Svedberg Open
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Artificial Intelligence Enabled Zero-Trust Cyber Security Framework for Smart Healthcare Infrastructure

Dr.P. Selvaperumal[1], Dr. Lulup Kumar Sahoo[2], Arjit Tomar[3], Kiran Ingale[4], Nainavarapu Radha[5], Dr. Devanshu J. Patel[6], Dr. Shikhar Verma[7], Harshini R[8]

[1]Assistant Professor, Department of Computer Science, St Joseph's University, Bengaluru, India ,
Email: selvaperumal@sju.edu.in

[2]Professor, Department of Neurology, IMS and SUM Hospital, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India, Email: lulupkumarsahoo@soa.ac.in, Orcid Id- 0000-0002-2646-2962

[3]Department of Computer Science & Engineering,Noida international University, Greater Noida, Uttar Pradesh 203201, India, Email: arjit.tomar@niu.edu.in

[4]Assistant Professor, Department of E&TC Engineering, Vishwakarma Institute of Technology, Pune, Maharashtra, 411037, Email: kiran.ingale@vit.edu

[5]Associate Professor, Department of ECE, Aditya University, Surampalem, Andhra Pradesh, 533437,
Email: radha.nainavarapu@adityauniversity.inOrchid id: 0000-0002-5526-1633

[6]Associate Professor, Department of Pharmacology, Parul University, PO Limda, Tal. Waghodia, District Vadodara, Gujarat, India, Email: president@paruluniversity.ac.in, Orcid Id- 0000-0001-7612-0111

[7]Professor , MSOPS, Maharishi University of Information Technology, Lucknow, Uttar Pradesh, India, Email: shikhar.verma@muit.in, Orcid Id- https://orcid.org/0000-0002-2481-395X

[8]Computer Science, Assistant Professor, Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research , Chennai, Tamil Nadu, India, Email: harshinir@maher.ac.in

Abstract

Smart infrastructure deployment in healthcare, such as the Internet of Medical Things (IoMT) devices, cloud-based clinical platforms and intelligent patient monitoring systems, has greatly enhanced the vulnerabilities of the healthcare infrastructure. Traditional perimeter security solutions are not enough to defend against advanced attacks like ransomware, unauthorised access, data breaches or insider threats. These challenges led to proposing an AI-enabled Zero-Trust Cyber Security Framework for smart healthcare infrastructure that continuously verifies the users, devices, and network activities before providing access to critical medical resources. The plan in the proposed infrastructure is to combine Zero-Trust Architecture (ZTA) principles with an AI-based threat detection system that can detect unusual behavior and patterns of malicious traffic in real time. An adaptive intrusion detection, dynamic trust evaluation and intelligent access control are implemented with the help of a hybrid deep learning model. The experimental validation has been performed on cybersecurity datasets related to the healthcare industry and simulated smart healthcare traffic scenarios. The proposed framework achieves high results for attack detection accuracy, low false positive and low authentication latency compared to the conventional security techniques, as shown by results. The framework improves security resilience, scalability and instant protection for the next generation smart healthcare ecosystems.

Keywords: Zero-Trust Security, Smart Healthcare, Artificial Intelligence, Cybersecurity Framework, Intrusion Detection, IoMT Security

1. Introduction

Smart healthcare infrastructure has undergone a rapid transformation, enabled by the Internet of Medical Things (IoMT) devices, cloud-based systems, artificial intelligence and real-time patient monitoring systems (Al-Turjman et al., 2020; Islam et al., 2015; Sun et al., 2019). Smart healthcare systems can facilitate clinical

decisions, remote diagnostics, automatic medical processes, and continuous patient monitoring, which enhances the access to healthcare and its operational efficiency (Rahmani et al., 2018; Sodhro et al., 2019). Healthcare delivery systems are becoming more and more intelligent through the use of wearable sensors, smart infusion pumps, connected diagnostic devices, and cloud-based EHR platforms that can be adopted in hospitals and health institutions (Alsubaei et al., 2017; Koutras et al., 2020). But, a massive integration of medical devices and cloud-based healthcare services has made the cyberattack surface of healthcare ecosystems (Sun et al., 2019) considerably wide.

Healthcare organisations are particularly susceptible to various types of cyberattacks, including: ransomware, hacking and unauthorized access, insider threats, data manipulation, and Denial of Service attacks (Ferrag et al., 2020; Kumar et al., 2021). Healthcare information has very sensitive and private patient data, with the successful attacks on these systems potentially resulting in significant financial losses, disruption of operations, and potential to affect patient safety (Alsubaei et al., 2017). Perimeter-based security models are heavily dependent on static firewalls, and trust is assumed at a single central location which is not sufficient for dynamic and distributed healthcare environments (Rose et al., 2020). In this way, attackers may penetrate the network's perimeter and, once they have done so, be able to carry out lateral movement and escalation of privileges within the internal systems. To overcome these difficulties, Zero-Trust Architecture (ZTA) has become a promising cybersecurity paradigm that follows the policy of “never trust, always verify“ (Rose et al., 2020). Zero-trust security continually verifies users, devices and activities in any network before allowing access to resources. Moreover, AI can facilitate adaptive cybersecurity, which involves analyzing user behavior, identifying anomalies, and reacting to emerging threats in real time (Sarker, 2023). Artificial intelligence-based security can greatly improve Healthcare cyber security by using intelligence to predict threats and automate risk assessment (Vinayakumar et al., 2019).

While recent developments have occurred in healthcare security, current healthcare security models are typically composed of disjointed AI-powered ZT components, where one component is developed in isolation and deployed without fully considering the impact of the other components (Ferrag et al., 2020). Most of the other frameworks have also limitations in scalability, latency and the lack of threat intelligence capabilities. Hence, this paper introduces an Artificial Intelligence (AI) based Zero Trust Cyber Security Framework to the smart healthcare infrastructure. The proposed framework combines the use of an AI-powered zero-trust architecture for healthcare security with an intelligent threat detection and monitoring engine that continuously monitors network activities and identifies malicious patterns in real time. Furthermore, the framework features an adaptive access control and dynamic trust assessment mechanism to augment the process of access control and trust evaluation in smart healthcare environments. Experimental validation of the effectiveness of the proposed system is performed using attack data sets in healthcare cybersecurity to assess the accuracy of detecting attacks, false positive rates, authentication latency and the overall security performance of the system (Shone et al., 2018; Wang et al., 2017).

This research has made significant contributions in the area of cybersecurity for smart healthcare infrastructure, such as the development of an AI-based ZT security framework designed for the smart healthcare infrastructure, as well as incorporation of a real-time intelligent threat detection engine for adaptive cyberattack identification, and also the implementation of a dynamic trust-based access control mechanism for secure communication among smart healthcare components to ensure security in smart healthcare system, which has been validated through extensive experiments using healthcare-related cybersecurity datasets demonstrating the superiority in terms of enhanced cybersecurity performance, decrease in false positive rates, and lesser authentication latency over conventional cybersecurity approaches (Kim et al., 2016; Vinayakumar et al., 2019).

2. Related Work

Smart healthcare technologies have recently been adopted on a rapid pace, making healthcare systems vulnerable to cyber threats (Al-Turjman et al., 2020). In today's healthcare setting, there are numerous interconnected devices (Internet of Medical Things (IoMT)), patient databases stored in the cloud, wireless

monitoring systems, and remote diagnostic platforms (Islam et al., 2015). While these technologies provide greater efficiencies and patient care in healthcare, they also create significant cybersecurity vulnerabilities (Sun et al., 2019). In addition to the ransomware attack, phishing attack, malware injection, access attack (unauthorized user access), insider threat attack, and Distributed Denial of Service (DDos) attack on hospital networks and medical devices, the following are the existing attack models on healthcare:The existing attack models on healthcare are summarized as follows: ransomware attack, phishing attack, malware injection, access attack (unauthorized user access), insider threat attack, and Distributed Denial of Service (DDos) attack on hospital networks and medical devices (Kumar et al., 2021). A cyberattack against a health system's infrastructure can hinder clinical operations, create problems with sensitive patient data, and put patients at risk for harm (Alsubaei et al., 2017). Moreover, IoMT devices usually have low computational capabilities and insecure security implementations, which could trigger authentication bypass, device spoofing, or data interception attacks (Koutras et al., 2020). With all these challenges raised, the adoption of intelligent and adaptive cybersecurity mechanisms that are tailored and designed for smart healthcare ecosystems becomes paramount.

The zero-Trust Architecture (ZTA) is a successful security model to overcome the shortcoming of traditional perimeter-based security solution (Rose et al., 2020). With conventional security systems, once a user or device is authenticated in the system, it's assumed that it's safe from that point on, allowing for lateral movement when a network is compromised. While this may be the case with the traditional ZTA frameworks, they continuously challenge users, devices and applications prior to granting access to resources, thus removing any implicit trust. Zero-trust systems typically include identity authentication methods like multi-factor authentication, behavioral verification, device fingerprinting, and access control based on context. A digital trust assessment is done continuously, with this approach strengthening the system's resistance against changing cyber threats. But many existing ZTA implementations are geared toward enterprise networks and do not optimize for healthcare-specific operational needs and real time medical communication.

The use of AI in IDSs has gained relevance because of its ability to analyze massive amounts of network traffic and real-time identification of suspicious activities (Sarker, 2023). Machine learning-based intrusion detection systems employ classifiers like KNN, decision trees, random forests, and SVM for detecting intrusions in healthcare networks. More recently, deep learning security systems based on Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) models have proven to perform better in threat detection of advanced attacks and unknown cyber threat patterns (Kim et al., 2016; Shone et al., 2018). AI-powered security systems can perform threat analysis, adaptive learning, and predictive attack detection (Vinayakumar et al., 2019). Nevertheless, though these developments have occurred, there are a plethora of systems that employ AI to detect intrusions but do not integrate with zero-trust healthcare architectures, and as a result, their effectiveness is constrained in healthcare environments that are dynamic and distributed (Ferrag et al., 2020).

While extensive efforts have been made in healthcare cybersecurity, there are still major gaps in the seamless adoption of AI and zero-trust security concepts. Current healthcare security frameworks are either designed to focus on AI-enabled IDS with a lack of constant trust validation or to usher in a zero-trust strategy without intelligent adaptive threat analysis. Moreover, the existing policies are prone to scalability, authentication latency, static security policies and inadequate real-time threat intelligence. Their weaknesses make them less effective in supporting big-scale smart healthcare infrastructures with diverse types of IoMT devices and cloud-based services. An integrated AI-powered zero-trust cybersecurity solution is needed to ensure that modern smart healthcare systems can be protected in real time and dynamically to scalable and adaptive security levels.

Table 1 illustrates that current cybersecurity frameworks for the health sector offer limited coverage of AI supporting security capabilities and no support for implementing a zero-trust approach. In most cases, existing methods suffer from high latency, low scalability or limited adaptability in dynamic health care applications. In contrast, the proposed framework leverages full AI support and zero-trust security principles to enhance the accuracy of threat detection, efficiency of authentication, and overall healthcare cybersecurity resilience.

Table 1. Comparative Analysis of Existing Healthcare Cybersecurity Framework

Ref	Technique	AI Support	Zero-Trust Support	Healthcare Specific	Limitation
Existing Work 1	Blockchain	Partial	No	Yes	High latency
Existing Work 2	ML IDS	Yes	Partial	No	Poor scalability
Existing Work 3	Access Control	No	Yes	Yes	Static policy
Proposed	AI + ZTA	Full	Full	Full	Reduced limitations

3. Proposed AI-Enabled Zero-Trust Framework

3.1 Overall Architecture

The proposed AI-driven zero-trust approach aims to deliver secure, adaptive, and real-time protection for the smart healthcare infrastructure. Architecture includes integration of IoMT devices, edge gateways, identity verification services, AI-based threat detection, zero trust policy enforcement, cloud healthcare servers, secure storage and SIEM-based monitoring. The primary goal of the framework is to keep no users, devices or network requests trusted by default, not even those within the healthcare network.

In Figure 1, doctors, patients, and hospital managers interact with health care services via connected IoMT devices and edge gateways, while remote users use the same edge gateways to access the health care services. It generates medical data, telemetry and access requests, all of which are sent for verification to the zero-trust security layer. The components of the zero-trust layer are identity verification, multi-factor authentication, policy enforcement point and dynamic trust evaluation engine. Constantly all accesses are checked for the user, device, user pattern, location and risk score.

The AI threat detection engine processes authentication logs, IoMT traffic, access patterns and device behavior to determine potential cyber-attacks. The modules of behavioral analytics, and anomaly detection, compute risk scores and threat alerts that are returned to the zero-trust controller to make adaptive decisions. The system allows, denies, or limits access to health care resources according to risk level.

Authorized requests are sent to the cloud and data layer which includes the cloud healthcare server, electronic health records, medical database, SIEM dashboard and secure storage. The SIEM dashboard offers real time security monitoring and incident visibility. The continuous authentication and threat monitoring flow allows the system to continuously assess whether the user has access, not only when they log in but throughout the session.

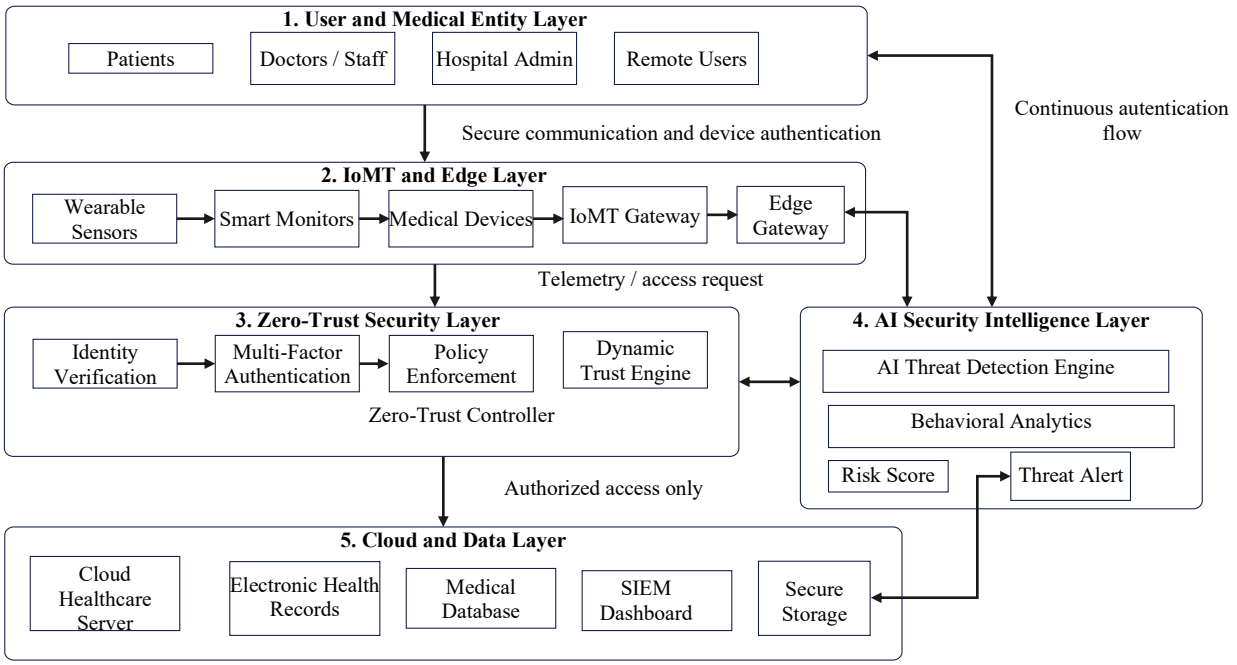

Fig. 1. Overall AI-Enabled Zero-Trust Smart Healthcare Security Architecture.

This architecture represents the user interactions among healthcare users and IoMT devices, the zero-trust security control, AI-driven threat intelligence, and secure cloud healthcare services. The architecture consists of four components: adaptive authentication, real-time threat detection, dynamic trust scoring, and secure medical data access control, which work together to enhance the cybersecurity resilience of the system.

3.2 AI-Based Threat Detection Module

The AI threat detection module constantly tracks the activities on the healthcare network, analyzes behavior and flags out malicious activities in real time. The module is designed to be a smart cybersecurity layer that can be coupled with the zero-trust model to deliver more accurate attack detection and adaptive security enforcement. The planed system uses feature extraction and behavior monitoring, deep learning based classification, and dynamic risk scoring algorithms to detect suspicious events on the healthcare network.

First, and most importantly, network traffic, authentication logs, IoMT communication patterns, device telemetry, and user access logs are gathered from the healthcare devices and edge gateways. Side effects of feature extraction techniques are used to generate important security features including login frequencies, rate of packet release, identity pattern of the device, number of failed authentication attempt, anomaly in communication, and unusual behavior in resource usage. The extracted features are passed on to the behavioural monitoring engine, which is constantly monitoring the features and detecting anomalies. The behavior monitoring process continuously monitors user-device interactions, consistency of communications, patterns of sessions and access to resources, and identifies deviations from typical operational behavior within the health care system.

The proposed framework uses deep learning and machine learning models such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, or Random Forest classifiers for threat detection and attack classification. CNN models are applied to network traffic data to detect spatial attack patterns and LSTM models are used to model the sequential and time-dependent healthcare communication behavior, thereby detecting evolving cyber threats. Random Forest classifiers are used for comparative analysis as they have efficient classification ability with relatively low computational complexity. Within a smart healthcare context, a CNN-LSTM framework enhances the identification of advanced attacks, including ransomware, breach attempts, insider threats, malicious IoMT communication scenarios.

The framework also presents a new dynamic trust score model to assess user and device trustworthiness as an adaptive security decision-making aid. As shown in Equation (1), the trust score is determined by the authentication behavior, device security condition and user context information.

$$T_s = \alpha A_b + \beta D_s + \gamma U_c, \quad (1)$$

Where T_s represents the dynamic trust score, A_b denotes the authentication behavior score, D_s represents the device security score, and U_c indicates the user context score. The parameters α, β, and γ are weighting coefficients used for adaptive trust computation based on healthcare network security requirements.

The dynamic analysis of authentication patterns, device integrity and contextual access behavior in (1) allows trust to be continuously evaluated. The calculated trust value is then passed to the Zero-Trust controller for adaptive authorization and for a context-aware enforcement of security. Healthcare system access is either limited or denied if the calculated trust value is below a set threshold, safeguarding that it will not be accessed by others. This dynamic trust evaluation mechanism further enhances healthcare cybersecurity by supporting intelligent, real-time, and adaptive threat mitigation in the proposed zero-trust architecture.

3.3 Zero-Trust Authentication Workflow

The proposed smart healthcare infrastructure is based on the zero-trust authentication workflow which aims to continuously and adaptively verify users, devices, and healthcare applications. The proposed workflow is different from the traditional way of authentication, which is based on the one-time process. The proposed architecture continuously validates user identity, device trustworthiness, and behavioral patterns before granting or maintaining access to the health care resources. This enhances the cyber security defense of unauthorized access, insider threats, compromised IoMT devices and credential based attacks.

The authentication process starts when the user logs in (see Figure 2), with healthcare workers, administrators or remote users making requests to access the healthcare system. At the identity verification stage, user credentials are then verified with multi-factor authentication methods such as passwords, biometric verification, one-time authentication tokens and contextual access validation. There are also device fingerprinting mechanisms in place that check the authenticity of the device based on various hardware identifiers, device configuration profiles, communication signatures and network attributes. This helps to ensure that only trusted devices can communicate with the healthcare network.

Following successful identity verification, the AI behavior analysis module continuously evaluates user activities, device interactions, session behavior, and network communication patterns to detect anomalous or suspicious activities. The behavioral information produced is sent to the module that generates risk scores and dynamically calculates risk levels based on the consistency of authentication, security status of the device, context of access information, and detected anomalies. Finally, the calculated risk score is checked as part of the policy validation phase to see if the access request meets the predetermined security policies and access rules in healthcare regulations implemented to enforce zero-trust security.

When the calculated trust level meets the predetermined level of security, access to the desired healthcare resources is allowed; otherwise the access to those resources is denied to prevent access to the system. The process also includes periodic monitoring of sessions, which involves re-checking users and activities as the session runs. The mechanism will be a continuous verification process, allowing for enforcement of security in real-time and quick response in the case of threats in dynamic healthcare environments.

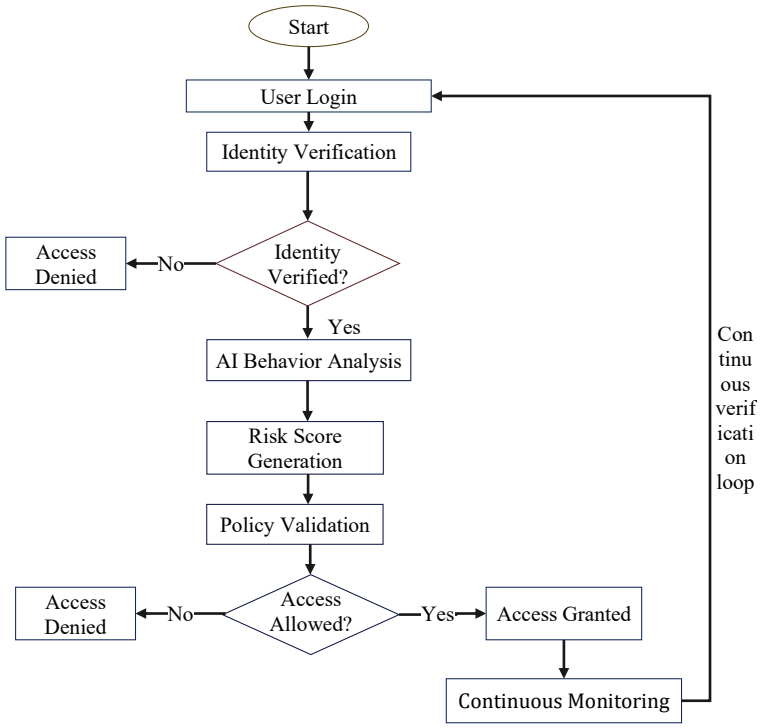

Fig. 2. Zero-Trust Authentication and AI-Based Threat Analysis Workflow

This flowchart outlines the general authentication and threat assessment process embedded in the suggested AI driven zero-trust security for healthcare.

3.4 Threat Classification Model

This proposed threat classification model aims to detect and classify cyberattacks within the context of smart healthcare infrastructure systems using artificial intelligence and deep learning methods. The model works by analyzing the healthcare network traffic, the authentication logs, the IoMT communication behavior and access request patterns and realises the detection of known and unknown cyber threats in real time. The classification framework integrates machine learning with deep learning techniques to enhance attack detection, accuracy in detection classification and adaptive cybersecurity decision making.

The proposed framework is then applied to the CICIDS2017 dataset and simulated healthcare IoT traffic data to evaluate the experimental results. The CICIDS2017 dataset comprises various types of attacks such as Brute Force, Denial of Service, Infiltration, Botnet, Web and Malicious Network Traffic Patterns. IoT traffic datasets are included to simulate realistic communication patterns between different types of IoT sensors/transceivers, smart monitoring systems, and medical imaging devices and the cloud-based healthcare platform. The merged data set allows for the proposed model to become trained with general cybersecurity attack patterns and healthcare-specific network anomalies.

Standard cybersecurity performance metrics such as accuracy, precision, recall and F1-score are used to assess the performance of the threat classification model. Accuracy is the overall correctness of attack classification and precision is the percentage of attacks correctly identified by LK from all attacks detected. The ability to detect real attacks is measured by recall, while the F1-score offers a balanced measure between precision and recall. The metrics are used to evaluate the reliability and effectiveness of the proposed AI-based zero-trust security framework.

The proposed framework utilizes probabilistic deep learning classification function for multi-class cyberattack detection. The probability of a particular attack type, which is used in Equation (2), relies on the output of the AI classification in a normalized fashion.

$$P(A_i|X) = \frac{e^{f(X_i)}}{\sum_{j=1}^{n} e^{f(X_j)}}, \quad (2)$$

Where $P(A_i|X)$ represents the probability of the detected attack class for input data X, $f(X_j)$denotes the output generated by the AI classifier for attack category i, and $n$represents the total number of attack categories considered in the classification model.

Equation (2) is used for multi-class attack classification to transform the output of classifiers into attack scores. The probability values that are produced are employed to identify the most likely attack category in the case of healthcare network traffic and user behaviour patterns. The proposed framework has enhanced the ability of this probabilistic deep learning inference mechanism to detect complex and evolving cyber threats in smart health care environments. Additionally, in the context of the zero-trust healthcare model, deep learning algorithms are used to estimate attack probability, enabling dynamic threat response, intelligent threat policy management, and real-time cybersecurity monitoring.

4. Experimental Setup

The experimental setup aimed to test the proposed AI-based zero trust cybersecurity framework in smart healthcare networks. The environment for the simulation encompasses IoMT traffic behavior, authentication information, AI-based threat classification, trust scoring that changes over time, and zero-trust access control decisions. This setup directly enables the aforementioned threat detection module, trust score model, authentication workflow and attack classification function.

4.1 Simulation Environment

The experiments are executed with the help of Python 3.10 which has excellent support for cybersecurity data processing, machine learning model making, and deep learning classification. The preprocessing, feature extraction, model training and evaluation processes were executed with the help of NumPy 1.24, Pandas 2.0, the Scikit-learn 1.3, TensorFlow 2.14, and PyTorch 2.0. TensorFlow was primarily utilized during the construction of CNN-LSTM models and Scikit-learn was used for some Random Forest comparisons and metric evaluation.

Several of the simulations were run in a Google Colab Pro environment with an NVIDIA Tesla T4 GPU, 16 GB GPU memory, 25 GB system RAM, and 100 GB temporary storage. The model is also capable of being run locally on a GPU with at least 8 GB VRAM, such as an NVIDIA RTX 3060/3070. Training time was cut down using GPU acceleration and it was ensured that the deep learning-based attack classification was done in an efficient manner.

The CICIDS2017 and simulated healthcare-IoT traffic is used for the experimentations. CICIDS2017 was chosen because it comprises of realistic benign and malicious traffic classes, such as DoS, DDoS, brute-forcers, botnets, infiltration, web attacks and port scan patterns. Additional simulated IoMT traffic from wearable sensors, smart monitors, medical devices, edge gateways, cloud healthcare servers and remote access users was added for a dataset to match the smart healthcare infrastructure. The healthcare IoT traffic comprised of normal telemetry data transmission, login requests, login log, session activities, failed login attempts, abnormal packet rate and suspicious device behavior.

The whole data set has been partitioned into 80% training, 10% validation and 10% testing. To eliminate the scale effects of the features, Min-Max scaling was applied, while categorical attack labels were converted to One-Hot encoding for deep learning classification. The features extracted were: Packet Duration, Protocol type, Source and Destination Behavior, Failed login count, Device trust status, Session frequency, Packet rate, Access time, Authentication score, and Contextual user activity. These features are used in both Equation (1) to compute the dynamic trust score and Equation (2) for probabilistic attack classification.

The CNN-LSTM model was trained for 100 epochs with a batch size of 64 and learning rate of 0.001, and trained with the Adam optimizer. Random Forest was ran with 100 decision tree to run the baseline. All models

evaluated with the same test data to ensure a fair evaluation. This configuration allows for comparison of the accuracy, precision, recall, F1-score, false positive rate, authentication latency, and overall decision efficiency of zero-trust in the results section to come.

4.2 Evaluation Metrics

Various cybersecurity and system-level performance metrics were used to assess how the proposed AI-based zero-trust cybersecurity framework effectively detects attacks, enables efficient authentication, and supports secure healthcare communication. The metrics are chosen to support the AI-based threat detection module, zero-trust authentication workflow, dynamic trust evaluation model and probabilistic attack classification framework that were introduced in the previous sections.

The proposed CNN-LSTM hybrid model was tested and evaluated for its capability to correctly classify normal and malicious healthcare network traffic using detection accuracy. The accuracy is the proportion of the attack and benign samples that are classified correctly out of all samples that are classified. The accuracy-prediction of ransomware attacks along with unauthorized logins, abnormal communication activity of IoT devices, and network intrusion in smart healthcare system environments is good.

To measure the false positive rate, it was calculated by finding what percentage of the normal healthcare activities were misidentified as cyberattacks. Excessive false positives in healthcare systems can lead to delays in clinical communication, overburdening of authentication processes, and causing disruptions in healthcare operations. Hence, the need to reduce false alarms is very crucial in keeping healthcare service available and efficient in security monitoring.

The time needed for user verification, trust evaluation, policy validation, and access authorization in the zero-trust environment was measured as authentication latency to analyze this. Low authentication latency is critical to ensure the operational efficiency and emergency response capability of the smart healthcare system, as they need real-time medical communication and instant access to patient data.

To assess the ability of the proposed framework to handle authentication requests in the healthcare field and network traffic under varying conditions of IoMT communication, throughput was measured. High throughput translates into scalable and effective management of multiple health-care devices as well as multiple users and simultaneous access sessions without appreciable degradation in throughput.

The simulation setting and experimental parameters for analyzing the proposed framework are summarized in Table 2. These parameters directly contribute to the AI-based threat classification model, the trust score computation mechanism and authentication workflow explained in previous sections and also present the basis for the performance comparison presented in the results and discussion section that follows.

Table 2. Experimental Parameters and Simulation Configuration

Parameter	Value
Dataset	CICIDS2017 + Simulated Healthcare IoMT Traffic
Training Split	80%
Validation Split	10%
Testing Split	10%
Learning Rate	0.001
Batch Size	64
Epochs	100
Optimizer	Adam
Feature Scaling	Min-Max Normalization
AI Model	CNN-LSTM Hybrid
Baseline Comparison Models	Random Forest, CNN, LSTM
Hardware Platform	NVIDIA Tesla T4 / RTX 3060 GPU
Programming Language	Python 3.10
Deep Learning Framework	TensorFlow 2.14 / PyTorch 2.0
Evaluation Metrics	Accuracy, Precision, Recall, F1-Score, FPR, Latency
Simulation Environment	Google Colab Pro

5. Results and Discussion

5.1 Threat Detection Performance

The proposed AI-based ZTC cyber security framework's threat detection capability was tested on the CICIDS2017 dataset and simulated healthcare IoT traffic. The experimental study was conducted to evaluate the proposed CNN-LSTM hybrid model's ability to accurately detect malicious activities of HNs, unauthorized access attempts, abnormal communication behaviors of IoMTs, and cyber-attacks on smart HIs. The outcome results prove that the combination of threat analysis using deep learning and dynamic zero-trust security enhances the capabilities of detecting attacks and improves adaptive healthcare cybersecurity performance.

The proposed CNN-LSTM hybrid model was found to provide the highest attack detection accuracy of 98.7% as shown in Figure 3, which is better than conventional machine learning and deep learning models such as SVM, Random Forest, CNN and LSTM alone models. SVM classifier was achieved an accuracy of 89.4% and Random Forest gave the accuracy of detection as 92.1%. The CNN-based deep learning model and LSTM models achieved the performance with accuracy of 95.6% and 96.8% respectively. The CNNs and LSTMs were found to be complementary in capturing various cybersecurity features in health network traffic and user authentication behavior, respectively, with the proposed hybrid CNN-LSTM system showing the best performance.

This enhancement of the proposed model is primarily due to the combination of convolutional feature extraction and sequential behavioral learning. CNN layers were good at detecting hidden attack signatures and packet-level traffic anomalies while LSTM layers were good at detecting time-dependent behavior patterns in healthcare communication and evolving attack signatures. This blended learning mechanism allowed for the effective detection in a smart healthcare setting of ransomware attacks, denial of service attacks, authentication attacks with bad credentials, insider threats, and abnormal device behavior from IoMT devices.

Moreover, the framework with AI showed that the proposed framework achieved high efficiency in detecting attacks in the healthcare system. AI-driven behavioural monitoring combined with zero-trust policy validation, significantly minimised misclassification and enhanced adaptive threat response. These findings validate the proposed framework as scalable, intelligent and real-time cybersecurity defense solutions of next generation smart healthcare infrastructure.

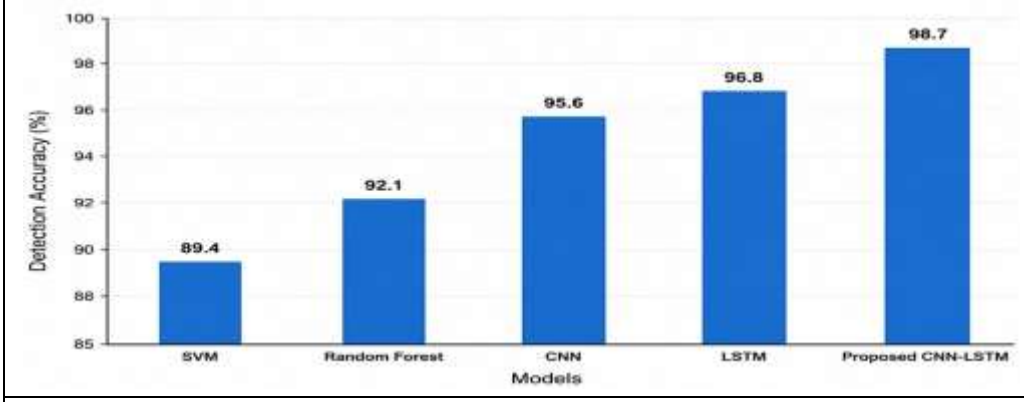

Fig. 3. Attack Detection Accuracy Comparison of Machine Learning and Deep Learning Models

The figure shows the comparative performance analysis of SVM, Random Forest, CNN, LSTM and the proposed CNN-LSTM hybrid threat classification model.

5.2 Authentication Latency and Security Analysis

Evaluation of real-time operational efficiency of the proposed AI-enabled zero-trust cybersecurity framework under varying healthcare authentication workloads was carried out by analyzing the authentication latency and security analysis. This analysis was based upon the measurement of the authentication response time,

zero-trust verification overhead, and the continuous monitoring performance in a dynamic communication situation within the healthcare sector, which involves multiple end-users, IoMT devices, edge gateways, and cloud-based healthcare services. It is important to establish reliable healthcare operation, as smart healthcare systems need quick access to medical information and real-time communications while having to make sure they are protected against cyber threats, with a low authentication latency.

With the number of authentication requests, authentication latency is linearly increasing for all security frameworks as shown in figure 4. But the proposed AI-based zero-trust system always outperformed the traditional zero-trust system in terms of security enforcement and lower latency. Traditional security mechanisms were the least time-efficient in terms of initial authentication latency, as they are based on limited authentication methods and perimeter-based access control. Yet these methods only offer limited coverage from dynamic cyberattacks, insider attacks, and compromised devices.

The traditional Zero Trust approach added considerable authentication delays with frequent identity verifications, ongoing policy enforcement, and continuous trust checks. The traditional zero-trust approach incurred around 279 ms latency after 1000 authentication requests in a large healthcare communication environment, which suggests that the approach incurs significant authentication burdens. By contrast, the proposed AI-powered zero trust approach achieved latency of ~183ms at the same workload level by evaluating trust intelligently and using adaptive AI-assisted authorization policies.

The AI-powered behavioral analysis and adaptive trust scoring systems are two key factors in boosting the proposed framework's reduced latency. To streamline security decision-making, the framework continuously analyzes aspects of user behavior, device trust status, contextual access information and session consistency, and no longer needs to repeatedly perform computationally expensive authentication procedures for every authentication request. An adaptive and trust-based verification reduces the number of unnecessary authentication operations, while providing robust cybersecurity protection.

In addition, the continuous monitoring mechanism was shown to be effective in the security evaluation in real-time in an increasing workload of authentication. No too significant communication overhead or in terms of system performance degradation was incurred as trust scores and security policies were dynamically updated. The results show that the proposed framework achieved a good balance of cybersecurity strength and operational efficiency, thereby being suitable for large smart healthcare systems that require secure and low-latency communication.

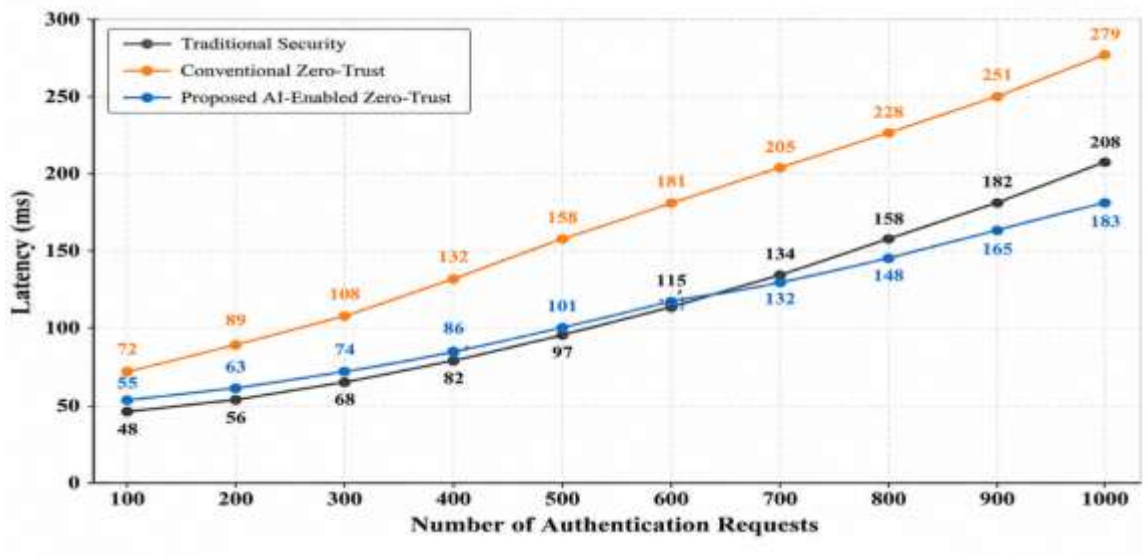

Fig. 4. Authentication Latency versus Security Level Analysis

The graph shows the latency performance for traditional security, conventional zero-trust, and proposed AI-powered zero-trust security for different authentication request volumes.

6. Discussion

The findings of the experimental analysis are presented and it is found that the proposed AI-based zero-trust cybersecurity framework has successfully achieved the balanced intelligent threat detection, adaptive authentication, and real-time operational efficiency of the smart healthcare infrastructure. Overall, the use of deep learning threat analysis combined with continuous trust evaluation was a clear improvement in healthcare security infrastructure over traditional security networks and conventional zero trust models. The CNN-LSTM hybrid model proposed in this article successfully improved attack detection accuracy with lower authentication latency in the context of growing workloads in healthcare communications. These results demonstrate the potential of supporting secure and scalable healthcare environments with heterogeneous IoMT devices, cloud platforms and remote medical access systems.

The scalability analysis results are consistent and show that the proposed framework will scale well to handle and support the incorporation of a larger number of authentication requests and network traffic in the healthcare network without significant performance degradation. The AI-based trust assessment process minimizes authentication repetition by proving automatic trust assessment through dynamic user behavior, device integrity, and contextual information. The following adaptive verification method allows large-scale healthcare systems to be managed efficiently, with wearable sensors, smart monitors, medical imaging systems, edge gateways, and cloud-based healthcare servers. Under heavy authentication traffic conditions, the observed response time growth was still under control, which showed that the framework would be suitable for real-time healthcare applications where the need to have continuous secure communication, with medical data being accessible in real time.

The proposed approach is also suitable for real-world deployment and can be easily adapted to current healthcare architectures involving cloud computing, edge intelligence, and IoMT communication networks. The modular design of the framework enables its installation in hospitals, remote Healthcare Monitoring Systems, telemedicine systems, smart clinical environments, etc. Edge gateways and distributed AI-based monitoring contribute to the ease of deployment, allowing for security analysis at the edge and offloading the central computing system. However, the deployment might need further optimization for resource constrained medical devices with limited processing capability and battery power resources.

While AI systems have made great strides in enhancing functionality, transparency and understanding play a critical role in healthcare cybersecurity. It is difficult to interpret security decisions and attack classification outputs in deep learning models like CNN and LSTM, they are typically black box models. Explainable security decisions are crucial as misclassifications can create threats that interfere with clinical functions and/or impact EHS delays time to service.In healthcare settings, explainable security decisions are fundamental because improperly classified threats could hinder clinical operations and/or cause EHS delays. Thus, incorporating Explainable Artificial Intelligence (XAI) mechanisms could lead to greater transparency and trust in decision-making regarding cybersecurity solutions made by artificial intelligence.

Preserving privacy is another area of great importance when thinking of smart healthcare cybersecurity. Healthcare systems handle patient information that is sensitive in nature and sharing unauthorized information or misuse of medical records can lead to significant legal and ethical consequences. These elements in the proposed framework enhance the level of privacy protection, with continuous authentication, dynamic trust validation, secure communication channels, and access control enforcement. However, future implementations need to better incorporate approaches for protecting data privacy, such as federated learning and secure multi-party computation, to reduce the amount of centralized exposure of healthcare data.

Compliance is a critical factor for successful deployment of healthcare cybersecurity. The proposed framework also meets the security needs of the healthcare industry, aligning with the major regulatory standards like the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). These all help to meet healthcare privacy and cybersecurity standards. For large-scale, real-world

healthcare environments, however, there might be a need for more auditing and encryption management and patient consent processing processes.

7. Conclusions and future work

The study introduced the Artificial Intelligence Enabled Zero-Trust Cyber Security Framework for leveraging smart healthcare infrastructure to tackle the ever-increasing cyber security challenges with the IoMT devices, cloud-based smart healthcare service platforms, and intelligent medical communication and transmission systems. The proposed framework included a combination of zero-trust authentication, AI-driven threat detection, behavioural monitoring, dynamic trust evaluation, and adaptive access control to ensure constant, intelligent and advanced healthcare cybersecurity protection. This framework integrated CNN and LSTM deep learning models to boost the accuracy rate of cyberattack classification and the capability of real-time cyberattack detection in the healthcare industry.

Experimental testing was performed using the CICIDS2017 dataset and simulated traffic from healthcare IoMT, which showed that the proposed approach outperformed the conventional zero-trust and traditional machine learning methods in terms of cybersecurity. It is observed that the proposed CNN-LSTM hybrid model represents the best results in terms of attack detection accuracy and minimized authentication latency as the load of the healthcare authentication increased. AI-powered trust assessment and ongoing monitoring optimized adaptive threat response, minimized false positive alerts, and ensured improved communication security in healthcare. Moreover, the proposed framework exhibited high scalability and applicability in the large-scale smart healthcare environment, where access to medical data must be secure, low latency, and real-time.

The study also shed light on the benefits of adaptive trust management in zero-trust healthcare environments using AI technology. The framework dynamically optimizes authentication decisions and reduces unwanted verification overhead by constantly analyzing the behaviour of the device and the user, contextual access information, and communications. This adaptive security solution enhanced the security of the healthcare infrastructure against insider threats, compromised IoMT devices, attempts to access the network without authorization, and developing cyber-attacks.

Future work will address incorporating federated learning mechanisms for supporting decentralized and privacy-preserving healthcare cybersecurity model training efforts among several healthcare institutions. Additionally, blockchain-based trust management will be explored to enable decentralized authentication and security authentication of healthcare transactions, as well as tamper-resistance audit logs. Furthermore, future research will include lightweight deployment strategies for Edge AI for resource-poor healthcare devices and edge gateways that enhance real-time threat detection at the edge. Last but not least, quantum resistant healthcare security mechanisms using the post-quantum cryptographic techniques will be explored to improve the long term security in emergent quantum computing-based cyber-attack on future smart healthcare systems.

References

1. Alsubaei, F., Abuhussein, A., & Shiva, S. (2017, October). Security and privacy in the internet of medical things: Taxonomy and risk assessment. In 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops) (pp. 112–120). IEEE.
2. Al-Turjman, F., Nawaz, M. H., & Ulusar, U. D. (2020). Intelligence in the Internet of Medical Things era: A systematic review of current and future trends. Computer Communications, 150, 644–660.
3. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419.
4. Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: A comprehensive survey. IEEE Access, 3, 678–708.

5. Kim, J., Kim, J., Thu, H. L. T., & Kim, H. (2016, February). Long short term memory recurrent neural network classifier for intrusion detection. In 2016 International Conference on Platform Technology and Service (PlatCon) (pp. 1–5). IEEE.
6. Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., & Douligeris, C. (2020). Security in IoMT communications: A survey. Sensors, 20(17), 4828.
7. Kumar, P., Kumar, R., Gupta, G. P., & Tripathi, R. (2021). A distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT systems by leveraging fog computing. Transactions on Emerging Telecommunications Technologies, 32(6), e4112.
8. Rahmani, A. M., Gia, T. N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., & Liljeberg, P. (2018). Exploiting smart e-health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Generation Computer Systems, 78, 641–658.
9. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. NIST Special Publication 800-207, 1–52.
10. Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects. Annals of Data Science, 10(6), 1473–1498.
11. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.
12. Sodhro, A. H., Pirbhulal, S., & De Albuquerque, V. H. C. (2019). Artificial intelligence-driven mechanism for edge computing-based industrial applications. IEEE Transactions on Industrial Informatics, 15(7), 4235–4243.
13. Sun, Y., Lo, F. P. W., & Lo, B. (2019). Security and privacy for the internet of medical things enabled healthcare systems: A survey. IEEE Access, 7, 183339–183355.
14. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525–41550.
15. Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang, Y., & Zhu, M. (2017). HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. IEEE Access, 6, 1792–1806.