Received: 30 December 2022 | Revised: 4 September 2023 | Accepted: 5 October 2023

DOI: 10.1002/ett.4884

SURVEY ARTICLE

WILEY

Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions

Rucha Shinde[1] | **Shruti Patil**[2] | **Ketan Kotecha**[2] | **Vidyasagar Potdar**[3] | **Ganeshsree Selvachandran**[1,4] | **Ajith Abraham**[5]

[1]Symbiosis Institute of Technology (SIT), Symbiosis International (Deemed University), Pune, Maharashtra, India

[2]Symbiosis Centre for Applied Artificial Intelligence (SCAAI), Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune, Maharashtra, India

[3]Blockchain Research and Development Laboratory, Curtin University, Perth, Western Australia, Australia

[4]School of Business, Monash University Malaysia, Subang Jaya, Selangor, Malaysia

[5]School of Computer Science Engineering & Technology, Bennett University, Greater Noida, Uttar Pradesh, India

Correspondence
Ganeshsree Selvachandran, School of Business, Monash University Malaysia, Subang Jaya, Selangor, Malaysia and Shruti Patil, Symbiosis Institute of Technology (SIT), Symbiosis International (Deemed University), Pune 412115, Maharashtra, India.
Email:
ganeshsree.selvachandran@monash.edu;
ganeshsree86@yahoo.com;
shruti.patil@sitpune.edu.in

Abstract

Healthcare institutions are progressively integrating artificial intelligence (AI) into their operations. The extraordinary potential of AI is restricted by insufficient medical data for AI model training and adversarial attacks wherein attackers perturb the dataset by adding some noise to it, which leads to the malfunctioning of the AI models, and a lack of trust caused by the opaque operational approach it employs. This Systematic Literature Review (SLR) is a state-of-the-art survey of the research on blockchain technology for securing AI-integrated healthcare applications. The most relevant articles from the Scopus and Web of Science (WoS) databases were identified using the PRISMA model. Most of the existing literature is about protecting the healthcare data used by AI-based healthcare systems using blockchain technology, but the modality of data (text, images, audio, and sound) was not specifically mentioned. Information on protecting the training phase and model deployment for AI-based healthcare systems considering the variations in feature extraction based on the modality of data was also not clearly specified. Hence, the three subfields of AI, namely, natural language processing (NLP), computer vision, and acoustic AI are further studied to identify security loopholes in its implementation pipeline. The three phases, namely the dataset, the training phase, and the trained models need to be protected from adversaries to avoid malfunctioning of the deployed AI models. The nature of the data processed by NLP, computer vision, and acoustic AI, underlying deep neural network (DNN) architectures, the complexity of attacks, and the perceivability of attacks by humans are analyzed to identify the need for security. A blockchain solution for AI-based healthcare systems is synthesized based on the findings that have demonstrated the distinctive technological features of blockchains. It offers a solution for the privacy and security issues encountered by NLP, computer vision, and acoustic AI to boost the widespread adoption of AI applications in healthcare.

1 | INTRODUCTION

The healthcare sector needs technology handholding from infectious diseases to cancer disease management. There are countless ways to use technologies to provide more accurate, reliable, and effective treatments. These treatments can be precise at the right time in a clinical decision. Artificial Intelligence uses a computer program with precise commands to execute functions that usually require human intelligence. Algorithms are coded programming rules. Machine Learning is a method of the constant improvement of an algorithm. The improvement process utilizes vast volumes of data and is performed dynamically, enabling the algorithm to adjust and improve the accuracy of the said Artificial Intelligence. AI can understand and interpret language, identify objects, detect sounds, and learn patterns to execute problem-solving operations.

In this review, insight is provided into three main domains of artificial intelligence (AI), namely, Natural Language Processing (NLP), computer vision (CV), and acoustic AI, and their specific challenges in healthcare, as shown in Figure 1. The primary objective of Natural Language Processing for computers is to comprehend texts and languages as grasped by humans. Computer systems can interpret, deduce, summarize, translate, and synthesize exact text and language. A vast amount of textual data is generated in healthcare systems in the form of clinical reports, lab reports, handwritten notes, and other documents like admission, discharge notes, and many more. The overweighing task for clinical experts is to handle and manually analyze this enormous data. The primary tasks that can be driven through NLP are extracting important facts from text, classification of information, and opinion mining. NLP helps the analysis and conversion of these growing data to a manageable computer format. It can help to assist clinical decisions, the identification of critical patients, and the classification of diseases and disorders.

The rapidly growing area of computer vision is concerned with training computers to mimic human vision and understand the items opposite to them. Computer vision fixes this by leveraging Artificial Intelligence algorithms, which aid in the analysis of images. X-ray, Computerized Tomography (CT), Magnetic Resonance Imaging (MRI), Fluorescence-MRI, ultrasound images and videos have been proven to be among the most vital tools in deciding on the diagnosis for a patient.[1]

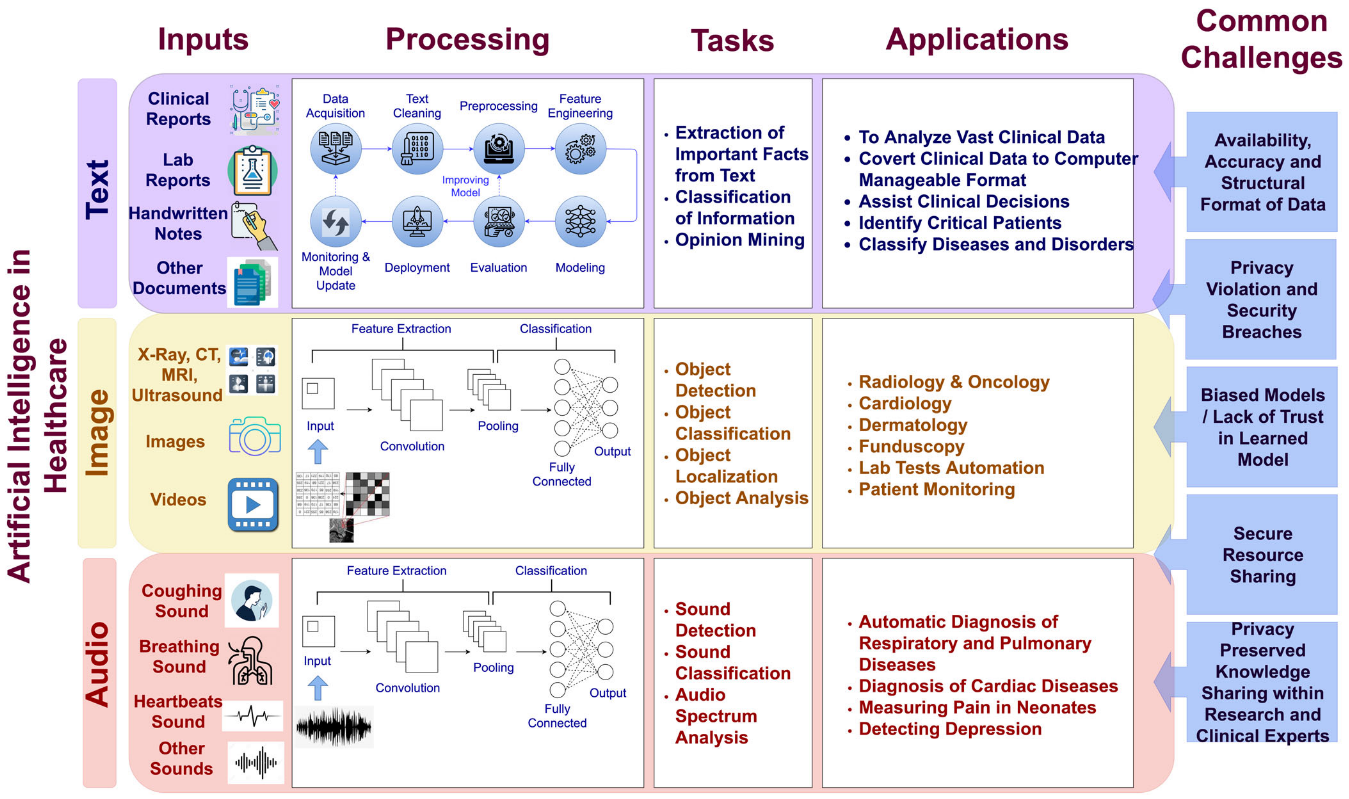


FIGURE 1 Artificial intelligence in healthcare.

Computer vision can promote remote patient monitoring, automated diagnosis, and automated lab reports through different tasks like object detection, classification, localization, and analysis from images or videos. It can promote the emergence of numerous applications that can be lifesaving for patients in radiology, oncology, cardiology, dermatology, and fundoscopy.

Certain sounds such as coughing, breathing, heartbeats, and crying play a major role in diagnosing respiratory, pulmonary, and cardiac diseases, as well as pain in neonates and detecting depression in human beings. AI assists in the automation of these diagnoses by sound detection, performing classification, and their analysis through the audio spectrum. Various state-of-the-art deep learning algorithms are available for audio signal processing, which can be helpful in the healthcare industry.

There are certain common challenges faced by AI models for their wider adoption in the healthcare industry, which is mentioned in Figure 1. When AI models are trained on sufficiently large datasets, they can work with precision. Therefore, the availability of vast, accurate, and trusted datasets for the training is one of the major challenges. This is achievable by aggregating data from different resources. But the data should be protected from privacy violations and security breaches as the organizations continue to collect, store, and transport the sensitive health vitals of the individual. It is difficult to identify biased models as AI models are black boxes in nature. There must be the provenance of prediction or classification resulting in specific healthcare input to overcome the lack of trust in the learned model. Human lives are at stake if the wrong treatment is followed based on the AI results. There should be secure resource sharing to overcome the threat of rogue devices. Knowledge sharing among researchers and clinical experts may be prone to information privacy issues. Hence, a proven strategy is a prerequisite to overcoming these challenges and establishing the dominance of AI over the healthcare industry in the future.[2]

1.1 | Background of study

Blockchain technology can address the challenges faced by AI in several ways. A blockchain is a distributed ledger with transactions that are replicated throughout the Blockchain ecosystem. The security and privacy feature of Blockchain is enriched with the cryptographic linkage of information in chronicle order, consensus protocol within the network, and smart contracts. Moreover, it builds strong trust among the users. Hence it can also establish trust, organize data, and allow sharing of resources while supporting interoperability in AI-based healthcare.[3] This study mainly targets the applicability of Blockchain in AI-based healthcare systems taking into consideration security and privacy issues in three vertical aspects, namely natural language processing (NLP), computer vision, and acoustic AI.

Figure 2 depicts the flow of activities in the Blockchain network. Blockchain technology features a distributed ledger in the peer-to-peer network. The distributed ledger securely maintains the transactional records. This feature promotes secured Distributed Learning or Federated Learning on heterogeneous data by recording local gradients on Blockchain. Moreover, a smart contract automates the execution of a transaction in the distributed network without any third-party or centralized authority. The smart contract is an executable code available at every node, which gets triggered on transaction initialization. Smart contracts validate the transaction. Access control rules can be imposed for data access through smart contracts. User provenance is possible with a smart contract. A block is generated for the transactional data. The miners are responsible for committing the block in the Blockchain by using consensus algorithms which are responsible for mining the block. It makes miners solve difficult cryptographic puzzles and share their results with a group of miners. The miner who first solves the puzzle gets a chance to mine a block of the transactions into the existing chain of blocks and replicate the new chain at every node. Consensus algorithms is the proven technique for collective decision-making on the diagnosis and treatment in AI-based healthcare systems. The blocks are linked with each other cryptographically, which makes them immutable and auditable. The same copy of the ledger is replicated at all nodes in the network, henceforth it achieves the highest degree of availability and transparency. Cryptographic linkage can validate the medical data and support its tamperproof copy. There are three types of Blockchain available, namely Public Blockchain, Private Blockchain, and Consortium Blockchain. In Public Blockchain, anyone can enter the network and participate in the transaction process. In contrast, Private Blockchain restricts entry without proper authentication and verification. Consortium Blockchain combines the features of public and private Blockchain.

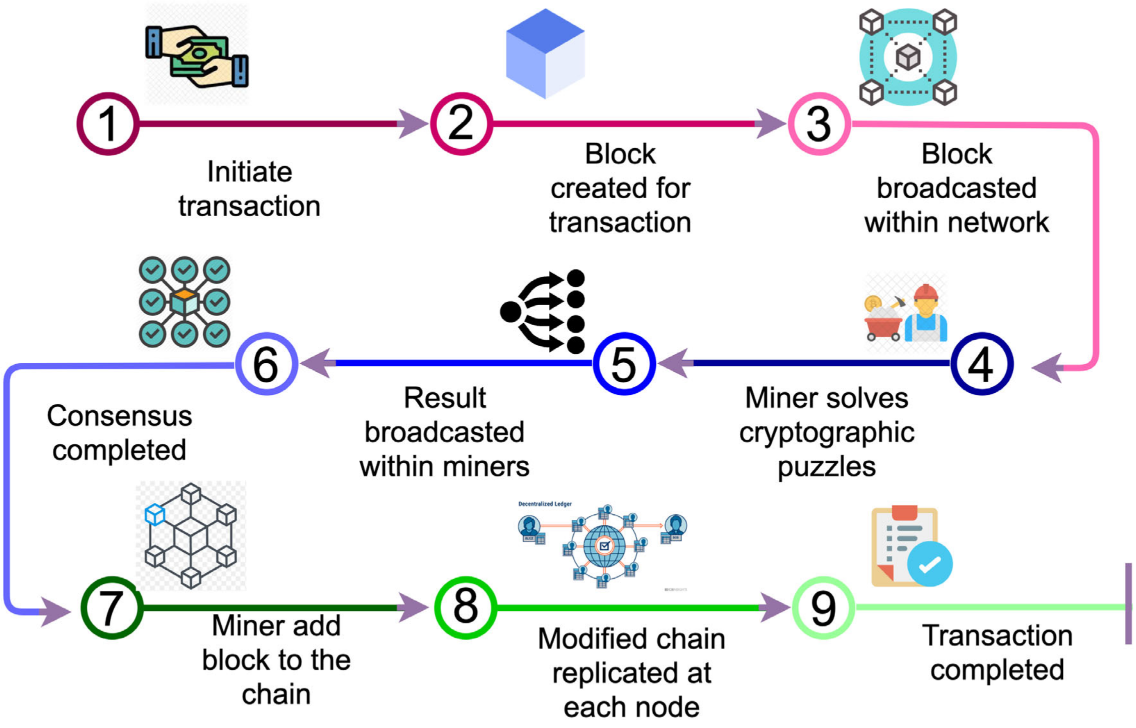

1
Initiate transaction
2
Block created for transaction
3
Block broadcasted within network
4
Miner solves cryptographic puzzles
5
Result broadcasted within miners
6
Consensus completed
7
Miner add block to the chain
8
Decentralized Ledger
Modified chain replicated at each node
9
Transaction completed

FIGURE 2 Blockchain implementation process.

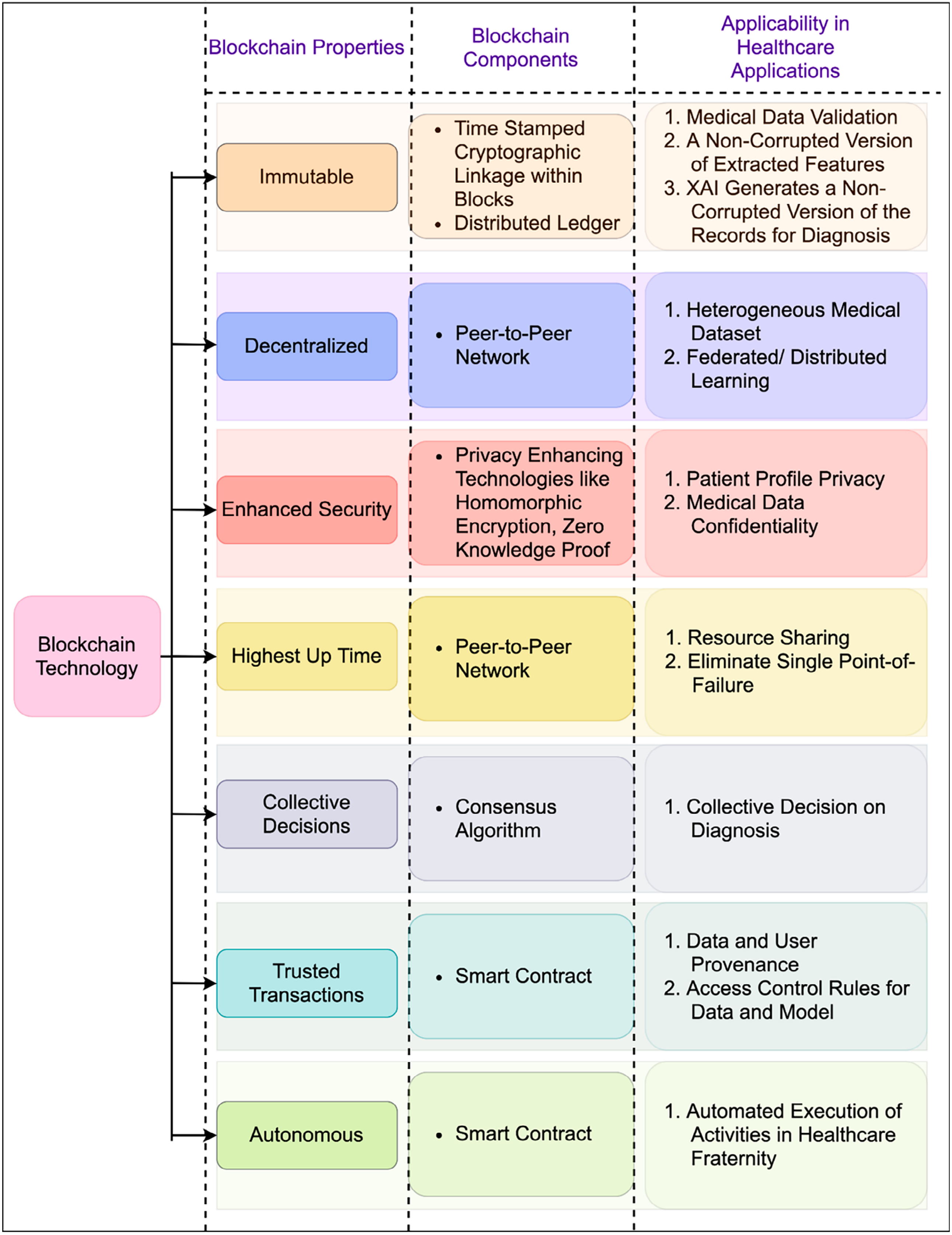
1.2 | Significance of study

The data-driven learning and exploration will improve awareness and productivity in terms of the precise diagnosis and treatment ahead in AI-based healthcare systems. It will give rise to certain challenges like anonymity, data control, and revenue generation from the sensitive information of the patient. It would be critical to establish a strong trust in the data, which is used to boost AI tools. Healthcare systems need to treat chronic diseases or acute illnesses in a timely manner to ensure the high quality of the resulting treatment and the assistance received by the patients. Though Artificial Intelligence and Machine Learning in medicine have enormous potential to improve healthcare facilities, there is a possibility of different adversarial attacks on NLP, computer vision, and acoustic AI. These attacks limit AI's real-time adoption in healthcare. These attacks cannot be tolerated in sensitive application areas such as healthcare.

Blockchain can protect against adversarial attacks considering the security requirements of NLP, computer vision, and acoustic AI, respectively. When it comes to security and privacy, the convergence of Blockchain and AI-based healthcare systems has the potential to be transformative.[4] Figure 3 provides the detailed applicability of the properties and features of blockchain that enable it to protect and validate datasets, protect classifiers/algorithms, and protect the post-training environment in AI. The distinctive properties of blockchains are expounded as follows.

I. Immutable

This immutability property protects any document or data from unauthorized modifications or deletion so that the data will remain untampered. Timestamped cryptographic linkages within blocks make it possible to achieve immutability in the blockchain with the help of hash value. Blockchain only allows the insertion of new blocks as the deletion and modification of blocks are not possible in a blockchain. A ledger of transactions is also available with each node in the blockchain network. This makes it difficult for an attacker to modify the data as modified/deleted data can be recovered from other replicas. Hence, in healthcare systems, blockchains can be used for medical data validation. The characteristics or features that will be extracted using an AI model will be kept in their original, unaltered state using Blockchain. In the case of an explainable AI-based healthcare system, an explanation for the diagnosis can be safely recorded in the blockchain for further provenance.



Blockchain Properties	Blockchain Components	Applicability in Healthcare Applications
Immutable	- Time Stamped Cryptographic Linkage within Blocks - Distributed Ledger	1. Medical Data Validation 2. A Non-Corrupted Version of Extracted Features 3. XAI Generates a Non-Corrupted Version of the Records for Diagnosis
Decentralized	- Peer-to-Peer Network	1. Heterogeneous Medical Dataset 2. Federated/ Distributed Learning
Enhanced Security	- Privacy Enhancing Technologies like Homomorphic Encryption, Zero Knowledge Proof	1. Patient Profile Privacy 2. Medical Data Confidentiality
Highest Up Time	- Peer-to-Peer Network	1. Resource Sharing 2. Eliminate Single Point-of-Failure
Collective Decisions	- Consensus Algorithm	1. Collective Decision on Diagnosis
Trusted Transactions	- Smart Contract	1. Data and User Provenance 2. Access Control Rules for Data and Model
Autonomous	- Smart Contract	1. Automated Execution of Activities in Healthcare Fraternity

FIGURE 3 Blockchain for AI-based healthcare explained.

II. Decentralized

As the name suggests, the blockchain network does not follow a conventional Client–Server architecture as it is decentralized. It is a peer-to-peer network in which every node connected to the blockchain network can initiate a transaction. Hence in healthcare systems, there can be heterogeneous medical datasets, and secure federated learning/distributed learning can be implemented in this secure peer-to-peer network.

III. Enhanced security

Privacy-enhancing technologies like homomorphic encryption, and zero-knowledge proof are implemented in blockchain. This will help to maintain patient profile privacy and medical data confidentiality as privacy-enhancing technologies are digital technologies that enable data collection, processing, analysis, and sharing while preserving data privacy and confidentiality.

IV. Highest up time

Due to the decentralized nature of blockchains, the peer-to-peer network allows the sharing of resources along with the elimination of single points of failure. This feature will be helpful in critical applications like healthcare systems, where downtimes cannot be tolerated.

V. Collective decisions

Consensus Algorithms play an important role in committing transactions in the blockchain. The responsibility of the consensus algorithm is to verify that every new block added to the blockchain is guaranteed to be the only version of the facts accepted by all the nodes in the blockchain. The blockchain consensus protocol includes particular objectives like achieving an understanding, collaboration, and cooperation, giving every node equal right, and requiring each node to take part in the consensus process. Therefore, a consensus algorithm seeks to identify an agreement that benefits the whole network, and this helps in collective decisions on diagnosis/treatments in AI-based healthcare systems.

VI. Trusted transactions and autonomous

Data and user provenance are possible with the help of smart contracts installed at each node of the blockchain network. Smart Contracts consist of the rules which need to be followed during transaction execution. Whenever any new transaction is initiated in the blockchain network, the smart contract is automatically triggered and executed. Hence, in AI-based healthcare systems, access control rules for healthcare data and AI models can be imposed through smart contracts. The automated execution of activities in healthcare systems is also made possible with smart contracts.

This study uncovers the existing blockchain-integrated AI-based healthcare applications. A conceptual framework is synthesized that maps the blockchain solution to the adversarial attacks in NLP, Computer Vision, and Acoustic AI to bring robustness to AI-based healthcare systems. This contribution will help to further academic knowledge in the Blockchain for AI-envisioned healthcare applications.

1.3 | Evolution of blockchain in Healthcare 4.0 and start of Healthcare 5.0

Healthcare 4.0 has underlined global healthcare with real-time monitoring and involves AI and data analytics. In 2016, Blockchain was suggested for the first time in the healthcare system to liberate inefficient assets, address critical organizational issues, and manage electronic transfers and exchange of healthcare records. Drug manufacturing systems can also be monitored.[5] MedRec framework based on Blockchain technologies was proposed to manage Electronic Medical Records (EMRs) in Reference 6, while in Reference 7, it was mentioned that Blockchain provided trusted data marketplaces. The privacy-preserved healthcare data management system MediBchain was proposed later, considering the privacy issues in public networks.[8] In 2018, the healthcare sector underwent a transformative shift with the innovative integration of Blockchain, AI, and Internet of Things (IoT). This fusion brought about a revolutionary impact on various aspects of healthcare, including enhanced management of Electronic Health Records (EHR), remote patient monitoring, self-directed diagnosis, and distributed parallel computing for precision medicine.[9–13] Progressing into 2019, a pioneering telemedicine framework utilizing Blockchain emerged, securing the remote provision of medical services to underserved rural areas in Bangladesh, while safeguarding the confidentiality of patients' sensitive health data.[14] A groundbreaking fog monitoring system was also proposed in 2019, utilizing Blockchain technology to identify human activities. This framework, an expansion of e-Healthcare capabilities, operates on the creation of clustered feature vectors, thereby advancing remote patient monitoring systems integrated with extensive big data analytics.[15,16] Later in 2020, the convergence of Blockchain extended to Federated Learning, Explainable AI, and 5G and 6G networks.[17,18] Protection and privacy are important during the collection, management, and distribution of EHR data.[19] Synthesis of AI and Blockchain provides a blueprint for a Blockchain-assisted open bionetwork of private healthcare records to accelerate emerging methodologies for medication development and preventative healthcare. The start of Healthcare 5.0 era has begun with the Intelligent Tele-surgery technology with 6G-enabled Tactile Internet (TI) built on the Blockchain to provide real-time and intelligent ultra-responsive healthcare facilities, virtually with high effectiveness and productivity.[20] Vulnerability analysis of the security solutions for software-defined cyber-physical systems was reviewed in the study in Reference 21. In early 2021, research in secured image processing and sharing is uplifted with Blockchain.[22] Deep Learning (DL) with Blockchain-assisted secured image transmission and diagnostic model is invented for the Internet of Medical Things (IoMT) environment.[23] The Hyperledger Fabric technology has proved effective again, to provide adequate protection against all cyber-attacks in the healthcare industry.[24] Figure 4 highlights the milestones in Healthcare 4.0 and the start of Healthcare 5.0 with Blockchain technology.

1.4 | Important terminologies

A brief overview of some of the commonly encountered terminologies used in this systematic literature review are as follows.

i. Blockchain: A blockchain is a distributed, decentralized, immutable ledger over a network.
ii. Encryption: Encryption is the process of translating data or information into codes, particularly to restrict data leakage.
iii. Nodes: These are the computers in a Blockchain network which maintain a replica of the distributed ledger.
iv. Block: Each block holds the transaction data along with the hash of the block itself and hash of the previous block.
v. Transaction: An exchange or transfer of assets that occurs between two or more individuals and generates a contractual relationship.
vi. Cryptographic hash: Cryptographic hash is a fixed size of value generated from an arbitrary size of the data by applying cryptographic functions.
vii. Genesis block: The genesis block can be called Block 0 as it is the first block in a Blockchain on which the subsequent blocks are built.
viii. Smart Contract: A smart contract is a computer program, or a transaction protocol designed to execute, control, or document contractually important events and that acts under the conditions of a contractual agreement.
ix. Consensus Algorithm: A consensus algorithm is a computer program that allows distributed processes or systems to agree on a single data value.
x. Natural Language Processing (NLP): NLP trains computers with the potential to interpret text and spoken languages.
xi. Computer Vision: Computer vision trains the computers to interpret and comprehend the visual environment.
xii. Acoustic AI: Acoustic AI consists of audio signal processing algorithms that understand sounds in the environment on an immense scale.
xiii. Adversarial Attack: An adversarial attack introduces tiny perturbation to the input of AI model/datasets used to train the AI Model and causes the AI model to malfunction.
xiv. Federated Learning: Federated learning is a machine learning approach in which an algorithm is trained across several decentralized edge devices or servers without exchanging the local data samples.
xv. Explainable AI: Explainable AI is a collection of tools and frameworks designed to assist in understanding and interpreting predictions generated by the AI model.

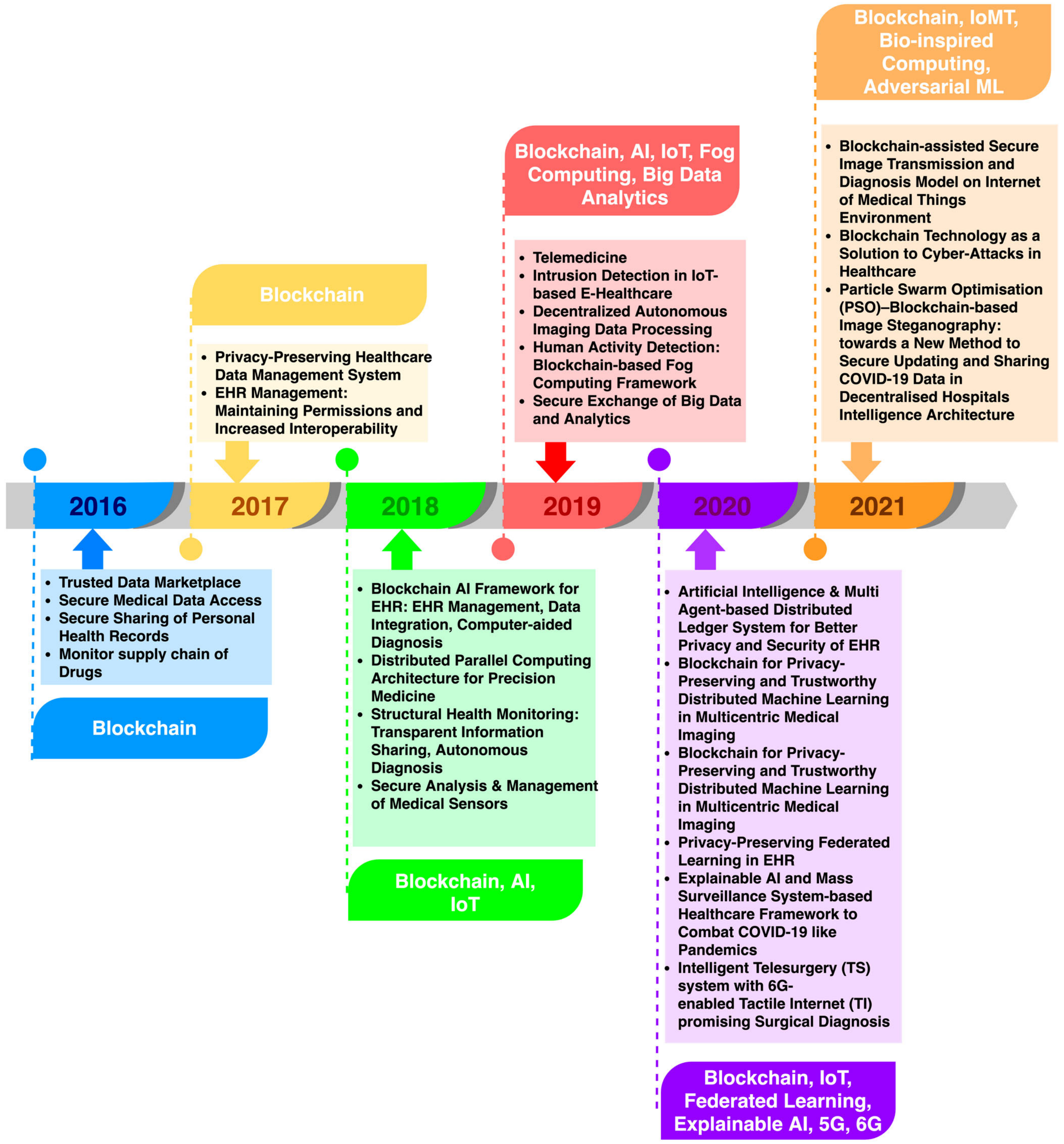

Blockchain, IoMT, Bio-inspired Computing, Adversarial ML
Blockchain, AI, IoT, Fog Computing, Big Data Analytics
• Blockchain-assisted Secure Image Transmission and Diagnosis Model on Internet of Medical Things Environment
• Blockchain Technology as a Solution to Cyber-Attacks in Healthcare
• Particle Swarm Optimisation (PSO)–Blockchain-based Image Steganography: towards a New Method to Secure Updating and Sharing COVID-19 Data in Decentralised Hospitals Intelligence Architecture
Blockchain
• Telemedicine
• Intrusion Detection in IoT-based E-Healthcare
• Decentralized Autonomous Imaging Data Processing
• Human Activity Detection: Blockchain-based Fog Computing Framework
• Secure Exchange of Big Data and Analytics
• Privacy-Preserving Healthcare Data Management System
• EHR Management: Maintaining Permissions and Increased Interoperability
2016
2017
2018
2019
2020
2021
• Trusted Data Marketplace
• Secure Medical Data Access
• Secure Sharing of Personal Health Records
• Monitor supply chain of Drugs
Blockchain
• Blockchain AI Framework for EHR: EHR Management, Data Integration, Computer-aided Diagnosis
• Distributed Parallel Computing Architecture for Precision Medicine
• Structural Health Monitoring: Transparent Information Sharing, Autonomous Diagnosis
• Secure Analysis & Management of Medical Sensors
Blockchain, AI, IoT
• Artificial Intelligence & Multi Agent-based Distributed Ledger System for Better Privacy and Security of EHR
• Blockchain for Privacy-Preserving and Trustworthy Distributed Machine Learning in Multicentric Medical Imaging
• Blockchain for Privacy-Preserving and Trustworthy Distributed Machine Learning in Multicentric Medical Imaging
• Privacy-Preserving Federated Learning in EHR
• Explainable AI and Mass Surveillance System-based Healthcare Framework to Combat COVID-19 like Pandemics
• Intelligent Telesurgery (TS) system with 6G-enabled Tactile Internet (TI) promising Surgical Diagnosis
Blockchain, IoT, Federated Learning, Explainable AI, 5G, 6G

FIGURE 4 Blockchain evolution in Healthcare 4.0.

2 | PRIOR RESEARCH

There are a lot of relevant literature reviews related to Blockchain in the healthcare domain. The examination conducted in Reference 25 explored the management of patient information and identification. The primary emphasis was on Electronic Health Records (EHR) and Patient Health Records (PHR), investigating how Blockchain technology empowers patients by giving them control over their data and enabling self-governing identity. The study in Reference 26 highlighted Blockchain-enabled healthcare applications and investigated and validated Blockchain adaptability

TABLE 1 Comparison of existing literature reviews on Blockchain in healthcare.

Reference No.	Focus on Artificial Intelligence-based healthcare application	Uncovered cyber-attacks/ Adversarial attacks	Specified type of Blockchain platform	Mentioned issues of integrating Blockchain into healthcare	Provided solution for issues in integration of Blockchain with healthcare system
26	N	Y	Y	Y	Y
29	N	N	N	Y	N
30	N	N	Y	Y	N
31	N	N	Y	Y	Y
32	N	N	N	Y	N
36	N	Y	Y	Y	Y
28	N	N	Y	Y	N
37	N	N	N	Y	N
27	N	N	Y	Y	Y
33	N	N	N	Y	N
35	N	N	Y	Y	N
34	N	N	N	Y	N
Our study	Y	Y	Y	Y	Y

in healthcare. The study in Reference 27 focuses on Smart contracts for EHR access control in healthcare taking into consideration Blockchains that require permissions and are permissionless. The reviews in References 28–30 have investigated various Blockchain implementations in the healthcare domain and proposed potential research directions and trends in healthcare as precise diagnosis, cybercrime protection, and enhancing patient care in case of emergencies and remote patient monitoring. The study concluded that by using Blockchain technologies in the healthcare sector, information security could be enhanced by allowing the processing and sharing of healthcare data while maintaining data privacy and security.[31] Following a comprehensive analysis of the prevailing significant concerns within the healthcare domain, the assessment in Reference 32 explored the potential of Blockchain solutions to enhance the security, privacy, and compatibility of healthcare data. This investigation proposed several novel applications of Blockchain in healthcare, encompassing collaborative Blockchain utilization, intelligent processing of healthcare claims through smart contracts, authorization mechanisms, as well as the integration of wearable fitness devices and health monitoring. The studies in References 33,34 investigated the effectiveness of Blockchain for healthcare and opportunities and challenges, emphasizing the use of Telemedicine, Telehealth, and E-Health. The scope of the review in Reference 35 is restricted to information on Blockchain for clinical trials and challenges. The study in Reference 36 focused on Blockchain applications exclusively for EHR. Table 1 depicts the comparison of existing reviews on Blockchain in healthcare.

There are several shortcomings in the past studies reviewed above, all of which are summarized as follows:

i. Previous studies mainly focused on EHR and some specific specialized healthcare services, for example, Telemedicine and Telehealth.
ii. The existing literature is not concentrated on Blockchain for AI-enabled healthcare. Henceforth, it does not go into depth about the use of Blockchain technology to mitigate adversarial attacks or cyber threats in AI-enabled healthcare systems.
iii. None of the surveys reviewed above studied the use of Blockchain technology to incorporate robustness in NLP, computer vision, and acoustic AI domains for the development of automated and precise healthcare services.

Although this is not the first review in Blockchain for healthcare, it is significantly distinct from the existing surveys in literature. This SLR is comprehensive in highlighting innovation, strategies, and threats related to state-of-the-art

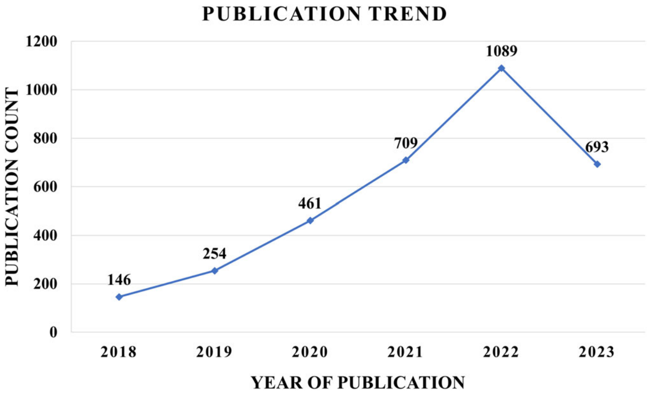


FIGURE 5 Year-wise publication trend for AI in Healthcare (2018–2023). *Source*: www.scopus.com (Accessed on August 15, 2023).

Blockchain-envisioned AI-based healthcare applications targeting NLP, computer vision, and acoustic AI domains by considering the potential of AI in healthcare along with the adversarial attacks they may face. In addition, our SLR emphasizes the research gaps to highlight prospective research pathways.

2.1 | Motivation

Human intelligence and physical abilities are restricted by certain boundaries, which leads to automation in healthcare. The healthcare sector is receiving overwhelming breakthroughs in digital transformation with AI. Researchers are coming up with innovative AI solutions in the healthcare system to provide better clinical diagnosis and treatment.[38] As shown in Figure 5, over the last 6 years, there has been a rapid increase in the number of research articles related to AI-based healthcare in the Scopus database (limited to articles published in the English language only). During the year 2021, the World Health Organization (WHO) released ethical and governance guidelines for the incorporation of AI in the healthcare sector.[39] This endeavor seeks to ensure that these advancements align with the goals of promoting equitable and comprehensive worldwide health, upholding health and safety criteria, and contributing to the realization of enduring progress in healthcare. The overall investment in AI for healthcare by the public and private sectors increasing at an exponential rate, and Accenture estimates that by 2026, cutting-edge AI applications can save a whopping $150 billion annually.[40]

However, it is unclear how much patients will trust AI resources/tools and be inclined to obey an AI diagnosis or adopt the treatment proposed by AI. For the sustained use of AI and to ensure the survival of AI in healthcare, it is imperative that the users trust that the algorithms used to make decisions are based on sound clinical guidelines, and the data that strengthens these AI-based tools are precise, relevant, transparent, and reliable. Although AI tools are inherently complex, healthcare developers must provide trust and transparency to the fullest in diagnosis and treatment. This study targets Blockchain technology as a solution to the shortcomings mentioned earlier. In a pandemic, a large medical workforce is required. So, intelligent AI-based healthcare automation will alleviate the strain on the healthcare workforce. The decentralized structure of the Blockchain makes it immune to attacks by hackers who are looking to steal anything valuable, including sensitive and confidential information. Existing storage solutions that rely on centralized storage systems are vulnerable. The adoption of AI-based healthcare systems may indeed be aided by Blockchain technology as this will make AI-based healthcare systems more robust and trustworthy. However, the work done in Blockchain to improve AI-based healthcare processes is not comprehensive. This study details the advances in AI-based healthcare that is made possible by Blockchain technology and its potential directions, which will encourage researchers to further investigate Blockchain technology for AI-based healthcare systems with a new perspective of breaking down the domain into three subdomains, namely NLP, computer vision, and acoustic AI.

2.2 | Research objectives

This study highlights privacy and security aspects of AI-based healthcare systems and risk mitigation with Blockchain technology. Healthcare applications from three domains, namely NLP, computer vision, and acoustic AI are considered

TABLE 2 Research objectives.

No.	Research question	Research objectives	Answered in section
1	How can AI improve traditional healthcare systems?	The objective is to investigate how NLP, computer vision, and acoustic AI have made potential improvements in traditional healthcare.	Section 1 Section 6.2 Section 7.2 Section 8.2
2	What are the potential vulnerabilities/threats in AI which make it difficult to adapt AI-based healthcare applications in real-time?	The goal is to examine various potential attacks on AI that may limit its adoption.	Section 5 Section 6.3 Section 7.3 Section 8.3
3	How can Blockchain help to enhance AI-based healthcare applications?	The aim is to investigate how Blockchain can improve the robustness of AI-based healthcare as Blockchain technology can address privacy and security issues in AI.	Section 4 Section 9
4	What are the advancements in Blockchain technology that help AI healthcare?	Another objective is to explore advancements in Blockchain that can be compatible with AI-based healthcare.	Section 10.3

in this study. Four research questions have been formulated to achieve the objectives of this systematic literature review, and these are presented in Table 2.

2.3 | Contributions of study

This work focuses on NLP, computer vision, and acoustic AI-based healthcare applications in this study. Various healthcare applications from the above-listed domains and their challenges have been listed and expounded. This survey has focused on adversarial attacks on NLP, computer vision, and acoustic AI, which threaten the use of AI in healthcare. The authors have reviewed existing Blockchain research for AI-based healthcare to address security and privacy concerns in AI. Furthermore, different Blockchain algorithms and techniques have been proposed to mitigate adversarial attacks on NLP, computer vision, and acoustic AI. Blockchain technology can play a pertinent role in creating a more robust AI-based healthcare system as it has the potential to deal with pertinent security and privacy issues. Finally, the challenges and constraints of adopting Blockchain in healthcare and the future research directions in Blockchain AI- envisioned healthcare are discussed.

2.4 | Organization of study

This study is organized as follows. The study investigates the use of blockchains for improving the robustness of the three main domains, namely NLP, computer vision, and acoustic AI, especially for healthcare applications. As shown in Figure 6, Section 1, has covered the significance of the study, the evolution of Blockchain in Healthcare 4.0, and the start of Healthcare 5.0. Section 2, provides a comparison of existing surveys for Blockchain in healthcare, and discusses the motivation, research objectives, the contributions of the study, and the organization of this study. Section 3, describes the research methodology based on selection criteria, quality assessment, and selection results. In Section 4, a review of the past literature related to Blockchain for AI-based healthcare and its challenges is presented while Section 5 describes the attack surface of AI, that is, how attacks target data, classifier/algorithm, and model. Section 6 briefly describes NLP, including its different techniques and applications in healthcare, different adversarial attacks on NLP based systems, and available defense to protect NLP from adversarial attacks. Section 7 provides detailed information about computer vision and the techniques and applications of CV in healthcare, along with possible adversarial attacks on CV, and defense

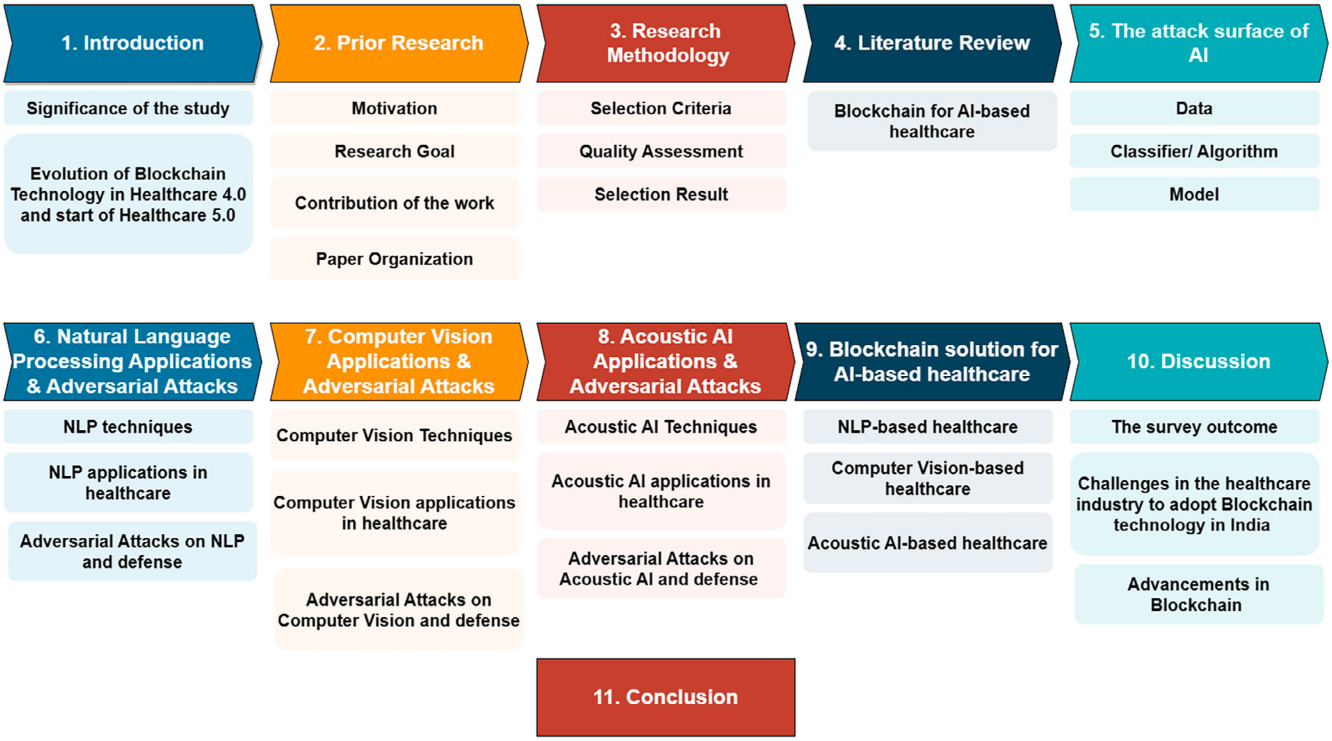

1. Introduction
Significance of the study
Evolution of Blockchain Technology in Healthcare 4.0 and start of Healthcare 5.0
2. Prior Research
Motivation
Research Goal
Contribution of the work
Paper Organization
3. Research Methodology
Selection Criteria
Quality Assessment
Selection Result
4. Literature Review
Blockchain for AI-based healthcare
5. The attack surface of AI
Data
Classifier/ Algorithm
Model
6. Natural Language Processing Applications & Adversarial Attacks
NLP techniques
NLP applications in healthcare
Adversarial Attacks on NLP and defense
7. Computer Vision Applications & Adversarial Attacks
Computer Vision Techniques
Computer Vision applications in healthcare
Adversarial Attacks on Computer Vision and defense
8. Acoustic AI Applications & Adversarial Attacks
Acoustic AI Techniques
Acoustic AI applications in healthcare
Adversarial Attacks on Acoustic AI and defense
9. Blockchain solution for AI-based healthcare
NLP-based healthcare
Computer Vision-based healthcare
Acoustic AI-based healthcare
10. Discussion
The survey outcome
Challenges in the healthcare industry to adopt Blockchain technology in India
Advancements in Blockchain
11. Conclusion

FIGURE 6 Organization of study.

techniques available. Section 8 depicts acoustic AI with its techniques and healthcare applications, adversarial attacks on acoustic AI, and the work done so far in the defense of acoustic AI from adversarial attacks. Then in Section 9, a Blockchain solution for AI-based healthcare that considers NLP-based healthcare, computer vision-based healthcare, and acoustic AI-based healthcare is proposed. Section 10 discusses the outcome of the survey, challenges in the healthcare industry to adopt Blockchain technology in India, and finally, the advancements in Blockchain. Concluding remarks are presented in Section 11, followed by the list of statements and declarations, and the list of references.

3 | RESEARCH METHODOLOGY

The processes or strategies used to locate, select, process, and analyze information on a topic are referred to as research methodology. In this study, a systematic literature survey using the PRISMA approach is presented to answer the research questions that investigates the robustness of the healthcare system. This technique is split into the following areas: selection criteria, quality assessment, and selection result.

3.1 | Selection criteria

The Scopus and Web of Science (WoS) databases were selected to find the relevant documents. A specific query is created to obtain the documents through multiple database searches. Table 3 depicts the keyword selection process using the PIOC (Population, Intervention, Outcome, and Context) method. Table 4 represents the search string, that is, the query used to retrieve the number of documents, using the keywords listed in Table 3.

After conducting a keyword query search in Scopus and WoS, a list of inclusion criteria for selecting research articles and exclusion criteria for rejecting research articles for the systematic review is developed. Table 5 shows the inclusion and exclusion criteria that were used for selecting articles for the systematic review.

TABLE 3 Keywords selection.

Parameter	Meaning	Keywords used
Population	It is a field of application.	"Healthcare" OR "Medical"
Intervention	It refers to the software methodology.	"Blockchain" AND ("Artificial Intelligence" OR "Machine Learning" OR "NLP" OR "Computer Vision" OR "Acoustic AI" OR "Federated Learning" OR "Explainable AI")
Outcome	It should be related to important aspects, such as increased accuracy, robustness, and trustworthiness.	"Adversarial Attack" OR "Security Issues" or "Privacy Issues"
Context	It refers to situations in which the solution is carried out.	"Data" OR "Classifier" OR "Algorithm" OR "Model" OR "Text" OR "Image" OR "Video" OR "Sound" OR "Audio"

TABLE 4 Database source and query executed.

Database	Search query	No. of documents
Scopus	(TITLE-ABS KEY ("Healthcare" OR "Medical") AND TITLE ABS-KEY ("Blockchain") AND TITLE-ABS-KEY ("Artificial Intelligence" OR "Machine Learning" OR "Federated Learning" OR "Explainable AI" OR "NLP" OR "Computer Vision" OR "Acoustic AI"))	299
WoS	("Healthcare" OR "Medical") AND ("Blockchain") AND ("Artificial Intelligence" OR "Machine Learning" OR "Federated Learning" OR "Explainable AI" OR "NLP" OR "Computer Vision" OR "Acoustic AI")	178

TABLE 5 Inclusion and exclusion criteria.

Sr. no.	Inclusion criteria	Exclusion criteria
1	Published in peer-reviewed journal	Non-English articles
2	Document published after the year 2016	Book chapters
3	Content directly relevant to Blockchain as the solution for AI-based healthcare systems	Little or no focus on a Blockchain solution for AI-based healthcare systems
4	An article answering research questions	Duplicate articles

3.2 | Quality assessment

The following criteria were considered for quality assessment. The articles which meet the criteria are then considered for the systematic review.

- *Application area*: The article emphasizes healthcare applications or medical domain.
- *Objectives*: The article discusses the challenges in AI-based healthcare and mitigating those with Blockchain.
- *Techniques*: Proposed or implemented framework in the article must have Blockchain technology integrated with AI methods.
- *Security measures*: The article must identify the features of Blockchain and use them to achieve privacy, security, and integrity.

3.3 | Selection results

Figure 7 represents the selection procedure of relevant articles included for the systematic literature review of "Blockchain for AI-based Healthcare Applications." At the initial stage, after executing search queries on both Scopus and WoS databases, 299 and 178 articles were obtained simultaneously. Out of these 477 articles, around 112 articles were found to

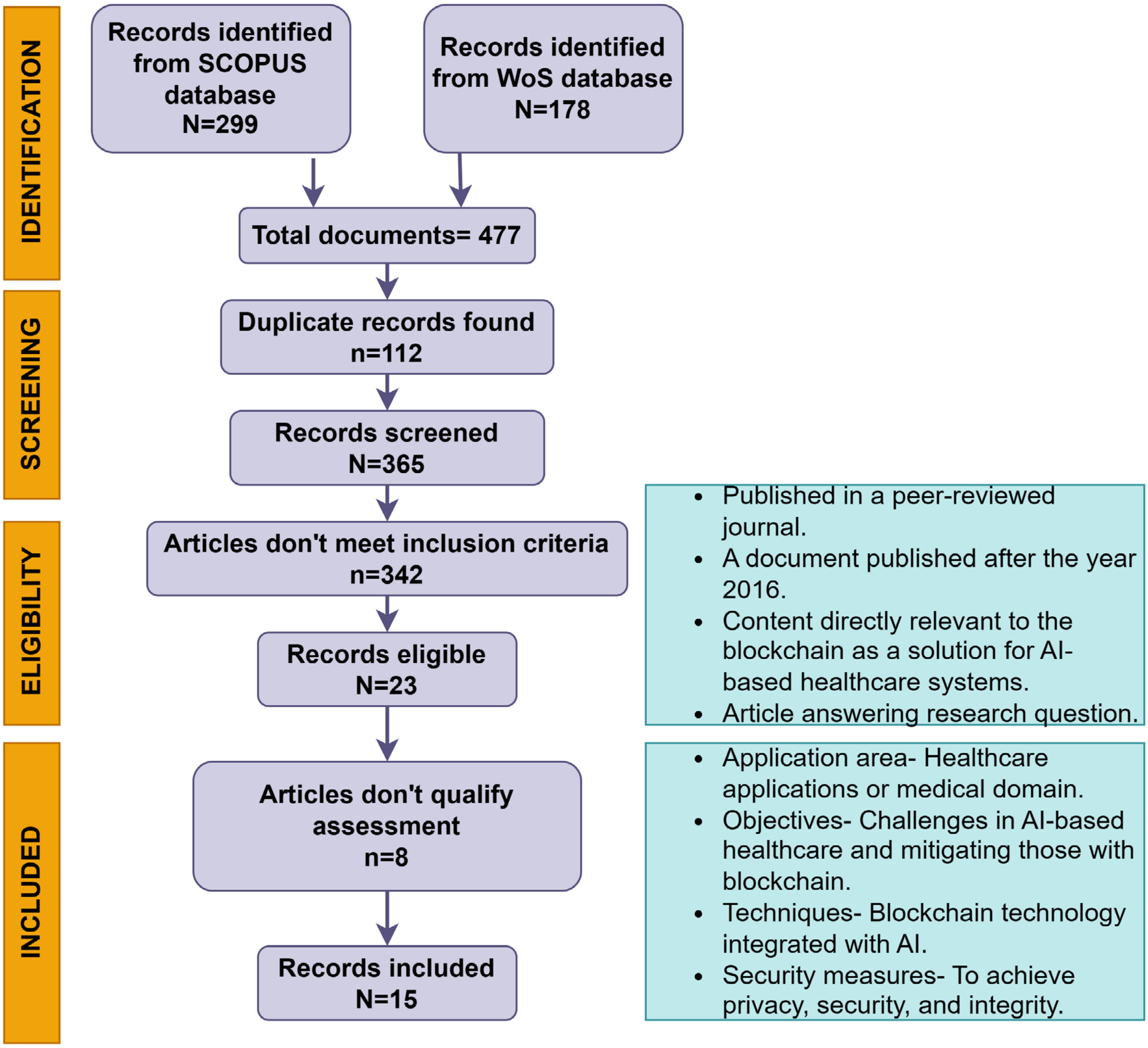

IDENTIFICATION
SCREENING
ELIGIBILITY
INCLUDED
Records identified from SCOPUS database N=299
Records identified from WoS database N=178
Total documents= 477
Duplicate records found n=112
Records screened N=365
Articles don't meet inclusion criteria n=342
Records eligible N=23
Articles don't qualify assessment n=8
Records included N=15
Published in a peer-reviewed journal.
A document published after the year 2016.
Content directly relevant to the blockchain as a solution for AI-based healthcare systems.
Article answering research question.
Application area- Healthcare applications or medical domain.
Objectives- Challenges in AI-based healthcare and mitigating those with blockchain.
Techniques- Blockchain technology integrated with AI.
Security measures- To achieve privacy, security, and integrity.

FIGURE 7 PRISMA flow diagram on the selection process of relevant articles.

be duplicates after screening, and these 112 duplicate articles were then removed from the list. In the next step, based on the inclusion criteria, the articles were tested for their eligibility. As a result, 342 articles out of 365 articles which did not meet the eligibility criteria were removed from the documents collection. Furthermore, out of the 23 articles that were retained, 8 articles did not qualify for the quality assessment. Therefore, 15 articles were finally retained and included in the article collection for conducting a systematic literature review.

4 | LITERATURE REVIEW

This section presents a thorough review of the recent and relevant literature related to the core areas of this review.

4.1 | Blockchain for AI-based healthcare

The deep models have been extensively utilized to tackle several difficulties in medical treatments in image analysis. Deep learning often works more efficiently when trained on large volumes of data. Hospitals, diagnostic laboratories, research institutions, and patients may exchange valuable findings and work together to improve the AI model. However, they face challenges in sharing important, confidential data with third parties due to privacy and security concerns. Hence, secure data sharing becomes an obstacle in improving the quality of AI-based healthcare systems. Neelakandan et al.[41] proposed a BDL-SMDTD model for secure image transmission to provide a solution to the above-mentioned obstacles, wherein Blockchain is used to store encrypted images. Kumar et al.[42] proposed a strategy that involves sharing local models via the Blockchain network which was leveraged to collectively develop a global model for an improved prediction of lung cancer using CT scan images. As a result, the collectively updated model aids in the accurate diagnosis of patients' diseases, resulting in improved treatment and therapy. This will avoid the actual sharing of data and hence maintains the privacy of patients. The organizations will upload their data over the Interplanetary File System (IPFS) and share local gradients through smart contracts. Delegated Proof-of-Stake consensus algorithm is used to train the global model. Confidence in the data is established through a smart contract, with the Blockchain retaining the hash of the nearby gradient. Kim and Huh[43] introduced a Blockchain-based algorithm for validating the enhanced data, utilizing the HyperPOR consensus algorithm within the Blockchain framework. The HyperPOR algorithm functions by confirming the identity of the business partner. The generation block then validates and accomplishes distributed computing and adds sharding technology for protecting the Patient Health Records (PHR). Nguyen et al.[44] proposed an intrusion detection system to protect data transmission in the Cyber-Physical system for healthcare.

Most of the time, patients have little control over who can access their medical records and are ignorant of the full worth of the information they possess. Mamoshina et al.[11] presented a Blockchain and AI-based solution to speed up biomedical research to provide patients with new technologies for controlling and profiting from their personal information and incentives to undertake periodic health checkups. They have proposed Exonum as a permissioned Blockchain framework wherein patients can sell their health records using tokens. Nonetheless, this structure lacks authority once the data is transferred to regulatory entities. Jennath et al.[45] put forward a dependable hybrid AI-Blockchain framework for e-health. They employed an unchangeable distributed ledger to document the origin of individual permissions and the credibility of data origins, serving the purpose of constructing and refining the AI model.

Rahman et al.[46] used Blockchain and off-chain to safeguard from manipulation and illegal access, bringing confidence to the provenance of datasets and distributed models to protect the privacy and security of the Internet of Health Things (IoHT) data. The insecure central gradient aggregator is replaced with a secure, tamper-proof gradient mining and distributed consensus-based aggregator in the Blockchain. The edge training, trust management, and authentication of participating federated nodes, the dissemination of globally or locally trained models, and the identity of edge nodes and their contributed datasets or models are managed by Smart Contracts. This system provides the complete encryption of both, a dataset and a trained model. Puri et al.[47] implemented a decentralized healthcare framework powered by AI that accesses and authenticates Internet of Things (IoT) devices while instilling confidence and transparency in the PHR. The technique is based on AI-enabled Smart Contracts and the development of a Public Blockchain network. In addition, this framework detects potentially dangerous IoT nodes in the network. Gupta et al.[48] offer BITS, a unique intelligent TS system based on Blockchain. They provide thorough insights into the Cloud-based and Blockchain-based smart TS frameworks, emphasizing the challenges of security, dependability, confidentiality, and data management. If rogue devices start communicating erroneous local model updates, the global model's accuracy will be skewed. Here, Blockchain can assure that the local updates in Federated Learning come from trusted devices. The presence of local modifications within the Blockchain aids in additional validation of the precision of the acquired model. Polap et al.[49] introduced a Federated Learning approach that merges decentralized learning with Blockchain-driven security, offering a resolution for constructing intelligent systems using locally stored data in a decentralized manner to enhance the security and confidentiality of the Internet of Medical Things. This approach serves as a countermeasure against model poisoning attacks. The study in Reference 50 stated a way for training a global model cooperatively utilizing Blockchain technology and Federated Learning while maintaining anonymity in detecting Covid-19 patients using CT images.

Technological advances, such as distributed learning, provide a road ahead, but they are plagued by a lack of openness, thereby reducing trust in the data utilized for analysis. To solve these challenges, Zerka et al.[51] have projected that Chained Distributed Machine Learning (C-DistriM), a novel distributed learning that blends sequential distributed learning with a Blockchain framework would be developed in medical imaging. Blockchain is used to record the immutable history of computation and protect from the threat of model poisoning. After training, it encrypted the local models and uploaded them on the cloud simultaneously, by the removal of all local copies of the model. Subsequent to this, unapproved users are prevented from accessing the cloud by the Smart Contract. Kuo et al.[52] introduced the Explorer Chain framework, which integrates two cutting-edge technologies, Online Machine Learning and a decentralized Blockchain, to develop a predictive model across multiple institutions within a distributed structure, eliminating the necessity for sharing patient-level data or relying on a central coordinating node.

Many published deep learning systems lack clarity about model validation and testing outcomes. Blockchain technology could potentially provide a suitable solution to these issues by functioning as a decentralized, secure, and reliable distributed ledger for data administration. It also offers the ability to track and ensure accountability for the reporting of testing results. Schmetterer et al.[53] implemented a Blockchain-driven AI platform to establish real-world data transmission, model transfer, and model testing across three locations in Singapore and China, demonstrating the proof of concept. The researchers aimed to develop and assess deep learning algorithms for the identification of myopic macular degeneration and extreme myopia, utilizing retinal images from diverse multiethnic populations across various countries. They leveraged a blockchain-enabled AI infrastructure that helps to have secure, persistent, and verifiable data transmission, model transfer, and transparency in the diagnostic performance of deep learning algorithms. However, it does not maintain the privacy of data.

Khan et al.[54] explored a wireless capsule endoscopy frame-based automated method for detecting stomach infections. A Blockchain-based technique is used in a convolutional neural network (CNN) model to secure the network for the precise identification of stomach ailments such as ulcers and bleeding. Each layer comprises an additional block that keeps certain information to resist all tempering and modification attacks. Pilozzi et al.[55] state that AI technologies, particularly NLP, are effective tools for classifying the emotions and tonality of texts, like in social media posts. These approaches could be used to investigate the public perception of Alzheimer's disease. The incorporation of secure and decentralized data transfer and storage methods like Blockchain will give patients greater control over their data. It will help to relieve most of the insecurities of mistakenly revealing the personal information of a patient to an entity that may discriminate against the patient.

Figure 8 gives an overview of the past work on Blockchain for AI-based healthcare. It represents the type of Blockchain used for the different modalities of data. There are three types of Blockchains, namely Public, Private, and Consortium Blockchains. Ethereum is often preferred for Public Blockchains, while Hyperledger Fabric and Hyperledger Sawtooth are often preferred for Private Blockchains. This survey is focused on text, image, and audio modality of data in healthcare systems. The survey found that no specific work was done in Blockchain for acoustic AI. Table 6 provides the overview

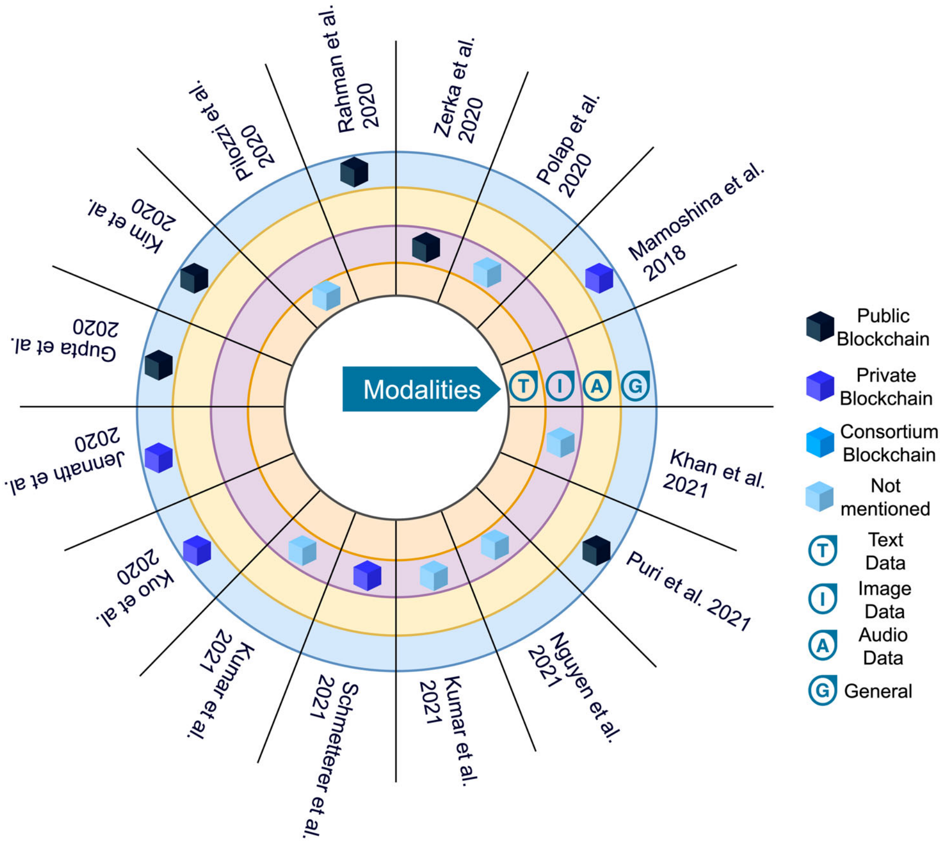


FIGURE 8 Blockchain for AI healthcare—types of Blockchain and data modalities.

TABLE 6 Existing literature in Blockchain for AI healthcare.

Sr. no.	Ref.	Year	Goal	Implementation	A novel Blockchain framework	Smart contract	Consensus algorithm	Type of Blockchain	Performance evaluation	Limitations	Future scope
1	11	2018	To propose a Blockchain-based secure and distributed personal data marketplace for DL technologies in healthcare.	×	✓	✓	✓	✓	×	The proposed solution does not protect data leakage, once it has been sold.	Blockchain featured AI data marketplace can create advanced research and treatment capabilities in healthcare.
2	49	2020	Security and privacy of the Internet of Medical Things with Blockchain.	In progress	×	×	×	×	×	No proper architecture is suggested for Blockchain in Federated Learning.	Experimentation can be expanded for the different types of data and classifiers.
3	51	2020	To promote transparency and confidence in multi-centric research and eventually to speed up AI adoption.	✓	✓	✓	✓	✓	✓	Not mentioned	To explore how C-DistriM behaves when fraudulent collaborators are deliberately introduced to the network.
4	46	2020	To protect the privacy and security of Internet of Health Things (IoHT) data.	✓	✓	✓	✓	✓	✓	GPU computation memory may be a problem for professional cloud providers' trusted execution environment enclaves.	To improve enclave computing in the future.
5	55	2020	To review the technologies like AI and Blockchain that can overcome Alzheimer's disease stigma.	×	×	×	×	×	×	Not mentioned.	AI and Blockchain can prove invaluable in fighting Alzheimer's disease stigma.
6	43	2020	To employ Artificial Intelligence Blockchain algorithms to enable secure PHR data verification and accurate medical data verification in the medical institutions.	✓	✓	✓	✓	✓	✓	Blockchain technology is in its early stages.	The post-commercial aspect should be evaluated to make the system safer and easier to use for the individuals.

(Continues)

TABLE 6 (Continued)

Sr. no.	Ref.	Year	Goal	Implementation	A novel Blockchain framework	Smart contract	Consensus algorithm	Type of Blockchain	Performance evaluation	Limitations	Future scope
7	48	2020	To resolve security, privacy, and trust issues in Telesurgery.	✓	✓	✓	×	✓	✓	5G may introduce a delay in communication.	To identify the challenges and issues in the real-life implementation of the proposed framework.
8	45	2020	To address the security and privacy of existing e-Health systems.	✓	✓	✓	✓	✓	✓	The system incorporates limited data management capabilities.	Patient mobility and access permission strategies need to be addressed in the future.
9	52	2020	To provide an alternative solution based on a decentralized approach for healthcare AI models.	✓	✓	✓	✓	✓	✓	There seem to be many conflicting views and misunderstandings regarding Blockchain technology and its possible benefits in healthcare and Genomics, as there are many unanswered issues.	To explore the future of Blockchain technology in healthcare and Genomics applications.
10	42	2021	To maintain privacy while allowing an exchange of information to detect lung cancer using CT images.	✓	×	✓	✓	×	✓	Not mentioned.	Not mentioned.
11	53	2021	To develop an algorithm with the management of a variety of datasets available from many nations and centers.	✓	×	✓	✓	✓	✓	Due to the lack of several images with specific lesions, the developed algorithm can detect the presence or an absence of myopic macular degeneration except its categories. It does not maintain the privacy of data.	Widespread adoption of Blockchain with Deep Learning might have far-reaching impacts on AI research in medicine.

(Continues)

TABLE 6 (Continued)

Sr. no.	Ref.	Year	Goal	Implementation	A novel Blockchain framework	Smart contract	Consensus algorithm	Type of Blockchain	Performance evaluation	Limitations	Future scope
12	50	2021	To address the issue of data sharing among hospitals like privacy and security in case of the training model for detecting Covid-19 patients, using CT images.	✓	×	✓	✓	×	✓	Not mentioned.	Not mentioned.
13	44	2021	To build intrusion detection system, using Blockchain-enabled data transmission and classification algorithm in healthcare.	✓	×	×	×	×	✓	Not mentioned.	The system performance can be increased with the use of Hyper-parameter tuning techniques and a learning rate scheduler.
14	47	2021	To resolve single-point failure, security, privacy, and non-transparency issues with the data in the remote patient monitoring.	✓	✓	✓	✓	✓	✓	Not mentioned.	It is possible to do research on trustworthy AI using the suggested framework to improve the reliability of the system and build more lightweight algorithms to reduce the cost of energy and gas.
15	54	2021	To address the patient information privacy and time-consuming, costly inspection of stomach abnormalities.	✓	✓	✓	×	×	✓	Not mentioned.	Secure CNN may be made more secure by utilizing various hashing algorithms, and sophisticated integration of layer ledger blocks with CNN.

of existing work done in Blockchain for AI healthcare systems that considers their objectives/goals, implementation and performance evaluation, limitations, and future scope.

5 | THE ATTACK SURFACE OF ARTIFICIAL INTELLIGENCE

Machine learning is a data processing technique that automates the development of analytical models. It is a subfield of AI that is focused on the principle that computers can learn from data, recognize patterns, and make decisions excluding human involvement. These tasks require obtaining the validated data, using which the classifiers are trained. After successful training, the model is deployed. It might proceed with retraining and feedback loops for performance improvement. Figure 9 shows the different phases involved in the successful deployment of the AI model. It starts with the data collection and its preparation for training by looking for bias or labeling the data. Then, based on the requirement of the application that is being studied, the classifier is either developed or selected from existing ones. A classifier is trained for the acquired dataset and can be further improved by adjusting the parameters. The trained model is deployed at the end, and the model will proceed with retraining for performance improvement and enhancement.

An attack on a device or an information system is any action to reveal, change, disable, damage, capture, or collect information by exploiting the vulnerabilities available in the system. The basic security requirement for any system is maintaining the privacy of sensitive data or processes, getting untampered data or processes, and allowing data or processes to be available to an intended user at any time. Henceforth this CIA (Confidentiality, Integrity, Availability) triad applies to the phases mentioned above for securely deploying the ML model. Figure 10 focuses on the attack surface of AI. Data, classifier/algorithm, and learned model are the targeted areas for imposing attacks by any adversary in any AI-based systems.

5.1 | Data

The most critical component of AI is data. Any model cannot be trained without data, and all current technological development will be for naught. There is an enormous investment of money only to collect specific data as much

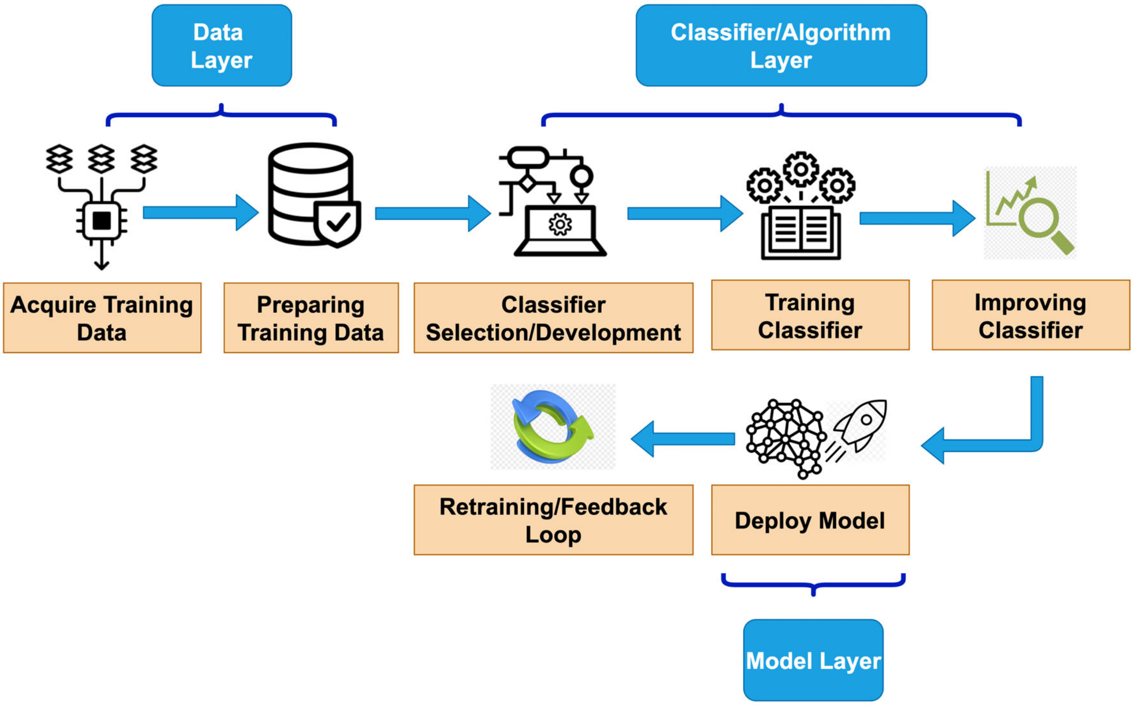


FIGURE 9 Phases involved in deploying AI models.

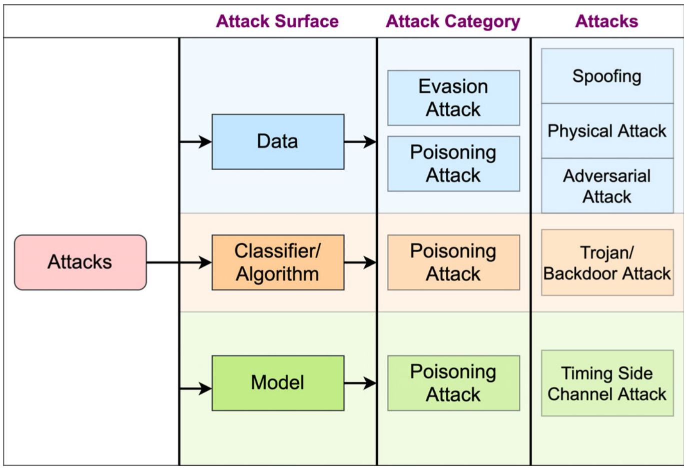


FIGURE 10 Attack surface of AI.

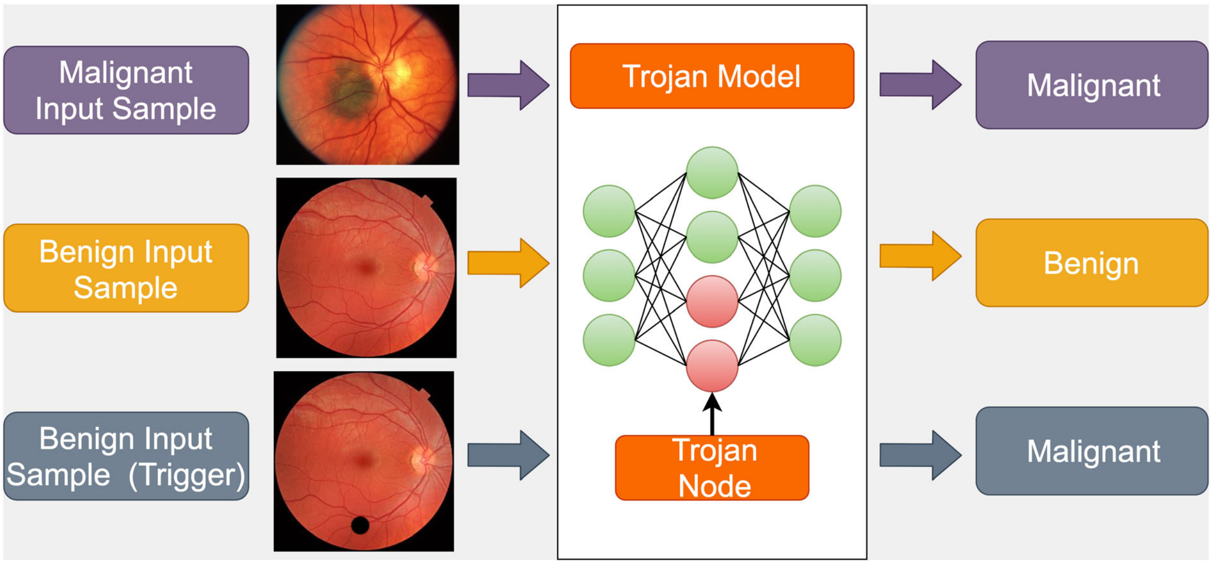


FIGURE 11 Trojan attack.

as possible. Targeting data for the attack has a drastic impact on AI-based systems. The integrity of data can be undermined during either the training or testing stages by exploiting the AI models' susceptibility to minor input variations, resulting in abnormal model behavior referred to as poisoning and evasion attacks. These attacks can be facilitated by spoofing,[56] which involves deceptive tactics by an adversary to deceive computer networks by posing as a legitimate entity, utilizing computers, devices, or networks. The malicious opponents frequently lack access to the training phase of the model. They create an adversarial input to deceive a classifier or elude detection from a neural network during the testing phase. These can be either physical or digital types of attacks. This study focuses on digital types of attacks. A digital approach directly imparts tiny perturbations in the input. In this scenario, the assailant can manipulate the specific system without triggering any alerts from the intrusion detection mechanism. Evasion attacks can also result in a concept drift.[57] Potential aggressors might additionally infiltrate the training dataset and introduce malicious samples, referred to as poisoning attacks, thereby contaminating the dataset. Adversarial attacks in AI-based healthcare systems have the potential to harm human beings, as discussed in the subsequent sections.

5.2 | Classifiers/algorithms

5.2.1 | Trojan/backdoor attack

A Trojan attack compromises the genuine model by inserting a backdoor into the neural network, activated with a specific pattern in the testing sample. A Trojan attack targets the origin of vulnerabilities in a neural network like data, algorithm, and program or hardware. It will modify the network with a compromised dataset.[58] At the time of the training phase, neural Trojans are injected into the network.[59] Trojan attacks are different from adversarial attacks, although both take place only during the training phase. It does not force the neural network to modify itself in the case of an adversarial attack; rather it merely affects the result. However, in a Trojan attack, poisoned input samples compel the network to modify itself to work with the accuracy of the benign input samples. It will malfunction only when it is triggered by a Trojan. It is difficult for a user to identify the Trojan attack.[60] A Stealthy Poisoning Attack (SPA) depends on a Generalized Adversary Network (GAN) which can lead to a Trojan attack.[61] Badnet[62] is also an example of a neural Trojan attack. Figure 11 depicts the scenario of a Trojan attack.

5.3 | Models

I. Timing side-channel attack

The characteristics of neural networks for having different times for execution based on the depth of the network make it vulnerable to attacks like Timing Side Channels. An adversary can conclude with the number of layers, the depth of the neural network, by observing the time required for generating the output by the model. This adversary uses a regressor, trained using different execution times along with the respective number of layers in the network. This information is then utilized to mimic substitute models with similar functionalities to the original network.[63] Information about the CNN model can be leaked using reverse engineering of structure and weights with the help of memory and timing side-channel attacks. The memory access patterns explode the vital features of a neural network such as the total number of layers, the size of the layer, and their dependencies.[64]

6 | NATURAL LANGUAGE PROCESSING (NLP)

The important aspects of NLP are expounded in this section.

6.1 | NLP techniques

I. Named entity recognition

The most fundamental method in NLP is retrieving entities from the text. It emphasizes the key topics and connections in the text. Named Entity Recognition (NER) extracts entities from the text such as persons, places, organizations, and dates. Grammar rules and supervised models are commonly used.

II. Sentiment analysis

Sentiment Analysis is the most used approach in NLP. Sentiment analysis is particularly effective when individuals express their thoughts and feedback, such as through customer surveys, reviews, and social media comments. The most basic result of sentiment analysis is a three-point scale: positive/negative/neutral. The result can be a numerical score grouped into as many categories as the user desires in more sophisticated instances.

III. Text summarization

This NLP method aids in the summarization of lengthy passages of text. Text summarization is commonly utilized in situations such as news articles and research articles. Extraction and abstraction are two major techniques for text summarization. The extraction methods generate a summary by extracting pieces of writing. The abstraction approaches provide a summary by producing new texts that express the essence of the original material.

IV. Aspect mining

Aspect mining identifies the various perspectives in a text. It retrieves complete information from the text that can be used in combination with sentiment analysis. Part-of-speech tagging is one of the simplest ways of aspect mining. When aspect mining and sentiment analysis are applied to a text, the outcome reveals the whole intention of the text.

V. Topic modeling

One of the more difficult approaches for identifying natural concepts in the text is topic modeling. The fact that topic modeling is an unsupervised approach is a significant benefit. There is no need for model training or a labeled training dataset.

6.2 | NLP applications in healthcare

There are many inputs to Clinical Decision Support Systems (CDDS) like semi-structured data, such as XML documents or two-column laboratory results, structured data such as Electronic Health Records (EHR), and narrative text, and unstructured data such as patients' clinical findings, radiology reports, and operative notes. Several solutions have been proposed that NLP techniques should be used with unstructured data as input to support clinical decisions, especially to compute and automate diagnoses or treatments. NLP provides adequate mechanisms for the automated extraction of important facts from free text, which CDSS uses to generate the results and recommendations provided to healthcare professionals to assist them in the best decision-making process.[65–67] The clinical notes, including patients' health history, are crucial assets for resolving sensitive clinical problems that may be difficult to access from other EHR components, like lab results. NLP makes it easy to retrieve meaningful features from clinical notes that can be used to build machine learning models. Unified Medical Language System (UMLS) resources and clinical notes become effective and valuable tools with NLP for predicting the mortality in diabetic patients in the critical care environment. However, more research databases and patient cohorts are needed to test the model.[68] A sentiment scoring algorithm, also known as opinion mining, has been used to determine sentiment from a repository of narrative hospital admission and discharge statements.[69] NLP makes it possible to identify and extract the important features from radiology reports which are in unstructured form and convert them into manageable computer formats.[70] The supervised machine learning-based NLP approach is based solely on the content of clinical notes to identify its medical subdomain. It can assist clinical experts in promptly directing patients' unresolved problems to the appropriate healthcare professionals and experts.[71] NLP finds utility in researching viral transmission, ocular manifestations, and treatment trajectories for ophthalmology patient care through the analysis of COVID-19 ophthalmology-related literature.[72] In fields like gastroenterology, NLP has the potential to bring about transformative changes by scrutinizing extensive volumes of narrative medical reports.[73] Within the context of Kawasaki disease (KD), an NLP model known as KD-NLP demonstrated noteworthy enhancements in comparison to manual chart analysis by clinicians, aiding in the identification of pediatric emergency department patients with a heightened likelihood of having Kawasaki disease.[74] A hybrid NLP framework, adept at extracting information about Adverse Drug Effects (ADE) and medication-related insights, has practical applications in real-world scenarios, facilitating scientific decisions concerning ADEs and drugs.[75] Additionally, a chatbot system integrated with NLP, endowed with knowledge about various diseases, can comprehend user inquiries and provide suitable responses.[76] The widespread adoption of deep learning in clinical NLP is substantiated by the surge in medical data, signifying its broad acceptance.[77] NLP has been used in recent research to classify diseases and disorders that are hard to diagnose, using only clinical gestalt. Information Retrieval (IR) takes less time and effort when NLP-based solutions are used, which ultimately fosters the treatment.[78,79]

6.3 | Adversarial attacks on NLP and defense

Adversarial text is a perturbation in the text regarding semantics, syntax, and visual similarity which will mislead NLP. Figure 12 depicts the methods for generating adversarial text. The adversarial examples in the text can be a tiny attempt to modify minimum characters and create genuine typing errors comparable to those made by humans to affect the prediction of models. This attack keeps the sequence of appearance of text very close to the original one. The attacks like DeepWordBug,[80] Hotflip,[81] and Textbugger[82] come under this approach of attack. Another approach to generating adversarial text depends on paraphrasing the original text. This attack will generate the semantical equivalence of the original text, but the model output will be different for the original and paraphrased text. Alzantot,[83] Bae,[84] Bert-attack,[85] IGA,[86] PWWS,[87] Textbugger,[82] and Textfooler[88] are some attacks that generate adversarial text under the mentioned approach. Textbugger is the combination of both approaches for targeting adversarial attacks on NLP.

Figure 13 illustrates the toxic effect of an adversarial attack on NLP-based healthcare applications. The NLP can be fooled by just replacing the words with their synonym while maintaining the semantics of the text. The wrong prediction of the severity of the disease ultimately leads to the administering of incorrect treatment and puts lives at risk. Table 7 gives an overview of the adversarial attacks on text.

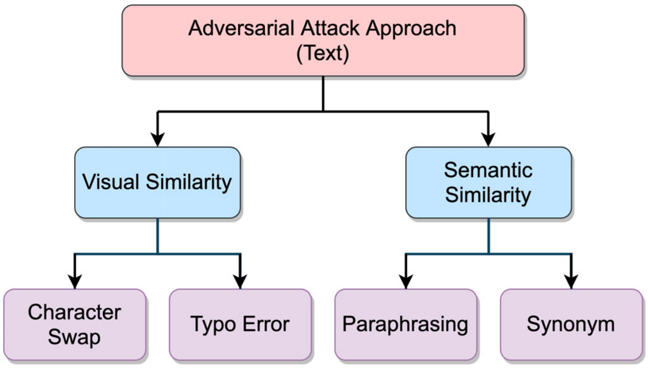


FIGURE 12 Taxonomy of adversarial attack on text.

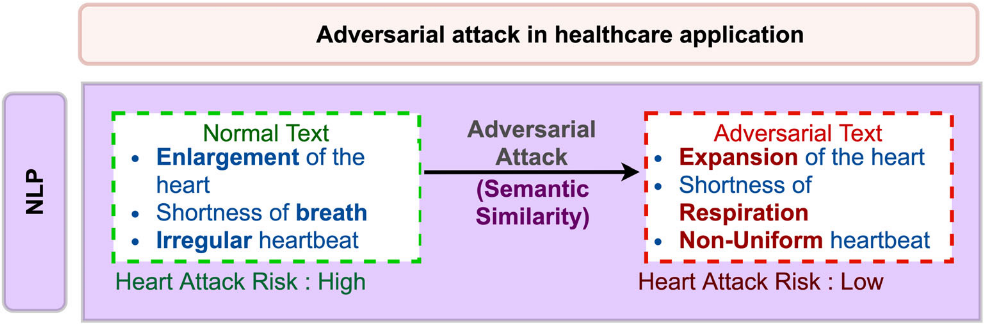


FIGURE 13 Adversarial attack on NLP-based healthcare applications.

TABLE 7 Adversarial attacks on NLP.

Approach	Attack	Threat model	Perturbation	Target model
Visual similarity	DeepWordBug	Black box	Character level	Word-LSTM, Char-CNN model
	Hotflip	White box	Character level, word level	CNN
	Textbugger	White box/black box	Character/word level	LR, CNN, LSTM
Semantic similarity	Alzantot	Black box	Word level	LSTM
	Bae	Black box	Sentence level	Word-LSTM, Word-CNN
	Bert-attack	Black box	Word level	CNN
	IGA	Black box	Word level	Word-CNN, LSTN, Bi-LSTM
	PWWS	Black box	Word level	Word-CNN, Char-CNN, LSTN, Bi-LSTM
	Textfooler	Black box	Word level	Word-CNN, Char-CNN, LSTN

TABLE 8 Defense techniques for adversarial attacks on NLP.

Adversarial attack	Defense technique	Accuracy	Limitation
DeepWordBug	Adversarial training	62%	A new class of attacks makes adversarial training-based defense vulnerable.
HotFlip	Adversarial training	69.32%	The discrete property of texts makes it difficult to broaden the categories of attacks covered during training.
TextBugger	Adversarial training	>75%	A new class of attacks makes adversarial training-based defense vulnerable.
IGA	Synonym Encoding Method (SEM)	>50% and <87% depending on dataset and network model	Works better for only Greedy Search Algorithm, PWWS, Genetic Algorithm, and IGA attacks
PWWS	adversarial Training	80%	Defense is limited to PWWS attack.

Table 8 depicts the defense techniques for the adversarial attacks on the NLP model and their limitations. Adversarial training has been observed to be the most robust defense technique for a particular adversarial attack on the NLP model.

7 | COMPUTER VISION

In this section, an overview of computer vision, the important techniques related to computer vision, and the applications of computer vision in healthcare systems are presented.

7.1 | Computer vision techniques

I. Image classification

A collection of images labeled with a specific category is available, and the objective of this task is to forecast these categories for a new set of test images and assess the accuracy of those predictions. This job has several difficulties, including perspective variation, size variation, intra-class variance, image distortion, image occlusion, lighting conditions, and backdrop clutter.

II. Object detection

Defining objects inside pictures often entails producing bounding boxes and labels for each item. This procedure varies from the classification/localization job in which the classification and localization are applied to many items rather than to a single dominating object. There are only two types of object classification: object-bounding boxes and non-object-bounding boxes.

III. Object tracking

The practice of following a particular object of interest, or several objects in each scene, is referred to as object tracking. Historically, it has been used in video and real-world interfaces, where the inspections are performed after initial object identification.

IV. Semantic segmentation

The technique of segmentation, which splits the whole picture into pixel groupings, that may subsequently be labeled and categorized, is essential to computer vision. Semantic segmentation attempts to grasp the semantic role of each pixel in a picture. The bounds of each item must also be defined. As a result, unlike categorization, detailed pixel-by-pixel predictions from our models are required.

V. Instance segmentation

Instance segmentation goes beyond semantic segmentation by segmenting various instances of classes. There is usually a picture with a single item in the center of classification, and the objective is to identify that image. However, considerably more complicated activities must be done to segment the instances. Complex scenes with many overlapping items and diverse backgrounds are observed, and it not only classifies these things but also recognizes their borders, distinctions, and relationships with each other.

7.2 Computer vision applications in healthcare

Intelligent intervention using a brain-like structure aids in the understanding and analysis of different forms of dynamic data using cutting-edge technologies such as deep learning and computer vision.[89] Computer vision is a scientific form of deep learning, whereby it detects objects from captured series of videos and images. Deep learning algorithms known as CNNs are designed to process image data and assign importance to various aspects to distinguish one image. CNNs have a structural architecture like the connectivity pattern of neurons in the brain. In object classification activities, state-of-the-art computer vision accuracy outperformed humans in terms of accuracy. The National Cancer Institute's National Lung Screening Trial (NLST) found that lung cancer screening with low-dose CT scans has reduced mortality rates by 20%.[90] The ImageNet Large-Scale Visual Recognition Challenge (ILSVRC) brought together a large group of deep learning researchers, who competed and collaborated to develop strategies for a variety of computer vision tasks.[91] Computer vision has a longstanding experience of allowing computers to meaningfully interpret visual imagery. Identifying the type of an object in an image, the position of present objects and both type and location simultaneously are referred to as object classification, localization, and detection, respectively.[92] Progress in computer vision and deep learning has elevated the efficiency of intelligent monitoring. A novel system leveraging computer vision and deep learning for posture monitoring is presented, enabling the prediction of physical irregularities related to Generalized Anxiety Disorder (GAD) in individuals within their work environment.[93] Concurrently, initiating early and frequent patient mobilization has been shown to lower the likelihood of post-intensive care syndrome and long-term cognitive impairment. In an adult ICU, computer vision algorithms identify patient mobilization activities like moving the patient into and out of bed and into and out of a chair.[94] Deep CNNs provide a significant opportunity as a diagnostic tool for otologic prognosis based on otoscopic ear images.[95] Researchers combined computer vision approaches with deep learning neural network techniques to create a comprehensive image processing model to predict human embryo viability.[96] Automated herbal medications based on tongue images are possible with deep learning to investigate the relevance of the tongue with herbal medication.[97] Using a deep learning-based automated platform to test diabetic retinopathy (DR) from color fundus images may offer an alternative approach to reducing medication errors. A deep learning-based automated tool has significant advantages in cutting down screening rates, increasing healthcare coverage, and ensuring early treatment.[98,99] The Confidence-Aware Anomaly Detection (CAAD) model considered a feature extractor, an anomaly detection module, and a confidence predictor module for detecting viral pneumonia from chest x-rays may be of considerable use for large-scale screening and infection control.[100] Hip fractures from pelvic x-rays can also be detected using a computer vision algorithm.[101] An innovative CNN approach for rapidly and accurately detecting esophageal cancer, encompassing squamous cell carcinoma and adenocarcinoma, has been developed to analyze recorded endoscopic images.[102] Deep learning algorithms enable the automatic identification of IntraCranial Hemorrhage (ICH) and its variations from non-contrast head CT scans.[103] Diagnostic outcomes can be derived from chest CT images through a swift and automated deep learning algorithm.[104] To mitigate the risk of doctor-patient cross-infection and prevent the spread of the COVID-19 virus, a pioneering visual SLAM algorithm has been devised for tracking and locating robots in dynamic situations.[105]

7.3 Adversarial attacks on computer vision and defense

Adversarial images are those wherein the pixels are intentionally perturbed to confound and fool models. They seem innocuous and benign to human eyes at the same time. Adversarial images mislead DNNs as a minute perturbation

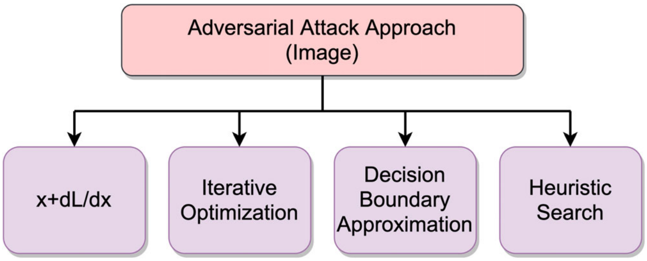

Adversarial Attack Approach (Image)
x+dL/dx
Iterative Optimization
Decision Boundary Approximation
Heuristic Search

FIGURE 14 Taxonomy for adversarial attack on images.

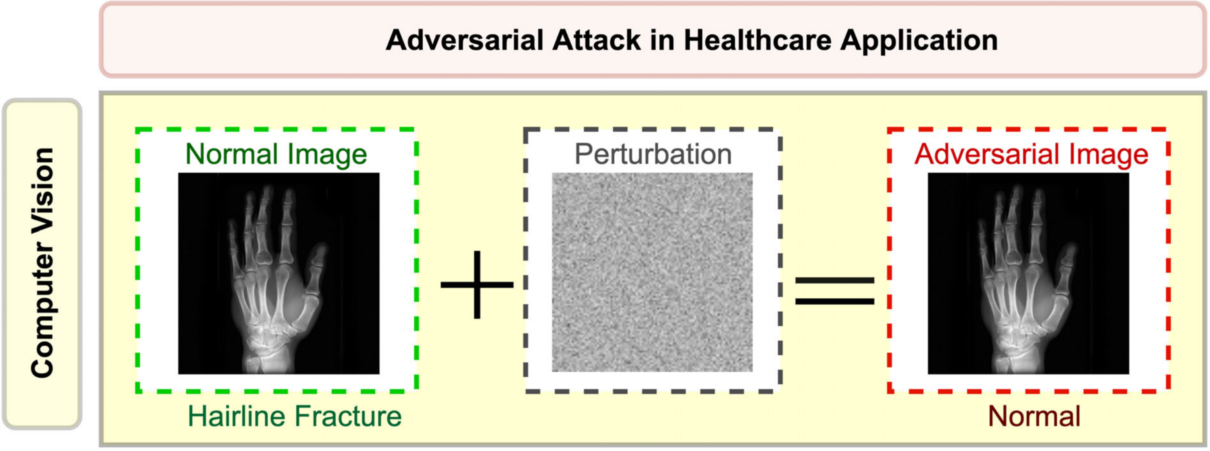


FIGURE 15 Adversarial attack on computer vision-based healthcare application.

in the input makes DNNs vulnerable. Figure 14 represents the approaches for an adversarial attack on an image. Some approaches for an attack depend on the first-order derivative by computing the derivative of the loss, concerning input for targeting an increase in the loss, for example, FGSM,[106] BIM,[107] and R + FGSM.[108] The other attacks depend on an incremental optimization procedure on the multiple goal objective functions, allowing an attacker to include additional hostile criteria into the targeted function, for example, L-BFGS,[109] C&W,[110] ATN,[111] stAdv,[112] Deepfool, and Universal Adversarial Perturbations (UAP). An adversary may benefit from the transferability property of adversarial samples to attack a black box model by targeting a substitute model trained using a labeled dataset of the black box model, for example, a substitute black box attack.[113] Another black box approach is based on crawling closer to the decision boundary within adversarial input and non-adversarial input, for example, boundary attacks.[114]

Figure 15 reflects the adversarial effect of adding some perturbation in the original hand x-ray image. Though the perturbed image is identical to the original image from human perception, the AI model interprets the wrong result after processing. For example, the adversarial attack changes the prediction from a hairline fracture to normal. Table 9 gives the details of the adversarial attacks on the image.

Table 10 highlights the advantages and disadvantages of defense techniques designed to mitigate different adversarial attacks on computer vision models. It has been identified that the defense technique can handle only a particular kind of attack. Adversarial training and other techniques each have their limitations. Hence, framing a global solution to mitigate all types of adversarial attacks is a challenging task.

8 | ACOUSTIC AI

In this section, an overview of acoustic AI and its applications in healthcare systems will be presented.

TABLE 9 Adversarial attacks in computer vision.

Approach	Attack	Distance metric	Threat model	Objective
Derivative function	FGSM	L_∞	White box	Targeted attack
	BIM	L_∞	White box	Non-targeted attack
	R + FGSM	L_∞	White box	Targeted attack
Iterative optimization	L-BFGS	L_∞	White box	Targeted attack
	C&W	L_0, L_2, and L_∞	White box	Targeted attack
	ATN	L_∞	White box	Targeted attack
	stAdv	NA (spatial location-based)	White box	Targeted attack
	UAP	L_1, L_∞	White box	Targeted attack
	Deepfool	L_2	White box	Non-targeted attack
Decision boundary approximation	Boundary attack	NA (decision based)	Black box	Targeted/non-targeted attack
Heuristic search	Substitute model	NA	Black box	Targeted attack

TABLE 10 Defense techniques for the adversarial attacks on computer vision.

Defense technique	Advantages	Disadvantages
Adversarial training[115,116] 1. FGSM adversarial training 2. Adversarial Logit Pairing 3. PGD adversarial training 4. Ensemble adversarial training	It achieves state-of-the-art accuracy on several benchmarks.	It will fail for the data outside the training set/new attack.
Randomization[115] 1. Random input transformation 2. Random noising 3. Random feature pruning	Best results for black-box and gray-box settings.	Not effective in white-box setting.
Denoising[117] 1. Conventional input rectification 2. GAN-based input cleansing 3. Auto encoder-based input denoising (MagNet) 4. Feature denoising	It can mitigate the C&W attack.	EAD and CW2 can bypass the input squeezing system with an increasing adversary strength. Adaptive white-box CW2 attack can easily defeat APE-GAN. MagNet is vulnerable to the transferable adversarial samples generated by the CW2 attack. HGD is compromised by a PGD adversary under a white box setting.
Provable defenses[117] 1. Semi definite programming-based certificated defense 2. Dual approach-based provable defense 3. Distributional robustness certification	It maintains certain accuracy under a well-defined class of attacks.	Scalability has been a common problem shared by most of the certificated defenses.
QR Code[118]	An alteration in the dataset is easily identified.	The storage requirement increases linearly with the number of images in the dataset.

8.1 | Acoustic AI techniques

I. Selective noise canceling

AI Noise Canceling technology improves the headset microphones by removing background noise, resulting in crystal-clear online audio conversation. A processor with AI-enhanced profiles eliminates more than 50 million different forms of background noise while maintaining speech harmonics.

II. Hi-Fi audio reconstruction

Recently, there has been a surge of interest in utilizing deep neural networks to perform up sampling on raw audio waveforms. The neural networks are trained to infer additional time-domain samples from an audio signal, equivalent to the picture super-resolution issue, in which individual audio samples are analogous to pixels. It is possible to train a network to generate realistic audio by teaching the method of the normalcy of the recording sound.

III. Analog audio emulation

It involves calculating the complicated interactions of non-linear analogue audio components. It investigates how a deep neural network can learn the lengthy temporal dependencies that define these effect units with the possibility of matching non-linearities within the audio effects using convolutional, recurrent, and fully connected layers. It investigates linear and non-linear time-varying emulation as a content-based transformation without explicitly finding the time-variant solution.

IV. Speech processing

The computer receives input data of sound vibrations in speech recognition. This is accomplished by employing an analogue to digital converter, which transforms the sound waves into a digital format that can be comprehended by the computer. Advanced speech recognition in AI also includes AI voice recognition in which the computer can recognize the voice of a specific speaker.

V. Improved spatial simulation

An improved spatial simulation is used for binaural processing and reverb. Binaural processing in hearing equipment typically employs device communication to recognize and improve the loudest speech signal in the environment. Reverb is caused by sound reflecting and echoing off walls, floors, ceilings, or other surfaces.

8.2 | Acoustic AI applications in healthcare

The "Firefly" app is an application framework and underlying Software Development Kit (SDK), which uses advanced Digital Signal Processing (DSP) technology and AI algorithms to detect sleep cycles, respiration rate, snoring, and Obstructive Sleep Apnea (OSA) patterns, which are then used to measure the precise respiratory rates of a human in bed via smartphones. This application combines Active Sonar with Passive Acoustic Analysis.[119] In Reference 120, the spectral analysis of acoustic signals was used to measure feature vectors and was validated using a series of machine learning methods to provide the most efficient identification of cardiac valve defects based on heart sounds, and this study proved that the CNN model is an effective method for increasing efficiency. A new method of automated sound processing based on neural networks has been introduced in a framework that captures respiratory sounds using an electronic stethoscope. It can recognize four types of auscultatory sounds: wheezes, rhonchi, and fine and coarse crackles which led to a reduction in human errors during auscultation examination.[121] In the studies conducted in References 122,123, deep learning-based classification models and techniques that classify respiratory sounds based on mel-spectrograms were developed to classify breathing sound anomalies (e.g., wheeze, crackle) for the automatic diagnosis of respiratory and pulmonary diseases, and these were proven to be efficient methods. In Reference 124, audio characteristics of coughs were used to build classifiers that can differentiate various respiratory disorders in adults.

In addition, recent developments in generative adversarial networks were used to balance and expand a dataset by adding brilliantly constructed synthetic cough samples for each type of serious respiratory disease. CoughGAN creates simulated coughs that reflect significant pulmonary symptoms to aid physicians and predictive algorithms in the detection of the early stages of lung disease. Thus, clinical experts can establish the right preventative treatment plans and reduce morbidity through early and accurate detection of advanced respiratory conditions like chronic obstructive pulmonary disease and emphysema. A lot of studies have used various types of neural networks for AI-based classification of respiratory sounds. The study in Reference 125 proposed a Noise Masking Recurrent Neural Network (NMRNN) for respiratory sound classification, the work in Reference 126 used the Support Vector Machine (SVM) model for pediatric breath sound classification,[126] while the study in Reference 127 used a back-propagation neural network for the detection of lung sound signals. In Reference 128, a convolutional recurrent neural network (CRNN) with a reinforcement learning (RL) agent was proposed for lungs auscultation examination, whereas a novel CNN architecture called the N-CNN model was used in conjunction with the VGG-16 and ResNet50 CNN architectures to measure the pain in new-borns on based on crying sounds in Reference 129. The findings of the experiments showed that using the N-CNN model for measuring pain in neonates has significant therapeutic value and has proven to be a good alternative to conventional evaluation methods.

8.3 | Adversarial attacks on acoustic AI and defense

Adversarial audio is sound with perceptible noise, that is, adversarial perturbations, which can deceive a range of sound classification systems. Figure 16 represents the taxonomy for an adversarial attack on audio signals. Some attacks target generating an adversarial audio sample that seems very similar to the original one, but the learned model would result in the wrong classification. These attacks come under speech-to-label kind of attacks. The assailant has the ability to employ gradient-free genetic algorithms to create adversarial audio samples, utilizing the initial audio input and the intended output label. This process introduces random noise while ensuring it remains imperceptible to humans.[130] The manipulation of advanced learning systems with imperceptible audio alterations is enabled through a novel technique named Houdini, utilizing a Probabilistic Loss Function.[131] Additionally, an adversary may seek to manipulate acoustic processing during speech-to-text conversion in order to achieve the desired output. These attacks are known as Speech-to-Text attacks. Mel Frequency Cepstral Coefficients (MFCC) parameters of the input audio signal can be modified, and then it will be reconstructed with reverse MFCC applied to the genuine extracted features.[132] Changing the audio spectrum into the desired transcript can be changed by merely adding a small distortion using optimization-based attacks.[133]

Figure 17 shows that after processing the audio signal of the cough sound that is perturbed by adding frequency, it changed the prediction from normal cough to bronchitis. These adversarial attacks spoil the integrity of the AI models.

Unfortunately, there are very few studies in the literature related to protecting against adversarial audio attacks. The construction of a general and strong defensive mechanism to address this issue is still a work in progress. The study in Reference 134 has developed a proactive defensive system to restore the structure of the original input and eliminate the perturbations. General protection against voice recognition systems includes code modulation and audio compression.

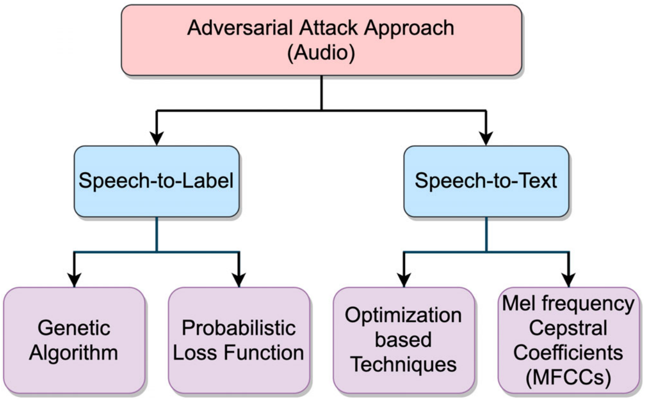

Adversarial Attack Approach (Audio)
Speech-to-Label
Speech-to-Text
Genetic Algorithm
Probabilistic Loss Function
Optimization based Techniques
Mel frequency Cepstral Coefficients (MFCCs)

FIGURE 16 Taxonomy for adversarial attack on audio.

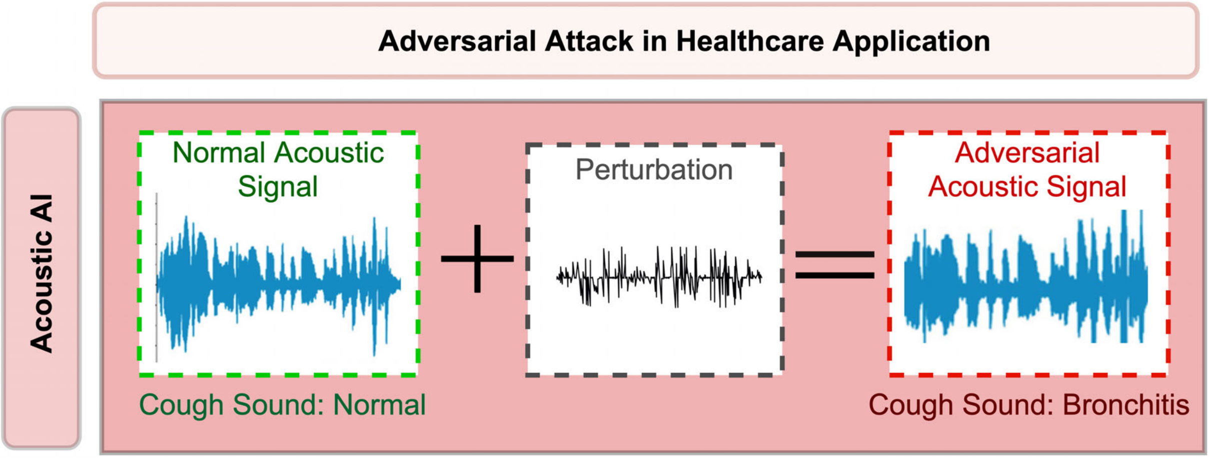


FIGURE 17 Adversarial attack on acoustic-based healthcare applications.

Code modulation combines the G.729 narrow-band vocoder-based audio data compression method with PCM, to modify and convert the audio waveform. The audio compression eliminates unwanted audio information that surpasses human hearing by utilizing MP3 compression. The study in Reference 135 has discovered that frame offsets with a blank clip inserted at the beginning of audio can deteriorate adversarial perturbations to normal noise by examining the features of the automatic speech recognition system. Even though this technique can identify and protect the audio adversarial scenario, the perturbations remain as noise, affecting the identification accuracy of the system. The study in Reference 136 deployed two adversarial training designs, namely Vanilla and Unique Similarity-based Adversarial Training Contribution to protect against adversarial attacks. Adversarial training intends to train both actual and fictitious data. However, vast adversarial data is required to train the detector.

9 | BLOCKCHAIN SOLUTION FOR AI-BASED HEALTHCARE

AI can enhance care delivery, productivity, and efficiency, which allows healthcare organizations to get better treatment for many more patients. In addition, AI can help to reduce the burden placed on healthcare professionals by allowing them to concentrate on acute care and pertinent treatment. According to the literature that was studied, NLP, computer vision, and acoustic AI are the three main tools in processing healthcare data, including texts, pictures, and audio simultaneously, and assisting medical professionals in diagnosing and treating patients. Though there are far more benefits to adopting AI in the healthcare industry, certain threats slow down the acceptance of AI in the critical applications of healthcare. Data, classifiers/algorithms, and models are the attack surfaces of AI. Various adversarial attacks were studied independently on texts, images, and audio. A comparative study that compares the findings for adversarial attacks on NLP, computer vision, and acoustic AI is presented in Table 11.

Considering the adverse effect of such attacks on healthcare applications, the authors have gone through different defense techniques for adversarial attacks. However, each of the defense techniques has its advantages and disadvantages, as discussed in the earlier sections. Furthermore, many of the defense techniques are AI-based and very specific to the

TABLE 11 Comparative analysis of adversarial attacks on NLP, computer vision and acoustic AI.

Parameter	NLP	Computer vision	Acoustic AI
Nature of data	Discrete nature	Continuous pixels	Continuous-time series
Underlying DNN architectures	Convolution/recurrent	Convolution	Recurrent
Complexity of attack	Moderate	Easy	Difficult
Perceivability by humans	Easy	Difficult	Moderate

kind of adversarial attack. So far, no defense strategy has been capable of managing all sorts of adversarial attacks. Hence, this article proposes a Blockchain-based solution to mitigate different attacks on AI-based healthcare systems.

9.1 | NLP-based healthcare

NLP is an innovative technique for improving information extraction methods where data is discrete. NLP algorithms can be protected with immutable, tamperproof, and trusted Blockchain technology by carrying critical data extracted after the NLP algorithms, thereby fulfilling the requirement of data provenance and 100% uptime for the system, with its distributed nature. As discussed in Section 6.3, the NLP suffers from various types of adversarial attacks. However, the complexity of these attacks is moderate, and in the case of textual data, adversarial attacks can be easily perceived by human eyes. Therefore, the probability of such attacks might be moderate. Blockchain-based solutions for addressing attack surfaces like data, classifiers, and models in NLP have been proposed.

9.1.1 | Synthesized framework

I. Dataset building

In NLP, data can reside on local machines of data owners like doctors, hospitals, and laboratories. They can build a peer-to-peer network of Blockchain within distributed owners to resolve the need for sufficiently large data for training AI models. At the same time, the privacy of data can be maintained by prohibiting the data owners from directly sharing the data with a third party. This framework supports off-chain storage of data. This peer-to-peer network offers a direct exchange of services through a proper authentication mechanism. Thousands of machines can be connected without any centralized server. The node in the P2P Blockchain network can either act as a requester or service provider. The access control rules can be implied to have authorized and trusted sharing of data through smart contracts. A hash value is generated at each data station and maintained in Blockchain to check the integrity of the distributed data. A hash will be recalculated and validated through Blockchain at the time of data utilization for training purposes. Figure 18 illustrates the dataset building with Blockchain for NLP.

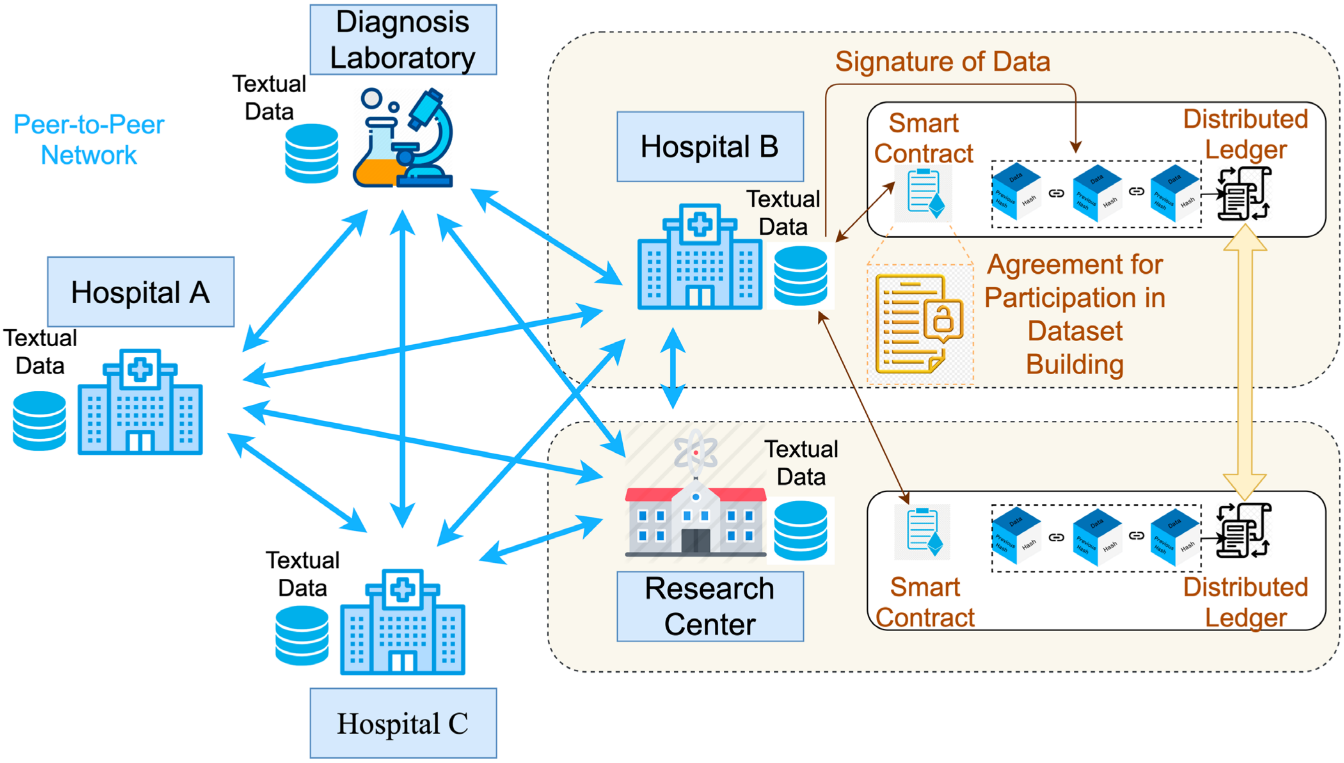


FIGURE 18 Dataset building with Blockchain in NLP-based healthcare applications.

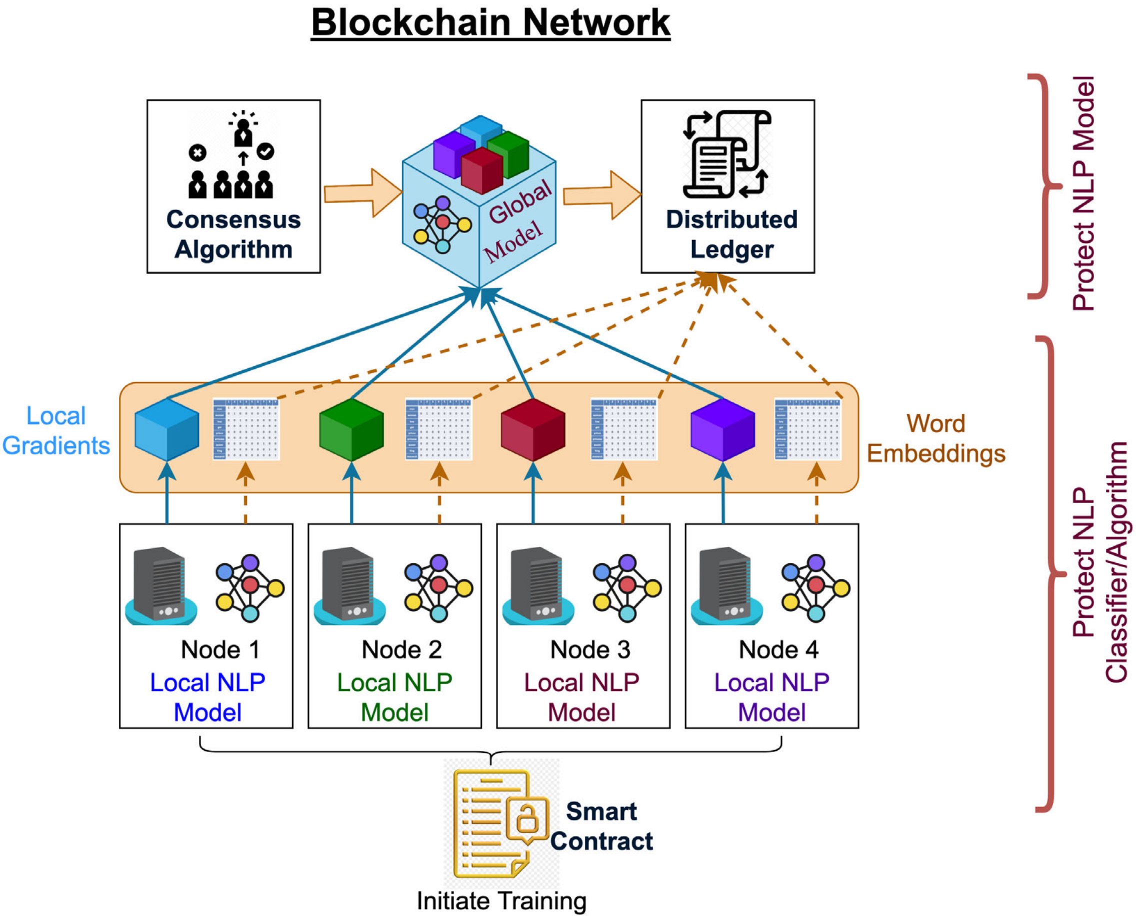


FIGURE 19 Blockchain solution to protect training phase of NLP.

The participants in the Blockchain network can be various hospitals, diagnosis laboratories, research centers, and others, with a database of textual data like clinical reports and notes. There will be peer-to-peer connections within each participant, and Blockchain will govern their communication. For example, suppose the research center needs access to the dataset from the hospital, then it will initiate a request for data access through a Smart Contract. The hospitals can respond with an agreement for participation in dataset building, mentioning rules or restrictions for data sharing and usage for training the AI model. A copy of the distributed ledger is available to each participant. The hash value can be generated and stored in the Blockchain as its signature for future integrity checks of data for the data at each station. This way, many data stations can contribute to trusted dataset building with Blockchain.

II. Training phase

Federated learning comes into the picture to train a learning algorithm using the distributed dataset. Federated learning faces challenges like malfunctioned nodes, trust in local gradients, and global gradient aggregation. Leveraging Blockchain in federated learning helps to solve these challenges and protect the model from poisoning attacks. Training can be initiated through a Smart Contract so that it can check on the participant's legitimacy. Local gradients at federated nodes will then be communicated through a block. It will lock local gradients in the Blockchain to avoid tampering and to be used in the future for verification. The miners in the Blockchain network will validate and generate global gradients using a consensus algorithm. This is how Blockchain can bring authenticity to the federated network. Each node embeds the extracted features in vector space, and those will be saved for further use in the distributed ledger. Word embeddings are a kind of word representation that meaningfully connects a human's grasp of knowledge to the understanding of a machine. For example, a set of real numbers can be used as a depiction (a vector). Word embeddings are a dispersed representation of a text in an n-dimensional space that attempts to capture the meaning of the words. Figure 19 illustrates the Blockchain solution for protecting classifiers/algorithms in NLP.

III. Post-training phase

The output of the trained model depends on the genuineness of the input in the post-training phase. Malfunctioning of the NLP model can be expected for adversarial text input. Hence, to mitigate certain adversarial attacks, Blockchain technology can be leveraged in NLP-based healthcare systems. The Blockchain version of the extracted features from a dataset used for model training plays an important role in discriminating adversarial text. The word embedding will be generated through a Smart Contract for the given input. It will look for a similar corpus of word embedding in the distributed ledger based on synonyms. The resultant extracts are further distributed among the miners in the Blockchain network. The miners will compute the result for the assigned features, using a trained model, instead of proof of work. The results will then be shared among the miners, and based on the majority of votes, the result will be recorded with the consensus in the Blockchain. This framework will defend the model from the synonym-based adversarial attack on the text as described in Figure 20.

9.2 | Computer vision-based healthcare

Computers must "understand" an image and comprehend its features to take full advantage of images. Computer vision enriches computers with the capability to unlock image data. Computer vision plays a vital role in healthcare, as discussed in Section 7.2, but at the same time, it is also prone to malfunction due to potential adversarial attacks. AI-based healthcare applications cannot survive in such an adversarial environment. After studying the adversarial attacks on computer vision, it was found that the complexity of adversarial attacks on images is less and non-perceivable. Hence it is needed to focus on designing preventive measures. Here, a systematic strategy to handle the adversarial environment in computer vision with Blockchain is proposed.

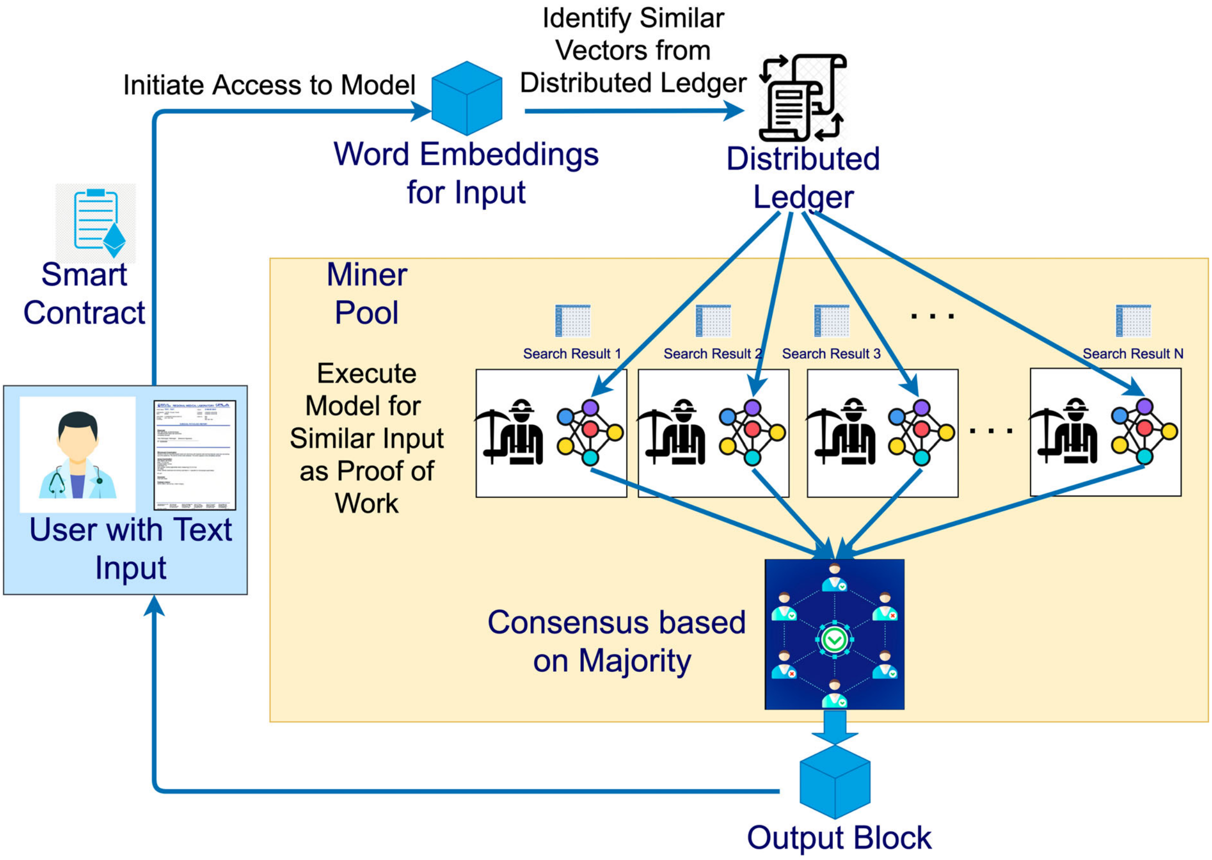


FIGURE 20 Post-training Blockchain solution for NLP-based healthcare.

9.2.1 | Synthesized framework

I. Dataset building

As images are more prone to adversarial attacks, the proposed solution mainly focuses on preventive measures, as shown in Figure 21. The images will be uploaded to IPFS with the help of Blockchain technology. IPFS is a file-sharing technology that may be effectively used to store and distribute big files. It is based on cryptographic hashes, which can be effortlessly preserved on a Blockchain. Cryptographic hashes are used to validate the integrity of the images. First, data owners like different hospitals, and diagnostic centers request for uploading medical images on IPFS. Smart Contracts validate the data owner and upload the data on IPFS. A cryptographic hash is generated at IPFS for an uploaded set of images, which is further stored in Blockchain. The research centers which need medical image datasets to train an AI model can request Blockchain to access image datasets. Smart Contract authenticates the user and provides hash value stored in the Blockchain for the data available in IPFS. The users will approach IPFS with hash value and get access to the image dataset. It will be easy to detect adversarial images with hash values as the small changes in the images will drastically change the generated hash. This is how the dataset will be secure at IPFS with Blockchain.

II. Training phase

Computer vision provides real-time data for visual inputs. Therefore, AI models must be trained with image datasets, informing the model about what each input shows. This training phase can be protected with Blockchain, as shown in

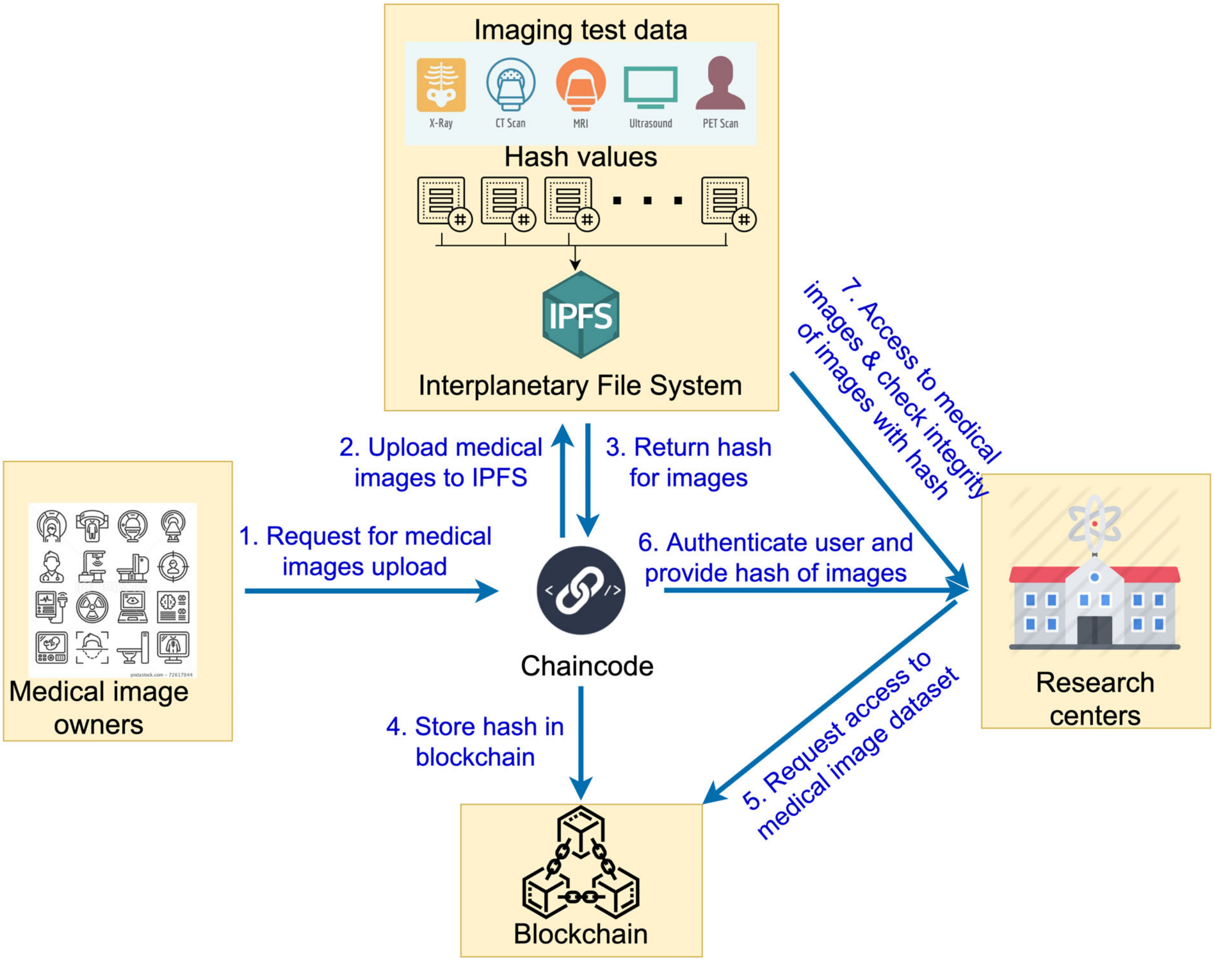

Imaging test data
X-Ray
CT Scan
MRI
Ultrasound
PET Scan
Hash values
IPFS
Interplanetary File System
2. Upload medical images to IPFS
3. Return hash for images
7. Access to medical images & check integrity of images with hash
Medical image owners
1. Request for medical images upload
Chaincode
6. Authenticate user and provide hash of images
Research centers
4. Store hash in blockchain
5. Request access to medical image dataset
Blockchain

FIGURE 21 Dataset building in computer vision-based healthcare applications.

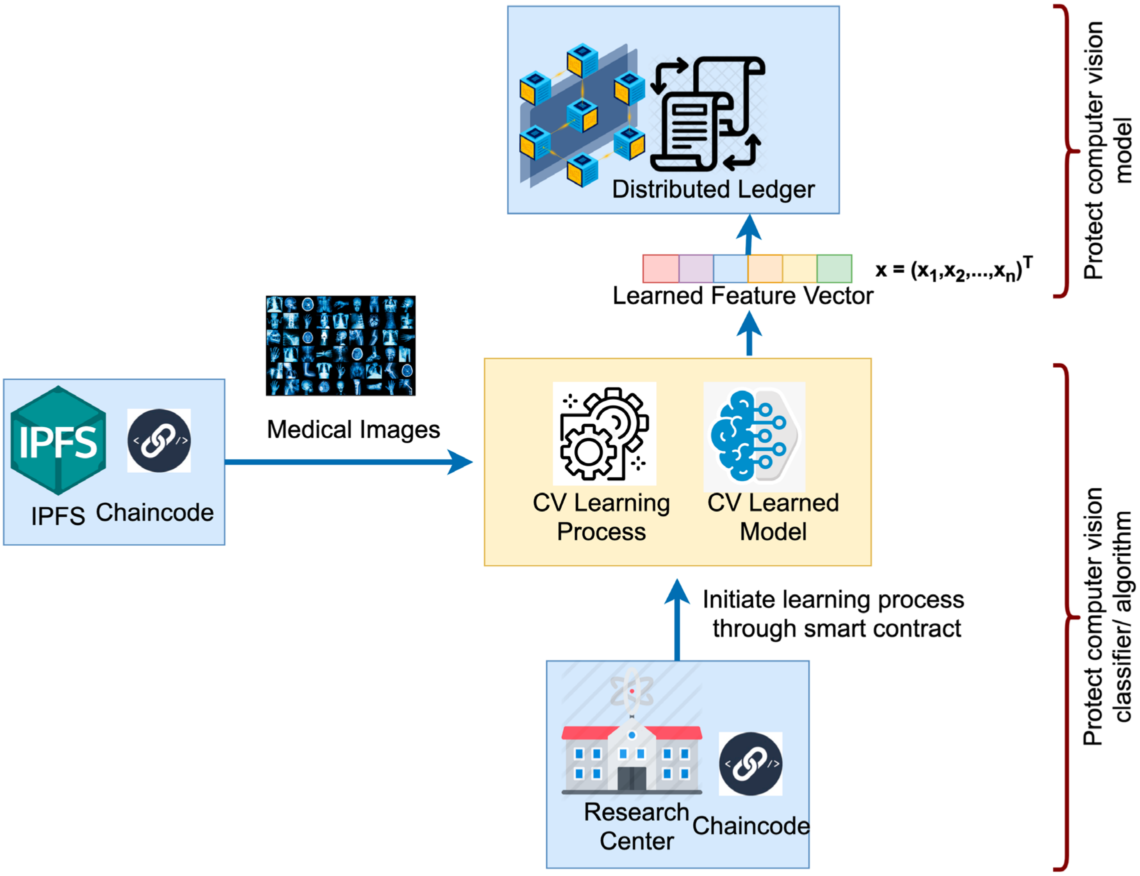

Distributed Ledger
x = $(x_1, x_2, \ldots, x_n)^T$
Learned Feature Vector
Protect computer vision model
Medical Images
IPFS
IPFS
Chaincode
CV Learning Process
CV Learned Model
Initiate learning process through smart contract
Research Center
Chaincode
Protect computer vision classifier/ algorithm

FIGURE 22 Blockchain solution to protect training phase of computer vision.

Figure 22. The research centers must initiate the learning process through Smart Contracts only after proper authentication. Once the model is trained, the extracted features will be stored in Blockchain for further reference in the feature vector $X = (X_1, X_2, X_3, \ldots, X_n)^T$, where n is the number of features extracted and T represents the transpose operation along with the metadata. This framework will protect the entire training environment for computer vision, and thus, a tamper-proof record of features will be extracted by the learning process.

III. Post-training phase

The result generated for a given image input should be self-explanatory, describing justification for output in the post-training phase of computer vision-based healthcare. Access to the trained model is restricted through Smart Contracts. The model can be accessed only by authorized doctors and researchers. It will check with the stored feature vector in the distributed ledger for validating the integrity of the model run. This article proposes the use of explainable AI to make healthcare applications more trustworthy and transparent. Explainable AI (XAI) is a novel concept in machine learning that explains how AI systems make black box choices. XAI examines and attempts to clarify the models and the different stages of decision-making. XAI prepares the description of the output generated for a given input image. The metadata of these descriptions is stored in the Blockchain for further verification and validation. This is how a tamper-proof and accurate comprehensive diagnosis with an explanation is achieved in a secure Blockchain environment as illustrated in Figure 23.

9.3 | Acoustic AI-based healthcare

Most recent advancements and transformational possibilities of machine learning, particularly deep learning is in acoustics. Machine learning is data-driven in comparison to traditional acoustics and signal processing. Thus, acoustic AI can

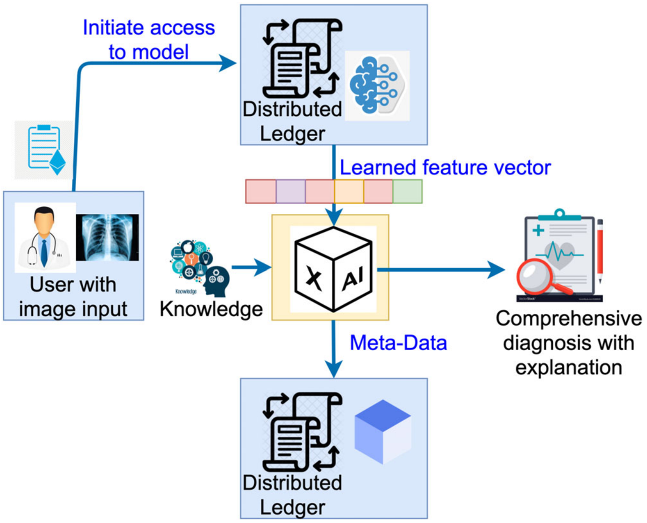


FIGURE 23 Post-training blockchain solution for computer vision-based healthcare.

have profound potential in analyzing acoustic signals in healthcare applications. However, as discussed in Section 8.3, healthcare applications have the biggest threat of adversarial attacks, which are harmful in the healthcare domain. Adversarial attacks on acoustic signals are complex and have a moderate level of perceivability. Therefore, acoustic medical data can be kept on local machines and impose federated learning with Blockchain technology to protect acoustic AI-based healthcare applications from adversarial attacks.

9.3.1 | Synthesized framework

I. Dataset building

In acoustic AI, data can reside on local machines of data owners like doctors, hospitals, and laboratories, as described in Blockchain solutions for NLP-based healthcare. Figure 24 illustrates the dataset building with Blockchain for acoustic AI-based healthcare. The various IoMT devices can threaten the security of each data owner as rogue devices can enter the IoMT network, affecting the data generation process. Hence, a rogue device mitigation strategy based on Blockchain can be introduced in dataset building. The access control rules will be implied on acoustic data storage, and IoMT devices must go through proper registration and authentication procedure to contribute to dataset building through Smart Contracts. Data sharing for dataset building in acoustic AI-based healthcare is like the NLP-based healthcare dataset building framework described in Section 9.1.

II. Training phase

As acoustic data is in distributed form, a Federated Learning approach is adopted in the proposed secure framework for training the acoustic AI model. Each data owner acts as a node in the network running the local acoustic AI model. The extracted features from audio samples will be kept secure in distributed ledgers for further validation and reference. Extracted features of audio samples can be in any form based on the learning approach. Consider a traditional machine learning approach, in which case, extracted features can be Amplitude Envelope, Zero-Crossing Rate (ZCR), Root Mean Square (RMS) Energy, Spectral Centroid, Band Energy Ratio, and Spectral Bandwidth, whereas the spectrograms, Mel-spectrograms, and Mel-Frequency Cepstral Coefficients (MFCCs) could be used for deep learning approaches. Each local gradient is stored in Blockchain, and consensus algorithms drive the global model generation task. The learned global model is then available in the distributed ledger, preventing unauthorized access to the model. This is how the acoustic AI classifiers/algorithms and models are protected with Blockchain technology as described in Figure 25.

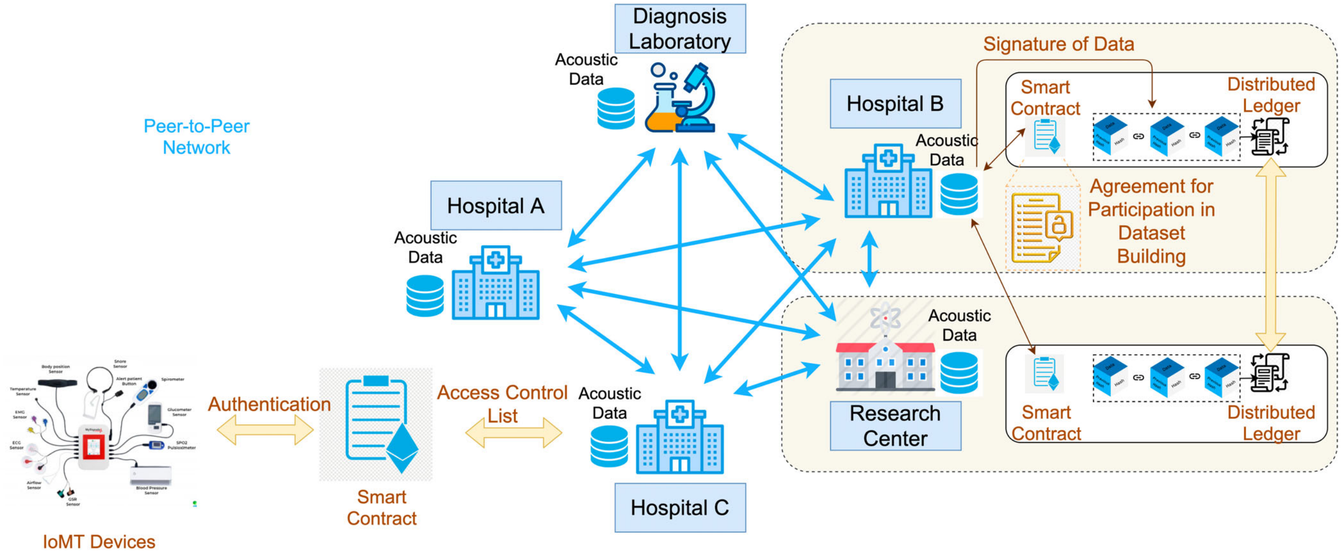


FIGURE 24 Dataset building in acoustic AI-based healthcare with Blockchain.

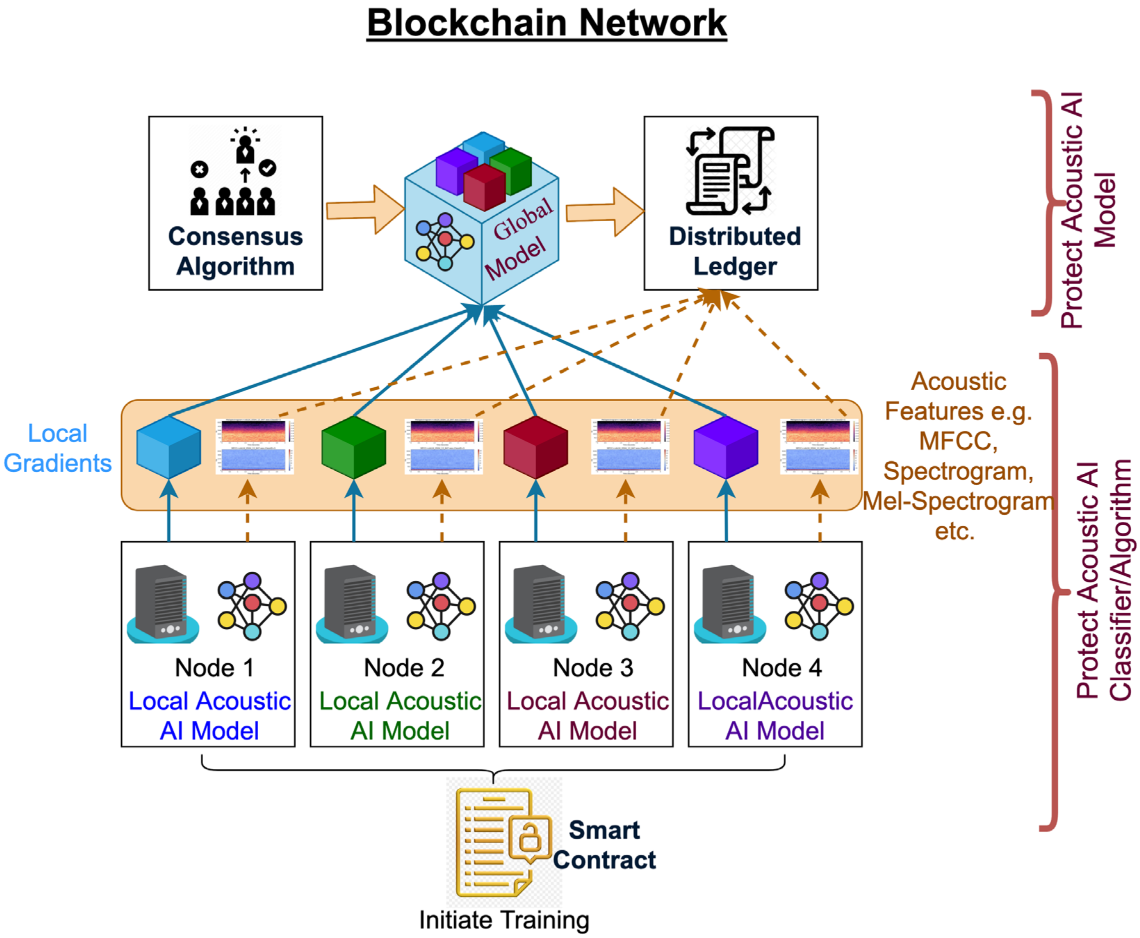


FIGURE 25 Protecting training phase of acoustic AI-based healthcare with Blockchain.

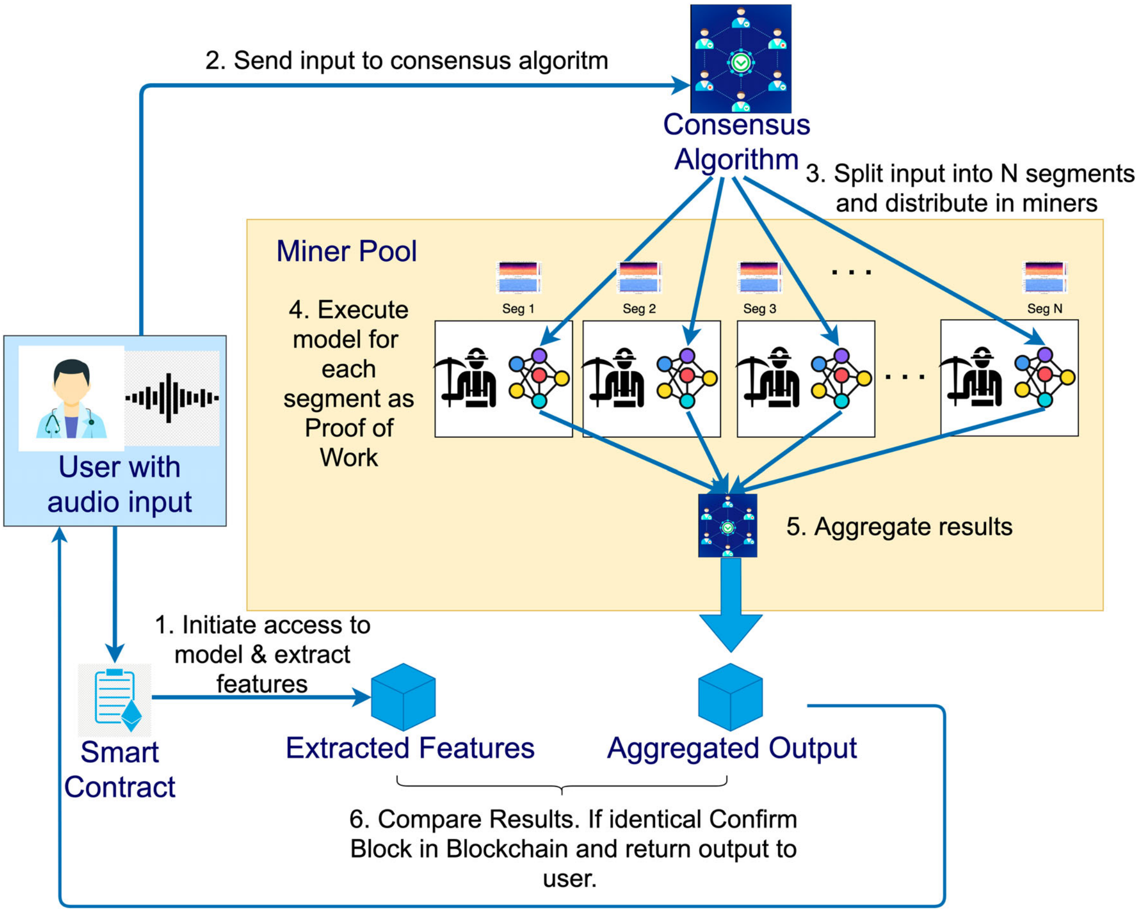

2. Send input to consensus algoritm
Consensus Algorithm
3. Split input into N segments and distribute in miners
Miner Pool
4. Execute model for each segment as Proof of Work
Seg 1
Seg 2
Seg 3
Seg N
. . .
User with audio input
5. Aggregate results
1. Initiate access to model & extract features
Smart Contract
Extracted Features
Aggregated Output
6. Compare Results. If identical Confirm Block in Blockchain and return output to user.

FIGURE 26 Protecting post training phase of acoustic AI-based healthcare with Blockchain.

III. Post-training phase

In the post-training phase of acoustic AI-based healthcare applications, using Blockchain adversarial input to the model will be identified. It will be kept as a secure learned model by restricting access through Smart Contracts, as shown in Figure 26. Temporal dependency is an important characteristic of audio signals. These characteristics and a consensus algorithm are used to detect the integrity of the input to the model. Figure 26 demonstrates the Blockchain framework designed for protecting the post-training phase of acoustic AI-based healthcare. First, a Smart Contract initiates access to the model and gets the result for audio input provided by the user. Then the original input is passed to the consensus algorithm in the Blockchain network. It will split the input into *N* number of segments and assign each segment to each miner available in the miner pool. Miners will again execute the model for segments and at the end, all miners consensually will combine the result generated for each segment. Due to temporal dependency, if that input is adversarial, then the aggregated results will not make any sense and will be different from the generated output at the first step. This strategy will help to detect the adversarial input to the model and increase trust in the model.

10 | DISCUSSION

Blockchain technology gathers real-time data, stores it on several servers to keep it hack-resistant, limits access to only approved individuals, and maintains an updated version of the file for every visit.

10.1 | The outcome of the survey

This survey aids in comprehending the significance of Blockchain in AI-based healthcare applications. According to this literature review, Blockchain technology offers more promising security, privacy, and trust in AI-based healthcare applications. Authors of past studies have synthesized a Blockchain framework that can mitigate adversarial attacks, considering the need for individual NLP, computer vision, and acoustic AI domains, to help improve the wide acceptance and develop more robust AI applications in healthcare. Furthermore, authors have applied knowledge of Blockchain features and properties to protect datasets, classifiers/algorithms, and AI models from adversarial attacks.

10.2 | Challenges in the healthcare industry to adopt blockchain technology in India

Due to the highly regulated environment and low-risk appetite of the healthcare industry, the healthcare industry is often late in adopting digital technology.

I. Lack of robust computational environment

Blockchain requires large computational power to keep the transaction information encrypted. The Blockchain solution uses a lot of electricity and generates heat. India has a shortage of electricity supply, and typically the temperature in India is warm. Hence, India may consider decreasing the number of servers or employing a single server to conserve power. Blockchain storage facilities should be built in cooler areas with Internet access. The challenges faced are that most healthcare facilities lack computers, patient data are often handwritten, and Internet access is inconsistent due to poor connection. The expense of operating such a system must be shared equally among the government, healthcare providers, pharmaceutical companies, insurance companies, and other stakeholders.

II. Lack of uniform IT system and interoperability

There is currently no unified IT system for healthcare in India. The interoperability difficulties arise because of several digital solutions. Interoperability is particularly difficult to establish since various healthcare facilities employ different models and have their own set of codes. When patients switch service providers for unanticipated reasons, the problem becomes worse. The patients are then forced to repeat the diagnostic tests and treatment procedures, thereby increasing overhead expenses and patient dissatisfaction.

10.3 | Advancements in blockchain

I. Quantum blockchain

The term “Quantum Blockchain” can be considered a decentralized, encrypted, and distributed database reliant on quantum computing and quantum information theory. The key features of Quantum Blockchain are security and efficiency. Quantum Secure Direct Communication (QSDC) or Quantum Key Distribution (QKD) can be used to ensure communication security between the nodes. As a result, the characteristics of quantum physics provide network authentication. Traditional encryption techniques used in digital signatures, such as RSA, might be deceptive in the face of quantum computer attacks. The quantum digital signature technique can be employed in quantum Blockchain to overcome this problem. As a result, the quantum Blockchain possesses quantum security properties. As a result, quantum computers might not be able to attack the quantum Blockchain. The Blockchain with quantum technology also can quickly execute transactions.[137–139]

II. Hyperledger

Hyperledger is specifically a Blockchain-based platform that is utilized to incorporate healthcare data management developments. Healthcare applications built on Hyperledger Fabric have emerged as a popular Blockchain deployment. The Linux Foundation hosts an open-source community called Hyperledger, that seeks to offer suitable foundations, rules, libraries, and tools for creating global business Blockchain projects. Hyperledger is ideally suited for healthcare applications. It also provides complete control over Smart Contracts written in several computer languages, including Node.js and JavaScript. Bitcoin and Ethereum, on the other hand, can execute seven and 15 transactions per second, respectively. Hyperledger beats this competition with transaction speeds of up to 3000 transactions per second. Another benefit is that it has a high transaction throughput and low transaction cost. Hyperledger Fabric is the most sophisticated Blockchain framework available compared to other Blockchain frameworks.[140,141]

III. Zero-knowledge proof (ZKP)

Zero-Knowledge Proof (ZKP) has been used as one of the most effective methods for meeting transaction secrecy requirements. The purpose of the functionality of ZKP is to allow a prover to persuade a verifier of a certain truth, without exposing the real information. Interactive zero-knowledge proof and non-interactive zero-knowledge proof are the two most significant forms of ZKPs. Interactive ZKPs require the prover to execute a sequence of activities, to convince the verifier of a certain truth. The sequence of activities in interactive ZKPs is linked to the mathematical probability principles. Non-interactive ZKPs, on the other hand, do not include any interactive elements. The prover may generate all challenges simultaneously, and the verifier could reply afterward as in non-interactive ZKPs. Zero-knowledge-Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) is another significant type of ZKP that has recently developed. The zk-SNARK is the most popular among the zero-knowledge proof alternatives.[142] It can assist in the definition of a quadratic equation that uses public, private, and input data to generate evidence.

IV. Homomorphic encryption

Homomorphic encryption is among the most secure privacy-enhancing techniques for conducting operations on encrypted data. The operations on encrypted data would provide the same outcomes on unencrypted data. As a result, organizations may employ homomorphic encryption for data analysis without sacrificing data anonymity or privacy. Homomorphic encryption can be leveraged for privacy-preserving outsourced storage and computing. Homomorphic encryption makes it possible to encrypt data before sending it for processing to commercial cloud environments. Homomorphic encryption may be thought of as an evolution of asymmetric-key or public-key cryptography. The encryption and decryption functions may be thought of as a homomorphism between plaintext and cipher text spaces, like homomorphism in algebra.[143,144]

V. Other distributed ledger technologies

Systemic inadequacies and scalability issues drove researchers to seek solutions outside the Blockchain framework. As a result, there have been innovative and creative inventions such as hashgraphs, Directed Acyclic Graphs (DAGs), and Holochains.[145,146] In general, the goal is to maintain the original purpose of the Blockchain framework and keep it alive in the context of different challenges and different environments.

a. Hashgraph

Hashgraph is a form of Distributed Ledger Technology based on consensus building. Distributed Ledger Technology (DLT) especially depends on consensus time stamping to ensure that network transactions agree with every node in the network. The consensus algorithm highlights the stability and excellence of the network in DLT. This sort of DLT network, unlike typical DLT networks, achieves success in transactions exclusively by consensus. Consensus time stamping prevents Blockchain issues such as transaction cancelation or inclusion on future blocks. Since there is no requirement for proof of work on this DLT network, there may be thousands of TPS.

b. Directed acyclic graphs (DAGs)

DAG is a Distributed Ledger Technology that uses consensus methods. Consensus algorithms function in such a fashion that transactions that succeed only require the majority support of the network. There is considerably more collaboration and teamwork in such a network, and nodes possess equal opportunities. The primary goal of a DLT was to democratize the Internet economy. For example, a Private Blockchain network is led by a centralized authority which removes democracy from the DLT. On the other hand, this DLT offers equal weight to every node in the network. As a result, each node is not required to refer to the other. IOTA's Tangle is one of the most famous "current generation" networks that use the DAG data structure. In this case, miners/nodes can undertake dual functions that nodes

TABLE 12 Comparison of the different Distributed Ledger Technologies.

Parameter	Blockchain	Hashgraph	DAG	Holochain
Launched in	2008	2018	2015	2018
Consensus algorithm	Many algorithms available	Virtual voting	The previous transaction validates the new one	Not required
Scalability	Limited	High	High	Infinite
Transaction execution speed	Limited	High	High	Highest
Data structure	Blocks are generated as per the sequence of transactions	Gossip about Gossip Protocol	Directed Acyclic Graph	Distributed among nodes
Examples	Bitcoin, Ethereum, and so forth	Swirlds and NOIA	NXT, Tangle, ByteBall, and so forth	Holochain

do independently in the Blockchain. This means that a Tangle miner can originate and approve a transaction at the same time.

c. Holochain

Holochain aspires to build a distributed network that will serve as the foundation for the "next-generation Internet." Holochain is a hybrid of Blockchain, BitTorrent, and Github. This is a DLT that distributes data across nodes to limit centralized control over data flow. This distributed platform essentially means that each node will run on its chain. This means that nodes or miners are individually free to operate. In addition, users can store data using specific keys in what the Holochain team refers to as a Distributed Hash Table (DHT). This data, however, remains "distributed" in physical places throughout the world. Table 12 provides a comparison of these DLTs.

11 | CONCLUSION

This systematic literature review underscores the significance of Blockchain technology in enhancing the security of AI-based healthcare applications. The primary objective of this investigation was to illuminate the various avenues of attack that threaten AI-based healthcare applications. These include adversarial attacks on datasets, spoofing, backdoor/Trojan attacks, and timing side-channel attacks, all of which have the potential to endanger patients' lives. The heightened susceptibility of AI models to even minor input alterations underscore the need to address the models' aberrant behavior. The findings gleaned from this survey reveal that existing solutions aimed at countering AI attacks are often specialized, focusing on distinct attack vectors. However, a majority of these solutions are themselves AI-based, rendering them susceptible to adversarial exploits. Consequently, this survey underscores the value of Blockchain technology. By facilitating real-time data collection, distributed storage across multiple servers to avert hacking, access restriction to authorized personnel, and the preservation of current file versions with each interaction, Blockchain serves as a pivotal solution. This study introduces a Blockchain-centered approach to fortify the entirety of the AI development pipeline in healthcare, encompassing dataset creation, training phases, and post-training stages for NLP, computer vision, and acoustic AI. This proposal recognizes the potency of Blockchain technology in addressing the domain's unique challenges. It is important to note that the healthcare sector, due to its rigorous regulatory framework and aversion to risk, often adopts new technologies at a gradual pace. The lack of a standardized IT infrastructure and interoperability further compounds the challenges in this field. Future research avenues could involve the implementation of sophisticated lightweight Blockchain solutions tailored to the demands of AI-based healthcare applications. Such endeavors hold the promise of ushering in a new era of secure and resilient healthcare technology.

AUTHOR CONTRIBUTIONS

All authors have contributed to the conception and design of the study. Material preparation, data collection, data visualization, and data analysis are performed by Rucha Shinde and Shruti Patil. The advanced data analysis and validation are done by Ketan Kotecha, Vidyasagar Potdar, and Ganeshsree Selvachandran. The first draft of the manuscript has been written by Rucha Shinde, Shruti Patil, and Ketan Kotecha. The second draft has been prepared and edited by Vidyasagar Potdar, Ganeshsree Selvachandran, and Ajith Abraham. The previous versions of the manuscript have included the comments of all the authors. The final manuscript has been approved by all the authors.

ACKNOWLEDGMENT

The authors would like to thank the Editors and the anonymous reviewers for their valuable comments and suggestions which have enhanced the precision of the article. Open access publishing facilitated by Monash University, as part of the Wiley - Monash University agreement via the Council of Australian University Librarians.

CONFLICT OF INTEREST STATEMENT

The authors have no relevant financial or non-financial interests to disclose.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Ganeshsree Selvachandran https://orcid.org/0000-0001-7161-2109

REFERENCES

1. Pushparaj TL, Irudaya Raj EF, Irudaya Rani EF. A detailed review of contrast-enhanced fluorescence magnetic resonance imaging techniques for earlier prediction and easy detection of COVID-19. *Comput Methods Biomech Biomed Eng Imag Visualiz*. 2022;11:1450-1462. doi:10.1080/21681163.2022.2144762
2. Ali O, Abdelbaki W, Shrestha A, Elbasi E, Alryalat MAA, Dwivedi YK. A systematic literature review of artificial intelligence in the healthcare sector: benefits, challenges, methodologies, and functionalities. *J Innov Knowl*. 2023;8(1):100333.
3. Villarreal ERD, Garcia-Alonso J, Moguel E, Alegria JAH. Blockchain for healthcare management systems: a survey on interoperability and security. *IEEE Access*. 2023;11:5629-5652.
4. Shinde R, Patil S, Kotecha K, Ruikar K. Blockchain for securing AI applications and open innovations. *J Open Innovat Technol Mark Complex*. 2021;7(3):189.
5. Mettler M. Blockchain technology in healthcare: the revolution starts here. In: *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Munich, Germany; 2016:1-3. doi:10.1109/HealthCom.2016.7749510
6. Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. In: *2016 2nd International Conference on Open and Big Data (OBD)*, Vienna, Austria; 2016:25-30. doi:10.1109/OBD.2016.11
7. Roman D, Stefano G. Towards a reference architecture for trusted data marketplaces: the credit scoring perspective. In: *2016 2nd International Conference on Open and Big Data (OBD)*, Vienna, Austria; 2016:95-101. doi:10.1109/OBD.2016.21
8. Al Omar A, Rahman MS, Basu A, Kiyomoto S. MediBchain: a blockchain based privacy preserving platform for healthcare data. In: Wang G, Atiquzzaman M, Yan Z, Choo KK, eds. *Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2017. Lecture Notes in Computer Science, 10658*. Springer; 2017. doi:10.1007/978-3-319-72395-2_49
9. Youssef W, Zaabi MA, Svetinovic D. Blockchain AI framework for healthcare records management: constrained goal model. In: *2018 26th Telecommunications Forum (TELFOR)*, Belgrade, Serbia; 2018:420-425. doi:10.1109/TELFOR.2018.8611900
10. Shae Z, Tsai JJP. Transform blockchain into distributed parallel computing architecture for precision medicine. In: *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, Vienna, Austria; 2018:1290-1299. doi:10.1109/ICDCS.2018.00129
11. Mamoshina P, Ojomoko L, Yanovich Y, et al. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget*. 2018;9:5665-5690.
12. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J Med Syst*. 2018;42:130.
13. Jo BW, Khan RMA, Lee Y-S. Hybrid blockchain and internet-of-things network for underground structure health monitoring. *Sensors*. 2018;18(12):4268.
14. Nusrat SA, Ferdous J, Ajmat SB, Ali A, Sorwar G. Telemedicine system design using blockchain in Bangladesh. In: *2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, Melbourne, VIC, Australia; 2019:1-5. doi:10.1109/CSDE48274.2019.9162401
15. Islam N, Faheem Y, Din IU, Talha M, Guizani M, Khalil M. A blockchain-based fog computing framework for activity recognition as an application to e-healthcare services. *Fut Gen Comput Syst*. 2019;100:569-578.
16. Hathaliya J, Sharma P, Tanwar S, Gupta R. Blockchain-based remote patient monitoring in healthcare 4.0. In: *2019 IEEE 9th International Conference on Advanced Computing (IACC)*, Tiruchirappalli, India; 2019:87-91. doi:10.1109/IACC48062.2019.8971593

17. Passerat-Palmbach J, Farnan T, McCoy M, et al. Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. In: *2020 IEEE International Conference on Blockchain (Blockchain)*, Rhodes, Greece; 2020:550-555. doi:10.1109/Blockchain50366.2020.00080
18. Shamim Hossain M, Muhammad G, Guizani N. Explainable AI and mass surveillance system-based healthcare framework to combat COVID-I9 like pandemics. *IEEE Network*. 2020;34(4):126-132.
19. Alruwaili FF. Artificial intelligence and multi agent based distributed ledger system for better privacy and security of electronic healthcare records. *PeerJ Comput Sci*. 2020;6:e323.
20. Lobo VB, Analin J, Laban RM, More SS. Convergence of blockchain and artificial intelligence to decentralize healthcare systems. In: *Proceedings of the 4th International Conference on Computing Methodologies and Communication, ICCMC 2020*; 2020:925-931.
21. Snehi M, Bhandari A. Vulnerability retrospection of security solutions for software-defined cyber–physical system against DDoS and IoT-DDoS attacks. *Comput Sci Rev*. 2021;40:100371.
22. Mohsin AH, Zaidan AA, Zaidan BB, et al. PSO–blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture. *Multimed Tools Appl*. 2021;80:14137-14161.
23. Alqaralleh BAY, Vaiyapuri T, Parvathy VS, Gupta D, Khanna A, Shankar K. Blockchain-assisted secure image transmission and diagnosis model on internet of medical things environment. *Pers Ubiquit Comput*. 2021. doi:10.1007/s00779-021-01543-2
24. Nwosu AU, Goyal SB, Bedi P. Blockchain transforming cyber-attacks: healthcare industry. In: Abraham A, Sasaki H, Rios R, Gandhi N, Singh U, Ma K, eds. *Innovations in Bio-Inspired Computing and Applications. IBICA 2020. Advances in Intelligent Systems and Computing*. Vol 1372. Springer; 2021. doi:10.1007/978-3-030-73603-3_24
25. Houtan B, Hafid AS, Makrakis D. A survey on blockchain-based self-sovereign patient identity in healthcare. *IEEE Access*. 2020;8:90478-90494.
26. Hussien HM, Yasin SM, Udzir SNI, Zaidan AA, Zaidan BB. A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. *J Med Syst*. 2019;43:320.
27. Sookhak M, Jabbarpour MR, Safa NS, Yu FR. Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues. *J Network Comput Appl*. 2021;178:102950.
28. Tandon A, Dhir A, Islam N, Mäntymäki M. Blockchain in healthcare: a systematic literature review, synthesizing framework and future research agenda. *Comput Ind*. 2020;122:103290.
29. Khezr S, Moniruzzaman M, Yassine A, Benlamri R. Blockchain technology in healthcare: a comprehensive review and directions for future research. *Appl Sci*. 2019;9(9):1736.
30. Avdoshin S, Pesotskaya E. Blockchain revolution in the healthcare industry. In: Arai K, Bhatia R, Kapoor S, eds. *Proceedings of the Future Technologies Conference (FTC) 2018. FTC 2018. Advances in Intelligent Systems and Computing*. Vol 880. Springer; 2019. doi:10.1007/978-3-030-02686-8_47
31. Farouk A, Alahmadi A, Ghose S, Mashatan A. Blockchain platform for industrial healthcare: vision and future opportunities. *Comput Commun*. 2020;154:223-235.
32. Narikimilli NRS, Kumar A, Antu AD, Xie B. Blockchain applications in healthcare – a review and future perspective. In: Chen Z, Cui L, Palanisamy B, Zhang LJ, eds. *Blockchain – ICBC 2020. ICBC 2020. Lecture Notes in Computer Science*. Vol 12404. Springer; 2020. doi:10.1007/978-3-030-59638-5_14
33. Hussien HM, Yasin SM, Udzir NI, Ninggal MIH, Salman S. Blockchain technology in the healthcare industry: trends and opportunities. *J Ind Inf Integr*. 2021;22:100217.
34. Ahmad RW, Salah K, Jayaraman R, Yaqoob I, Ellahham S, Omar M. The role of blockchain technology in telehealth and telemedicine. *Int J Med Inform*. 2021;148:104399.
35. Omar IA, Jayaraman R, Salah K, Yaqoob I, Ellahham S. Applications of blockchain technology in clinical trials: review and open challenges. *Arab J Sci Eng*. 2021;46(4):3001-3015.
36. Shi S, He D, Li L, Kumar N, Khan MK, Choo KKR. Applications of blockchain in ensuring the security and privacy of electronic health record systems: a survey. *Comput Secur*. 2020;97:101966.
37. Prabha P, Chatterjee K. Securing telecare medical information system with blockchain technology. In: *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, Greater Noida, India; 2020:846-851. doi:10.1109/ICACCCN51052.2020.9362871
38. Dicuonzo G, Donofrio F, Fusco A, Shini M. Healthcare system: moving forward with artificial intelligence. *Dent Tech*. 2023;120:102510.
39. *Ethics and Governance of Artificial Intelligence for Health*; 2021. https://apps.who.int/bookorders
40. *Accenture: AI Will Lead To $150 Billion In Annual Savings By 2026*. https://ictandhealth.com/accenture-ai-will-lead-to-150-billion-in-annual-savings-by-2026/news/#:~:text=Growth%20opportunities%20are%20hard%20to%20come%20by%20withoutsavings%20for%20the%20US%20healthcare%20economy%20by%202026
41. Neelakandan S, Beulah JR, Prathiba L, Murthy GLN, Irudaya Raj EF, Arulkumar N. Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model. *Int J Model Simul Sci Comput*. 2022;13(4):2241006.
42. Kumar R, Wang WY, Kumar J, et al. An integration of blockchain and AI for secure data sharing and detection of CT images for the hospitals. *Comput Med Imaging Graph*. 2021;87:101812.
43. Kim SK, Huh JH. Artificial neural network blockchain techniques for healthcare system: focusing on the personal health records. *Electronics*. 2020;9(5):763.

44. Nguyen GN, le Viet NH, Elhoseny M, Shankar K, Gupta BB, El-Latif AAA. Secure blockchain enabled cyber–physical systems in healthcare using deep belief network with ResNet model. *J Parall Distrib Comput*. 2021;153:150-160.
45. Jennath HS, Anoop VS, Asharaf S. Blockchain for healthcare: securing patient data and enabling trusted artificial intelligence. *Int J Interact Multim Artif Intellig*. 2020;6(3):15.
46. Rahman MA, Hossain SM, Islam MS, Alrajeh NA, Muhammad G. Secure and provenance enhanced internet of health things framework: a blockchain managed federated learning approach. *IEEE Access*. 2020;8:205071-205087.
47. Puri V, Kataria A, Sharma V. Artificial intelligence-powered decentralized framework for internet of things in healthcare 4.0. *Trans Emerg Telecommun Technol*. 2021;e4245. doi:10.1002/ett.4245
48. Gupta R, Thakker U, Tanwar S, Obaidat MS, Hsiao KF. BITS: a blockchain-driven intelligent scheme for telesurgery system. In: *International Conference on Computer, Information and Telecommunication Systems (CITS)*, Hangzhou, China; 2020:1-5.
49. Polap D, Srivastava G, Jolfaei A, Parizi RM. Blockchain technology and neural networks for the internet of medical things. In: *Proceedings of the EEE INFOCOM 2020 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Toronto, ON, Canada; 2020:508-513.
50. Kumar R, Khan AA, Kumar J, et al. Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging. *IEEE Sens J*. 2021;21(14):16301-16314.
51. Zerka F, Urovi V, Vaidyanathan A, et al. Blockchain for privacy preserving and trustworthy distributed machine learning in multicentric medical imaging (C-DistriM). *IEEE Access*. 2020;8:183939-183951.
52. Kuo TT, Gabriel RA, Cidambi KR, Ohno-Machado L. EXpectation propagation LOgistic REgRession on permissioned blockCHAIN (ExplorerChain): decentralized online healthcare/genomics predictive model learning. *J Am Med Inform Assoc*. 2020;27(5):747-756.
53. Tan T-E, Anees A, Chen C, et al. Retinal photograph-based deep learning algorithms for myopia and a blockchain platform to facilitate artificial intelligence medical research: a retrospective multicohort study. *Lancet Digit Health*. 2021;3(5):E317-E329.
54. Khan MA, Nasir IM, Sharif M, et al. A blockchain based framework for stomach abnormalities recognition. *Comput Mater Continua*. 2021;67(1):141-158.
55. Pilozzi A, Huang X. Overcoming Alzheimer's disease stigma by leveraging artificial intelligence and blockchain technologies. *Brain Sci*. 2020;10(3):183.
56. Ramesh P, Bhaskari DL, Satyanarayana CH. A comprehensive analysis of spoofing. *Int J Adv Comput Sci Appl*. 2010;1(6):157-162. doi:10.14569/IJACSA.2010.010623
57. Sethi TS, Kantardzic M. Handling adversarial concept drift in streaming data. *Exp Syst Appl*. 2018;97:18-40.
58. Geigel A. Neural network trojan. *J Comput Secur*. 2013;21(2):191-232.
59. Liu Y, Xie Y, Srivastava A. Neural Trojans. In: *2017 IEEE International Conference on Computer Design (ICCD)*, Boston, MA, USA; 2017:45-48. doi:10.1109/ICCD.2017.16
60. Gao H, Chen Y, Zhang W. Detection of Trojaning attack on neural networks via cost of sample classification. *Secur Commun Networks*. 2019;2019:1953839.
61. Chen J, Zhang L, Zheng H, Xuan Q. SPA: stealthy poisoning attack. In: *Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies*, Guangzhou, China; 2021:303-309. doi:10.1145/3444370.3444589
62. Gu T, Liu K, Dolan-Gavitt B, Garg S. BadNets: evaluating backdooring attacks on deep neural networks. *IEEE Access*. 2019;7:47230-47243.
63. Duddu V, Samanta D, Rao DV, Balas VE. Stealing neural networks via timing side channels. *arXiv:1812.11720* [cs.CR]; 2018. doi:10.48550/arXiv.1812.11720
64. Hua W, Zhang Z, Suh GE. Reverse engineering convolutional neural networks through side-channel information leaks. In: *Proceedings of the 55th Annual Design Automation Conference*. Vol 4; 2018:1-6. doi:10.1145/3195970.3196105
65. Reyes-Ortiz JA, Gonzalez-Beltran BA, Gallardo-Lopez L. Clinical decision support systems: a survey of NLP-based approaches from unstructured data. In: *2015 26th International Workshop on Database and Expert Systems Applications (DEXA)*, Valencia, Spain; 2015:163-167. doi:10.1109/DEXA.2015.47
66. Tou H, Yao L, Wei Z, Zhuang X, Zhang B. Automatic infection detection based on electronic medical records. *BMC Bioinform*. 2018;19:117. doi:10.1186/s12859-018-2101-x
67. Cruz NP, Canales L, Muñoz JG, Pérez B, Arnott I. Improving adherence to clinical pathways through natural language processing on electronic medical records. *Stud Health Technol Inform*. 2019;264:561-565. doi:10.3233/SHTI190285
68. Ye J, Yao L, Shen J, Janarthanam R, Luo Y. Predicting mortality in critically ill patients with diabetes using machine learning and clinical notes. *BMC Med Inform Decis Mak*. 2020;20:295.
69. McCoy TH, Castro VM, Cagan A, Roberson AM, Kohane IS, Perlis RH. Sentiment measured in hospital discharge notes is associated with readmission and mortality risk: an electronic health record study. *PloS One*. 2015;10(8):e0136341.
70. Pons E, Braun LMM, Hunink MGM, Kors JA. Natural language processing in radiology: a systematic review. *Radiology*. 2016;279(2):329-343. doi:10.1148/radiol.16142770
71. Weng WH, Wagholikar KB, McCray AT, Szolovits P, Chueh HC. Medical subdomain classification of clinical notes using a machine learning-based natural language processing approach. *BMC Med Inform Decis Mak*. 2017;17:155.
72. Hallak JA, Scanzera AC, Azar DT, Chan RVP. Artificial intelligence in ophthalmology during COVID-19 and in the post COVID-19 era. *Curr Opin Ophthalmol*. 2020;31(5):447-453.
73. Nehme F, Feldman K. Evolving role and future directions of natural language processing in gastroenterology. *Dig Dis Sci*. 2021;66:29-40.
74. Doan S, Maehara CK, Chaparro JD, et al. Building a natural language processing tool to identify patients with high clinical suspicion for Kawasaki disease from emergency department notes. *Acad Emerg Med*. 2016;23(5):628-636.

75. Chen L, Gu Y, Ji X, et al. Extracting medications and associated adverse drug events using a natural language processing system combining knowledge base and deep learning. *J Am Med Inform Assoc*. 2020;27(1):56-64.
76. Kidwai B, Nadesh RK. Design and development of diagnostic chabot for supporting primary health care systems. *Proc Comput Sci*. 2020;167:75-84.
77. Wu S, Roberts K, Datta S, et al. Deep learning in clinical natural language processing: a methodical review. *J Am Med Inform Assoc*. 2020;27(3):457-470.
78. Lee S, Mohr NM, Street NW, Nadkarni P. Machine learning in relation to emergency medicine clinical and operational scenarios: an overview. *West J Emerg Med*. 2019;20(2):219-227.
79. Xu J, Yang P, Xue S, et al. Translating cancer genomics into precision medicine with artificial intelligence: applications, challenges and future perspectives. *Hum Genet*. 2019;138:109-124.
80. Gao J, Lanchantin J, Soffa ML, Qi Y. Black-box generation of adversarial text sequences to evade deep learning classifiers. In: *2018 IEEE Security and Privacy Workshops (SPW)*, San Francisco, CA, USA; 2018:50-56. doi:10.1109/SPW.2018.00016
81. Ebrahimi J, Rao A, Lowd D, Dou D. HotFlip: white-box adversarial examples for text classification. *Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics (Volume 2: Short Papers), Melbourne, Australia*. Association for Computational Linguistics; 2018:31-36. doi:10.18653/v1/P18-2006
82. Li J, Ji S, Du T, Li B, Wang T. TextBugger: generating adversarial text against real-world applications. In: *Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2019*, San Diego, CA, USA; 2019. doi:10.14722/ndss.2019.23138
83. Alzantot M, Sharma Y, Elgohary A, Ho B-J, Srivastava M, Chang K-W. Generating natural language adversarial examples. In: *Proceedings of the 2018 ACL Conference on Empirical Methods in Natural Language Processing*, Brussels, Belgium; 2018:2890-2896. doi:10.18653/v1/D18-1316
84. Garg S, Ramakrishnan G. BAE: BERT-based adversarial examples for text classification. In: *Proceedings of the 2020 ACL Conference on Empirical Methods in Natural Language Processing (EMNLP)*; 2020:6174-6181. doi:10.18653/v1/2020.emnlp-main.498
85. Li L, Ma R, Guo Q, Xue X, Qiu X. BERT-ATTACK: adversarial attack against BERT using BERT. In: *Proceedings of the 2020 ACL Conference on Empirical Methods in Natural Language Processing (EMNLP)*; 2020:6193-6202. doi:10.18653/v1/2020.emnlp-main.500
86. Huber L, Kuhn MA, Mosca E, Groh G. Detecting word-level adversarial text attacks via SHapley additive exPlanations. In: *Proceedings of the 7th Workshop on Representation Learning for NLP*, Dublin, Ireland; 2022:156-166. doi:10.18653/v1/2022.repl4nlp-1.16
87. Ren S, Deng Y, He K, Che W. Generating natural language adversarial examples through probability weighted word saliency. In: *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, Florence, Italy; 2019:1085-1097. doi:10.18653/v1/P19-1103
88. Jin D, Jin Z, Zhou JT, Szolovits P. Is BERT really robust? A strong baseline for natural language attack on text classification and entailment. *Proc AAAI Conf Artif Intellig*. 2020;34(5):8018-8025. doi:10.1609/aaai.v34i05.6311
89. Divya R, Peter JD. Smart healthcare system-a brain-like computing approach for analyzing the performance of detectron2 and PoseNet models for anomalous action detection in aged people with movement impairments. *Comp Intellig Syst*. 2022;8:3021-3040.
90. Khemasuwan D, Sorensen JS, Colt HG. Artificial intelligence in pulmonary medicine: computer vision, predictive model and Covid-19. *Eur Respir Rev*. 2020;29:200181.
91. Russakovsky O, Deng J, Su H, et al. ImageNet large scale visual recognition challenge. *Int J Comput Vis*. 2015;115:211-252.
92. Esteva A, Chou K, Yeung S, et al. Deep learning-enabled medical computer vision. *npj Digit Med*. 2021;4:5.
93. Manocha A, Singh R. Computer vision based working environment monitoring to analyze generalized anxiety disorder (GAD). *Multimed Tools Appl*. 2019;78:30457-30484.
94. Yeung S, Rinaldo F, Jopling J, et al. A computer vision system for deep learning-based detection of patient mobilization activities in the ICU. *npj Digit Med*. 2019;2:11.
95. Livingstone D, Talai AS, Chau J, Forkert ND. Building an otoscopic screening prototype tool using deep learning. *J Otolaryngol Head Neck Surg*. 2019;48:66.
96. VerMilyea M, Hall JMM, Diakiw SM, et al. Development of an artificial intelligence-based assessment model for prediction of embryo viability using static images captured by optical light microscopy during IVF. *Hum Reprod*. 2020;35(4):770-784.
97. Hu Y, Wen G, Liao H, Wang C, Dai D, Yu Z. Automatic construction of Chinese herbal prescriptions from tongue images using cnns and auxiliary latent therapy topics. *IEEE Trans Cybern*. 2021;51(2):708-721.
98. Islam MT, Al-Absi HRH, Ruagh EA, Alam T. DiaNet: a deep learning based architecture to diagnose diabetes using retinal images only. *IEEE Access*. 2021;9:15686-15695.
99. Islam MM, Yang HC, Poly TN, Jian WS, Li Y-CJ. Deep learning algorithms for detection of diabetic retinopathy in retinal fundus photographs: a systematic review and meta-analysis. *Comput Methods Programs Biomed*. 2020;191:105320.
100. Zhang J, Xie Y, Pang G, et al. Viral pneumonia screening on chest X-rays using confidence-aware anomaly detection. *IEEE Trans Med Imaging*. 2021;40(3):879-890.
101. Choi J, Hui JZ, Spain D, Su YS, Cheng CT, Liao CH. Practical computer vision application to detect hip fractures on pelvic X-rays: a bi-institutional study. *Trauma Surg Acute Care Open*. 2021;6:e000705.
102. Horie Y, Yoshio T, Aoyama K, et al. Diagnostic outcomes of esophageal cancer by artificial intelligence using convolutional neural networks. *Gastrointest Endosc*. 2019;89(1):25-32.
103. Chilamkurthy S, Ghosh R, Tanamala S, et al. Deep learning algorithms for detection of critical findings in head CT scans: a retrospective study. *The Lancet*. 2018;392(10162):2388-2396.

104. Chen X, Yao L, Zhou T, Dong J, Zhang Y. Momentum contrastive learning for few-shot COVID-19 diagnosis from chest CT images. *Pattern Recogn*. 2021;113:107826.
105. Fang B, Mei G, Yuan X, Wang L, Wang Z, Wang J. Visual SLAM for robot navigation in healthcare facility. *Pattern Recogn*. 2021;113:107822.
106. Goodfellow IJ, Shlens J, Szegedy C. Explaining and harnessing adversarial examples. *arXiv:1412.6572 [stat.ML]*; 2014. https://github.com/lisa-lab/pylearn2/tree/master/pylearn2/scripts/
107. Kurakin A, Goodfellow I, Bengio S. Adversarial examples in the physical world. *arXiv:1607.02533 [cs.CV]*; 2017. doi:10.48550/arXiv.1607.02533
108. Tramèr F, Kurakin A, Papernot N, Goodfellow I, Boneh D, McDaniel P. Ensemble adversarial training: attacks and defenses. *arXiv:1705.07204 [stat.ML]*; 2017. doi:10.48550/arXiv.1705.07204
109. Szegedy C, Zaremba W, Sutskever I, et al. Intriguing properties of neural networks. *arXiv:1312.6199* [cs.CV]; 2014. doi:10.48550/arXiv.1312.6199
110. Carlini N, Wagner D. Towards evaluating the robustness of neural networks. In: *2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA; 2017:39-57. doi:10.1109/SP.2017.49
111. Baluja S, Fischer I. Adversarial transformation networks: learning to generate adversarial examples. *arXiv:1703.09387 [cs.NE]*; 2017. doi:10.48550/arXiv.1703.09387
112. Xiao C, Zhu J-Y, Li B, He W, Liu M, Song D. Spatially transformed adversarial examples. *arXiv:1801.02612 [cs.CR]*; 2018. doi:10.48550/arXiv.1801.02612
113. Papernot N, McDaniel P, Goodfellow I. Transferability in machine learning: from phenomena to black-box attacks using adversarial samples. *arXiv:1605.07277 [cs.CR]*; 2016. doi:10.48550/arXiv.1605.07277
114. Brendel W, Rauber J, Bethge M. Decision-based adversarial attacks: reliable attacks against black-box machine learning models. *arXiv:1712.04248 [stat.ML]*; 2018. doi:10.48550/arXiv.1712.04248
115. Ren K, Zheng T, Qin Z, Liu X. Adversarial attacks and defenses in deep learning. *Engineering*. 2020;6(3):346-360.
116. Patil S, Varadarajan V, Walimbe D, et al. Improving the robustness of AI-based malware detection using adversarial machine learning. *Algorithms*. 2021;14(10):297.
117. Ma X, Niu Y, Gu L, et al. Understanding adversarial attacks on deep learning based medical image analysis systems. *Pattern Recogn*. 2021;110:107332.
118. Chow Y-W, Susilo W, Wang J, et al. Utilizing QR codes to verify the visual fidelity of image datasets for machine learning. *J Network Comput Appl*. 2021;173:102834.
119. Tiron R, Lyon G, Kilroy H, et al. Screening for obstructive sleep apnea with novel hybrid acoustic smartphone app technology. *J Thorac Dis*. 2020;12(8):4476-4495.
120. Kucharski D, Kajor M, Grochala D, Iwaniec M, Iwaniec J. Combining spectral analysis with artificial intelligence in heart sound study. *Adv Sci Technol Res J*. 2019;13(2):112-118.
121. Grzywalski T, Piecuch M, Szajek M, et al. Practical implementation of artificial intelligence algorithms in pulmonary auscultation examination. *Eur J Pediatr*. 2019;178:883-890.
122. Acharya J, Basu A. Deep neural network for respiratory sound classification in wearable devices enabled by patient specific model tuning. *IEEE Trans Biomed Circ Syst*. 2020;14(3):535-544.
123. Srivastava A, Jain S, Miranda R, Patil S, Pandya S, Kotecha K. Deep learning based respiratory sound analysis for detection of chronic obstructive pulmonary disease. *PeerJ Comput Sci*. 2021;7:e369.
124. Ramesh V, Vatanparvar K, Nemati E, Nathan V, Rahman MM, Kuang J. CoughGAN: generating synthetic coughs that improve respiratory disease classification. In: *2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*, Montreal, QC, Canada; 2020:5682-5688. doi:10.1109/EMBC44109.2020.9175597
125. Kochetov K, Putin E, Balashov M, Filchenkov A, Shalyto A. Noise masking recurrent neural network for respiratory sound classification. In: Kůrková V, Manolopoulos Y, Hammer B, Iliadis L, Maglogiannis I, eds. *Artificial Neural Networks and Machine Learning – ICANN 2018. ICANN 2018. Lecture Notes in Computer Science, 11141*. Springer; 2018. doi:10.1007/978-3-030-01424-7_21
126. Zhang J, Wang H-S, Zhou H-Y, et al. Real-world verification of artificial intelligence algorithm-assisted auscultation of breath sounds in children. *Front Pediatr*. 2021;9:627337. doi:10.3389/fped.2021.627337
127. Chen MY, Huang CC. Application of time-frequency analysis and back-propagation neural network in the lung sound signal recognition. *Appl Mech Mater*. 2012;190-191:927-930. www.scientific.net/AMM.190-191.927
128. Grzywalski T, Belluzzo R, Piecuch M, et al. Fully interactive lungs auscultation with AI enabled digital stethoscope. In: *Artificial Intelligence in Medicine: Proceedings of the 17th Conference on Artificial Intelligence in Medicine, AIME 2019*, Poznan, Poland; 2019:31-35. doi:10.1007/978-3-030-21642-9_5
129. Salekin MS, Zamzmi G, Paul R, et al. Harnessing the power of deep learning methods in healthcare: neonatal pain assessment from crying sound. In: *2019 IEEE Healthcare Innovations and Point of Care Technologies (HI-POCT)*, Bethesda, MD, USA; 2019:127-130. doi:10.1109/HI-POCT45284.2019.8962827
130. Alzantot M, Balaji B, Srivastava M. Did you hear that? Adversarial examples against automatic speech recognition. In: *31st Conference on Neural Information Processing Systems (NIPS 2017)*, Long Beach, CA, USA. 2018 https://www.synergylabs.org/bharath/files/Alzantot_MachineDeception_DidYouHearThat.pdf
131. Cisse M, Adi Y, Neverova N, Keshet J. Houdini: fooling deep structured visual and speech recognition models with adversarial examples. In: *Proceedings of the 31st International Conference on Neural Information Processing Systems (NIPS'17)*, Long Beach, California, USA; 2017:6980-6990. doi:10.5555/3295222.3295441

132. Vaidya T, Zhang Y, Sherr M, Shields C. Cocaine noodles: exploiting the gap between human and machine speech recognition. In: *WOOT'15: Proceedings of the 9th USENIX Conference on Offensive Technologies*, Washington DC, USA; 2015:1-16. doi:10.5555/2831211.2831227
133. Carlini N, Wagner D. Audio adversarial examples: targeted attacks on speech-to-text. In: *2018 IEEE Security and Privacy Workshops (SPW)*, San Francisco, CA, USA; 2018:1-7. doi:10.1109/SPW.2018.00009
134. Zhang J, Zhang B, Zhang B. Defending adversarial attacks on cloud-aided automatic speech recognition systems. In: *SCC'19: Proceedings of the Seventh International Workshop on Security in Cloud Computing*; 2019:23-31. doi:10.1145/3327962.3331456
135. Gong Y, Yan D, Mao T, Wang D, Wang R. Defending and detecting audio adversarial example using frame offsets. *KSII Trans Intern Inform Syst*. 2021;15(4):1538-1552. doi:10.3837/tiis.2021.04.019
136. Ren Z, Baird A, Han J, Zhang Z, Schuller B. Generating and protecting against adversarial attacks for deep speech-based emotion recognition models. In: *ICASSP 2020–2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Barcelona, Spain; 2020:7184-7188. doi:10.1109/ICASSP40776.2020.9054087
137. Li C, Xu Y, Tang J, Liu W. Quantum blockchain: a decentralized, encrypted and distributed database based on quantum mechanics. *J Quant Comput*. 2019;1(2):49-63. doi:10.32604/jqc.2019.06715
138. Gao Y-L, Chen X-B, Xu G, Yuan K-G, Liu W, Yang Y-X. A novel quantum blockchain scheme base on quantum entanglement and DPoS. *Quant Inform Process*. 2020;19:420.
139. Krishnaswamy D. Quantum blockchain networks. In: *Mobihoc'20: Proceedings of the Twenty-First International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*; 2020:327-332. doi:10.1145/3397166.3412802
140. Dabbagh M, Kakavand M, Tahir M, Amphawan A. Performance analysis of blockchain platforms: empirical evaluation of hyperledger fabric and ethereum. In: *2020 IEEE 2nd International Conference on Artificial Intelligence in Engineering and Technology (IICAIET), Kota Kinabalu, Malaysia*;2020:1-6. doi:10.1109/IICAIET49801.2020.9257811
141. Al-Sumaidaee G, Alkhudary R, Zilic Z, Swidan A. Performance analysis of a private blockchain network built on Hyperledger fabric for healthcare. *Inf Process Manag*. 2023;60(2):103160.
142. Panait AE, Olimid RF. On using zk-SNARKs and zk-STARKs in blockchain-based identity management. In: Maimut D, Oprina AG, Sauveron D, eds. *Innovative Security Solutions for Information Technology and Communications. SecITC 2020. Lecture Notes in Computer Science, 12596*. Springer; 2021:130-145. doi:10.1007/978-3-030-69255-1_9
143. Chen J, You F. Application of homomorphic encryption in blockchain data security. In: *EITCE'20: Proceedings of the 2020 4th International Conference on Electronic Information Technology and Computer Engineering*; 2020:205-209. doi:10.1145/3443467.3443754
144. Olegovich KD. Overview of privacy preserving technologies for distributed ledgers. *Eur J Math Comput Appl*. 2021;9(1):55-58.
145. Akhtar Z. From blockchain to hashgraph: distributed ledger technologies in the wild. In: *2019 International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, Aligarh, India; 2019:1-6. doi:10.1109/UPCON47278.2019.8980029
146. Panwar A, Bhatnagar V. Distributed ledger technology (DLT): the beginning of a technological revolution for blockchain. In: *2nd International Conference on Data, Engineering and Applications (IDEA)*, Bhopal, India; 2020:1-5. doi:10.1109/IDEA49133.2020.9170699

How to cite this article: Shinde R, Patil S, Kotecha K, Potdar V, Selvachandran G, Abraham A. Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions. *Trans Emerging Tel Tech*. 2024;35(1):e4884. doi: 10.1002/ett.4884