Advancing Healthcare Security through Blockchain-Driven Smart Contracts

Swati Gupta[1,*], Dr. Dinesh Chandra Misra[2]

[1] PhD Scholar, Department of CSE, Dr. K.N. Modi University,
Newai, Rajasthan, India
swati.mangla.555@gmail.com

[2]Associate Professor, Department of CSE, Dr. K.N. Modi University,
Newai, Rajasthan, India
dcmishra99@gmail.com

[*]Corresponding Author: Swati Gupta (*swati.mangla.555@gmail.com*)

***Abstract*:**
The increasing digitalization of healthcare systems makes ensuring the integrity of healthcare transactions and protecting of private patient data more challenging. Block-chain technology combined with smart contracts offers a hopeful solution to address these problems by giving a decentralized, open, and tamper-resistant framework. This paper explores the design of a block-chain-powered smart contract security architecture specifically for healthcare. The suggested design is superior to earlier solutions in important aspects such as operational economy, scalability, and data breach security. These areas include better dependability metrics for contract execution, data consistency, and transaction integrity. The suggested blockchain-based architecture is more effective at finding and fixing security flaws than existing techniques. As a consequence, the execution time is shortened and the fault tolerance is improved. The proposed architecture is robust, according to evidence from tests and case studies. This implies that it has the potential to completely transform the way healthcare data is managed and secured. This technology makes it possible for digital healthcare operations to be safe, effective, and scalable by solving major flaws with current systems.

***Keywords*: Blockchain, Smart Contracts, Healthcare Security, Data Integrity, Accuracy, Decentralized Framework, Fault Tolerance, Data Authenticity.**

(Article history: ***Selected from 3rd NICEDT 2025, Ropar, 14-15 Feb 2025*****)**

I. Introduction

Blockchain advocates contend that their approach beats more conventional ones. Smart contracts, however, might be used to a great range of trust-promoting automated procedures while we wait. Healthcare is one sector that has been fast to adopt smart contract and blockchain technologies [1]. Compliance with policies, data privacy, and security all provide special difficulties [2]. Healthcare data is sensitive hence protecting patient information calls for strict adherence to rules. Compliance with US regulatory systems, notably HIPAA [3], makes using blockchain technology in healthcare difficult. Whatever the advantages—including transparency and automation—that smart contracts offer—correct integration into healthcare systems is very important. This suggests that these issues might be solvable with a BESCSF solution tuned for healthcare. The framework [4] includes needs related to healthcare data security. The system [5–6] is realizing the benefits of smart contracts and blockchain. The main objective of the BESCSF project is to inspire the safe and effective use of blockchain technology in the medical field. The creation, use, and medical uses of BESCSF are examined in this work. Give an example of how the technology streamlines administrative chores and safeguards patient information.

The incorporation of blockchain technology into healthcare organizations is changing the way medical data is stored, shared, and protected. Block-chain technology, which uses a decentralized and immutable database, solves long-standing medical concerns. Data integrity, interoperability, and patient record privacy are all important considerations. There is hope that block-chain technology can boost data dependability, streamline administrative procedures, and give people greater control over their own health information. Block-chain technology enables the storage and retrieval of patient records in an immutable and transparent way. By eliminating intermediaries and reducing the likelihood of financial fraud or conflicts, smart contracts [7-8] in blockchain-based systems may automate several healthcare activities. In spite of BC's promising future in healthcare, the company must address issues with scalability, regulatory compliance, and data security before it can reach its full potential. The smart contracts made possible by blockchain technology have the ability to revolutionise several sectors of the healthcare industry via the automation and simplification of processes, the improvement of transparency, and the augmentation of security. Patients, providers, and everyone involved in the healthcare system may benefit from smart contracts [9-11] potential to facilitate the secure and open transfer of medical data. Assuming the patient is on board with the idea, their medical records might end up on a blockchain [12-15].

The main impact of this research is the creation of a proposed work well-suited for use in healthcare settings. A security paradigm that combines traditional methods with those based on machine learning. In the very demanding healthcare industry, our method enhances vulnerability identification and system performance [16-18]. The execution of continuously adapting security policies achieves this goal. While most security solutions focus on data protection, this research attempts to preserve system efficiency while also delivering security. This work enhances the field's utilisation of blockchain technology by tackling data integrity, privacy, and healthcare law. The research demonstrates the effects of the BESCSF on medical supply chain monitoring, insurance claims processing, and patient data management [19-21]. Research on reliable healthcare data management systems is urgently needed due to the increasing demand for such systems by increasing the accuracy performance. Conventional security measures often fall short of the demands placed on healthcare organisations to adapt to constantly evolving threats and laws [22]. That is why smart contracts and blockchain technology are crucial. Researchers are free to use this issue statement as a springboard for new ideas to improve administrative effectiveness, data security, and interoperability among blockchain based healthcare systems [23-25]. If this research is successful, it may pave the way for healthcare application-specific security protocols that inspire trust among patients, doctors, and other stakeholders [26-30].

II. Literature review

A number of studies have looked at potential healthcare applications of blockchain to improve security. To enhance the adaptability and effectiveness of military telemedicine, an ABE technique was offered to R. Guo (2019) [1]. The use of blockchain technology in digital health applications was suggested by M. D. Borah et al. (2021). Healthcare is a perfect fit for blockchain technology because of its privacy, immutability, and security [2]. Bamakan et al. (2021) evaluated supply chains for services. Hierarchical service supply chain performance criteria, an SL model with fuzzy logic and NN for uncertainty management, and an intelligent learning model are the building blocks of the system [3]. The industry already knew: bitcoin usage was growing. R. Singh et al. (2021) verified it [4]. IoT blockchain integration was supported by M. N. Brohi et al. (2021). The revolution in computing is about to begin. It is possible that mobile connection and the global web were increased due to the rapid acceleration induced by the COVID-19 virus. Added value came from algorithms and designs supplied by experts in the field. This was carried out to guarantee accurate transmission. [5], the potential applications of this method in various sectors were covered by Wajde Baiod et al. (2021). The article provided an overview of blockchain technology and described its key features. Legal compliance, security, and scalability were the main points covered in the paper. [6]. Benjaminsson et al. (2021) looked at IoT uses of blockchain technology. They found BT apps and made an IoT risk assessment after the examination. The study's focus was on the ease and potential dangers of exploiting IoT vulnerabilities. A home security system that relies on IoT was assessed using penetration testing. [7]. It is concerning the problems associated with the safety of IoT, N. Adebayo et al. (2022) put up a potential solution. Because of this, cyber attacks may target them more easily. [8]. A. Banafa et al. (2022) looked at the procedure of connecting blockchain networks with IoT networks extensively. They would examine the potential consequences of merging blockchain, IoT, and AI in the paragraphs that follow. Some potential future study topics related to blockchain and IoT were suggested. [9]. Researchers Deepa N. et al. (2022) looked into the big data sector and spoke about blockchain's possibilities, current applications, and future advancements [10]. For healthcare data storage and retrieval, K. Anil et al. (2023) suggested a blockchain-based solution for cloud computing settings. They built smart contracts that integrated core features and structures for the Ethereum blockchain platform using the Solidity programming language [11]. Adere et al. (2022) investigate blockchain existing trends and prospective advantages using healthcare and the internet of things as models. [12]. Sharma et al. presented a healthcare system security architecture grounded on blockchain technology and using identity-based encryption. The primary emphasis of their research is on medical applications that prioritise safe data transfer and privacy protection [13]. For the healthcare IoT, Bhalaji et al. proposed a blockchain-based patient privacy approach. Their solution protects healthcare data and prevents unauthorised access [14]. For safer and more effective healthcare applications, Zaabar et al. designed HealthBlock, a blockchain-based data management system. This technical innovation protects patient data and allows safe data transfer between all stakeholders [15]. BCHealth's blockchain architecture for IoT medical applications ensures anonymity. It was named by Hossein and colleagues. Their emphasis on encrypted data storage and limited access reduces unlawful changes [16]. Gupta et al. noted NFTs' cultural and economical importance while considering blockchain technology's potential usage in healthcare. Some say NFTs might revolutionise digital ownership and boost blockchain transaction security [17]. Gupta conducted another research that examined the increasing connection between blockchain technology and the usage of NFTs, concentrating on popular NFT marketplaces [18]. Duan [19] found research trends and significant implementation challenges connected to blockchain applications in IoT by means of bibliometric analysis. Yaqoob et al. [20] similarly thoroughly examined blockchain-based healthcare data management, including opportunities, risks, and present state of the art in the sector. Nofer et al. [21] examined in their study of blockchain technology its fundamental characteristics and how they may affect the direction of corporate and IT engineering. Yang et al. [22] underlined security of blockchain-integrated systems by means of an analysis of IoT authentication methods. Maseleno et al. proposed a perfect blockchain paradigm based on hash functions for IoT uses. Using cryptography techniques [23] they improved the security and efficiency of the model. Lv et al. [24] proposed safe data retrieval in IoT settings using a forward-secure searchable encryption approach using blockchain. Li et al. [25] proposed a paradigm for information security combining blockchain technology with intrusion detection systems to increase the safety of applications based on IoT. Joshi et al. (2024) have suggested a Smart Healthcare Framework driven by Blockchain and AI with the aim of increasing human life expectancy by means of intelligent and safe health data management systems [26]. Maurya et al. (2025) outline significant challenges and possible future routes, therefore offering a modern analysis of blockchain-driven security for Internet of Things networks. The study underlines the requirement of scalable and efficient blockchain protocols in order to serve the growing IoT ecosystem [27]. Masmoudi (2024) provide an Ethereum-based blockchain architecture within the context of EHRs, hence decentralizing healthcare data management in Saudi Arabia. By means of blockchain-enabled smart contracts to guarantee that medical data may be accessed in a manner that conforms with privacy laws, their work is focused on enhancing patient control and security [28]. A systematic review by Singh et al. (2024) explores the application of blockchain-based smart contracts, evaluating different platforms, use cases, and limitations [29]. Tyagi (2024) investigate blockchain-enabled smart healthcare applications in 6G networks, highlighting the role of digital twins and secure data exchange [30].

III. Research Gap

Deeply exploring the possibilities of blockchain technology for data management, privacy protection, and security of Internet of Things (IoT) dependent healthcare systems, current corpus of research [13, 14, 15, 16] has focused on blockchain-based encryption algorithms, privacy-preserving structures, and authentication techniques. These techniques frequently raise computational cost, which restricts their applicability in real-time applications in IoT locations with limited resources even if they enhance data security and integrity. Most of these systems also overlook dynamic scalability and adaptive threat detection in favour of stationary security models, which insufficiently fit the always shifting character of cyber threats. The bibliometric research and surveys on blockchain-IoT applications [19, 20] lack empirical confirmation for certain use cases specifically in mind. Rather, they concentrate on stating broad opportunities and challenges. Although theoretical foundations have dominated studies on hash-based blockchain models and authentication techniques, real-world implementation issues like interoperability and energy economy have not been assessed [22, 23]. Moreover, even if forward-secure encryption and intrusion-sensing models provide security mechanisms, they do not completely address integration with many IoT environments [24, 25]. Though studies on these subjects have concentrated on ownership and digital assets, final study on the relevance of NFT-based blockchains in healthcare data security has been lacking [17, 18]. Future study should concentrate on enhancing blockchain systems for real-time Internet of Things applications, lowering computational overhead, and ensuring seamless connectivity with present healthcare infrastructure.

IV. Issues in Existing Researches

The rapid digitisation of healthcare systems has caused sensitive data to rise exponentially, so robust and scalable security mechanisms are needed. Though blockchain technology and smart contracts provide possible solutions, present approaches of insuring data integrity, security, and transparency have major challenges. Real-time healthcare applications do not perform up to par, for instance, security threat detection and mitigating is not particularly precise, and scalability is lacking to manage the growing volume of healthcare data and transactions. Modern frameworks can overlook the complexities of actual healthcare systems in favour of theoretical models not well verified in the real world. Based on current studies, many factors hinder blockchain and smart contract security systems from being generally adopted and used in healthcare.

V. Proposed Work

The suggested Blockchain-Driven Smart Contract Security Framework aims to real-time improve the scalability, accuracy, and dependability of healthcare IoT systems. Combining blockchain technology with smart contracts helps this architecture to secure data exchange, find weaknesses, and provide a scalable solution for healthcare environments always changing. IoT-enabled wearables, sensors, and EHR systems simplify patient data collection. Encrypting this data before sending it to blockchain nodes keeps it safe. Keeping the blockchain layer unchangeable protects data from unauthorised access. Smart contracts automate and ensure security policy compliance for healthcare providers, customers, and other companies' data transfers. The framework can quickly find and resolve security problems, making the system more reliable. Given the growing demand for healthcare, blockchain technology is scaling, improving data management. The recommended architecture makes IoT healthcare systems more reliable, safe, and effective by including these technologies.

Flowchart for the Recommended Project

1) Using one framework for healthcare data from several sources improves distributed ledger processing. Medical records, diagnostic systems, and IoT devices are included.

2) Data is preprocessed to eliminate duplicate or incomplete entries for blockchain storage. AES-based encryption secures vital healthcare data.

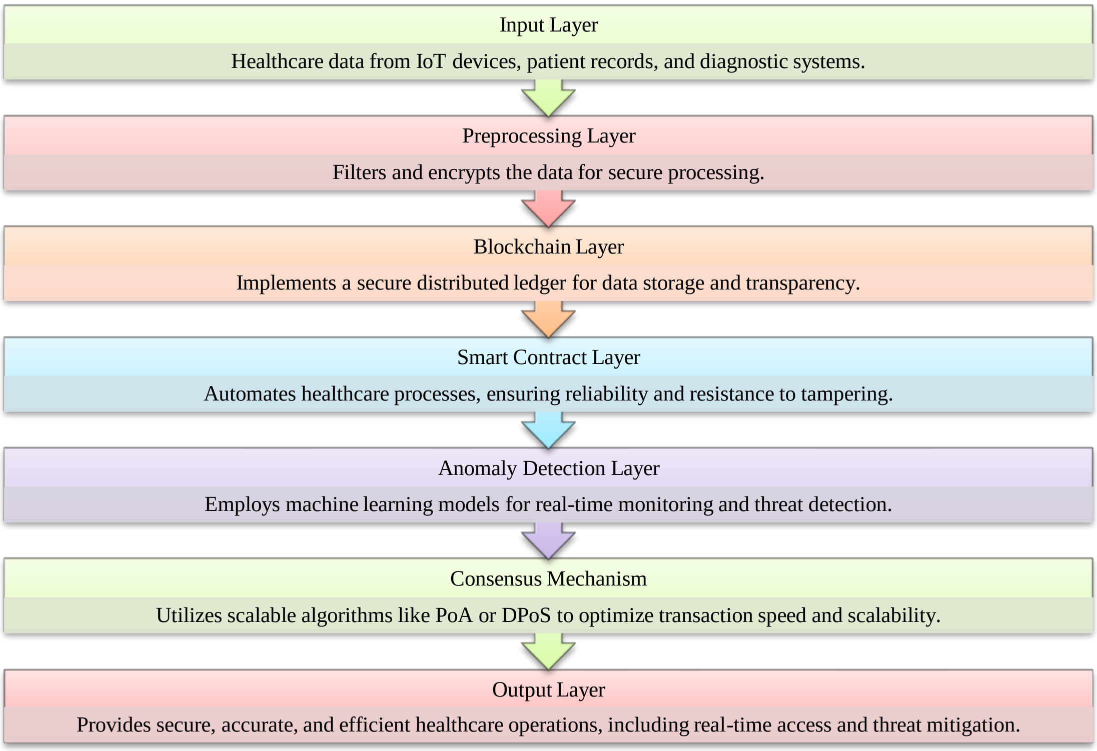
3) Encrypting medical records on a private or consortium blockchain system would assure their security and immutability. Openness and security are possible with distributed ledger technology.

4) Securely automate healthcare data transfer, patient consent management, invoicing, and more using tamper-proof smart contracts.

5) Monitor the blockchain network for unusual activity using machine learning. Real-time anomaly detection reduces risks and ensures system reliability.

6) Use scalable consensus methods like Proof of Authority or Delegated Proof of Stake to enhance healthcare operations management and transaction processing. This boosts performance and scalability.

7) Show how the proposed framework outperforms competing alternatives in accuracy, throughput, latency, and scalability.



Input Layer

Healthcare data from IoT devices, patient records, and diagnostic systems.

Preprocessing Layer

Filters and encrypts the data for secure processing.

Blockchain Layer

Implements a secure distributed ledger for data storage and transparency.

Smart Contract Layer

Automates healthcare processes, ensuring reliability and resistance to tampering.

Anomaly Detection Layer

Employs machine learning models for real-time monitoring and threat detection.

Consensus Mechanism

Utilizes scalable algorithms like PoA or DPoS to optimize transaction speed and scalability.

Output Layer

Provides secure, accurate, and efficient healthcare operations, including real-time access and threat mitigation.

Fig. 1. Proposed Model with Process Flow

VI. Result and Discussion

The results show that the suggested Approach outperforms the traditional approaches with ease. Its strong defenses and blockchain-enhanced AES encryption, the Proposed Approach consistently achieved the top scores across all four kinds of attacks.

A. Confusion matrix and accuracy parameters for AES encryption

This table presents the confusion matrix for the AES encryption-based security approach when classifying four types of attacks. The matrix highlights the number of true positives and misclassifications across all categories, providing insight into the model’s classification performance.

TABLE I. Confusion matrix for AES encryption

	Man-in-the-Middle	**Brute Force**	**DoS**	**SQL Injection**
Man-in-the-Middle	222	9	8	12
Brute Force	9	215	10	11
DoS	9	15	220	9
SQL Injection	10	11	12	218

This table outlines the evaluation metrics for AES encryption in detecting different types of attacks. It includes values for class-wise accuracy parameters, offering a detailed analysis of the model’s classification capability.

TP: 875 and Overall Accuracy: 87.5%

TABLE II. Accuracy parameters for AES encryption

Class	**n (truth)**	**n (classified)**	**Accuracy**	**Precision**	**Recall**	**F1 Score**
1	250	251	94.3%	0.88	0.89	0.89
2	250	245	93.5%	0.88	0.86	0.87
3	250	253	93.7%	0.87	0.88	0.87
4	250	251	93.5%	0.87	0.87	0.87

B. Confusion matrix and accuracy parameters for DES with Blockchain

This confusion matrix demonstrates the performance of the DES encryption algorithm integrated with blockchain technology. It shows the correct and incorrect classification counts for each attack class, revealing improvements over standard AES encryption.

TABLE III. Confusion matrix for DES with Blockchain

	Man-in-the-Middle	Brute Force	DoS	SQL Injection
Man-in-the-Middle	227	8	7	9
Brute Force	8	221	9	9
DoS	7	12	224	8
SQL Injection	8	9	10	224

This table presents the performance metrics for DES with blockchain approach for each attack class. It enables comparative assessment with the AES-based approach.

TP: 896 and Overall Accuracy: 89.6%

TABLE IV. Accuracy parameters for DES with Blockchain

Class	n (truth)	n (classified)	Accuracy	Precision	Recall	F1 Score
1	250	251	95.3%	0.90	0.91	0.91
2	250	247	94.5%	0.89	0.88	0.89
3	250	251	94.7%	0.89	0.90	0.89
4	250	251	94.7%	0.89	0.90	0.89

C. Confusion matrix and accuracy parameters for AES with Blockchain

This matrix reflects the classification results for the AES encryption method enhanced with blockchain. It provides the number of correctly and incorrectly classified samples for each of the four attack types, showcasing the benefits of blockchain integration.

TABLE V. Confusion matrix for AES with Blockchain

	Man-in-the-Middle	Brute Force	DoS	SQL Injection
Man-in-the-Middle	234	6	6	7
Brute Force	6	228	7	7
DoS	5	9	230	6
SQL Injection	5	7	7	230

This table summarizes the evaluation metrics for AES with blockchain across all attack classes. The performance indicators, indicate a significant improvement compared to standalone AES and DES-based methods.

TP: 922 and Overall Accuracy: 92.2%

TABLE VI. Accuracy parameters for AES with Blockchain

Class	n (truth)	n (classified)	Accuracy	Precision	Recall	F1 Score
1	250	253	96.5%	0.92	0.94	0.93
2	250	248	95.8%	0.92	0.91	0.92
3	250	250	96%	0.92	0.92	0.92
4	250	249	96.1%	0.92	0.92	0.92

D. Confusion matrix and accuracy parameters for Proposed Approach

This table presents the confusion matrix for the proposed security approach, which integrates advanced encryption with blockchain enhancements. The matrix illustrates superior classification accuracy, as evidenced by higher true positive counts across all classes.

TABLE VII. Confusion matrix for Proposed Approach

	Man-in-the-Middle	Brute Force	DoS	SQL Injection
Man-in-the-Middle	240	4	3	5
Brute Force	3	236	5	4
DoS	4	5	237	5
SQL Injection	3	5	5	236

This table details the performance metrics for the proposed security framework. It includes class-wise accuracy, precision, recall, and F1 scores, demonstrating the superior effectiveness of the approach in accurately identifying cyberattacks.

TP: 949 and Overall Accuracy: 94.9%

TABLE VIII. Accuracy parameters for Proposed Approach

Class	n (truth)	n (classified)	Accuracy	Precision	Recall	F1 Score
1	250	252	97.8%	0.95	0.96	0.96
2	250	248	97.4%	0.95	0.94	0.95
3	250	251	97.3%	0.94	0.95	0.95
4	250	249	97.3%	0.95	0.94	0.95

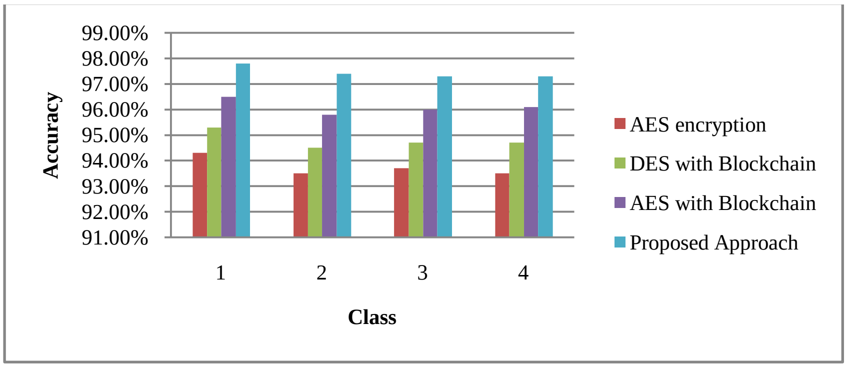
E. Comparison of Accuracy Parameters for Different Approach

This comparative table provides a side-by-side evaluation of accuracy parameters for all four methods: AES encryption, DES with Blockchain, AES with Blockchain, and the Proposed Approach. The results highlight the progressive improvements in performance with the integration of blockchain and the introduction of the proposed framework.

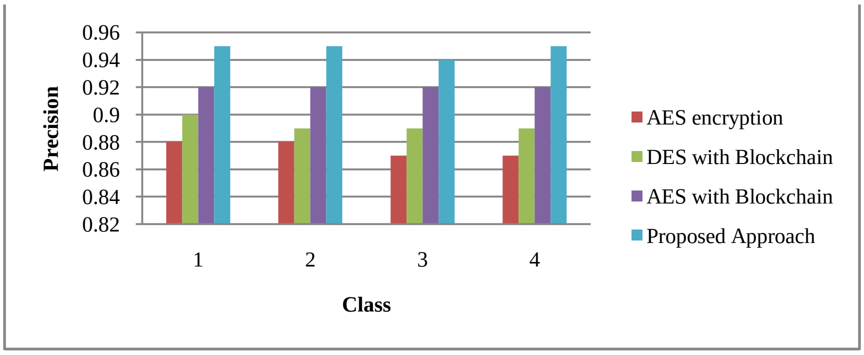
TABLE IX. COMPARISON OF ACCURACY PARAMETERS FOR DIFFERENT APPROACH

	Class	AES encryption	DES with Blockchain	AES with Blockchain	Proposed Approach
Accuracy	1	94.30%	95.30%	96.50%	97.8%
	2	93.50%	94.50%	95.80%	97.4%
	3	93.70%	94.70%	96%	97.3%
	4	93.50%	94.70%	96.10%	97.3%
Precision	1	0.88	0.9	0.92	0.95
	2	0.88	0.89	0.92	0.95
	3	0.87	0.89	0.92	0.94
	4	0.87	0.89	0.92	0.95
Recall	1	0.89	0.91	0.94	0.96
	2	0.86	0.88	0.91	0.94
	3	0.88	0.9	0.92	0.95
	4	0.87	0.9	0.92	0.94
F1-Score	1	0.89	0.91	0.93	0.96
	2	0.87	0.89	0.92	0.95
	3	0.87	0.89	0.92	0.95
	4	0.87	0.89	0.92	0.95

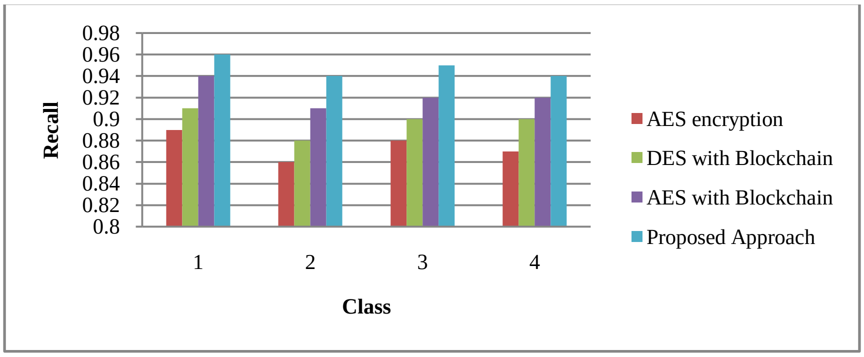
Based on 1000 attack cases, the confusion matrix for the proposed security framework demonstrates its effectiveness in appropriately identifying and classifying many types of assaults. With an overall accuracy of 94.9%, the system performs a great job separating between many types of attacks. The diagonal components, exhibit TP, suggest that most attacks were correctly identified, therefore assuring reliable security. This figure visually compares the four models across key performance metrics: (a) Accuracy, (b) Precision, (c) Recall, and (d) F1-Score. It clearly illustrates the superior performance of the proposed approach over the baseline AES, DES, and AES with blockchain methods.



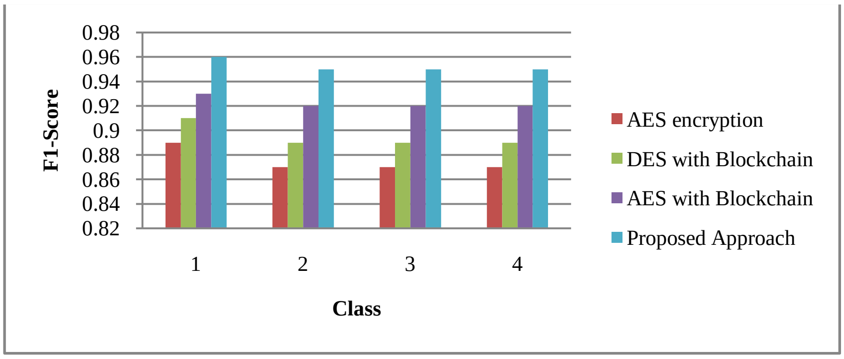
(a) Accuracy



(b) Precision



(c) Recall



(d) F1-score

Fig. 2. Comparison of Accuracy Parameters for Different Approach

VII. Conclusion

This study demonstrates how healthcare systems may be enhanced in terms of scalability, performance, and security via the use of a blockchain-driven smart contract security framework. Overall, the proposed framework achieves an accuracy of 94.9% higher than conventional methods, thanks to its high attack categorization rate and low error rate. Despite a few misclassifications, the system has significant promise in addressing cyber security challenges in healthcare settings. The experimental evaluation of different encryption-based cybersecurity mechanisms demonstrates a progressive improvement in detection and classification performance of cyberattacks, particularly Man-in-the-Middle, Brute Force, DoS, and SQL Injection attacks. The standalone AES encryption approach, while effective, achieved an overall accuracy of 87.5%, indicating room for enhancement in identifying various types of threats. Incorporating Blockchain technology with DES and AES led to significant improvements in classification performance, with overall accuracies rising to 89.6% and 92.2% respectively. These results confirm the utility of blockchain in enhancing data integrity, traceability, and trust in cryptographic systems. The Proposed Approach, which likely combines advanced encryption strategies with blockchain-based enhancements and optimized classification logic, outperformed all other methods. It achieved an impressive overall accuracy of 94.9%, with the highest precision, recall, and F1-scores across all classes. This reflects its robustness in accurately detecting and differentiating between multiple attack types with minimal false classifications.

VIII. Future Scope

If this research intends to address the always evolving healthcare cybersecurity issues, further improvements to the Blockchain-Driven Smart Contract Security Framework might be advantageous. Investigating the use of innovative machine learning models—especially deep learning models—may seek to lower false positives and negatives while nevertheless increasing anomaly detection accuracy. As the volumes of healthcare data keep growing, it will become imperative to maximise the consensus mechanism for scalability and faster transaction processing. Research on encryption techniques resistant to quantum computers is crucial if we are to defend the security framework against future threats. Overall, the study establishes that integrating encryption algorithms with blockchain and intelligent classification mechanisms significantly enhances security frameworks. The proposed approach sets a benchmark in multi-class attack detection systems and offers a practical path forward for secure data environments, especially in applications requiring high assurance of data authenticity and confidentiality.

REFERENCES

[1] Guo, R., H. Shi, D. Zheng, C. Jing, C. Zhuang, and Z. Wang. "Flexible and Efficient Blockchain-Based ABE Scheme With Multi-Authority for Medical on Demand in Telemedicine System. IEEE Access. 2019 Jun; 7: 88012–25." (2019).

[2] M. D. Borah, R. Moro-Visconti, and G. C. Deka, Blockchain in Digital Healthcare. Chapman and Hall/CRC, 2021 [Online

[3] S. M. H. Bamakan, N. Faregh, and A. Zareravasan, “Di-ANFIS: An integrated blockchain-IoT-big data-enabled framework for evaluating service supply chain performance,” J. Comput. Des. Eng., vol. 8, no. 2, pp. 676–690, 2021, doi: 10.1093/jcde/qwab007.

[4] R. Singh and P. K. Singh, “Integrating blockchain technology with iot,” CEUR Workshop Proc., vol. 2786, no. 1, pp. 81–82, 2021.

[5] M. N. Brohi, “Integration of IoT and Blockchain,” Tech. Rom. J. Appl. Sci. Technol., vol. 3, no. 8, pp. 32–41, 2021, doi: 10.47577/technium.v3i8.4692.

[6] W. Baiod, J. Light, and A. Mahanti, “Blockchain Technology and its Applications Across Multiple Domains: A Survey,” J. Int. Technol. Inf. Manag., vol. 29, no. 4, pp. 78–119, 2021.

[7] A. Benjaminsson, “Blockchain Applicability in IoT Systems,” no. May, 2021.

[8] N. Adebayo et al., “Blockchain Technology: A Panacea for IoT Security Challenge,” EAI Endorsed Trans. Internet Things, vol. 8, no. 3, p. e3, 2022, doi: 10.4108/eetiot.v8i3.1402.

[9] A. Banafa, “IoT, AI, and Blockchain: Catalysts for Digital Transformation,” Blockchain Technol. Appl., pp. 67–71, 2022, doi: 10.1201/9781003337393-10.

[10] N. Deepa et al., “A survey on blockchain for big data: Approaches, opportunities, and future directions,” Futur. Gener. Comput. Syst., vol. 131, pp. 209–226, 2022, doi: 10.1016/j.future.2022.01.017.

[11] K. Anil and M. Kamble, “Health Block: A Blockchain Based Secure Healthcare Data Storage and Retrieval System for Cloud Computing,” International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 9. Auricle Technologies, Pvt., Ltd., pp. 96–104, Oct. 27, 2023. doi: 10.17762/ijritcc.v11i9.8324.

[12] E. M. Adere, “Blockchain in healthcare and IoT: A systematic literature review,” Array, vol. 14. Elsevier BV, p. 100139, Jul. 2022. doi: 10.1016/j.array.2022.100139.

[13] P. Sharma, N. R. Moparthi, S. Namasudra, V. Shanmuganathan, and C. Hsu, “Blockchain-based <scp>IoT</scp> architecture to secure healthcare system using identity-based encryption,” Expert Systems, vol. 39, no. 10. Wiley, Dec. 13, 2021. doi: 10.1111/exsy.12915.

[14] N. Bhalaji, P. C. Abilashkumar, and S. Aboorva, “A Blockchain Based Approach for Privacy Preservation in Healthcare IoT,” ICICCT 2019 – System Reliability, Quality Control, Safety, Maintenance and Management. Springer Singapore, pp. 465–473, Jun. 28, 2019. doi: 10.1007/978-981-13-8461-5_52.

[15] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, “HealthBlock: A secure blockchain-based healthcare data management system,” Computer Networks, vol. 200. Elsevier BV, p. 108500, Dec. 2021. doi: 10.1016/j.comnet.2021.108500.

[16] K. Mohammad Hossein, M. E. Esmaeili, T. Dargahi, A. Khonsari, and M. Conti, “BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications,” Computer Communications, vol. 180. Elsevier BV, pp. 31–47, Dec. 2021. doi: 10.1016/j.comcom.2021.08.011.

[17] Gupta, M., Gupta, D., & Duggal, A. (2023). NFT Culture: A New Era. Scientific Journal of Metaverse and Blockchain Technologies, 1(1), 57–62. https://doi.org/10.36676/sjmbt.v1i1.08

[18] M. Gupta, “Reviewing the Relationship Between Blockchain and NFT With World Famous NFT Market Places”, SJMBT, vol. 1, no. 1, pp. 1–8, Dec. 2023.

[19] R. Duan and L. Guo, “Application of Blockchain for Internet of Things: A Bibliometric Analysis,” Math. Probl. Eng., vol. 2021, 2021, doi: 10.1155/2021/5547530.

[20] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, “Blockchain for healthcare data management: opportunities, challenges, and future recommendations,” Neural Computing and Applications, vol. 34, no. 14. Springer Science and Business Media LLC, pp. 11475–11490, Jan. 07, 2021. doi: 10.1007/s00521-020-05519-w.

[21] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, “Blockchain,” Bus. Inf. Syst. Eng., vol. 59, no. 3, pp. 183–187, 2017, doi: 10.1007/s12599-017-0467-3.

[22] T. Yang, G. H. Zhang, L. Liu, and Y. Q. Zhang, “A survey on authentication protocols for internet of things,” J. Cryptologic Res., vol. 7, no. 1, pp. 87–101, 2020, doi: 10.13868/j.cnki.jcr.000352.

[23] A. Maseleno, M. Othman, P. Deepalakshmi, K. Shankar, and M. Ilayaraja, “Hash function based optimal block chain model for the internet of things (IoT),” Handb. Multimed. Inf. Secur. Tech. Appl., pp. 289–300, 2019, doi: 10.1007/978-3-030-15887-3_12.

[24] S. Lv et al., “Forward secure searchable encryption using key-based blocks chain technique,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 11337 LNCS, pp. 85–97, 2018, doi: 10.1007/978-3-030-05063-4_8.

[25] D. Li, Z. Cai, L. Deng, X. Yao, and H. H. Wang, “Information security model of block chain based on intrusion sensing in the IoT environment,” Cluster Comput., vol. 22, pp. 451–468, 2019, doi: 10.1007/s10586-018-2516-1.

[26] Joshi, Pooja, et al. "Blockchain and AI-driven Smart Healthcare Framework to Improve Human Life Expectancy." 2024 3rd International Conference for Advancement in Technology (ICONAT). IEEE, 2024.

[27] Maurya, Vinay, et al. "Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions." Peer-to-Peer Networking and Applications 18.1 (2025): 1-35.

[28] Masmoudi, Atef, and Maha Saeed. "Blockchain-Driven Decentralization of Electronic Health Records in Saudi Arabia: An Ethereum-Based Framework for Enhanced Security and Patient Control." International Journal of Advanced Computer Science & Applications 15.4 (2024).

[29] Singh, Renu, Ashlesha Gupta, and Poonam Mittal. "A Systematic Literature Review on Blockchain-based Smart Contracts: Platforms, Applications, and Challenges." Distributed Ledger Technologies: Research and Practice (2024).

[30] Tyagi, Amit Kumar, and Shrikant Tiwari. "Blockchain-Enabled Smart Healthcare Applications in 6G Networks." Digital Twin and Blockchain for Smart Cities (2024): 459-494.