Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 607-625
https://doi.org//10.47514/kjcs/2024.1.3.0015

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Artificial Intelligence & Blockchain Technology in Modern Telehealth Systems-A Systematic Review

Odunayo E. Oduntan[1*], Hassan J. Bature[1], Daniel D. Wisdom[2], Ugwunna C. Okechukwu[3], Samson Isaac[4] and Cathrine F. Falayi[5]

[1*, 2]Department of Computer Sciences, Chrisland University Abeokuta, Ogun State, Nigeria.
[1]Department of Computer Sciences, Federal University Oye-Ekiti, Ekiti State, Nigeria,
[4]Department of Computer Science, Kaduna State University, Kaduna, Nigeria
[3,5]Department of Computer Sciences, Federal University of Agriculture Abeokuta, Ogun State, Nigeria,
eoduntan@chrislanduniversity.edu.ng[1*], joshua.hassan@fuoye.edu.ng[3], ddaniel@chrislanduniversity.edu.ng[3], ugwunnnaco@funaab.edu.ng[3], samson.isaac@kasu.edu.ng[4], falayi.febisolac@pg.funaab.edu.ng[5]

Abstract

Background: *Telehealth systems have significantly transformed healthcare delivery, particularly in remote areas. However, traditional telehealth models face substantial security and privacy challenges, which hinder their effectiveness and safety.* ***Aim:*** *This study aims to explore the potential of Artificial Intelligence (AI) and blockchain technology in addressing the security vulnerabilities and privacy concerns in telehealth systems and to propose an integrated solution that enhances the efficiency, security, and scalability of these systems.* ***Methodology:*** *The Study presents a survey on existing research on telehealth, and challenges, evaluating AI's role in improving healthcare delivery through data analytics and blockchain's ability to secure healthcare data. The study introduces the Smart Secure Telehealth (SST) algorithm, combining AI and blockchain in an eight-step telehealth operation model covering system initialization, patient data handling, and AI-powered analysis.* ***Result:*** *The paper presents a robust, secure, and scalable telehealth framework. The study highlights the necessity of integrating AI and blockchain for a more secure, patient-centered telehealth system, with potential future improvements including IoT integration for enhanced health monitoring. In addition, the survey presents important gaps for further studies. The proposed Smart Secure Telehealth (SST) algorithm presents a robust solution that may enhances the security, efficiency, and scalability of telehealth systems, paving the way for a more secure and patient-centered healthcare future, if carefully implemented.*

Keywords: Telehealth, AI, Blockchain-Technology, Challenges & Data Security.

1. Introduction

Telehealth, which uses technology to deliver healthcare services remotely, has become an essential part of modern healthcare. By allowing patients to access care without needing to physically visit a clinic or hospital, telehealth offers unprecedented convenience, especially in areas where access to healthcare is limited. Over recent years, its importance has surged, fueled by advancements in technology and the growing demand for more accessible healthcare solutions. Among the transformative technologies emerging in this field are Artificial Intelligence (AI) and blockchain. These tools are being recognized for their potential to improve healthcare delivery by enhancing data analysis, security, and efficiency (Jabarulla & Lee, 2021). Telehealth now plays a key role in the digital transformation of healthcare, making it easier for patients to consult doctors, receive diagnoses, and even undergo treatment remotely (Wisdom *et al.*, 2023a). The rise of telehealth has been driven by its ability to overcome geographical barriers and deliver healthcare services to patients in remote or underserved areas. In many parts of the world, access to healthcare is limited by distance, transportation difficulties, and a lack of nearby medical facilities. Telehealth bridges these gaps by connecting patients with healthcare professionals through digital platforms, allowing consultations, follow-up care, and monitoring to occur without physical proximity

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 607-625
https://doi.org//10.47514/kjcs/2024.1.3.0015
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

(Gudu *et al.,* 2024).This technology becomes even more critical during emergencies, such as natural disasters, pandemics, or sudden medical crises. In these situations, telehealth provides an efficient way to deliver care to those who need it most. For instance, during the COVID-19 pandemic, telehealth proved invaluable as healthcare systems worldwide became overwhelmed. It allowed patients to receive medical attention without the risk of exposure, alleviating the pressure on hospitals and ensuring continuous care for those with chronic conditions (Wisdom *et al.,* 2021). By enabling rapid access to medical advice and support during emergencies, telehealth has the potential to save lives when traditional healthcare systems are strained.

Beyond emergencies, telehealth's benefits extend into routine healthcare services. It has become a fundamental component of modern healthcare, offering ongoing care, chronic disease management, mental health support, and preventive services. The ability for patients to receive care from the comfort of their homes enhances convenience and reduces the need for travel, making healthcare more accessible to those who might otherwise face barriers due to location, mobility, or other constraints. Telehealth has particularly helped individuals with chronic conditions who require continuous monitoring and care, enabling them to avoid frequent hospital visits (Garba *et al.,* 2023).As telehealth continues to evolve, integrating advanced technologies such as AI and blockchain is becoming increasingly important. AI, with its powerful data analytics capabilities, can enhance the efficiency and accuracy of telehealth services. For example, AI-driven algorithms can analyze patient data, identify patterns, and provide early warnings of potential health issues, helping doctors make more informed decisions. AI can also enable personalized treatment plans, optimize the scheduling of appointments, and ensure that patients receive timely care.

In telehealth, AI can assist with triage by quickly assessing a patient's symptoms and directing them to the appropriate level of care. This is especially valuable in high-demand environments, where healthcare professionals may not have the time or resources to handle every case in detail. Through AI-powered analysis, telehealth systems can prioritize urgent cases, provide personalized recommendations, and reduce the burden on healthcare staff by automating routine tasks (Wisdom *et al.,* 2024a). Blockchain technology, on the other hand, offers a solution to one of the most significant challenges in telehealth: ensuring the security and privacy of patient data. In traditional telehealth systems, patient information is transmitted across various platforms, which can expose sensitive data to hacking, breaches, or unauthorized access. Blockchain's decentralized and transparent nature provides a way to securely manage healthcare data. Each transaction or data exchange is recorded in an immutable ledger, ensuring that patient information remains secure, traceable, and tamper-proof.

The integration of blockchain can also address the challenge of interoperability in healthcare systems. Different healthcare providers often use disparate systems that do not communicate effectively with one another, leading to fragmented patient data and inefficiencies. By using blockchain, healthcare providers can create a unified, secure platform where patient information is accessible across multiple systems without compromising privacy or security (Jabarulla & Lee, 2021). This not only streamlines operations but also ensures that patients' health records are complete and up-to-date, regardless of where they receive care. While telehealth offers numerous benefits, it also raises significant concerns about the security and privacy of patient information. Healthcare data is one of the most sensitive forms of personal information, and telehealth platforms are prime targets for cyberattacks. Data breaches can result in the exposure of private medical records, financial information, and other personal details, leading to identity theft and other harmful consequences for patients (Wisdom *et al.,* 2024b). To address these challenges, this paper proposes a solution that integrates AI and blockchain to create a secure, efficient, and scalable telehealth system. The proposed Smart Secure Telehealth (SST) algorithm leverages the strengths of both AI and blockchain to protect patient data while enhancing the quality of care. Through AI-powered analysis, the system can provide accurate diagnoses, personalized treatment recommendations, and real-time monitoring, improving the overall efficiency of telehealth services. Blockchain ensures that all patient data is securely stored, shared, and managed, preventing unauthorized access and tampering (Wisdom *et al.,* 2024c).

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 607-625
https://doi.org//10.47514/kjcs/2024.1.3.0015
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

The SST algorithm works through an eight-step process designed to ensure security, compliance, and continuous improvement. This process begins with system initialization, where users and healthcare professionals are authenticated using blockchain technology to create a secure environment. Next, patient data is collected and encrypted using blockchain, ensuring that it remains private and tamper-proof throughout its lifecycle. AI is then used to analyze the data, providing real-time insights that assist healthcare professionals in making informed decisions (Wisdom *et al.*, 2024d).

As part of the system's continuous improvement process, AI continuously learns from the data it processes, enabling it to deliver increasingly accurate diagnoses and treatment recommendations over time. Blockchain ensures that all changes to patient data are transparent and traceable, promoting compliance with healthcare regulations and protecting patient privacy (Wisdom *et al.*, 2024e).

Finally, Telehealth has emerged as a vital tool in transforming healthcare access, especially in remote and underserved areas. It provides critical healthcare services during emergencies and offers ongoing care to patients in diverse situations. However, telehealth faces challenges related to data security and privacy, which must be addressed to ensure its continued growth and adoption. By integrating AI and blockchain, the proposed Smart Secure Telehealth (SST) algorithm provides a robust solution that enhances the security, efficiency, and scalability of telehealth systems, paving the way for a more secure and patient-centered healthcare future. Figure 1 presents an AI-Powered Healthcare Systems scenario.

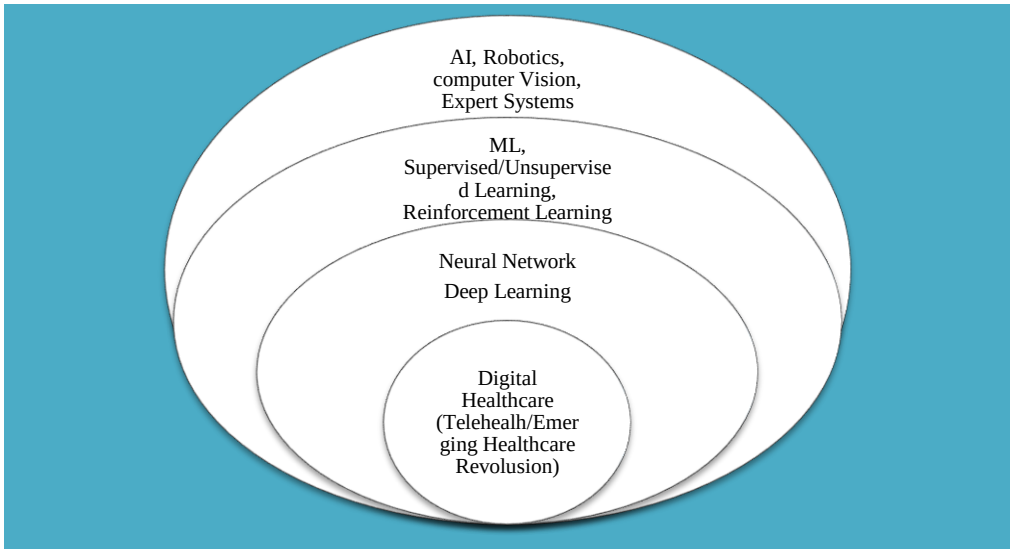


Figure 1: AI-Powered Healthcare Systems

2 Related Works

Telehealth systems offer a convenient way for patients to receive healthcare but also present vulnerabilities concerning data security and patient privacy. One of the primary concerns is data privacy. Telehealth platforms collect sensitive patient information, including medical records and personal details, which can be exploited if breached (Li *et al.*, 2021). The cybersecurity risks in traditional telehealth systems, such as hacking and malware attacks, are another major challenge. These risks can lead to unauthorized access to sensitive data, posing serious threats to patient privacy.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

A common issue is inadequate encryption. Without proper encryption, data transmitted during telehealth consultations can be intercepted by malicious actors. Furthermore, the lack of strong authentication methods allows unauthorized access to patient records, increasing the risk of impersonation and data breaches. Another problem arises from third-party risks, where telehealth platforms rely on external service providers for data storage and video conferencing. These providers may not always implement sufficient security measures, making patient data vulnerable. In addition, telehealth systems must comply with data protection regulations such as HIPAA or GDPR, adding complexity and cost. Failing to comply can result in legal and financial consequences. Lastly, device and network security is a concern since telehealth sessions occur over various devices, often on insecure networks. These devices may be susceptible to malware or phishing attacks, further compromising patient information. To address these challenges, telehealth systems need robust security measures, including encryption, strong authentication, and regular security audits. Educating both patients and healthcare providers on the importance of data security is also essential.

Traditional telehealth systems face several critical challenges and limitations that impact data security and patient privacy. One major issue is inadequate encryption protocols. Many systems fail to use strong encryption, leaving patient data vulnerable during transmission. This weakness allows malicious actors to intercept and exploit sensitive information, compromising confidentiality (Al-Fuqaha *et al.*, 2015). Another challenge is the vulnerability of communication channels. Telehealth platforms often use internet-based messaging and video conferencing tools, which may have unencrypted communication pathways or be susceptible to man-in-the-middle attacks. These vulnerabilities jeopardize the privacy of patient data (Alhassoun *et al*., 2019). Insufficient authentication mechanisms further exacerbate the problem. Weak or absent authentication can lead to unauthorized access to patient records and communications. Without robust authentication measures, there is a risk of impersonation, where malicious actors could gain access to confidential medical information. Data storage risks also pose significant concerns. Telehealth systems store extensive patient data on servers or in the cloud. Inadequate security for these repositories can result in unauthorized access or data breaches, exposing patients to identity theft and other privacy violations (Wisdom *et al.*, 2023a).

Additionally, reliance on third-party service providers for hosting and data storage increases the risk of data breaches if these providers do not implement stringent security standards. Compliance with data protection regulations like HIPAA or GDPR adds complexity and cost, particularly for smaller healthcare providers. Device and network security is another critical issue. Telehealth consultations occur over various devices and networks, including smartphones and home Wi-Fi. The security of these devices and networks can vary, making them susceptible to malware, phishing, and other attacks (Wisdom *et al.*, 2023b). To address these challenges, a unique approach could involve the development of a unified telehealth security framework that integrates advanced technologies such as, AI and blockchain. This framework could offer enhanced encryption, real-time threat detection, and decentralized data storage, providing a comprehensive solution to the security and privacy issues in telehealth systems. This paper presents a survey on Artificial Intelligence & Blockchain Technology in Modern Telehealth Systems revealing emerging technologies for the evolution of the healthcare systems. The study employs a Systematic Literature Review (SLR) methodology in conducting comprehensive exploratory learning of relevant existing studies on telehealth systems using the novel preferred reporting Item Metha-Analysis (PRISMA). The paper conducted a systematic review study as presented in Table 1, providing a comprehensive Summary of various findings on telehealth systems. In the survey, a search strategy was developed and utilized to identify unique databases in search of up-to-date, relevant research Articles on telehealth. An initial search yielded 72 articles, which were subjected to screaming, after careful study of the abstracts, methodology and the

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 607-625
https://doi.org//10.47514/kjcs/2024.1.3.0015
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

findings. 55 of the articles were discarded some due to paywall, improper methodology and lack of potential further research gap. After careful screening of the retrieved articles 17 were found suitable and are presented in table 1. The study presents open research gap for further studies. Table 1. Presents a Summary of Related studies.

Table.1. Summary of Related Works

References	Research Focus	Objectives	Methodology	Results/Findings	Limitations /Weakness	What is Missing	Future Work
Ahmed *et al.*, 2022.	The research focuses on developing a smart healthcare system that leverages Artificial Intelligence (AI) and Blockchain technology to monitor and detect COVID-19 in biomedical images.	Develop a blockchain and AI-enabled system for COVID-19 detection. Enhance data security and analytics quality in the healthcare sector.	A multi-layer deep learning architecture was developed and implemented. Gradient-weighted Class Activation Mapping (Grad-CAM) was used for visualization of test results.	The proposed deep learning architecture achieved a classification accuracy rate of 0.96. The system provided reliable data gathering and promising security solutions for COVID-19 data analytics.	The paper does not discuss the system's performance in real-world scenarios or its scalability. The deep learning model's performance on data other than the benchmark data set is not explored.	here is no analysis of how the system performs with diverse or unstructured data. Details on the integration of the system with existing healthcare infrastructures are missing.	Extend the research to analyze and segment other viral infections. Explore different segmentation approaches based on deep learning for the classification and detection of various viral diseases.
Mozumder, *et al.*, 2023.	The paper explores how integrating the metaverse with AI, blockchain, and IoT technologies can enhance digital anti-aging healthcare, improve service quality, and extend patient life expectancy.	Highlight the benefits of using the metaverse in healthcare. Discuss the integration of AI, blockchain, and IoT in digital anti-aging. Identify challenges and propose future directions for implementing these technologies.	The paper reviews potential use cases and technologies in the metaverse environment. It discusses the integration of AI for personalized treatment, blockchain for data security, and IoT for real-time data collection.	Integration of AI, blockchain, and IoT in the metaverse can significantly enhance healthcare delivery. These technologies offer potential for more personalized, secure, and efficient care. Improved patient outcomes and reduced healthcare costs are anticipated benefits.	Specific technical and practical challenges in implementing these technologies are not fully addressed.	There is a lack of detailed analysis on how to practically implement and integrate these technologies within existing healthcare systems. The paper does not explore potential barriers or limitations in the adoption of metaverse technologies in healthcare.	Explore specific use cases and develop practical solutions for integrating AI, blockchain, and IoT in the metaverse.
Wisdom *et al.*, 2021	The research focuses on developing a comprehensive	To address the growing concern of cybersecurity	Developed and implemented a	The proposed algorithm effectively reduces the risk of	The study was primarily theoretical,	Empirical testing of the algorithm in live healthcare environments.	Conduct a detailed empirical study in real-

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 607-625
https://doi.org//10.47514/kjcs/2024.1.3.0015
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

	cybersecurity algorithm to mitigate risks in healthcare systems, with an emphasis on preventing unauthorized access to sensitive patient data and reducing the risk of data breaches.	threats in the healthcare industry. To develop a robust algorithm that incorporates regular risk assessments, strong authentication, access control measures, employee training, encryption of data, software updates, and incident response plans.	comprehensive algorithm using Python programming, incorporating multi-factor authentication and role-based access control to restrict unauthorized access.	data breaches and enhances the protection of sensitive patient data. The research demonstrated the importance of integrating multiple layers of security (e.g., risk assessments, access control, encryption, and employee training) to enhance cybersecurity in healthcare systems.	relying on a review of existing literature and simulated implementation without empirical testing in real-world healthcare environments.	Detailed analysis of the challenges healthcare institutions might face during the implementation of the algorithm. Consideration of the cost and resource implications for smaller healthcare providers when adopting the proposed security measures.	world healthcare settings to test the algorithm's effectiveness. Gather data on cybersecurity incidents before and after implementing the algorithm to measure its impact. Explore integrating emerging technologies enhance the robustness of the cybersecurity algorithm.
Aithal, *et al.*, 2021.	The paper focuses on the application of blockchain technology within the healthcare industry. It examines current implementations, potential benefits, and challenges of blockchain technology in various healthcare sectors, including security, data management, and clinical trials.	To review and analyze the potential applications of blockchain technology in healthcare. To identify current implementations and challenges faced by blockchain technology in healthcare services. To propose future research agendas for improving blockchain integration in healthcare.	The study is descriptive and exploratory, relying on a systematic review of secondary sources, including scholarly literature from various journals and databases.	The paper identifies several areas where blockchain can enhance healthcare services, such as healthcare security, clinical trials, data management, and telemedicine. It highlights the advantages of blockchain in terms of data integrity, transparency, and decentralization. The study also outlines several challenges and limitations, including network speed, transaction costs, and interoperability issues.	Complexity and the need for cryptographic mechanisms make blockchain technology challenging to implement. speeds as blockchain networks grow. Data quality and security concerns due to potential vulnerabilities in blockchain systems.	The paper does not provide detailed case studies or real-world examples of successful blockchain implementations in healthcare. It lacks specific quantitative data on the impact of blockchain technology on healthcare outcomes. There is limited discussion on the practicalities and cost implications of implementing blockchain technology in existing healthcare infrastructures.	Developing methods to achieve 100% security, transparency, Exploring blockchain applications in more specific healthcare contexts, such as personalized medicine and public health surveillance. Investigating the integration of blockchain with other emerging technologies in healthcare.
Wisdom *et al.*, 2021	Mitigating cybersecurity risks in healthcare	To address cybersecurity threats in healthcare by	Developed and implemented the	The proposed algorithm reduced the risk of data breaches and	The study lacks empirical validation in	Empirical testing of the algorithm in actual healthcare environments.	Explore the integration of emerging technologies

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

	systems by developing a comprehensive algorithm that prevents unauthorized access and reduces the risk of data breaches.	proposing a robust algorithm that enhances data protection through regular assessments, authentication measures, employee training, and other security protocols.	proposed algorithm using Python programming code, incorporating multi-factor authentication and role-based access control.	improved the security of patient data through the integration of strong cybersecurity measures.	real-world healthcare settings to test the algorithm's practical effectiveness.	Evaluation of challenges in real-world implementation.	like AI and blockchain to further strengthen healthcare cybersecurity measures.
Jabarulla, *et al.*, 2021.	Developing a decentralized, patient-centric healthcare framework using blockchain and AI to enhance public healthcare responses during the COVID-19 pandemic.	To address the limitations of existing digital healthcare technologies exposed by the COVID-19 pandemic by improving data sharing, privacy, data management, and the efficiency of healthcare delivery using blockchain and AI.	The use of federated learning, where AI models are trained on COVID-19 data while preserving patient privacy, with global AI model parameters aggregated from various nodes.	Conceptual improvements in interoperability, secure data ownership, enhanced medical research through AI, and privacy-preserving federated learning. No specific results were detailed in the provided text.	Lack of empirical evidence or real-world case study results to demonstrate the framework's effectiveness. Absence of quantitative data to substantiate improvements in healthcare management	Practical validation of the framework in real healthcare settings. Quantitative analysis of its impact during health crises like pandemics.	Implement and test the framework in real-world healthcare environments. Refine AI models for greater accuracy and explore broader applications of blockchain in healthcare.
Shaikh, 2023.	The research focuses on the integration of Blockchain Technology and Artificial Intelligence (AI) in the healthcare system. It examines how these technologies can enhance security, interoperability, and overall performance in healthcare applications.	propose a framework for integrating Blockchain Technology and Artificial Intelligence in the healthcare system. To explore how these technologies can improve performance, security, and transparency in sharing medical data.	It discusses the integration of Blockchain and AI in healthcare, outlines various potential applications, and identifies challenges and opportunities based on existing literature and theoretical frameworks.	has the potential to enhance the performance and interoperability of healthcare systems. Challenges and limitations are identified, such as the need for more research and the lack of experts in the field.	lack of experts and insufficient research to fully understand and develop these technologies securely and efficiently. It acknowledges that Blockchain and AI are not a cure-all solution for all healthcare challenges.	The article lacks detailed exploration of the limitations and practical implementation challenges of Blockchain and AI in real-world healthcare settings.	Future work should focus on implementing these technologies with electronic medical records and evaluating their effectiveness using various AI techniques.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Wisdom *et al.*, 2023c.	Enhancing the security of healthcare systems by integrating advanced cybersecurity measures such as AI, machine learning, and encrypted communication methods.	To explore and address the challenges posed by cyber threats to healthcare systems and to propose comprehensive cybersecurity strategies, including emerging technologies like blockchain.	Performed qualitative assessments of cybersecurity incidents and emerging technologies to mitigate risks.	Evaluates the potential impact of AI, machine learning, and blockchain on improving healthcare system security.	The study lacks empirical testing or real-world application of the proposed cybersecurity strategies in healthcare settings.	Practical implementation of the cybersecurity strategies in actual healthcare environments to assess their effectiveness.	Explore further integration of newer technologies and continuously update cybersecurity practices to combat evolving digital threats.
Jabaru & Lee, 2021	The research focuses on integrating blockchain and artificial intelligence (AI) technologies to develop a decentralized, patient-centric healthcare system. The goal is to address challenges posed by the COVID-19 pandemic and improve healthcare delivery by enhancing data privacy, interoperability, and predictive capabilities.	To propose a conceptual framework for a decentralized, patient-centric healthcare system that integrates blockchain and AI technologies. To explore how this framework can improve interoperability among healthcare stakeholders, secure patient data, and enhance medical research and treatment	The paper uses a conceptual approach to propose a framework integrating blockchain and AI for a patient-centric healthcare system. It includes an exploration of the potential applications of this integrated approach in combating COVID-19, emphasizing how these technologies can be applied in real-world scenarios.	The proposed framework enhances interoperability between different healthcare stakeholders and provides patients with secure control over their health data. Blockchain technology helps reduce siloed patient data and supports federated learning, allowing AI models to be trained on decentralized data while maintaining privacy. The integrated system can improve traditional public health strategies for COVID-19, including contact tracing, outbreak management, and clinical data handling.	The paper does not provide empirical data or case studies to demonstrate the practical implementation and effectiveness of the proposed framework. There may be challenges related to the adoption and integration of blockchain and AI technologies in existing healthcare systems, including technical and regulatory hurdles.	Detailed case studies or real-world implementations of the proposed framework are not provided. The paper lacks a comprehensive discussion on the technical and logistical challenges of integrating blockchain and AI into existing healthcare systems. There is limited exploration of the cost implications and resource requirements for implementing the proposed technologies.	Conduct empirical research and pilot projects to validate the proposed framework and its applications in real-world healthcare settings. Explore the technical and regulatory challenges of integrating blockchain and AI technologies and develop strategies to address these issues. Investigate the scalability of the proposed solutions and their effectiveness in various healthcare contexts beyond the COVID-19 pandemic.
Gudu *et al.*, 2021.	Developing a mathematical model to analyze and control the transmission	To provide actionable strategies to control COVID-19 transmission	Created and simulated a mathematical model that calculated	Completely eradicating the disease requires vaccinating 75% of both infected	Achieving the necessary vaccination levels and	Real-time, practical application of the model to manage COVID-19 spread	Integrating IoT technologies to better map and manage disease spread.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

	dynamics of COVID-19 in Nigeria, with a focus on achieving disease-free equilibrium and managing the endemic state.	through vaccination and prevention measures.	epidemiological markers like R0. Analyzed the impact of different vaccination and prevention strategies on the disease spread.	and susceptible populations, which is difficult to achieve. Reducing R0 below 1 is crucial, but managing the disease through increased vaccination and preventive measures is a more viable approach.	maintaining prevention practices consistently is challenging.	through IoT technologies and more data-driven methods.	Developing more active measures to mitigate the risks of future infectious disease outbreaks and enhance the predictive capabilities of the model.
Kim, & Huh, 2020	The research focuses on the integration of artificial intelligence (AI) and blockchain technology in healthcare systems, specifically targeting the management and security of personal health records (PHR). It explores how these technologies can enhance the verification, security, and efficiency of healthcare data systems.	To evaluate how artificial neural networks and blockchain technology can be applied to personal health records (PHR) in the healthcare system. To propose and verify frameworks and algorithms for integrating these technologies to improve data security, privacy, and efficiency.	The paper uses conceptual analysis and framework development to address the integration of AI and blockchain technology in healthcare. The study involves theoretical exploration and experimentation with blockchain consensus algorithms and neural networks for healthcare data management.	AI and blockchain technologies can enhance the security, transparency, and integrity of personal health records. Various frameworks and algorithms were presented to improve the accuracy and reliability of healthcare data systems. Challenges related to the scalability, security, and regulatory aspects of blockchain technology were identified.	The study acknowledges that blockchain technology is still immature and faces issues with scalability and security, which hinder its application in the medical industry. There are difficulties in reconciling blockchain's immutable nature with evolving legal and regulatory requirements.	The paper lacks detailed empirical data or real-world case studies demonstrating the practical application and effectiveness of the proposed frameworks. There is limited discussion on how the proposed solutions can be practically implemented and scaled in existing healthcare systems.	Future work should explore the integration of blockchain with evolving legal frameworks and privacy regulations. The development of practical implementations and pilot projects to validate the proposed frameworks in real-world healthcare settings is suggested.
Gudu *et al.*, 2024.	Developing a mathematical model to simulate the spread and control of COVID-19 using quarantine strategies facilitated by treatment centers.	To decrease and mitigate the global rise in COVID-19 cases by creating a mathematical model that predicts outcomes based on various quarantine and	A compartmental model based on a non-linear ordinary differential equation approach was developed.	Increasing treatment rates leads to higher recovery rates. Early detection and treatment significantly reduce the spread of COVID-19. The model's predictions were supported by	There was no mention of comparing the model's predictions with actual COVID-19 case data to validate its accuracy and real-world	Validation of the model with real-world data. A practical application of the model in real-time public health scenarios.	Integrating Internet of Things (IoT) technologies to map infection spread more effectively. Incorporating real-time data and predictive analytics to enhance public

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

		treatment strategies.	The population was divided into six compartments.	simulations displayed in figures.	applicability.		health management and responses to future outbreaks.
El-Sheri *et al.*, 2022	The paper focuses on the role of digital health services, specifically telehealth and artificial intelligence (AI), in responding to the COVID-19 pandemic. It examines how these technologies can address healthcare challenges during the pandemic and proposes best practices for future healthcare systems.	To explore the adoption and impact of digital health services, including telehealth and AI, in managing the COVID-19 pandemic. To address privacy, transparency, and safety concerns associated with AI in healthcare.	The paper provides a comprehensive overview and analysis of digital health services and their applications during the COVID-19 pandemic. It discusses theoretical and practical aspects of AI and telehealth, emphasizing their benefits and challenges.	Digital health services, including AI and telehealth, have been crucial in managing the COVID-19 pandemic by providing remote monitoring, diagnostics, and decision-making support. AI has shown potential in various applications such as detection, therapy monitoring, and predicting disease patterns. Telehealth has expanded access to healthcare, reduced exposure risk, and optimized resource use during the pandemic.	The paper does not provide empirical data or specific case studies demonstrating the practical implementation of AI and telehealth solutions. There is limited discussion on the technical challenges and limitations faced during the implementation of these technologies in different healthcare settings.	Detailed case studies or real-world examples showcasing successful applications of AI and telehealth during the COVID-19 pandemic. An in-depth analysis of the barriers and enablers for widespread adoption of these technologies in various healthcare systems.	Address privacy, security, and regulatory challenges to facilitate the safe deployment of AI and telehealth technologies. Develop strategies for integrating AI and telehealth into existing healthcare systems to enhance resilience and preparedness for future health crises.
Kumar, *et al.*, 2023	The paper focuses on the integration of artificial intelligence (AI) and blockchain technology within the healthcare sector. It explores how these technologies can enhance healthcare services, improve data security, and address various	To provide a comprehensive review of AI and blockchain technologies and their applications in healthcare. To discuss the integration of AI with blockchain and how it can enhance the efficiency and security of healthcare systems.	The paper is a review article that synthesizes findings from 120 research articles on AI-powered blockchain applications in healthcare. It provides an overview of the conceptual and	AI and blockchain integration has the potential to significantly enhance healthcare by improving data security, automating data analysis, and facilitating secure management of EHRs and other medical records. Applications of AI-powered blockchain include EHR	The paper does not provide empirical data or specific case studies that demonstrate practical implementations of AI-powered blockchain in healthcare. limited discussion on the	Detailed case studies or real-world examples showcasing successful implementations of AI and blockchain technologies in healthcare. In-depth analysis of specific technical challenges faced during the integration of these technologies.	Develop strategies to address these technologies' privacy, security, and legal challenges. Explore ways to enhance the integration of AI and blockchain in various healthcare applications to improve data management

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

	challenges in public health.	To identify the open challenges and limitations of current AI-powered blockchain systems in healthcare.	functional aspects of AI and blockchain technologies.	management, remote health monitoring, bioinformatics, clinical trial management, drug discovery, and outbreak prediction.	technical details and real-world challenges of integrating AI and blockchain technologies.		and patient care.
Bublitz, *et al.*, 2019	The study aims to provide an overview of the use of these technologies in addressing environmental impacts on health.	provide a review of AI, Blockchain, and IoT technologies and their application in health and environmental data collection. To present a high-level reference architecture for potential use in the pan-Canadian surveillance system.	. The authors propose a software architecture for integrating AI, Blockchain, and IoT into future health and environmental monitoring systems.	These technologies are already in use in various sectors for data collection, remote monitoring, and surveillance. The authors propose a reference architecture that integrates these technologies into a cohesive framework for monitoring environmental impacts on health	There is a lack of public trust in the use of disruptive technologies for health monitoring. The paper does not provide empirical evidence or case studies demonstrating the proposed architecture in real-world applications, focusing primarily on conceptual ideas.	Practical case studies or pilot studies that demonstrate the implementation of the proposed technologies in real-world scenarios. Detailed discussion of the regulatory and ethical challenges that may arise during the integration of these technologies into health surveillance.	The paper suggests conducting pilot studies to test the proposed architecture and to refine it based on the results. There is a call for more research into the legal, ethical, and privacy issues surrounding the integration of AI, Blockchain, and IoT into health and environmental surveillance.
Pap, & Onig 2022	The paper highlights how AI has been integrated into remote healthcare services, especially in the wake of the COVID-19 pandemic, and the potential of AI to enhance healthcare delivery in remote and underserved areas.	To provide an overview of technologies used in eHealth, focusing on the role of AI. To explore the use of AI in various healthcare sectors, particularly in remote monitoring and data analysis.	The paper focuses on case studies and applications where AI has been successfully integrated into telemedicine and other eHealth systems.	The paper highlights specific applications like AI in cardio-oncology and seizure prediction, demonstrating the technology's real-world benefits in healthcare.	discussion on ethical and regulatory challenges associated with the widespread use of AI in eHealth. They do not explore the scalability of AI solutions across diverse healthcare systems.	The paper does not provide detailed case studies or pilot projects that evaluate the long-term effectiveness of AI in eHealth. There is limited attention to the potential privacy and security risks posed by AI-based eHealth systems.	Future work could explore the integration of AI with other emerging technologies, such as blockchain, to improve data security and trust in eHealth systems.
Bawany, *et*	The research aims to improve the privacy,	To design and develop a blockchain-	they proposed the BlockHeal	It demonstrated successful application across	The research focuses on the	There is limited discussion on the ethical and legal	Future research will involve

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

al., 2022	security, and efficiency of telehealth services using blockchain technology, addressing limitations in existing telehealth systems.	based telehealth framework that consolidates all healthcare services and stakeholders. To ensure secure, transparent, and decentralized data management in telehealth using blockchain technology.	framework, which integrates blockchain technology to provide a secure and fault-tolerant telehealth system. The framework was validated using several healthcare use cases.	six healthcare scenarios, showcasing the effectiveness of blockchain technology in delivering secure, timely, and trusted healthcare services.	technological solution without addressing potential regulatory and legal challenges that could impact the large-scale adoption of blockchain-based telehealth services.	implications of using blockchain in healthcare. It lacks detailed consideration of how BlockHeal can be scaled up for widespread adoption across diverse healthcare systems.	refining the framework based on feedback from the pilot project and exploring additional functionalities to enhance telehealth services further.

3 Methodology

This section presents how AI can transform telehealth. **Advanced Diagnostics**: AI-powered diagnostic tools can analyze medical images, such as X-rays, MRIs, and CT scans, with remarkable accuracy and speed. Machine learning algorithms can detect patterns and anomalies in medical images, assisting healthcare providers in making more timely and accurate diagnoses. This capability can significantly improve patient outcomes by enabling early detection of diseases and conditions. **Personalized Treatment Plans**: AI algorithms can analyze vast amounts of patient data, including medical history, genetic information, and lifestyle factors, to develop personalized treatment plans tailored to individual patient needs. By considering various factors unique to each patient, AI can optimize treatment efficacy and minimize adverse effects, leading to better health outcomes. **Continuous Remote Patient Monitoring**: AI-powered remote monitoring systems enable continuous tracking of patients' vital signs, symptoms, and medication adherence outside traditional healthcare settings. These systems use sensors, wearable devices, and AI algorithms to detect deviations from baseline health parameters and alert healthcare providers to potential issues in real time. Continuous monitoring allows for early intervention, reducing the likelihood of hospital readmissions and improving patient management. **Virtual Health Assistants**: AI-driven virtual health assistants, powered by natural language processing (NLP) and machine learning, can interact with patients in real time, answering questions, providing medical advice, and assisting with appointment scheduling and medication reminders. These virtual assistants offer convenient access to healthcare services, enhance patient engagement, and streamline administrative tasks for healthcare providers. **Predictive Analytics:** AI algorithms can analyze large datasets to identify trends, predict disease outbreaks, and assess population health risks. By leveraging predictive analytics, telehealth systems can proactively address public health challenges, allocate resources more efficiently, and implement preventive interventions to improve community health outcomes. **Clinical Decision Support Systems**: AI-based clinical decision support systems provide healthcare providers with evidence-based recommendations and guidelines at the point of care. These systems integrate patient data, medical literature, and clinical guidelines to assist healthcare providers in making informed decisions about diagnosis, treatment, and management plans. finally, AI has the potential to revolutionize telehealth by enhancing diagnostic accuracy, personalizing treatment approaches, enabling continuous monitoring, improving patient engagement, and optimizing healthcare delivery. As AI technologies continue to advance, telehealth

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 607-625
https://doi.org//10.47514/kjcs/2024.1.3.0015
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

platforms will increasingly leverage these capabilities to provide more accessible, efficient, and patient-centered care (Wisdom *et al.*, 2023c). Figure 2 presents Transformative tools in the Healthcare systems.

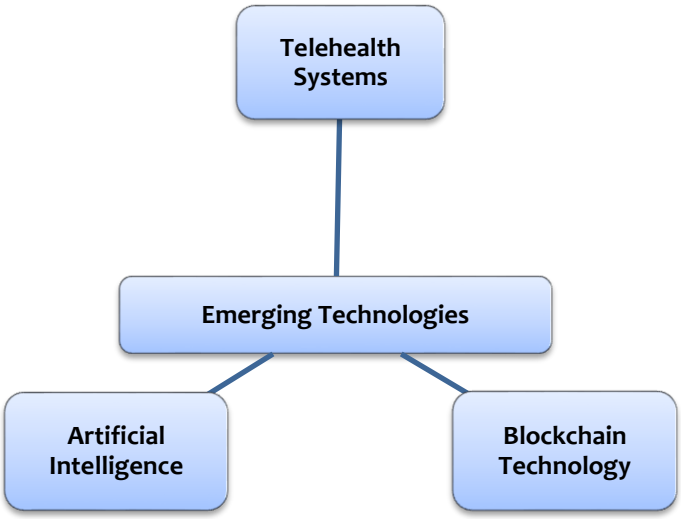


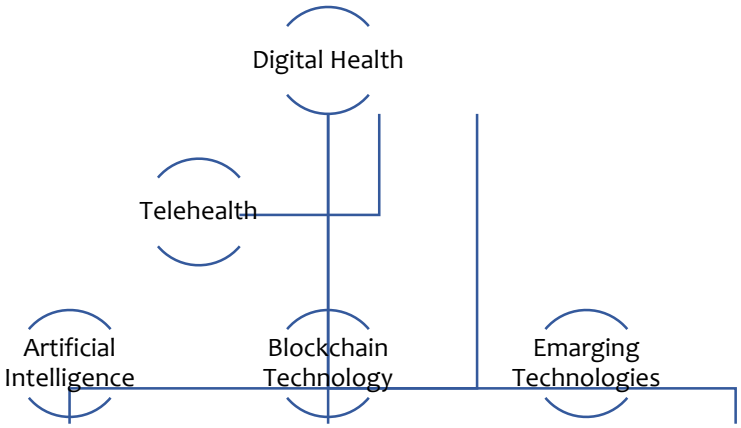
Figure 2: Transformative tools in the Healthcare systems

4 Results and Discussion

Blockchain technology holds significant promise in revolutionizing the healthcare industry by addressing critical issues such as data security, integrity, and transparency. At its core, blockchain is a decentralized and immutable ledger that records transactions across a network of computers. The fundamental features of blockchain, including decentralization and data immutability, align closely with the requirements of secure and transparent healthcare data management (Gudu, *et al.*, 2024, Wisdom, *et al.*, 2023).

1. **Decentralization:** Traditional healthcare data management systems often suffer from centralized control, making them vulnerable to breaches and data manipulation. In contrast, blockchain operates on a decentralized network, where data is distributed across multiple nodes. This decentralized structure eliminates the need for a central authority, reducing the risk of a single point of failure and enhancing resilience against cyber-attacks (Wisdom, *et al.*, 2024c).
2. **Data Immutability**: In blockchain, once a transaction is recorded and verified, it is cryptographically sealed into a block and linked to previous blocks, forming a chain of immutable records. This immutability ensures that once data is entered into the blockchain, it cannot be altered or deleted retroactively without consensus from the network participants. In healthcare, where data integrity is paramount, this feature assures that patient records, treatment histories, and other sensitive information remain tamper-proof and trustworthy. Figure 3 presents an Emerging Revolution in the Digital Health Systems

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 607-625
https://doi.org//10.47514/kjcs/2024.1.3.0015
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng



4.1 The Need for Secure and Transparent Healthcare Data Ecosystem

The increasing digitization of healthcare data has led to a growing imperative for a secure and transparent healthcare data ecosystem. With the proliferation of electronic health records (EHRs), medical IoT devices, and telemedicine platforms, the volume and complexity of healthcare data have surged, amplifying the risks associated with data breaches, unauthorized access, and data manipulation.

1. **Data Security**: Healthcare data, which includes highly sensitive information such as patient diagnoses, treatment plans, and billing details, is a prime target for cybercriminals. Data breaches not only compromise patient privacy but also pose serious financial and reputational risks to healthcare organizations. By leveraging blockchain technology's cryptographic protocols and decentralized architecture, healthcare stakeholders can enhance data security and protect against unauthorized access and malicious attacks (Terziyan, *et al.*, 2023).

2. **Data Integrity**: Maintaining the integrity of healthcare data is essential for ensuring accurate diagnoses, effective treatment outcomes, and compliance with regulatory requirements. However, traditional data management systems lack robust mechanisms for detecting and preventing data tampering. By harnessing blockchain's immutable ledger, healthcare providers can track the entire lifecycle of patient data, from creation to sharing, while ensuring its integrity and authenticity (. Nazir, *et al.*, 2021).

3. **Data Transparency**: Transparency in healthcare data management is crucial for fostering trust among patients, healthcare providers, and other stakeholders. Patients should have visibility into how their data is collected, shared, and used, while healthcare providers require access to accurate and up-to-date information for delivering quality care. Blockchain technology enables transparent and auditable data transactions, enabling real-time access to reliable healthcare data without compromising privacy or security. By combining the power of artificial intelligence (AI) and blockchain, healthcare organizations can unlock new opportunities for improving patient outcomes, streamlining administrative processes, and advancing medical research. AI algorithms can analyze vast amounts of healthcare data to extract valuable insights and facilitate personalized treatments, while blockchain ensures the integrity, security, and transparency of this data throughout its lifecycle. Together, AI and blockchain form a formidable synergy that holds the potential to reshape the future of healthcare delivery and management.

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 607-625
https://doi.org//10.47514/kjcs/2024.1.3.0015
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

4.2 Rising Concerns About Healthcare Data Security

In recent years, there has been a significant rise in concerns regarding healthcare data security, driven by an escalating number of data breaches and patient privacy violations. Healthcare organizations face mounting pressure to safeguard sensitive patient information from malicious actors seeking to exploit vulnerabilities in digital systems. These breaches not only compromise patient privacy but also erode trust in the healthcare system and can have far-reaching consequences for individuals and institutions alike. Amidst this backdrop of heightened concerns, our research takes on paramount importance in addressing these pressing challenges and fortifying the security and privacy of healthcare data. By exploring the intersection of artificial intelligence (AI) and blockchain technology in telehealth, we aim to develop innovative solutions that offer robust protection against data breaches and unauthorized access while ensuring patient confidentiality and trust. AI-powered algorithms play a pivotal role in enhancing healthcare data security by identifying anomalies, detecting potential threats, and enabling proactive responses to security incidents. Additionally, blockchain technology offers a decentralized and immutable framework for storing and managing healthcare data, mitigating the risk of tampering, manipulation, and unauthorized access (Wisdom, *et al.,* 2024b). By leveraging the combined strengths of AI and blockchain, our research endeavors to create a secure and transparent healthcare data ecosystem that prioritizes patient privacy and confidentiality. Furthermore, our research aims to provide practical insights and actionable strategies for healthcare organizations to strengthen their cybersecurity posture and mitigate the risk of data breaches. By identifying emerging threats, analyzing best practices, and offering guidance on regulatory compliance, we empower healthcare stakeholders to safeguard sensitive patient information effectively. Therefore, the rising concerns about healthcare data security emphasize the critical need for innovative approaches to protect patient privacy and confidentiality. this research seeks to address these challenges head-on by harnessing the power of AI and blockchain technology to fortify the security and privacy of healthcare data, ultimately enhancing trust and confidence in the healthcare system while providing vital education on telehealth systems (Wisdom, *et al.,* 2024e).

4.3 Smart Secure Telehealth (SST) Algorithm

To effectively leverage both Artificial Intelligence (AI) and Blockchain technology in modern telehealth systems, we propose a strategic algorithm called, **Smart Secure Telehealth (SST).** This algorithm is designed to enhance the efficiency, security, and reliability of telehealth services. A step-by-step procedure of the SST algorithm is presented as follows.

Pseudocode

```
Algorithm SST

// Step 1: System Initialization
BEGIN
   Initialize telehealth system
   Load AI libraries and Blockchain protocols
   Configure network settings
   Set up security protocols (e.g., encryption, authentication)

// Step 2: Patient Data Handling
BEGIN
   Input patient data (medical history, symptoms)
   Encrypt patient data using advanced encryption (e.g., AES, ECC)
   Store encrypted patient data securely in blockchain
```

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 607-625
https://doi.org//10.47514/kjcs/2024.1.3.0015
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

```
// Step 3: AI-Powered Analysis
BEGIN
   Retrieve encrypted patient data from blockchain
   Decrypt data for AI analysis
   Analyze patient data using AI algorithms (e.g., machine learning models)
   Generate insights (e.g., health predictions, treatment recommendations)
   Encrypt analysis results
   Store encrypted analysis results back in blockchain

// Step 4: Blockchain for Data Integrity and Access Management
BEGIN
   Record all transactions and data handling operations on blockchain
   Use smart contracts to manage data access permissions
   Ensure access is limited to authorized personnel (e.g., doctors, healthcare providers)

// Step 5: Real-Time Monitoring and Alerts
BEGIN
   Monitor system performance and access logs in real-time
   Detect unusual activities or security threats
   IF security threat detected THEN
      Generate alert/notification
      Initiate security protocol to mitigate the threat
   END IF

// Step 6: Telehealth Service Delivery
BEGIN
   Provide telehealth services (e.g., virtual consultation, remote patient monitoring)
   Maintain data privacy and integrity during service delivery
   Use secure communication channels for healthcare provider-patient interaction

// Step 7: Compliance and Reporting
BEGIN
   Verify compliance with data protection regulations (e.g., HIPAA, GDPR)
   Generate compliance reports and audit trails
   Address non-compliance issues as needed

// Step 8: Continuous Improvement and Scalability
BEGIN
   Collect user feedback (from patients and healthcare providers)
   Analyze system performance metrics
   Identify areas for improvement
   Update AI algorithms and blockchain protocols as required
   Scale system to support additional users and data
END Algorithm SST
```

This structured pseudocode outlines each step clearly, detailing the system's flow from initialization to continuous improvement.

The Smart Secure Telehealth (SST) algorithm is designed to enhance telehealth services by leveraging AI and blockchain technologies.

Step 1: System Initialization, Set up a private blockchain network for secure and transparent logging of all telehealth interactions. Integrate AI models for predictive analytics, diagnosis assistance, and personalized treatment. Ensure seamless interaction between AI and blockchain for data handling.

Step 2: Patient Data Handling, Collect patient data through wearables, mobile apps, and consultations. Anonymize data where necessary and store it securely on the blockchain, benefiting from its encryption and decentralization features.

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 607-625
https://doi.org//10.47514/kjcs/2024.1.3.0015
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Step 3: AI-Powered Analysis, Process collected data with AI algorithms to predict diseases, monitor health, and issue emergency alerts. Implement a feedback loop to continuously refine AI algorithms based on new data and outcomes, enabling self-learning capabilities.
Step 4: Blockchain for Data Integrity and Access Management, Record patient interactions and AI insights on the blockchain to ensure immutability and traceability. Use smart contracts to manage access rights, ensuring only authorized personnel can view sensitive data.
Step 5: Real-time Monitoring and Alerts, Deploy AI systems for continuous health data monitoring, detecting deviations or potential issues. Set up automatic alerts to notify healthcare providers of anomalies requiring immediate attention.
Step 6: Telehealth Service Delivery, facilitate secure virtual consultations using blockchain for identity verification and AI for diagnostic support. Provide personalized treatment recommendations based on AI analysis, with all decisions recorded on the blockchain.
Step 7: Compliance and Reporting, Ensure compliance with health data protection regulations like HIPAA and GDPR through blockchain's secure framework. Implement automated reporting for patients and providers, storing health reports on the blockchain for secure access.
Step 8: Continuous Improvement and Scalability, Design the blockchain network to scale with increasing data and transactions. Regularly assess AI and blockchain performance to identify improvements and update the system as needed.
The SST algorithm aims to revolutionize telehealth by offering a secure, efficient, and intelligent platform for healthcare delivery while maintaining high standards of data privacy and system integrity. Future developments may include integrating IoT devices for expanded health monitoring.

5 Conclusion

Telehealth systems are crucial for improving healthcare access, especially in remote areas. However, telehealth systems face significant security and privacy issues that can compromise patient data. This Survey study highlights these challenges and proposes a solution using Artificial Intelligence (AI) and blockchain technology. AI enhances telehealth by analyzing data to improve care and operational efficiency. Blockchain, on the other hand, ensures secure and transparent data exchanges, protecting against cyber threats. The Smart Secure Telehealth (SST) algorithm integrates these technologies into a comprehensive framework. It involves eight key steps: initializing the system, handling patient data, analyzing with AI, using blockchain for data integrity and access, monitoring in real-time, delivering telehealth services, ensuring compliance, and continuously improving and scaling. The survey presents a secure, efficient, patient-focused telehealth system. While achieving fully secure telehealth is complex, the combination of AI and blockchain offers a promising solution. Future advancements, including integrating technologies such as IoT, will further enhance telehealth systems, making healthcare more accessible and resilient against cyber threats.

References

Ahmed, I., Chehri, A., & Jeon, G. (2022). Artificial intelligence and blockchain-enabled smart healthcare system for monitoring and detection of COVID-19 in biomedical images. *Journal of LaTeX Class Files, 22*(6), 1-10.

Jabarulla, M. Y., & Lee, H.-N. (2021). A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications. *MDPI*.

Mozumder, M. A. I., Armand, T. P. T., Uddin, S. M. I., Athar, A., Sumon, R. I., Hussain, A., & Kim, H.-C.(2023). Metaverse for digital anti-aging healthcare: An overview of potential use cases based on artificial

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

intelligence, blockchain, IoT technologies, its challenges, and future directions. *Applied Sciences, 13*(8), 5127. MDPI, https://doi.org/10.3390/app13085127

Wisdom, D. D., Vincent, O. R., Igulu, K. T., Arowolo, M. O., Hyacinth, E. A., Christian, A. U., Oduntan, O. E.,Baba, G. A., (2023a). Mitigating Cyber Threats in Healthcare Systems: The Role of Artificial Intelligence and Machine Learning, *Artificial Intelligence and Blockchain Technology in Modern Telehealth Systems.* Institute of Engineering and Technology (IET), UK.

Aithal, P. S., Aithal, A., & Dias, E. (2021). Blockchain technology - Current status and future research opportunities in various areas of the healthcare industry. *International Journal of Health Sciences and Pharmacy (IJHSP)*, 5(1), 130-150. https://doi.org/10.5281/zenodo.5105896

Wisdom, D. D., & Vincent, O. R. (2024a). Cybersecurity concerns and risks in emerging healthcare systems. Cybersecurity in Emerging Healthcare Systems, Institute of Engineering and Technology (IET), UK.

Shaikh, A. H. (2023). Challenges of blockchain technology using artificial intelligence in the healthcare system. *International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), 12*(1). https://doi.org/10.15680/IJIRSET.2023.1201010

Garba, A. B., Wisdom, D. D., & Igulu, K. T. (2023). Unlocking Efficiency: Leveraging AI and Machine Learningin Information Technology Management. *Annual International Conference on Computing and Technological Advancement (ICCTA-2023), 23rd-25th August 2023. Ignatius Ajuru University of Education*, Rumuolumeni, Port Harcourt, River State, Nigeria.

Kim, S.-K., & Huh, J.-H. (2020). Artificial neural network blockchain techniques for healthcare system: Focusingon the personal health records. Electronics, MDPI, 9(5), 763. https://doi.org/10.3390/electronics9050763.

Wisdom, D. D., Singh, T. P., Igulu, K. T., & Choudhary, R. (2023b). ChatGPT and its Impact on Humans-Computer Interaction: A Comprehension. In Proceedings of the 4th International Conference on Computational Intelligence & Internet of Things (ICCIIoT). Springer PROMS. 4-6, 2023. The Faculty of ICT, University of Malta, Msida, Malta.

Jabarulla, M. Y., & Lee, H.-N. (2021). A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications. *Healthcare, 9*(8), 1019. https://doi.org/10.3390/healthcare9081019.

Li, Y., Zhou, Z., & Zhang, Q. (2021). A survey on 5G security: Challenges and solutions. *Future Generation Computer Systems*, 119, 339-354.

Wisdom, D. D., Garba, A. B., & Igulu, K. T. (2023c). Strategic Integration of AI/ML in General Management: A Paradigm Shift in Decision-Making. *In Annual International Conference on Computing and Technological Advancement (ICCTA-2023), 23rd-25th August 2023. Ignatius Ajuru University of Education, Rumuolumeni*, Port Harcourt, River State, Nigeria.

Attar, A., Stavrou, A., & Voas, J. (2019). The Internet of Things: A survey of topics and trends. IEEE Communications Surveys & Tutorials, 21(2), 1250-1284.

Wisdom, D. D., Odewale, O. O., Ajayi, E. A., & Hamza, M. K. (2019). Cybercrime: A threat to a moral society. *In Proceedings of the 2nd International Conference on Education and Development (ITED)* (pp. 364-375). Baze University, Abuja, Nigeria.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Surveyon Enabling Technologies, Protocols, and Applications.IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

Wisdom, D. D., Christian, A. U., Igulu, K., Hyacinth, E. A., Odunayo, O. E. & Umar, B. (2024b). Industrial IoT Security Infrastructure and Threats. In A. Prasad, T.P. Singh and S.D. Sharma(Eds.), *Communication technologies in IoT and their security challenges: Present and future. Springer Nature.*

El-Sherif, D. M., Abouzid, M., Elzarif, M. T., Ahmed, A. A., Albakri, A., & Alshehri, M. M. (2022). Telehealth and artificial intelligence insights into healthcare during the COVID-19 pandemic. *Healthcare, 10*(2), 385.https://doi.org/10.3390/healthcare10020385

Alhassoun, N. S., Uddin, M. Y. S., & Venkatasubramanian, N. (2019). Context-aware energy Optimization for perpetual IoT-based safe communities. SustainableComputing: Informatics and Systems, 22, 96-106. doi: 10.1016/j.suscom.2019.05.010.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Wisdom, D. D., Vincent, O. R., Igulu, K., Christian, A. U., Hyacinth, E. A., Baba, G. A., Esther, O. O. (2024c). The Protection of Industry 4.0 and 5.0: Cybersecurity Strategies and Innovations, *CI-Industry-4.0: Computational Intelligence in Industry 4.0 and 5.0 Applications*. *Taylor and Francis group.*

Kumar, R., Arjunaditya, Singh, D., Srinivasan, K., & Hu, Y.-C. (2023). AI-powered blockchain technology for public health: A contemporary review, open challenges, and future research directions. *Healthcare, 11*(1), 81. https://doi.org/10.3390/healthcare11010081.

Gudu, E. B., Wisdom, D. D., Igulu, K., Hyacinth, E. A., Christian, A. U., Hauni, A. G., Senchi, J. D., Baba, G. A., Esther, O. O. (2024). Transmission dynamics of COVID-19 virus disease. *Artificial Intelligence in Biomedical and Modern Healthcare Informatics, Elsevier,* 2024.

Nazir, A., Sholla, S., & Bashir, A. (2021). Internet of Things Security: Issues, Challenges and Counter-Measures. International Journal of Advanced Computer Science and Applications, 12(2), 165-172. https://doi.org/10.14569/IJACSA.2021.0120207.

Bublitz, F. M., Oetomo, A., Sahu, K. S., Kuang, A., Fadrique, L. X., Velmovitsky, P. E., Nobrega, R. M., &Morita, P. P. (2019). Disruptive technologies for environment and health research: An overview of artificial intelligence, blockchain, and the internet of things. *International Journal of Environmental Research and Public Health, 16*(20), 3847. https://doi.org/10.3390/ijerph16203847.

Wisdom, D. D., Christian, A. U., Hyacinth, E. A., Igulu, K., Oduntan, O. E., & Umar, B. (2024d). Mitigating Cybersecurity Risks in Healthcare: Best Practices and Strategies, *Proceeding of International Conference on Computing and Technological Advancements, 2024*

Terziyan, V., Malyk, D., Golovianko, M., & Branytskyi, V. (2023). Encryption and Generation of Images for Privacy-Preserving ML in Smart Manufacturing. In Proceedings of the 4th International Conference on Industry 4.0and Smart Manufacturing, Procedia Computer Science, 217, 91-101. 27.

Wisdom, D.D., Vincent, O.R., Abayomi-Alli, A., Olusegun, F., Ayetuoma, I.O., & Baba, G.A. (2024e) Security Measures in Computational Modeling and Simulations, In CRC Computational Taylor and Francis, 2024.

Pap, I. A., & Oniga, S. (2022). A review of converging technologies in eHealth pertaining to artificial intelligence. *International Journal of Environmental Research and Public Health, 19*(18), 11413. https://doi.org/10.3390/ijerph191811413

Wisdom, D. D., Igulu, K., Esther, O. O., Baba, G. A., Ahmad, A., & Sidi, A. (2021). A Review of Best Practices and Methods of Mitigating Cybersecurity Risks in Healthcare Systems and a Newly Proposed Algorithm. Computology: *Journal of Applied Computer Science and Intelligen Technologies*, 1 (2), 27-36. DOI: 10.17492/computology. v1i2.2104.

Bawany, N. Z., Qamar, T., Tariq, H., & Adnan, S. (2022). Integrating healthcare services using blockchain-based telehealth framework. *IEEE Access, 10*, 36505–36519. https://doi.org/10.1109/ACCESS.2022.3161944.

Gudu, E. B., Wisdom, D. D., Joseph, G. G., Ahmad, M. A., Isaac, S., & Akinyemi, E. A. (2021). Mathematical recipe for curbing coronavirus (COVID-19) transmission dynamics. In Data Science for COVID-19: Computational perspectives (pp. 527-545). Elsevier. https://doi.org/10.1016/B978-0-12-824536-1.00013-7.