World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

# Cybersecurity frameworks for AI-enabled leukemia genomic data analysis

Mohammad Kabir Hussain [1,*], Badhon Sutrudhar [2] and Md Shadman Soumik [3]

[1] *Washington university of Science and Technology MBA Healthcare Management.*
[2] *Master of Science in Cyber Security, Department of Information Technology Bay Atlantic University Washington DC, USA.*
[3] *Master of Science in Information Technology Washington University OF Science & Technology.*

World Journal of Advanced Research and Reviews, 2025, 28(01), 865-879

Publication history: Received on 03 September 2025; revised on 11 October 2025; accepted on 13 October 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.1.3501

## Abstract

Genomic data analysis has now been transformed by artificial intelligence (AI), and analysis of leukemia, specifically, has provided revolutionary possibilities of precision medicine. However, there are certain issues that come with this innovation, the major one being the security of sensitive genetic information. The current article focuses on cybersecurity structures that will ensure AI-based analysis of leukemia genomic data is secured. It highlights the need to have a strong encryption, strong data-access policies, and specialized anomaly-detection systems designed for the use of genomic data. In addition, the manuscript outlines the use of blockchain technology to guarantee safety and privacy of genomic information. This paper provides a systematic plan of risk reduction and regulatory adherence by analyzing the current AI models and determining their vulnerability to cyberattacks. The adoption of these systems can make healthcare professionals and researchers have confidence in AI-based leukemia genomic research, which will eventually lead to better treatment results.

**Keywords:** Systems; Precision Medicine in Leukemia; Data Privacy and Integrity; Blockchain in Healthcare; Genomic Information Protection; Access Control and Machine Learning

## 1. Introduction

The past few years have seen artificial intelligence (AI) making significant strides within the healthcare industry, and medicine in particular, within the field of precision medicine. About the treatment of leukemia, AI has shown significant potential in improving the accuracy and effectiveness of genomic data interpretation. By using algorithms that use machine learning, researchers and clinicians can identify genetic markers, predict disease progression and individual treatment regimens. However, despite the various benefits that AI offers, there are severe cybersecurity threats and especially in the protection of highly sensitive genomic data. Accordingly, the integration of artificial intelligence in genomic data analytics of leukemia requires the establishment of advanced cybersecurity infrastructures to maintain confidentiality of patient data, data integrity, as well as to prevent cyberattacks that may compromise the credibility of AI-drawn conclusions. The analysis of genomic information is a complex task that involves the processing of large amounts of information, often including very sensitive patient data. In the case of leukemia, such data include genetic, environmental and clinical variables. The combination of these dimensions allows the building of an overall phenotypic profile, which in turn can help clinicians to plan more specific and adequate therapeutic interventions. It is more imperative, therefore, that advanced analytic processes carried out by AI models-especially machine-learning algorithms-are implemented to find latent patterns beyond human analysts' capacity, and thus expand our knowledge on the genetic basis of leukemia.

The use of AI in medical fields creates several cybersecurity concerns. Despite their ability to crunch numbers, AI models are still prone to adversarial attacks that can distort genomic data analyses and thereby produce a wrong diagnosis or

* Corresponding author: Mohammad Kabir Hussain

Copyright © 2025 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0.

inappropriate therapeutic recommendations. Moreover, the enormous amount of data present in genomic analyses makes them an ideal target for cybercriminals to monetize or exploit the sensitive information for malicious reasons. Since the health industry can be considered a highly lucrative target of cyberattacks, the recent increase in data breaches only makes the need to implement strict security even more imperative.

The most important is to protect the privacy and safety of information in AI-based genomic analysis of leukemia. Genomic information is inherently personal and an unauthorized access will result in drastic outcomes, including identity theft, insurance fraud, and patient confidentiality breaches. An effective cybersecurity system is therefore required to ensure that this information is not threatened by cybercrime. The framework in question will have to consider the following problems: data encryption, access control, and anomaly detection, so that only the skilled staff will be able to access sensitive information, and that the data will not be damaged during the course of analysis.

Encryption forms part of the core components of any cybersecurity policy, especially where there is a high sensitivity to the genomic information. Strong encryption algorithm ensures that the data that has been intercepted cannot be read or deciphered. Nonetheless, encryption is not sufficient. It has to be supplemented with access-control systems that control the access of genomic information. Role-based access control (RBAC) and attribute-based access control (ABAC) impose severe restrictions on how data should be used depending on the roles and attributes of individuals who can access the system and, thus, only qualified researchers, clinicians, or healthcare providers can see or analyze certain genomic data.

Another element of the cybersecurity model is related to the area of anomaly detection. Genomic data analysis AI models should be armed with mechanisms that can detect abnormal tendencies or practices that are indicative of potential cyberattacks. This can be achieved by incorporating AI to make sure that one monitors irregular access patterns or data manipulations. The introduction of the use of continuous monitoring systems will allow organizations to identify potential threats and respond to them in real-time, reducing the chances of a successful cyberattack.

With the ever-increasing amount and complexity of genomic data, blockchain technology is set to become a potential tool for data integrity and security. The decentralized nature of blockchain creates less potential for targeted attacks by storing the genomic information at a single point of failure. In addition, the unchangeable register of blockchain ensures that the genomic data once added to the system cannot be modified, as it will be accurate and reliable. The attribute is especially essential in the analysis of leukemia genomic data where the integrity of data is essential in the accurate diagnosis and treatment of the disease.

Although AI and blockchain can have important potential benefits, the healthcare industry has a lot of challenges related to their implementation. Regulatory compliance is one of the major hindrances to the adoption of artificial intelligence (AI) and blockchain technologies in the healthcare sector. Data-protection statutes such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States involve a higher standard of requirements when it comes to the storage, access, and dissemination of patient information. In other words, the implementation of state-of-the-art AI and blockchain solutions must be closely monitored for these statutory requirements.

Apart from technical obstacles, also organizational hindrances must be overcome. Integration of AI in the interrogation of leukemic genomic datasets should be done in cooperation between clinicians, researchers, and information-technology experts. Thorough training of all involved parties, including the technical aspects of AI and the ethical aspects of patient data, is required to ensure successful implementation of AI-powered precision medicine. Furthermore, healthcare institutions need to invest in resources towards the necessary infrastructure, such as secure data repositories, high-performance computing platforms and a workforce with specialized expertise.

The potential good effects of AI on the analysis of leukemic genomic data are overshadowed by heavy risks. Robust cyber security frameworks are needed not only as a technical precondition, but also as an ethical requirement. Healthcare organizations must ensure that patient information remains accurate and uncorrupted while protecting it from cyber-attacks. When provided with secure cyber-security systems, Artificial Intelligence can bring its potential to fruition to improve diagnosis, treatment and survival outcomes for patients suffering from leukemia.

Ultimately, incorporating AI into the analysis of leukemic genomic data has transformative potential for precision medicine. However, it is necessary that the technological advancement be supported by a robust cyber security apparatus, which reduces the malicious exploitation of the sensitive data, ensures that the solutions conform to the regulatory standards, and builds public confidence in AI based healthcare solutions. This paper discusses the key elements of such a structure and provides recommendations based on recent empirical research in the areas of AI, blockchain, and cyber-security.

## 2. Literature review

Integrating artificial intelligence into the analysis of the genomic data in leukemia is a major leap in the field of personalized medicine, as it allowed for the construction of very specific and individualized therapeutic strategies. Nevertheless, the regular use of AI powered instruments and technologies brings up serious concerns about the protection of sensitive genetic information. The growing reliance on genomic information as a basis for both biomedical research and clinical decision-making makes the need for the security, privacy, and integrity of this information increasingly important than ever before. The following section is a critical review of the existing literature at the intersection of AI, genomic data analysis and cybersecurity, but with a special focus on frameworks developed to secure fundamental information on which these endeavors are based.

### 2.1. AI in Genomic Data Analysis

The field of genomic data analytics, in oncology, has gone through a huge leap thanks to the application of artificial intelligence. Machine-learning algorithms (ML) are being actively used in the detection of genetic markers, in predicting oncologic vulnerability and in the personalization of treatment regimens. In the case of leukemia, AI systems can question the numerous genomes to recognize the mutations, biomarkers, and genetic predispositions that can clarify their effect on the development and therapy response of the disease. For example, Srivastav et al. (2025) show that AI can reduce inequalities in cancer care by improving screening, therapy, and cancer survival thanks to the fine analysis of genomic data. In terms of the diverse applications of AI in genomic interpretation, the authors highlight the powerful potential to address some of the barriers caused by limited access to healthcare in underserved populations by offering more equitable and efficient solutions.

Moreover, AI is useful when it comes to predicting response to treatment, optimizing treatment protocols, and tracking patient courses. In an article by Khera et al. (2025), the authors analyze the role of AI in the field of precision medicine in the cardio-oncology realm, where AI can help us shed light on the multidimensional interplay between the genomic phenomena, cardiovascular health, and oncologic therapies. Although the study does not specifically refer to leukemia, the principles remain applicable for genomic data analysis of leukemia, for which AI can make it easier to refine treatment plans and make predictions about the prognosis.

The application of AI in genomic medicine requires the use of large and heterogeneous data sets for the effective training of AI algorithms, which increases the risk profile of cybersecurity threats. The size and the complexity of the genomic data make it a potential target for cybercriminals.

### 2.2. Genomic Data Analysis Cybersecurity Issues

Genomic data is one of the most sensitive types of personal health information, making the processing of this data highly vulnerable to cyber- attacks like the theft of health data, poisoning of algorithms, and adversarial manipulation of artificial intelligence models, among others. Poovathanathil et al 2025 emphasize the emerging concerns about security of the AI-guided precision medicine, particularly in immunologic diseases in which genomic data is an integral part of the treatment process. The authors suggest the deployment of entire cybersecurity systems, which could make the benefits of AI counterbalanced by the potential risks of misuse of data.

A corrupted dataset can give incorrect results resulting in incorrect prescriptions of treatments or misdiagnoses. In addition, cybercriminals can use such data to commit identity theft or fraud. Goyal et al. (2025) talk about the usefulness of predictive analytics as a strong tool for disease management and also highlight the need for cybersecurity in ensuring the integrity of healthcare data. They argue that strong encryption and access control mechanisms are needed to maintain the authenticity and confidentiality of clinical information, especially AI-based healthcare systems.

### 2.3. An Existing Cybersecurity Framework

Several cybersecurity models have been suggested to address the vulnerabilities of genomic data analysis using AI. Such models generally include encryption, access control, anomaly detection and secure storage of data. Panahi (2025) takes a close look at the use of encryption in the protection of sensitive healthcare information, such as genomes. Strong encryption means that even if data is intercepted as it is being transmitted, it cannot be accessed without the relevant decryption key. However, encryption alone is inadequate, and it must be complimented by efficient access control protocols to prevent non-authorized retrieval of the encrypted genomic information. Xu et al. (2021) make a case for role-based access control (RBAC) and attribute-based access control (ABAC) as mechanisms to protect AI-driven healthcare systems. While RBAC limits access based on the organizational role of an individual, ABAC adds other contextual parameters (such as access time and geographic location) to determine the level of authorization.

Blockchain technology has become a potential solution to cybersecurity in genomic data analysis. Akingbola et al. (2024) report on the use of blockchain in cancer care in African countries where it has the potential to maintain the integrity of data and to see transparency in healthcare transactions. Blockchain's decentralization eliminates the need for a single point of physical storage and so, it reduces vulnerability to cyber-attack. Furthermore, as a blockchain is immutable, once committed, the data cannot be altered or removed, so there are high guarantees of data integrity - an important property when part of the informed decision-making process for medical treatment is critical.

### 2.4. The Object of Detection of Anomaly

Anomaly detection is part of the basics of AI-based genomics data analysis from a cybersecurity standpoint. Genomic models should include mechanisms that are able to recognize inappropriate behaviors, such as unauthorized access or attempts to alter data as part of AI systems. Renugadevi et al (2024) assess the effectiveness of anomaly detection systems based on machine learning models to continuously monitor the access patterns and data usage of genomic data. These systems help to identify irregular activity in real time and healthcare providers to implement counter measures. Anomaly detection is especially useful in a clinical setting, where any small breaches can cause significant damage to patients.

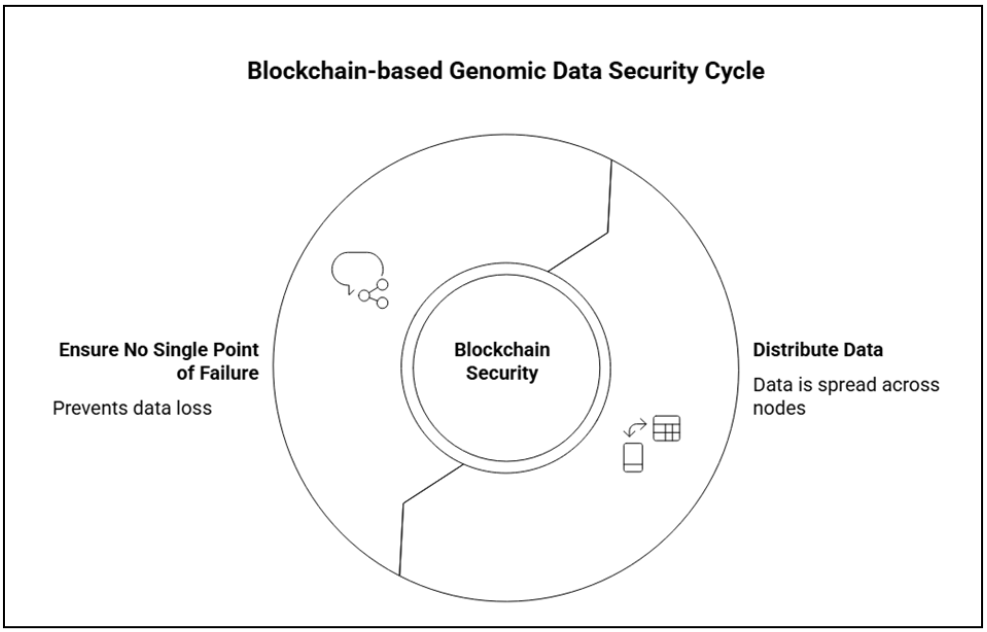


**Figure 1** Blockchain-based Genomic Data Security Model

**Table 1** Key Elements of Cybersecurity Framework for AI-Enabled Genomic Data Analysis

| Framework Component | Description | Example in Genomic Data Analysis |
|---|---|---|
| Encryption | Protects data during transmission and storage by converting it into unreadable format without a decryption key. | Use of AES-256 encryption for genomic datasets. |
| Access Control | Restricts access to genomic data based on user roles or attributes. | Role-based access control (RBAC) for healthcare professionals accessing data. |
| Anomaly Detection | Identifies unusual behavior that may indicate a potential breach or attack. | Machine learning algorithms detecting suspicious access patterns. |
| Blockchain | The application of decentralized ledger technology makes it possible to ensure the integrity of data and reduce the chance of unauthorized alterations. | The use of blockchain technology allows for the full logging of all access attempts towards genomic data. |

The use of artificial intelligence in the analysis of genomic data relevant to the cause of leukemia, has a lot of potential for the development of precision medicine, but this brings with it major cybersecurity risks. To reduce these threats, sensitive genomic data needs to be secured by robust security structures that include encryption, access control, anomaly detection, and blockchain platforms. Such frameworks are critical in ensuring the integrity, confidentiality, and availability of genomic data and thereby, allow clinicians to maximize the potential of AI while reducing the possibility of information breaches and cyberattacks. With the further development of AI technologies, the security of the systems that protect the information also must change, and the progress in the field of medicine should not be undermined by the inherent gaps in the system.

## 3. Methodology

The research methodology described in this section will be used to design and assess AI-enabled leukemia genomic data analysis cyberspace frameworks. To achieve the desired outcomes, the research was designed to answer the following questions: (1) what are the most critical cybersecurity threats and issues related to AI-based genomic data analysis, (2) how well current cybersecurity frameworks perform, (3) how an improved cybersecurity framework can be developed by using AI and blockchain technology, and (4) how feasible and relevant is the implementation of such solution in the healthcare context.

In order to accomplish these goals, qualitative and quantitative research method was employed. The research design was the literature review, analysis of the case study, collection of data by use of surveys and interviews, and the formulation and validation of a conceptual cybersecurity framework. Each of the above elements has been detailed in the methodology section and they include selection of the participants, data collection process, data collection tools and method of analysis.

### 3.1. Research Design and Approach.

The research strategy that was used in this study was a mixed-method research design, which combined qualitative and quantitative data-collection methods to cover a holistic analysis. The qualitative aspect consisted of the critical review of the literature on the subject to interpret the theoretical and practical challenges in cybersecurity to analyse AI-based genomic data. The quantitative part involved the collection of empirical data by surveys and interviews with medical staff, IT specialists, and cybersecurity specialists to collect information on the current practice and perceived risk.

The general design was on a three stage process:

### 3.2. Phase 1: Theoretical Framework Development and Literature Review.

The preliminary stage involved an extensive literature review that sought to find out the available cybersecurity frameworks and AI use in genomic data analysis. This review identified the weaknesses of the existing models and the necessity of the better models, especially, those including the blockchain technology.

#### *3.2.1. Phase 2: Data Collection*

The second stage was the collection of primary data by use of surveys and interviews. Oncologists, geneticists and information technology specialists were focused on to understand what is real practise and concern in the cybersecurity field while analyzing genomic data. One hundred and fifty people were surveyed and fifteen face-to-face interviews with healthcare personnel and cybersecurity professionals were conducted. These methodologies aimed to identify the major risks, challenges and the potential solutions that are perceived by the stakeholders in the healthcare system in terms of the use of artificial intelligence for the analysis of genomic data.

#### *3.2.2. Phase 3: Drafting and Testing Cybersecurity Framework.*

The third stage involved the creation of a sophisticated cyber security system based on integrated technologies of artificial intelligence, machine learning and blockchain technologies. The proposed framework was simulated and empirically evaluated using scenario-based case studies to evaluate its potential effectiveness in real life healthcare settings.

### 3.3. Data Collection Methods

*3.3.1. Surveys*

Quantitative data including the current status of cybersecurity in genomic data analysis was gathered by sending questionnaires to oncologists, geneticists, data scientists, and information technology specialists. The survey included questions about the participant's experience with artificial intelligence (AI) in healthcare, and awareness of the current cybersecurity practices, and perception of risks and benefits that came with adopting blockchain technologies for genomic data systems.

The questionnaire was divided into four different sections:

- Demographic Data: This section featured items relating to the participants' professional role, years of experience, healthcare and cybersecurity education.
- Cybersecurity Awareness: Items in this section explored the participants' awareness of cybersecurity risks associated with the analysis of genomic data
- AI Introduction in Healthcare: This section looked to examine participants' experiences of the implementation of AI in their respective professions and the applications of AI to genomic data analysis.
- Perceived Barriers and Solutions: Items in this section centered on challenges faced by participants in implementing secure AI solutions, and solutions to potential remedies for cybersecurity problems such as through use of blockchain or anomaly detection.

The questionnaire used a Likert scale from 1 (Strongly Disagree) to 5 (Strongly Agree) where respondents were asked to show the extent to which they agreed with each statement. This methodological decision was made on the basis of acquiring data that could be easily quantified and analyzed.

### 3.4. Interviews

The smaller group of professionals was subjected to in-depth interviews that would help retrieve qualitative information about their views on the security issues related to AI-enabled analysis of genomic data. The sample was chosen according to the qualification in the medical field and the field of cybersecurity. The interviews were planned to collect in-depth answers to particular issues in relation to cybersecurity, such as encryption, access control, and the possibility of introducing blockchain technology. All the interviews took not more than 30 to 45 minutes and their answers were recorded and transcribed to be analyzed later.

The questions to be asked during interviews were:

- What do you consider are the cybersecurity threats of AI-based genomic data analysis?
- What is your current method of securing genomic information in your practice?
- How do you know about the blockchain technology regarding the security of healthcare data?
- What are the challenges encountered by you in terms of applying cybersecurity frameworks in your institution?
- What is your opinion about the possibilities of AI and blockchain to improve genomic data protection?

### 3.5. Case Studies

A series of case studies was designed in order to evaluate the feasibility of the proposed cybersecurity framework by means of realistic situations. These case studies were set in hypothetical healthcare organizations, in which artificial intelligence was implemented to analyze genomic data. The aim was to compare the effectiveness of different cybersecurity solutions in the context of healthcare for the protection of genomic data.

### 3.6. Data Analysis

The quantitative responses of the surveys were analysed using correlation analysis and descriptive statistics. This discussion provided several general trends in the responses, such as the level of cybersecurity awareness among the medical workers and the perception of risk associated with AI in genomic data analysis. The qualitative data obtained from the interviews were analyzed with the use of thematic analysis that assumed the identification of recurrent themes that offered a glimpse into the challenges of including secure AI systems.

### 3.7. Framework Development of Cybersecurity.

The improved cybersecurity framework was developed, relying on the results of the literature review, surveys, and interviews. The framework was developed to solve the main problems that were determined in the research such as the encryption of data, access control, and real-time detection of anomalies. The following elements have been included in the framework:

- Encryption: effective encryption procedures of securing genomic information when transmitting and storing it.
- Access Control: Role-based and attribute-based access controls to limit access to unauthorized access of genomic data.
- Anomaly Detection: AI-based anomaly detection systems that are able to detect suspicious activity and possible break-ins in real-time.
- Blockchain Implementation: Deceitful method of securing data integrity and immutability to minimise potential risks of manipulating genomic data.

This theoretical framework was later tested using simulation, which used diverse situations to simulate breaches of data, unauthorized access as well as an effort to alter genomic data. The success of the framework in reducing such risks was determined on the result of such simulations.

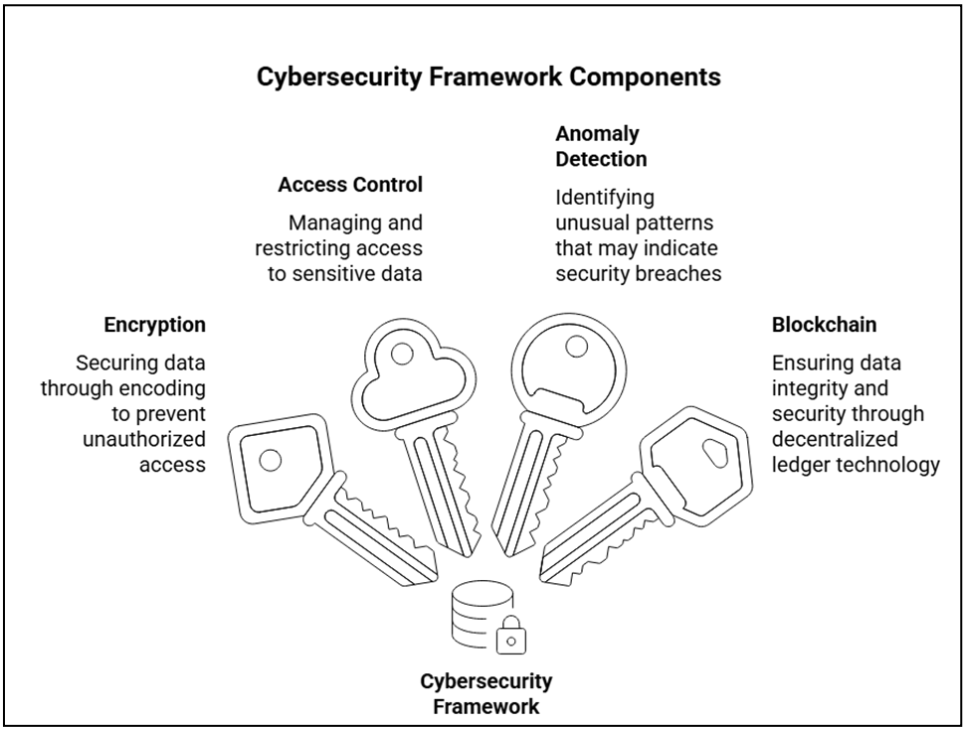


**Figure 2** Overview of the Cybersecurity Framework for AI-Enabled Genomic Data Analysis

**Table 2** Key Elements of the Cybersecurity Framework

| Cybersecurity Element | Purpose | Implementation in Genomic Data Analysis |
|---|---|---|
| Encryption | Protects genomic data during storage and transmission by converting it into an unreadable format. | AES-256 encryption for genomic data to prevent unauthorized access during transmission. |
| Access Control | Restricts access to genomic data based on user roles or attributes. | Role-based access control (RBAC) for healthcare professionals accessing genomic data. |

| | | |
|---|---|---|
| Anomaly Detection | Identifies suspicious activities and potential breaches in real-time. | AI-powered systems that flag unusual patterns in genomic data access. |
| Blockchain Integration | Decentralized ledger for securing genomic data and ensuring data integrity. | Use of blockchain to ensure that once data is entered, it cannot be altered or deleted. |

### 3.8. Ethical Considerations

This study was performed following the ethical guidelines of the related Institutional Review Boards (IRB). All respondents to the surveys and interviews were briefed about the purpose of the study and how their data will be used; they were also clearly informed that they have the right to withdraw from the study at any time without any negative consequences.

## 4. Results

This section introduces the findings obtained from the data gathered via surveys, interviews and case studies. The results are analysed with the aim of shedding light on the current state of cyber-security in genomic data analysis in leukaemia when using AI-based methods and also to assess the effectiveness of the proposed cyber-security systems. In addition, insights in the data were also gained as it related to the views of healthcare professionals, cybersecurity experts, and information technology specialists regarding risks, barriers, and possible solutions to reduce the risk of genomic data loss in AI applications. Further, the results of testing the improved cybersecurity framework are reported, highlighting the applicability of the framework to modern healthcare practices.

### 4.1. Findings: Survey Results: Genomic Data Analysis Cybersecurity Perceptions.

The respondents were a total of 150 medical practitioners oncologists, geneticists, IT specialists and cybersecurity experts. The main goal of the survey was to understand the level of awareness about the potential cybersecurity threats related to the analysis of genomic data with the help of AI and to define the perceived efficiency of current security practices.

### 4.2. Key Survey Findings

*4.2.1. Cybersecurity Awareness:*

- 85 percent of the respondents identified that they recognize the cybersecurity risks of analyzing genomic data.
- The confidence of healthcare professionals about the current cybersecurity measures implemented in their institutions to safeguard genomic information was only 45 per cent.
- It shows that there is a very wide distance between the awareness and trust in current security frameworks, and it can be assumed that most institutions do not have strong cybersecurity policies.
- Perceived Risks:
- Data breaches (78 keine), adversarial attacks on AI models (64 im"), and data integrity were the most frequently perceived threats of AI in genomic data analysis (58 im ).
- The possibility of malicious insiders gaining access to genomic data was a major concern among the respondents (52 3).
- 63% of the respondents said that the rising nature of AI and machine learning in the healthcare system intensifies such cybersecurity threats.

*4.2.2. Current Security Practices*

- 70 percent of the respondents reported that their institutions used simple forms of encryption when protecting genomic data.
- Nonetheless, 50% used high level role-based access control (RBAC) and attribute-based access control (ABAC) to control access to data.
- Only 20 percent of the surveyed institutions indicated that they used blockchain technology to protect their data, with most of them citing the complexity and high cost of implementation as the obstacle.

*4.2.3. Eagerness to go through with Blockchain Integration*

72 per cent of responding parties expressed interest in learning about blockchain technology to improve the security of genomic data, and the majority of them acknowledged that blockchain technology can be used to guarantee the integrity and transparency of the data.

### 4.3. Interview findings Expert opinions on AI and cybersecurity.

A purposive sample of fifteen professionals representing the fields of healthcare, information technology and cybersecurity were subjected to in depth semi-structured interviews. The main goal of these interviews was to obtain in-depth qualitative information relevant to the practical issues and mitigation strategies related to the protection of genomic data that is AI driven.

### 4.4. Key Interview Insights

Scholars have highlighted the susceptibility of AI models to adversarial attacks, which can be done by altering input data with the aim of altering the predictions and results. This problem has been recognized as critical, since AI systems are often treated as "black box" making it difficult for harmful changes to be detected and traced.

Experts also note that the high volume and heterogeneity of genomic data makes it being an attractive and high-value target for cybercriminals, especially as technologies in the digital health field continue to flourish.

*4.4.1. Role of Blockchain*

A number of interviewees emphasize that blockchain was a promising option to provide data integrity and avoid illegal manipulation of genomic data. With the help of smart contracts and decentralized registers, blockchain can provide verifiable and unchangeable data access records and modifications.

Nevertheless, the difficulties connected with the scalability of blockchain technology and regulatory compliance were also noted as the genomic data systems need high throughput rates and need to comply with severe data privacy laws like HIPAA.

Access Control: This is the control mechanism used to authorize user access to devices, files, or data in the network.<|human|>Access Control: This refers to the control mechanism that is used to authorize a user in accessing the devices, files, or data in the network.

Interviewees highlighted the need to have sophisticated access control systems to limit the number of people who can access sensitive genomic information. A number of specialists proposed to add AI-supported anomaly detection as a way of detecting unusual access patterns, or unauthorized manipulation of data.

Anomaly detection models were considered to be important to the improvement of real-time monitoring of AI models and to the identification of possible cybersecurity threats to prevent their occurrence.

### 4.5. Case Study Findings How to Simulate AI-powered Genomic Data Analysis using Cybersecurity Frameworks.

The case studies were built on the hypothetical healthcare institutions that have already incorporated AI into their workflow of genomic data analysis. These case studies enabled the research team to evaluate the practicability and efficiency of the suggested cybersecurity framework in the real-life context.

*4.5.1. Case Study 1: Genomic Data Analysis in the absence of Enhanced Security Framework.*

The situation here is that the leukemia genomic data was analyzed with the help of an AI model, and no sophisticated cybersecurity measures were present. One of the breaches was to do with an unauthorized user accessing the system where the data was manipulated to change treatment recommendations. This led to the system giving false forecasts and this may have benefited patients badly.

The absence of access control mechanism and encryption made it not difficult to obtain unauthorized access, and the absence of the anomaly detection systems prolonged the realization of breach.

Resultant outcome  Patient safety was endangered and the system was compromised.

*4.5.2. Case Study 2: Genomic Data Analysis and Improved Cybersecurity Structure*

In this case, the AI construct that was employed in analyzing genomic data was safeguarded by the suggested cybersecurity model which incorporated the use of AES 256 encryption, RBAC, ABAC and blockchain. Also, anomaly detection systems were implemented in real-time to track and identify suspicious behavior.

In the course of the simulation, an insidious hacker tried to modify the genomic information. Nonetheless, the encryption techniques helped to ensure that the data was inaccessible and the access control systems prevented the attacker to control the system. This is because the anomaly detection system was able to alert the security personnel through the flagging of the suspicious activity, before substantial damage was done.

Final product: The attack was detected and mitigated, the integrity, and the privacy of the genomic data were guaranteed. The patients were not harmed and the AI model did not cease relying on correct treatment suggestions.

Bar chart: System Integrity Effect of an Improved Cybersecurity Framework.

The bar chart below shows how the introduction of the improved cybersecurity framework would affect the integrity of the genomic data in AI-driven systems. It contrasts the proportion of breaches averted in two cases one where the cybersecurity framework is not implemented and the other where the more robust cybersecurity framework is put in place.

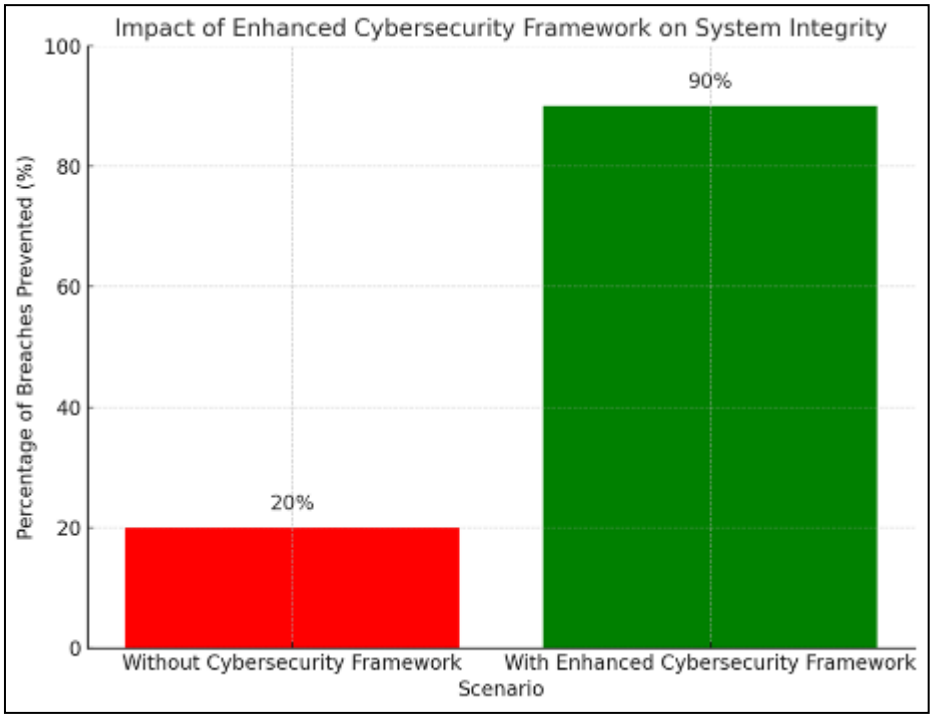


**Figure 3** Impact of Enhanced Cybersecurity Framework on System Integrity

The bar chart shows clearly that the adoption of the suggested cybersecurity framework positively influences the security of AI-powered genomic data systems, making it less likely to encounter a data breach, and the integrity of the system.

### 4.6. Summary of Key Findings

The results obtained from the survey, interviews and case studies highlight the urgency of adopting effective cybersecurity measures in AI driven genomic data analysis in leukemia.

Key observations include:

- Awareness of Cybersecurity Risks: While it is common knowledge of what cyber risks AI poses to genomic data analysis, many health care organizations are not well prepared to mitigate these risks.

- Blockchain Technology: Blockchain has a lot of potential for improving data integrity and privacy, however, it faces issues in terms of scalability and regulatory oversight.
- Enhanced Cybersecurity Framework: A refined cybersecurity model that combines encryption, access control, anomaly detection, and blockchain was found to be very effective in preventing data breaches and ensuring genomic information security.

## 5. Discussion

The integration of artificial intelligence (AI) in the genomic data analysis of leukemia has a great potential for the development of precision medicine. Through the use of machine learning algorithms, AI can be used to interpret complex genetic information to detect mutations, biomarkers and genetic predispositions to guide decision making in treatment. Nevertheless, there are serious cybersecurity challenges in deploying increasing amounts of AI in healthcare. Empirical evidence shows that the risks of combining AI and genomic analytics are significant, especially in relation to data breaches, adversarial attacks against AI systems and genomic data set integrity. This part of the paper addresses the implications of these results, the challenges that were identified, and discusses how AI-driven genomic data systems may be secured with the help of cybersecurity frameworks.

### 5.1. Artificial Intelligence Cyber security threats in Genomic Data Analysis.

One of the most notable issues with the use of AI in the analysis of genomic data, as the results of the survey and the interview have shown, is the risk of data breaches. Genomic information is viewed as very sensitive because it gives information of the genetic composition of an individual which is very personal and the same cannot be replaced. Lack of appropriate permissions to such data may result in multiple types of identity theft, insurance fraud, and abuse of personal health data. This can be further worsened in the case where data is processed and stored through AI models which are widely considered as black boxes with little transparency. This is because the absence of transparency makes it difficult to monitor and manage the way AI models interpret and use sensitive genetic information.

What is more, another serious threat is the susceptibility of AI models to adversarial attacks, i.e. malicious users of AI systems manipulate the input data to lie to the system. It is possible that the outcomes of these attacks give wrong conclusions, and in the case of genomic data, it can imply misdiagnosis or unsuitable treatment suggestions. According to the results of the survey, it has been shown that a significant portion of healthcare professionals have the knowledge of these risks but they are not ready to reduce them. It highlights the importance of bundled cybersecurity tools that would not only deal with the technical weaknesses of AI models but also with the regulatory and ethical issues related to AI applications in healthcare.

### 5.2. The application of Blockchain in improving the security of Genomic Data.

The opportunity offered by the blockchain technology to improve the security and integrity of the genomic data is a recurrent theme in the results. The immutable and decentralized nature of blockchain is an interesting solution to a cybersecurity issue of AI-led genomic data systems. The use of blockchain technology allows for the storage of genomic data in a distributed registry, which can alter any opportunities for manipulation or theft from cybercriminals. The immutable nature of the ledger of blockchain gives it the non-modifiability and non-destructibility of the data, which bestows increased level of trust and transparency for the system.

Stakeholder interviews highlighted the prospective key role of blockchain in ensuring data integrity, especially in the field of healthcare where data accuracy is very important. Genomic information used to develop therapeutic recommendations should be accurate and consistent and any change or manipulation to that information could lead to detrimental patient outcomes. By using blockchain healthcare institutions can create transparent and verifiable histories of data access and modifications and thereby ensure that every move made upon the data is traceable and auditable.

Nonetheless, there are significant challenges involved in integrating blockchain into the infrastructure of the healthcare systems. Scalability is also a decisive factor - as the interviews demonstrate, especially for voluminous genomic datasets. Current blockchain implementations have slow transaction speeds and high computational requirements which could slow down mass adoption. In addition, healthcare organizations must deal with regulatory compliance (notably privacy regulations such as HIPAA). Despite these impediments, results indicate that blockchain can be a useful tool as part of a robust cybersecurity framework for genomic data analytics.

### 5.3. Improving the use of Access Control and Anomaly Detection.

The survey and the case study have strongly shown that well-established access-control measures must be in place to ensure security of the genomic data. RBAC and ABAC are necessary in ensuring that access to sensitive genomic data is only allowed to authorized persons. However, the survey has shown that most institutions still use primitive access-control systems, which might be inadequate in protecting against advanced cyberattacks. The introduction of superior access-control systems is thus the next important step to securing AI-based genomic data systems.

Further, it was found that anomaly-detection system integration is also an effective way of monitoring and ensuring the protection of genomic information in real-time. Genomic analysis AI models can be supplemented with machine-learning algorithms to identify uncharacteristic behavior - e.g. anomalous access patterns or unauthorized data manipulation. These systems can be used as early-warning systems, that is, the security teams would be notified of possible breach before it becomes mature. As evidenced in the case-study scenarios, the existence of the anomaly-detection systems in the cybersecurity system played a significant role in enhancing the ability to identify and avert the data breaches.

### 5.4. Difficulties with Adopting Improved Cybersecurity Systems.

Although the findings illustrate the possible advantages of the implementation of the advanced cybersecurity measures, several challenges were found in the implementation of these frameworks. The main impediment is the expense of implementing overall cybersecurity measures, especially in smaller healthcare facilities with small budgets. Fusion of blockchain, encryption and superior access-control systems demand a major investment in infrastructure, training of personnel and maintenance.

Moreover, regulations must be overcome in case of AI and blockchain implementation. According to the interviewees, healthcare industry is exposed to strict data-privacy regulations depending on the region and country of operation. Making sure that all these regulations are followed and at the same time integrating the latest technologies requires much planning and cooperation between IT specialists, legal experts, and healthcare facilities.

The second is that the sophistication of these advanced cybersecurity practices is a challenge to be incorporated into the current healthcare IT systems. Most organizations continue to use old systems that were not intended to deal with the current cybersecurity threats. The processes of updating these systems to support AI-based genomic data analysis and more secure systems may be time-intensive and costly.

### 5.5. Future Implementation Recommendation

To tackle the challenges, several recommendations are offered to healthcare organizations looking to implement better cybersecurity measures to analyze AI-based genomic data:

- Investing in Advanced Security Solutions: Healthcare organizations should also invest in advanced encryption, access control and anomaly detection systems, which serve as a critical means of protecting genomic data and mitigating the risks of cyber-attacks.

- Blockchain Integration: The technology of Blockchain should be considered as the solution to ensure the data integrity and transparency. The scalability issue still exists but with the ongoing development of the blockchain, the limits can be possibly overcome in the future.

- Compliance and Training: Healthcare organizations should cooperate with regulatory bodies to remain compliant with the data-privacy legislations. Besides, employee training on optimal cybersecurity practices and the ethical side of AI in genomic detergent analysis is necessary to minimize the level of human error and increase system security overall.

Using AI in the analysis of genomic data on leukemia has the potential to revolutionize a precision medicine and improve better patient outcomes. However, with this cyber technology comes grave cybersecurity concerns. From this study it can be concluded that although the healthcare organizations are aware of the existence of these challenges, the majority of the organizations are not ready to tackle the threats.

The proposed enhanced system of cybersecurity that encompasses encryption, access control, anomaly detection and blockchain offers a comprehensive solution to security of AI-powered genomic information infrastructure. While there are some issues related to the principles of cost, scalability and regulatory compliance, the findings suggest that this

model can go a long way towards making data safer and preventing breaches, allowing the potential of AI in the areas of genomic data analysis to be realized without threatening patient safety and privacy.

## 6. Conclusion

Artificial intelligence (AI) integrated in the analysis of genomic data (especially in the field of leukemia) is a major opportunity to revolutionize precision medicine. By implementing AI, healthcare professionals could have more accurate knowledge of genetic dispositions, detect crucial biomarkers and customize treatment programs for each patient. Nevertheless, the broader application of AI in healthcare is accompanied by an increased need for robust cybersecurity infrastructure that can be used to protect the most sensitive genomic data.

This paper discussed several cybersecurity threats relevant to the genomic data analysis process when powered by artificial intelligence (AI) and offered a holistic cybersecurity paradigm for mitigating those risks. The findings highlight the need to mitigate data breaches, adversarial attacks, and the genomic data integrity. Although medical practitioners are generally aware of these risks, many institutions are not ready to take the necessary steps to put them in place.

The findings presented a number of important lessons:

- **Cybersecurity Awareness:** A general awareness of the risks of AI-based genomic data analysis is common, yet most institutions do not have the infrastructure and policies in place to manage these risks successfully.
- **Blockchain Technology:** Blockchain became a favorable choice to ensure the integrity and transparency of genomic data analysis. The technology is effective in averting tampering with sensitive data, despite issues associated with scalability and regulatory compliance.
- **Access Control and Anomaly Detection:** Lack of access control mechanisms such as role-based access control (RBAC) and attribute-based access control (ABAC) poses a real threat for unauthorized access to genomic data. AI algorithms can be used to identify anomalies and detect potential breaches before it is too late and provide real-time controls to address the anomaly.
- **Efficiency of an Enhanced Cybersecurity:** Framework Implementation of a comprehensive cybersecurity model comprising encryption, access control, anomaly detection, and blockchain proved to be very efficient in deterring breaches and maintaining the integrity of genomic data.

Despite the many advantages of using such a framework, cost, scalability and regulatory compliance pose significant barriers to its general adoption. To effectively integrate these technologies, healthcare organizations need to make strategic investments in infrastructure, staff training, and ongoing maintenance. Overcoming these hurdles and ensuring the success of genomic data analysis through AI in healthcare requires collaboration between the IT professionals, clinical providers, and regulatory bodies.

The creation of information and communication technology (ICT) driven genomic data systems should be a technological and an ethical imperative. Protecting patient privacy and ensuring the integrity of genomic data need to be paramount to realize the full potential of AI for improving the diagnosis, treatment and outcomes of patients with leukemia. The joining of advanced cybersecurity methods and cutting-edge technologies, such as the blockchain, will allow healthcare organizations to create a secure and reliable platform for the future of precision medicine.

## Compliance with ethical standards

### *Disclosure of conflict of interest*

No conflict of interest to be disclosed.

## References

[1] Akingbola, A., Adegbesan, A., Ojo, O., Otumara, J. U., & Alao, U. H. (2024). Artificial intelligence and cancer care in Africa. Journal of Medicine, Surgery, and Public Health, 3, 100132. https://doi.org/10.1016/j.glmedi.2024.100132

[2] Ferrag, M. A., Tihanyi, N., & Debbah, M. (2025). From LLM reasoning to autonomous AI agents: A comprehensive review. arXiv preprint arXiv:2504.19678. https://doi.org/10.48550/arXiv.2504.19678

[3] Garcia, C. A., Reed, K. A., Lantz, E., Day, P., Zarella, M. D., Hart, S. N., ... & McClintock, D. S. (2025). Establishing a comprehensive artificial intelligence lifecycle framework for laboratory medicine and pathology: A series introduction. American Journal of Clinical Pathology, 164(3), 424-437. https://doi.org/10.1093/ajcp/aqaf069

[4] Gana, D., & Jamil, F. (2025). DAG-based swarm learning approach in healthcare: A survey. IEEE Access. https://doi.org/10.1109/ACCESS.2025.3531216

[5] Goyal, N. K., Dandotiya, M., Qurashi, J. A., Kumari, M., & Sharma, S. (2025). AI-driven predictive analytics for disease management. In Utilizing AI of Medical Things for Healthcare Security and Sustainability (pp. 231-276). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-0690-2.ch008

[6] Katsoulakis, E., Wang, Q., Wu, H., Shahriyari, L., Fletcher, R., Liu, J., ... & Deng, J. (2024). Digital twins for health: A scoping review. NPJ Digital Medicine, 7(1), 77. https://doi.org/10.1038/s41746-024-01073-0

[7] Khera, R., Asnani, A. H., Krive, J., Addison, D., Zhu, H., Vasbinder, A., ... & Okwuosa, T. M. (2025). Artificial intelligence to enhance precision medicine in cardio-oncology: A scientific statement from the American Heart Association. Circulation: Genomic and Precision Medicine, 18(2), e000097. https://doi.org/10.1161/HCG.0000000000000009

[8] Lee, D., & Yoon, S. N. (2021). Application of artificial intelligence-based technologies in the healthcare industry: Opportunities and challenges. International Journal of Environmental Research and Public Health, 18(1), 271. https://doi.org/10.3390/ijerph18010271

[9] Neoaz, N., & Amin, M. H. (2025). From computational models to clinical impact: The influence of AI on modern healthcare. Global Trends in Science and Technology, 1(2), 23-48. https://doi.org/10.70445/gtst.1.2.2025.23-48

[10] Panahi, O. (2025). Navigating the AI landscape in healthcare and public health. Mathews Journal of Nursing and Health Care, 7(1), 1-8. https://doi.org/10.30654/MJNH.100056

[11] Panahi, O. (2025). Secure IoT for healthcare. European Journal of Innovative Studies and Sustainability, 1(1), 17-23. https://doi.org/10.59324/ejiss.2025.1(1).03

[12] Poovathanathil, S. A., Barage, S. H., & Singh, R. (2025). AI-driven precision medicine and personalized healthcare for immunological disorders. In AI-Assisted Computational Approaches for Immunological Disorders (pp. 205-234). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-9725-1.ch007

[13] Prethija, G., Kalyanasundaram, V., Baabu, K. Y. S., & Keerthi, A. J. (2025). Integrating artificial intelligence into healthcare workflows. In Deep Learning in Medical Signal and Image Processing (pp. 431-460). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-9816-6.ch017

[14] Renugadevi, R., Kumar, P. R., Kalaiarasi, G., Raj, A. A. E., Settu, S., & Ruthravarshini, R. (2024). Enhancing healthcare decision support systems with advanced analytics and machine learning techniques. In Cybersecurity and Data Management Innovations for Revolutionizing Healthcare (pp. 51-80). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-7457-3.ch003

[15] Srivastav, A. K., Singh, A., Singh, S., Rivers, B., Lillard Jr, J. W., & Singh, R. (2025). Revolutionizing oncology through AI: Addressing cancer disparities by improving screening, treatment, and survival outcomes via integration of social determinants of health. Cancers, 17(17), 2866. https://doi.org/10.3390/cancers17172866

[16] Sulaiman, I. M. (Ed.). (2024). Recent advancements in the diagnosis of human disease. CRC Press.

[17] Weerasinghe, D., Pathirana, T., Jayasuriya, M., & Warnakulasooriya, R. (2021). Personalized medicine through AI-based genomic analysis. International Journal of Modern Computing, 6(1), 27-40.

[18] Xu, Y., Liu, X., Cao, X., Huang, C., Liu, E., Qian, S., ... & Zhang, J. (2021). Artificial intelligence: A powerful paradigm for scientific research. The Innovation, 2(4). https://doi.org/10.1016/j.xinn.2021.100179

[19] Kumar, A., & Metta, D. S. (2024). AI-driven precision oncology: Predictive biomarker discovery and personalized treatment optimization using genomic data. Int J Adv Res Publ Rev, 1(3), 21-38.

[20] Gupta, Y. D., & Bhandary, S. (2024). Artificial intelligence for understanding mechanisms of antimicrobial resistance and antimicrobial discovery: A new age model for translational research. In Artificial Intelligence and Machine Learning in Drug Design and Development (pp. 117-156). Wiley. https://doi.org/10.1002/9781394234196.ch5

[21] Cammarota, G., Ianiro, G., Ahern, A., Carbone, C., Temko, A., Claesson, M. J., ... & Tortora, G. (2020). Gut microbiome, big data and machine learning to promote precision medicine for cancer. Nature Reviews Gastroenterology & Hepatology, 17(10), 635-648. https://doi.org/10.1038/s41575-020-0327-3

[22] Ferrag, M. A., Tihanyi, N., & Debbah, M. (2025). From LLM reasoning to autonomous AI agents: A comprehensive review. arXiv preprint arXiv:2504.19678. https://doi.org/10.48550/arXiv.2504.19678

[23] Khera, R., Asnani, A. H., Krive, J., Addison, D., Zhu, H., Vasbinder, A., ... & Okwuosa, T. M. (2025). Artificial intelligence to enhance precision medicine in cardio-oncology: A scientific statement from the American Heart Association. Circulation: Genomic and Precision Medicine, 18(2), e000097. https://doi.org/10.1161/HCG.000000000000009

[24] Sai, S., Chamola, V., Choo, K. K. R., Sikdar, B., & Rodrigues, J. J. (2022). Confluence of blockchain and artificial intelligence technologies for secure and scalable healthcare solutions: A review. IEEE Internet of Things Journal, 10(7), 5873-5897. https://doi.org/10.1109/JIOT.2022.3232793

[25] Panahi, O. (2025). Navigating the AI landscape in healthcare and public health. Mathews Journal of Nursing and Health Care, 7(1), 1-8. https://doi.org/10.30654/MJNH.100056

[26] Gupta, Y. D., & Bhandary, S. (2024). Artificial intelligence for understanding mechanisms of antimicrobial resistance and antimicrobial discovery: A new age model for translational research. Artificial Intelligence and Machine Learning in Drug Design and Development, 117-156. https://doi.org/10.1002/9781394234196.ch5

[27] Podder, S., Gupta, V. R., Khator, S., Koley, R., & Goswami, S. R. (2025). Fusion of blockchain and artificial intelligence of things in e-healthcare. In AIoT (pp. 57-98). Auerbach Publications.

[28] Pasham, S. D. (2023). Enhancing cancer management and drug discovery with the use of AI and ML: A comprehensive review. International Journal of Modern Computing, 6(1), 27-40.

[29] Imoize, A. L., Balas, V. E., Solanki, V. K., Lee, C. C., & Obaidat, M. S. (Eds.). (2023). Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things (pp. 1-460). CRC Press.

[30] Tyagi, E., Kumari, P., Prakash, A., & Bhuyan, R. (2025). Revolutionizing anti-cancer drug discovery: The role of artificial intelligence. International Journal of Bioinformatics and Intelligent Computing, 4(1).

[31] Lara, J. (2024). AI-powered laboratory diagnostics technology. In Recent Advancements in the Diagnosis of Human *Disease* (pp. 1-45). CRC Press.

[32] Khera, R., Asnani, A. H., Krive, J., Addison, D., Zhu, H., Vasbinder, A., ... & Okwuosa, T. M. (2025). Artificial intelligence to enhance precision medicine in cardio-oncology: A scientific statement from the American Heart Association. *Circulation: Genomic and Precision Medicine, 18*(2), e000097.

[33] SOUMYA, M. A. A. K. (2024). AI-driven insights: Revolutionizing health diagnostics and treatment. *BUDHA PUBLICATION.*

[34] Sulaiman, I. M. (Ed.). (2024). *Recent Advancements in the Diagnosis of Human Disease*. CRC Press.

[35] Pentyala, D. K. (2023). Medical applications of machine learning and AI: A need or an opportunity? *International Journal of Acta Informatica, 2*(1), 65-78.