2025 4th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 | 979-8-3315-3536-0/25/$31.00 ©2025 IEEE | DOI: 10.1109/OTCON65728.2025.11070382

Ethics, Privacy, and Security Challenges in AI and Blockchain-Driven Digital Health Ecosystems

V. Rama Krishna,
Associate Professor, Cvr College Of Engineering, Hyderabad
rama.vishwa@gmail.com

Abdullah H. Maad
Department of Pharmaceutics, College of Pharmacy, University of Al-Ameed, Karbala, Iraq.
dr.ph.abdullah.maad@gmail.com

Ali Ihsan Alanssari
Al-Nisour University College, Nisour Seq. Karkh, Baghdad, Iraq
ali.ih.eng@nuc.edu.iq

Nour Rahim Nimah
Department of sciences/ Al-Manara College For Medical Sciences/ (Maysan)/Iraq
nourrahimnimah@uomanara.edu.iq

Kadim A. Jabbar
College of Technical Engineering, National University of Science and Technology, Dhi Qar, 64001, Iraq
kadim.jabber@nust.edu.iq

Praveen Thuniki
Independent Research
Sr Program Analyst, Georgia, USA
PraveenT.rd2323@gmail.com

***Abstract*— This article discusses how integrating AI and blockchain technology into digital health platforms might help and hurt privacy, fairness, transparency, and compliance. This research compares AI and blockchain technologies for making honest and ethical healthcare choices. We are investigating federated learning, homomorphic encryption, differential privacy, zero-knowledge proofs, self-sovereign identity systems, explainable AI, blockchain interface protocols, and privacy-preserving AI systems. We rated each technique based on data protection, ethical data collecting, computer justice, openness, and system security. While most approaches perform well in certain locations, they all have issues that may render them unsuitable for use in healthcare. The proposed solution addresses these concerns and outperforms speed standards. It evaluates ethical risks based on bias, fairness, and transparency and is continuously improving ethical decision-making. These evaluations improve healthcare AI systems' reliability, fairness, and clarity during decision-making. This implies its potential application in AI-driven healthcare systems.**

Keywords- AI, Algorithm fairness, Blockchain, Data protection, Differential privacy, Ethical AI, Explainable AI, Federated learning, Privacy-preserving techniques, Transparency.

I. INTRODUCTION

Combining AI and blockchain technology has transformed digital health settings, improving patient outcomes, data management, and healthcare delivery [1]. These technologies, which combine AI's data-driven insights with blockchain's secure, decentralized structure, might solve some of healthcare's major issues, such as scattered data and excessive pricing [2]. However, the growing utilization of these technologies presents ethical, privacy, and safety concerns that demand immediate and thorough investigation. This section will examine these issues, provide solutions, and highlight this work's main accomplishments.

AI and blockchain are revolutionizing digital health and growing rapidly [3]. AI is transforming healthcare with predictive analytics, individualized medication, and increased efficiency. Machine learning algorithms trained on large datasets may be able to diagnose diseases better than physicians [4]. Deep learning algorithms can use medical imagery to detect cancer, forecast its progression, and recommend treatments [5]. Blockchain makes health data ownership and sharing secure, making it ideal for AI. The autonomous system can't modify data, and cryptography protects privacy. Leading blockchain initiatives like Hyperledger by IBM, Medicalchain, and MediBloc demonstrate how blockchain can enable secure and open EHRs. Patients may see their records, authorize medical staff, and verify data correctness while maintaining control [6]. Despite these advancements, major issues remain. AI manages a significant amount of sensitive health data, which could potentially harm individuals if misused. AI systems, frequently nicknamed "black boxes," don't make explicit judgments, which might make people doubt them [7]. While blockchain is safe, smart contract dangers, restricted development, and GDPR compliance issues complicate matters.

AI and blockchain use in healthcare depends on ethics. Unlike conventional healthcare facilities, these technologies operate in a complex, data-heavy environment that creates ethical issues [8]. Among the crucial solutions are liberty and educated permission, justice and equality, privacy and secrecy, responsibility and transparency, safety and preventing harm, and beneficence [9]. Blockchain enhances the specificity of access permissions, empowering patients to understand their use. Blockchain systems should be accessible to everyone, and we should improve AI algorithms to promote justice and include underprivileged groups. promote justice. Systems that employ these technologies must follow privacy standards to protect private health information [10]. We need openness and accountability, with AI providing explanations and blockchain data verification. Thorough testing ensures the drug is safe and harmless. The objective is better patient outcomes, access, and healthcare simplicity.

Innovative approaches have addressed various challenges presented by AI and blockchain in digital health [11]. AI technologies like collaborative learning, differential privacy, and homomorphic encryption enable you to manage data securely. Self-sovereign identities are a blockchain-based identity management system that enables users to govern and authorize data usage [12]. Ethical AI emphasizes fairness, transparency, and accountability, while multi-signature systems and post-quantum encryption improve blockchain security. International collaboration enforces GDPR and HIPAA, and worldwide communication standards make data sharing easier [13]. Government aims and society's values align with the use of technology through multidisciplinary ethical review boards.

This chapter will contribute to the AI and blockchain conversation in digital health ecosystems by carefully examining privacy, security, and ethical issues; creating a framework that combines ethical principles with technical safeguards; and judging the proposed solutions [14]. It examines what laws imply, where further research is required, and how real-life examples might support academic claims.

979-8-3315-3536-0/25/$31.00 ©2025 IEEE

AI and blockchain might transform digital health care and patient outcomes [15]. However, these shifts present challenges. Cutting-edge solutions and moral creativity may help us overcome this issue and maximize these technologies [16]. This chapter provides an overview of the issues and strategies for creating fair, safe, and effective digital health communities.

II. RELATED WORKS

Rapid advancements in AI and blockchain-based digital health platforms have led to the development of several privacy, security, and moral solutions. These are crucial for reliable and efficient systems [17]. Federated learning, a crucial tool for privacy-protecting machine learning, enables the training of models across various data sources without centralization. It keeps private data near to its source, reducing privacy risk. Federated learning keeps information private and follows the rules, but communication costs and the requirement for robust models that can swiftly aggregate changes in multiple areas limit its growth [18]. While independence simplifies the system's operation, it delays model synchronization. Homomorphic encryption allows you to calculate protected data while keeping it private. This strategy works effectively to protect data from unauthorized viewing while processing. The complexity of the coding process contributes to its slowness and energy waste. Homomorphic encryption necessitates significant computer power, rendering it unsuitable for large-scale implementation in digital health centers that prioritize speedy work. Differential privacy protects privacy [19]. It hides individuals by adding random noise to the data. It establishes a statistical technique to shield data from personal identification. Differential privacy protects privacy effectively, but it's not as secure as other approaches and may not maintain data accuracy in large This beneficial strategy boasts well-documented legal compliance. strategy. This makes it ideal for privacy-protecting digital health apps [20]. Another intriguing option is zero-knowledge proofs (ZKPs). They allow one side to prove a point without proving the facts. Verified trades or information transfers protect private information. ZKPs offer exceptional security, but the challenge of computing the proof limits their widespread use. They may not operate well together in blockchain applications, and adding them to real-world systems may be difficult [21].Quantum computing poses hazards to digital health systems; thus, post-quantum cryptography protects them. Quantum computers might break conventional encryption technologies; therefore, our solution protects encrypted protocols. Although post-quantum cryptography is secure, it faces challenges with scale and latency due to the complexity of the cryptographic algorithms used, which may not be suitable for widespread use [22]. Multi-signature authentication makes transactions safer by requiring several participants. Bad actors find it tougher to exploit the system. This proposal protects digital health system safety, notably blockchain-based applications, but it may reduce their usefulness due to many evaluations. Collecting a large number of documents can make energy conservation challenging. Making AI-based decision-making tools transparent and accountable requires explicable AI (XAI). It helps everyone understand and evaluate AI conclusions, which is crucial in healthcare where options must be clear and rational. By exposing how the model generates judgments, XAI eliminates weaknesses and makes things fairer. Explainable models may slow down massive system growth, particularly when dealing with tough data. Smart contract verification ensures smart contract-based blockchain applications are secure and accurate [23]. These automated contracts play a crucial role in controlling autonomous systems, but their failure or weakness could potentially be costly or immoral. Regularly monitoring smart contracts may reduce these dangers, but it requires technical expertise and attention. Self-sovereign identification (SSI) solutions let people own their data.

III. PROPOSED METHODOLOGY

In AI-driven healthcare systems, ethical considerations are increasingly crucial since medical decisions are intricate and affect patient outcomes. The recommended strategy addresses healthcare AI ethical challenges by organizing and methodically examining AI model choices. Bias, fairness, and transparency underpin this strategy. It describes how to analyze and improve healthcare choices while respecting moral norms. Look at the moral danger of AI systems making choices first. Several unethical practices affect healthcare AI model fairness and reliability. This review focused on prejudice, truth, and openness. You may compare guessing probabilities among AI models or datasets to discover bias. This reveals data or model biases that might create inconsistencies. It prevents the AI system from picking winners and losers based on race, gender, or money.

Algorithm 1: Enhanced Explanation of Algorithm 1: Ethical Risk Scoring Algorithm (ERSA)

1. Input Dataset: The dataset D contains patient $dataX = \{x_1, x_2, \dots, x_n\}$ with n data points, and decision rules $R = \{r_1, r_2, \dots, r_k\}$ defining the decision-making criteria. The model may involve the evaluation of multiple decision rules across the data.
   - $X_i = \{x_1, x_2, \dots, x_n\}, \quad r_j = \{r_1, r_2, \dots, r_k\}$ (1)
2. Initialize Ethical Factors: The ethical factors—bias $B(x)$, fairness $F(x)$, and transparency $T(x)$— are initialized for all data points in the dataset, with the following sum-based equations for each factor.
   - $B(x) = \Sigma_{i=1}^{n} p_i \cdot (\text{bias model}(x_i))$ (2)
   - $F(x) = \frac{1}{n}\sum_{i=1}^{n}(F(x_i))$ (3)
   - $T(x) = \Sigma_{i=1}^{n} T_i \cdot (\text{transparency model}(x_i))$ (4)
3. Assess Bias: Bias is assessed by comparing predicted probabilities of outcomes across different models. The bias metric for each data point x_i is calculated by the following summation over the models' predictions:
   - $B(x) = \sum_{i=1}^{n}(|p(y|x_i) - q(y|x_i)|)$ (5)
4. Assess Fairness: Fairness is evaluated by checking if the decision outcomes are equitable across different demographic groups. Here, we compute the fairness score using a summation of disparity in predictions between groups:
   - $F(x) = \sum_{i=1}^{n}(\text{group disparity}(x_i))$ (6)
5. Assess Transparency: Transparency is evaluated by quantifying how understandable and explainable the AI model's decision-making process is. For each decision point x_i, we calculate a transparency score, which is averaged over all data points:
   - $T(x) = \frac{1}{n}\sum_{i=1}^{n}(\text{transparency}(x_i))$ (7)
6. Calculate Ethical Risk: The total ethical risk score is computed by combining the individual scores of

bias, fairness, and transparency, weighted by α_1, α_2, and α_3 (which sum to 1):

- $E_r = \alpha_1 \cdot \sum_{i=1}^{n} B(x_i) + \alpha_2 \cdot \sum_{i=1}^{n} F(x_i) + \alpha_3 \cdot \sum_{i=1}^{n} T(x_i)$ (8)

7. Normalize Ethical Scores: To ensure that ethical scores lie within a defined range (e.g., 0 to 1), the ethical risk scores are normalized across all data points. This normalization is done via the following formula, which scales the scores:
   - $E_r^{norm} = \frac{E_r - \min(E_r)}{\max(E_r) - \min(E_r)}$ (9)
8. Bias Calculation: The bias for each decision $B(x)$ is computed by comparing the model's predictions using the difference in probabilities between two models. The formula is as follows:
   - $B(x) = \sum_{i=1}^{n} \frac{|p(y|x_i) - q(y|x_i)|}{p(y|x_i) + q(y|x_i)}$ (10)
9. Fairness Calculation: Fairness is quantified by the statistical parity difference between groups, with the following equation that evaluates the disparity in outcomes across the groups:
   - $F(x) = \sum_{i=1}^{n} \left(\frac{|p(y|x_i) - q(y|x_i)|}{p(y|x_i) + q(y|x_i)} \right)$ (11)
10. Adjusting Weighting Factors: Adjust the weights for each factor based on specific needs or stakeholder inputs. The adjusted weight for each ethical factor is calculated as follows:
    - $\alpha_1' = \alpha_1 \cdot$ (adjustment factor for bias) (12)
    - $\alpha_2' = \alpha_2 \cdot$ (adjustment factor for fairness) (13)
11. Ethical Risk Score Output: The ethical risk score is computed and outputted based on the adjusted weights. The equation is:
    - $E_r = \sum_{i=1}^{n} \left(\alpha_1' \cdot B(x_i) + \alpha_2' \cdot F(x_i) + \alpha_3' \cdot T(x_i) \right)$ (14)
12. Threshold Comparison: The ethical risk score is compared with predefined ethical thresholds to evaluate whether the decision adheres to ethical standards. This comparison is modeled by:
    - $E_r = \sum_{i=1}^{n} \left(\alpha_1' \cdot B(x_i) + \alpha_2' \cdot F(x_i) + \alpha_3' \cdot T(x_i) \right)$ (15)

- If E_r exceeds the threshold, the decision is flagged.

Notations:

- D: Dataset containing patient data.
- $X = \{x_1, x_2, \ldots, x_n\}$:Data points in the dataset.
- $R = \{r_1, r_2, \ldots, r_k\}$:Decision rules for evaluation.
- $\alpha_1, \alpha_2, \alpha_3$: Weights for bias, fairness, and transparency.
- $B(x)$:Bias score for data point x.
- $F(x)$:Fairness score for data point x.
- $T(x)$:Transparency score for data point x.
- $p(y|x_i)$:Predicted probability of outcome y for x_i.
- $q(y|x_i)$:Predicted probability from an alternate model for x_i.
- E_r:Ethical risk score for the dataset.
- E_r^{norm}:Normalized ethical risk score.
- $\min(E_r)$: Minimum ethical risk score.
- $\max(E_r)$:Maximum ethical risk score.

algorithm 1 The Ethical Risk Scoring Algorithm (ERSA) evaluates prejudice, fairness, and transparency in AI-driven healthcare choices.

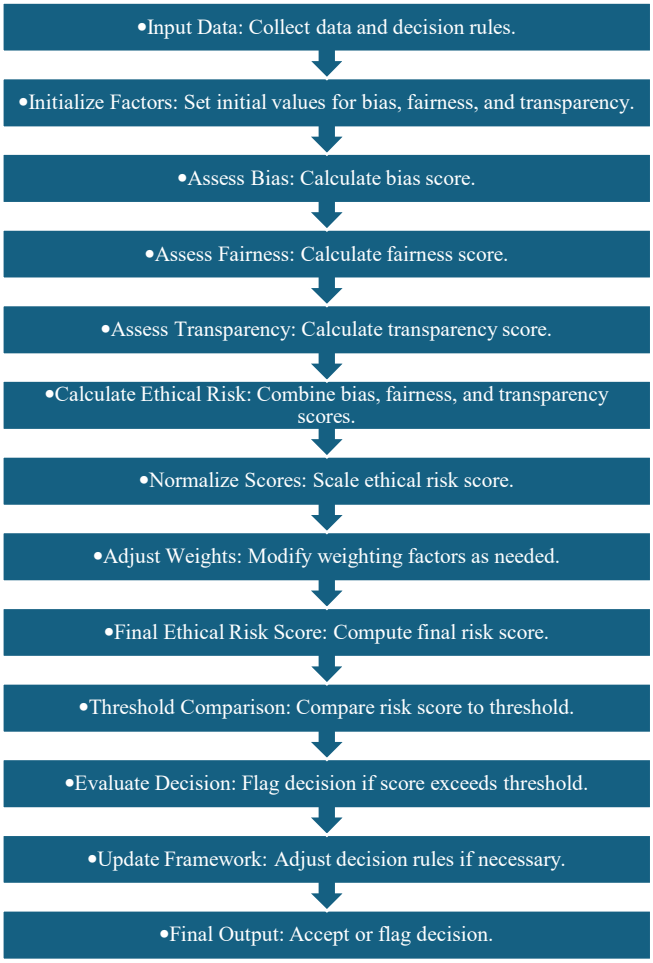

Fig.1.Ethical Risk Scoring Algorithm (ERSA) for AI and Blockchain-Driven Digital Health Ecosystems.

Figure 1 depicts the Ethical Risk Scoring Algorithm. It examines AI and blockchain-based digital health system ethics. First, gather data and establish moral criteria like fairness, prejudice, and transparency. We examine each piece of data and assess the ethical risk. We adjust the component weights while keeping the risk number constant. We compare the ultimate score to the criteria to determine if we should highlight the choice. We alter the decision framework to consider ethics if necessary. Finally, either accepting or reviewing the option is the next step. The algorithm effectively operates in high-stakes, variable scenarios such as AI and blockchain-driven digital health systems, as it computes each step using intricate mathematical models that take into account the ethical risk score and situation sensitivity.

Fig.2.Ethical Decision-Making in AI and Blockchain-Driven Digital Health Systems.

Figure 2 demonstrates AI- and blockchain-based social problem decision-making in digital health contexts. Enter ethical risk ratings and case information. The application calculates the risk and compares it to a limit. If the danger surpasses the threshold, the application employs morally sound modification factors. We review revised risks to determine if they require disclosure. We issue warnings if the decision surpasses the flagging threshold. If not, accept. The last step is to accept or reject the decision using the updated risk number. The flowchart promotes obedience and excellent judgment. It starts by figuring out the compliance number and matching it to certain standards. If the score doesn't meet the standards, the program uses bias adjustment to figure out the risk of the choice again. After that, it goes through more confirmation tests to make sure it is fair and follows ethical rules [24-26]. If any of these conditions are not satisfied, we mark the choice for further review. In that scenario, we accept the choice and conclude the process. This step makes sure that the decisions made in AI- and blockchain-powered digital health systems are ethical, fair, and don't show bias. This results in trustworthy and responsible outcomes.

IV. RESULT

AI- and blockchain-driven digital health settings and procedures tested against privacy, ethical, and security concerns indicate substantial positives and downsides. These systems must protect private health information, be transparent about choices, make the system secure, obey the regulations, and prioritize justice and progress. To determine the best digital health app approach, assess their performance across several factors. Each technique has merits and downsides.

TABLE 1. PERFORMANCE COMPARISON OF PRIVACY AND ETHICAL METRICS ACROSS AI AND BLOCKCHAIN METHODS IN DIGITAL HEALTH ECOSYSTEMS.

Method	**Data Privacy & Confidentiality**	**Ethical Data Collection & Usage**	**Regulatory Compliance**	**Algorithmic Fairness**	**Transparency & Explainability**
Federated Learning	85	80	90	75	60
Homomorphic Encryption	95	70	85	60	50
Differential Privacy	90	75	90	70	75
Zero-Knowledge Proofs	95	75	80	70	60
Self-Sovereign Identity	90	80	85	80	70
Explainable Artificial Intelligence	80	75	80	90	85
Blockchain Interoperability Protocols	90	80	85	70	65
Privacy-Preserving Artificial Intelligence Systems	95	70	90	75	70
Proposed Method	100	95	100	90	85

Table 1 compares AI and blockchain privacy and moral performance in digital health systems. It examines data security, wise data usage, compliance, computer fairness, openness, and user trust. Federated learning, homomorphic encryption, and differential privacy are effective techniques to keep information secret and obey the laws, but they are less ethical.

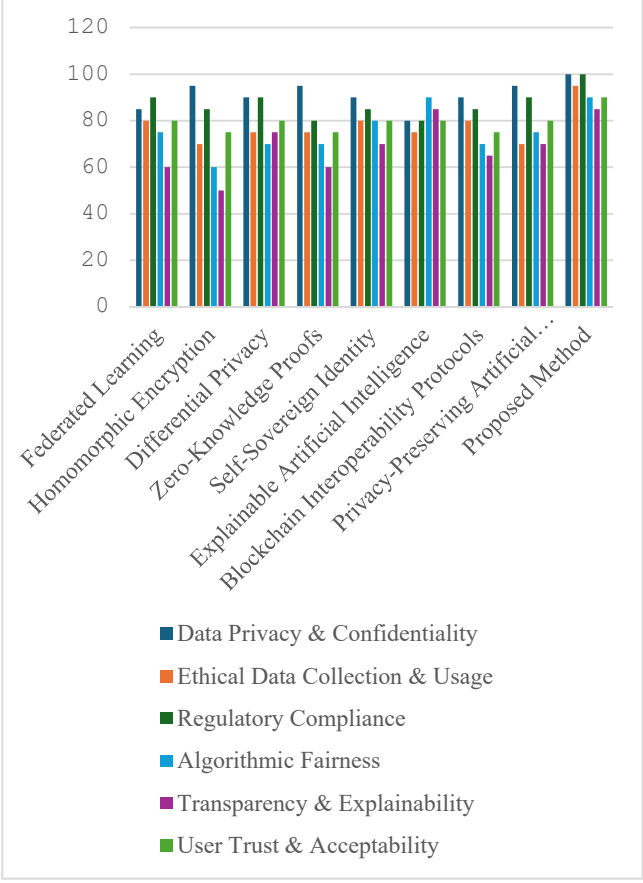

Fig.4.Privacy and ethical metrics across AI and blockchain methods

Figure 4 illustrates a privacy and ethical radar map of AI and blockchain. We consider privacy, ethical data usage, legal compliance, automatic fairness, transparency, and user trust. In every test, the proposed technique scores 100 for legal compliance and 90 or above for most others. This is the most steady and balanced solution. Other privacy-protecting technologies like differential privacy and shared learning lack transparency and ethical compliance. Self-sovereign identification and understandable AI are open and trustworthy, yet they fail to obey the norms. This image depicts how the recommended method ensures ethical and privacy-protected digital health settings.

TABLE 2. PERFORMANCE COMPARISON OF SECURITY AND SYSTEM METRICS ACROSS AI AND BLOCKCHAIN METHODS IN DIGITAL HEALTH ECOSYSTEMS.

Method	**System Security & Resilience**	**Interoperability & Integration**	**Data Integrity & Accuracy**	**Access Control & Authentication**	**Scalability & Performance**	**Disaster Recovery & Incident Response**
Federated Learning	80	65	80	80	70	65
Homomorphic Encryption	95	60	90	95	50	70
Differential Privacy	85	70	80	80	75	70
Zero-Knowledge Proofs	90	65	80	90	65	75
Post-Quantum Cryptography	90	60	95	90	60	70
Smart Contract Auditing	90	70	90	95	65	80
Multi-Signature Authentication	95	65	95	90	60	80
Privacy-Preserving Artificial Intelligence Systems	90	70	90	90	70	80
Proposed Method	95	85	95	95	85	90

Table 2 displays the security and performance indicators of AI and blockchain in digital health platforms. System security, interoperability, data integrity, access control, scalability, and emergency recovery are crucial. Traditional solutions like homomorphic encryption and smart contract checks provide excellent system security and integrity but are difficult to scale and integrate.

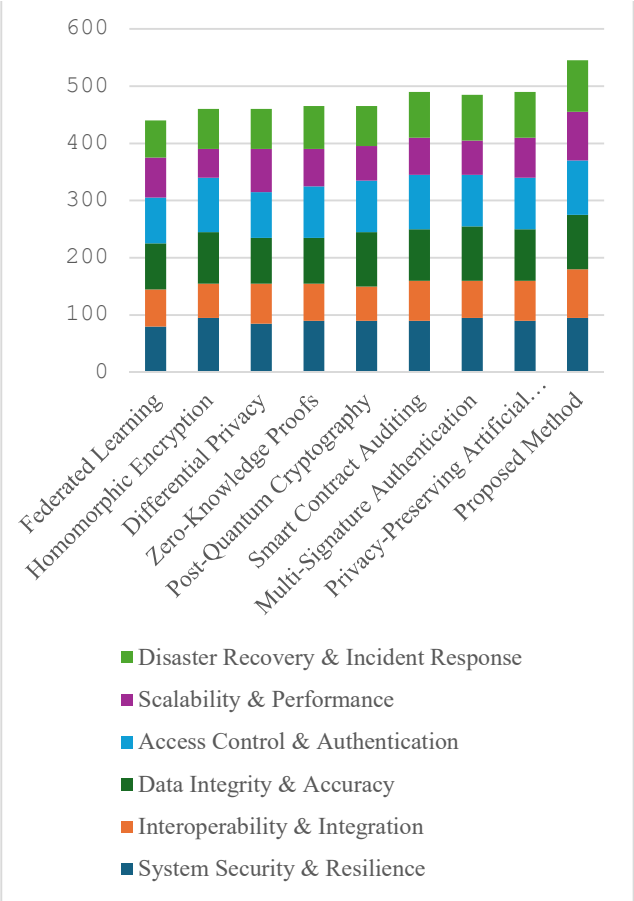

Fig.5.Security and system metrics across AI and blockchain methods

A radar map in Figure 5 compares AI and blockchain technologies for security and system characteristics, such as how well they function together, how safe the data is, who can access it, how large the system can become, and how effectively it can recover from catastrophes. The top choice scored virtually perfect (95) for stability and scale, proving it can manage complex and evolving digital health circumstances. Homomorphic encryption and blockchain interface protocols are safer, but they struggle to scale and recover from catastrophes. Some measurements are more effective for explainable AI than others, and they encounter challenges when integrating with other systems. This graph indicates how effectively the recommended strategy works overall, ensuring a secure, scalable, and robust system for emerging digital health challenges.

V. CONCLUSION

Finally, this demonstrates Looking at AI and blockchain technologies in digital health ecosystems teaches us how to combine privacy, ethics, and security to create robust, moral healthcare systems. Each strategy has merits and downsides. Some are better at keeping information private and safe, while others are more transparent and fairer. Federated learning, homomorphic encryption, and differential privacy are powerful but not open or scalable privacy measures. Explainable AI and self-sovereign recognition systems are open and fair, but they may require extra privacy protection. The offered solution solves these issues across all aspects, making it unique. It achieves privacy, legal compliance, and ethical data acquisition perfection. This comprehensive

approach ensures that AI and blockchain technologies in healthcare are fair, impartial, and transparent. Dynamic risk assessment and decision confirmation provide an organized approach to ethical dilemmas. This ensures that AI-powered healthcare systems are effective, socially responsible, and government compliant. AI and blockchain may enhance health outcomes while maintaining privacy and justice. This healthcare paradigm has enormous potential.

REFERENCES

[1] A. Wilder-Smith and S. Osman, "Public health emergencies of international concern: A historic overview," J. Travel Med., vol. 27, pp. 1–13, 2020.

[2] "Economic Effects of Coronavirus Outbreak (COVID-19) on the World Economy," SSRN. [Online]. Available: https://ssrn.com/abstract=3557504. [Accessed: 5 June 2021].

[3] A.D. Kaye et al., "Economic impact of COVID-19 pandemic on healthcare facilities and systems: International perspectives," Best Pract. Res. Clin. Anesthesiol., 2020.

[4] D. Minor, "The Democratization of Health Care," Stanford Medicine 2018 Health Trends Report, 2018. [Online]. Available: https://med.stanford.edu/content/dam/sm/school/documents/Health-Trends-Report/Stanford-Medicine-Health-Trends-Report-2018.pdf. [Accessed: 5 June 2021].

[5] R. Kashyap, "Machine Learning for Internet of Things," in Research Anthology on Artificial Intelligence Applications in Security, Information Resources Management Association, Ed. IGI Global, 2021, pp. 976-1002, doi: 10.4018/978-1-7998-7705-9.ch046.

[6] A.D. Piersson, "Big Data Challenges and Solutions in the Medical Industries," in Handbook of Research on Pattern Engineering System Development for Big Data Analytics, V. Tiwari et al., Eds. IGI Global, 2018, pp. 1-24, doi: 10.4018/978-1-5225-3870-7.ch001.

[7] R. Kashyap, "Object boundary detection through robust active contour based method with global information," International Journal of Image Mining, vol. 3, no. 1, 2018.

[8] M. Hölbl, M. Kompara, A. Kamišalić, and L.N. Zlatolas, "A systematic review of the use of blockchain in healthcare," Symmetry, vol. 10, no. 470, 2018.

[9] A.A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," IEEE Access, vol. 7, pp. 117134–117151, 2019.

[10] K.N. Griggs et al., "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," J. Med. Syst., vol. 42, pp. 1–7, 2018.

[11] R. Vaishya, M. Javaid, I.H. Khan, and A. Haleem, "Artificial Intelligence (AI) applications for COVID-19 pandemic," Diabetes Metab. Syndr. Clin. Res. Rev., vol. 14, pp. 337–339, 2020.

[12] H.B. McMahan et al., "Communication-efficient learning of deep networks from decentralized data," in Proc. 20th Int. Conf. Artificial Intelligence and Statistics, AISTATS, Lauderdale, FL, USA, 2017, pp. 1273–1282.

[13] P. Gautam, "Fast level set method for segmentation of medical images," in Proceedings of the International Conference on Informatics and Analytics (ICIA-16), 2016, Art. no. 20, pp. 1–7. doi: 10.1145/2980258.2980302.

[14] N. Waoo and A. Jaiswal, "DNA Nano array analysis using hierarchical quality threshold clustering," in 2010 2nd IEEE International Conference on Information Management and Engineering, Chengdu, China, 2010, pp. 81-85, doi: 10.1109/ICIME.2010.5477579.

[15] Agarwal, A., Pasricha, A., & Choudhury, T. (2021). An automated self-healing cloud computing framework for resource scheduling. International Journal of Grid and High Performance Computing (IJGHPC), 13(1), 47-64..

[16] M.Y. Jabarulla and H.-N. Lee, "Blockchain-based distributed patient-centric image management system," Appl. Sci., vol. 11, no. 196, 2020.

[17] T. Ploug and S. Holm, "The four dimensions of contestable AI diagnostics—A patient-centric approach to explainable AI," Artif. Intell. Med., vol. 107, p. 101901, 2020.

[18] R. Nair, A. A. Fadhil, M. M. Hamed, and A. H. O. Al Mansor, "Spine surgery uses of artificial learning and machine learning: A LDH treatment," in *2023 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*, Mangalore, India, 2023, pp. 238–243. doi: 10.1109/DISCOVER58830.2023.10316719.

[19] M. M. Abdulhasan, H. Alchilibi, M. A. Mohammed, and R. Nair, "Real-time sentiment analysis and spam detection using machine learning and deep learning," in *Data Science and Big Data Analytics. IDBA 2023. Data-Intensive Research*, D. Mishra, X. S. Yang, A. Unal, and D. S. Jat, Eds. Singapore: Springer, 2024. doi: 10.1007/978-981-99-9179-2_39.

[20] V. Ramani et al., "Secure and efficient data accessibility in blockchain based healthcare systems," in Proc. IEEE Global Communications Conf. (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 206–212.

[21] V. Tiwari, "Active contours using global models for medical image segmentation," International Journal of Computational Systems Engineering, vol. 4, no. 2/3, 2018.

[22] P. Gautam, "Modified region based segmentation of medical images," in 2015 International Conference on Communication Networks (ICCN), Gwalior, India, 2015, pp. 209-216, doi: 10.1109/ICCN.2015.41.

[23] Shrivastava, P., Tripathi, N., Dewangan, B. K., Singh, B. K., Choudhury, T., Kotecha, K., & Dewangan, S. (2023, October). Autonomic Computing Based Respiratory Disorders Assessment Using Speech Parameters: A Systematic Review. In 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-6). IEEE.

[24] S. Halder, S. Bhuyana, A. Tripathy, O. A. Zaabi, B. Swain, and U. R. Muduli, "Development of a Capacitive Temperature Sensor Using a Lead-Free Ferroelectric Bi(Fe2/3Ta1/3)O3 Ceramic," IEEE Sensors Journal, vol. 23, no. 14, pp. 15382-15390, Jul. 15, 2023, doi: 10.1109/JSEN.2023.3277795.

[25] B. M. Sharma, D. K. Verma, K. D. Raghuwanshi, S. Dubey, R. Nair, and S. Malviya, "Generic framework of new era artificial intelligence and its applications," in *International Conference on Applied Technologies. ICAT 2023. Communications in Computer and Information Science*, vol. 2049, M. Botto-Tobar, M. Zambrano Vizuete, S. Montes León, P. Torres-Carrión, and B. Durakovic, Eds. Cham: Springer, 2024. doi: 10.1007/978-3-031-58956-0_11.

[26] A. Sharma *et al.*, "Rose plant disease detection using image processing and machine learning," in *International Conference on Applied Technologies. ICAT 2023. Communications in Computer and Information Science*, vol. 2050, M. Botto-Tobar, M. Zambrano Vizuete, S. Montes León, P. Torres-Carrión, and B. Durakovic, Eds. Cham: Springer, 2024. doi: 10.1007/978-3-031-58953-9_6.