develop similar drugs, undermining the original company's market position and revenue. It might as well cause delays in research and projects as well as loss of research data integrity. Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) provide a legal framework where they outline privacy regulations that all pharmaceutical companies must enhance [25].

One recent example that hit the world was the case of Pfizer and BioNTech during the COVID-19 pandemic where there was a Vaccine Data Breach in December 2020. The cyberattack occurred on the European Medicines Agency (EMA) where the companies were researching and developing the first COVID-19 vaccines [6]. Unauthorized persons accessed the database pertaining regulatory submission of the vaccine. The breach did not directly affect the manufacture of the drug but the mere fact that the systems were breached and formulas as well as data pertaining to such critical processes was stolen highlights the dire need for a robust security system.

b. Intellectual Property (IP) Theft

The pharmaceutical companies have been able to attract high value investors due to the production of drugs and disease research. Drug research and development for instance, takes a lot of time ranging from one year to ten or 15 years as it requires a lot of data analysis, clinical experiments and trials, as well as pilot studies to determine the effects of the drugs to the general users [26]. This means that there is a lot of information and data in circulation for any given drug development procedure. This is therefore why some cyberattacks are aimed at stealing this valuable information such as drug formulation formulas or even the AI used to drive the drug development process. Loss of such information could set back the companies in terms of costs and competitive edge they possess as a result of the drug development process [18]. Starting the whole process over again can delay discovery of new drugs which might be devastating to the intended consumers.

An example of Intellectual Property (IP) Theft was back in 2016 where the GlaxoSmithKline (GSK) systems were breached and their trade secrets exposed by one of their employees Yu Xue. GSK is one of the largest British pharmaceutical research and development companies in the world with its headquarters in London [20]. The trade secrets were intended for GSK competitors in China. Yu Xue was charged with an attempt to steal company data and sell to competitors and was sentenced to 8 months in prison [11]. GSK on the other hand did not incur direct financial loss as a result but it would only be a matter of time before they know the real damage from the loss of intellectual property.

c. Ransomware Attacks

Another major cyberattack element is the ransomware. This has been one of the major ways through which cyber attackers have managed to infiltrate organizations and gain access to private and confidential data. In ransomware attacks, the attackers infiltrate an organization's systems and take over the systems by encrypting data and then asking for a ransom for them to release the system back to them [17]. While under attack, an organization's system cannot be accessed nor can any functionality be performed until the hacker allows it. This therefore leads to halting of services and operations such as research and developments, clinical trials or even production process of drugs. In cases where the ransom is paid, there is no guarantee that the systems will be surrendered back to them or more money will be requested. The confidential information accessed can also be stolen and used in the black market as well.

One of the most notable ransomware attack in the pharmaceutical industry was back in 2017 when Merck & Co., one of the largest pharmaceutical companies in the world, fell victim to the NotPetya ransomware attack. Initially, the attack started off in Ukraine but quickly spread out catching Merck & Co. unawares [29]. The attacker was able to paralyze the company's operations which lead to time and financial losses. According to the company's reports, an estimated \$900 million was lost as a result of the ransomware attack. Another ransomware attack in pharmaceutical company was back in 2020 when Fresenius, a global healthcare company and one of the largest private hospital operators in Europe, fell victim to cyber attackers [4]. The attackers infiltrated the company systems and encrypted it and demanded a ransom. The company attack affected their operations as well as patient care.

d. Supply Chain Attacks

Supply chain attacks target the suppliers, vendors and distributors of the pharmaceutical products. Cyber attackers use the supply chain network to gain access to the information technology systems of the companies involved. In most cases, the attackers exploit vendors to gain access to the primary pharmaceutical company. They later introduce malware in the systems or even rely on data breaches to cause harm to the company.

e. Insider threats

Insiders pose the greatest single source of data breaches in the history of cybersecurity. The biggest cybersecurity threats according to a report in 2022 was social engineering or people followed by attacks through ransomware [5]. Insider threats can either be done intentionally or unintentionally. Some of the key insiders are people who work for the company such as employees or even those that work in conjunction with the company. Contractors and partners can be sources of insider threats as they help attackers gain access to confidential information. Malicious insiders may steal data for personal gain or in collaboration with external attackers. They might as well help attackers gain access as a way of getting back at the company for termination of work contracts. Unintentional insider threats can result from human error, such as accidentally disclosing sensitive information or falling victim to phishing attacks [12].

One notable insider threat in the pharmaceutical industry was back in 2020 when AstraZeneca company witnessed a Cyber Espionage Attempt during the COVID-19 pandemic [23]. AstraZeneca is a giant manufacture of pharmaceutical products and was instrumental in manufacture and distribution of COVID-19 vaccines. Suspected North Korean hackers sent fake job offers to the staff members if AstraZeneca through LinkedIn and added malicious links in the offers. Their attempt to gain access to the company’s firewall and systems did not bear fruits as the malware-laced documents were mainly ineffective and did not compromise the company’s networks.

What is your biggest cybersecurity concern?

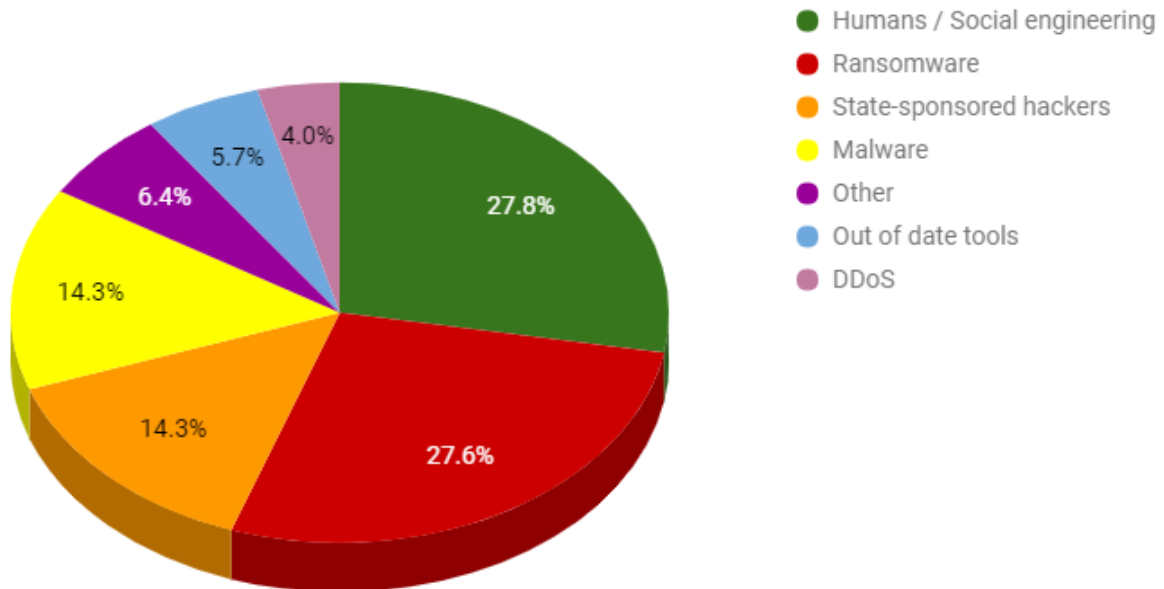


Figure 4: Pie chart showing the biggest cybersecurity concerns (McCaskill, 2017).

III. STRATEGIES FOR IMPROVING CYBERSECURITY IN PHARMACEUTICAL IT SYSTEMS

The advantages of using artificial intelligence in pharmaceutical process continue to accrue with more opportunities in the offering. It seems like pharmaceutical companies will continue to utilize the technology to gain competitive advantage as well as reduce labor and costs of drug development and manufacture [16]]. Therefore, protecting sensitive data and ensuring the integrity of IT systems are critical to safeguarding patient information, intellectual property, and maintaining regulatory compliance. Many companies have invested heavily in cybersecurity in order to ensure that they control damages as a result of attacks. There have been several strategies that have proven fruitful in keeping off cyber-attacks in the pharmaceutical industry as discussed below.

Steps taken to improve Cyber Resilience

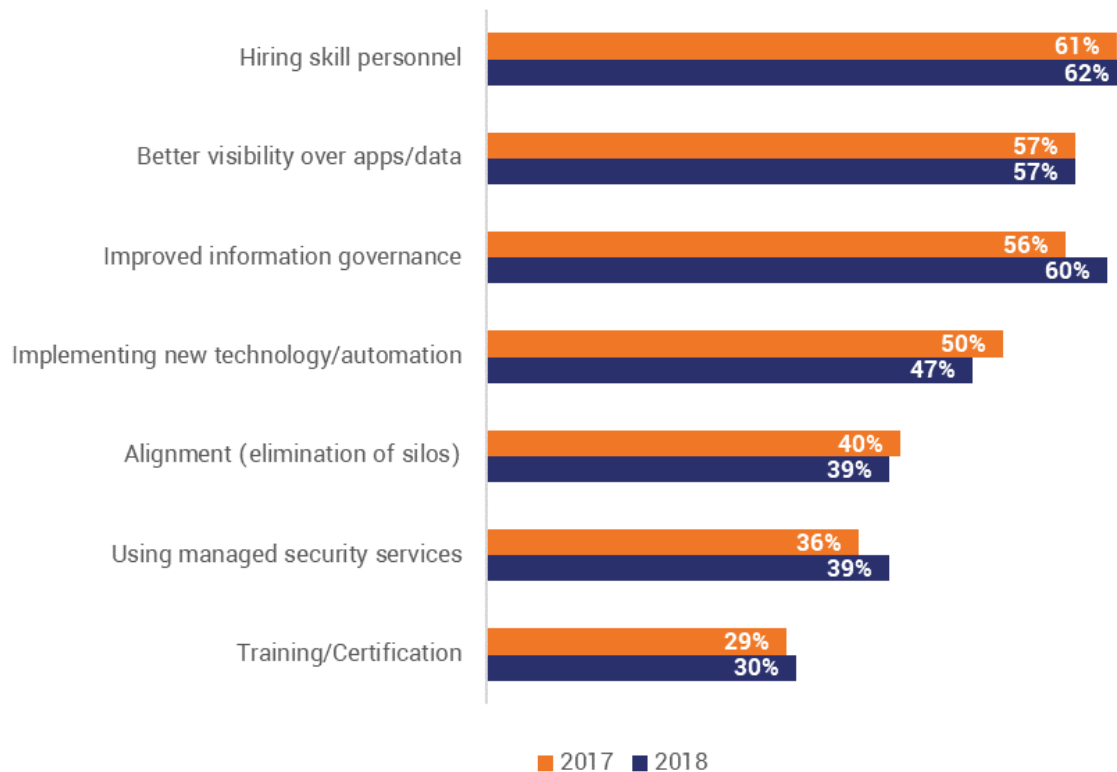


Figure 5: Bar chart showing steps taken to improve cyber resilience (Nohe, 2019)

a. Implementing Strong Access Controls

The main strategy to put off any attacks is to secure entry points for data such that only authorized persons can access the data. Having a robust access control with a limited number of authorized persons will ensure enhanced cybersecurity. In some cases, enabling multi-factor authentication (MFA) would add security layers which would require users to provide at least two verification factors at entry point [24]. Having employees assigned specific roles will also ensure that only specific user roles can access sensitive data within the organization. This will ensure that the data access is restricted to only specific job functions. Adding biometrics security to any safe room capable of accessing the data servers and cloud storage is a must for any up to date security measures. Having time logs will also ensure that every entry is recorded for easier tracking. By having strong access control, almost half of the security work is done.

b. Securing AI and Machine Learning Systems

Another critical strategy for preventing cyber-attacks is to secure the AI and machine learning systems which present an entry point for a majority of attacks. This is because AI systems are quite complex and challenging to understand for companies which attracts the cyber attackers. One of the ways to ensure that the AI and machine learning systems are secure is to ensure data integrity [11]. This means ensuring that the data being processed by AI technology is authentic and verifiable which ensures that malicious data is not introduced into the system. Another way is to ensure a robust model of AI where the model is built to withstand any infiltration and attack. Lastly, there is need to continuously monitor the AI systems to ensure that abnormalities in the system are promptly identified before they cause much damage.

c. Implementing Incident Response Plans

A company can do so much as ensure that preventive mechanisms are employed well in advance before any attack is registered. However, if a company does not handle all the loopholes and avenues through which attackers can penetrate their systems, they need to have a plan of action that will help the company in case of an attack. Having a well-defined incident response plan is crucial for minimizing the impact of such incidents [30]. The plan should outline procedures for detecting, responding to, and recovering from cybersecurity breaches. One of the key elements of a response report is to establish the protocol for reporting the security breach.

This should be done in a way that places the threat at the top most priority in the company. Next there needs to be a response team who have very clear roles related to stopping further infiltration into their systems. There should also be some clear method of communication especially to stakeholders and shareholders. Lastly, there should be clear recovery protocols that outline a step by step system restoration as well as post-incident analysis to prevent future occurrences [8].

d. Regular Security Audits and Vulnerability Assessments

The best preventive measure to stop any cyber threat is to be proactive and perform regular audits to assess key areas of vulnerability and safeguarding these areas to avoid any access. Regular audits are meant to identify any potential weak areas in IT system which can be rectified before it's too late. In most cases, these audits need to be performed by an expert who is also an external member of the organization. This ensures that there is no bias and provides a credible report on how best to rectify vulnerable areas. Regularly updating and patching software, including AI systems and applications, is critical to protect against known vulnerabilities [14]. Adopting a Zero Trust security model will ensure that companies do not take any chances when it comes to security issues. Always having guards up will ensure that even the slightest threats is neutralized. Zero Trust model requires micro-segmentation, continuous monitoring and having strict access controls.

e. Encryption of Data

Data encryption ensures that data is unusable or incomprehensible if data falls into the wrong hands. Data encryption helps protect sensitive data from unauthorized persons in and outside the organization. Data encryption process entails generating a master key to convert a plaintext into a ciphered text that can only be understood through decryption. This can be very useful in pharmaceutical companies especially when done to critical data that is passed from one end to another which ensures that the data is unusable if the data is intercepted in transit. Advanced encryption standards (AES) and other robust encryption protocols should be used to secure sensitive data, including patient records, proprietary research data, and financial information [3].

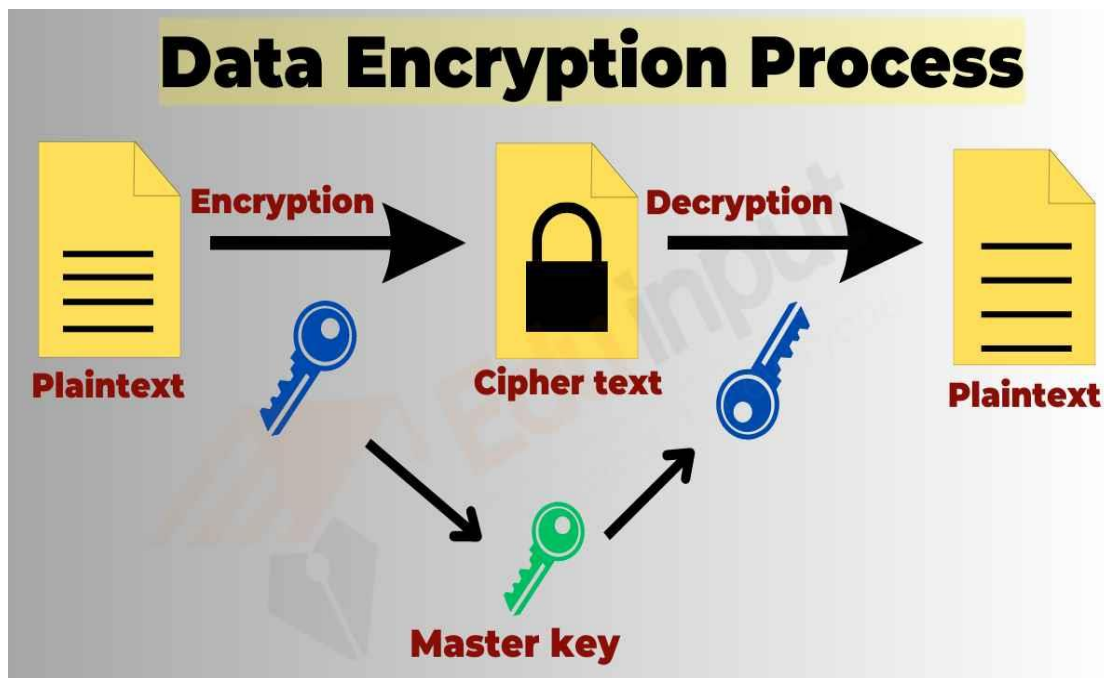


Figure 6: Diagram of the data encryption process (Basharat, 2023)

f. Employee Training and Awareness Programs

As earlier noted, human or social engineering was reported as the single source or cyberattacks origin. Employee training and awareness program entails educating the employees on the emerging forms of cyberattacks and how they are perpetuated. It also entails making them aware of signs that might be seen to lead to a cyber-attack. Comprehensive training programs for employees on cybersecurity best practices can significantly reduce the risk of security incidents. These training also ensure that employees are taught on precautionary measures that they should take in case of any initiated cyber-attack [9].

Warning them of severe consequences in case they intentionally divulge any information to outsiders is also a way to prevent any attacks. Regularly updating training materials and conducting simulated phishing exercises can help keep employees vigilant and prepared to respond to potential threats.

g. Collaboration with Industry Partners and Regulatory Bodies

Collaboration brings about sharing of ideas among key industry players, regulatory bodies and other cybersecurity organizations, on the best way of handling cyber threats. This can come in handy especially if an attack is launched in one company, they can alert the other companies and prevent even further attacks in the pharmaceutical industry. Participating in industry forums and working groups focused on cybersecurity can provide valuable insights and foster a collaborative approach to addressing common challenges [28].

IV. FUTURE TRENDS AND DEVELOPMENTS

More and more firms in the pharmaceutical industry continue to incorporate AI technologies in their daily running of activities. It is projected that the global artificial intelligence in healthcare market is in an uptrend with projected \$280.77 billion investment by companies by the end of 2032 from a value of \$19.45 billion in 2022 [7]. This can only be explained by the numerous benefits that companies derive from AI usage in their pharmaceutical operations. AI-driven cybersecurity solutions can provide more effective and efficient protection against cyber threats. For instance, machine learning and AI algorithms can process large data sets within a very short timeframe with high accuracy levels which is ideal for the clinical trials. AI is also capable of performing real time monitoring of patients' progress which enables prompt decision making. Predictive analytics powered by AI can also anticipate potential threats based on historical data, enabling proactive measures to prevent attacks before they occur [10].

Global Artificial Intelligence in Healthcare Market

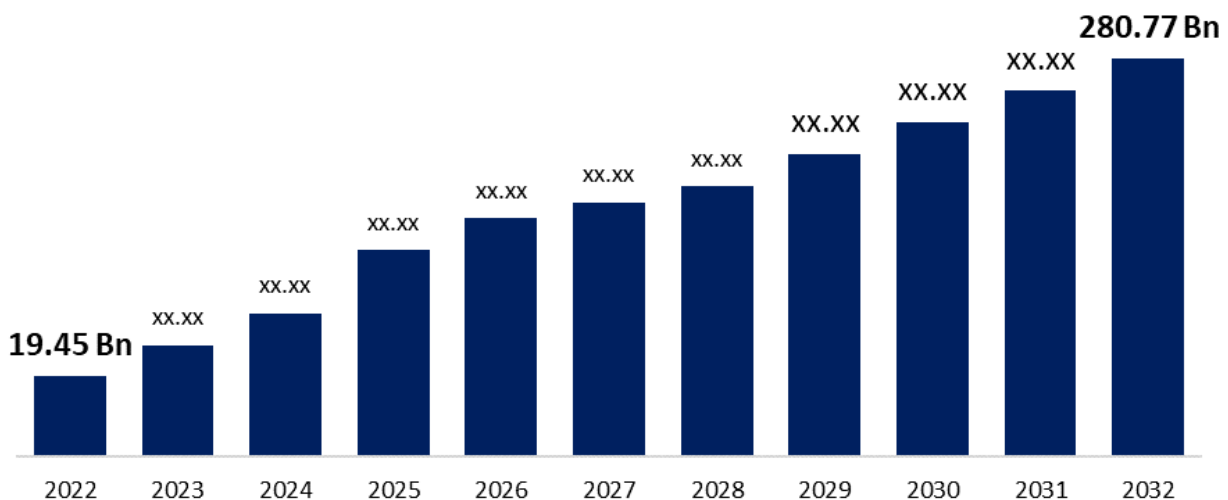


Figure 7: Bar chart showing Global artificial intelligence in healthcare market (Spherical insight, 2023)

These advantages make it promising that AI usage will continue in the near future. However, as technology evolves so do cyber criminals who prey upon companies with weak security measures. The pharmaceutical companies must anticipate threats and put in place measures that will help manage or prevent cyber-attacks. For instance, there is a roaming threat of advanced ransomware that might render many firms' security protocols redundant. The companies must therefore ensure that they stay updated and that their security features are improved on a regular basis [14]. Another evolving threat is cyber espionage, where state-sponsored actors target pharmaceutical companies to steal valuable intellectual property and sensitive research data. Pharmaceutical firms need to invest heavily on protecting patients' data and keeping cyber-attacks at bay.

One promising factor that will ensure that minimal losses are incurred during cyber-attacks is global collaboration as well as information sharing in the pharmaceutical industry. Since all the pharmaceutical companies in the world are prone to attacks, it is important to share crucial information on ways of combating cybersecurity threats. Pharmaceutical companies, governments, and cybersecurity experts need to continuously work together to keep updated on recent threats and also firewall protocols [19]. International cooperation is vital in addressing regulatory challenges and ensuring a consistent approach to cybersecurity across different jurisdictions. By fostering a culture of collaboration and transparency, the pharmaceutical industry can enhance its resilience against cyber threats and protect the integrity of its critical operations.

V. CONCLUSION

Artificial Intelligence is revolutionizing the pharmaceutical industry by enhancing efficiency, accuracy, and innovation in drug discovery, development, and personalized medicine. Despite these benefits, the industry faces significant cybersecurity challenges, such as data breaches, intellectual property theft, ransomware attacks, and insider threats. Implementing strong cybersecurity measures, including access controls, securing AI systems, incident response plans, regular audits, data encryption, employee training, and industry collaboration, is essential to safeguard sensitive data and maintain regulatory compliance. As AI technology and cyber threats evolve, continuous improvement and proactive strategies will be crucial in ensuring the pharmaceutical industry's resilience against cyberattacks. By fostering global collaboration and information sharing, the industry can enhance its cybersecurity posture and protect its critical operations.

REFERENCES

- [1] Alabdulatif, A., Khalil, I., & Saidur Rahman, M. (2022). Security of blockchain and AI-empowered smart healthcare: application-based analysis. *Applied Sciences*, 12(21), 11039.
- [2] AL-Dosari, K., Fetais, N., & Kucukvar, M. (2024). Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. *Cybernetics and systems*, 55(2), 302-330.
- [3] Al-Mansoori, S., & Salem, M. B. (2023). The role of artificial intelligence and machine learning in shaping the future of cybersecurity: trends, applications, and ethical considerations. *International Journal of Social Analytics*, 8(9), 1-16.
- [4] Almalawi, A., Khan, A. I., Alsolami, F., Abushark, Y. B., & Alfakeeh, A. S. (2023). Managing security of healthcare data for a modern healthcare system. *Sensors*, 23(7), 3612.
- [5] Alshehri, M. (2023). Blockchain-assisted cyber security in medical things using artificial intelligence. *Electron. Res. Arch*, 31(2), 708-728.
- [6] Arif, H., Kumar, A., Fahad, M., & Hussain, H. K. (2024). Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research. *International Journal of Multidisciplinary Sciences and Arts*, 3(1), 242-251.
- [7] Biasin, E., & Kamenjašević, E. (2022). Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals. *International Cybersecurity Law Review*, 3(1), 163-180.
- [8] Biasin, E., Kamenjašević, E., & Ludvigsen, K. R. (2024). Cybersecurity of AI medical devices: risks, legislation, and challenges. In *Research Handbook on Health, AI and the Law* (pp. 57-74). Edward Elgar Publishing.
- [9] Crane C (2022). 22 Ransomware Statistics You're Powerless to Resist Reading in 2022. Retrieved from <https://www.thesslstore.com/blog/ransomware-statistics/>
- [10] Chakraborty, C., Nagarajan, S. M., Devarajan, G. G., Ramana, T. V., & Mohanty, R. (2023). Intelligent ai-based healthcare cyber security system using multi-source transfer learning method. *ACM Transactions on Sensor Networks*.
- [11] Del Giorgio S. F. (2022). Impacts of Cyber Security and Supply Chain Risk on Digital Operations.
- [12] Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber-attacks: A review. *Applied Artificial Intelligence*, 36(1), 2037254.
- [13] Low J. (2018). Low Down. Which Industries Are Investing In AI - And For What Purposes? Retrieved from <https://www.thelowdownblog.com/2018/12/which-industries-are-investing-in-ai.html>
- [14] Kelly, B., Quinn, C., Lawlor, A., Killeen, R., & Burrell, J. (2023). Cybersecurity in Healthcare. *Trends of Artificial Intelligence and Big Data for E-Health*, 213-231.
- [15] Kiener, M. (2021). Artificial intelligence in medicine and the disclosure of risks. *AI & society*, 36(3), 705-713.
- [16] Maddireddy, B. R., & Maddireddy, B. R. (2022). Cybersecurity Threat Landscape: Predictive Modelling Using Advanced AI Algorithms. *International Journal of Advanced Engineering Technologies and Innovations*, 1(2), 270-285.

- [17] McCaskill S. (2017). Ransomware & Humans Are Silicon Readers' Biggest Cybersecurity Concerns. Retrieved from <https://www.silicon.co.uk/security/biggest-security-concern-220287>
- [18] Medical Packaging (2023). The Future of AI in Healthcare: Advanced Pharma Manufacturing, Limitations, & Precision Medicine. Retrieved from <https://medpak.com/ai-pharmacy/>
- [19] Michael, K., Abbas, R., & Roussos, G. (2023). AI in cybersecurity: The paradox. *IEEE Transactions on Technology and Society*, 4(2), 104-109.
- [20] Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*, 10(2), 2272358.
- [21] Mohammed, I. A. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. *Artif. Intell*, 7(9), 1-5.
- [22] Muheidat, F., & Tawalbeh, L. A. (2021). Artificial intelligence and blockchain for cybersecurity applications. In *Artificial intelligence and blockchain for future cybersecurity applications* (pp. 3-29). Cham: Springer International Publishing.
- [23] Nohe P. (2019). The Rise of Cyber Resilience. Retrieved from <https://www.thesslstore.com/blog/the-rise-of-cyber-resilience/>
- [24] Punia, V., & Aggarwal, G. Impact of Artificial Intelligence (AI) in Cybersecurity. In *Recent Advances in Computational Intelligence and Cyber Security* (pp. 183-193). CRC Press.
- [25] Radanliev, P., & De Roure, D. (2022). Advancing the cybersecurity of the healthcare system with self-optimising and self-adaptative artificial intelligence (part 2). *Health and Technology*, 12(5), 923-929.
- [26] Salama, R., & Al-Turjman, F. (2024). Future uses of AI and blockchain technology in the global value chain and cybersecurity. In *Smart Global Value Chain* (pp. 257-269). CRC Press.
- [27] SARCEA, O. A. (2024, July). AI & Cybersecurity—connection, impacts, way ahead. In *International Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings* (Vol. 1, pp. 17-26).
- [28] Basharat S. (May 17, 2023). Data Encryption in the Cloud – Types, Examples, and Software. Retrieved from <https://eduinput.com/data-encryption-in-the-cloud/>
- [29] Sen, R., Heim, G., & Zhu, Q. (2022). Artificial intelligence and machine learning in cybersecurity: Applications, challenges, and opportunities for mis academics. *Communications of the Association for Information Systems*, 51(1), 28.
- [30] Solfa, F. D. G. (2022). Impacts of cyber security and supply chain risk on digital operations: evidence from the pharmaceutical industry. *International Journal of Technology, Innovation and Management (IJTIM)*, 2(2), 18-32.
- [31] Spherical insight, (2023). Global Artificial Intelligence in Healthcare Market Insights Forecasts to 2032. Retrieved from <https://www.sphericalinsights.com/reports/artificial-intelligence-in-healthcare-market>
- [32] Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive*, 11(1), 1810-1817.
- [33] Walters, R., & Novak, M. (2021). *Cyber security, artificial intelligence, data protection & the law*. Springer.
- [34] Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. *SN computer science*, 3(2), 127.
- [35] Yildirim, M. (2021). Artificial intelligence-based solutions for cyber security problems. In *artificial intelligence paradigms for smart cyber-physical systems* (pp. 68-86). IGI Global.
- [36] Zaid, T., & Garai, S. (2024). Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers. *Blockchain in Healthcare Today*, 7.
- [37] Zaldivar, D., Lo' Ai, A. T., & Muheidat, F. (2020, January). Investigating the security threats on networked medical devices. In *2020 10th annual computing and communication workshop and conference (CCWC)* (pp. 0488-0493). IEEE.