ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26apr1595

Zero Trust-Based Secure Healthcare Data Access System with LSTM Behavioral Analysis

Anbarasi M. S.[1]; Imayavaramban P.[2]; Saranya S.[3]; Saran V.[4]

[1,2,3,4]Department of Information Technology, Puducherry Technological University, Puducherry, India

Publication Date: 2026/05/11

Abstract: In the current scenario after pandemic, remote health monitoring systems play a vital role for real-time patient healthcare. Sensitive data such as patient personal information and medical records are transmitted between patients, hospital databases, and healthcare specialists, often via Virtual Private Networks (VPNs). However, VPNs are susceptible to malware and phishing attacks, and traditional perimeter-based security models fail to provide adequate protection against insider threats and lateral movement within networks. This project proposes Zero Trust-Based Secure Healthcare Data Access System with LSTM Behavioral Analysis, a layered security that integrates Zero Trust Network Access, continuous identity verification, machine learning-driven behavioral anomaly detection, and automated incident response. The system enforces identity-certificate-based network isolation, per-request authentication, and attribute-based policy control to ensure no device or user gains access without continuous verification. User sessions are monitored in real time using a Long Short-Term Memory model that analyses sequential behavioral patterns and computes dynamic trust scores, enabling detection of insider threats that bypass traditional access control. Based on these scores, the system automatically applies graduated containment actions from enhanced monitoring to complete session revocation, eliminating the delay between detection and active response. By unifying network-level isolation, behavioral intelligence, and automated enforcement, the proposed system bridges the gap between static access control and the adaptive security demanded by modern healthcare environments.

Keywords: *Zero Trust Architecture, Long Short-Term Memory, Behavioral Anomaly Detection, Healthcare Data Security, Electronic Health Records, Insider Threat Detection, Mutual TLS, Open Policy Agent, Automated Incident Response*.

How to Cite: Anbarasi M. S. ; Imayavaramban P. ; Saranya S. ; Saran V. (2026). Zero Trust-Based Secure Healthcare Data Access System with LSTM Behavioral Analysis. *International Journal of Innovative Science and Research Technology*, 11(4), 4060-4066. https://doi.org/10.38124/ijisrt/26apr1595

I. INTRODUCTION

The proposed system is designed as a secure for real-time healthcare data access control and insider threat detection. It begins with device and identity verification, where identity-certificate-based network enforcement ensures that only trusted devices holding valid cryptographic credentials can discover and connect to backend healthcare services. This is followed by continuous user authentication, where signed tokens are validated on every individual request rather than only at session establishment, ensuring uninterrupted identity verification throughout the session.

The system then enforces fine-grained access control through a policy-driven decision engine that evaluates both user role and contextual attributes before permitting access to any Electronic Health Record resource. This hybrid policy model ensures that access decisions are made dynamically based on what is being requested and by whom, rather than relying on static permission assignments made at role creation time.

Once access is granted, the system continuously monitors authenticated user behaviour using a Long Short-Term Memory model that analyses sequential activity patterns across sessions. The model computes a dynamic trust score for each active user, enabling detection of insider threats that operate entirely within permitted access boundaries and cannot be identified through access control mechanisms alone.

Based on the computed trust score, the system activates an automated incident response layer that applies graduated containment actions proportional to the detected threat level. These actions range from enhanced session monitoring and step-up verification through to immediate session revocation and account quarantine, all executed without requiring manual administrator intervention.

Overall, the proposed system transforms conventional VPN-based healthcare access into an intelligent, continuously verified, and behaviourally aware security, addressing key limitations such as implicit network trust, absence of insider threat detection, and delayed incident containment.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26apr1595

II. RELATED WORKS

The literature survey focuses on major components of Zero Trust security, behavioral anomaly detection, insider threat analysis, and automated incident response in healthcare environments.

Al-Shaer et al. [1] conducted a comprehensive review of Zero Trust Architecture for healthcare environments, identifying continuous verification and least-privilege enforcement as foundational requirements. Chaturvedi et al. [2] proposed a ZTA for digital privacy in healthcare settings, emphasizing identity-based tunnelling. Wang et al. [12] introduced a dynamic Zero Trust access control model that evaluates device trust prior to granting resource access; however, it lacks certificate-based overlay network enforcement that hides backend services from unauthorized discovery. Gupta et al. [4] proposed a token-based authentication mechanism for healthcare systems using identity and role-based tokens for session validation, but it does not support per-request continuous validation. Sangeetha et al. [9] proposed the Secure Healthcare Access Control System (SHACS), integrating RBAC, ABAC, and ML-based anomaly detection in cloud-based healthcare environments, serving as a primary baseline in this work.

Liu et al. [7] surveyed machine learning and deep learning techniques for insider threat detection, identifying LSTM-based sequential modelling as particularly effective for capturing temporal behavioural patterns. Shu et al. [11] proposed an insider threat detection system based on user behaviour analysis in healthcare information systems using session log temporal features; however, it relies on static thresholds that do not adapt to individual user baselines. Kumar et al. [6] applied LSTM-based anomaly detection to EHR access control in telemedicine environments but limited feature sources to a single log stream. Sharma et al. [10] proposed a trust score generation for Zero Trust environments; however, it treats each session independently, losing the contextual memory critical for detecting gradual insider threat escalation.

Chen et al. [3] proposed an ML-enhanced automated incident response for healthcare cyber threats that classifies threat severity and maps it to predefined response playbooks, but requires manual administrator approval before enforcement. Paul et al. [8] integrated AI-driven threat classification with automated policy adjustment in a Zero Trust, but applied broad network-level blocks that disrupt legitimate concurrent sessions. Khanizadeh et al. [5] developed a regulated transformer-based anomaly detection with structured incident logging, but limited its output to alerting without executing automated enforcement actions. The proposed system addresses these limitations by automating a graduated response pipeline with direct integration into Keycloak session management and OPA policy enforcement.

Overall, existing works address individual aspects such as Zero Trust access control, behavioural anomaly detection, trust scoring, or incident response. However, they lack a unified system that integrates network-level isolation, continuous per-request authentication, sequential behavioural analysis, real-time trust scoring, and automated graduated containment into a single cohesive.

The proposed system addresses these limitations by providing a complete and integrated architecture that combines identity-certificate-based dark network enforcement, hybrid policy-driven access control, Long Short-Term Memory based trust scoring, and automated incident response into a unified real-time security pipeline for healthcare environments.

III. PROPOSED WORK

Fig. 1 shows the architecture of the proposed system. The proposed system focuses on the design and implementation of a secure and intelligent healthcare data access that protects Electronic Health Record systems from both network-level intrusion and identity-based insider threats. It is developed as a sequence of steps that connects device authentication, continuous identity verification, behavioural anomaly detection, and automated incident response into a single unified work. The system continuously evaluates every access request and user session to ensure that trust is never implicitly granted but always actively verified and behaviourally validated.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26apr1595

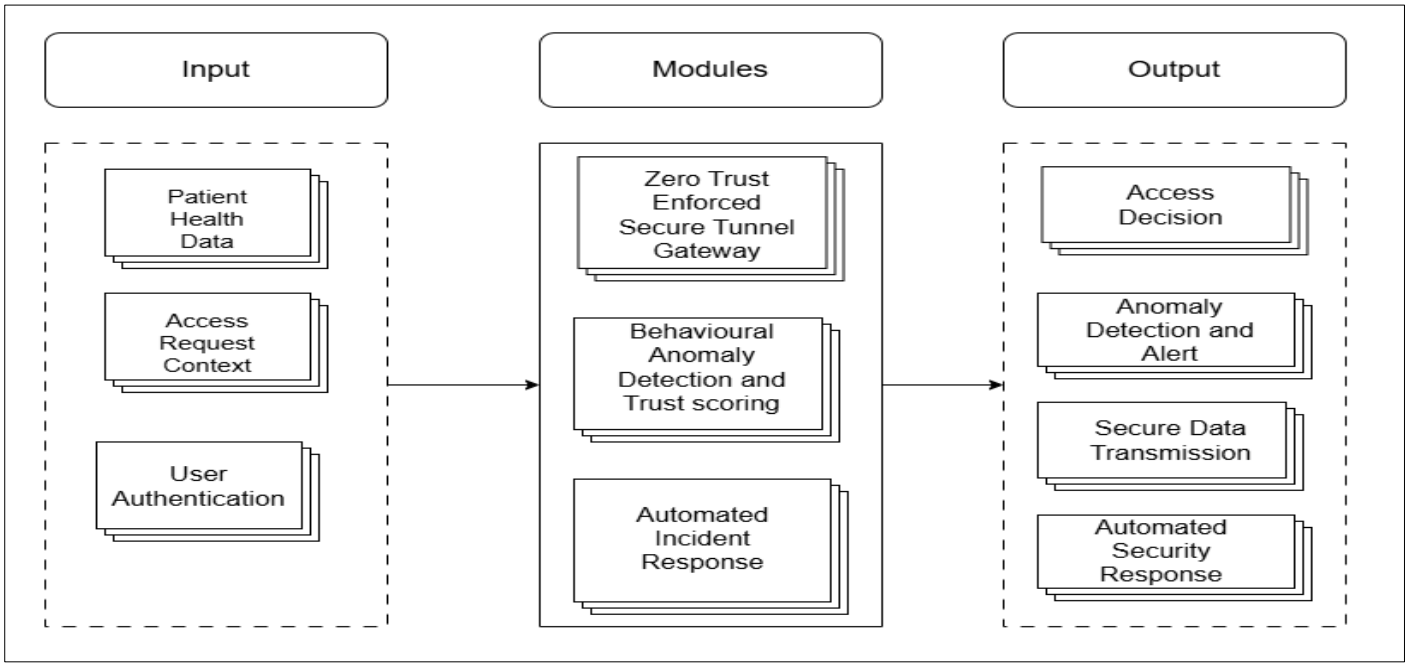

Fig 1 Architecture Diagram of the Proposed Model

The system is divided into three modules, where each module performs a specific stage in the overall security workflow. This modular structure improves scalability, maintainability, and enforcement efficiency.

➢ *Module – I: Zero Trust Enforced Secure Tunnel Gateway*

This module, represented in Fig. 2, is responsible for establishing a secure and verified entry point for all incoming healthcare data access requests. It ensures that no device or user can reach backend Electronic Health Record services without passing through a strict chain of identity verification, authentication, and policy enforcement. The module converts raw access requests into fully verified, policy-approved interactions before any healthcare resource is exposed.

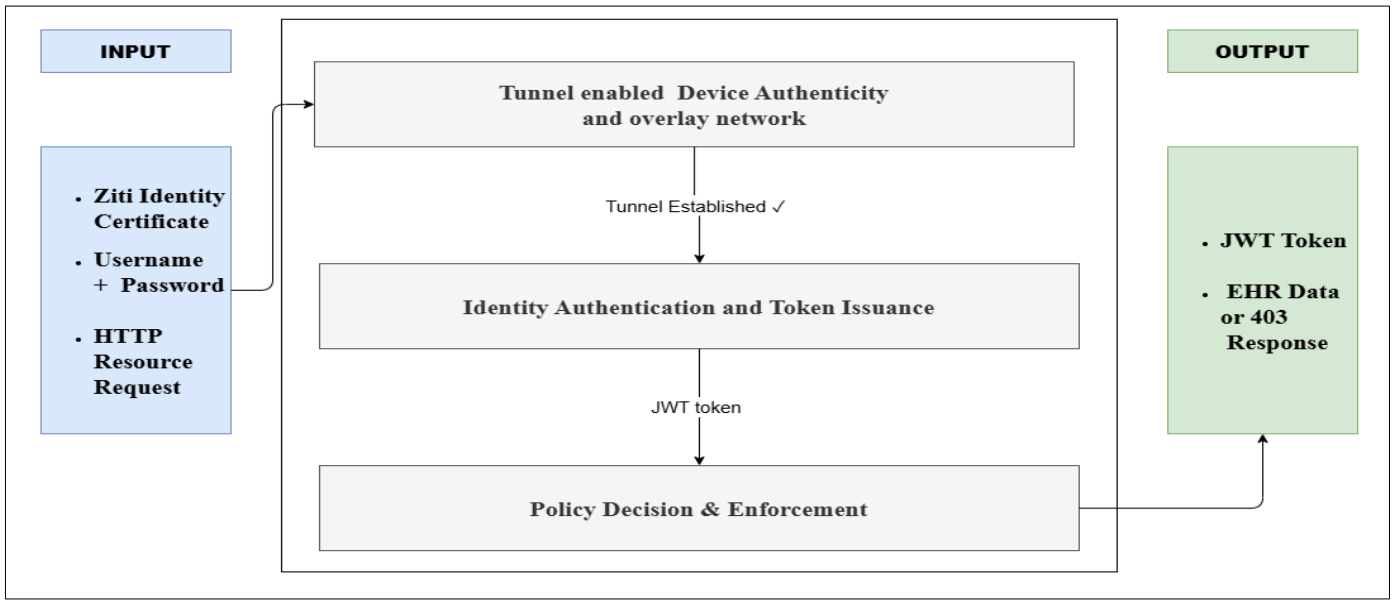

Fig 2 Module Diagram of Zero Trust Enforced Secure Tunnel Gateway

- *Device-Level Dark Network Enforcement*

The system deploys OpenZiti to make the backend Electronic Health Record API completely invisible on the network. No direct connection to the backend service is possible from any node without a valid enrolled identity certificate. Each hospital role is issued a unique cryptographic identity certificate, and the Ziti edge router intercepts all traffic and validates the certificate before forwarding the request. This ensures that even if an attacker gains access to the hospital network, the backend service remains completely unreachable without the correct certificate, eliminating lateral movement at the network layer.

- *Mutual TLS Authentication*

Every connection between a user node and the edge router is protected using Mutual Transport Layer Security,

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26apr1595

where both the client and the server present and verify certificates during the handshake. This bidirectional verification ensures that neither party can impersonate the other, providing strong resistance against man-in-the-middle attacks and session hijacking. Validation is enforced for every session rather than only at initial connection.

- *JWT-Based Stateless Authentication*

After successful user authentication, the identity provider issues a signed JSON Web Token containing the user identity, assigned hospital role, and expiry time. The backend service validates this token on every incoming request by verifying its cryptographic signature. If the token is expired, tampered with, or missing, the request is rejected before it reaches any data layer. This ensures that identity verification occurs at every single request, fulfilling the continuous verification requirement of Zero Trust Architecture.

- *Hybrid RBAC+ABAC Policy Enforcement*

The policy engine evaluates hybrid Role-Based and Attribute-Based Access Control rules for each request, allowing or denying access based on the user's assigned role and contextual attributes such as resource type and sensitivity level. A cardiologist is permitted access to clinical patient data but denied access to billing records, while an auditor is permitted access to billing records but denied access to clinical data. No data is returned unless the policy engine explicitly approves the request.

- *PDP/PEP/PIP Architecture Separation*

The security decision pipeline is decomposed into three distinct functional components following the NIST SP 800-207 Zero Trust Architecture. The identity provider serves as the Policy Information Point by supplying verified identity claims. The policy engine serves as the Policy Decision Point by evaluating whether the identity and context satisfy the access policy. The backend application serves as the Policy Enforcement Point by intercepting every request and enforcing the policy decision. This strict separation ensures that compromising any single component does not automatically grant unauthorized access.

➢ *Module– II: Behavioral Anomaly Detection and Trust Scoring*

This module, represented in Fig. 3, is responsible for continuously monitoring the behavioral patterns of authenticated users after they have been granted access through Module I. It analyses the sequence of actions performed by each user during their session and computes a numerical trust score that represents how closely the current behavior matches that user's established historical baseline. The module treats each request as part of an ongoing behavioral sequence rather than an isolated event, enabling detection of insider threats that operate entirely within permitted access boundaries.

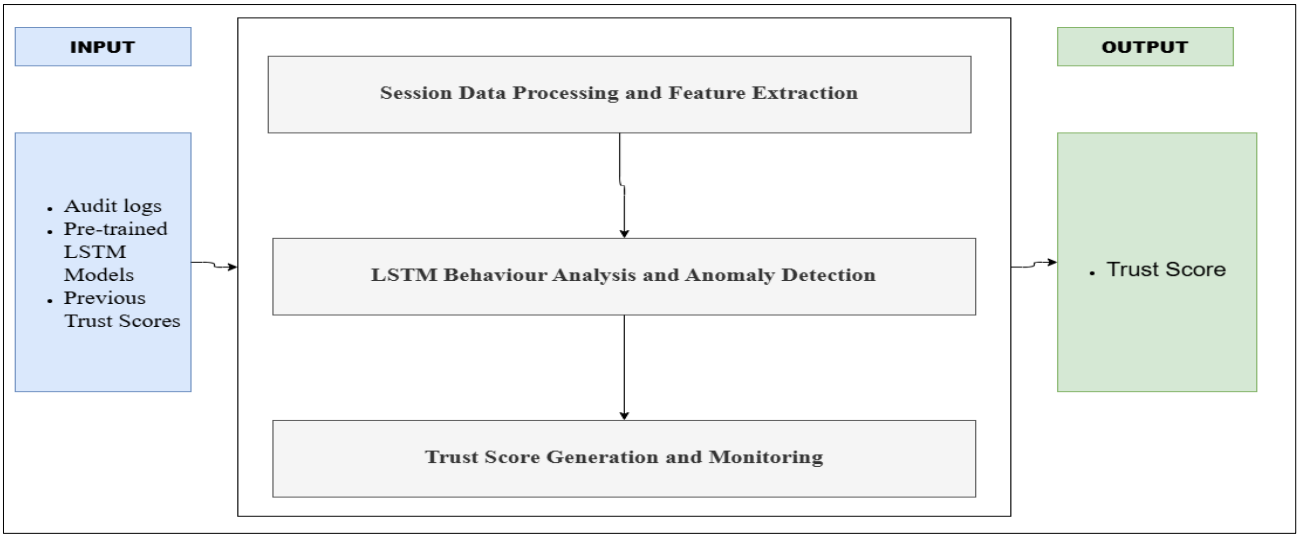

Fig 3 Module Diagram of Behavioral Anomaly Detection and Trust Scoring

- *Session Data Processing and Feature Extraction*

The system collects raw activity logs from multiple sources and processes them into a structured feature matrix for model training and runtime inference. Seven daily behavioural features are extracted from each user's session activity: requests per minute, hour of day, data volume accessed, number of unique resources accessed, device change flag, role mismatch attempts, and billing access ratio. The billing access ratio is a healthcare-specific feature that measures the proportion of financial data accessed relative to total requests, providing a strong discriminating signal for detecting billing-related insider threats. These features together form a comprehensive behavioural profile for each active user.

- *LSTM Behaviour Analysis and Anomaly Detection*

A Long Short-Term Memory model is trained on the CERT Insider Threat Dataset to learn normal and malicious behavioural patterns from real-world organisational activity logs. Unlike static models that evaluate each session independently, the LSTM captures sequential dependencies across time, identifying gradual behavioural deviations that emerge over multiple sessions rather than sudden isolated anomalies. The model architecture consists of two stacked

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26apr1595

LSTM layers followed by a sigmoid output layer for binary anomaly classification. A sliding window of twenty consecutive daily activity records is applied to each user's timeline, generating fixed-length input sequences for both training and runtime inference. Class-weighted binary cross-entropy loss is applied during training to ensure that the model focuses appropriately on the minority malicious class rather than defaulting to the majority normal class.

- *Trust Score Generation and Monitoring*

The trained LSTM model is deployed as a continuously running inference agent that monitors active user sessions at fixed intervals. For each active user, the system retrieves the most recent activity logs from the database, processes them into the seven-dimensional feature vectors, and feeds the resulting sequence into the LSTM model. The anomaly probability output is normalised into a trust score between zero and one, where a higher score indicates closer alignment with normal behaviour and a lower score indicates increasing suspicion. Trust scores are updated every five minutes and expire after ten minutes to ensure freshness. These scores are consumed directly by the policy engine in Module I, creating a dynamic feedback loop where behavioural deterioration automatically tightens access control without manual intervention. If insufficient historical data exists for a user, a monitored state is applied as a precautionary measure.

➢ *Module– III: Automated Incident Response*

This module, represented in Fig. 4, is responsible for taking immediate and adaptive actions based on the trust scores and anomaly detections generated in Module II. It ensures that suspicious or malicious activities are contained in real time by dynamically enforcing security responses such as access restriction, session termination, and alert generation. Instead of relying on manual intervention, the module automates incident handling to minimize response time and reduce potential damage caused by insider threats or compromised accounts. The system continuously evaluates trust score variations and triggers appropriate response mechanisms based on predefined thresholds and policies.

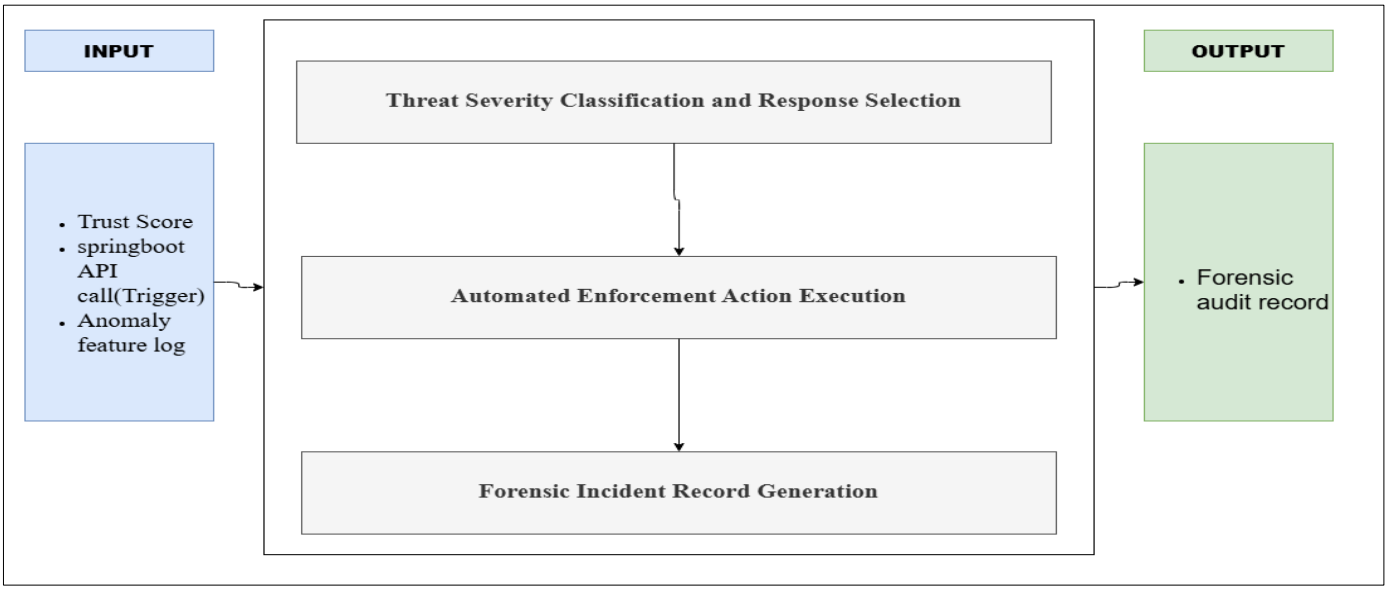

Fig 4 Module Diagram of Automated Incident Response

- *Threshold-Based Decision Engine*

The system defines multiple trust score thresholds to categorize user behaviour into different risk levels such as safe, suspicious, and critical. These thresholds are configured based on organizational security policies and risk tolerance levels. When the trust score of a user falls below a certain threshold, the system automatically classifies the session as anomalous. This classification acts as the primary trigger for initiating appropriate incident response actions without delay.

- *Dynamic Access Control and Restriction*

Based on the evaluated risk level, the system dynamically modifies user permissions in real time. For moderately suspicious behaviour, access may be restricted to only low-risk resources, while high-risk behaviour results in immediate blocking of sensitive data access. This adaptive control mechanism ensures that users are not completely disconnected unless necessary, but their actions are strictly limited to prevent misuse of critical healthcare data.

- *Session Termination and Re-Authentication*

For critical threat scenarios where the trust score drops significantly or malicious activity is confirmed, the system forcibly terminates the active session. Users may be required to undergo re-authentication using stronger verification methods before regaining access. This step prevents attackers from maintaining persistent access and ensures that compromised sessions are immediately invalidated.

- *Adaptive Learning and Policy Improvement*

The system supports continuous improvement by incorporating feedback from detected incidents into policy updates and model refinement. Patterns identified from previous attacks or anomalies can be used to fine-tune threshold values and response strategies. This adaptive capability ensures that the system evolves over time, becoming more resilient against emerging threats and sophisticated attack techniques.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26apr1595

IV. RESULTS ANALYSIS

The proposed Zero Trust–based secure access and monitoring system was evaluated to analyze its effectiveness in detecting anomalous behaviour, maintaining secure communication, and enforcing adaptive access control in healthcare environments. The system integrates authentication, behavioural analysis, trust scoring, and automated response mechanisms, and its performance was assessed based on security accuracy, response time, and system adaptability.

The behavioural anomaly detection model based on Long Short-Term Memory demonstrated strong capability in identifying deviations from normal user activity. By analysing sequential user behaviour rather than isolated events, the model successfully detected gradual insider threats and unusual access patterns. The use of multiple behavioural features such as request frequency, data access patterns, and device changes significantly improved detection accuracy and reduced false positives.

The trust scoring mechanism provided a continuous and dynamic representation of user behaviour. Users with normal activity consistently maintained high trust scores, while anomalous behaviour resulted in rapid score degradation. This enabled the system to respond proactively rather than reactively. The integration of trust scores with the policy enforcement layer ensured that access decisions were continuously updated based on real-time behaviour.

The Zero Trust Enforced Secure Tunnel Gateway effectively ensured secure communication by establishing encrypted, session-specific tunnels. Unlike traditional perimeter-based approaches, the system validated every request independently, thereby minimizing the risk of unauthorized access and lateral movement within the network. This approach enhanced data confidentiality and integrity, which are critical in healthcare systems handling sensitive patient information.

The Automated Incident Response module demonstrated efficient handling of security threats through real-time actions such as access restriction, session termination, and alert generation. The response time was significantly reduced compared to manual intervention, ensuring that potential threats were contained before causing major impact. Additionally, the logging and auditing mechanisms provided a detailed record of system activities, supporting compliance and forensic analysis.

Overall, the system showed improved security performance by combining continuous monitoring, adaptive access control, and automated response strategies. The integration of Zero Trust principles with machine learning–based behavioural analysis resulted in a robust and scalable solution capable of addressing modern cybersecurity challenges in healthcare environments.

➢ *The Dataset Used:*

- The CERT Insider Threat Dataset r4.2: This project utilizes the CERT Insider Threat Dataset r4.2, developed by Carnegie Mellon University, which contains simulated activity logs of approximately 1,000 employees over a period of 17 months.
- Comprehensive Activity Logs: The dataset includes diverse machine-readable records such as logon/logoff events, file operations, and email activity, providing labelled scenarios for both normal behaviour and malicious insider threats like data theft.

V. CONCLUSION AND FUTURE ENHANCEMENTS

The proposed system presents a comprehensive security based on Zero Trust principles for protecting sensitive healthcare data. By eliminating implicit trust and enforcing continuous verification, the system ensures that every access request is validated based on user identity, device trust, and contextual parameters. The integration of secure tunnel communication, behavioural anomaly detection, and dynamic trust scoring enhances the overall security posture and reduces the risk of unauthorized access and insider threats.

The use of Long Short-Term Memory for behavioural analysis enables the system to capture sequential user activity patterns and detect subtle anomalies that traditional methods fail to identify. The Automated Incident Response module further strengthens the system by enabling real-time actions such as access restriction, session termination, and alert generation, thereby minimizing response time and potential damage.

For future enhancements, the system can be extended by incorporating advanced deep learning models such as transformer-based architectures for improved behavioural prediction and anomaly detection. Integration with real-time healthcare systems and IoT medical devices can further enhance security coverage across distributed environments. Additionally, implementing federated learning approaches can enable privacy-preserving model training across multiple healthcare organizations without sharing sensitive data. The inclusion of explainable AI techniques can also improve transparency in decision-making, allowing administrators to better understand and trust the system's actions. These enhancements will further strengthen the system's capability to address evolving cybersecurity threats in complex healthcare infrastructures.

Overall, the system provides a scalable, adaptive, and efficient solution for modern healthcare cybersecurity challenges. It successfully combines Zero Trust Architecture with machine learning–based behavioural analysis to deliver continuous monitoring, dynamic access control, and proactive threat mitigation.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26apr1595

REFERENCES

[1]. A. Al-Shaer, J. Al-Haj, and F. Binsaeed, "Zero Trust Architecture for healthcare: A comprehensive review and implementation framework," in Proc. IEEE Int. Conf. Cyber Security and Cloud Computing (CSCloud), Shenzhen, China, 2024, pp. 112–119.

[2]. I. Chaturvedi, P. M. Pawar, R. Muthalagu, and P. S. Tamizharasan, "Zero Trust Security Architecture for digital privacy in healthcare," in Information Technology Security, Singapore: Springer, 2024, pp. 1–22.

[3]. L. Chen, Y. Zhang, and H. Wang, "ML-Enhanced Automated Incident Response Framework for Healthcare Cyber Threats," Journal of Cybersecurity and Privacy, vol. 4, no. 2, pp. 287–305, 2024.

[4]. D. S. Gupta, N. Mazumdar, A. Nag, and J. P. Singh, "Secure data authentication and access control protocol for industrial healthcare systems," Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 5, pp. 4853–4864, 2023.

[5]. F. Khanizadeh, A. Ettefaghian, G. Wilson, A. Shirazibeheshti, T. Radwan, and C. Luca, "RTAD-HIS: Regulated transformer architecture based anomaly detection framework towards security in healthcare IoT systems," Applied Soft Computing, vol. 170, Art. no. 112565, 2025.

[6]. R. Kumar, A. Sharma, and P. Singh, "LSTM-based anomaly detection for EHR access control in telemedicine environments," in Proc. International Conference on Artificial Intelligence in Healthcare (ICAIH), New Delhi, India, 2024, pp. 45–52.

[7]. Y. Liu, X. Dong, J. Li, and X. Zhang, "A survey on insider threat detection using machine learning and deep learning," IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 3, pp. 1523–1540, 2024.

[8]. E. M. Paul, U. Mmaduekwe, J. D. Kessie, and M. D. Salawudeen, "Zero trust architecture and AI: A synergistic approach to next-generation cybersecurity frameworks," International Journal of Science and Research Archive, vol. 13, no. 2, pp. 1–12, 2024.

[9]. S. K. B. Sangeetha, C. Selvarathi, S. K. Mathivanan, J. Cho, and S. V. Easwaramoorthy, "Secure Healthcare Access Control System (SHACS) for anomaly detection and enhanced security in cloud-based healthcare applications," IEEE Access, vol. 12, pp. 164543–164559, 2024.

[10]. R. K. Sharma, P. Kumar, and S. Mishra, "Implementing Zero Trust Security Model in Healthcare Cloud Environments: Challenges and Solutions," IEEE Access, vol. 12, pp. 45123–45138, 2024.

[11]. T. Shu, X. Zhao, H. Pei, L. Zhang, and D. Zou, "Insider threat detection based on user behaviour analysis in healthcare information systems," Future Generation Computer Systems, vol. 148, pp. 234–247, 2023.

[12]. R. Wang, C. Li, K. Zhang, and B. Tu, "Zero-trust based dynamic access control for cloud computing," Cybersecurity, vol. 8, no. 1, Art. no. 7, 2025.

AUTHOR'S BIOGRAPHY

Anbarasi M. S.
Professor in the Department of Information Technology, Puducherry Technological University. B.E., M.E., Ph.D., with specialization in Data Mining for Healthcare Predictions, Big Data Analytics, Cloud Computing, and Software Engineering. Actively involved in teaching and research in the areas of data analytics, cloud computing, and secure computing technologies.

Imayavaramban P.
A B.Tech Information Technology student at Puducherry Technological University with a strong focus on full-stack web development and real-world application building. Skilled in Python, JavaScript, and modern frameworks, with hands-on experience developing dynamic projects such as admin dashboards, CRUD-based web applications, and interactive systems. Driven to create practical, user-centered solutions while continuously improving problem-solving skills and technical depth.

Saranya S.
A B.Tech Information Technology student at Puducherry Technological University with a strong interest in Artificial Intelligence/Machine Learning. Proficient in technologies such as React, Flask, Node.js, and MySQL, with a focus on building scalable and efficient web applications. Focused on developing intelligent systems and applying modern computing techniques to address real-world challenges while continuously strengthening technical knowledge.

Saran V.
A B.Tech Information Technology student at Puducherry Technological University with a strong interest in web development. Skilled in Python and C, with experience developing applications such as games, music, and other interactive platforms. Focused on building efficient and creative solutions that integrate strong backend logic with engaging, user-friendly interfaces.