Journal of Frontiers in Multidisciplinary Research

Integrating AI, Blockchain, and Big Data to Strengthen Healthcare Data Security, Privacy, and Patient Outcomes

Ernest Chinonso Chianumba [1*], Nura Ikhalea [2], Ashiata Yetunde Mustapha [3], Adelaide Yeboah Forkuo [4], Damilola Osamika [5]

[1] Data Analyst, Dozie & Dozie's Pharmaceuticals Limited, Nigeria
[2] Independent Researcher, Texas, USA
[3] Kwara State Ministry of Health, Nigeria
[4] Independent Researcher, Ghana
[5] Department of Environmental Health, Margaret Mosunmola College of Health Science and Technology, Nigeria

* Corresponding Author: **Ernest Chinonso Chianumba**

Article Info
E-ISSN: 3050-9726
P-ISSN: 3050-9718
Volume: 03
Issue: 01
January-June 2022
Received: 27-11-2021
Accepted: 25-12-2021
Published: 22-01-2022
Page No: 124-129

Abstract
This paper presents a conceptual model for integrating Artificial Intelligence (AI), Blockchain, and Big Data to enhance healthcare data security, privacy, and patient outcomes. The rapid digitization of healthcare has led to an increase in the volume and complexity of healthcare data, which in turn has raised significant challenges regarding data protection and patient privacy. The paper explores the potential of AI, blockchain, and big data to mitigate these challenges and improve the quality of care. AI is examined for its role in securing sensitive data through encryption, improving decision-making processes, and detecting security threats. Blockchain is explored for its ability to ensure data integrity, decentralize storage, and facilitate secure data sharing through smart contracts. Furthermore, big data analytics is discussed for its capacity to predict patient outcomes, integrate diverse healthcare data sources for holistic insights, and ensure privacy compliance. Despite the promise of these technologies, the paper also addresses the technical, regulatory, and operational challenges associated with their adoption, and proposes risk mitigation strategies. Finally, the future outlook highlights emerging AI, blockchain, and big data innovations that could further strengthen healthcare data security and improve patient care.

DOI: https://doi.org/10.54660/.IJFMR.2022.3.1.124-129

Keywords: Healthcare Data Security, Artificial Intelligence (AI), Blockchain Technology, Big Data Analytics, Patient Outcomes, Data Privacy

1. Introduction

1.1 Overview of healthcare data security and privacy challenges

Healthcare data security and privacy have emerged as critical concerns as the industry has increasingly moved toward digitalization. Sensitive patient information, such as medical records and personal health data, are frequently stored and exchanged electronically, which has made them vulnerable to cyber threats, unauthorized access, and data breaches [1, 2]. Healthcare organizations, while adopting advanced technology for more efficient patient care, often face challenges in implementing robust data security measures due to the complexities of health data management [3, 4]. The rise in cyberattacks, particularly ransomware, targeted at healthcare institutions highlights the increasing risks. Additionally, gaps in healthcare personnel training, inadequate security protocols, and insufficient data encryption practices contribute to the ongoing challenges of safeguarding sensitive information [5, 6].

As healthcare systems rely on a multitude of digital platforms for data sharing, the threat landscape continues to expand. The evolving nature of privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S., complicates the compliance process [7]. Healthcare data breaches not only jeopardize patient privacy but can also result in significant financial losses, legal repercussions, and damaged reputations for institutions. Addressing these challenges requires a multifaceted approach that includes technological advancements, policy changes, and enhanced risk management strategies [8-10].

1.2 Importance of AI, blockchain, and big data in healthcare

Artificial Intelligence (AI), blockchain, and big data are transforming healthcare by offering innovative solutions to longstanding data security and privacy issues. AI, with its ability to process and analyze large volumes of data, is a key enabler in the identification of security threats and vulnerabilities [11]. By using machine learning algorithms, AI can detect anomalies in real-time, providing healthcare organizations with the necessary tools to prevent unauthorized access and protect patient data proactively. Moreover, AI-driven tools can help enhance the precision of healthcare decision-making, improving patient care outcomes while adhering to privacy requirements [12-14].
Blockchain, known for its decentralized and immutable nature, offers a robust solution for ensuring the integrity and transparency of healthcare data. By recording transactions in a secure, unalterable ledger, blockchain can significantly reduce the risk of data tampering, providing a transparent audit trail that strengthens data privacy [15]. Big data analytics, on the other hand, is reshaping healthcare by enabling the integration and analysis of diverse datasets, including clinical, genetic, and behavioral data. These technologies support better clinical decision-making and contribute to the broader goal of improving healthcare accessibility and outcomes, particularly in underserved regions. Together, these technologies hold the promise of a more secure, efficient, and equitable healthcare ecosystem [16-18].

1.3 Purpose and scope of the conceptual model

The purpose of this paper is to propose a conceptual model that integrates AI, blockchain, and big data to enhance healthcare data security, privacy, and patient outcomes. The model aims to leverage the unique strengths of each technology to address the multifaceted challenges faced by healthcare providers in managing sensitive data. Combining AI's predictive capabilities, blockchain's decentralized security, and big data's analytical power, the paper seeks to provide a framework that healthcare organizations can adopt to protect patient information, improve decision-making processes, and ultimately enhance patient care.
The scope of the model includes its application across a variety of healthcare settings, with a particular focus on those that are underserved and vulnerable to data breaches. The conceptual model will explore how these technologies can be integrated into existing healthcare infrastructures to optimize data security protocols, streamline patient data management, and ensure compliance with privacy regulations. Through a strategic and holistic approach, this paper aims to demonstrate how the combination of AI, blockchain, and big data can create a resilient and future-proof healthcare system that prioritizes both security and patient outcomes.

2. AI in healthcare data security and privacy

2.1 AI for data protection and encryption

Artificial Intelligence (AI) plays a crucial role in securing sensitive healthcare data, particularly through advanced encryption techniques. With the increasing digitization of healthcare records, AI-driven encryption systems are capable of adapting and evolving to meet the demands of protecting large amounts of health data [19]. Machine learning algorithms, a subset of AI, are employed to enhance encryption methods by analyzing patterns and predicting potential vulnerabilities in data storage and transmission. These algorithms can continuously monitor and update encryption protocols to address emerging threats, ensuring that healthcare data remains protected even as cyberattack tactics evolve [20, 21].
Moreover, AI can also support encryption key management, making it easier for healthcare organizations to maintain strong access controls. By automating key generation and distribution processes, AI reduces the risk of human error and ensures that sensitive data is accessible only to authorized personnel. This adaptive, intelligent approach to encryption helps secure health information both in transit and at rest, mitigating the risks posed by increasingly sophisticated cyberattacks [22, 23].

2.2 AI-driven healthcare decision-making

AI is revolutionizing healthcare decision-making by providing healthcare professionals with data-driven insights that enhance clinical judgments. Through predictive analytics, AI can process vast amounts of patient data to identify patterns and make recommendations that improve decision-making processes [24]. These systems analyze historical medical records, real-time data from wearable devices, and genetic information to predict disease progression and suggest personalized treatment plans. By automating data analysis, AI reduces human error, improves diagnostic accuracy, and helps healthcare providers make more informed decisions, ultimately leading to better patient outcomes [25, 26].
At the same time, AI tools are designed with privacy safeguards, ensuring that sensitive patient information remains secure. By utilizing advanced algorithms and maintaining a clear separation between sensitive data and actionable insights, AI can support decision-making without compromising privacy [27]. These AI systems not only help healthcare professionals make more accurate diagnoses but also optimize resource allocation and treatment strategies, ensuring that healthcare services are delivered efficiently and effectively, especially in resource-constrained settings [28, 29].

2.3 AI for threat detection and risk mitigation

AI technologies are increasingly being leveraged to detect potential security threats and mitigate risks proactively in healthcare environments. Machine learning models can continuously monitor healthcare networks for unusual activity, such as unauthorized access attempts or abnormal data transactions. By analyzing patterns in data flow and user behavior, AI can identify early warning signs of a data breach or cyberattack, alerting administrators before significant damage is done. These technologies can even predict potential vulnerabilities in systems, allowing for preemptive measures to be taken to secure healthcare data [30].
Additionally, AI-powered threat detection tools can operate in real-time, providing immediate responses to detected

threats. For example, AI can automate the process of isolating infected systems or blocking malicious IP addresses, significantly reducing the time between detection and response [31]. This proactive approach to security helps mitigate risks by preventing data breaches, ensuring the integrity of patient information, and safeguarding healthcare institutions from financial and reputational damage. As the volume and sophistication of cyber threats continue to grow, AI's ability to adapt and respond swiftly is crucial in maintaining a secure healthcare environment [32].

3. Blockchain for healthcare data integrity and privacy

3.1 Blockchain technology in healthcare systems

Blockchain technology has gained significant attention in healthcare due to its potential to secure data, improve access control, and ensure the integrity of patient information. Blockchain operates through a decentralized, distributed ledger that records transactions in a secure and immutable way. Each transaction, or "block," is verified by multiple participants in the network, making it nearly impossible for any single entity to alter the data. This makes blockchain particularly suitable for securing healthcare data, as it ensures that patient records and sensitive health information cannot be tampered with, providing an unprecedented level of trust and transparency [33].

In healthcare systems, blockchain can be used to store patient data in a manner that eliminates the need for centralized databases. Healthcare providers, patients, and other stakeholders can securely access and update data without the risk of unauthorized modifications [15]. Furthermore, blockchain's transparent nature allows all participants in the network to have a clear view of the data's history, enhancing accountability and reducing the likelihood of fraudulent activities. By leveraging blockchain technology, healthcare systems can significantly improve data integrity, privacy, and security, while also streamlining administrative processes [34].

3.2 Decentralized data storage and access control

One of the key benefits of blockchain technology is its decentralized approach to data storage and access control. Unlike traditional centralized systems, where data is stored in a single location and accessed by a central authority, blockchain distributes data across a network of participants, ensuring that no single entity controls the entire system [35]. This decentralization eliminates the risk of a single point of failure, making it more resilient to cyberattacks and data breaches. Each participant in the blockchain network has a unique cryptographic key that grants them access to specific data, and the blockchain ensures that access is granted only to authorized individuals or entities [36].

In healthcare, decentralized data storage offers enhanced privacy and security. Patients have control over their own data and can determine who has access to it, whether it is a healthcare provider, insurer, or researcher [37]. Access rights are managed through cryptographic keys, ensuring that data is shared only with authorized individuals. This approach provides patients with greater autonomy over their healthcare information, reduces the risk of data breaches, and enhances overall data security. Moreover, by ensuring that no single entity holds the data, blockchain eliminates the risk of data manipulation or unauthorized alterations, thus improving the integrity of healthcare information [15].

3.3 Smart contracts for secure data sharing

Blockchain-based smart contracts can play a pivotal role in facilitating secure, transparent, and auditable data sharing among healthcare providers. Smart contracts are self-executing contracts with the terms of the agreement directly written into lines of code [38]. These contracts automatically execute actions once predefined conditions are met, eliminating the need for intermediaries and reducing the potential for human error. In healthcare, smart contracts can be used to facilitate the secure exchange of patient data between hospitals, clinics, research institutions, and other healthcare providers, ensuring that data is shared in compliance with privacy regulations [39].

Smart contracts can enforce strict access control and data sharing protocols, ensuring that patient information is only shared when appropriate and with authorized parties. These contracts can also be programmed to ensure that patient consent is obtained before data is accessed or shared, maintaining privacy and regulatory compliance [40]. Additionally, because blockchain maintains a transparent and immutable ledger, all actions taken through smart contracts are auditable, providing a clear trail of data exchanges and helping to prevent fraudulent activity or unauthorized sharing of sensitive information. This transparency and automation make blockchain-based smart contracts a powerful tool for enhancing data security and trust in healthcare data sharing processes [41].

4. Big data in enhancing healthcare decision-making and outcomes

4.1 Big data analytics for patient outcome prediction

Big data analytics has transformed the way healthcare providers predict patient outcomes by enabling the processing and analysis of vast amounts of data from multiple sources. Predictive modeling, powered by big data, can identify patterns and trends in patient data that may not be immediately apparent through traditional diagnostic methods [42]. By analyzing historical patient records, clinical notes, laboratory results, and even genomic data, predictive models can forecast future health events, such as disease progression or the likelihood of complications. These insights allow healthcare professionals to intervene earlier, personalize treatment plans, and ultimately improve patient outcomes [42].

For instance, big data analytics can be used to predict which patients are at higher risk for chronic conditions, such as diabetes or heart disease, based on a variety of factors like age, family history, lifestyle, and previous health data. By integrating and analyzing this data, healthcare providers can offer targeted interventions, tailored to the individual needs of the patient. The ability to predict and prevent adverse health outcomes not only improves patient care but also reduces healthcare costs by preventing hospital readmissions and emergency interventions, leading to a more efficient healthcare system [43].

4.2 Data integration for holistic healthcare insights

Integrating various healthcare data sources is essential for providing holistic insights that support better decision-making. In healthcare, data is often siloed in different systems, such as electronic health records (EHRs), patient monitoring devices, and laboratory results [44]. Big data analytics allows these disparate data sources to be unified into a comprehensive view of a patient's health status. By combining information from EHRs, wearable devices, diagnostic tests, and even social determinants of health, healthcare providers can gain a more complete picture of a patient's well-being [45].

This integrated data approach enhances decision-making by enabling providers to identify correlations between various health factors and make more informed choices. For example, by combining wearable device data (e.g., heart rate, physical activity) with EHRs, healthcare providers can better monitor chronic conditions, track medication adherence, and optimize treatment plans. Furthermore, integrating data from various healthcare touchpoints supports the shift towards personalized medicine, where treatment and prevention strategies are tailored to the individual needs of the patient. This holistic approach leads to more effective healthcare interventions and better patient outcomes [46].

4.3 Privacy-enhanced big data solutions

As the use of big data in healthcare grows, so does the need to ensure that data is used ethically and securely. Privacy-enhanced big data solutions are designed to protect sensitive patient information while enabling the valuable insights that big data can provide. One of the key approaches to ensuring privacy in big data solutions is through the use of advanced anonymization and encryption techniques. Anonymizing data removes personally identifiable information (PII), allowing healthcare providers and researchers to analyze large datasets without compromising patient privacy. Additionally, encryption ensures that data is only accessible to authorized individuals, preventing unauthorized access or breaches [47].

Privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and the General Data Protection Regulation (GDPR) in Europe, impose strict requirements on how patient data should be handled. Big data solutions must be designed with these regulations in mind, ensuring that data usage complies with privacy laws [48]. One effective approach is the use of federated learning, where data remains on the source system (such as a hospital's local server), and only aggregated insights are shared. This method allows healthcare providers to benefit from big data analytics without transferring sensitive information, ensuring that patient privacy is maintained. By incorporating privacy-enhancing technologies, healthcare systems can harness the power of big data while safeguarding patient rights [49].

5. Conclude

5.1 Challenges of implementing AI, blockchain, and big data in healthcare

Implementing AI, blockchain, and big data in healthcare presents several technical, regulatory, and operational challenges. From a technical perspective, healthcare data systems are often fragmented, with patient data spread across multiple platforms and institutions, which makes integration and standardization difficult. Additionally, the complexity of healthcare data—ranging from structured clinical data to unstructured clinical notes—requires sophisticated algorithms and systems to process and analyze it effectively. Many healthcare providers also lack the necessary technical infrastructure to support advanced technologies like AI and blockchain, leading to gaps in deployment.

Regulatory challenges further complicate the adoption of these technologies. In healthcare, privacy regulations such as HIPAA in the U.S. and GDPR in Europe impose strict guidelines for data storage and sharing, making it difficult to implement systems like blockchain, which requires data to be distributed across decentralized networks. AI models must also meet regulatory requirements to ensure that they make accurate and unbiased predictions. The transparency and interpretability of AI algorithms are also a concern, as healthcare professionals must trust the decisions made by AI without fully understanding the underlying processes. Operationally, healthcare organizations must overcome resistance to change, invest in training, and ensure that their workforce is equipped to work with these technologies. The need for significant investment in resources and skilled personnel adds to the complexity of integrating these advanced technologies into healthcare systems.

5.2 Risk mitigation strategies

To mitigate the risks associated with AI, blockchain, and big data in healthcare, organizations can implement several strategies. First, comprehensive cybersecurity measures should be prioritized to safeguard sensitive data. For AI, ensuring robust validation processes and transparency in decision-making can help minimize errors in predictions. Regular audits of AI models for biases and performance validation against real-world data can improve accuracy and trustworthiness. In addition, healthcare institutions can invest in AI algorithms that offer explainability, enabling healthcare providers to understand the rationale behind AI-driven decisions.

For blockchain, ensuring that the underlying infrastructure is secure and resilient is essential. Healthcare organizations must adopt blockchain platforms with strong encryption and multi-factor authentication to safeguard data and prevent unauthorized access. Additionally, regular updates and patches must be applied to blockchain systems to address vulnerabilities. In terms of big data, encryption and anonymization techniques should be employed to maintain privacy and comply with regulatory requirements. Data governance frameworks are also necessary to ensure that data is ethically used and that patient consent is obtained before data is accessed or shared. To address data breaches, real-time monitoring and advanced threat detection systems should be deployed to identify and respond to potential security incidents quickly.

5.3 Future outlook and innovations

The future outlook for AI, blockchain, and big data in healthcare is promising, with continuous advancements poised further to strengthen data security, privacy, and patient outcomes. In AI, explainable AI (XAI) innovations are expected to enhance the transparency of decision-making processes, enabling healthcare providers to trust AI-driven recommendations. Additionally, AI models will become more refined with the integration of more diverse and larger datasets, improving the accuracy of predictions and treatment suggestions. AI-powered personalized medicine is also expected to advance significantly, offering even more tailored treatment plans based on individual patient data.

Blockchain innovations will likely focus on scalability and interoperability. Future blockchain solutions will allow for seamless integration with existing healthcare systems, enabling greater adoption while maintaining decentralized data control. Enhanced consensus algorithms and faster transaction speeds will address current limitations, making blockchain more efficient for real-time applications. In the big data space, the adoption of edge computing and federated learning is set to grow, ensuring that sensitive data remains secure and localized while still benefiting from big data analytics. These innovations will drive greater efficiency, improved data accuracy, and better decision-making processes, ultimately contributing to enhanced healthcare outcomes. As these technologies evolve, they will continue to provide powerful tools to tackle the complex challenges of healthcare data security and patient care.

6. References

1. Abisoye A, Akerele JI. A high-impact data-driven decision-making model for integrating cutting-edge cybersecurity strategies into public policy, governance, and organizational frameworks.
2. Abisoye A, Akerele JI, Odio PE, Collins A, Babatunde GO, Mustapha SD. Using AI and machine learning to predict and mitigate cybersecurity risks in critical infrastructure.
3. Abisoye A, Akerele JI, Odio PE, Collins A, Babatunde GO, Mustapha SD. A data-driven approach to strengthening cybersecurity policies in government agencies: best practices and case studies.
4. Adekunle BI, Chukwuma-Eke EC, Balogun ED, Ogunsola KO. A predictive modeling approach to optimizing business operations: a case study on reducing operational inefficiencies through machine learning.
5. Adelodun MO, Anyanwu EC. Evaluating the environmental impact of innovative radiation therapy techniques in cancer treatment.
6. Adelodun MO, Anyanwu EC. Global standards in radiation safety: a comparative analysis of healthcare regulations.
7. Ogunsola KO, Balogun ED, Ogunmokun AS. Enhancing financial integrity through an advanced internal audit risk assessment and governance model. 2021.
8. Ike CC, Ige AB, Oladosu S, Adepoju P, Afolabi AI. Advancing predictive analytics models for supply chain optimization in global trade systems. Int J Appl Res Soc Sci. 2023;6(12):1769. https://doi.org/10.51594/ijarss.v6i12.1769
9. Egbuhuzor NS, Ajayi AJ, Akhigbe EE, Agbede O, Ewim C, Ajiga D. Cloud-based CRM systems: revolutionizing customer engagement in the financial sector with artificial intelligence. Int J Sci Res Arch. 2021;3(1):215-34.
10. Ewim CP-M, Omokhoa HE, Ogundeji IA, Ibeh AI. Future of work in banking: adapting workforce skills to digital transformation challenges. Future. 2021;2(1).
11. Chattu VK. A review of artificial intelligence, big data, and blockchain technology applications in medicine and global health. Big Data Cogn Comput. 2021;5(3):41.
12. Adelodun MO, Anyanwu EC. Telehealth implementation: a review of project management practices and outcomes.
13. Abisoye A, Akerele JI. A practical framework for advancing cybersecurity, artificial intelligence and technological ecosystems to support regional economic development and innovation. Int J Multidiscip Res Growth Eval. 2022;3(1):700-13.
14. Achumie GO, Oyegbade IK, Igwe AN, Ofodile OC, Azubuike C. A conceptual model for reducing occupational exposure risks in high-risk manufacturing and petrochemical industries through industrial hygiene practices. 2022.
15. Yaqoob I, Salah K, Jayaraman R, Al-Hammadi Y. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput Appl. 2022:1-16.
16. Afolabi AI, Chukwurah N, Abieba OA. Implementing cutting-edge software engineering practices for cross-functional team success.
17. Afolabi AI, Chukwurah N, Abieba OA. Agile software engineering framework for real-time personalization in financial applications.
18. Isibor NJ, Ibeh AI, Ewim CP-M, Sam-Bulya NJ, Martha E. A financial control and performance management framework for SMEs: strengthening budgeting, risk mitigation, and profitability. 2022.
19. Wu H, Han H, Wang X, Sun S. Research on artificial intelligence enhancing internet of things security: a survey. IEEE Access. 2020;8:153826-48.
20. Ahmadu J, *et al*. The influence of corporate social responsibility on modern project management practices.
21. Alozie CE, Ajayi OO, Akerele JI, Kamau E, Myllynen T. Standardization in cloud services: ensuring compliance and supportability through site reliability engineering practices.
22. Alozie CE, Ajayi OO, Akerele JI, Kamau E, Myllynen T. The role of automation in site reliability engineering: enhancing efficiency and reducing downtime in cloud operations.
23. Chigboh VM, Zouo SJC, Olamijuwon J. Health data analytics for precision medicine: a review of current practices and future directions.
24. Gudavalli S, Tangudu A. AI-driven customer insight models in healthcare. Int J Res Anal Rev (IJRAR). 2020;7(2).
25. Edoh NL, Chigboh VM, Zouo SJC, Olamijuwon J. The role of data analytics in reducing healthcare disparities: a review of predictive models for health equity.
26. Famoti O, Adelodun MO, Abieba OA, Chukwurah N, Afolabi AI. Agile software engineering framework for real-time personalization in financial applications.
27. Wang C, Zhang J, Lassi N, Zhang X. Privacy protection in using artificial intelligence for healthcare: Chinese regulation in comparative perspective. Healthcare. 2022;10(10):1878.
28. Igunma TO, Adeleke AK, Nwokediegwu ZS. Developing nanometrology and non-destructive testing methods to ensure medical device manufacturing accuracy and safety.
29. Isibor NJ, Ewim CP-M, Ibeh AI, Adaga EM, Sam-Bulya NJ, Achumie GO. A generalizable social media utilization framework for entrepreneurs: enhancing digital branding, customer engagement, and growth.
30. Reddy ARP. The role of artificial intelligence in proactive cyber threat detection in cloud environments. NeuroQuantology. 2021;19(12):764–73.
31. Tanikonda A, Pandey BK, Peddinti SR, Katragadda SR. Advanced AI-driven cybersecurity solutions for proactive threat detection and response in complex ecosystems. J Sci Technol. 2022;3(1).
32. Wang B-X, Chen J-L, Yu C-L. An AI-powered network threat detection system. IEEE Access. 2022;10:54029–37.
33. Attaran M. Blockchain technology in healthcare: challenges and opportunities. Int J Healthc Manag.

2022;15(1):70–83.
34. Zaabar B, Cheikhrouhou O, Jamil F, Ammi M, Abid M. HealthBlock: a secure blockchain-based healthcare data management system. Comput Netw. 2021;200:108500.
35. Wang S, Zhang Y, Zhang Y. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access. 2018;6:38437–50.
36. Habib G, Sharma S, Ibrahim S, Ahmad I, Qureshi S, Ishfaq M. Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet. 2022;14(11):341.
37. 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.
38. Rodwal A. Blockchain and smart contracts in healthcare payments: securing transactions and reducing fraud. Int J Sci Eng. 2021;7(4):57–67.
39. Hewa TM, Hu Y, Liyanage M, Kanhare SS, Ylianttila M. Survey on blockchain-based smart contracts: technical aspects and future research. IEEE Access. 2021;9:87643–62.
40. 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 Netw Comput Appl. 2021;178:102950.
41. Saini A, Zhu Q, Singh N, Xiang Y, Gao L, Zhang Y. A smart-contract-based access control framework for cloud smart healthcare system. IEEE Internet Things J. 2020;8(7):5914–25.
42. Razzak MI, Imran M, Xu G. Big data analytics for preventive medicine. Neural Comput Appl. 2020;32(9):4417–51.
43. Du Z, Zhang X, Han Y, Li Q, Zhang J, Zhao Y, *et al*. Accurate prediction of coronary heart disease for patients with hypertension from electronic health records with big data and machine-learning methods: model development and performance evaluation. JMIR Med Inform. 2020;8(7):e17257.
44. Gade KR. Data-driven decision making in a complex world. J Comput Innov. 2021;1(1).
45. Jayaratne M, Alahakoon D, Lee YH, Nawaratne R, Perera N. A data integration platform for patient-centered e-healthcare and clinical decision support. Future Gener Comput Syst. 2019;92:996–1008.
46. Cohen DJ, Keller SR, Hayes GR, Dorr DA, Ash JS, Sittig DF. Integrating patient-generated health data into clinical care settings or clinical decision-making: lessons learned from project HealthDesign. JMIR Hum Factors. 2016;3(2):e5919.
47. Edwards A, Elwyn G. Shared decision-making in health care: achieving evidence-based patient choice. Oxford: Oxford University Press; 2009.
48. Determann L. Healthy data protection. Mich Tech Law Rev. 2019;26:229.
49. Terry N. Existential challenges for healthcare data protection in the United States. Ethics Med Public Health. 2017;3(1):19–27.