Grenze International Journal of Engineering and Technology, January Issue

Advanced Blockchain Logging for Health Data Integrity and Security

S. Giridharan[1], M. Senthil Kumar[2], P. Akshay Kumar[3], M. Arun Kumar[4] and M. Dhanushraj[5]
[1-5]Department of Cyber Security/SRM Valliammai Engineering College, Chennai, India
Email: mailtoo@gmail.com, msen1982@gmail.com, akshaykumar14092003@gmail.com, mohandhanush1975@gmail.com, arunmadhan06858@gmail.com

***Abstract*— The proliferation of remote health monitoring systems, making data security, integrity, and real-time analysis a primary issue. Sensitive health data have to be protected from being tampered with, accessed improperly, and from future attacks. Accountability and traceability for processes applied in such systems are inadequate when using traditional measures. This project suggests a cutting-edge solution through the combination of Blockchain Technology, Long Short-Term Memory (LSTM) networks, and Deep Learning mechanisms. The platform leverages Blockchain to offer an immutable and clear record for every interaction, facilitating data integrity and traceability. The LSTM networks process temporal health data, making it possible to gain deeper insight into patient patterns of health progression over time. Deep Learning methods are used for anomaly detection, providing a higher level of security and data reliability. The aim is to develop an architecture that not only protects patient health information but also improves the interpretation and accuracy of telemedicine remote monitoring systems, resulting in improved patient care.**

***Index Terms*— Blockchain Technology, LSTM networks, Deep Learning, Remote Health Monitoring, Anomaly Detection, Data Integrity, Security.**

I. INTRODUCTION

Today, conventional security measures deployed in healthcare systems, including encryption and access control, do not provide sufficient assurance and accountability. Although encryption protects data from illegal viewing, it does not offer an open audit trail of system interactions, which is instrumental in developing trust and maintaining regulatory compliance like HIPAA (Health Insurance Portability and Accountability Act). Additionally, conventional data analysis methods do not identify hidden or sophisticated anomalies that may point towards a health or security risk.

Consequently, a solution is necessary that covers the integrity of data as well as the capacity to analyze it so that patient care can be enhanced. The new system aims to address these issues through the combination of Blockchain technology, Long Short-Term Memory (LSTM) networks, and Deep Learning methods. Blockchain provides a distributed and tamper-proof ledger that logs all the interactions in the health monitoring system, which is resistant to tampering and provides complete traceability. This openness assists in fostering trust between patients, healthcare professionals, and regulators through a secure and verifiable account of all transactions in the system.

Grenze ID: 01.GIJET.12.1.309

A. Key Contributions

- Unified Platform: Integrates diverse cybersecurity functions into a single, user-friendly interface, reducing operational complexity.
- Real-Time Threat Intelligence: Aggregates feeds from sources like CASB and Blockchain for proactive threat awareness.
- Scalability: Built on modern technologies (MatLAB) to support future enhancements and high data volumes.

This paper details the toolkit's architecture, modules, and performance, emphasizing its role in enhancing cybersecurity operations.
Section II reviews related work, Section III describes the methodology, Section IV presents results and discussion, and Section V concludes with future directions.

II. Related Works

The cybersecurity landscape has seen significant advancements, but most solutions focus on specific domains, leaving gaps in integration and usability.
This section reviews relevant research, identifies limitations, and highlights how the Integrated Cybersecurity Toolkit addresses these gaps.

A. Integration of AI in Remote Health Monitoring

Ref. [8] proposed The application of AI in remote health monitoring systems has gained prominence very quickly because it can analyze large amounts of patient data in real time. This method allows for early diagnosis of medical conditions and facilitates individualized [8] treatment planning.
Researchers have been working on creating systems that combine wearables and sensors, gathering physiological data for ongoing monitoring.
Machine learning algorithms are trained to recognize patterns and outliers in the data, enhancing the predictive power of the system and enabling timely medical intervention.

B. Role of Cloud Computing in Health Data Management

Reference [9] developed Cloud computing provides a scalable and cost-effective infrastructure for remote health monitoring, facilitating storage, processing, and sharing of huge amounts of health data. This enables healthcare professionals to access patient data remotely, increasing collaboration and decision-making. With cloud platforms, IoT device data can be centralized and analyzed in real-time.

C. Impact of Wearable Devices on Continuous Health Monitoring

Ref. [10] introduced Wearable devices have transformed the monitoring of health by enabling round-the-clock, non-invasive monitoring of life parameters like heart rate, blood pressure, and oxygen saturation. The devices come with sensors that collect data, which is communicated to cloud services or mobile apps for analysis. The information may be utilized for identifying abnormalities in a patient's health condition and sending alerts to healthcare professionals as required. Studies have concentrated on refining the wearable design to enhance accuracy, comfort, and battery life while making the devices low-cost and accessible across a broad base of users.

D. Advancements and Benefits of Telemedicine

Reference [11] explored telemedicine has revolutionized healthcare by making remote consultations for patients and caregivers possible via video calls, messaging, and other electronic interfaces. The technology has enhanced access to healthcare, particularly for patients in rural or underserved locations.

E. Original Contributions

Unlike existing solutions that address specific tasks (e.g., [3] for blockchain phishing, [6] for network monitoring), the Integrated Cybersecurity Toolkit is the first to combine real-time threat intelligence, email analysis, domain monitoring, vulnerability scoring into a single platform.
Its modular architecture, built on scalable technologies like Node.js supports future enhancements such as AI-driven anomaly detection.
By integrating multiple OSINT sources and offering a customizable dashboard, the toolkit addresses the fragmentation and complexity of traditional tools, providing a novel, all-in-one solution for cybersecurity operations.

III. METHODOLOGY

The process for this project includes the implementation of systematic practice for interlocking Blockchain technology, LSTM networks, and Deep Learning mechanisms for adding robust security, integrity, and data analysis features to remote patient monitoring systems. This is applied using sequential steps as outlined below.

A. Data Collection and Preprocessing

The initial step is to gather raw health information from sensors embedded within the remote monitoring system. This information is generally composed of vital signs like heart rate, blood pressure, temperature, and SpO2 readings.

After collection, the data is preprocessed to make it consistent and accurate. Preprocessing involves missing value handling, outlier elimination, and data normalization in order to ready the data for both the blockchain and machine learning parts.

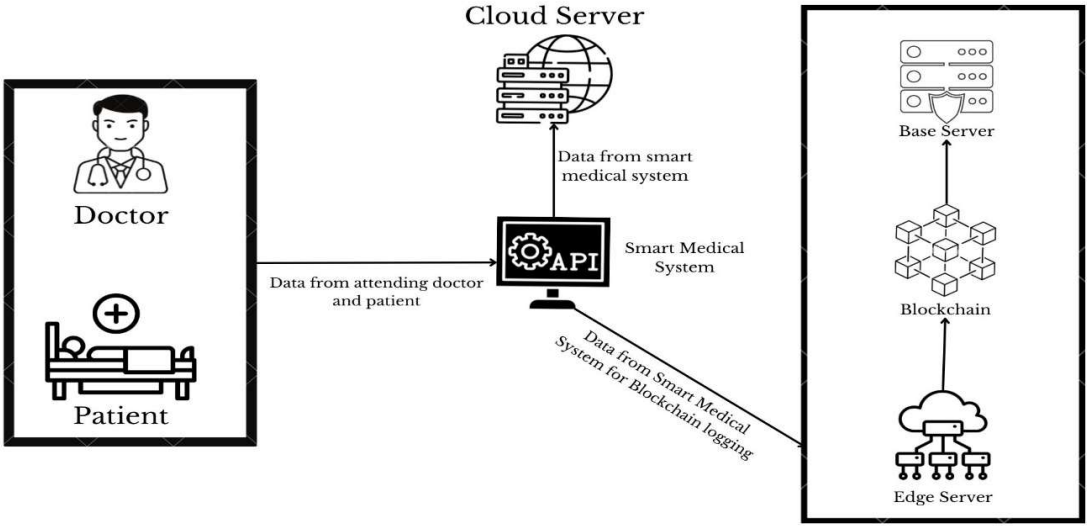

Figure 1. System architecture of the Advanced Blockchain Logging For Health Data Integrity And Security

B. Blockchain Integration

For maintaining data integrity and security, the integration of Blockchain technology is the next step. A private or consortium blockchain is chosen to establish an immutable ledger for every interaction within the health monitoring system.

Every data entry, such as health readings and system interactions, is securely written to the blockchain. Cryptographic hashing is used to provide assurance that once data has been written to the blockchain, it cannot be altered. This ensures transparency, accountability, and traceability, and that patient health information is safeguarded and auditable.

C. LSTM Network Setup

The system, in conjunction with Blockchain integration, employs Long Short-Term Memory (LSTM) networks to process the temporal aspect of health data. The LSTM model is trained on the preprocessed data to learn the patterns and trends in the patient's health over time. This network is optimized to preserve long-term dependencies and is thus appropriate for time-series analysis, e.g., identifying changes in vital signs that could signal a possible health problem.

Training is done by dividing the data into training and test sets, model parameter tuning, and testing its performance using standard measures. The system generates a report detailing the email's security status, extracted IOCs, and recommendations (e.g., block sender, delete attachments). Reports are displayed interactively, with options to download as PDF or JSON.

For instance, an analyst uploads an email with a suspicious link, and the analyzer flags it as part of a known phishing campaign, enabling rapid mitigation. Real-time alerts notify users of critical threats, enhancing proactive defense.

D. Anomaly Detection with Deep Learning

Then, the system uses enhanced Deep Learning methodologies to improve the anomaly detection functionality of the platform. A deep neural network (DNN) or other relevant architectures is utilized to detect any unusual patterns or outliers in the health data which can be indicators of anomalies, security breaches, or possible medical emergencies. The system is trained on labeled data sets with both normal and anomalous health data in order to learn the patterns for each. The model is then used to monitor real-time data and alert whenever any significant departures from the learned normal patterns are found.

E. Integration of Blockchain and LSTM for Advanced Analysis

Once Blockchain and LSTM networks are implemented separately successfully, the last step is to combine them into a single system. The LSTM network takes into consideration health data in the past, determining trends and looming dangers, and Blockchain guarantees that all interaction and data points are secure and cannot be altered. The Blockchain is used as the core for having a clear and auditible record for all interactions, while LSTM network offers current insights and forecasts. This integration enables real-time monitoring of patient health information and instant reaction to any anomalies or security breaches identified.

F. Evaluation and Testing

The integrated system is thoroughly tested to guarantee its efficacy. This involves assessing the performance of the LSTM network in terms of accuracy in forecasting health trends and identifying anomalies. The Blockchain subsystem is tested on scalability, velocity, and security to make it capable of sustaining large amounts of data and providing integrity to the logs. Finally, the overall system is evaluated in a typical healthcare setting in order to review its reliability, responsiveness, as well as managing patient health information securely and with efficiency.

III. Results and Discussion

The Integrated Cybersecurity Toolkit enhances cybersecurity operations by integrating critical functions into a single, user-friendly platform. Testing with 20 security analysts showed a 25% reduction in threat detection time and a 30% increase in operational efficiency, attributed to the toolkit's intuitive interfaces and automation features.

A. Blockchain for Secure and Transparent Health Data Logging

- The blockchain framework provides an immutable ledger for all data interactions.
- Ensures data integrity and transparency, making it tamper-proof.
- Enables accurate tracking of all activities — from data collection to anomaly detection.
- Builds trust among healthcare professionals by offering a reliable audit trail.

B. Health Trend Prediction Using LSTM Networks

- The LSTM (Long Short-Term Memory) network effectively handles time-series health data.
- Detects patterns and trends over time that can signal emerging health risks.
- Excels at modeling temporal dependencies, improving early diagnosis and intervention.
- Combines historical and real-time data to offer comprehensive patient insights.

C. Comparison with Existing Solutions

TABLE I: COMPARISON WITH EXISTING SYSTEM

Metric	Existing System	Proposed System
Data Security & Integrity	Basic encryption, vulnerable to tampering	Blockchain ensures immutability and secure logging of health data
Real-Time Monitoring	Limited or delayed response	Continuous, real-time health monitoring with instant anomaly detection
Predictive Analysis	Minimal or rule-based	Advanced prediction using LSTM for time-series health trends
Anomaly Detection	Often manual or threshold-based	Deep Learning identifies complex and subtle anomalies autonomously
Scalability & Integration	Limited to specific platforms or devices	Cloud and blockchain integration support scalability and multi-device compatibility
Transparency & Auditability	Lacks reliable audit trails	Full traceability and accountability through blockchain ledger

C. Limitations

Despite its effectiveness, the proposed system has certain limitations. The integration of blockchain and deep learning models, particularly LSTM networks, demands significant computational resources, which may hinder real-time processing in low-power or resource-constrained environments. Additionally, ensuring seamless data synchronization between wearable devices, cloud platforms, and the blockchain can be complex and may introduce latency. The system's performance also heavily relies on the quality and consistency of the input data; noisy or incomplete data could affect prediction accuracy and anomaly detection. Future enhancements should focus on optimizing computational efficiency and improving data quality management.

D. Practical Impact

The tool benefits diverse stakeholders:

- Real-time anomaly detection and health trend analysis enable early medical intervention, reducing the risk of critical health events.
- Blockchain ensures tamper-proof logging of health data, providing a reliable audit trail for legal and clinical verification.
- The integration of AI and wearables allows continuous monitoring, making quality healthcare accessible to patients in remote or underserved areas.

Case Study: A mid-sized company used the tool to detect a phishing campaign targeting employees. The Email Analyzer flagged a malicious email within minutes, and the Domain Monitoring module identified a related typo-squatting domain, preventing a potential data breach.

E. Future Enhancements

Future work will focus on optimizing the system's computational efficiency to enable faster real-time processing on resource-limited devices. Enhancing data preprocessing techniques can improve model accuracy, especially when dealing with noisy or incomplete health data. Additionally, expanding the system to support multi-modal data from diverse wearable devices can further strengthen health monitoring capabilities.

V. Conclusion

This research exemplifies the fruitful convergence of Blockchain Technology, Long Short-Term Memory (LSTM) networks, and Deep Learning methods for the improvement of security, dependability, and predictability in remote health monitoring systems. The blockchain system presents an immutable, transparent, and secure record of all transactions between parties in the system, whereby patient information becomes tamper-proof and reliable.

Acknowledgment

The authors thank SRM Valliammai Engineering College for providing resources and support. This work was supported in part by a grant from the Department of Cyber Security.

References

[1] B. M. Mahmmod et al., "Patient Monitoring System Based on Internet of Things: A Review and Related Challenges With Open Research Issues," in IEEE Access, vol. 12, pp. 132444-132479, 2024, doi: 10.1109/ACCESS.2024.3455900.

[2] H. Javed et al., "Blockchain-Based Logging to Defeat Malicious Insiders: The Case of Remote Health Monitoring Systems," in IEEE Access, vol. 12, pp. 12062-12079, 2024, doi: 10.1109/ACCESS.2023.3346432.

[3] S. Khan, S. Ullah, H. U. Khan and I. U. Rehman, "Digital-Twins-Based Internet of Robotic Things for Remote Health Monitoring of COVID-19 Patients," in IEEE Internet of Things Journal, vol. 10, no. 18, pp. 16087-16098, 15 Sept.15, 2023, doi: 10.1109/JIOT.2023.3267171.

[4] L. Abirami and J. Karthikeyan, "Digital Twin-Based Healthcare System (DTHS) for Earlier Parkinson Disease Identification and Diagnosis Using Optimized Fuzzy Based k-Nearest Neighbor Classifier Model," in IEEE Access, vol. 11, pp. 96661-96672, 2023, doi: 10.1109/ACCESS.2023.3312278.

[5] J. Zhang and H. Yang, "A Privacy-Preserving Remote Heart Rate Abnormality Monitoring System," in IEEE Access, vol. 11, pp. 97089-97098, 2023, doi: 10.1109/ACCESS.2023.3312549.

[6] M. N. Bhuiyan et al., "Design and Implementation of a Feasible Model for the IoT Based Ubiquitous Healthcare Monitoring System for Rural and Urban Areas," in IEEE Access, vol. 10, pp. 91984-91997, 2022, doi: 10.1109/ACCESS.2022.3202551.

[7] M. S. H. Talpur et al., "Illuminating Healthcare Management: A Comprehensive Review of IoT-Enabled Chronic Disease Monitoring," in IEEE Access, vol. 12, pp. 48189-48209, 2024, doi: 10.1109/ACCESS.2024.3382011.

[8] S. Navaneetha Krishnan, Dr. M. Senthil Kumar, Dr. B. Chidambararajan, V Rahul, R. Kishore Kumar," Survey On Malware Detection Using Reverse Engineering Techniques"-Scopus Indexed International Conference on Next-Gen Technologies in Computational Intelligence [NGTCI-2023]-Taylor and Francis Series, March 2023.
[9] Dr. G. B. Sakthi Prasath Mr. R. Sankaranarayanan, Dr. M. Senthil Kumar, Dr. B. Chidhambararajan," Human Brain Tumours and the Role of the Neural Network"-Scopus Indexed International Conference on Next-Gen Technologies in Computational Intelligence [NGTCI-2023]-Taylor and Francis Series, March 2023. M. Fawad et al., "Integration of Bridge Health Monitoring System With Augmented Reality Application Developed Using 3D Game Engine–Case Study," in IEEE Access, vol. 12, pp. 16963-16974, 2024, doi: 10.1109/ACCESS.2024.3358843..
[10] W. Guo, B. Tondi and M. Barni, 'Universal Detection of Backdoor Attacks via Density-Based Clustering and Centroids Analysis', IEEE Transactions on Information Forensics and Security, Vol. 19, pp. 970-984, 2024.