SAVONIA
University of Applied Sciences

THESIS – BACHELOR'S DEGREE PROGRAMME
TECHNOLOGY, COMMUNICATION AND TRANSPORT

ADVANCED METHODOLOGIES FOR TECHNOLOGICAL IMPLEMENTATION FOR ETHICAL CONSIDERATIONS IN AI POWERED HEALTHCARE SYSTEMS

AUTHOR/S Maham Akhlaq

SAVONIA UNIVERSITY OF APPLIED SCIENCES THESIS
Abstract

Field of Study Technology, Communication and Transport	
Degree Programme Degree Programme in Information Technology, Internet of Things	
Author(s) Maham Akhlaq	
Title of Thesis Advanced methodologies for technological implementation for ethical considerations in AI Powered Healthcare Systems	
Date 27 April 2024	Pages/Number of appendices 36
Client Organisation /Partners	

Abstract

This thesis examined the integration of artificial intelligence (AI) into healthcare systems, focusing on its role, ethical considerations, model development, challenges, and future implications. It explored how AI revolutionizes disease detection, enhances patient care, streamlines administrative tasks, improves drug discovery, facilitates remote monitoring, and enhances medical imaging interpretation. The critical importance of data in healthcare and the imperative of data privacy were addressed, emphasizing the need for robust security measures and compliance frameworks.

Ethical challenges in AI-powered healthcare systems were discussed, along with regulatory frameworks and privacy laws. The thesis proposed the "PERBE" ethical framework to guide the responsible development of AI-powered healthcare systems. Model development using privacy-preserving techniques such as pseudonymization and encryption was presented, along with implementation and testing outcomes.

Identified limitations and challenges, including data bias in AI models, were discussed, highlighting the necessity for diverse data collection and rigorous analysis practices. Future implications of AI in healthcare were explored, emphasizing robust data processing techniques, fair and unbiased algorithms, regulatory compliance, patient-centric AI, and ethics screening in AI models. The conclusion underscored the importance of addressing ethical considerations to ensure patient-centered, equitable, and responsible use of AI in healthcare.

Keywords

Artifical Intelligence, AI, Ethical Considerations, Privacy, Data Protection, Pseudonymization, Encryption, Ethical Framework, Development of Model, Security Risks, Regulations, Healthcare, AI-powered healthcare systems

CONTENTS

1 INTRODUCTION 6
1.1 Overview 6
1.2 Evolution of AI and Healthcare 6
1.3 Research Objectives and Structure 7
2 LITERATURE REVIEW 8
2.1 Overview of AI in Healthcare 8
2.2 Data Privacy in Healthcare 8
2.3 Security Risks Associated with IoT and AI 9
2.3.1 AI Security Risks 9
2.3.2 IoT Security Risks 9
2.4 Ethical Considerations 10
2.5 Gaps and Challenges 11
3 AI AND DATA IN HEALTHCARE 12
3.1 The Role of AI in Healthcare 12
3.2 The Critical Importance of Data in Healthcare 14
3.3 The Imperative of Data Privacy in Healthcare 15
4 ETHICAL CONSIDERATIONS IN AI POWERED HEALTHCARE SYSTEMS 16
4.1 Ethical Challenges in AI Powered Healthcare Data Processing 16
4.2 Regulatory Frameworks and Privacy Laws 17
4.3 Ethical Framework for AI-Powered Healthcare Systems 17
4.3.1 Introducing the PERBE Ethical Framework 18
4.4 Methods for Ensuring Data Privacy 19
4.4.1 Pseudonymization 19
4.4.2 Encryption 21
4.4.3 Anonymization 22
4.4.4 Comparison Between Pseudonymization and Anonymization 22
5 MODEL DEVELOPMENT FOR AI-POWERED HEALTHCARE SYSTEMS 23
5.1 Privacy-Preserving Techniques Model Framework 23
5.2 Development of Model 1 Using Pseudonymization Method 23
5.3 Development of Model 2 Using Encryption Model 26
5.4 Implementation and Testing 28

5.4.1 Implementation Process 28
5.4.2 Model Testing 29
5.5 Results and Discussion 31
6 CHALLENGES AND LIMITATIONS 31
6.1 Identified Limitations 31
6.2 Data Bias in AI Models 31
7 FUTURE IMPLICATIONS OF AI IN HEALTHCARE 32
8 CONCLUSION 32
REFERENCES 33

LIST OF FIGURES

Figure 1. Evolution of Healthcare 1.0 to 4.0 Systems (Ocident Bongomin) 6
Figure 2. Privacy Challenges in Healthcare (Khalid et al. 2023). 8
Figure 3. The Role of AI in Healthcare (Infosense AI). 12
Figure 4. Overview of the privacy attacks in AI techniques. (Khalid et al. 2023). 14
Figure 5. Report of Data Breaches in Healthcare in 2023 (Source: ENISA Threat Landscape: Health Sector. Fig. 4.). 15
Figure 6. The Proposed Ethical Framework for AI-Powered Healthcare Systems. 18
Figure 7. Original Database (Table 1) (Murray 2024). 20
Figure 8. Pseudonymized Database (Table 2) (Murray 2024). 20
Figure 9. Mapping Database (Table 3) (Murray 2024). 21
Figure 10. Importing the necessary libraries. 23
Figure 11. Defining the function 'pseudonymize_data' 24
Figure 12. Loading the dataset. 24
Figure 13. Pseudonymizing the data. 24
Figure 14. Saving the pseudonymized data to a new CSV file. 25
Figure 15. Prints a message indicating completion of the process. 25
Figure 16. Importing the necessary libraries for encryption. 26
Figure 17. Defining the 'encrypt_data' function. 27
Figure 18. Defining the 'decrypt_data' function. 27
Figure 19. Define the 'main' function. 27
Figure 20. Run the main function if the script is executed. 28
Figure 21. The original dataset used for pseudonymization (Kaggle.com 2024). 29
Figure 22. The pseudonymized dataset after running the code. 29

Figure 23. Entering the user input and storing it in the database. 30

Figure 24. Database after the data being stored in encrypted form. 30

1 INTRODUCTION

1.1 Overview

The term artificial intelligence (AI) describes the ability of a software or machine to simulate intelligent human behavior such as instantly solving problems, doing calculations, and evaluating new data based on previously evaluated data. The evolution of AI and its tools and services are at a rapid speed. AI plays a significant role in various industries and sectors, such as manufacturing, agriculture, production, autonomous vehicles, finance, sports, healthcare, medical systems, and many more. The industries are confident about the potential of AI as they are already witnessing the benefits of this technology in their work (Farhud & Zokaei 2021). This technology is like a "Trojan horse". Although it has a lot of beneficial impacts, it also carries hidden threats or dangers that demand attention and proactive management. This thesis explores the advanced methodologies for technology implementation for ethical considerations in AI-powered healthcare systems.

1.2 Evolution of AI and Healthcare

AI is revolutionizing various industries such as healthcare, finance, production, education, manufacturing, transportation and many more. The impact of AI will only increase with time. AI in research, analyzing large datasets to find patterns that humans might miss, is leading to discoveries in many different fields. AI in education, AI powered tutoring systems are enhancing learning outcomes (Bodra 2022). In healthcare, AI assists in diagnostics and personalized treatments plans. It is essential to ensure responsible development which benefits all as the AI continues to evolve.

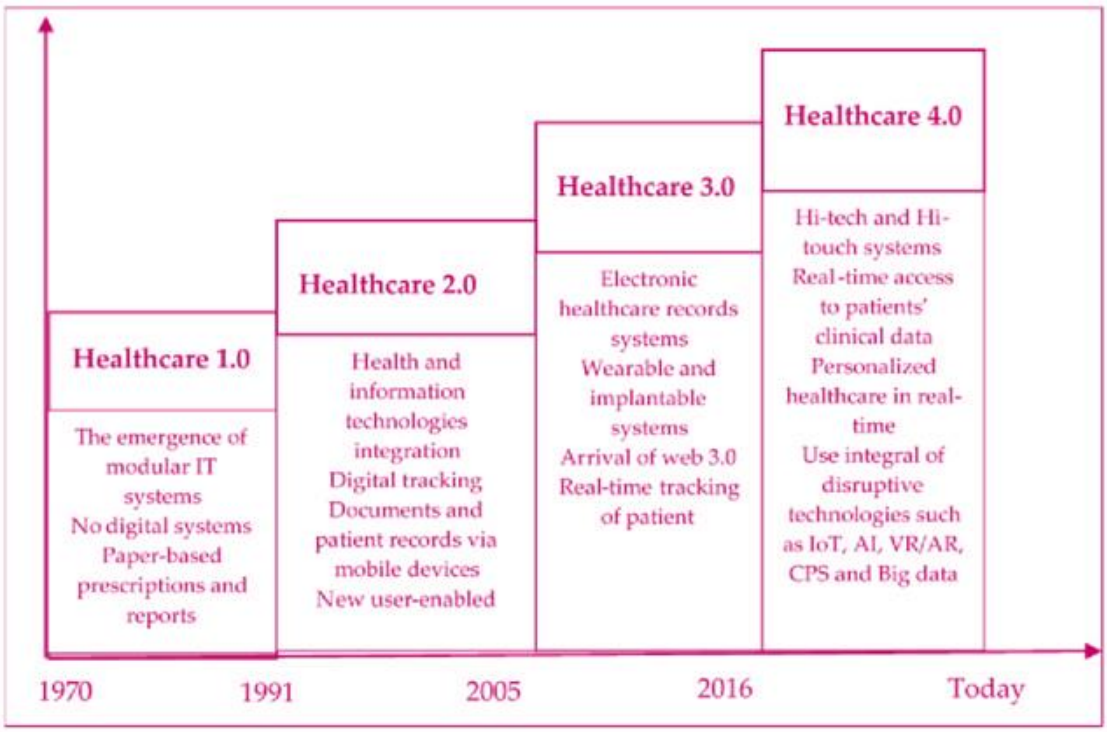


Figure 1. Evolution of Healthcare 1.0 to 4.0 Systems (Ocident Bongomin)

Figure 1 illustrates the evolution of healthcare from a physician-centric model in Healthcare 1.0 to the highly digitized and proactive system of Healthcare 4.0. Over the years, the industry has integrated electronic health records, personalized care through genomics, and advanced technologies like AI and

predictive analytics, transforming patient care and participation. In recent decades, technological advancements like AI have significantly improved the health sector. AI, a branch of computer science focused on creating intelligent machines that mimic human behavior, has revolutionized various healthcare processes. It enhances the personalization and accuracy of diagnoses, enables effective treatments, and provides quick responses during emergencies. AI technology can perform significant tasks such as surveillance, predictive analytics, consultation, risk assessments (e.g., predicting heart disease or injuries), and automated image diagnosis (Zuhair et al., 2024). The digital transformation of healthcare facilities and procedures has been a major driver of AI's growth in the industry.

1.3 Research Objectives and Structure

As healthcare systems navigate this technological transformation, a balanced approach that prioritizes both scientific advancement and ethical principles is crucial. Ongoing research, interdisciplinary collaboration, and robust governance frameworks are necessary to ensure that AI-powered healthcare systems are deployed in a responsible, equitable, and patient-centric manner. However, ethical concerns around data privacy, algorithmic bias, and health disparities must be addressed (Wiens et al., 2019).

The thesis aims to investigate how AI-powered healthcare systems can be developed and implemented while incorporating strong IT security measures and ethical design principles.

To explore the evolution and current applications of AI in the healthcare sector.
To examine the critical role of data in healthcare and the importance of ensuring data privacy.
To identify and analyze the ethical considerations involved in processing healthcare data.
To develop and evaluate AI models tailored for healthcare applications.
To identify and discuss the challenges and limitations associated with AI in healthcare, including data bias.
To speculate on future implications and potential developments of AI in the healthcare industry.

2 LITERATURE REVIEW

2.1 Overview of AI in Healthcare

The integration of Artificial Intelligence (AI) in healthcare marks a significant shift, revolutionizing diagnostic procedures, clinical decision-making, and patient care practices. AI technologies are reshaping medical fields by improving disease detection accuracy, optimizing treatment plans, and facilitating personalized medicine through the analysis of extensive datasets with unparalleled speed and precision. Furthermore, AI-driven surgical systems enhance procedural precision, mitigating risks and enhancing patient outcomes (Yadav et al. 2023). AI has the potential to revolutionize healthcare delivery and improve population health outcomes. As it develops, this suggests a paradigm shift towards data-centric, patient-centered, or human-centric system.

2.2 Data Privacy in Healthcare

The digitization of healthcare and AI integration raises pressing concerns about data privacy. Securing patient information is crucial amidst risks like data breaches and unauthorized access. Robust privacy measures, compliance protocols, and ethical considerations are essential to maintain patient confidentiality and trust in healthcare systems (Yadav et al. 2023). Advanced data analytics in healthcare presents significant privacy risks, including data breaches, re-identification, and unauthorized access to sensitive medical records. Balancing innovation with robust privacy measures is essential to maintain patient trust and comply with regulatory requirements. (Ethical Considerations in Healthcare Data Analysis and Privacy 2024)

Figure 2. Privacy Challenges in Healthcare (Khalid et al. 2023).

In Figure 2, it highlights privacy challenges in healthcare: robustness, ethics, privacy vs. utility, security, legibility, scalability, adaptability, confidentiality, and integrity. These challenges encompass

system resilience, responsible data use, protecting and utilizing data effectively, ensuring clarity, handling growth, evolving with needs, and maintaining accurate, confidential patient information.

2.3 Security Risks Associated with IoT and AI

In today's increasingly interconnected digital world, data privacy and security have become critical issues for individuals, organizations, and governments (Fayayola et al. 2024). "In 2019 alone, over 41 million patient records were compromised, leading to severe financial and reputational consequences for healthcare organizations." (Moldstud 2019). This section explores the security risks associated with the Internet of Things (IoT) and artificial intelligence (AI):

2.3.1 AI Security Risks

Data Privacy: AI systems require large datasets for training and decision-making. Protecting data privacy during collection, storage, and processing is essential.

Bias and Fairness: AI algorithms can unintentionally perpetuate biases if trained on biased data, leading to unfair and discriminatory outcomes.

Adversarial Attacks: AI models can be deceived by adversarial inputs, compromising their integrity.

Model Poisoning: Malicious actors may tamper with training data to introduce vulnerabilities or biases into AI models.

Explainability: The lack of transparency in AI decision-making processes can undermine trust and make it difficult to identify security issues. (Fayayola et al. 2024)

2.3.2 IoT Security Risks

Device Vulnerabilities: Many IoT devices lack robust security features, making them vulnerable to cyberattacks. Attackers can exploit these weaknesses to launch distributed denial-of-service (DDoS) attacks, gather sensitive information or gain unauthorized network access.

Lack of Updates: Many IoT devices do not receive regular security updates, leaving them exposed to known security flaws.

Insecure Communication: The absence or weakness of encryption during data transmission can result in the exposure of sensitive data.

Physical Attacks: Physical access to IoT devices can lead to unauthorized data access or manipulation. (Fayayola et al. 2024)

2.4 Ethical Considerations

This chapter outlines the major ethical concerns in AI-powered Healthcare Systems:

Table 1. Common Ethical Concerns in AI Powered Health Systems

Ethical Concerns	Description
Privacy	In artificial intelligence (AI) powered Healthcare systems, "privacy" refers to keeping personal data safe from being misused, illegally accessed, and breaches of private information. Assuring that confidentiality, integrity, and accessibility are maintained. (ARThink AI 2024)
Transparency	Transparency in AI powered healthcare systems is essential and crucial for ethical considerations. Due to their complexity, it's often hard to explain AI decisions to doctors and patients, which can affect trust. Patients need to know why an AI suggests a certain treatment or diagnosis, and healthcare professionals must understand these decisions to make informed choices. Clear explanations and disclosure of AI limitations are necessary to ensure AI in healthcare is practical and trustworthy. (Yelne et al. 2023)
Fairness	"Fairness" is a ubiquitous term in artificial intelligence (AI) (Smith 2020). Fairness in AI means that processing personal data should not lead to unjust discrimination. Data Protection Act 2018 focuses on protecting individuals' rights and freedoms, including their right to privacy and non-discrimination. Ensuring fairness is a core aspect of this act, both explicitly and implicitly. (ICO s.a.)
Accountability	Accountability is a fundamental pillar in the regulation of artificial intelligence (AI) (Novelli et al. 2023). Accountability refers to being responsible for or answerable for a system, its behavior, and its impacts, encompassing both legal and moral (ethical) aspects (What is accountability? - Ethics of AI s.a.). Accountability in AI ethics has three components: identifying who is responsible for the impact of AI, the societal systems that develop and use AI, the AI system itself (Novelli et al. 2023).
Bias Mitigation	AI algorithms have the possibility to inherit biases from their training data which impacts diagnosis, treatment, and patient care and results in discriminatory decisions. To prevent or minimize biased decisions, healthcare organizations must use unbiased training data, and the AI developers should implement bias detection and mitigation mechanisms into the systems. (Yelne et al. 2023)

Table 1 summarizes the key ethical concerns in AI-powered healthcare systems: privacy, transparency, fairness, accountability, and bias mitigation. Privacy protects personal data, while transparency builds trust through clear explanations of AI decisions. Fairness prevents unjust discrimination, aligned with the Data Protection Act 2018. Accountability ensures responsibility for AI's behavior and impacts, and bias mitigation addresses the need for unbiased data and detection mechanisms to prevent discriminatory practices.

2.5 Gaps and Challenges

Healthcare organizations encounter significant challenges in complying with privacy regulations, which necessitate a delicate balance between data accessibility and patient information protection. Adhering to stringent data protection standards is essential to avoid severe penalties and sustain trust (Fayayola et al. 2024). Data anonymization is vital for protecting patient privacy while enabling data analytics. It preserves privacy, encourages data sharing, facilitates ethical research, and reduces breach risks. However, maintaining data utility while anonymizing poses a significant challenge (Ethical Considerations in Healthcare Data Analysis and Privacy 2024).

In Danese & Jindal's research, it has been discovered that integrating AI into healthcare presents several key gaps and challenges: AI systems require greater transparency and specificity to achieve reliable accuracy. Robust and practical regulatory frameworks are needed to address AI complexities. Efforts to correct algorithms biases are crucial for promoting fairness and inclusivity in AI applications. Additionally, industry-wide collaboration and standardization are essential for ensuring seamless co-operation among diverse AI systems and mitigation real-time risks. (Danese & Jindal 2024)

In another study, it has been discussed that integrating AI into healthcare faces several gaps and challenges. Bias can arise in AI life cycle stages like data collection and model development, exacerbating health disparities (Chen et al. 2023). Ethical considerations such as data privacy, security, and appropriate AI decision-making are crucial. Additionally, implementation challenges include overfitting, feedback loops, human errors, and model interpretability. Addressing these issues is essential for effective AI integration in healthcare.

It is necessary to address the complexity of ensuring regulatory compliance and the safety of AI-driven medical devices while fostering innovation. Emphasizing collaboration among regulatory authorities, industry stakeholders, and healthcare enterprises, it stresses the need for clear guidelines and standards to ensure transparency and efficacy in healthcare AI implementation (Etzel 2024). Patient consent is crucial for ethical data sharing, ensuring individuals have control over their medical information. Challenges include complex consent forms, difficulty in tracking consent, and ensuring easy revocation of consent, which require streamlined management systems (Ethical Considerations in Healthcare Data Analysis and Privacy 2024).

3 AI AND DATA IN HEALTHCARE

3.1 The Role of AI in Healthcare

The integration of artificial intelligence (AI) into healthcare systems has significantly increased over the past decades. AI is revolutionizing healthcare by enhancing various processes and improving efficiency, accuracy, and patient outcomes. This technology is being utilized in numerous ways, including:

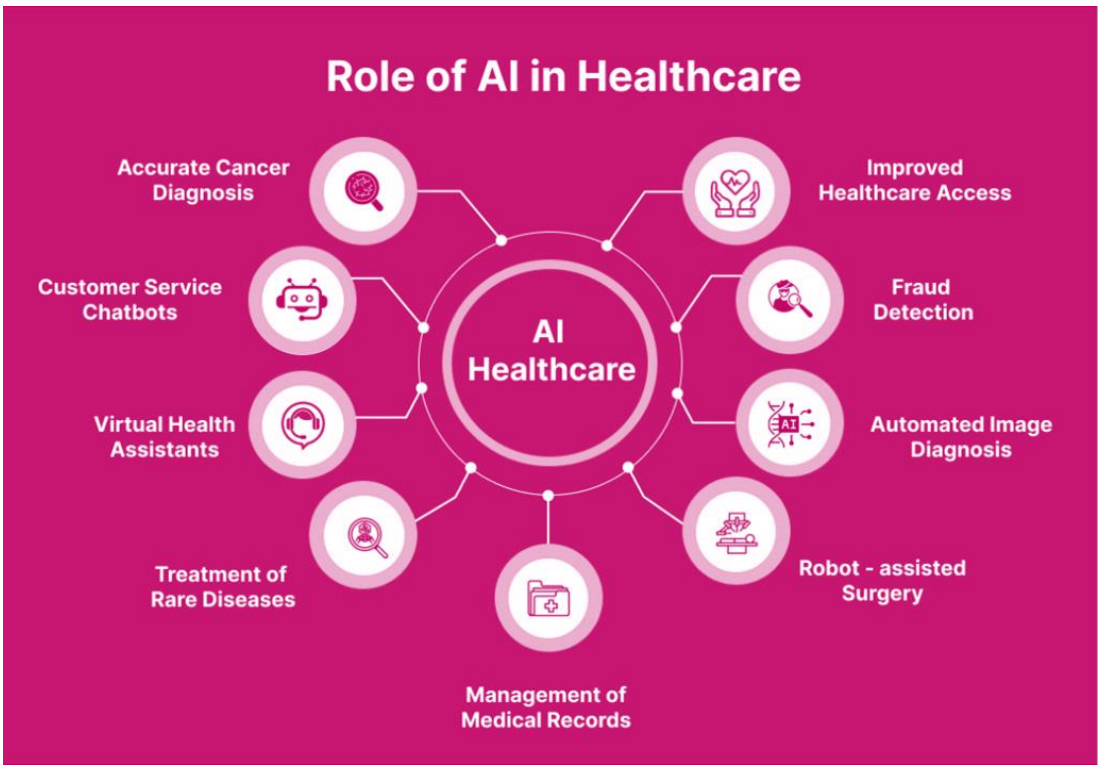


Figure 3. The Role of AI in Healthcare (Infosense AI).

In Figure 3, various roles of AI in healthcare are depicted, including improved healthcare access, fraud detection, automated image diagnosis, robot-assisted surgery, management of medical records, treatment of rare diseases, virtual health assistants, customer service chatbots, and accurate cancer diagnosis. These applications demonstrate AI's vast potential in transforming healthcare processes, enhancing patient care, and improving outcomes across different areas of the healthcare system.

1. Revolutionizing Disease Detection: The way diseases are analyzed, detected, diagnosed, and treated has been revolutionized through AI-powered healthcare tools. AI-powered diagnostic tools have improved the accuracy of analyzing the data and images for early diagnostic of the disease. It is not just assisting in diagnosis but also minimized the misdiagnosis for improved treatment efficacy. (Stephenson 2021)
2. Enhancing Patient Care and Personalized Medicine: AI-driven advancements revolutionize patient care and personalized medicine in healthcare systems. By analyzing extensive patient data, AI tailors' treatment plans for individuals, improving outcomes and chronic condition management. This personalized approach enhances patient care and treatment efficacy. AI's evolution promises to transform healthcare delivery, leading to better outcomes and efficiency. (Mathur & Sutton 2017)

3. Streamlining Administrative Tasks: Efficient healthcare administration is crucial for quality patient care, particularly with AI's evolving role. Utilizing AI-driven strategies like virtual receptionists, EHR systems, automated scheduling, telehealth, optimized revenue cycles, centralized communication, and outsourcing non-core functions enhances efficiency. These measures bolster patient satisfaction, minimize errors, and ensure compliance, empowering healthcare organizations to prioritize delivering superior care while navigating the dynamic landscape of AI-driven healthcare technologies. (Paulsen & Paulsen 2024)
4. Improving Drug Discovery and Development: AI involves harnessing vast data to accelerate processes and optimize outcomes. While AI holds promise in rationalizing early phases, predicting properties, and personalizing treatments, its efficacy relies on data quality and understanding biological complexities. Despite advancements, AI's integration into R&D remains in its infancy, requiring rigorous validation and a critical scientific approach to ensure meaningful results. (Singh et al. 2023)
5. Facilitating Remote Monitoring and Telemedicine: AI in healthcare has evolved to support telemedicine and remote monitoring with self-intelligent devices that autonomously acquire and process data. These advancements improve patient self-care and enable timely medical interventions by physicians. The integration of AI-driven, interoperable systems enhances efficiency, reduces costs, and increases the effectiveness of remote health monitoring and management. (Volterrani & Sposato 2019)
6. Enhancing Medical Imaging and Interpretation: The evolution of AI in healthcare has significantly enhanced medical imaging and interpretation. AI, particularly deep learning, improves early disease detection, accurate diagnosis, and personalized treatment planning by analyzing complex patterns in medical images (Pinto-Coelho 2023). Emerging AI-powered diagnostics and personalized medicine highlight the future potential and transformative impact of AI in healthcare visualization.

3.2 The Critical Importance of Data in Healthcare

Data collection and analysis in healthcare are indispensable for making informed decisions about patient care. As the sheer volume of data produced globally underscores the need for effective data management to improve healthcare outcomes (Smile Foundation 2023). Accurate and timely patient data, facilitated by technologies like Electronic Health Records (EHRs) and Electronic Medical Records (EMRs), enable healthcare providers to make precise diagnoses and devise effective treatment plans. The integration of AI further enhances these capabilities by quickly processing large datasets to identify patterns and provide clinical decision support, ultimately reducing errors and improving patient outcomes (Importance of Data Collection in Healthcare | ForeSee Medical s.a.). This seamless access to comprehensive patient data ensures that every member of the healthcare team is well-informed, fostering better coordination and more personalized patient care.

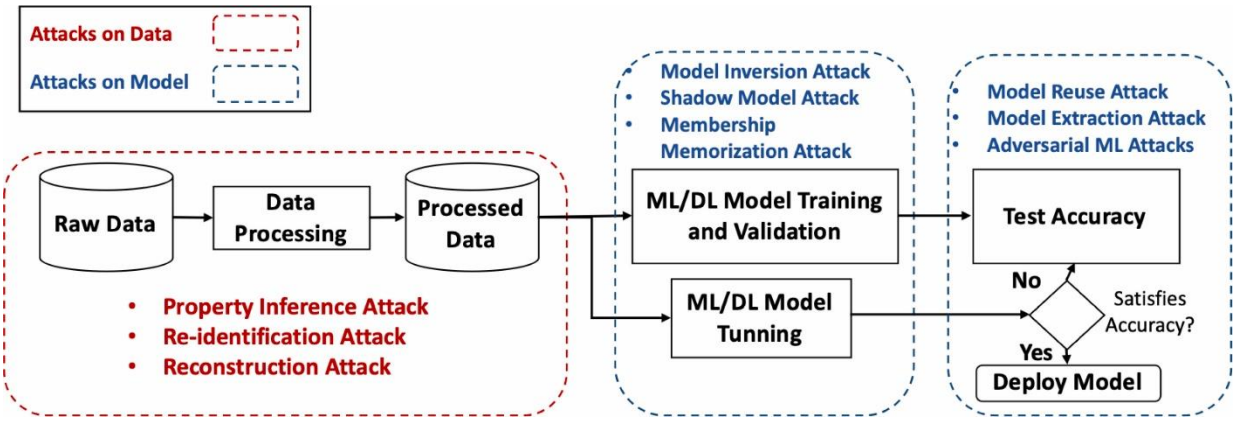


Figure 4. Overview of the privacy attacks in AI techniques. (Khalid et al. 2023).

The figure 4, illustrates the flow from raw data to model deployment in AI systems. It highlights privacy attacks occurring at various stages: Property Inference, Re-identification, and Reconstruction Attacks during data processing; Model Inversion, Shadow Mode, and Membership Memorization Attacks during Model Training and Tuning; and Model Reuse, Model Extraction, and Adversarial ML Attacks during testing and deployment. Attacks on data are denoted in red, while attacks on the model are shown in blue.

By ensuring that accurate data is readily available, healthcare systems can prevent epidemics and respond swiftly to public health challenges, further underscoring the critical importance of robust data management practices in the healthcare industry (Smile Foundation, 2023). Furthermore, the transition from traditional paper-based records to modern database systems has accelerated the accessibility and exchange of patient information, enabling seamless collaboration among healthcare professionals. This transformation not only streamlines administrative processes but also ensures that vital medical information is readily accessible, facilitating comprehensive treatment planning and improving patient outcomes. Failure to share patient data across healthcare entities can impede medical progress and compromise patient safety, highlighting the importance of interoperable data systems in advancing healthcare delivery and innovation (Importance of Data Collection in Healthcare | ForeSee Medical, n.d.). Preserving the data privacy while processing the data which go through different channels in AI-powered healthcare systems is challenging, but it is essential to maintain.

3.3 The Imperative of Data Privacy in Healthcare

Data privacy in AI healthcare is pivotal to maintaining patient trust, complying with regulations, and securing sensitive medical information. Embracing robust security measures and stringent compliance frameworks is imperative for the seamless integration of AI in healthcare while prioritizing patient privacy. (ARThink AI 2024)

With AI applications ranging from imaging and electronic medical records to laboratory diagnosis and treatment, the demand for data processing has surged. However, this increased reliance on AI technologies for data analysis and decision-making poses significant challenges to data security and privacy. As AI systems analyze vast amounts of personal health information, the risk of data breaches and privacy violations escalates. Strengthening data protection measures is crucial to mitigate these risks and uphold patient confidentiality. Moreover, the imperative of addressing ethical considerations surrounding AI-driven medical decisions, emphasizing the need to prioritize patient autonomy and consent in data processing practices. In essence, while AI offers immense potential to revolutionize healthcare, ensuring robust data protection mechanisms is essential to navigate the evolving landscape of healthcare data processing responsibly and ethically. (Farhud & Zokaei 2021)

Figure 4: Targets (number of incidents per entity type)

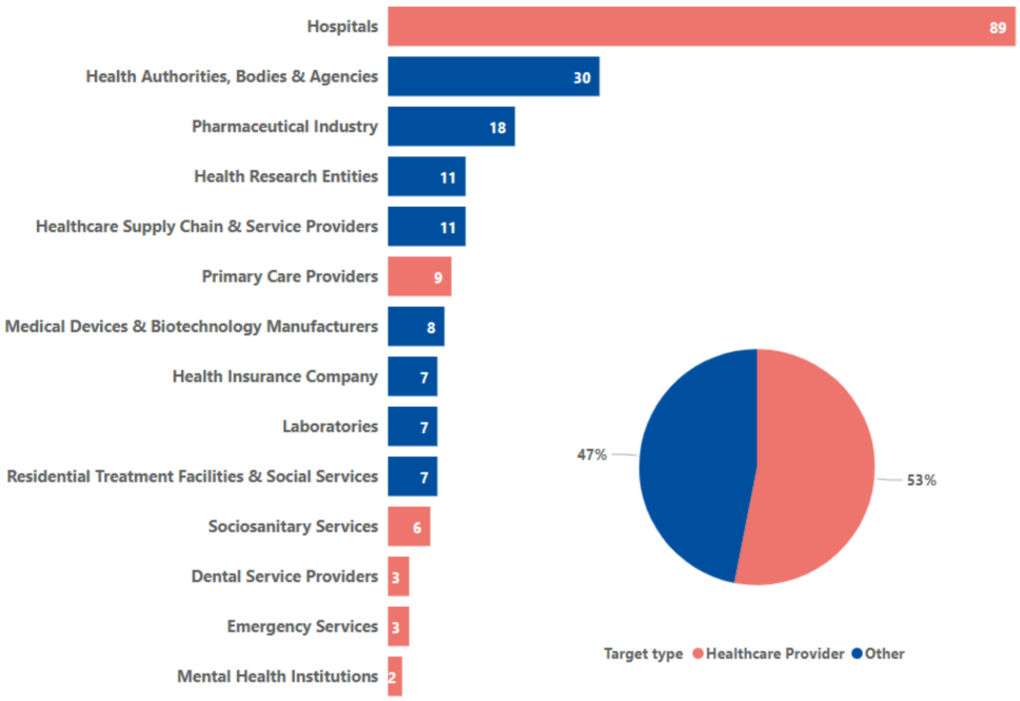


Figure 5. Report of Data Breaches in Healthcare in 2023 (Source: ENISA Threat Landscape: Health Sector. Fig. 4.).

In Figure 5, Mora (2024) states, "The European Union Agency for Cybersecurity (ENISA) conducted a report documenting all cybersecurity incidents reported at the start of 2023. Of these incidents, 53% were aimed at healthcare providers, with hospitals being the main target of attacks."

4 ETHICAL CONSIDERATIONS IN AI POWERED HEALTHCARE SYSTEMS

4.1 Ethical Challenges in AI Powered Healthcare Data Processing

Addressing the ethical challenges, risks, and potential solutions in AI healthcare is essential. Let's explore the complexities of bias, privacy concerns, and confidentiality in AI systems. By examining each issue, we aim to provide a comprehensive understanding and propose ideal solutions for navigating these ethical challenges.

Table 2. Addressing ethical issues, risks, and potential solutions.

Ethical Issues	Description
Privacy and Confidentiality	AI systems in healthcare handle vast amounts of sensitive patient data. Ensuring the privacy and confidentiality of this data is paramount. There is a risk of data breaches and unauthorized access, which can lead to misuse of personal health information. Strong data protection measures, including encryption and strict access controls, are essential to secure patient privacy (Yadav et al. 2023).
Bias and Fairness	Algorithms can unintentionally replicate or even amplify existing biases in the data they are trained on which leads to differences in healthcare outcomes among various demographic groups. Ensuring fairness involves rigorous testing of AI systems for biases, using diverse datasets for training, and implementing mechanisms to identify and mitigate bias in AI decision-making processes (Danese & Jindal 2024).
Informed Consent	Patients should be informed about the use of AI in their care and should provide consent for their data to be used. This involves transparent communication about what the AI system does, the benefits and risks involved, and how their data will be protected and utilized (Ethical Considerations in Healthcare Data Analysis and Privacy 2024).

Table 2 summarizes key ethical issues in AI-powered healthcare data processing: privacy and confidentiality, bias and fairness, and informed consent. Privacy concerns emphasize the importance of robust data protection measures, while addressing bias and ensuring fairness requires rigorous testing and diverse datasets. Informed consent underscores the need for transparent communication with patients regarding the use of AI in their care.

By proactively addressing these ethical challenges, healthcare organizations can uphold patient trust, ensure equitable access to care, and safeguard sensitive health information.

4.2 Regulatory Frameworks and Privacy Laws

There are various regulatory frameworks and privacy laws, such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA). These laws aim to secure individuals' health data and ensure privacy protections in the face of evolving technologies like AI and data analytics. (Shachar et al. 2020)

Table 3. The Laws and Acts which address ethical concerns.

Ethical Concerns	Laws & Acts
Privacy	• General Data Protection Regulation (GDPR) [2018, EU] • California Consumer Privacy Act (CCPA) [2020, USA]
Transparency	• General Data Protection Regulation (GDPR) [2018, EU] • EU AI Act [EU]
Fairness	• General Data Protection Regulation (GDPR) [2018, EU] • Data Protection Act 2018 [UK]
Accountability	• Algorithmic Accountability Act [USA] • EU AI Act [EU]
Bias Mitigation	• General Data Protection Regulation (GDPR) [2018, EU] • EU AI Act [EU]

Table 3 outlines key ethical concerns in AI-powered healthcare data processing and the corresponding laws and acts addressing them. Privacy laws such as the GDPR and CCPA ensure the protection of individuals' health data, while transparency and fairness are addressed through regulations like the GDPR and the EU AI Act. Accountability is emphasized by acts like the Algorithmic Accountability Act in the USA and the EU AI Act. Bias mitigation is tackled by laws such as the GDPR and the EU AI Act.

By adhering to these regulatory frameworks and privacy laws, healthcare organizations can navigate ethical concerns and ensure the responsible and ethical use of AI in healthcare data processing.

4.3 Ethical Framework for AI-Powered Healthcare Systems

It is essential that ethical issues are addressed and considered for responsible development and deployment of AI in healthcare systems. As AI revolutionizes healthcare through advancements in diagnostics, treatment, and patient management, addressing these ethical considerations is crucial to ensure the technology benefits all while mitigating potential risks (Bohr & Memarzadeh 2020).

Ensuring privacy, transparency, fairness, accountability, and bias mitigation is crucial to leveraging AI's benefits while minimizing risks. To address the significant ethical challenges that come along with the benefits of evolution of AI in healthcare systems, we propose the "PERBE" Ethical Framework.

Figure 6. The Proposed Ethical Framework for AI-Powered Healthcare Systems.

The Proposed Ethical Framework for AI-Powered Healthcare Systems, outlined in Figure 6, offers a structured approach to address ethical challenges in the development and deployment of AI in healthcare, promoting responsible and equitable use of technology for the benefit of patients and society.

4.3.1 Introducing the PERBE Ethical Framework

The proposal of "PERBE", the ethical framework is designed to guide the responsible development, deployment, and use of AI-powered healthcare systems.

P – Privacy-Preserving Techniques

This component focuses on implementing robust measures to protect patient privacy and confidentiality in AI-powered healthcare systems. It involves pseudonymization, encryption, anonymization, and access control mechanisms to ensure that sensitive medical data is securely handled and only accessed by authorized personnel.

E – Ethical AI Design Principles

This component highlights the integration of ethical considerations into the design, development and deployment of AI algorithms and systems in the healthcare sector. It includes principles such as privacy, transparency, accountability, fairness, and inclusivity (unbiased) to ensure that AI technologies are in accordance with ethical standards and promote positive outcomes with patients and stakeholders.

R – Regulatory Compliance Frameworks

This component addresses the need for compliance with relevant regulations and standards set by the authorities for the use of AI in healthcare. It adheres to national and international regulatory standards such as GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and newly adopted The EU AI Act (Formally passed on 13 March 2024). This framework ensures the compliance of legal and ethical handling of patient data and AI systems operations, protecting patient rights and data integrity.

B – Bias Mitigation Strategies

This component focuses on identifying and mitigating biases inherent from data sources into AI algorithms used for healthcare systems. It includes techniques or methods to eliminate or minimize the risk of biased decision-making and promote equity and fairness in healthcare by using data sampling techniques, bias detection, and algorithmic fairness assessments on each possible step of development and deployment.

E – Ethical Decision-Support Systems

This component pertains to the development of AI powered decision-making support systems that prioritize ethical considerations and support healthcare professionals in making decisions that are patient-centered or human-centric and ethically upright. The integrates the ethical guidelines, clinical data, and patient preferences to assist healthcare professionals in navigating complex ethical dilemmas and delivering personalized treatment care.

By implementing these components of this ethical framework, it could be assured that AI-powered healthcare systems uphold principles of privacy, ethics, regulatory compliance, bias mitigation, and support in decision-making, ultimately building trust, and exhibiting transparency.

4.4 Methods for Ensuring Data Privacy

Balancing data utility and privacy is essential. Techniques like differential privacy and federated learning help preserve privacy while deriving insights. To ensure the privacy and protection of data, the implementation of following methods and techniques could be helpful for protecting the data.

4.4.1 Pseudonymization

Pseudonymization is a security technique aimed at securing sensitive data by replacing it with fictional data, as per GDPR guidelines. Its main purpose is to maintain referential integrity and statistical accuracy while facilitating various business processes, development systems, and data analysis. This method finds application in scenarios requiring realistic data, including application development, testing, data warehousing, and analytical data stores. Pseudonymization enhances data security, ensures compliance with regulations, and protects the confidentiality of sensitive information (Pseudonymization 1 B.C.E.). This technique, often used alongside encryption, helps maintain user privacy by masking personal information.

Pseudonymization involves replacing personal identifiable data with artificial identifiers or pseudonyms, maintaining data validity while ensuring the privacy and security of an individual.

Key steps include:

- Identifying personal identifiable information.
- Applying pseudonymization algorithms.
- Securely storing mappings between original data and pseudonyms.

For example, instead of storing a user's name like "Michael" in a database, a streaming service might record it as "PPP 12458." This approach ensures that while the data remains useful for analysis, it is not easily traced back to the individual, thereby protecting their identity.

Let's illustrate some examples of how pseudonymization works in a database.

Patient ID	Name	Address	Diagnosis
1	John Doe	123 Main Street	Hypertension
2	Jane Smith	456 Maple Avenue	Diabetes
3	Sam Lee	789 Elm Drive	Asthma

Figure 7. Original Database (Table 1) (Murray 2024).

Figure 7 illustrates the process of identifying personally identifiable information (PII) fields, such as 'Name' and 'Address,' which necessitate the use of pseudonyms. This step is crucial for securing individuals' privacy and ensuring compliance with data protection regulations.

Patient ID	Name	Address	Diagnosis
1	XH54K1	AD34Z9	Hypertension
2	RG78P2	FG16B7	Diabetes
3	UI23N6	KO89V5	Asthma

Figure 8. Pseudonymized Database (Table 2) (Murray 2024).

Figure 8 displays the Pseudonymized Database (Table 2), as described by Murray in 2024. It demonstrates the application of pseudonymization algorithms on selected fields, replacing original data with pseudonymized forms. This process enhances data privacy and security while retaining the usability of the database for analysis and research purposes.

Pseudonym	Original Data
XH54K1	John Doe
RG78P2	Jane Smith
UI23N6	Sam Lee
AD34Z9	123 Main Street
FG16B7	456 Maple Avenue
KO89V5	789 Elm Drive

Figure 9. Mapping Database (Table 3) (Murray 2024).

Figure 9 showcases the secure storage of mappings between original data and pseudonyms, ensuring data integrity and confidentiality in pseudonymized datasets.

These steps ensure data privacy and the risk of data theft and misuse while also ensuring that the data is beneficial for data processing, health analysis and other purposes.

4.4.2 Encryption

Encryption is a vital tool for securing personal data by converting it into an unreadable format, ensuring compliance with regulations like GDPR and PCI DSS. Encryption algorithms such as AES (Advanced Encryption Standard) and RSA scramble data, making it inaccessible to unauthorized users, even in the event of a data breach. However, effective implementation is crucial, as encryption keys must be carefully managed to prevent loss or theft, and algorithms must be regularly updated to withstand evolving cyber threats. (Rodrigues 2024)

Database encryption employs an algorithm to change readable data into unreadable ciphertext. This process involves a key, also created by the algorithm, which users can use to decrypt and access the original information when necessary. (N-Able 2024)

The types of most secure encryptions:

- **AES:** The Advanced Encryption Standard is a highly secure symmetric algorithm used by various entities, including the U.S. government, utilizing block lengths of 128, 192, or 256 bits.
- **RSA:** Rivest-Shamir-Adleman is an asymmetric algorithm that uses a public key for encryption and a private key for decryption, providing high security with key sizes between 1024 and 2048 bits but at a slower speed.

- **3DES:** Triple Data Encryption Standard uses three 56-bit keys to encrypt data three times, resulting in a 168-bit key, offering reasonable security but is slower and becoming outdated.
- **Twofish:** Twofish is a flexible, license-free symmetric block cipher with key sizes from 128 to 256 bits, featuring 16 encryption rounds and customizable key setup or encryption speed.

For example, instead of storing a user's name like "Michael" in a database, an encryption system might record it as "9f1b2c3d." This ensures that the data is secure and not easily linked back to the individual, thus protecting their identity.

4.4.3 Anonymization

Anonymization and de-identification are techniques used to hide or secure personal information in data. These techniques involve methods of removing or encrypting specific details that could identify individuals, such as names, addresses which prevents individuals from being re-identified, thus securing their privacy (ARThink AI 2024). By implementing these measures, the risk of someone being able to link the data back to a specific person is greatly reduced.

4.4.4 Comparison Between Pseudonymization and Anonymization

When it comes to protecting personal data, two commonly used techniques are pseudonymization and anonymization. Both methods serve to secure sensitive information, but they differ significantly in their approach and effectiveness. The following table (Table 4) compares pseudonymization and anonymization across various criteria, including data protection level, reversibility, linkage to original identities, and GDPR compliance.

Table 4. Comparison of Pseudonymization and Anonymization.

Criteria	Pseudonymization	Anonymization
Data Protection Level	• Moderate	• High
Reversibility	• Reversible	• Irreversible
Linkage to Original Identities	• Reduces linkage but does not eliminate it	• Completely eliminates linkage
GDPR Compliance	• Recommended by GDPR as it still allows data to be linked to individuals	• Not regulated by GDPR since data cannot be traced back to individuals

The choice between pseudonymization and anonymization depends on the specific use case, the sensitivity of the data, and the required level of security and privacy (Murray 2024). Pseudonymization offers moderate protection and compliance with GDPR, while anonymization ensures a higher level of privacy by making re-identification nearly impossible. In the context of medical research, pseudonymization is valuable as it allows for the retention of data linkages necessary for analysis while still protecting individual privacy.

5 MODEL DEVELOPMENT FOR AI-POWERED HEALTHCARE SYSTEMS

5.1 Privacy-Preserving Techniques Model Framework

The proposed model focuses on three primary goals: security, integrity, and processing speed. First, ensuring the security of healthcare data is crucial due to the prevalence of internet attackers seeking to exploit confidential information. In an AI powered healthcare system or can also be called IoT based healthcare systems (Das & Namasudra 2022), data transmission over the internet necessitates robust security measures. Second, maintaining data integrity is vital as any alteration in healthcare data could lead to severe consequences, including patient harm. The use of digital signatures is implemented to uphold data integrity. Third, the efficiency of the healthcare system relies on its processing speed. A system with slow processing times can reduce overall efficiency, so the design aims to achieve high processing speed and low computation time. (Das & Namasudra 2022).

5.2 Development of Model 1 Using Pseudonymization Method

The first model is developed using the pseudonymization method to ensure privacy and security. I am developing a Python script to pseudonymize sensitive data in a healthcare dataset. The script utilizes the hashlib library to hash sensitive columns such as 'Name', 'Doctor', 'Hospital', and 'Room Number'. This process helps protect individual privacy while retaining the usability of the dataset for analysis purposes.

I am using Python, specifically Python 3.11, to implement the pseudonymization process. The script loads the dataset from a CSV file, pseudonymizes the sensitive columns using hashing techniques, and then saves the pseudonymized data to a new CSV file.

This code performs the following tasks:

```
1  import pandas as pd
2  import hashlib
3
```

Figure 10. Importing the necessary libraries.

Figure 10 illustrates the initial step of the pseudonymization process, which involves importing the necessary libraries in Python. The ‘pandas’ (Pandas - Python Data Analysis Library s.a.) library is imported for data manipulation and analysis, while ‘hashlib’ (Hashlib — Secure Hashes and Message Digests s.a.) is imported to utilize cryptographic hashing functions. These libraries provide essential functionality for handling and pseudonymizing sensitive healthcare data in the subsequent steps of the script.

```
5  def pseudonymize_data(data):
6      # Pseudonymize sensitive columns using hashing
7      pseudonymized_data = data.copy()
8      sensitive_columns = ['Name', 'Doctor', 'Hospital', 'Room Number']  # Example sensitive columns
9
10     for column in sensitive_columns:
11         pseudonymized_data[column] = pseudonymized_data[column].apply(lambda x: hashlib.sha256(str(x).encode()).hexdigest())
12
13     return pseudonymized_data
14
```

Figure 11. Defining the function ‘pseudonymize_data’

Figure 11 outlines the process of defining the function ‘pseudonymize_data’ in Python for pseudonymizing sensitive data:

- The function ‘pseudonymize_data’ takes a DataFrame ‘data’ as input, ensuring flexibility in handling different datasets without modifying the original data.
- It creates a copy of the input DataFrame to avoid modifying the original data.
- It defines a list of sensitive columns that need to be pseudonymized.
- For each column in the list, it applies a hashing function (‘sha256’) to each value in the column. The hashing function converts the value to a hash, which is a fixed-size string of characters that appears random.
- The lambda function inside the apply method converts each value to a string, encodes it to bytes, and then hashes it using SHA-256. The resulting hash is stored back in the DataFrame.
- The pseudonymized DataFrame is returned.

```
16  # Load dataset
17  dataset_path = 'Healthcare_Data.csv'
18  data = pd.read_csv(dataset_path)
19
```

Figure 12. Loading the dataset.

Figure 12 illustrates the loading of a dataset into a DataFrame in Python:

The path to the dataset is specified as 'dataset_path', providing the location of the dataset file within the file system.

The 'pd.read_csv' function is used to load the dataset from the specified path into a DataFrame named 'data'. This function is part of the 'pandas' library and is specifically designed to read CSV files and create DataFrame objects from them.

By loading the dataset into a DataFrame, the data becomes structured and accessible for further analysis and manipulation within the Python environment.

```
20  # Pseudonymize data
21  pseudonymized_data = pseudonymize_data(data)
```

Figure 13. Pseudonymizing the data.

Figure 13 describes the process of pseudonymizing the loaded data:

The function 'pseudonymize_data' is invoked with the loaded data DataFrame as the argument, utilizing the pseudonymization function defined earlier.

The pseudonymized DataFrame returned by the 'pseudonymize_data' function is assigned to the variable 'pseudonymized_data', allowing easy access to the pseudonymized dataset for further analysis or storage.

This process ensures that sensitive data within the dataset is pseudonymized, enhancing privacy and security while preserving the integrity of the data for analysis purposes.

```
23  # Save pseudonymized data to a new CSV file
24  output_path = 'pseudonymized_data.csv'
25  pseudonymized_data.to_csv(output_path, index=False)
26
```

Figure 14. Saving the pseudonymized data to a new CSV file.

Figure 14 demonstrates the process of saving the pseudonymized data to a new CSV file:

The path where the pseudonymized dataset will be saved is specified as 'output_path', defining the location and filename of the output CSV file.

The pseudonymized DataFrame, which was previously generated and stored in the variable 'pseudonymized_data', is then saved to a new CSV file using the 'to_csv' method. The parameter 'index=False' is included to exclude the DataFrame index from being saved as a separate column in the CSV file.

By saving the pseudonymized data to a new file, the privacy-enhanced dataset is preserved for future use while ensuring that sensitive information remains protected.

```
26
27  print("Data pseudonymization completed. Pseudonymized dataset saved to:", output_path)
28
```

Figure 15. Prints a message indicating completion of the process.

Figure 15 signifies the final step of the pseudonymization process:

A message is printed to indicate that the pseudonymization process is complete and the pseudonymized dataset has been saved to the specified path.

The main purpose of this code is to protect sensitive information in the dataset by replacing it with hashed pseudonyms, which helps maintain privacy while still allowing analysis.

5.3 Development of Model 2 Using Encryption Model

The second model is developed using an encryption-based approach to enhance data security. I am developing a Python script to encrypt patient data using the AES algorithm and store it in an SQLite database.

Python is being used to write this script. It's a high-level programming language known for its simplicity and readability. The Python version used for this script is Python 3.11.

The script imports necessary libraries from the PyCryptoDome package, including AES cipher for encryption, functions for generating random bytes, and utilities for padding and base64 encoding.

The 'encrypt_data' function encrypts patient information using AES encryption with Cipher Block Chaining (CBC) mode, while 'decrypt_data' decrypts the encrypted data. The main function prompts the user for patient information, encrypts sensitive data, and stores it securely in an SQLite database.

The code follows best practices for data encryption, ensuring patient confidentiality and compliance with data protection regulations.

This code performs the following tasks:

```
1  from Crypto.Cipher import AES
2  from Crypto.Random import get_random_bytes
3  from Crypto.Util.Padding import pad, unpad
4  import sqlite3
5  import base64
6
```

Figure 16. Importing the necessary libraries for encryption.

'Crypto.Cipher' (Crypto.Cipher Package — PyCryptodome 3.210b0 Documentation s.a.),

'Crypto.Random' (Crypto.Random Package — PyCryptodome 3.210b0 Documentation s.a.),

'Crypto.Util.Padding' (Crypto.Util Package — PyCryptodome 3.210b0 Documentation s.a.),

'sqlite3' (Sqlite3 — DB-API 2.0 Interface for SQLite Databases s.a.),

and 'base64' (Base64 — Base16, Base32, Base64, Base85 Data Encodings n.d.) are imported for encryption, padding, database operations, and encoding.

By importing these libraries (Figure 16), the script ensures that patient data can be securely encrypted and stored in a database, adhering to best practices for data protection and encryption. This setup is crucial for maintaining the confidentiality and integrity of sensitive patient information.

```
def encrypt_data(data, key):
    data_bytes = data.encode('utf-8')
    iv = get_random_bytes(AES.block_size)
    cipher = AES.new(key, AES.MODE_CBC, iv)
    padded_data = pad(data_bytes, AES.block_size)
    ciphertext = cipher.encrypt(padded_data)
    return base64.b64encode(iv).decode('utf-8'), base64.b64encode(ciphertext).decode('utf-8')
```

Figure 17. Defining the 'encrypt_data' function.

Figure 17 defines the encrypt_data function, which converts data to bytes, generates a random IV, creates an AES cipher, pads the data to fit the AES block size, encrypts it, and returns the IV and ciphertext as base64 encoded strings, ensuring secure encryption of sensitive information.

```
def decrypt_data(iv, ciphertext, key):
    iv = base64.b64decode(iv)
    ciphertext = base64.b64decode(ciphertext)
    cipher = AES.new(key, AES.MODE_CBC, iv)
    decrypted_data = unpad(cipher.decrypt(ciphertext), AES.block_size)
    return decrypted_data.decode('utf-8')
```

Figure 18. Defining the 'decrypt_data' function.

Figure 18 defines the decrypt_data function, which decodes base64 encoded IV and ciphertext, creates an AES cipher using the provided key and IV, decrypts the ciphertext, removes the padding added during encryption, and returns the original data as a string, ensuring secure decryption of the encrypted information.

```
def main():
    key = get_random_bytes(16)
    name = input("Enter patient name: ")
    dob = input("Enter patient date of birth (YYYY-MM-DD): ")
    age = input("Enter patient age: ")
    gender = input("Enter patient gender: ")
    date = input("Enter the date of record (YYYY-MM-DD): ")
    medical_conditions = input("Enter medical conditions: ")
    prescription = input("Enter prescription: ")

    iv_name, encrypted_name = encrypt_data(name, key)
    iv_dob, encrypted_dob = encrypt_data(dob, key)

    conn = sqlite3.connect('patient_record.db')
    c = conn.cursor()
    c.execute('''CREATE TABLE IF NOT EXISTS Patients
                 (Name TEXT, DOB TEXT, Age TEXT, Gender TEXT, Date TEXT, MedicalConditions TEXT, Prescription TEXT)''')

    c.execute("INSERT INTO Patients (Name, IV_Name, DOB, IV_DOB, Age, "
              "Gender, Date, MedicalConditions, Prescription) VALUES (?, ?, ?, ?, ?, ?, ?, ?, ?)",
              (encrypted_name, iv_name, encrypted_dob, iv_dob, age, gender, date, medical_conditions, prescription))
    conn.commit()
    print("Patient data has been encrypted and stored in the database.")
    conn.close()
```

Figure 19. Define the 'main' function.

Figure 19 defines the 'main' function, which generates an encryption key, prompts user for patient data, encrypts name and DOB, connects to an SQLite database, creates a table if it doesn't exist, inserts data into the database, and prints a confirmation message.

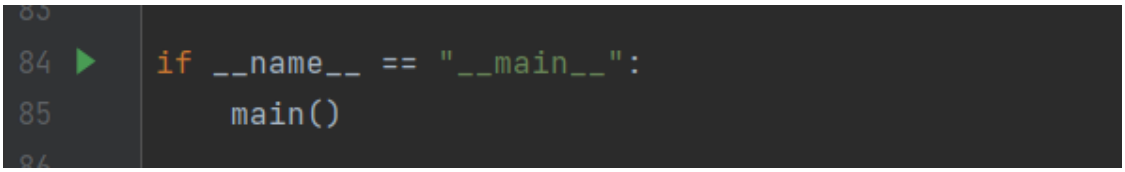


Figure 20. Run the main function if the script is executed.

Figure 20 calls for the main function to execute the script, ensuring that the encryption and data storage process is initiated when the script is run.

The code encrypts sensitive patient data using AES encryption in CBC mode with a 16-byte key. The encrypted data is concatenated with the initialization vector (IV) and then base64 encoded.

5.4 Implementation and Testing

Here's an explanation of the implementation process and model testing outcome.

5.4.1 Implementation Process

Data Identification: Identify sensitive data requiring protection (e.g., personal information).

Data Anonymization or Encryption Method: Choose between pseudonymization (e.g., hashing) or encryption (e.g., AES) to safeguard sensitive data.

Data Processing: Apply the chosen method to anonymize or encrypt sensitive data securely.

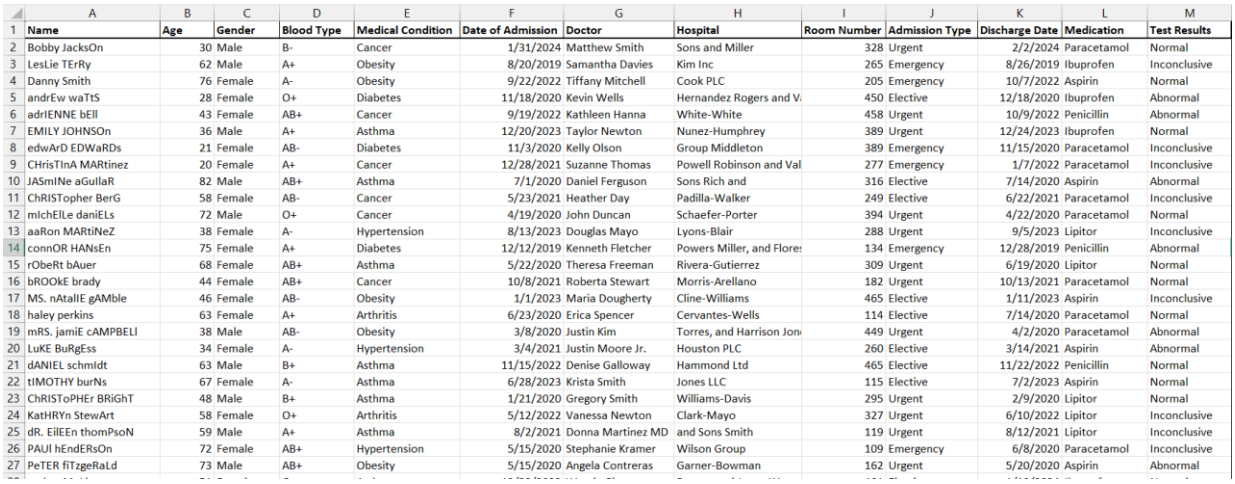
Data Storage: Store pseudonymized or encrypted data securely, ensuring protection against unauthorized access.

Compliance: Ensure adherence to data protection regulations and industry standards.

5.4.2 Model Testing

Pseudonymized data model testing:

Original Dataset

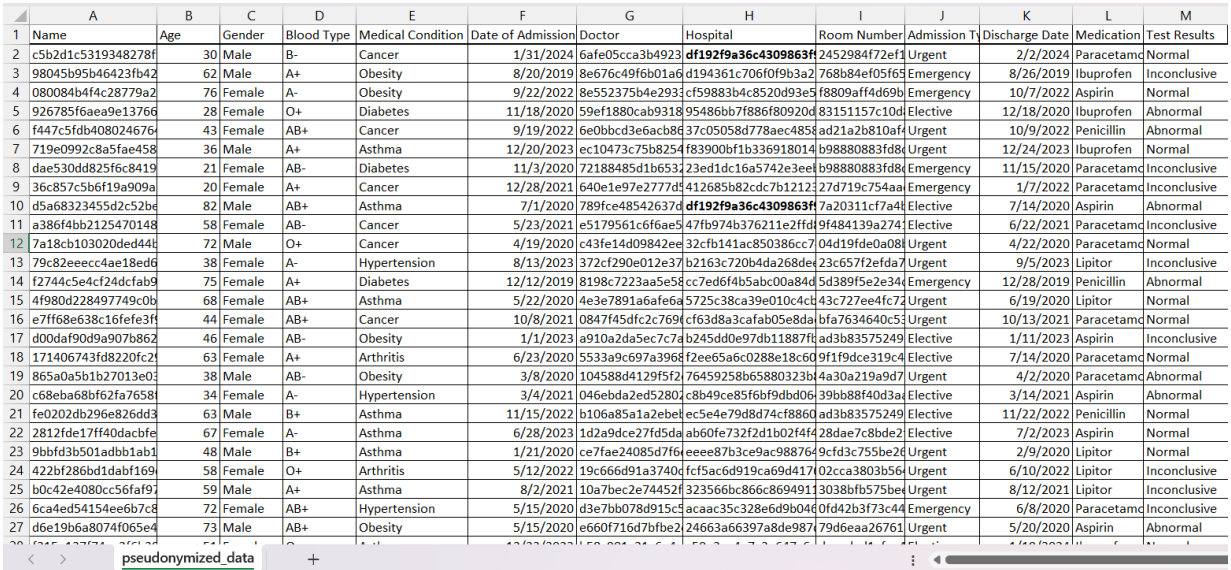


	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Name	Age	Gender	Blood Type	Medical Condition	Date of Admission	Doctor	Hospital	Room Number	Admission Type	Discharge Date	Medication	Test Results
2	Bobby JacksOn	30	Male	B-	Cancer	1/31/2024	Matthew Smith	Sons and Miller	328	Urgent	2/2/2024	Paracetamol	Normal
3	LesLie TErRy	62	Male	A+	Obesity	8/20/2019	Samantha Davies	Kim Inc	265	Emergency	8/26/2019	Ibuprofen	Inconclusive
4	Danny Smith	76	Female	A-	Obesity	9/22/2022	Tiffany Mitchell	Cook PLC	205	Emergency	10/7/2022	Aspirin	Normal
5	andrEw waTtS	28	Female	O+	Diabetes	11/18/2020	Kevin Wells	Hernandez Rogers and V	450	Elective	12/18/2020	Ibuprofen	Abnormal
6	adrIENNE bEll	43	Female	AB+	Cancer	9/19/2022	Kathleen Hanna	White-White	458	Urgent	10/9/2022	Penicillin	Abnormal
7	EMILY JOHNSOn	36	Male	A+	Asthma	12/20/2023	Taylor Newton	Nunez-Humphrey	389	Urgent	12/24/2023	Ibuprofen	Normal
8	edwArD EDWaRDs	21	Female	AB-	Diabetes	11/3/2020	Kelly Olson	Group Middleton	389	Emergency	11/15/2020	Paracetamol	Inconclusive
9	CHrisTInA MARtinez	20	Female	A+	Cancer	12/28/2021	Suzanne Thomas	Powell Robinson and Val	277	Emergency	1/7/2022	Paracetamol	Inconclusive
10	JASmINe aGullaR	82	Male	AB+	Asthma	7/1/2020	Daniel Ferguson	Sons Rich and	316	Elective	7/14/2020	Aspirin	Abnormal
11	ChRISTopher BerG	58	Female	AB-	Cancer	5/23/2021	Heather Day	Padilla-Walker	249	Elective	6/22/2021	Paracetamol	Inconclusive
12	mIchElLe daniELs	72	Male	O+	Cancer	4/19/2020	John Duncan	Schaefer-Porter	394	Urgent	4/22/2020	Paracetamol	Normal
13	aaRon MARtiNeZ	38	Female	A-	Hypertension	8/13/2023	Douglas Mayo	Lyons-Blair	288	Urgent	9/5/2023	Lipitor	Inconclusive
14	connOR HANsEn	75	Female	A+	Diabetes	12/12/2019	Kenneth Fletcher	Powers Miller, and Flores	134	Emergency	12/28/2019	Penicillin	Abnormal
15	rObeRt bAuer	68	Female	AB+	Asthma	5/22/2020	Theresa Freeman	Rivera-Gutierrez	309	Urgent	6/19/2020	Lipitor	Normal
16	bROOkE brady	44	Female	AB+	Cancer	10/8/2021	Roberta Stewart	Morris-Arellano	182	Urgent	10/13/2021	Paracetamol	Normal
17	MS. nAtalIE gAMble	46	Female	AB-	Obesity	1/1/2023	Maria Dougherty	Cline-Williams	465	Elective	1/11/2023	Aspirin	Inconclusive
18	haley perkins	63	Female	A+	Arthritis	6/23/2020	Erica Spencer	Cervantes-Wells	114	Elective	7/14/2020	Paracetamol	Normal
19	mRS. jamiE cAMPBELl	38	Male	AB-	Obesity	3/8/2020	Justin Kim	Torres, and Harrison Jon	449	Urgent	4/2/2020	Paracetamol	Abnormal
20	LuKE BuRgEss	34	Female	A-	Hypertension	3/4/2021	Justin Moore Jr.	Houston PLC	260	Elective	3/14/2021	Aspirin	Abnormal
21	dANIEL schmIdt	63	Male	B+	Asthma	11/15/2022	Denise Galloway	Hammond Ltd	465	Elective	11/22/2022	Penicillin	Normal
22	tIMOTHY burNs	67	Female	A-	Asthma	6/28/2023	Krista Smith	Jones LLC	115	Elective	7/2/2023	Aspirin	Normal
23	ChRISToPHEr BRiGhT	48	Male	B+	Asthma	1/21/2020	Gregory Smith	Williams-Davis	295	Urgent	2/9/2020	Lipitor	Normal
24	KatHRYn StewArt	58	Female	O+	Arthritis	5/12/2022	Vanessa Newton	Clark-Mayo	327	Urgent	6/10/2022	Lipitor	Inconclusive
25	dR. EilEEn thomPsoN	59	Male	A+	Asthma	8/2/2021	Donna Martinez MD	and Sons Smith	119	Urgent	8/12/2021	Lipitor	Inconclusive
26	PAUl hEndERsOn	72	Female	AB+	Hypertension	5/15/2020	Stephanie Kramer	Wilson Group	109	Emergency	6/8/2020	Paracetamol	Inconclusive
27	PeTER fiTzgeRaLd	73	Male	AB+	Obesity	5/15/2020	Angela Contreras	Garner-Bowman	162	Urgent	5/20/2020	Aspirin	Abnormal

Figure 21. The original dataset used for pseudonymization (Kaggle.com 2024).

Figure 21 shows the original dataset used for pseudonymization, sourced from dummy data on Kaggle.com (Kaggle.com 2024). This dataset contains various sensitive fields that require pseudonymization to protect personal information.

Pseudonymized Data



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Name	Age	Gender	Blood Type	Medical Condition	Date of Admission	Doctor	Hospital	Room Number	Admission Ty	Discharge Date	Medication	Test Results
2	c5b2d1c5319348278f	30	Male	B-	Cancer	1/31/2024	6afe05cca3b4923	**df192f9a36c4309863f**	2452984f72ef1	Urgent	2/2/2024	Paracetamc	Normal
3	98045b95b46423fb42	62	Male	A+	Obesity	8/20/2019	8e676c49f6b01a6	d194361c706f0f9b3a2	768b84ef05f65	Emergency	8/26/2019	Ibuprofen	Inconclusive
4	080084b4f4c28779a2	76	Female	A-	Obesity	9/22/2022	8e552375b4e2933	cf59883b4c8520d93e5	f8809aff4d69b	Emergency	10/7/2022	Aspirin	Normal
5	926785f6aea9e13766	28	Female	O+	Diabetes	11/18/2020	59ef1880cab9318	95486bb7f886f80920d	83151157c10d	Elective	12/18/2020	Ibuprofen	Abnormal
6	f447c5fdb408024676	43	Female	AB+	Cancer	9/19/2022	6e0bbcd3e6acb86	37c05058d778aec4858	ad21a2b810af	Urgent	10/9/2022	Penicillin	Abnormal
7	719e0992c8a5fae458	36	Male	A+	Asthma	12/20/2023	ec10473c75b8254	f83900bf1b336918014	b98880883fd8	Urgent	12/24/2023	Ibuprofen	Normal
8	dae530dd825f6c8419	21	Female	AB-	Diabetes	11/3/2020	72188485d1b653	23ed1dc16a5742e3ee	b98880883fd8	Emergency	11/15/2020	Paracetamc	Inconclusive
9	36c857c5b6f19a909a	20	Female	A+	Cancer	12/28/2021	640e1e97e2777d5	412685b82cdc7b1212	27d719c754aa	Emergency	1/7/2022	Paracetamc	Inconclusive
10	d5a68323455d2c52be	82	Male	AB+	Asthma	7/1/2020	789fce48542637d	**df192f9a36c4309863f**	7a20311cf7a4	Elective	7/14/2020	Aspirin	Abnormal
11	a386f4bb2125470148	58	Female	AB-	Cancer	5/23/2021	e5179561c6f6ae5	47fb974b376211e2ffd	9f484139a274	Elective	6/22/2021	Paracetamc	Inconclusive
12	7a18cb103020ded44b	72	Male	O+	Cancer	4/19/2020	c43fe14d09842ee	32cfb141ac850386cc7	04d19fde0a08	Urgent	4/22/2020	Paracetamc	Normal
13	79c82eeecc4ae18ed6	38	Female	A-	Hypertension	8/13/2023	372cf290e012e37	b2163c720b4da268de	23c657f2efda7	Urgent	9/5/2023	Lipitor	Inconclusive
14	f2744c5e4cf24dcfab9	75	Female	A+	Diabetes	12/12/2019	8198c7223aa5e58	cc7ed6f4b5abc00a84d	5d389f5e2e34	Emergency	12/28/2019	Penicillin	Abnormal
15	4f980d228497749c0b	68	Female	AB+	Asthma	5/22/2020	4e3e7891a6afe6a	5725c38ca39e010c4cb	43c727ee4fc72	Urgent	6/19/2020	Lipitor	Normal
16	e7ff68e638c16fefe3f9	44	Female	AB+	Cancer	10/8/2021	0847f45dfc2c769	cf63d8a3cafab05e8da	bfa7634640c53	Urgent	10/13/2021	Paracetamc	Normal
17	d00daf90d9a907b862	46	Female	AB-	Obesity	1/1/2023	a910a2da5ec7c7a	b245dd0e97db11887f8	ad3b83575249	Elective	1/11/2023	Aspirin	Inconclusive
18	171406743fd8220fc2	63	Female	A+	Arthritis	6/23/2020	5533a9c697a3968	f2ee65a6c0288e18c60	9f1f9dce319c4	Elective	7/14/2020	Paracetamc	Normal
19	865a0a5b1b27013e03	38	Male	AB-	Obesity	3/8/2020	104588d4129f5f2	76459258b65880323b4	4a30a219a9d7	Urgent	4/2/2020	Paracetamc	Abnormal
20	c68eba68bf62fa7658	34	Female	A-	Hypertension	3/4/2021	046ebda2ed52802	c8b49ce85f6bf9dbd06	39bb88f40d3a4	Elective	3/14/2021	Aspirin	Abnormal
21	fe0202db296e826dd3	63	Male	B+	Asthma	11/15/2022	b106a85a1a2ebeb	ec5e4e79d8d74cf8860	ad3b83575249	Elective	11/22/2022	Penicillin	Normal
22	2812fde17ff40dacbfe	67	Female	A-	Asthma	6/28/2023	1d2a9dce27fd5da	ab60fe732f2d1b02f4f4	28dae7c8bde2	Elective	7/2/2023	Aspirin	Normal
23	9bbfd3b501adbb1ab1	48	Male	B+	Asthma	1/21/2020	ce7fae24085d7f6	eeee87b3ce9ac988764	9cfd3c755be26	Urgent	2/9/2020	Lipitor	Normal
24	422bf286bd1dabf169	58	Female	O+	Arthritis	5/12/2022	19c666d91a3740c	fcf5ac6d919ca69d417	02cca3803b56	Urgent	6/10/2022	Lipitor	Inconclusive
25	b0c42e4080cc56faf97	59	Male	A+	Asthma	8/2/2021	10a7bec2e74452f	323566bc866c8694911	3038bfb575be	Urgent	8/12/2021	Lipitor	Inconclusive
26	6ca4ed54154ee6b7c8	72	Female	AB+	Hypertension	5/15/2020	d3e7bb078d915c5	acaac35c328e6d9b046	0fd42b3f73c44	Emergency	6/8/2020	Paracetamc	Inconclusive
27	d6e19b6a8074f065e4	73	Male	AB+	Obesity	5/15/2020	e660f716d7bfbe2	24663a66397a8de987	79d6eaa26761	Urgent	5/20/2020	Aspirin	Abnormal

pseudonymized_data

Figure 22. The pseudonymized dataset after running the code.

As shown in Figure 22, the pseudonymized dataset is produced by running the code, which replaces sensitive information with hashed values to protect patient privacy while maintaining the utility of the data for analysis.

Encryption data model testing:

After running the code, it asks for the user input of the patient's data.

```
Enter patient name: Olive Fred
Enter patient date of birth (YYYY-MM-DD): 1975
Enter patient age: 75
Enter patient gender: Female
Enter the date of record (YYYY-MM-DD): 2024-01-03
Enter medical conditions: Hypertension
Enter prescription: Lipitor
Patient data has been encrypted and stored in the database.
```

Figure 23. Entering the user input and storing it in the database.

After running the code, it prompts the user to input the patient's data. As shown in Figure 23, the entered user data is then encrypted and securely stored in the database, ensuring both confidentiality and integrity of the sensitive information.

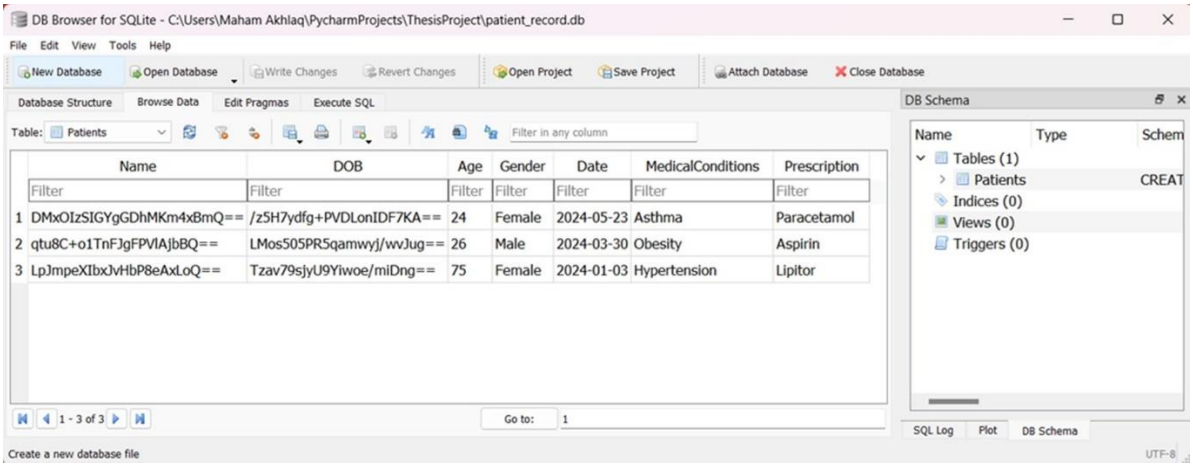


Figure 24. Database after the data being stored in encrypted form.

The database content can be viewed using DB Browser for SQLite. As illustrated in Figure 24, the patient data is stored in an encrypted form, ensuring the confidentiality and security of sensitive information. This demonstrates the effectiveness of the encryption process in protecting patient data.

The testing process verifies that sensitive information remains confidential and protected from unauthorized access through the implementation of pseudonymization and encryption techniques. Screenshots provide visual evidence of these data protection measures, validating their effectiveness.

As shown in Figure 21, the original dataset contains sensitive information that requires protection. This raw data includes personally identifiable information (PII) that is vulnerable to privacy breaches.

Figure 22 demonstrates the pseudonymized dataset after running the pseudonymization code. The sensitive columns, such as 'Name', 'Doctor', 'Hospital', and 'Room Number', have been replaced with hashed values, ensuring that the original information cannot be easily traced back to individuals.

Figure 23 illustrates the process of entering user input and storing it in the database. The user is prompted to provide patient data, which includes both sensitive and non-sensitive information. This input is then encrypted before storage.

Figure 24 shows the encrypted data stored in the database using DB Browser for SQLite. The patient names and dates of birth are encrypted, and the initialization vectors (IVs) used for encryption are stored separately. This visual evidence confirms that the encryption process effectively secures the sensitive information, making it unreadable without the correct decryption key.

Through these figures, the implementation of pseudonymization and encryption is verified. The original sensitive information is transformed into secure, non-identifiable formats, demonstrating that the data protection measures are functioning as intended.

5.5 Results and Discussion

The proposal of the "PERBE" ethical framework's each component addresses critical aspects of AI implementation in healthcare, including safeguarding patient privacy, integrating ethical considerations into AI design, complying with regulatory standards, mitigating biases, and supporting ethical decision-making. By adhering to these components, AI-powered healthcare systems can prioritize privacy, ethics, regulatory compliance, bias mitigation, and patient-centered decision-making, thereby fostering trust and transparency within the healthcare ecosystem.

The effectiveness of the implemented data protection measures, including pseudonymization and encryption, was evaluated. Through rigorous testing methodologies, it was confirmed that both pseudonymized and encrypted data are maintaining integrity, accuracy, and confidentiality. Additionally, usability testing demonstrated that both pseudonymized and encrypted data retained their usability for intended analysis purposes, further underscoring the balance between data protection and usability requirements.

6 CHALLENGES AND LIMITATIONS

6.1 Identified Limitations

During the research and model development, implementing the PERBE ethical framework posed resource and expertise challenges for healthcare organizations. Integrating ethical decision-support systems faced complexity in acceptance by healthcare professionals. Despite these challenges, efforts were made to prioritize responsible AI-powered healthcare system development.

Furthermore, implementing pseudonymization and encryption models revealed challenges. Pseudonymization techniques struggled to balance privacy and data usability, potentially compromising data utility. Encryption methods introduced computational overhead and performance issues, particularly in resource-constrained healthcare settings. Integrating these measures into existing systems required significant modifications and technical expertise. Nonetheless, we endeavored to overcome these challenges, ensuring secure handling of sensitive healthcare data through robust pseudonymization and encryption methods.

6.2 Data Bias in AI Models

Healthcare data often contains biases from historical disparities, such as sample, selection, measurement, and confirmation biases. These biases can lead to unequal treatment, delayed diagnoses, inaccurate research findings, and reinforcement of stereotypes, necessitating diverse data collection and

rigorous analysis practices (Ethical Considerations in Healthcare Data Analysis and Privacy, 2024). Bias mitigation strategies depended on diverse dataset availability, potentially limited in some healthcare settings.

The importance of mitigating biases is underscored by the necessity for diverse data collection and rigorous analysis methods. Moreover, there is an increasing demand for AI systems in healthcare to be transparent, explainable, and accountable, facilitating ethical decision-making. With the growing integration of AI into contemporary digital frameworks, emphasizing ethical considerations becomes crucial for enhancing patient outcomes and propelling healthcare methodologies forward (Naik et al., 2022).

7 FUTURE IMPLICATIONS OF AI IN HEALTHCARE

As artificial intelligence (AI) continues to evolve, ongoing collaboration among stakeholders, including healthcare professionals, policymakers, and technology experts, is essential to shape the future of ethical considerations in AI powered healthcare systems. In future, the advanced methodologies that should be used for developing ethical AI in Healthcare:

- Robust Data Processing Techniques
- Development of Fair and Unbiased Data Processing Algorithms
- Regulatory and Compliance Model
- Focus on Patient-Centric AI
- Ethics Screening in AI Models

By implementing these advanced methodologies, the future implications of AI in healthcare can lead to enhanced patient care, improved efficiency, and greater trust in AI-powered healthcare systems.

8 CONCLUSION

In conclusion, while AI has the potential to revolutionize healthcare, addressing the ethical considerations in data processing is imperative. By prioritizing patient autonomy, privacy, fairness, transparency, and responsible data use, healthcare providers and developers can harness the benefits of AI while securing the rights and dignity of patients. The PERBE framework provides a comprehensive approach to guide the ethical development and deployment of AI in healthcare. The ethical implementation of AI in healthcare requires a multifaced approach, encompassing ethics, regulation, and innovation to ensure patient-centered, equitable, and responsible use of advanced technologies. Additionally, the integration of pseudonymization and encryption methods used in development of the models enhances data protection, ensuring sensitive information remains secure and usable while complying with regulations. Overall, the results privacy-preserving techniques represented the effectiveness of the implemented data protection measures in securing sensitive data.

REFERENCES

ChatGPT 2023. OpenAI. GPT-3.5. Accessed for language check, May 2024. https://chat.openai.com

ARThink AI. 2024. Data privacy in AI Healthcare apps | OnFiT AI | Medium. Medium. https://medium.com/@ARThink.ai/data-privacy-in-ai-healthcare-apps-safeguarding-patient-information-9859783d569d. Accessed 11.05.2024.

base64 — Base16, Base32, Base64, Base85 Data Encodings. s.a. Python documentation. https://docs.python.org/3/library/base64.html. Accessed 02.05.2024.

Bodra, G. 2022. The role of artificial intelligence in industries such as healthcare, finance, and transportation. Medium. https://medium.com/ai-revolution-transforming-the-way-we-live-and/the-role-of-artificial-intelligence-in-industries-such-as-healthcare-finance-and-transportation-e81633185a6a. Accessed 01.05.2024.

Bohr, A., & Memarzadeh, K. 2020. The rise of artificial intelligence in healthcare applications. In Elsevier eBooks (pp. 25–60). https://doi.org/10.1016/b978-0-12-818438-7.00002-2. Accessed 03.05.2024.

Bongomin, O., Yemane, A., Kembabazi, B., Malanda, C., Mwape, M. C., Mpofu, N. S., & Tigalana, D. 2020. The Hype and Disruptive Technologies of Industry 4.0 in Major Industrial Sectors: A State of the Art. https://doi.org/10.20944/preprints202006.0007.v1. Accessed 22.05.2024.

Chen, Y., Clayton, E. W., Novak, L. L., Anders, S., & Malin, B. 2023. Human-Centered Design to Address Biases in Artificial Intelligence. Journal of medical Internet research, 25, e43251. https://doi.org/10.2196/43251. Accessed 05.05.2024.

Crypto.Cipher package — PyCryptodome 3.210b0 documentation. s.a. https://pycryptodome.readthedocs.io/en/latest/src/cipher/cipher.html. Accessed 02.05.2024.

Crypto.Random package — PyCryptodome 3.210b0 documentation. s.a. https://pycryptodome.readthedocs.io/en/latest/src/random/random.html. Accessed 02.05.2024.

Crypto.Util package — PyCryptodome 3.210b0 documentation. s.a. https://pycryptodome.readthedocs.io/en/latest/src/util/util.html. Accessed 02.05.2024.

Danese, J., & Jindal, N. 2024. Artificial intelligence in healthcare: Addressing ethical and regulatory hurdles. Birlasoft. https://www.birlasoft.com/articles/artificial-intelligence-in-healthcare-addressing-ethical-and-regulatory-hurdles#:~:text=Ethical%20guidelines%20for%20AI%20developers,working%20to%20eliminate%20discriminatory%20outcomes. Accessed 17.05.2024.

Das, S., & Namasudra, S. 2022. A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure. Computers and Electrical Engineering, 101, 107991. Accessed 21.04.2024.

Etzel, W. A. 2024. Navigating the regulatory landscape for AI in healthcare. Medium. https://medium.com/@winfried.etzel/navigating-the-regulatory-landscape-for-ai-in-healthcare-6462ebb021d9. Accessed 15.05.2024.

Farhud, D. D., & Zokaei, S. 2021. Ethical Issues of Artificial Intelligence in Medicine and Healthcare. Iranian journal of public health, 50(11), i–v. https://doi.org/10.18502/ijph.v50i11.7600. Accessed 12.04.2024.

Fayayola, N. O. A., Olorunfemi, N. O. L., & Shoetan, N. P. O. 2024. DATA PRIVACY AND SECURITY IN IT: A REVIEW OF TECHNIQUES AND CHALLENGES. Computer Science & IT Research Journal, 5(3), 606–615. https://doi.org/10.51594/csitrj.v5i3.909. Accessed 11.05.2024.

hashlib — Secure hashes and message digests. s.a. Python documentation. https://docs.python.org/3/library/hashlib.html. Accessed 02.05.2024.

Healthcare Dataset. 2024. Kaggle. https://www.kaggle.com/datasets/prasad22/healthcare-dataset. Accessed 19.04.2024.

ICO. s.a. How do we ensure fairness in AI? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/#:~:text=Any%20processing%20of%20personal%20data,not%20just%20their%20information%20rights. Accessed 11.05.2024.

Importance of data collection in healthcare | ForeSee Medical. (n.d.). ForeSee Medical. https://www.foreseemed.com/importance-of-data-collection-in-healthcare#:~:text=When%20healthcare%20providers%20have%20access,development%20and%20can%20cost%20lives. Accessed 31.04.2024.

InfosenseAI. 2023. Role of AI in healthcare. https://www.linkedin.com/pulse/role-ai-healthcare-infosense-ai/. Accessed 02.04.2024.

Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. 2023. Privacy-preserving artificial intelligence in healthcare: Techniques and applications. Computers in Biology and Medicine, 158, 106848. https://doi.org/10.1016/j.compbiomed.2023.106848. Accessed 27.04.2024.

Mathur, S., & Sutton, J. 2017. Personalized medicine could transform healthcare. Biomedical reports, 7(1), 3–5. https://doi.org/10.3892/br.2017.922. Accessed 10.04.2024.

Moldstud. 2019. Ethical considerations in healthcare data analysis and privacy. Retrieved from https://moldstud.com/articles/p-ethical-considerations-in-healthcare-data-analysis-and-privacy. Accessed 24.04.2024.

Mora, J. 2024. Healthcare Data Breaches of 2023 | InternXT blog. Internxt. https://blog.internxt.com/healthcare-data-breaches/. Accessed 27.04.2024.

Murray, L. 2024. What is Pseudonymization | Safeguarding Data with Fictional IDs | Imperva. Learning Center. https://www.imperva.com/learn/data-security/pseudonymization/. Accessed 29.04.2024.

N-Able. 2024. Types of database encryption methods. N-able. https://www.n-able.com/blog/types-database-encryption-methods. Accessed 17.05.2024.

Naik, N., Hameed, B. M. Z., Shetty, D. K., Swain, D., Shah, M., Paul, R., Aggarwal, K., Ibrahim, S., Patil, V., Smriti, K., Shetty, S., Rai, B. P., Chlosta, P., & Somani, B. K. 2022. Legal and ethical consideration in artificial intelligence in healthcare: Who takes responsibility? Frontiers in Surgery, 9. https://doi.org/10.3389/fsurg.2022.862322. Accessed 08.05.2024.

Novelli, C., Taddeo, M., & Floridi, L. 2023. Accountability in artificial intelligence: what it is and how it works. AI & Society. https://doi.org/10.1007/s00146-023-01635-y. Accessed 23.04.2024.

pandas - Python Data Analysis Library. s.a. https://pandas.pydata.org/. Accessed 02.05.2024.

Paulsen, R., & Paulsen, R. 2024, April 3. 7 Ways to Streamline administrative healthcare tasks. Intelligent Living. https://www.intelligentliving.co/7-streamline-administrative-healthcare/. Accessed 17.04.2024.

Pinto-Coelho L. 2023. How Artificial Intelligence Is Shaping Medical Imaging Technology: A Survey of Innovations and Applications. Bioengineering (Basel, Switzerland), 10(12), 1435. https://doi.org/10.3390/bioengineering10121435. Accessed 22.05.2024.

Pseudonymization. (1 B.C.E.). Imperva. https://www.imperva.com/learn/data-security/pseudonymization/. Accessed 21.05.2024.

Rodrigues, J. 2024. Top 5 methods of protecting data. TitanFile. https://www.titanfile.com/blog/5-methods-of-protecting-data/. Accessed 01.05.2024.

Shachar, C., Gerke, S., & Adashi, E. Y. 2020. AI Surveillance during Pandemics: Ethical Implementation Imperatives. The Hastings Center report, 50(3), 18–21. https://doi.org/10.1002/hast.1125. Accessed 01.04.2024.

Singh, N., Vayer, P., Tanwar, S., Poyet, J., Tsaioun, K., & Villoutreix, B. O. 2023. Drug discovery and development: introduction to the general public and patient groups. Frontiers in Drug Discovery, 3. https://doi.org/10.3389/fddsv.2023.1201419. Accessed 01.05.2024.

Smile Foundation. 2023. The importance of data in healthcare. https://www.smilefoundationindia.org/blog/the-importance-of-data-in-healthcare/. Accessed 02.05.2024.

Smith, G., Kohli, N., & Rustagi, I. 2020. What does "fairness" mean for machine learning systems. Berkeley Haas EGAL. Accessed 23.05.2024.

sqlite3 — DB-API 2.0 interface for SQLite databases. s.a. Python documentation. https://docs.python.org/3/library/sqlite3.html. Accessed 02.05.2024.

Stephenson, D. 2021. Artificial intelligence in medical diagnosis. Southern Medical Association. https://sma.org/ai-in-medical-diagnosis/. Accessed 20.05.2024.

Volterrani, M., & Sposato, B. 2019. Remote monitoring and telemedicine. European Heart Journal Supplements, 21(Supplement_M), M54–M56. https://doi.org/10.1093/eurheartj/suz266. Accessed 16.04.2024.

What is accountability? - Ethics of AI. s.a. https://ethics-of-ai.mooc.fi/chapter-3/2-what-is-accountability. Accessed 23.05.2024.

Wiens, J., Saria, S., Sendak, M., Ghassemi, M., Liu, V. X., Doshi-Velez, F., Jung, K., Heller, K., Kale, D., Saeed, M., Ossorio, P. N., Thadaney-Israni, S., & Goldenberg, A. 2019. Do no harm: a roadmap for responsible machine learning for health care. Nature Medicine, 25(9), 1337–1340. https://doi.org/10.1038/s41591-019-0548-6. Accessed 06.05.2024.

Yadav, N., Pandey, S., Gupta, A., Dudani, P., Gupta, S., & Rangarajan, K. 2023. Data Privacy in Healthcare: In the Era of Artificial Intelligence. Indian Dermatology Online Journal, 14(6), 788-792. Accessed 25.04.2024.

Yelne, S., Chaudhary, M., Dod, K., Sayyad, A., & Sharma, R. 2023. Harnessing the Power of AI: A Comprehensive review of its impact and challenges in nursing science and healthcare. Curēus. https://doi.org/10.7759/cureus.49252. Accessed 22.04.2024.

Zuhair, V., Babar, A., Ali, R., Olatunde Oduoye, M., Noor, Z., Chris, K., Ime Okon, I., & Ur Rehman, L. 2024. Exploring the Impact of Artificial Intelligence on Global Health and Enhancing Healthcare in Developing Nations. ncbi.nlm.nih.gov. Accessed 09.05.2024.