American Academic Scientific Research Journal for Engineering, Technology, and Sciences
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402
https://asrjetsjournal.org/index.php/American_Scientific_Journal/index

MLNN-Based Anomaly Detection and Blockchain-Enabled Security for Wearable Healthcare Systems

George N Wainaina[a]*, Dr.Nelson Masese(PhD)[b], Dr.Ruth Oginga(PhD)[c]

[a,b,c]*School of Science Engineering and Technology, Kabarak University, Box: 20157 Nakuru, Kenya*
[a]*Email: georgewainaina58@gmail.com/0009-0009-8862-2528*
[b]*Email: NMasese@kabarak.ac.ke/0009-0005-5700-3952*
[c]*Email: ROginga@kabarak.ac.ke/0009-0004-8301-6901*

Abstract

Wearable healthcare systems have become integral components of modern healthcare delivery by enabling continuous monitoring of patient physiological conditions, remote patient management, and real-time clinical decision-making. Despite their benefits, wearable devices remain vulnerable to cyber threats that compromise patient privacy, system integrity, and healthcare service availability. Traditional security approaches struggle to identify sophisticated attacks due to their reliance on static security mechanisms and signature-based detection methods, making them ineffective against emerging and previously unknown threats. This study presents an integrated security model combining Multi-Layer Neural Network (MLNN)-based anomaly detection with blockchain-enabled security to enhance cyber threat identification and mitigation within wearable healthcare systems. The model integrates intelligent anomaly detection, decentralized transaction validation, immutable audit trails, and data integrity protection within a unified cybersecurity architecture. The MLNN component analyzes network traffic characteristics, authentication records, user behavior patterns, device communications, and session activities to detect abnormal system behavior in real time. Blockchain technology complements the detection mechanism by providing secure transaction validation, tamper-resistant record management, transparency, accountability, and decentralized storage of healthcare transactions. A Design Science Research (DSR) methodology was employed to guide the design, development, implementation, and evaluation of the model. A prototype system was developed within a wearable healthcare environment and evaluated using healthcare monitoring data generated by wearable devices. Experimental evaluation demonstrated excellent detection performance, achieving an accuracy of 97.1%, precision of 96.8%, recall of 97.4%, F1-score of 97.1%, and ROC-AUC value of 0.993. Blockchain evaluation further demonstrated efficient transaction processing, a consensus success rate of 99.4%, and a data integrity verification rate of 99.8%.

Received: *5/25/2026*
Accepted: *7/25/2026*
Published: *8/5/2026*

---

* Corresponding author.

The findings demonstrate that integrating machine learning with blockchain technology significantly enhanced cybersecurity resilience, strengthened data protection, and improved trust within wearable healthcare environments. The model provides an effective and scalable approach for securing healthcare data against contemporary and emerging cyber threats.

Keywords: Multi-Layer Neural Network; Blockchain Security; Cyber Threat Detection; Wearable Healthcare Systems; Anomaly Detection; Health Informatics.

1. Introduction

The rapid advancement of wearable healthcare technologies [1,2] has transformed healthcare delivery through continuous monitoring and remote patient management. Wearable devices collect and transmit physiological information, including heart rate, blood pressure, oxygen saturation, body temperature, and physical activity levels. Although these technologies improve healthcare accessibility and patient outcomes, they also introduce substantial cybersecurity challenges.

Wearable healthcare systems operate within highly connected environments [3,4], where sensitive patient information continuously traverses communication networks, cloud platforms, and healthcare databases. Cyber attackers increasingly target healthcare infrastructures due to the high value of medical information [3]. Common attacks include unauthorized access, malware infections, data manipulation, ransomware attacks, denial-of-service attacks, and insider threats [4]. Conventional security approaches primarily rely on predefined rules and signature databases, limiting their ability to detect emerging and previously unknown threats [5]. Consequently, intelligent cybersecurity mechanisms capable of learning evolving attack patterns have become essential [6,2]. This study investigates the use of MLNN and blockchain technology as complementary cybersecurity mechanisms for improving cyber threat detection and protecting healthcare data within wearable healthcare systems.

2. Empirical Review

2.1 Machine Learning in Healthcare Cybersecurity

Machine learning has emerged as an important component of healthcare cybersecurity due to its ability to process large datasets, recognize complex patterns, and identify anomalous behavior that may reveal potential security vulnerabilities and threats [5,2]. The widespread deployment of wearable healthcare devices generates continuous streams of physiological measurements, user behavior records, and communication data, creating security challenges that traditional rule-based systems often fail to address effectively [4]. As cyberattacks become increasingly sophisticated, static security mechanisms struggle to detect previously unknown attack techniques. Machine learning overcomes this limitation by learning from historical data and continuously adapting to emerging threat patterns, thereby enhancing the accuracy and efficiency of cybersecurity defenses [6].

Several machine learning techniques have been explored in healthcare security applications, particularly for intrusion detection, anomaly detection, and cyberattack classification. Frequently adopted algorithms include Support Vector Machines (SVM), Random Forests, Decision Trees, Artificial Neural Networks (ANN), and Deep

Learning models [7,5]. These approaches have shown effectiveness in identifying malicious activities such as unauthorized access attempts, malware infections, insider attacks, and network intrusions within healthcare environments [2]. Among the available machine learning methods, neural network-based approaches have gained significant attention because they can capture complex and nonlinear relationships commonly found in cybersecurity datasets [8,4]. Unlike conventional algorithms that often depend on manually selected features, neural networks can automatically discover relevant features from large and heterogeneous data sources [7]. This capability makes them particularly suitable for wearable healthcare systems, where security solutions must support continuous monitoring, rapid threat detection, and adaptive responses to protect sensitive patient information while ensuring system availability and reliability [9].

2.2 Multi-Layer Neural Networks

Multi-Layer Neural Networks are advanced artificial neural network architectures that learn complex data relationships through multiple layers of interconnected computational nodes known as neurons [8]. Their ability to model nonlinear patterns and perform high-accuracy classification has made them widely applicable in cybersecurity research and practice [4]. Through successive layers of computation, MLNNs can automatically extract important features from raw data and identify subtle patterns that may indicate suspicious or malicious behavior within information systems [7].

An MLNN architecture typically comprises an input layer, one or more hidden layers, and an output layer, each performing a distinct role in the learning and classification process. The input layer receives data from different sources, including network traffic logs, authentication records, user activities, and communication exchanges among devices. Hidden layers process the incoming information through a series of mathematical operations that enable the network to learn increasingly sophisticated representations of the data. The output layer then produces classification outcomes that determine whether observed activities are legitimate or potentially harmful [4,8]. During training, the network employs the backpropagation algorithm to iteratively adjust connection weights and minimize prediction errors, thereby improving its overall performance [7].

In cybersecurity environments, MLNNs are particularly valuable for anomaly detection because they can learn the normal behavioral characteristics of a system and distinguish them from abnormal events that may represent security threats [10,2]. This capability allows MLNN-based security solutions to identify both known attack signatures and previously unseen threats. As a result, they have become increasingly important in healthcare cybersecurity models, where timely threat detection and proactive response mechanisms are essential for safeguarding patient data and maintaining the secure operation of wearable healthcare technologies [4].

2.3 Blockchain Security in Healthcare

Blockchain technology provides a decentralized approach to record management through the use of distributed ledgers that are shared across multiple participating nodes [1,11]. Unlike traditional centralized databases, blockchain systems maintain synchronized copies of transaction records across the network, reducing dependence on a single point of control and increasing resilience against unauthorized modifications or system failures [3].

This decentralized structure has attracted significant interest in healthcare cybersecurity because it offers stronger guarantees for data integrity, transparency, and accountability [12].

Several security characteristics make blockchain particularly suitable for protecting healthcare information. Immutability ensures that once a transaction is recorded and validated within the ledger, it cannot be altered without detection. Transparency allows authorized participants to verify transactions and system activities, while traceability provides a complete historical record of data access and modifications [1]. Decentralization distributes trust among multiple nodes rather than relying on a single authority, thereby reducing the risk of centralized compromise. In addition, blockchain incorporates cryptographic mechanisms that enhance tamper resistance and help prevent unauthorized manipulation of sensitive healthcare records [3,13].

These characteristics are especially valuable in wearable healthcare environments where patient data is continuously generated, transmitted, and accessed by multiple stakeholders [12]. By providing secure transaction validation, audit trails, and verifiable data integrity, blockchain technology strengthens trust among patients, healthcare providers, and system administrators while supporting compliance with healthcare security and privacy requirements [1,6].

2.4 Research Gap

Existing studies have demonstrated the effectiveness of machine learning for anomaly detection [5,6,7,8] and block chain for secure data management in healthcare environments [1,3,11,13]. However, most studies have evaluated these technologies independently, with limited attention given to a unified cybersecurity solution for wearable healthcare systems. Furthermore, many existing approaches focus on either cyber threat detection or data protection rather than addressing both security requirements within a single architecture. This study addresses this gap by developing a unified cybersecurity model that combines intelligent threat detection with decentralized data protection to improve the security of wearable healthcare systems.

3. Research Methodology

This study adopted a Design Science Research (DSR) methodology to guide the development, implementation, and evaluation of an integrated cybersecurity model combining MLNN-based anomaly detection and blockchain-enabled security. The DSR approach was selected because it supports the systematic creation of innovative technological solutions while providing a structured process for validating their effectiveness in addressing real-world cybersecurity challenges within wearable healthcare environments. The research commenced with a comprehensive requirement analysis aimed at identifying the security challenges, functional requirements, and operational needs associated with wearable healthcare systems. Information gathered during this stage informed the design of a security architecture capable of supporting secure data transmission, intelligent threat detection, and data integrity protection. Based on the identified requirements, an MLNN-based anomaly detection model was developed to analyze system activities and classify behavior as either normal or malicious. The neural network was designed to learn complex attack patterns and improve threat detection capabilities through supervised learning techniques.

To complement the anomaly detection mechanism, blockchain technology was integrated into the model to provide decentralized transaction validation, immutable audit records, and enhanced data integrity protection. Following the development of these core security components, a prototype implementation was constructed within the wearable healthcare environment to demonstrate the practical feasibility of the model. The final stage involved extensive experimental evaluation using cybersecurity performance metrics, attack simulations, and security assessment procedures to determine the effectiveness of the integrated model in identifying cyber threats, protecting healthcare data, and improving overall system security. The outcomes of these evaluations provided evidence of the model's capability to enhance cybersecurity resilience within wearable healthcare systems.

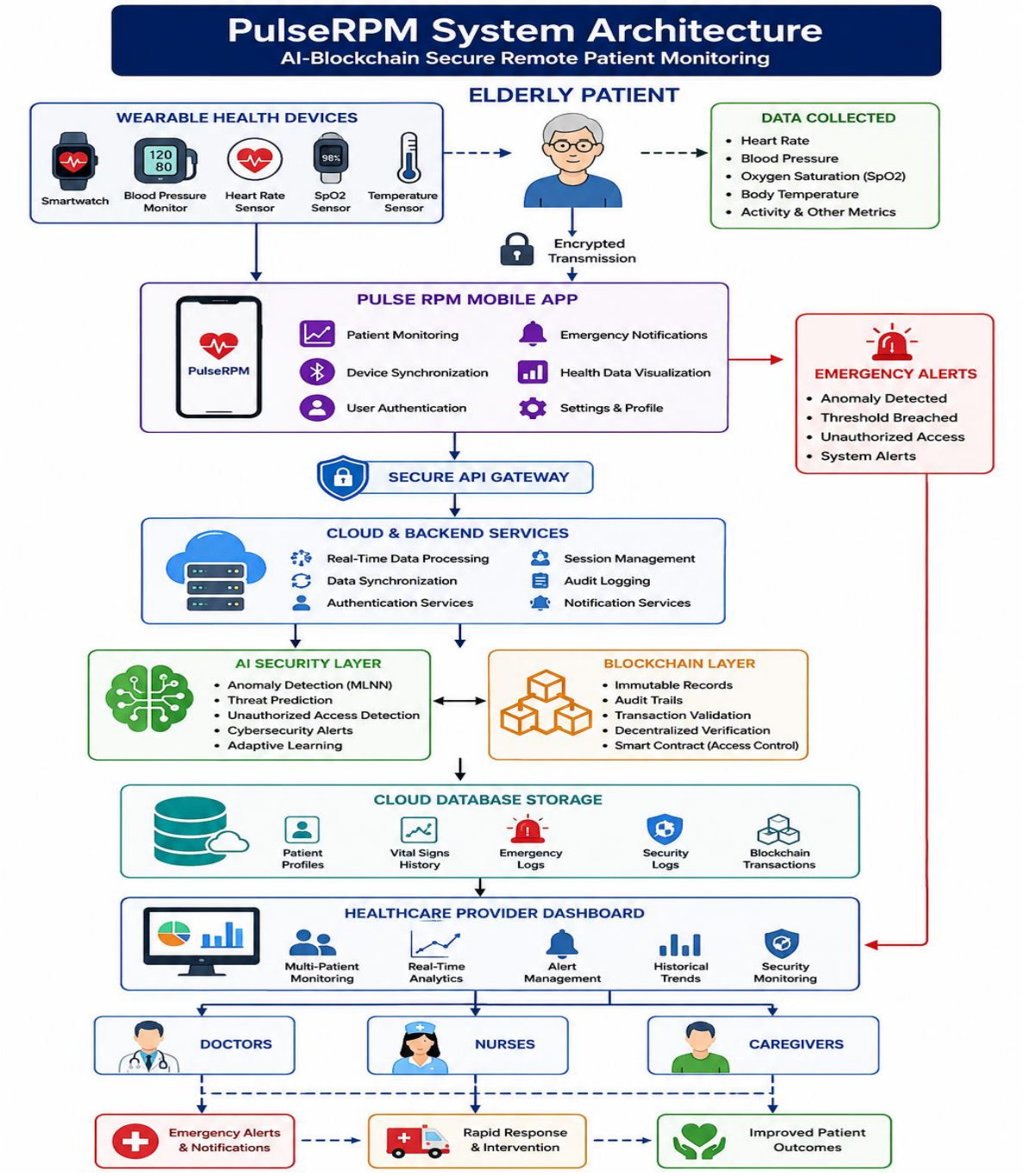

Figure 1: PulseRPM Model Architecture

The implementation was developed within the PulseRPM wearable healthcare platform.

4. Mlnn-Based Anomaly Detection Model

4.1 MLNN Architecture

The anomaly detection component employs a Multi-Layer Neural Network (MLNN) to identify and classify healthcare network activities as either normal or malicious [8]. The model learns complex patterns from security-related data generated within wearable healthcare environments, enabling the detection of abnormal behaviours that may indicate cyber threats [7]. MLNNs have been widely applied in cybersecurity because of their ability to model complex nonlinear relationships and accurately classify normal and malicious activities [4]. By analysing communication activities and system interactions, the MLNN enhances the capability of the cybersecurity model to detect both known and emerging attacks in real time. The architecture comprises four primary layers: The Input Layer, Hidden Layer 1, Hidden Layer 2, and the Output Layer. The Input Layer receives security attributes extracted from healthcare communication activities, including network traffic characteristics, authentication records, user behaviour patterns, and device communication data [7]. Hidden Layer 1 and Hidden Layer 2 perform feature extraction and pattern learning, enabling the network to identify complex relationships within the input data. The Output Layer generates the final classification result, indicating whether the observed activity is legitimate or represents a potential cyber threat. This layered architecture is consistent with multilayer neural network models reported in previous studies [8], while being adapted to the cybersecurity requirements of wearable healthcare systems.

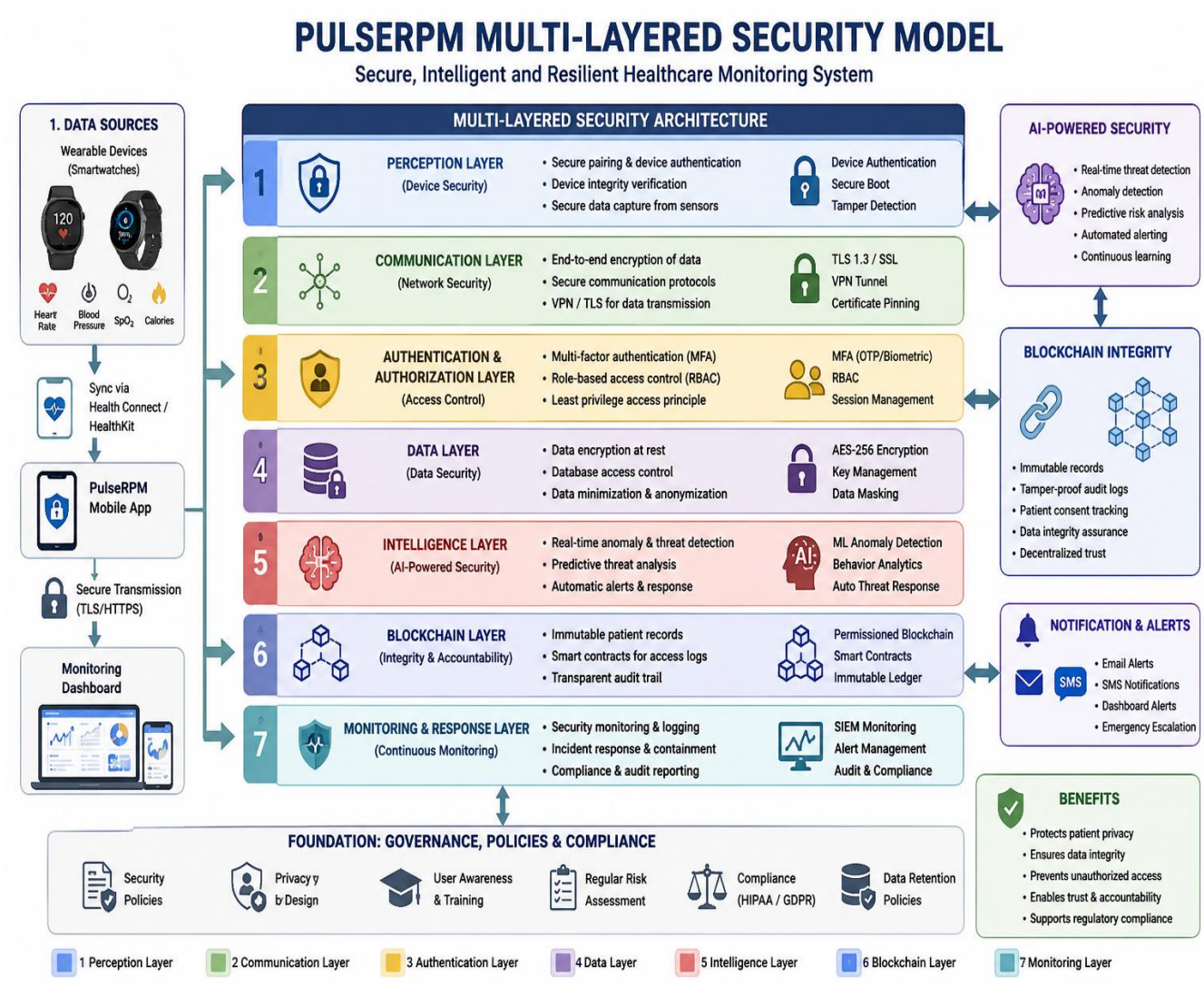

Figure 2: Multilayered Security Mode

4.2 Feature Extraction

The effectiveness of the MLNN model depends on its ability to analyse relevant security features extracted from healthcare communication activities [6]. These features provide valuable insights into system behaviour and enable the model to identify patterns associated with both normal operations and malicious activities. Feature extraction is a critical stage in machine learning because the quality of the selected features directly influences classification performance [7]. By examining multiple aspects of network and user interactions, the MLNN can detect unusual behaviours that may indicate potential cyber threats. The features analysed by the model include network traffic characteristics, authentication attempts, user behaviour patterns, access frequency, device communication records, and session activities [2].

Network traffic characteristics provide insights into data transmission behaviour, while authentication attempts help identify unauthorized access efforts. User behaviour patterns and access frequency enable the detection of abnormal user actions, whereas device communication records monitor interactions among wearable devices and

healthcare systems. Session activities further assist in identifying suspicious operations occurring during active user sessions. These security attributes have been widely used in anomaly detection models for identifying malicious activities within healthcare and IoMT environments [9]. Collectively, these features enable the MLNN to distinguish legitimate healthcare operations from potential cyber threats with a high level of accuracy.

4.3 Training Process

The MLNN model was trained using supervised learning techniques, where labelled data representing normal and malicious activities were used to teach the network how to distinguish between legitimate operations and potential cyber threats [8]. Supervised learning enables neural networks to learn classification patterns from labelled datasets and has been widely applied in cybersecurity for intrusion and anomaly detection [6]. The training process was designed to enable the model to learn meaningful patterns from healthcare communication data and improve its classification performance over time [7].

The training procedure involved several stages, including data preprocessing, feature normalization, training dataset generation, validation dataset generation, model optimization, and performance evaluation. Data preprocessing was performed to clean and prepare the dataset for analysis, while feature normalization ensured that all input variables were scaled appropriately for effective learning [7]. The dataset was then divided into training and validation sets to support model development and testing. During optimization, the network adjusted its internal parameters to reduce prediction errors and improve classification accuracy through iterative weight updates using the backpropagation learning algorithm [8]. Finally, performance evaluation was conducted using standard machine learning metrics to assess the effectiveness of the model. The overall objective was to minimize classification errors while maximizing the accuracy of cyber threat detection within wearable healthcare systems.

5. Blockchain-Enabled Security Model

5.1 Blockchain Architecture

The blockchain component provides a secure mechanism for managing healthcare transactions through distributed validation mechanisms. Instead of relying on a centralized authority, transactions are verified and recorded across a decentralized network of participating nodes [3,1]. This approach enhances security, transparency, and trust by ensuring that healthcare records cannot be altered without detection. The blockchain architecture strengthens the protection of sensitive patient information generated by wearable healthcare systems and supports secure data sharing among authorized stakeholders

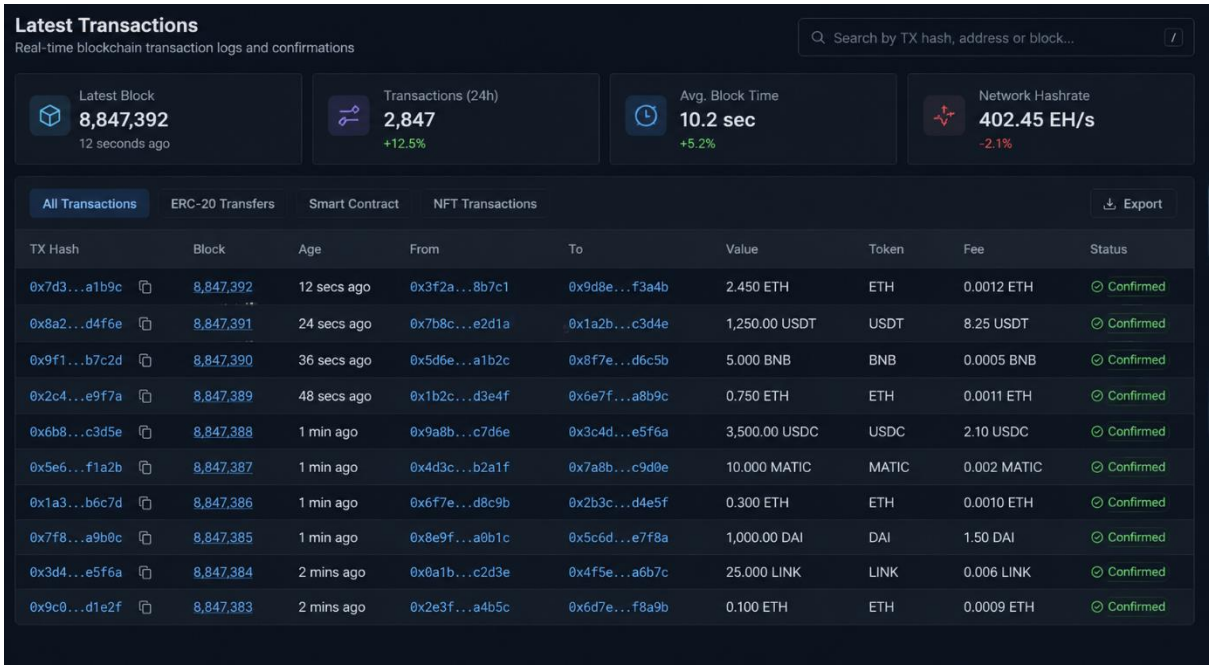

Figure 3: Blockchain Transaction Log

The blockchain layer performs several critical security functions, including transaction validation, integrity verification, audit logging, and decentralized record management [1]. Transaction validation ensures that only legitimate healthcare transactions are accepted into the network, while integrity verification confirms that stored records remain accurate and unaltered. Audit logging creates a transparent and traceable history of all activities, supporting accountability and regulatory compliance. In addition, decentralized record management distributes healthcare data across the blockchain network, reducing the risk of single points of failure and enhancing the overall resilience of the healthcare system [13].

5.2 Smart Contract Integration

Smart contracts [1] were integrated into the blockchain model to automate the enforcement of security policies within the wearable healthcare environment. A smart contract is a self-executing program stored on the blockchain that automatically performs predefined actions when specified conditions are met. By eliminating the need for manual intervention, smart contracts enhance security, improve operational efficiency, and ensure the consistent application of healthcare security policies.

The smart contract module performs several important functions, including access authorization, permission validation, transaction verification, and security event recording [3]. Access authorization ensures that only approved users and devices can interact with healthcare resources, while permission validation confirms that users operate within their assigned privileges. Transaction verification checks the legitimacy of healthcare transactions before they are recorded on the blockchain, thereby preventing unauthorized activities. Additionally, security event recording creates an immutable log of security-related actions, supporting transparency, accountability, and effective auditing within the healthcare system.

5.3 Data Integrity Protection

To ensure the integrity and security of healthcare information, each transaction undergoes cryptographic hashing Reference [13] before being recorded within the blockchain ledger. Cryptographic hashing generates a unique digital fingerprint for every transaction, making it extremely difficult for unauthorized individuals to alter stored records without detection. Any modification to a transaction changes its hash value, immediately indicating potential tampering. This mechanism preserves data integrity, strengthens trust among healthcare stakeholders, and supports the secure management of sensitive patient information [3].

In addition to data integrity protection, the model incorporates AI-based threat detection alerts through the MLNN anomaly detection module. The MLNN continuously monitors network traffic, user activities, authentication events, and device communications to identify suspicious behaviours that may indicate cyber threats. When abnormal activities are detected, the system automatically generates real-time security alerts, enabling healthcare administrators to respond promptly to potential attacks. The combination of blockchain-based integrity protection and AI-driven threat detection provides a proactive and resilient security environment for wearable healthcare systems.

Figure 4: AI Threat Alert Demonstration

6. Experimental Results

6.1 MLNN Classification Performance

The classification performance of the MLNN model was evaluated using standard machine learning metrics to determine its effectiveness in detecting cyber threats within wearable healthcare systems. Experimental results demonstrated strong predictive capability, with the model achieving an accuracy of 97.1%, precision of 96.8%,

recall of 97.4%, and an F1-score of 97.1%. The high accuracy indicates the model's ability to correctly classify both normal and malicious activities, while the precision value reflects its effectiveness in minimizing false alarms. Similarly, the high recall demonstrates the model's capability to identify the majority of actual cyber threats, and the F1-score indicates balanced performance between precision and recall. These results demonstrate the effectiveness of the MLNN in distinguishing legitimate healthcare operations from malicious behavior, making it a reliable component for real-time anomaly detection in wearable healthcare environments.

Table 1 : Confusion Matrix Results

Actual Class	Predicted Attack	Predicted Normal
Attack	487	13
Normal	16	484

Table 2: Neural Network Performance Results

Metric	Result
Accuracy	97.1%
Precision	96.8%
Recall	97.4%
F1-Score	97.1%
False Positive Rate	3.2%
False Negative Rate	2.6%
ROC-AUC	0.993

6.2 ROC Analysis

Receiver Operating Characteristic (ROC) analysis was performed to evaluate classification capability.

Table 3: ROC Threshold Analysis Results

Classification Threshold	True Positive Rate (TPR)	False Positive Rate (FPR)
0.10	1.000	1.000
0.20	0.994	0.186
0.30	0.989	0.108
0.40	0.982	0.061
0.50	0.974	0.032
0.60	0.960	0.018
0.70	0.938	0.010
0.80	0.901	0.005
0.90	0.842	0.002
1.00	0.000	0.000

Table 4: Trapezoidal Integration of ROC Curve

Segment	ROC Point 1 (FPR,TPR)	ROC Point 2 (FPR,TPR)	Width (ΔFPR)	Average Height ($(TPR_1+TPR_2)/2$)	Area
1	(1.000,1.000)	(0.186,0.994)	0.814	0.9970	0.8116
2	(0.186,0.994)	(0.108,0.989)	0.078	0.9915	0.0773
3	(0.108,0.989)	(0.061,0.982)	0.047	0.9855	0.0463
4	(0.061,0.982)	(0.032,0.974)	0.029	0.9780	0.0284
5	(0.032,0.974)	(0.018,0.960)	0.014	0.9670	0.0135
6	(0.018,0.960)	(0.010,0.938)	0.008	0.9490	0.0076
7	(0.010,0.938)	(0.005,0.901)	0.005	0.9195	0.0046
8	(0.005,0.901)	(0.002,0.842)	0.003	0.8715	0.0026
9	(0.002,0.842)	(0.000,0.000)	0.002	0.4210	0.0008

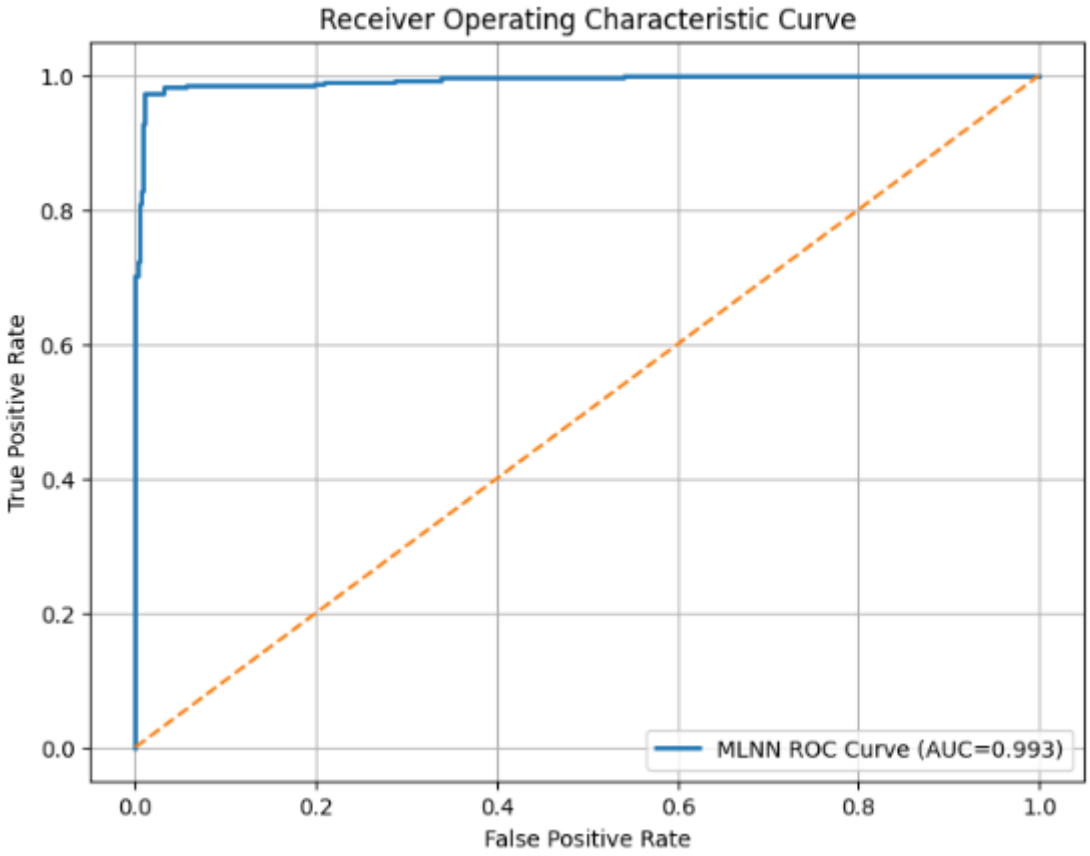

Figure 5: Receiver Operating Characteristic (ROC) Curve for the MLNN Classifier

The MLNN achieved an ROC-AUC value of 0.993, indicating exceptional classification performance.

6.3 Blockchain Performance Evaluation

The blockchain component was evaluated to determine its effectiveness in securing healthcare transactions and protecting sensitive patient information within wearable healthcare systems. The assessment focused on key performance indicators, including transaction validation efficiency, integrity verification performance, security reliability, and tamper resistance. These metrics were selected to measure the blockchain's ability to maintain accurate, secure, and trustworthy healthcare records while supporting efficient system operations.

The evaluation results demonstrated strong blockchain performance across all measured areas. The system achieved a transaction latency of 0.47 seconds, indicating efficient processing and validation of healthcare transactions. A throughput of 192 transactions per second (TPS) confirmed the capability of the blockchain network to handle a substantial volume of activities without significant delays. In addition, the blockchain achieved a consensus success rate of 99.4%, reflecting reliable agreement among participating nodes during transaction validation. The data integrity verification rate of 99.8% further demonstrated the blockchain's effectiveness in preserving the accuracy and authenticity of healthcare records. Overall, these findings confirm that the blockchain model provides a secure, reliable, and tamper-resistant mechanism for protecting healthcare data against unauthorized modification.

Table 5: Blockchain Performance Results

Metric	Result
Transaction Latency	0.47 sec
Throughput	192 TPS
Consensus Success Rate	99.4%
Data Integrity Verification Rate	99.8%

6.4 Security Evaluation

The integrated model was evaluated against various cyber threat scenarios, including unauthorized access attempts, data tampering, credential compromise attacks, replay attacks, and insider threats. The results presented in Tables 6–10 indicate that the model achieved high detection accuracy, low false positive rates, and efficient response times, demonstrating its effectiveness in protecting wearable healthcare systems. The security audit results further confirmed strong performance in unauthorized access prevention, authentication, data integrity protection, and access control compliance. Attack simulation outcomes showed a significant reduction in successful attacks compared to existing models, while the comparative evaluation demonstrated that the model outperformed traditional access control, IDS-based, blockchain-only, and AI-based approaches. Stakeholder evaluation also revealed positive perceptions regarding security effectiveness, system reliability, trust, compliance, and overall achievement of the model's objectives. Overall, the findings demonstrate substantial improvements in cyber threat detection and mitigation capabilities.

Table 6: Quantitative Security Performance Results

Metric	Result
Detection Accuracy	97.1%
False Positive Rate	3.2%
Average Detection Latency	0.58 sec
Average Encryption Time	0.39 sec

Table 7: Security Audit Results

Security Indicator	Successful Tests	Total Tests	Result
Unauthorized Access Prevention	989	1000	98.9%
Authentication Success Rate	991	1000	99.1%
Data Integrity Protection	996	1000	99.6%
Access Control Compliance	987	1000	98.7%

Table 8: Security Attack Simulation Results

Attack Type	Existing Model (Successful Attacks)	Model (Successful Attacks)
Spoofing Attack	37/100	4/100
Data Tampering	32/100	2/100
Unauthorized Access	28/100	1/100
Replay Attack	24/100	3/100
Ransomware Impact	35/100	5/100

Table 9: Comparative Evaluation Results

Model	Accuracy	FPR	Detection Rate
Traditional Access Control Model	83.4%	11.8%	81.5%
IDS-Based Model	88.6%	8.2%	86.7%
Blockchain-Only Model	91.2%	6.3%	89.5%
AI-Based Model	94.1%	4.7%	92.8%
Adaptive Cybersecurity Model	97.1%	3.2%	97.4%

Table 10: Summary of Stakeholder Evaluation Results

Evaluation Dimension	Strongly Disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly Agree (%)	Positive Response (%)	Mean Score
Security Effectiveness	2.0	4.0	6.0	38.0	50.0	88.0	4.30
System Effectiveness	1.0	5.0	8.0	41.0	45.0	86.0	4.24
User Satisfaction	3.0	6.0	10.0	39.0	42.0	81.0	4.11
Stakeholder Trust	2.0	4.0	9.0	40.0	45.0	85.0	4.22
IoMT Interoperability	3.0	5.0	10.0	42.0	40.0	82.0	4.11
Regulatory Compliance	1.0	4.0	11.0	43.0	41.0	84.0	4.19
Implementation Feasibility	2.0	5.0	10.0	40.0	43.0	83.0	4.17
Overall Goal Achievement	1.0	3.0	8.0	42.0	46.0	88.0	4.29

Positive Response (%) = Agree (%) + Strongly Agree (%). Mean Score calculated using the 5-point Likert scale: Strongly Disagree = 1, Disagree = 2, Neutral = 3, Agree = 4, Strongly Agree = 5.

The results demonstrated significant improvements in threat identification and mitigation capabilities.

7. Discussion

The findings indicate that integrating MLNN with blockchain technology provides complementary cybersecurity capabilities for wearable healthcare systems. While the MLNN continuously analyses communication patterns to identify abnormal activities, blockchain secures validated healthcare transactions through decentralized verification and immutable record management. The integration of these technologies creates multiple layers of protection that strengthen confidentiality, integrity, and accountability throughout the healthcare data lifecycle. The effectiveness of the MLNN can be attributed to its ability to learn complex behavioural patterns from healthcare communication data rather than relying solely on predefined attack signatures. This adaptive learning capability enables the model to detect both known and emerging cyber threats, making it more suitable for wearable healthcare environments where attack techniques continually evolve. Unlike conventional security mechanisms that primarily react to previously identified threats, the MLNN supports proactive threat identification by recognising deviations from normal system behaviour.

The blockchain component further enhances cybersecurity by ensuring that healthcare records remain transparent, traceable, and resistant to unauthorized modification. This complements the anomaly detection process by

protecting validated healthcare transactions after potential threats have been identified. The integration therefore addresses two critical cybersecurity requirements simultaneously: intelligent threat detection and secure data management. These findings are consistent with previous studies [6], which reported that neural-network-based approaches improve anomaly detection through adaptive learning capabilities. Similarly, machine learning techniques have been shown to provide better protection against evolving cyber threats than conventional rule-based security systems [2]. However, the present study extends previous research by integrating MLNN with blockchain technology within a single cybersecurity model designed specifically for wearable healthcare systems.

The blockchain findings also support earlier studies [1], which demonstrated that decentralized ledger technology improves healthcare data integrity and auditability. Similar observations were reported in [12], where combining blockchain with artificial intelligence strengthened trust and security within healthcare environments. The present study reinforces these observations by showing that blockchain not only protects healthcare records but also complements intelligent anomaly detection to provide a more comprehensive cybersecurity solution. The study also demonstrates the importance of adopting integrated cybersecurity strategies for Internet of Medical Things (IoMT) environments. Wearable healthcare systems generate continuous streams of sensitive patient information that require both real-time threat detection and secure data protection. Combining MLNN with blockchain addresses these requirements within a unified security architecture, suggesting that layered cybersecurity approaches are more appropriate for modern healthcare environments than relying on individual security mechanisms alone.

8. Limitations of the Study

Although the model demonstrated strong cybersecurity performance, several limitations should be acknowledged. The evaluation was conducted using a prototype implementation within a controlled wearable healthcare environment rather than a large-scale deployment in operational healthcare institutions. Consequently, the reported performance may differ under real-world conditions involving larger patient populations, heterogeneous wearable devices, and more complex healthcare infrastructures. The experimental evaluation relied primarily on healthcare communication datasets and simulated cyberattack scenarios. Although these datasets provided suitable conditions for evaluating the MLNN and blockchain components, they may not fully represent the diversity and complexity of cyber threats encountered in real healthcare environments.

The study focused on integrating Multi-Layer Neural Networks with blockchain technology and did not compare its performance with newer deep learning architectures such as Graph Neural Networks, Transformer-based models, or Federated Learning approaches. Future research could investigate whether these techniques further improve cybersecurity performance. The blockchain evaluation concentrated mainly on transaction validation, consensus performance, and data integrity verification. Other practical considerations, including long-term scalability, storage overhead, energy consumption, and deployment costs, were beyond the scope of this study and should be examined in future research. Despite these limitations, the findings indicate that the integrated MLNN-blockchain model provides a practical approach for strengthening cybersecurity in wearable healthcare systems.

9. Conclusion

This study presented an integrated cybersecurity model combining Multi-Layer Neural Network (MLNN)-based anomaly detection with blockchain-enabled security for wearable healthcare systems. Experimental evaluation demonstrated that the model effectively detected cyber threats while maintaining high levels of data integrity, transaction security, and system reliability. The MLNN achieved an accuracy of 97.1%, precision of 96.8%, recall of 97.4%, an F1-score of 97.1%, and an ROC-AUC value of 0.993, while blockchain evaluation demonstrated efficient transaction processing, high consensus reliability, and strong data integrity verification.

The findings indicate that integrating machine learning with blockchain technology provides complementary security capabilities that improve cyber threat detection, reduce successful attacks, and strengthen trust in wearable healthcare environments. Compared with conventional security approaches, the integrated model demonstrated superior detection performance and improved protection against unauthorized access, replay attacks, ransomware, spoofing, and data tampering. The study contributes to healthcare cybersecurity by demonstrating that combining intelligent anomaly detection with decentralized blockchain security creates a practical and scalable solution for protecting sensitive patient information within wearable healthcare systems. Future research should validate the model using real-world hospital deployments, larger healthcare datasets, additional wearable technologies, and emerging artificial intelligence techniques to further improve scalability, interoperability, and cybersecurity resilience.

References

[1] Y. Li, J. Chen, and X. Zhao, "Blockchain-enabled IoMT platforms in eldercare: Pilot deployment and evaluation," Sensors, vol. 23, no. 4, Art. no. 2115, 2023.

[2] M. A. Rahman, M. S. Hossain, and M. F. Alhamid, "Securing smart wearable healthcare systems with machine learning and context-aware intelligence," Future Generation Computer Systems, vol. 119, pp. 169–184, 2021.

[3] K. Bayoumy, M. Elhoseny, and T. Alghamdi, "Enhancing cybersecurity in IoMT systems: A review of challenges and blockchain-based solutions," Journal of Healthcare Informatics Research, vol. 7, no. 1, pp. 23–41, 2023.

[4] M. Sabry, T. Abdelzaher, and M. Zahran, "Security challenges in the Internet of Medical Things: A comprehensive survey," Journal of Medical Systems, vol. 46, no. 4, Art. no. 101, 2022.

[5] M. A. Khan, A. Alzahrani, and W. Iqbal, "AI-based threat detection for wearable healthcare systems: An edge computing perspective," Computers in Biology and Medicine, vol. 147, Art. no. 105731, 2022.

[6] A. Mughaid, S. Ahmed, and M. Zaher, "Real-time threat detection using neural networks in wearable healthcare systems," International Journal of Medical Informatics, vol. 183, Art. no. 105112, 2024.

[7] Y. Zhang, R. Zhang, and J. Huang, "Deep learning-based anomaly detection for Internet of Medical Things applications," Journal of Biomedical Informatics, vol. 113, Art. no. 103653, 2021.

[8] A. Javed and H. Afzal, "Tri-layer neural architecture for securing smart healthcare environments," IEEE Access, vol. 11, pp. 54321–54336, 2023.

[9] A. Mughaid, I. Obeidat, L. Abualigah, S. Alzubi, M. S. Daoud, and H. Migdady, "Intelligent cybersecurity approach for data protection in cloud computing based Internet of Things," International Journal of Information Security, vol. 23, no. 3, pp. 2123–2137, 2024.

[10] A. Mughaid, A. Al-Rahayfeh, I. Almomani, and M. Jarrah, "Securing IoMT systems using blockchain and deep learning: A comprehensive review," Health Information Science and Systems, vol. 12, no. 1, pp. 1–12, 2024.

[11] A. Mughaid, A. Al-Mazroei, and M. Othman, "Penetration testing and AI-driven anomaly detection for IoMT security: A comprehensive empirical study," Computers & Security, vol. 119, Art. no. 102918, 2024.

[12] R. Kumar and A. Singh, "Hybrid edge-blockchain-AI model for secure and low-latency wearable health monitoring," Journal of Medical Systems, vol. 48, no. 2, Art. no. 156, 2024.

[13] C. Shah, N. U. I. Hossain, M. M. Khan, and S. T. Alam, "A dynamic Bayesian network model for resilience assessment in blockchain-based Internet of Medical Things with time variation," Healthcare Analytics, vol. 4, Art. no. 100280, 2023.