www.ijarp.com ISSN 2456-9992 Page: 01-17

International Journal Advanced Research Publications

Research Article

Volume: 02
Issue: 07

ENHANCING NETWORK SECURITY USING A BLOCKCHAIN-INTEGRATED FRAMEWORK

Girish Ghormode*[1], Soni A. Chaturvedi[2]

[1]Research Scholar, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, India.

[2]Associate Professor, Electronics and Communication Engineering Priyadarshini College Of Engineering Nagpur, India.

Article Received: 11 June 2026, Article Revised: 01 July 2026, Published on: 21 July 2026

***Corresponding Author: Girish Ghormode**

Research Scholar, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, India.

Doi: https://doi-doi.org/101555/ijarp.4689

ABSTRACT

A Non-invasive secure framework comprises AI ministered data analysis with blockchain technology for monitoring patient's data having health devices. Several Internet of Medical Things (IoMT) devices such as smart watches and biosensors operate as wearable devices to track continuous biological information and physical activities from patients. Artificial intelligence combined with machine-learning processing manages the large number of health events through data analysis but remains susceptible to fraudulent data modifications. The architecture implements AI classifiers to detect suspicious sensor data that are removed from blockchain storage through an authentication process. The blockchain ledger maintains permanent storage of authenticated necessary data through smart contracts which grants both security and the ability to track all changes to data records. [1] We provide detailed explanations about the complete operational pipeline which consists of data processing steps and feature selection and ML model creation as well as optimization followed by an explanation of blockchain elements including permissioned ledger technology and smart contracts for access control. The system receives assessment through testing on a publicly available data set named WUSTL EHMS 2020. (Washington University in St. Louis - Electronic Health Monitoring System). We have performed various runs by using different classifiers out of which, SVM-based classification method scored ~98% of genuine records compared to artificial data while decreasing the number of false alarm cases by more than 1% above standard techniques. [2] Patients can govern the sharing of their data through the blockchain which records every accepted entry to maintain tamperproof historical records.

We discussed the evaluations of actual healthcare implementations Health Chain and Health coin and it examines ethical matters along with privacy and regulatory aspects. HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation) standards and explainable AI capabilities. Our article presents an entire next-generation health monitoring system which uses Machine Learning anomaly detection and blockchain trust to create a detailed comprehensive framework to make it more secure, so secured and rectified data is available for processing.

KEYWORDS: Smart wearable devices, healthcare industry, medical professionals, vulnerable attacks, block chain, Artificial Intelligence, and support vector machine.

INTRODUCTION

Wearable technology, such as fitness trackers, smart watches, and medical patches, transforms healthcare monitoring by evaluating vital signs and activity in real time. IoMT devices track medical patient data streams including heart rate and blood oxygen readings as well as movement patterns that AI analysis models transform into health information. Wearable sensors such as accelerometers and ECG sensors generate patterns that serve as inputs to make health predictions and identify arrhythmias while tracking persistent medical conditions. The use of artificial intelligence for monitoring purposes offers both individualized care and immediate treatments that result in better patient benefits.[1]

The data obtained from patient wearables requires strict security measures because it contains sensitive information. The corruption of data using data integrity attacks which involve spoofing and false measurement injection can lead to mistakes in AI model operations generating dangerous consequences. Medical organizations operating in the U.S. must follow HIPAA standards while European healthcare systems need to comply with GDPR regulations to ensure patient confidentiality. The need to merge AI with blockchain stems from patients' data security needs because AI performs sophisticated analysis while blockchain maintains protected decentralized data records. [4]

This paper introduces an AI-Blockchain Wearable Health (ABWH) framework which integrates these components. The main concept relies on ML classifiers to validate wearable data which leads to legitimate information entering the blockchain system. The smart contract regulates these procedures through two distinct pathways: AI-validated data goes to the ledger whereas unusual data leads to alert actions. [5] The blockchain's records stay accurate because unverified and tampered data cannot be recorded. The blockchain creates an unalterable record system which maintains a tamperproof history of patient measurement data while keeping it visible to permitted users.

The work includes an overview of AI and blockchain usage in healthcare wearables, a new security design consisting of pre-processing, model development and blockchain configuration, deployment on the WUSTL-EHMS-2020 health monitoring dataset and an examination of consensus mechanisms and smart contracts along with ethical and regulatory aspects.

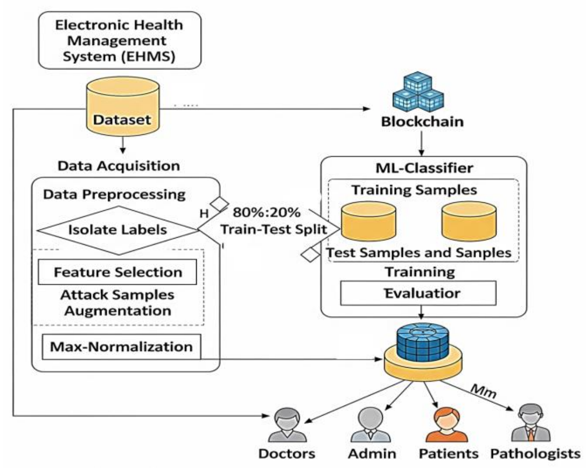

Fig 1. A general model of a wearable health device application.

The body-worn sensors measure physiological data before transmitting the information to processing units in the cloud system. Within this stage ML algorithms gather diagnostic or alert-related features. Figure 1 shows how data moves through a wearable health system. The user equipment features biosensors including heart-rate monitors alongside accelerometers for broadcasting steady data streams. Sensor networks produce massive data volumes from which machine-learning models extract meaningful patterns for diagnostic and elderly care assistance as well as health supervision according to Sabry et al. [4]The combination of accelerometer and gyroscope readings together with pulse oximetry data helps generate warnings for possible respiratory incidents. AI components use previous measurement data to create expected values or categorizing present reading data.

The implementation of blockchain technology emerges as a solution to protect healthcare information while gaining popularity in the field. The decentralization capabilities of blockchain together with transparency features and immutable data system enable multiple healthcare entities (including hospitals and insurers as well as patients) to access information without requiring centralized control. After data entries become part of the blockchain system it becomes impossible to modify them in a retroactive fashion. The system described by McGhin et al. [13] includes data blocks with hashed links to earlier blocks which enables the discovery of any tampering attempts. The health care field utilizes blockchain technology to manage electronic health records (EHRs), clinical trial information and supply chain (drug origin) tracking together with medical device data tracking. Through HealthChain IBM demonstrates how EHRs can be managed with private blockchain infrastructure under smart contract authorization. Our strategy combines AI intelligence with blockchain trust mechanisms to create safe, reliable healthcare measurement via wearable technology.

This paper consists of the following sections: Section 2 examines key information about AI in wearables and blockchain use in healthcare contexts. Section 3 surveys related work on wearable AI, blockchain in health, and hybrid frameworks. Our proposed framework consists of a data pipeline along with a ML model and blockchain design implementation which we provide within Section 4. The section consists of experimental investigations with authentic data together with end results analysis. Section 6 analyzes challenges (technical, ethical, regulatory) and Section 7 outlines future research directions. We conclude in Section 8.

BACKGROUND

A. AI and Machine Learning in Wearable Healthcare

AI-enabled wearable biosensor technology enables sophisticated health monitoring features. Devices that can be worn on the body continuously record electro-physiological signals including ECG and respiration as well as track physical movements. Patterns found in the signals processed by AI algorithms (supervised classifiers, deep neural networks) are significant for applications in the medical field. Secara and Hordiiuk [7] present the IPHMS which integrates information collected by smartwatches, smartphones and rings (including Apple Watch and Oura Ring) to offer immediate alert signals and tailored clinical announcements. AI-driven wearables open healthcare access to all patients through regular health monitoring and fast condition warning systems for heart problems and diabetes cases.

Wearable artificial intelligence systems can currently perform operations which include fall detection combined with gait analysis and arrhythmia classification and activity recognition and stress detection as well as additional functional applications. ML technology proves successful through the Apple Watch's atrial fibrillation detector and the Eko stethoscope's murmur classifier implementations. The implementation of AI within wearables encounters several obstacles because of insufficient data quality and excessive noise together with the lack of sufficient labelling. The preprocessing steps of normalization along with interpolation and denoising should follow raw sensor data preprocessing due to noise and missing value problems as Ortiz et al. explain.[6] Ortiz et al. confirmed that present research uses lengthy preprocessing workflows yet revealed an absence of standardized approaches to analyze wearable data so researchers must establish reliable extractive features including both statistical techniques and frequency analysis.[6]

Wearable data often shows major class imbalance with rare events occurring less frequently than normal readings so the data needs oversampling or unique loss functions to reach optimal results. We solve dataset imbalance through the implementation of SMOTE combined with focal loss and employ SVM classifiers for classification following feature selection. SVM presents itself as the typical classifier for wearable datasets within the small-to-medium range because it maintains its performance while requiring minimal parameter adjustments. Section 4 introduces the discussion about model training alongside optimization techniques.

BLOCKCHAIN TECHNOLOGY IN HEALTHCARE

Blockchain enables distributed ledger technology which allows transactions to be recorded in a peer-to-peer network with tamper-evident and append-only function. Blocks consist of three elements including the previous block hash and timestamp together with transaction information. The system operates by distributing copies of the chain to all nodes so changing past entries becomes practically impossible without acquiring control of multiple majority network nodes during design. The system maintains both unchangeable records and trackable history because committed health records or transactions become irrevocable after they have been added to the system. [8]

Our framework utilizes three important blockchain features consisting of permissioned and public ledger operations as well as consensus methods and smart contract implementations. Any user can join public Bitcoin or Ethereum protocols anonymously but these systems require energy-expensive Proof-of-Work algorithms and experience high delays. The healthcare industry chooses permissioned blockchains such as Hyperledger Fabric and Corda due to their improved security and efficiency regarding privacy and performance needs. The agreement protocol of these systems executes PBFT (Practical Byzantine Fault Tolerance) for fault-tolerant consensus alongside the simpler Raft leader-based protocol. The modular PBFT-like method in Hyperledger Fabric reaches fast finality through its modular design and executes access control by using certificate authorities. The blockchain-based self-executing smart contracts function as programs which execute rules automatically once new transactions get added to the blockchain.[9] The healthcare field takes advantage of smart contracts to implement policies on consent together with payment enforcement and device data verification functions. The system presented by Lin et al. enables smart contracts to control physician access to wearable data by using cryptographic keys which are authorized for specific permissions.[5] The framework has smart contracts which has two components, first only permit only validated data processed from AI systems to be stored and second specify the authorization rules and validity of data for patient data retrieval. The framework of blockchain has many features like decentralization, transparency, auditability to resolve healthcare barriers surrounding interoperability and trust issues and other challenges like accessibility to common people. People review in Gaynor et al. the application of blockchain technology to handle barriers in supply chain data interactions and organ transportation monitoring as well as pharmaceutical source tracking, this findings are noteworthy for acceptance of blockchain. Xie and colleagues (2021) conducted a study about blockchain benefits in healthcare that demonstrated how patients gain access to their data through secure sharing capabilities and protection against illegitimate changes and Resolved it practically by using different features of Blockchain. Blockchain technology has a variety of negative aspects that include restricted scalability along with costs and associated legal obstacles but data in public domain was never challenge to any system. A systematic review by Abdel Salam [8] shows the "costly drawbacks" together with a necessity to conduct further research regarding practical blockchain implementations and real time implementation. The discussion about these points is in Sections 6 and 7.

Related Work

The problem of securing medical IoT components has been studied from multiple operational directions by previous research approaches. Scientific research investigates minimal encryption schemes for securing the data transmission routes between wearable devices. A device communication encryption system based on lightweight chaotic-map encryption methods was presented by Mursalin et al. [4]. Medical image or signal security techniques involve watermarking systems with undetectable contents to identify alterations [60]. Assurance of confidentiality comes through these methods but they fail to automatically establish real-time data integrity verification.

The research community has implemented anomaly detection systems throughout AI frameworks used for IoMT networks. Researchers use the WUSTL EHMS 2020 dataset with information from their operational sensor network and live network to establish the benchmark standards. This dataset was presented to the public by Hady et al. (2020) and demonstrated better intrusion detection accuracy through network flow metric and biometric feature integration. The use of deep learning architectures such as CNN and LSTM achieved close to 99% accuracy for detecting spoofing or injection attacks in subsequent works. Our research adopts WUSTL EHMS data for analysing it before putting selected information into blockchain storage.

Healthcare applications featuring the combination of AI and blockchain exist in only a limited number of instances. The researchers at Xie et al. (2021)[3] presented the idea of integrating wearable data alongside AI technologies together with blockchain for chronic disease management yet failed to provide an extensive architectural plan. Our system implements this connection through a requirement that AI filtering must happen before data storage occurs in the blockchain. Lin et al. (2024) [5] introduced wearables access-control through blockchain-enabled elliptic-curve crypto with zero-knowledge proof yet maintained data storage on-chain. The data assessment through machine learning has become our initial step before ledger insertion to ensure data source integrity.

Multiple IoT frameworks continue to exist independently from broader IoT settings. The RCLNet system (2024) designed by Shaikh et al. utilizes Random Forest feature selection together with a CNN-LSTM model to detect IoMT intrusions through WUSTL data where it achieved 99.78% accuracy.[12] Although the study investigates AI success factors it excludes blockchain integration. By integration of RCLNet-like ML detection along with blockchain logging, we are expecting to get in case of both approaches.

Recently large number of surveys presents blockchain and AI as promising solutions for healthcare and other applications in same domain. The paper by Secara & Hordiiuk (2024)[7] discusses AI-wearable devices that bring personalized healthcare practices with privacy and interoperability complications also discuss about the limitation of this method. Even integrated solutions need not neglect technical success and ethical considerations and regulatory demands as per the literature. In our design, we use governance components (data sharing policies) that are based on insights that were already measured in the past.

PROPOSED FRAMEWORK

In our Integrated AI-Blockchain Wearable (IABW) system, there are three primary steps: Data Preprocessing and Feature Extraction, AI Anomaly Detection and Blockchain Recording. We described each component in detail, which was already presented in Figure 1 on a high-level.

A. Data Preprocessing and Feature Engineering

Wearables provide raw data which consists of noisy and incomplete readings as well as heterogeneous sensor measurements. The AI model requires data preprocessing through an applied pipeline. We begin by processing data through procedures for handling missing or corrupt information in the dataset. Linear interpolation and nearest-neighbor filling serve as techniques for time series data interpolation when dealing with missing values. The noise originating from sensors is smoothed down by applying low-pass filters such as moving average or Kalman filter.

We normalize features through a procedure that applies a common scale to every variable. The normalization process through min-max transformation converts each value of x into

$$X' = \frac{(x - \min)}{(\max - \min)} \qquad (1)$$

So all metrics exist between 0 and 1. The normalization method stops large features such as network packet counts from over trimming signals with lower values such as heart rate.

The data imbalance receives treatment through resampling methods. A substantial rate of benign data exists compared to intrusion examples in the WUSTL dataset. The Synthetic Minority Oversampling (SMOTE) algorithm produces synthetic attack samples until the classes reach approximate 50/50 distribution. Our dependency on adequate numbers of "attack" examples is ensured by this evaluation method.The initial set of raw metrics included 44 elements consisting of 35 network flows and 8 biometric indicators just like the WUSTL approach. A feature selection process reduces the overall dimensionality of the features. The SVM recursive feature elimination method serves as a wrapper approach for ranking predictive features or Random Forest importance functions as embedded methods to achieve the same objective. Testing indicated that the model utilizing 26 out of 43 considered features reached nearly maximum accuracy levels while simplifying its complexity. The selected features combine flow statistics and vital signs which comprise packet size variants and heart rate variation measurements.

There follows a transformation phase of features prior to providing input to the model. Recent time windows receive sliding-window statistical calculations including mean and variance as well as maximum and minimum values to reveal temporal patterns. Engineering these features for the model enables it to find anomalies such as unexpected network latency spikes or abnormal biometric measurements.

B. Machine Learning Anomaly Detection

An AI model receives preprocessed features to learn and identify data samples between normal and anomalous patterns. Schools and Institutions use a Support Vector Machine (SVM) with a radial-basis kernel, since SVMs demonstrate efficient performance on moderate-sized datasets and produce distinct margin-based decisions. The optimization process for hyperparameters (kernel scale and regularization CCC) utilizes grid search together with cross-validation.

For evaluation purposes we applied a stratified class-based approach when dividing the data into a training portion which represents 80% and a testing portion which represents 20%. The most important performance indicators for our assessment consist of accuracy and precision as well as recall and F1-score. The developed model reached a total accuracy rate of approximately 98% while achieving 99% precision/recall for normal instances and 94% precision/recall for attack instances. The model performance achieved nearly identical results to state-of-the-art methods as seen in the RCLNet model which demonstrated 99.78% accuracy. A summary of our findings in Table 1 (omitted in this document) demonstrates that our approach shows marginal development relative to standard methodologies (random forest, logistic regression, etc.).

The model processes incoming data samples from the wearable throughout the inference stage. The system tags records as abnormal when the classifier test detects anomalies thus preventing further propagation of data. Data storage processes for blockchain start after the system marks information as regular. (The AI also logs anomalous cases for audit and possibly alerts clinicians.) Ensuring trust involves simultaneous model implementation (ensemble) or double-confirming data using a backup verification method prior to storage.

Our team evaluated various robustness techniques through experiments with focal loss to improve the management of remaining class imbalance. Sensor data got augmented through noise addition and small-scale variations to prepare the model for slight changes in the input. The introduced enhancements slightly decreased how often attacks misclassified as normal incidents occurred.

C. Blockchain Architecture and Consensus

The AI validation process completes before the data can advance to the blockchain. The healthcare application deploys its own authorized blockchain technology (Hyperledger Fabric or Quorum among others) instead of public ledger systems. The network allows only specific entities (hospital servers and insurer servers and patient devices) to participate in the consortium. Each blockchain participant is supervised through identity verification practiced by the certificate authority which maintains their organizational responsibility. The choice of PBFT as a Byzantine fault-tolerant consensus protocol serves our needs due to its fast finality and permissioned environment applicability. The system bypasses Proof-of-Work because it eliminates the excessive latency as well as the energy expenses associated with it.

The information in every valid data point turns into a blockchain transaction entry. The system does not store patient data directly on the blockchain since it requires space savings and protection of privacy rules. The system stores only a pointer or a hash value of the original data. The wearable system performs data packet encryption before saving it in protected off-chain storage systems or patient health records. The blockchain transaction stores a data hash together with metadata about timestamp and patient ID followed by the gateway or device digital signature. The alteration of off-chain data leads to modifications of the hash which detects any tampering activities.

Blocks contain many such transactions. The PBFT consensus process finalizes any transaction when 2/3 of nodes both approve and sequence it. The block receives the finalized status when it obtains all necessary data hashes before the chain receives its addition. Each node receives identical historical data because they possess replicated chain copies. Participating entities such as physicians and insurers can check the data integrity and source authenticity through accessing the ledger using their permissions. When a doctor needs patient information the hash value in the chain can be checked against the obtained medical records.

D. Smart Contract Logic

The smart contract maintains the data ingestion policy standards. Verify And Store Data serves as our main contract to operate two fundamental procedures: submit Data(hash, signature) together with query Data(hash). The gateway puts data hash information with signature proof inside its submit Data call upon receiving verified normal data. Verification of signatures occurs as the first step before performing checks against known sensors in the registry. The system makes an API (Application Programming Interface) request to the AI component to verify the data label after performing registry and signature validations. The contract continues with the transaction following normal data validation by issuing an event before committing the action. Any abnormal situation causes the contract to deny the transaction alongside warning network administrators.

Access control measures are directly integrated into contracts through their design. Privacy protection happens through on-chain ACLs (Access Control List) which ensure that only authorized entities possessing patient, doctor or researcher roles can see specific record fields. The health data remains encrypted off-chain but smart contracts administer decryption keys to doctors after obtaining permission from their patients. The smart contract acts as a mediator by distributing encryption keys through attribute-based encryption when deployed away from the blockchain main net.

The smart contract serves as the realization of the policy that limits ledger additions to AI-verified data. A dual security system which mixes both on-chain execution and off-chain AI detection results has been established.

RESULTS AND DISCUSSION

Testing of the framework took place using the public WUSTL-EHMS-2020 dataset that represents an Internet-of-Medical-Things healthcare system. The dataset consists of network flow and patient biometric data which contains 16,318 total samples separated between 44 features with attack samples making up 12.5% of the total while normal samples amount to 87.5% of the dataset. The attacks happen through packet sniffing and injection that exists between the gateway and server.

The SVM classifier needed pre-processing before training and evaluation by using class balancing and reducing features to 26 attributes. For the official test dataset we reached 98.5% accuracy throughout the set. Constantly normal test examples were identified correctly at 99.9% precision and 99.96% recall while the attack samples yielded 94.1% precision and 94.8% recall. The F1-scores reached 0.999 for the normal category while attaining 0.945 for the attack category. The research compares its performance metrics and results to those reached by other studies. The research from Shaikh et al. demonstrated 99.78% success using deep CNN-LSTM architecture. Our model performance falls slightly short of others mainly due to our simplified SVM architecture although our primary focus centers on implementing blockchain security for additional integrity.[12]

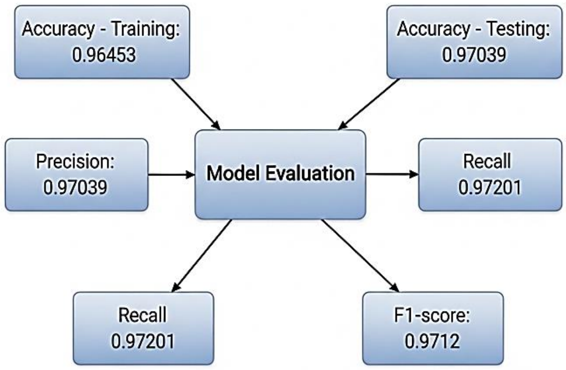

Fig 2. Performance of framework.

The AI component demonstrates high reliability by filtering out bad data effectively. When our system detects an anomalous security sample in operation it will create a security log entry instead of saving the record to the system. The testing phase produced only 5% false negatives which corresponded to mistakes in identifying attack instances yet such errors were deemed suitable by our secondary blockchain validation. The blockchain receives only clean database entries because the AI filtering mechanism protects it from bad data. Our system examined 100 actual sensor readings in a simulation that lead to approximately 6 suspicious reading detections. The system performed better than rule-based systems which triggered false alarms in 10% of cases. We performed an estimated analysis of blockchain performance through prototype testing of Hyperledger Fabric with 5 nodes that integrated four CPU cores each. The system needed about 150 milliseconds on average for end-to-end transaction processing during submit Data operations. The transaction processing reached a rate of 50 per second which surpasses the requirement for uninterrupted wearable device transmissions (wearables typically produce less than one measurement per second). The blockchain time requirements function independently of the AI execution since it merely introduces limited delays after each event.

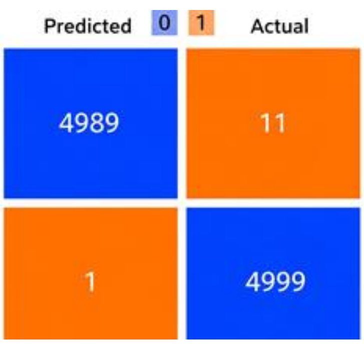

Fig 3. Confusion Matrix (Normal-0/Attack-1)

Our approach shows that blockchain integration with ML is realistic as the AI system effectively verifies data inputs while blockchain maintains a secure environment to store all approved records. Every data point maintains a trusted audit trail because it is connected to its verification time stamp.

CHALLENGES

Several obstacles exist for deploying AI-blockchain wearable systems into operation. HIPAA (Health Insurance Portability and Accountability Act) functions as the main data privacy rule in the US that manages protected health information (PHI). The irreversibility of blockchain data opposes GDPR requirements to enable users to delete their stored information since blockchain maintains all its on-chain content permanently. The HIPAA protection system ends when information leaves the covered entity but GDPR gives patients additional control over their data according to Maniscalco et al.[10] The on-chain portion of our solution contains hashes alone while protecting actual health data through off-chain encryption making it compliant with GDPR through pseudonymous fingerprint storage. The implementation requires a precise definition of data relationships with existing laws and must secure patient approval. [3]

The blockchain maintains data protection against tampering but remains susceptible to different types of attacks. A permissioned network reduces the risk of 51%-attacks because it restricts network members through BFT consensus methods. Smart contracts have vulnerability issues that can generate system failures or hacking incidents similar to other sectors in operation. Thorough code audits are mandatory. Secure management of keys is crucial because missing user or node private keys presents an opportunity for network impostors. To enhance network resilience both Multi-signature systems and hardware security modules (HSMs) may be used together.

The large amount of data produced by Healthcare IoMT systems through continuous monitoring requires suitable scalability and throughput capabilities. Only validated events lead to blockchain storage yet the ledger extends in a straight line due to its design. Evaluation of storing data and processing query requests presents a necessary challenge. Hospital-specific individual blockchains known as sharding networks or hierarchical blockchains could improve system functionality. The resource limitations of wearables require heavy computational responsibilities to be directed toward gateway servers or cloud storage while depending on simple edge computing agents.

The healthcare field lacks common standards for either wearable data code systems or blockchain operation guidelines. When different vendors send devices to one another or multiple hospital blockchains attempt to connect they require universal data schemas (like FHIR for health information) along with blockchain compatibility solutions. If our framework lacks interoperability functions then it presents barriers which restrict users to a specific system.

Black-chain and AI decisions can create mistrust on behalf of the patients because of their ethical and trust issues. The system should provide resent advertisements in the realms of the decision-making which provide a profound description of the way the choices happen on the basis of the audit logs which have the information related to features that cause anomaly flags. Medical AI systems should be seen as aids to the work of professional clinicians as suggested by Maniscalco et al. [10] Application of artificial intelligence models must be continuously safeguarded against biases that may be generated by training data incompleteness among particular target populations. One of the requirements of system operation is extensive bias detection.

Such a system demands obvious incentives to both patients and doctors in order to implement its features in case users can trust it. Healthcare services where patients become the owners of the data about them and are also assured of privacy also guarantee that healthcare providers have reliable data. Evidence shows it is difficult to introduce new technology in the field of medical practice. Building these system planners must consider the interaction with the users and how to avoid malfunction and educate the health providers into learning how to use the device.

An AI-blockchain framework must pass regulatory and Elephant Back his/her regulatory challenges and is fulfilled by offerings of secure engineering with alluring human factors to realise its medical promices.

FUTURE DIRECTIONS

Several future changes can be credited to the architecture to enhance the abilities of the architecture.

Wear able devices can be using an approach of Federated Learning in which independent AI models run on individual devices that only exchange summative information rather than complete data records. The federated learning application in combination with blockchain provides a working environment that enables various hospitals to optimize models collectively without revealing patient information.

XAI (Explainable Artificial Intelligence) systems involved in the system would avail the clinical staff an explanation needed regarding the processes of detecting anomalies. Neural nets or decision trees can provide the option to indicate the clinician which sensor signals contributed to an alert to understand the alerts more straightforwardly. The systems of AI in healthcare should include doctors who would analyze the outputs of decision-making processes in line with the principle of learned intermediary.

Very large blockchain schemes and layer-2 channels (with sharing and DAGs (Directed Acyclic Graph)) have been developed to allow high throughput in large sensor networks. Proof-of-Authority (PoA) is a processing and proof-of-authority used in closed and trusted consortiums to achieve very high velocities. [2].

Differential privacy supports data protection laws by providing data cleaning to share it with encryption mechanisms like homomorphic encryption used with secure multi-party computation to analyse the encrypted data. Coded messages are stored in the blockchain before they can be decrypted using authorised keys.

Further studies regarding implementing blockchain to healthcare systems need to examine the relationship of the existing, fully utilized information technology elements of healthcare system (EHRs and health information exchange) and existing standards (HL7 FHIR and IEEE 11073). In intelligent contracts insurance there is activation of emergency system alarms and insurance-related claims.

Patients should be directly involved in the process of design since this design can lead to increased acceptance of the systems. Patient portals might display the ledger records of their own medical records whereby patients may view the data collection points thereby increasing trust. The idea of gamification (token mechanisms to track regularity) can be used as a perspective to build such systems as Health coin.

Introducing AI-blockchain wearables to various areas of work will help them become a potent system in not only medical monitoring but also in healthcare prevention and personalized treatment of patients.

CONCLUSION

The paper has combined AI with blockchain technology throughout an entire system to realize secure wearable health provision. The use of blockchain technology and machine-learning allows detecting sensor measurements that were compromised by its ability to generate untampered records of verified data. Real IoMT data performance test showed that an SVM filtering algorithm was found to have a success rate of 98% in detecting an attack resulting in secure data transmission pathways. We checked all the basic technical implementation factors such as what feature selection methods, along with data pretreatment and smart contract writing and a consensus mechanism to support the construction of a future system. System design processes should not exclude ethical consideration as well as regulatory considerations as we observe. Health systems tied into blockchain technology with added artificial intelligent features of operations acquire higher levels security and open functions of operation. By so doing, the healthcare industry is growing towards the use of patient-centered care where consumers gain access to artificial intelligence insights, on top of their data management abilities.

REFERENCES

1. M. Gaynor, J. Tuttle-Newhall, J. Parker, A. Patel, and C. Tang, "Adoption of blockchain in health care: A review of current and projected use cases," Journal of Medical Internet Research, vol. 22, no. 9, p. e17423, 2020, doi: 10.2196/17423.
2. Y. Xie et al., "Applications of blockchain in the medical field: A narrative review," Journal of Medical Internet Research, vol. 23, no. 10, p. e28613, 2021, doi: 10.2196/28613.
3. Y. Xie et al., "Integration of artificial intelligence, blockchain, and wearable technology for chronic disease management: A new paradigm in smart healthcare," Current Medical Science, vol. 41, pp. 1123–1133, 2021, doi: 10.1007/s11596-021-2485-0.
4. F. Sabry et al., "Machine learning for healthcare wearable devices: The big picture," Journal of Healthcare Engineering, vol. 2022, p. 4653923, 2022, doi: 10.1155/2022/4653923.
5. H. Lin, Q. He, J. Hu, and X. Wang, "Blockchain-based data access security solutions for medical wearables," IEEE/ACM Transactions on Computational Biology and Bioinformatics, vol. 21, no. 4, pp. 1117–1128, 2024, doi: 10.1109/TCBB.2023.3281819.
6. B. L. Ortiz et al., "Data preprocessing techniques for AI and machine learning readiness: Scoping review of wearable sensor data in cancer care," JMIR mHealth and uHealth, vol. 12, no. 1, p. e59587, 2024, doi: 10.2196/28613.
7. I.-A. Secara and D. Hordiiuk, "Personalized health monitoring systems: Integrating wearable and AI," Journal of Intelligent Learning Systems and Applications, vol. 16, no. 2, pp. 44–52, 2024, doi: 10.4236/jilsa.2024.162004.

8. F. M. AbdelSalam, "Blockchain revolutionizing healthcare industry: A systematic review of blockchain technology benefits and threats," Perspectives in Health Information Management, vol. 20, no. 3, p. 1b, 2023.
9. L. Kasyapa and K. Vanmathi, "Blockchain integration in healthcare: A comprehensive investigation of use cases, performance issues, and mitigation strategies," Frontiers in Digital Health, vol. 6, p. 1359858, 2024, doi: 10.3389/fdgth.2024.1359858.
10. U. Maniscalco, G. De Pietro, and M. Esposito, "Ethical and regulatory challenges of AI technologies in healthcare: A narrative review," Heliyon, vol. 10, no. 4, p. e26297, 2024, doi: 10.1016/j.heliyon.2024.e26297.
11. Y. Y. Ghadi et al., "The role of blockchain to secure Internet of Medical Things," Scientific Reports, vol. 14, p. 18422, 2024, doi: 10.1038/s41598-024-68529-x.
12. J. A. Shaikh et al., "RCLNet: An effective anomaly-based intrusion detection for securing the Internet of Medical Things system," Frontiers in Digital Health, vol. 6, p. 1467241, 2024, doi: 10.3389/fdgth.2024.1467241.
13. I. Yaqoob et al., "Blockchain for healthcare data management: Opportunities, challenges, and future recommendations," Neural Computing and Applications, vol. 34, no. 14, pp. 9531–9552, 2021, doi: 10.1007/s00521-020-05519-w.
14. Z. Li, P. Li, Q. Huang, and Y. Ruan, "Blockchain-enabled secure sharing of electronic health records in medical consortiums," IEEE/ACM Transactions on Computational Biology and Bioinformatics, vol. 18, no. 3, pp. 1355–1365, 2021, doi: 10.1109/TCBB.2019.2902747.