IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2025

DOI: 10.17148/IJIREEICE.2025.134114

BLOCKCHAIN-BASED LOGGING TO DEFEAT MALICIOUS INSIDERS: THE CASE OF REMOTE HEALTH MONITORING SYSTEMS

Kasi Sailaja[1], Mudavath Chandi Priya (22WJ5A0522) [2], Md Kareemoddin (22WJ5A0519) [3], Sai Pratham Reddy (21WJ1A05T1) [4], Dr. Mahesh Kotha[5]

Assistant Professor, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad[1]

B. Tech IV Year, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad[2-4]

Associate professor, Department of CSE (AI&ML), CMR Technical Campus Hyderabad[5]

Abstract: This project aims to enhance the security and functionality of hospital management systems by implementing robust encryption techniques and access control mechanisms. The system allows the addition of doctors, who are required to obtain permission from the hospital before being granted access. Only authorized doctors are permitted to interact with patient data, ensuring that sensitive medical information remains secure. To protect patient data, the system includes an authentication process where user IDs and passwords are verified. If a mismatch occurs, the system detects and flags the access attempt as coming from a malicious user. The system also allows doctors to view patient details and send prescriptions, ensuring a smooth workflow for healthcare providers. Furthermore, medical staff can add and manage medicines within the system. To safeguard sensitive information, the project integrates the use of SHA-256 (Secure Hash Algorithm) and AES (Advanced Encryption Standard) encryption algorithms. These encryption methods ensure that all user data, patient records, and prescriptions are securely encrypted before being transmitted or stored, preventing unauthorized access and ensuring the privacy of all users.

Keywords: Insider attack, private blockchain, cloud access security broker, remote health.

I.INTRODUCTION

The advent of Remote Health Monitoring Systems (RHMS) has ushered in a new era in healthcare delivery, allowing continuous monitoring of patients outside traditional clinical settings. Despite their benefits, RHMS face significant security challenges, particularly from malicious insiders who can manipulate logs to conceal unauthorized activities or data breaches. Traditional logging mechanisms, often centralized and opaque, are insufficient to guarantee trust in such sensitive environments.

Blockchain technology, known for its decentralized, immutable, and transparent characteristics, offers a promising solution for securing audit logs against insider attacks. This paper explores the integration of blockchain technology into RHMS logging infrastructures to ensure integrity, traceability, and accountability.

Many people have hectic schedules that make it difficult to have regular exams, particularly for chronic diseases like diabetes and hypertension. Certain individuals, such as the old and frail, or those suffering from motion sickness, light sensitivity, or social anxiety, may have medical conditions that limit their mobility. There is now more fear of getting the virus or other diseases due to the recent Covid-19 pandemic. Smart IoT devices for remote health monitoring may be able to assist those who are unable or unwilling to make routine doctor's appointments. Monitoring of health IoT devices pair with a smartphone app to exchange patient health information and get recommendations from medical professionals. Because health data is sensitive and there are strict security standards in this field, a remote health monitoring system needs to protect user health data at every turn.

DOI: 10.17148/IJIREEICE.2025.134114

Ongoing system activity audits are the answer to detecting insider threats. Log data is used to record user activity together with timestamps for auditing purposes. But altering the log data itself is a problem. After gaining unauthorized access to patient health data, malicious administrators with log access can alter log data to hide their footprints. This issue requires an immutable logging system to be resolved. An inherent remedy for immutability is provided by blockchains. The blockchain is a distributed, decentralized ledger that cannot be altered. It is made up of many blocks that hold information on timestamp-based transactions. The hash of the previous block is kept in the header of each block. The Genesis block, the initial block in each blockchain, is devoid of any hash from the preceding blockchain. We contend that the mere fact that logs are accessible to a large number of users will deter insider attacks because blockchain records are permanent, even though this strategy has the flaw that users are not always tech-savvy or responsible enough to regularly monitor their data. If an insider is successful in a data breach, the data owner or an outside observer, such a regulatory agency, can quickly track down what they did using the tracking ID of the data item.lthough we plan to enhance this strategy in the future by integrating the system with an automatic intrusion detection system that examines logs and notifies users of anomalies, we currently think the system is strong enough to prevent insider attacks.

II.RELATED WORKS

IoT-based remote health monitoring is a promising technology to support patients who are unable to travel to medical facilities. Due to the sensitivity of health data, it is important to secure it against all possible threats. While a great deal of work has been done to secure IoT device-cloud communication and health records on the cloud, insider attacks remain a significant challenge. Malicious insiders may tamper, steal or change patients' health data, which results in a loss of patient trust in these systems. Audit logs in the cloud, which may point to illegal data access, may also be erased or forged by malicious insiders as they tend to have technical knowledge and privileged access to the system.

A private blockchain that immediately logs all actions happening in the backend of the web application and CASB. We evaluate the system's security and performance under varying numbers of patients and actions. the web application also receives data retrieval requests and passes them to the CASB to process according to its access control policies, which in turn passes the data back to the web application. Each action of the web application backend and the CASB, whether it is related to data storage or retrieval, is logged immediately into a private blockchain. To be effective at detecting insider attacks, logging systems usually need to be monitored, i.e., someone needs to continuously read the logs and identify when illegal access has occurred. In our case, we would define illegal access as an action performed on user data that is not directly or indirectly initiated by the user. For example, if a doctor updates a patient's record and the patient approves it for upload into the system, the data will be encrypted, indexed, and stored in the cloud.

Recent studies have explored blockchain applications in healthcare for data sharing, consent management, and EHR integrity. However, specific focus on insider-resistant logging for RHMS is sparse. Some notable works include:

- **MedRec (MIT, 2016):** Blockchain-based medical record management system.
- **GuardHealth:** Blockchain-enabled health data sharing with access control.

Existing solutions primarily address data sharing and access control, not audit logging under insider threat scenarios.

III.LITERATURE SURVEY

The integration of Remote Health Monitoring Systems (RHMS) with healthcare delivery has raised significant security concerns, particularly concerning insider threats. Traditional centralized logging systems are vulnerable to manipulation by insiders. Blockchain technology, with its properties of decentralization, immutability, and transparency, presents a promising solution to enhance log security. This literature survey explores the research landscape on blockchain-based logging approaches, their application in healthcare, and strategies to mitigate insider threats.

MedRec (Ekblaw et al., 2016): Introduced a blockchain-based solution for managing Electronic Health Records (EHRs) with decentralized access control. MedRec uses blockchain primarily for record access tracking rather than fine-grained event logging.

Limitations: High transaction costs and scalability concerns.

DOI: 10.17148/IJIREEICE.2025.134114

GuardHealth (Zhou et al., 2020): Developed a blockchain-enabled architecture for secure health data sharing across institutions. Smart contracts enforce patient-consent policies.

Insight: Emphasizes secure data sharing but lacks detailed discussion on logging internal activities.

FHIRChain (Zhang et al., 2018): Proposes using blockchain for secure sharing of clinical data following HL7 FHIR standards. Focuses on access control and patient consent rather than tamper-proof logs.

Scholz et al. (2020): Presented a blockchain-secured logging approach to ensure that logs are tamper-proof and verifiable. Their work highlights the advantages of using a permissioned blockchain network for audit trails in corporate environments.

Xu et al. (2019): Explored using hash chains and blockchain to secure system event logs against insider modifications. Introduced lightweight methods for frequent log entries, preserving performance.

Yang et al. (2020): Proposed a smart contract-based logging framework where every critical event triggers an on-chain transaction.

Challenge: High-frequency logs can result in blockchain congestion without careful design.

NIST Special Publication 800-53 (2013): Classifies insiders as significant threats capable of accessing sensitive data due to their legitimate privileges. Healthcare environments are particularly vulnerable due to complex access requirements.

While blockchain technology significantly strengthens logging mechanisms against insider threats, especially in sensitive systems like RHMS, practical deployment requires careful consideration of performance and privacy challenges. Future research directions should focus on optimizing blockchain-based logging architectures tailored specifically to healthcare environments, integrating privacy-preserving techniques, and ensuring compliance with legal and ethical standards.

Study	Objective	Blockchain Platform	Consensus Mechanism	Key Contributions
Javed et al. 2024	Develop a blockchain-based logging system to counter insider threats in RHMS	Solana	Proof of History (PoH)	Proposed a tamper-evident logging mechanism enhancing data integrity and traceability in RHMS.
Secure Data Sharing Review, 2023	Review blockchain applications for secure data sharing in RHM	Ethereum, Hyperledger Fabric	Varies	Systematic analysis of blockchain's role in enhancing data security and privacy in RHM applications.
Springer Review on Blockchain in RHM, 2023	Examine blockchain integration in RHM focusing on security and privacy	Ethereum, Hyperledger Fabric, Holochain	PBFT, PoW	Discussed smart contracts, consensus mechanisms, and challenges like latency and scalability in blockchain-based RHM.
2020	Propose a blockchain traceability system for insider threat detection	Not specified	Not specified	Introduced a system enhancing traceability and accountability to detect and prevent insider attacks.
Blockchain-Enabled Remote Healthcare Monitoring, 2023	Design a secure blockchain-based remote healthcare monitoring system	Private Blockchain	Not specified	Developed a system integrating blockchain for secure data transmission and storage in home isolation scenarios.
Blockchain-Based Privacy and Security in E-Health, 2022	Systematic review of blockchain applications in e-health for privacy and security	Various	Various	Analyzed blockchain features like anonymous signatures and smart contracts to enhance e-health data security.

Blockchain-Enabled Trust Management in Healthcare Smartphone Network, 2023	Introduce a trust management system using blockchain to detect malicious insiders	Not specified	Not specified	Proposed a Cluster-based Hierarchical Trust Management System (CHTMS) to identify and mitigate insider threats.

Table 1. Summary of the surveys.

The above table summarizes key studies focusing on blockchain-based solutions to address insider threats in RHMS. The consensus mechanisms and blockchain platforms vary across studies, reflecting the diversity in approaches to enhance security and privacy in healthcare monitoring systems.

IV.PROPOSED WORK

This paper, we propose a Cloud Access Security Broker (CASB) model that (a) logs every action performed on user data and (b) secures those logs by placing them in a private blockchain that is viewable by the data owners (i.e., patients). Patients can query the blockchain, track their data's movement, and be alerted if their data has been accessed by an administrator or moved outside the cloud storage. In this work, we practically implement a web application that receives health data from patients, a CASB that securely stores the records in the cloud, and integrate a private blockchain that immediately logs all actions happening in the backend of the web application and CASB. We evaluate the system's security and performance under varying numbers of patients and actions.

SHA is a cryptographic hash functions designed to produce a fixed-size output (hash) from input data of any size. The most commonly used SHA algorithms are SHA-256, which produce a 256-bit, respectively.

•Purpose: SHA is used for integrity verification and authentication. In the context of your hospital management system, it can be used to hash passwords or sensitive data before storing them in the database. This ensures that even if the database is compromised, the original data cannot be retrieved without the hash's corresponding salt (a random value added to the password before hashing).

•Process: When a user submits a password, it is passed through the SHA algorithm to generate a hash. This hash is then stored securely, and whenever the user attempts to log in, their input password is hashed again and compared to the stored hash. If the hashes match, the user is authenticated.

AES is a symmetric encryption algorithm widely used to protect sensitive data. It operates on blocks of data and uses keys of fixed sizes (128, 192, or 256 bits).

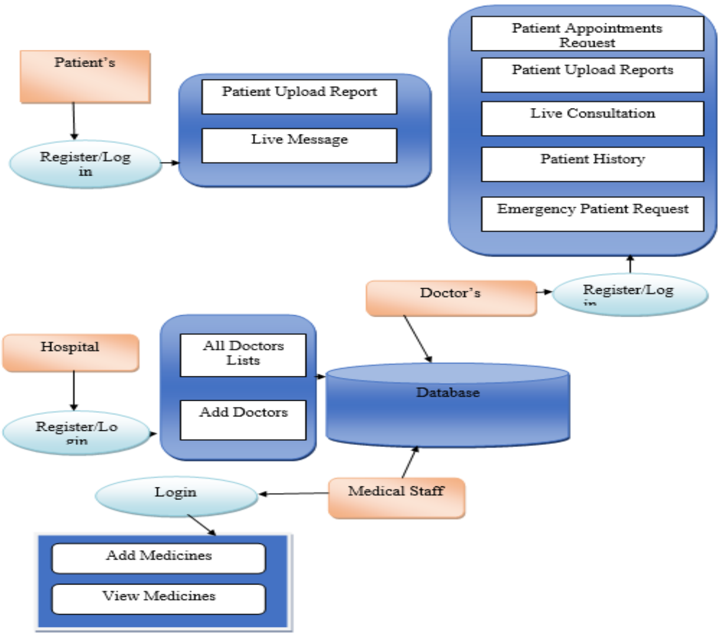


Figure 1. Architecture of the system.

DOI: 10.17148/IJIREEICE.2025.134114

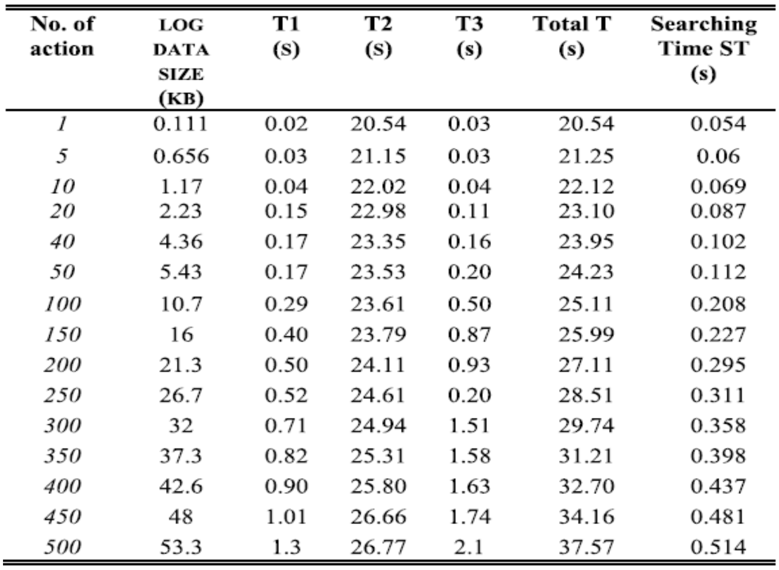
•Purpose: AES is used for encrypting patient data, prescriptions, and other sensitive information within your hospital management system. This ensures that even if the data is intercepted, it remains unreadable without the correct decryption key.

•Process: The system encrypts the data using AES with a secret key before storing or transmitting it. When authorized personnel (e.g., doctors or medical staff) access the data, they use the decryption key to decrypt the information back into its original form. The key management is crucial, and it must be kept secure to maintain the confidentiality of the encrypted data.

In our proposed system, we assume that a patient uses IoT-based wearable devices that continuously measure various health metrics and send data to the cloud. As the health record is very sensitive, it is, therefore, crucial to secure access to the web-based application used by medical practitioners for viewing patient data. Our system implements a CASB to enforce strict access control. Moreover, a blockchain-based log management system is integrated with the CASB to continuously store audit log data, which contains information about each action that was done on a patient's data, indexed by a tracking ID. Logged information includes the IP address and other identifying information of the user who accessed the data item and the time when the user acted.

V. RESULTS AND DISCUSSION

We use the following technology stack for each of the main
components:
• Cloud Storage: For storing patient data generated by IoT devices, we use Google Cloud storage.
• Frontend: The front web application consists of HTML, CSS, and JavaScript programming languages.
For developing the Dapp (Decentralized Application) to display log data, we use React.js, a JavaScript library.



No. of action	LOG DATA SIZE (KB)	T1 (S)	T2 (S)	T3 (s)	Total T (s)	Searching Time ST (s)
1	0.111	0.02	20.54	0.03	20.54	0.054
5	0.656	0.03	21.15	0.03	21.25	0.06
10	1.17	0.04	22.02	0.04	22.12	0.069
20	2.23	0.15	22.98	0.11	23.10	0.087
40	4.36	0.17	23.35	0.16	23.95	0.102
50	5.43	0.17	23.53	0.20	24.23	0.112
100	10.7	0.29	23.61	0.50	25.11	0.208
150	16	0.40	23.79	0.87	25.99	0.227
200	21.3	0.50	24.11	0.93	27.11	0.295
250	26.7	0.52	24.61	0.20	28.51	0.311
300	32	0.71	24.94	1.51	29.74	0.358
350	37.3	0.82	25.31	1.58	31.21	0.398
400	42.6	0.90	25.80	1.63	32.70	0.437
450	48	1.01	26.66	1.74	34.16	0.481
500	53.3	1.3	26.77	2.1	37.57	0.514

Table 2. Time in seconds for storing log data against different log sizes and number of actions.

• Backend: The CASB will be developed using PHP as a backend programming language and smart contract of Ethereum blockchain written in Solidity.
• Blockchain environment: We use Ganache which offers multiple nodes with 100 Ether per node. We may build, test, and release your smart contracts.
Ganache is a desktop application that is compatible with Ethereum and includes an easy-to-navigate user interface.
• Wallet: We use MetaMask wallet to perform blockchain transactions when log data has to be stored.
We evaluated our system using the time to transfer log data to the blockchain, relative to the size of the log. The result is shown in Table 3. At the backend of our own design Cloud Access Security Broker (CASB)-based prototype, we write script (Code) that calculates the time of log action and displays the result in terms of seconds on the front end of the screen. To run the system, we perform different actions like adding, deleting, or viewing patient data in web applications.

DOI: 10.17148/IJIREEICE.2025.134114

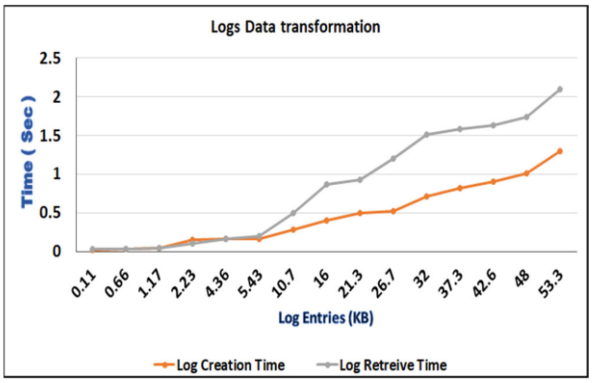


Figure 2. Creation and retrieving of logs data.

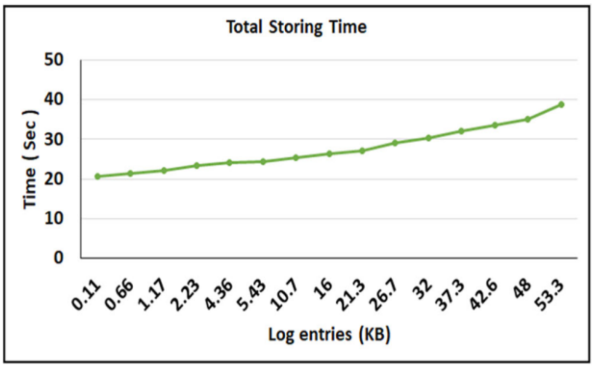


Figure 3. Logs data storing time.

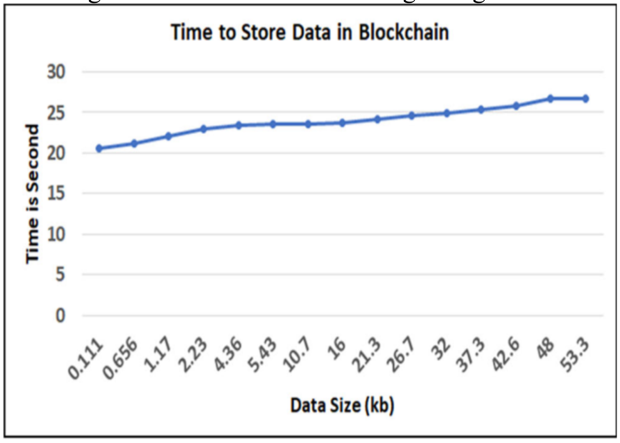


Figure 4. Total storing time of logs data from CASB to blockchain.

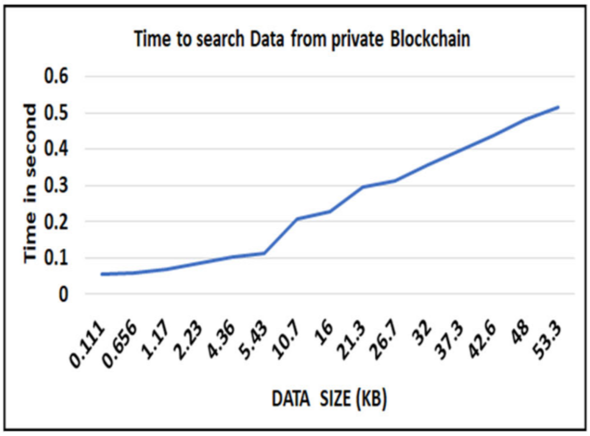


Figure 5. Logs searching time.

The log data will be generated automatically at the backend of the system based on these actions. The log data is then automatically loaded in DAPP and a transaction is performed to store log data in a private blockchain. Each block contains the most recent logs information, such as UserID 6712 doctors viewed the patient record on 2022-08-09 at 19:56:06 where an IP address is 192.172.1.1:30. Also Other important information includes the hash of the previous block, the transaction hash, the block number, the transaction number, the account number that performs the transaction, and the timestamp. The log data will be retrieved from the blockchain and shown in a web application, either as a whole or against a specific search query. We also report the retrieval and search time in our evaluation results. Table 3, shows the results against varying log sizes and number of actions.

VI.CONCLUSION

We have introduced a private blockchain-based system for remote health monitoring that guards against insider threats. The suggested approach provides partial decentralization, distribution, and immutability. A private blockchain that continuously tracks user activity to identify internal threats and the Cloud Access Security Broker (CASB) for managing actual health data make up our system. The blockchain would log and retain every user action, and CASB would offer end-to-end security, encompassing authentication, access control, and storage. However, stealing or tampering with log data is impossible because of the immutability of blockchain. Any user of the system, including auditors, patients, and physicians, can also check their log data using their ID from the blockchain and identify any fraudulent activity by the administrator.

The suggested method will be expanded to manage large log data in the future. Currently, we practically implement and evaluate the performance using a little quantity of data, such as KB or MB, but over time, a big amount of data possibly in GB or TB has been created. Despite this, blockchain does not allow data deletion. Furthermore, our suggested system's fundamental criterion is that no one be able to edit or remove the log data. As a result, we will need any way to compress the growing amount of log data in the blockchain. However, there is no way for the blockchain to compress this data

DOI: 10.17148/IJIREEICE.2025.134114

either. Therefore, the compression process will be possible on the cloud side that compresses every action of the user and stores it in the blockchain also compression does not affect real health data processing.

REFERENCES

[1] H. Javed, Z. Abaid, S. Akbar, M. A. Khan and S. M. Sait, "Blockchain-Based Logging to Defeat Malicious Insiders: The Case of Remote Health Monitoring Systems," Computers in Biology and Medicine, vol. 173, 2024, Art. no. 107888.

[2] Ravindra Changala, "Sustainable Manufacturing through Predictive Maintenance: A Hybrid Jaya Algorithm and Sea Lion Optimization and RNN Model for Industry 4.0", 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), ISSN: 2768-0673, DOI: 10.1109/I-SMAC61858.2024.10714701, October 2024, IEEE Xplore.

[3] Ravindra Changala, "Enhancing Robotic Surgery Precision and Safety Using a Hybrid Autoencoder and Deep Belief Network Approach: Real-Time Feedback and Adaptive Control from Image Data",2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), ISSN: 2768-0673, DOI: 10.1109/I-SMAC61858.2024.10714701, October 2024, IEEE Xplore.

[4] R. Kaur and S. Arora, "Secure Data Sharing with Blockchain for Remote Health Monitoring Applications: A Review," Health and Technology, vol. 13, 2023

[5] Ravindra Changala, "Swarm Intelligence for Multi-Robot Coordination in Agricultural Automation", 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS), ISSN: 2575-7288, DOI: 10.1109/ICACCS60874.2024.10717088, October 2024, IEEE Xplore.

[6] Ravindra Changala, "Hybrid AI Approach Combining Decision Trees and SVM for Intelligent Tutoring Systems in STEM Education", 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS), ISSN: 2575-7288, DOI: 10.1109/ICACCS60874.2024.10717088, October 2024, IEEE Xplore.

[7] S. S. Alsamhi, M. S. Ansari, and N. Srivastava, "Blockchain-Enabled Secure and Efficient Data Sharing Scheme for Trust Management in Healthcare Smartphone Network," Sensors, vol. 23, no. 8, p. 4098, 2023

[8] Ravindra Changala, "Sentiment Analysis in Mobile Language Learning Apps Utilizing LSTM-GRU for Enhanced User Engagement and Personalized Feedback", 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718406, October 2024, IEEE Xplore.

[9] B. Ahmad, M. Kiah, S. Hussain and A. Gani, "A Secure Blockchain-Enabled Remote Healthcare Monitoring System for Home Isolation," Journal of Sensor and Actuator Networks, vol. 13, no. 1, p. 13, 2023.

[10] Ravindra Changala, "Next-Gen Human-Computer Interaction: A Hybrid LSTM-CNN Model for Superior Adaptive User Experience", 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718496, October 2024, IEEE Xplore.

[11] Ravindra Changala, "Enhancing Early Heart Disease Prediction through Optimized CNN-GRU Algorithms: Advanced Techniques and Applications", 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718395, October 2024, IEEE Xplore.

[12] Y. Yuan and F. Wang, "Tracking the Insider Attacker: A Blockchain Traceability System for Insider Threats," IEEE Access, vol. 8, pp. 182338–182348, 2020.

[13] Ravindra Changala, "Image Classification Using Optimized Convolution Neural Network", 2024 Parul International Conference on Engineering and Technology (PICET), ISBN:979-8-3503-6974-8, DOI: 10.1109/PICET60765.2024.10716049, October 2024, IEEE Xplore.

[14] Ravindra Changala, "Sentiment Analysis Optimization Using Hybrid Machine Learning Techniques", 2024 Parul International Conference on Engineering and Technology (PICET), ISBN:979-8-3503-6974-8, DOI: 10.1109/PICET60765.2024.10716049, October 2024, IEEE Xplore.

[15] S. Sengupta, “A secured biometric-based authentication scheme in IoTbased patient monitoring system,” in Emerging Technology in Modelling and Graphics, 2020, pp. 501–518.

[16] Ravindra Changala, "Using Generative Adversarial Networks for Anomaly Detection in Network Traffic: Advancements in AI Cybersecurity", 2024 International Conference on Data Science and Network Security (ICDSNS), ISBN:979-8-3503-7311-0, DOI: 10.1109/ICDSNS62112.2024.10690857, October 2024, IEEE Xplore.

[17] Ravindra Changala, "Advancing Surveillance Systems: Leveraging Sparse Auto Encoder for Enhanced Anomaly Detection in Image Data Security", 2024 International Conference on Data Science and Network Security (ICDSNS), ISBN:979-8-3503-7311-0, DOI: 10.1109/ICDSNS62112.2024.10690857, October 2024, IEEE Xplore.

[18] J. Sun, X. Yao, S. Wang, and Y. Wu, “Blockchain-based secure storage and access scheme for electronic medical records in IPFS,” IEEE Access, vol. 8, pp. 59389–59401, 2020.

DOI: 10.17148/IJIREEICE.2025.134114

[19] Ravindra Changala, "Healthcare Data Management Optimization Using LSTM and GAN-Based Predictive Modeling: Towards Effective Health Service Delivery", 2024 International Conference on Data Science and Network Security (ICDSNS), ISBN:979-8-3503-7311-0, DOI: 10.1109/ICDSNS62112.2024.10690857, October 2024, IEEE Xplore.
[20] Ravindra Changala, "Monte Carlo Tree Search Algorithms for Strategic Planning in Humanoid Robotics", 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS), ISBN:979-8-3503-7274-8, DOI: 10.1109/ICC-ROBINS60238.2024.10533937, May 2024, IEEE Xplore.
[21] (2022). Bitglass CASB. [Online]. Available: https://www.bitglass. com/casb-cloud-access-security-broker.
[22] Ravindra Changala, "Implementing Genetic Algorithms for Optimization in Neuro-Cognitive Rehabilitation Robotics", 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS), ISBN:979-8-3503-7274-8, DOI: 10.1109/ICC-ROBINS60238.2024.10533965, May 2024, IEEE Xplore.
[23] (2022). Lookout CASB. [Online]. Available: https://www.lookout. com/products/casb-cloud-access-security-broker.
[24] Ravindra Changala, "Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527499, May 2024, IEEE Xplore.
[25] Ravindra Changala, "Real-Time Anomaly Detection in 5G Networks Through Edge Computing", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527501, May 2024, IEEE Xplore.
[26] Ravindra Changala, "Enhancing Quantum Machine Learning Algorithms for Optimized Financial Portfolio Management", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527612, May 2024, IEEE Xplore.
[27] Cisco Cloudlock. https://www.cisco.com/c/en/us/products/security/cloudlock/index.html.
[29] Ravindra Changala, "Optimizing 6G Network Slicing with the EvoNetSlice Model for Dynamic Resource Allocation and Real-Time QoS Management", International Research Journal of Multidisciplinary Technovation, Vol 6 Issue 4 Year 2024, 6(4) (2024) 325-340.
[30] Ravindra Changala, "Deep Learning Techniques to Analysis Facial Expression and Gender Detection", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10525942, May 2024, IEEE Xplore.
[31] Ravindra Changala, "UI/UX Design for Online Learning Approach by Predictive Student Experience", 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), ISBN:979-8-3503-4060-0, DOI: 10.1109/ICECA58529.2023.10395866, February 2024, IEEE Xplore.
[32] Ravindra Changala, Brain Tumor Detection and Classification Using Deep Learning Models on MRI Scans", EAI Endorsed Transactions on Pervasive Health and Technology, Volume 10, 2024.
[33] Ravindra Changala, "Optimization of Irrigation and Herbicides Using Artificial Intelligence in Agriculture", International Journal of Intelligent Systems and Applications in Engineering, 2023, 11(3), pp. 503–518.
[34] Ravindra Changala, "Integration of IoT and DNN Model to Support the Precision Crop", International Journal of Intelligent Systems and Applications in Engineering, Vol.12 No.16S (2024) .
[35] Ravindra Changala, Development of Predictive Model for Medical Domains to Predict Chronic Diseases (Diabetes) Using Machine Learning Algorithms and Classification Techniques, ARPN Journal of Engineering and Applied Sciences, Volume 14, Issue 6, 2019.
[36] Ravindra Changala, "Evaluation and Analysis of Discovered Patterns Using Pattern Classification Methods in Text Mining" in ARPN Journal of Engineering and Applied Sciences, Volume 13, Issue 11, Pages 3706-3717 with ISSN:1819-6608 in June 2018.
[37] Ravindra Changala "A Survey on Development of Pattern Evolving Model for Discovery of Patterns in Text Mining Using Data Mining Techniques" in Journal of Thoretical and Applied Information Technology, August 2017. Vol.95. No.16, ISSN: 1817-3195, pp.3974-3987.
[38] Microsoft Cloud App Security. https://www.microsoft.com/enus/security/business/siem-and-xdr/microsoft-defender-cloud-apps.