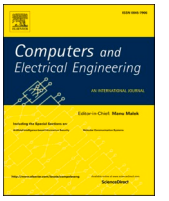
Computers and Electrical Engineering 129 (2026) 110808

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng



Enhancing internet of medical things security: A multi-layered approach using dynamic adaptive deep reinforcement learning and blockchain

Nikhil Sharma *, Prashant Giridhar Shambharkar

Department of Computer Science & Engineering, Delhi Technological University, Delhi, India

ARTICLE INFO

Keywords:
Blockchain
Interplanetary file system
Intrusion detection system
Deep learning
Internet of Medical Things
Zero-Knowledge Proofs

ABSTRACT

With the rapid proliferation of Internet of Medical Things (IoMT) systems, securing sensitive healthcare data and detecting cyber threats in real time has become a significant challenge. Existing solutions often fall short in scalability, adaptability, and data integrity. To address these limitations, this study proposes a comprehensive and intelligent security framework that integrates blockchain technology, deep learning, and advanced cryptographic mechanisms. The framework introduces a novel Dynamic Adaptive Deep Reinforcement Learning (DA-DRL) model for real-time AES key generation, improving resilience against evolving threats. A multi-layered security architecture incorporating SHA-512, Zero-Knowledge Proofs (ZKPs), Practical Byzantine Fault Tolerance (PBFT), and Attribute-Based Access Control (ABAC) ensures confidentiality, integrity, and secure access management. Furthermore, InterPlanetary File System (IPFS) is utilized for decentralized, tamper-proof storage of encrypted healthcare records. For intrusion detection, a hybrid deep learning model i.e., Secure and Dependable BiLSTM-GRU Intrusion Detection Model (SD-BiLSTMGRU-IDM) is developed, capturing bidirectional temporal dependencies to improve detection accuracy. The proposed model achieves 99.35% accuracy and a 99.32% F1-score, outperforming existing methods by 5.87%. Additionally, it maintains low latency (0.324 s), high throughput (72 Tx/sec), and minimal network overhead (1.41%). These contributions collectively present a scalable, adaptive, and secure framework for intrusion detection and data protection in real-world IoMT healthcare environments.

1. Introduction

The digital transformation of healthcare has ushered in a new era of data-driven medical services, fueled by technologies such as the Internet of Medical Things (IoMT), Electronic Health Records (EHRs), wearable sensors, and cloud computing [1]. These innovations have enabled real-time patient monitoring, personalized care, and predictive diagnostics, significantly enhancing the quality and efficiency of healthcare delivery [2]. However, this technological advancement also introduces new and complex security challenges. The highly sensitive nature of healthcare data makes it a prime target for cybercriminals. Reports of data breaches, ransomware attacks, and unauthorized access have become alarmingly frequent, threatening patient privacy, operational continuity, and institutional trust [3]. Traditional security approaches in healthcare systems are increasingly inadequate in mitigating evolving threats.

* Corresponding author.
E-mail address: nikhilsharma_2k21phdco04@dtu.ac.in (N. Sharma).

https://doi.org/10.1016/j.compeleceng.2025.110808
Received 12 November 2024; Received in revised form 23 September 2025; Accepted 22 October 2025
Available online 28 October 2025

Most rely on centralized architectures with static encryption and limited intrusion detection capabilities. Such systems are vulnerable to single points of failure, lack dynamic adaptability, and often fall short in meeting regulatory requirements for privacy and data governance [4]. Furthermore, the proliferation of interconnected devices in IoMT environments has dramatically expanded the attack surface, requiring novel, scalable, and context-aware security frameworks that go beyond conventional methods. In recent years, blockchain technology has emerged as a transformative force in securing distributed digital ecosystems [5]. Its inherent features of decentralization, immutability, and transparency make it particularly well-suited for addressing the limitations of centralized healthcare systems. When integrated with advanced cryptographic algorithms and artificial intelligence (AI)-driven threat detection, blockchain can offer a holistic security solution [6]. However, despite its potential, the application of blockchain in healthcare is still in its nascent stages. Existing implementations often grapple with key management complexities, scalability bottlenecks, and the inability to ensure real-time data processing in dynamic environments [7].

To address these multifaceted challenges, this study proposes a robust and scalable security framework specifically designed for modern healthcare systems. The framework combines the strengths of blockchain technology, advanced encryption mechanisms, dynamic key management, decentralized storage, and intelligent intrusion detection. At its core, it introduces an adaptive key generation mechanism using deep reinforcement learning. Unlike static key models, this dynamic approach evolves continuously by learning from the environment, enabling it to resist advanced threats and adapt to emerging attack vectors. Moreover, the proposed security model incorporates a multi-layered architecture that integrates symmetric encryption, hash-based data integrity checks, privacy-preserving authentication protocols, and consensus mechanisms tailored for fault-tolerant environments. This layered design ensures that data confidentiality, integrity, and availability are maintained across the healthcare data lifecycle. Data is encrypted using symmetric cryptographic algorithms and stored in a decentralized manner using the InterPlanetary File System (IPFS), which enhances data redundancy, ensures availability, and mitigates the risks associated with centralized storage systems [8].

To enable secure access control and authorization, the framework adopts a context-aware model based on user, resource, and environmental attributes [9]. This granular policy enforcement prevents unauthorized data access and ensures compliance with healthcare regulations. Transactions and data operations within the network are validated using a consensus protocol designed to withstand adversarial conditions, guaranteeing that only authorized actions are recorded on the blockchain ledger. Another pivotal component of the proposed system is a hybrid deep learning model tailored for intrusion detection. By leveraging bidirectional recurrent neural networks, the model captures both past and future contextual dependencies in network traffic patterns, thereby improving the detection accuracy of sophisticated, multi-stage cyberattacks. The integration of this model with encrypted data analytics enables real-time threat monitoring without compromising data privacy. The framework is deployed on a permissioned blockchain platform optimized for enterprise-grade security and scalability. The modular architecture supports private data channels, fine-grained access policies, and flexible governance models, making it particularly suited for applications involving confidential medical records, inter-institutional collaborations, and remote patient monitoring systems. This study provides a comprehensive view of how emerging technologies can be effectively harmonized to create a secure, intelligent, and privacy-preserving healthcare environment. The integration of blockchain, cryptography, and deep learning not only addresses current limitations in healthcare cybersecurity but also lays the groundwork for future-proofing medical data infrastructure. The proposed solution aligns with key data protection principles, such as data minimization, auditability, and privacy by design, offering a viable pathway for secure digital transformation in the healthcare domain.

1.1. Motivation

The digitalization of healthcare systems, driven by the proliferation of IoMT devices, electronic health records, and cloud-based services, has revolutionized patient care and medical data management. However, this digital shift has also made healthcare infrastructures increasingly vulnerable to cyber threats, including data breaches, ransomware attacks, and unauthorized access [10]. Given the critical and sensitive nature of medical data, ensuring its security, integrity, and privacy is of paramount importance. Conventional security approaches such as static key encryption, centralized data storage, and rule-based intrusion detection systems which are no longer sufficient to address the dynamic and evolving nature of cyber threats [11]. These methods lack adaptability, scalability, and resilience, especially in large-scale, real-time healthcare environments. This motivates the development of a novel, integrated framework that leverages blockchain technology, advanced encryption techniques, dynamic key generation using deep reinforcement learning, and intelligent intrusion detection through hybrid deep learning models. Such a system aims to ensure end-to-end protection of healthcare data while supporting scalability, real-time processing, and compliance with stringent privacy regulations. Our goal is to bridge existing gaps in healthcare cybersecurity by proposing a practical, future-proof solution capable of protecting sensitive data against modern threats, thereby fostering greater trust, safety, and reliability in digital healthcare ecosystems.

1.2. Contribution

This section presented major contributions that advance the state of security and detection systems in healthcare environments. Each contribution addresses key challenges and introduces novel solutions to enhance encryption, data protection, storage, transaction management, scalability, and intrusion detection, which are explained as follows:

- Dynamic Adaptive Deep Reinforcement Learning for Key Generation: We introduced Dynamic Adaptive Deep Reinforcement Learning (DA-DRL) for real-time, adaptive key generation in AES encryption. Unlike existing static key management techniques,

DA-DRL continuously evolves in response to security threats, learning optimal encryption strategies dynamically. This ensures enhanced resilience against emerging cyberattacks.

- Multi-Layered Security Framework for Healthcare Data Protection: We designed a novel multi-layered security framework by integrating AES, SHA-512, Attribute-Based Access Control (ABAC), Practical Byzantine Fault Tolerance (PBFT), and Zero-Knowledge Proofs (ZKPs). Unlike traditional single-layered security models, our framework simultaneously addresses multiple security concerns like encryption, authentication, access control, and consensus, providing end-to-end protection for healthcare environments.
- Decentralized and Immutable Data Storage with IPFS: We leveraged InterPlanetary File System (IPFS) to enable tamper-proof, decentralized storage of encrypted healthcare data. While IPFS is a known technology, its application in securing healthcare data is novel, ensuring data integrity, availability, and reduced storage overhead across distributed healthcare networks.
- Blockchain-Cryptography Fusion for Secure Transaction Management: We developed a hybrid blockchain-cryptographic approach that ensures transaction authenticity and integrity in healthcare systems. Unlike conventional centralized transaction models, our method combines distributed ledger security with advanced cryptographic proofs, mitigating risks of tampering, unauthorized access, and data breaches.
- Scalable and Adaptive Model for Large-Scale Healthcare Systems: We architected a scalable and real-time adaptable security system optimized for large-scale healthcare applications. By integrating dynamic key optimization mechanisms, our model efficiently handles high data loads and evolving security threats, overcoming the scalability issues of existing healthcare security solutions.
- Secure and Dependable BiLSTM-GRU Intrusion Detection Model (SD-BiLSTMGRU-IDM): We developed SD-BiLSTMGRU-IDM, a novel hybrid deep learning model that combines Bidirectional Long Short-Term Memory (BiLSTM) and Gated Recurrent Units (GRU) for high-accuracy intrusion detection. Unlike conventional models that only analyze forward dependencies, our approach captures bidirectional dependencies, significantly enhancing threat detection accuracy in complex attack scenarios.

Paper organization: The remainder of this paper is structured into five key sections. Section 2 provides a comprehensive review of the literature, highlighting the current challenges in intrusion detection systems (IDS), existing approaches, and the specific gaps that motivate the development of the proposed framework. Section 3 outlines the methodology in detail, including foundational concepts of blockchain technology, the overall system architecture, advanced encryption techniques, dynamic key generation using deep reinforcement learning, secure data storage through IPFS, decryption mechanisms, and the design of the DL-based IDS model. Section 4 presents the experimental setup, along with a thorough analysis of the system's performance across various evaluation metrics. Finally, Section 5 concludes the paper by summarizing the key findings and offering insights into potential directions for future research aimed at further enhancing data security and intrusion detection capabilities in healthcare environments.

2. Literature review

The integration of blockchain and deep learning technologies has gained momentum as a compelling strategy to enhance intrusion detection and security within healthcare and IoT environments. Yet, despite widespread interest, the literature reveals a lack of consensus on blockchain's specific role in such security architectures. Some researchers highlight blockchain's decentralized and immutable nature, emphasizing its potential for tamper-proof data management and secure transaction recording. Others, however, draw attention to critical concerns, particularly its limited scalability, increased latency, and computational overhead factors that hinder its effectiveness in real-time, resource-constrained systems. Barnett offers a balanced interpretation, viewing blockchain as both an enabler and a constraint: a technology that enhances data integrity and transparency, but one that also imposes performance trade-offs. This nuanced understanding is crucial, especially in sensitive sectors like healthcare, where data privacy, availability, and real-time access must be carefully balanced with security guarantees. To operationalize blockchain in healthcare security systems, researchers have proposed a range of architectural frameworks. Shamshad et al. [12], for instance, introduced a blockchain-based protocol for secure electronic health record (EHR) storage using private blockchains and public-key encryption. Tanwar et al. [13] implemented an access control mechanism within Hyperledger Fabric to streamline healthcare data sharing. Wang et al. [14] extended these models with GuardHealth, which incorporates a Graph Neural Network (GNN)-based trust framework to detect malicious nodes. Meanwhile, Zaabar et al. [15] explored OrbitDB with IPFS to facilitate decentralized and verifiable healthcare data storage, and Shukla et al. [16] proposed a hybrid model combining blockchain with fog computing to address latency and bandwidth issues in IoT environments. These implementations underscore blockchain's potential to reinforce healthcare data security, yet they also reveal persistent challenges, including high throughput demands and interoperability across systems. Emerging hybrid frameworks further reflect blockchain's expanding role in intelligent security systems. Rehman et al. [17] integrated federated learning with blockchain-based intrusion detection to enhance confidentiality without compromising learning performance. Azzaoui et al. [18] presented a Quantum Cloud-as-a-Service (QCaaS) model, combining quantum computing with blockchain to secure genomic data processing. Singh et al. [19] contributed a privacy-preserving federated learning model for smart cities that reduces cloud dependency while maintaining secure and decentralized data exchanges. Practical implementations such as Tomar et al.'s [20] BIoMTAKE protocol and Sharma et al.'s [21] blockchain-IoT architecture for verifying healthcare certificates illustrate the breadth of blockchain's applicability. In parallel, Mishra et al. [22] developed a decision support system using interval-valued Pythagorean fuzzy sets to evaluate blockchain solutions in healthcare supply chains, enabling more informed platform selection under uncertainty. Collectively, these studies highlight a transition in how blockchain is conceptualized, not merely as a secure data store, but as a dynamic layer within adaptive, privacy-preserving security architectures. However, they also converge on a shared limitation: the need for scalable, efficient models that can maintain strong security guarantees without incurring significant performance penalties. This gap informs the

design of the proposed model, which aims to unify blockchain, cryptography, and deep learning into a cohesive and scalable security framework tailored for modern healthcare environments. Table 1 shows the Comparative analysis of blockchain-based healthcare security frameworks.

The above existing work proposed by different researchers presents several limitations, which are discussed as follows:

(i) Insufficient Scalability Analysis

Many IDS studies fail to assess scalability in real-world environments, focusing on small-scale networks. Efficient intrusion detection requires handling high-volume traffic in real-time, but inadequate scalability analysis limits practical deployment due to computational constraints.

(ii) Lack of Discourse on Hyperparameter Tuning

Machine learning-based IDS models often rely on fixed or arbitrarily chosen hyperparameters, leading to suboptimal performance. Limited discussions on optimization techniques such as grid search, random search, and Bayesian optimization hinder model adaptability and effectiveness in dynamic network environments.

(iii) Inadequate Development of Integration of Deep Learning Models

Despite their potential, deep learning models are not seamlessly integrated into IDS frameworks. Key challenges include high computational costs, extensive labeled data requirements, and limited interpretability of model outputs. Addressing these concerns is crucial for real-world deployment.

(iv) Privacy Concerns

Intrusion detection often involves monitoring and analyzing network traffic, which can raise privacy concerns. Ensuring that IDS solutions comply with data protection regulations and respect user privacy while effectively detecting threats is a delicate balance that requires careful consideration and implementation.

3. Preliminaries

This section outlines the foundational principles of blockchain technology and its relevance to secure healthcare data management, which are explained as follows:

3.1. Blockchain overview

The proposed architecture leverages a decentralized ledger to maintain transparent and immutable medical records while ensuring patient confidentiality. By distributing transaction logs across multiple nodes, blockchain eliminates single points of failure and enables tamper-resistant data storage. Its inherent trust mechanism makes it highly suitable for safeguarding sensitive health information within a privacy-preserving and interoperable environment.

3.2. Blockchain architecture

The proposed blockchain architecture employs Hyperledger Fabric, a modular and permissioned platform well-suited for managing sensitive healthcare data. Its support for private channels ensures secure, confidential transactions, while its scalability enables effective deployment across large healthcare networks. To mitigate evolving security threats, the framework integrates a layered security approach, combining AES encryption, dynamic key management using Dynamic Adaptive Deep Reinforcement Learning (DA-DRL), SHA-512 hashing for integrity assurance, and Zero-Knowledge Proofs (ZKPs) for privacy-preserving verification. Practical Byzantine Fault Tolerance (PBFT) ensures secure consensus even under adversarial conditions, while Attribute-Based Access Control (ABAC) enforces granular access permissions based on user roles and contextual parameters. The architecture operates in two phases: Phase 1 securely stores encrypted data in the InterPlanetary File System (IPFS), and Phase 2 decrypts and analyzes this data using deep learning models for intrusion detection. Fig. 1 illustrates the proposed system, with a detailed discussion provided in the subsequent section.

3.3. Data management and privacy-preserving

This subsection provides an overview of the data management and privacy-preserving techniques, which are explained as follows:

3.3.1. Data encryption and decryption

Encryption and decryption play a vital role in securing delicate IoT data by converting it into protected formats during transmission and storage, ensuring only authorized access while preserving data integrity and preventing breaches or unauthorized modifications

Table 1
Comparative analysis of blockchain-based healthcare security frameworks.

Ref.	Blockchain Network Type	Finding	Pros	Cons	Cl	Sl	Tp	Au	Al	In	De	Di
Farouk et al. [23]	Permissioned Blockchain	Utilizing AI for data analysis and hybrid clouds for scalable applications enhances the overall effectiveness of IoT and blockchain implementations in healthcare.	Ensures secure data management and privacy preservation.	Ensuring correct access control to avoid data leakage is a significant challenge.	✓	×	✓	✓	×	✓	×	✓
Sharma et al. [24]	Permissioned Blockchain	The scheme ensures the privacy of medical big data by eliminating centralized control and mitigating privacy leakage risks.	Blockchain's inherent security features and smart contracts provide robust protection against unauthorized access and privacy breaches.	Blockchain systems may introduce performance overheads such as increased latency and lower throughput compared to traditional systems.	✓	×	✓	×	×	✓	✓	✓
Hossein et al. [25]	Permissioned Blockchain	BCHealth empowers data owners to set their desired access policies, ensuring better privacy and control over their healthcare data.	Clustering approach helps manage large volumes of data efficiently.	Integrating BCHealth with existing healthcare systems may require significant changes and adaptations.	✓	✓	✓	×	×	✓	✓	✓
Zhang et al. [26]	Permissioned Blockchain	The integration of pairing-based cryptography with blockchain ensures that EHRs are verifiable and protected from unauthorized modifications.	Combining blockchain with pairing-based cryptography ensures strong protection against unauthorized modifications and tampering.	The performance and scalability of the system could be impacted by the overhead associated with blockchain transactions and cryptographic operations.	✓	×	✓	×	×	✓	✓	✓
Chhikara et al. [27]	Permissioned Blockchain	The proposed framework utilizes blockchain technology to implement a robust authenticated access control system.	Ensures that only authorized entities can access and distribute medical materials.	Deploying and maintaining a blockchain-based access control system can be complex and require significant resources.	✓	×	✓	✓	×	✓	✓	✓
Moulahi et al. [28]	Permissioned Blockchain	Federated Learning ensures that personal data remains decentralized and private, mitigating risks associated with data centralization.	Addresses practical concerns in the medical field, such as data privacy and security, through an innovative approach.	Scaling the system to handle large volumes of data and numerous devices may pose challenges.	✓	×	✓	✓	×	✓	✓	✓
Taloba et al. [29]	Permissioned Blockchain	IoT integration helps in optimizing the distribution of healthcare resources and reducing costs while improving patient care.	Blockchain's hash-based record-keeping enhances data security and traceability.	The process of hashing and recording transactions on the Blockchain can introduce performance overhead.	×	×	✓	×	×	✓	✓	✓
Shari and Malip [30]	Permissioned Blockchain	The scheme ensures that malicious entities can be held accountable while maintaining patient privacy.	Sign-Proxy scheme provides robust security for data transmission while preserving privacy.	While the system is optimized for limited-resource devices, it may still face constraints in extremely low-resource environments.	✓	×	✓	✓	×	✓	✓	✓
Wang et al. [31]	Hybrid Blockchain	The $B+$ tree indexing provides efficient and	Combines private and consortium blockchains to	The hybrid approach might face challenges as the number of	✓	×	✓	✓	×	✓	✓	✓

(*continued on next page*)

Table 1 (*continued*)

Ref.	Blockchain Network Type	Finding	Pros	Cons	Cl	Sl	Tp	Au	Al	In	De	Di
		stable querying of historical health data.	address different sharing needs and enhance security.	users and data transactions grows.								
Rizzardi et al. [32]	Hyperledger Fabric, Permissioned Blockchain	The proposed architecture improves tracking and traceability of healthcare products.	Hyperledger Fabric's permissioned nature ensures privacy and access control.	While the system is evaluated for performance, scalability as the network grows and the number of transactions increases may be a concern.	✓	×	✓	✓	×	✓	✓	✓
Chen et al. [33]	Public or Consortium Blockchain	The hybrid storage structure provides fine-grained access control and guards against unauthorized access and attacks.	Reduces decryption overhead, making the scheme more efficient for healthcare data sharing.	Managing both blockchain and cloud storage may introduce additional complexity and overhead.	✓	×	✓	✓	×	✓	✓	✓
Ali et al. [34]	PBFT	The use of homomorphic encryption allows statistical and machine learning operations on encrypted data, enhancing data privacy and security.	Ensures data privacy and security throughout the data lifecycle.	Further research is needed to improve the model's scalability in real-world scenarios.	✓	×	✓	✓	×	✓	✓	✓
Rehman et al. [35]	Ethereum, hyperledger	The combination of Ethereum and Hyperledger Fabric addresses the scalability and privacy challenges of public blockchains and the centralization issues of private blockchains.	Combines public and private blockchain technologies for secure and trustless communication.	Potential interoperability challenges between Ethereum and Hyperledger Fabric.	✓	×	✓	✓	×	✓	✓	✓
Babu et al. [36]	Permissioned blockchain	The proposed model enhances IoT security by reducing false-positive rates and improving detection accuracy while ensuring secure alarm alerts across the IoT network.	Effective DDoS attack detection with lower false-positive rates.	Requires additional computational resources for blockchain operations.	✓	×	✓	✓	✓	✓	✓	✓
Li et al. [37]	Decentralized blockchain-based security management framework	The proposed framework significantly reduces error rates in trust evaluation and query allocation while improving detection accuracy and efficiency in CIDS.	Enhances trust in collaborative detection without requiring centralized authority.	Potentially higher computational overhead due to blockchain integration	✓	×	✓	✓	✓	✓	✓	✓
Sarhan et al. [38]	Permissioned blockchain	The HBFL framework enhances intrusion detection performance, ensures data privacy, and strengthens IoT security through a cloud–fog–edge architecture with secure smart contracts.	Strengthens IoT security by integrating blockchain for secure model updates.	Potentially higher computational costs due to federated learning and blockchain integration.	✓	×	✓	✓	✓	✓	✓	✓
Mahalingam et al. [39]	Hybrid (combination of public and private blockchain)	The proposed framework improves security, reliability, and performance in inter-domain routing	Reduces reliance on a single central authority by decentralizing routing decisions.	Scalability challenges when handling large-scale inter-domain networks.	✓	×	✓	✓	✓	✓	✓	✓

(*continued on next page*)

Table 1 (*continued*)

Ref.	Blockchain Network Type	Finding	Pros	Cons	Cl	Sl	Tp	Au	Al	In	De	Di
		by leveraging blockchain's tamper-proof ledger and digital signatures, achieving high efficiency in route filtering, fault tolerance, and convergence time.										
Baza et al. [40]	Hyperledger (Private Blockchain)	The proposed scheme efficiently manages private parking spot allocation while ensuring privacy and scalability, demonstrating high throughput and secure transaction handling.	Preserves privacy using encrypted request matching.	Computational overhead due to encryption and matching techniques	✓	×	✓	✓	✓	✓	✓	✓
Proposed Method	Permissioned Blockchain, Hyperledger, Deep Learning,	A unified framework combining advanced cryptographic techniques offers comprehensive protection against diverse attack vectors.	The integrated framework delivers strong, scalable security across multiple layers, overcoming the limitations of traditional methods.	—	✓	✓	✓	✓	✓	✓	✓	✓

Cl- Confidentiality, In- Integrity, Al- Availability, Di- Distributed, De- Decentralized, Tp-Tamper-Proof, Au- Authentication, Sl- Large Scalability.

across the network.

(i) Data Encryption

Data encryption is pivotal in safeguarding healthcare information privacy within the blockchain framework. The encryption process ensures that delicate data relics confidential and is available only to authorized parties.

(ii) Data decryption

Data decryption is the method of converting encrypted data back into its original, readable form. It's the inverse operation of encryption. To decrypt data, a decryption algorithm and the correct decryption key are required.

3.3.2. *Data immutability and integrity*

Blockchain technology ensures data integrity and immutability through its decentralized and distributed ledger. Each block in the blockchain contains a hash of the previous block, creating a chain that secures the data using Eq. (1). Each block B_i contains:

$$H(B_i) = H(H(B_{i-1})||T_i||D_i) \tag{1}$$

Where, H is a hash function, $H(B_{i\ -\ 1})$ is the hash of the previous block, T_i is the timestamp, and D_i is the data.

Once data is recorded in a block and added to the blockchain, it becomes part of the immutable chain. Altering any data would require recalculating all subsequent blocks' hashes, which is computationally infeasible.

3.3.3. *Privacy-Preserving techniques*

Zero-knowledge proofs (ZKPs) permit one party to prove the legitimacy of a statement without revealing the actual data. For Eq. (2) S, the prover demonstrates the truth of S without disclosing S itself:

$$Proof = ZKP(S) \tag{2}$$

Secure Multi-Party Computation (SMPC) enables multiple parties to collaboratively compute a function over their private inputs without exposing those inputs as represented using Eq. (3). The protocol ensures that

$$F(x_1,\ x_2,\ \ldots..,\ x_n)\ \textit{is computed while keeping}\ x_1,\ x_2,\ldots\ldots..,\ x_n\ \textit{private} \tag{3}$$

Where, F is a function and x_i are private inputs from different parties.

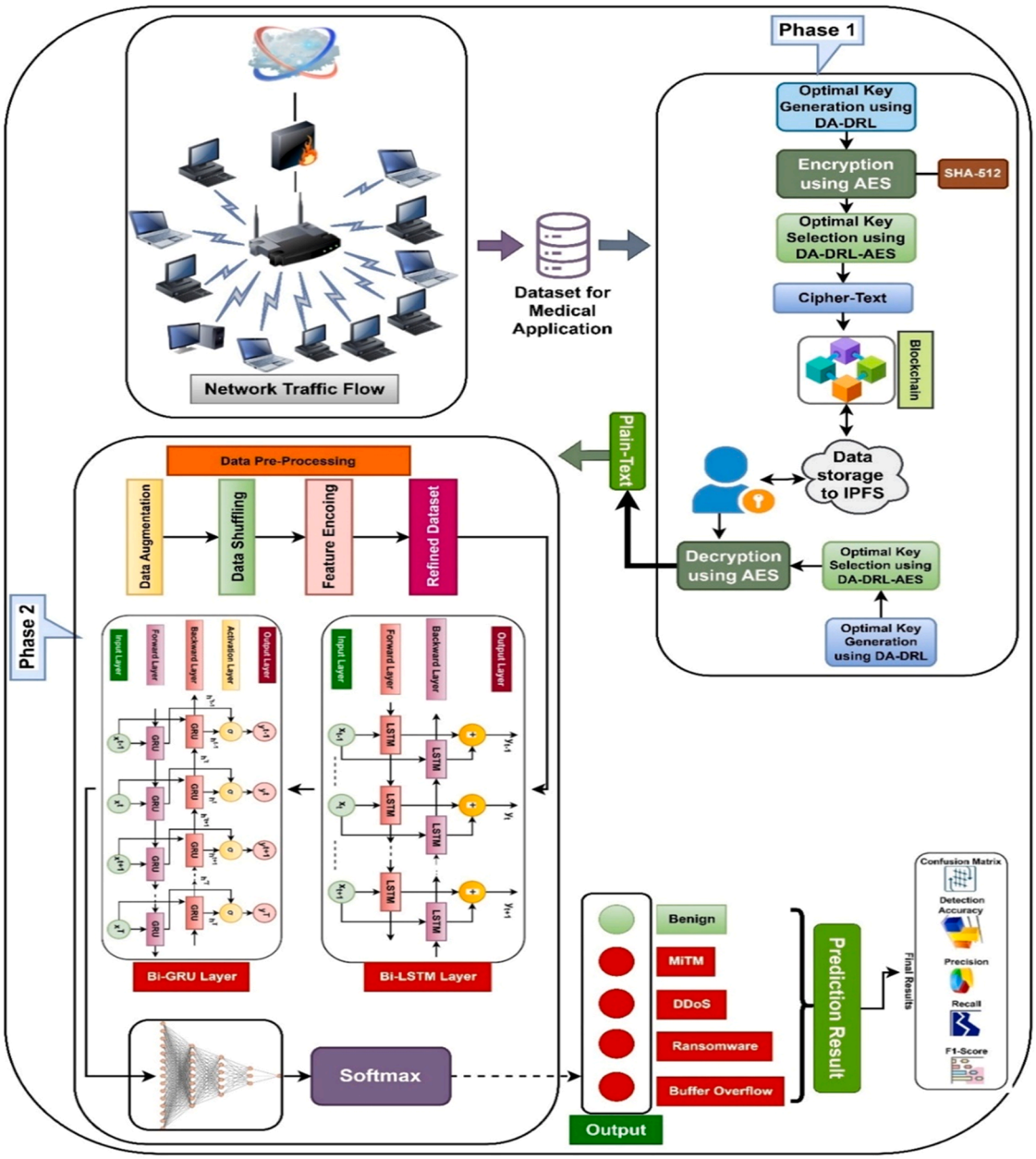


Fig. 1. A Dual-Layered Architecture for Smart Healthcare: Merging Blockchain with Deep Learning Intelligence.

3.3.4. Access control and authorization

Attribute-Based Access Control (ABAC) delivers more granular control by considering attributes of users, resources, and the environment. The access decision expressed using Eq. (4):

$$Access = Decision(A,\ P,\ R) \tag{4}$$

where A represents user attributes, P represents resource attributes, and R represents environmental conditions. The privacy-preserving blockchain framework integrates advanced encryption techniques, robust access control mechanisms, data integrity assurances, and privacy-preserving technologies to ensure the security and confidentiality of healthcare data. The comprehensive approach facilitates secure data management and analysis within a decentralized and tamper-proof system.

3.4. Proposed model for securing healthcare data with advanced techniques

The proposed model integrates a comprehensive approach to securing healthcare data by combining AES encryption, DA-DRL for key generation, SHA-512 hashing, ZKPs, PBFT, and ABAC. This section details each component and its role in the overall framework.

3.4.1. Advanced encryption standard (AES) encryption for data protection

Advanced Encryption Standard (AES) is leveraged to secure healthcare records through symmetric encryption. AES uses a fixed-size key to encrypt and decrypt data, providing robust security for sensitive information. Eq. (5–6) depicts the encryption and decryption process:

$$C = E(K, P) \tag{5}$$

Where, C is the cipertext, E is the AES encryption function, K is the symmetric key, and P is the plaintext data.

$$P = D(K, C) \tag{6}$$

Where, D is the AES decryption function. Given C and K, P are recovered.

3.4.2. Dynamic adaptive-deep reinforcement learning (DA-DRL)

DA-DRL strengthens cryptographic key management by continuously optimizing key generation through learning-based strategies. By applying reinforcement learning principles, DA-DRL adapts to emerging threats, producing secure, dynamic keys based on real-time feedback and evolving attack patterns, ensuring resilient and intelligent security in dynamic environments. It acclimatizes to changes in the security environment by using a deep reinforcement learning model that dynamically adjusts the key generation policy based on performance feedback and offers the following benefits:

Algorithm 1
Dynamic Adaptive Deep Reinforcement Learning (DA-DRL).

Steps				
1	Initialize Parameters			
		Define state space S, action space A, and reward function R. Initialize the key generation policy π. Set initial parameters for the deep learning model: learning rate α, discount factor γ, and exploration rate ε.		
2	For Each step			
		Initialize State: Set the initial state s based on the current security environment. For Each Time Step		
			Select Action: Use the policy π to select an action a (i.e., generate a key) based on the current state s.	$a = SelectAction(s, \pi)$
			Execute Action: Generate a key K using the selected action a. Observe Reward: Evaluate the effectiveness of the generated key using the reward function R.	$R(s, a) = EvaluateReward(K)$
			Observe New State: Transition to a new state s' based on the generated key K and its effectiveness. Update Policy: Adjust the policy π based on the observed reward and the transition from state $stos'$using a deep reinforcement learning model.	$\pi(s) \leftarrow \pi(s) + \alpha[R(s,a) + \gamma \max_{a'} \pi(s', a') - \pi(s,a)]$
			Update State: Set $s = s'$for the next time step.	
3	Repeat Until Convergence			
		Continue the process until the policy converges, meaning that the generated keys consistently meet the desired security criteria.		
4	Output Optimal Key Generation Policy			
		Once the policy has converged, use it to generate optimal keys for the current security environment.		

- Continuous Optimization: The DRL approach continuously learns and adjusts key generation strategies based on real-time performance and feedback.
- Dynamic Adaptation: It provides dynamic adjustments, which is crucial for environments with evolving threats and changing data requirements.
- Enhanced Learning: Utilizes advanced learning algorithms to refine and optimize key generation processes, leading to improved performance and security.
- Complexity Handling: It effectively handles complex key generation tasks by leveraging deep reinforcement learning's ability to learn from and adapt to complex environments.
- Security Enhancement: The dynamic nature of DA-DRL ensures that the key generation process remains robust against evolving threats, improving overall security.
- Performance Efficiency: It offers a balance between performance and adaptation, making it appropriate for real-time and large-scale applications like blockchain-based smart healthcare systems.

The DRL framework adapts to evolving threats and historical data to generate the most secure, context-aware key $K_{optimal}$. The reinforcement learning policy π is optimized according to the expected rewards R as shown in Eq. (7):

$$\pi^*(s) = \underset{\pi}{argmax}\mathbb{E}[R(s,\ \pi(s))] \tag{7}$$

Where s represents the state of the system, $R(s, \pi(s))$ is the reward function evaluating the effectiveness of policy π in generating the key.

(i) Reinforcement Learning Formulation

To operationalize the DA-DRL module, we define the reinforcement learning components as follows:

- State ($\boldsymbol{s}$): Represents the current security context, including historical intrusion patterns, entropy levels, prior key usage, and system resource metrics. It reflects the environmental conditions affecting the robustness of cryptographic key generation.
- Action ($\boldsymbol{a}$): Denotes the generation of a cryptographic key or selection of parameters such as key length, seed entropy, and algorithmic variation. Each action impacts the security properties of the resulting key.
- Reward ($\boldsymbol{R}$): Quantifies the strength of the generated key based on cryptographic metrics such as entropy, uniqueness, resistance to attacks, and adherence to standard key security benchmarks. Positive rewards are assigned to strong, unique keys, while low-entropy or weak keys incur penalties.
- Policy ($\boldsymbol{\pi}$):A deep neural network that maps states to actions, continuously refined through Q-learning or policy-gradient methods. The objective is to learn the optimal policy π^* that maximizes the expected long-term security reward.

DA-DRL enhances key generation by learning from historical security information and dynamically refining its policy to create a more secure key $K_{optimal}$. When vulnerable key patterns are identified, the algorithm adapts in real-time to mitigate threats. The stepwise functioning is outlined in Algorithm 1.

3.4.3. SHA-512 hashing for data integrity

SHA-512 (Secure Hash Algorithm 512-bit) ensures data integrity by generating a unique 512-bit hash value H for each data input D. The hashing process is represented using Eq. (8):

$$H = SHA - 512(D) \tag{8}$$

The hash value H serves as a digital fingerprint for D. Any alterations to D would result in a different hash value, indicating potential tampering. For example, if a healthcare record is hashed and kept on the blockchain, any unauthorized modifications to the record will be perceived by comparing the hash value against the stored hash.

3.4.4. Zero-Knowledge proofs (ZKPs)

ZKPs provide privacy by permitting one party (the prover) to validate knowledge of a piece of information without revealing the information itself. It enables the validation of a statement without revealing the underlying data. The proof generation and verification processes are expressed using Eq. (9):

$$Proof = ZKP(S,\ Witness) \tag{9}$$

Where S is the statement to be proven, and the witness represents the confidential data used to generate the proof. Eq. (10) verifies whether the proof corresponds to the statement S without disclosing the actual data.

$$Verify(Proof,\ S) = True/False \tag{10}$$

A healthcare provider can use ZKPs to demonstrate they have authorization to access specific data without revealing the data itself. The verification function confirms the provider's access rights without exposing delicate information.

3.4.5. Practical byzantine fault tolerance (PBFT)

PBFT attains consensus in a decentralized blockchain network, ensuring agreement among nodes even in the presence of faulty or malicious nodes. The consensus process involves multiple phases as shown in Eq. (11):

$$Consensus = PBFT(T) \tag{11}$$

where T represents the transaction. PBFT involves pre-preparation, preparation, and commitment phases, allowing nodes to propose and validate transactions collectively.

In the healthcare blockchain, PBFT ensures that all nodes reach a consensus on transactions involving patient data. This mechanism prevents fraud and maintains blockchain integrity by requiring nodes to agree on the validity of transactions.

3.4.6. Attribute-Based access control (ABAC) for granular access control (GAC)

ABAC enforces access control policies based on various attributes such as user roles, resource sensitivity, and contextual conditions. The access control decision is formulated using Eq. (12):

$$Access = Decision(U, R, C) \tag{12}$$

where U represents user attributes (e.g., role, clearance level), R represents resource attributes (e.g., data sensitivity), and C represents contextual attributes (e.g., time of access). A nurse's access to patient records is determined based on their role and department attributes. Access is granted only if these attributes meet the required criteria, ensuring that sensitive data is accessible only to authorized personnel.

The proposed model employs AES encryption, DA-DRL for dynamic key generation, SHA-512 hashing, ZKPs for privacy, PBFT for consensus, and ABAC for access control to create a comprehensive framework for managing healthcare data securely. AES ensures data confidentiality, DA-DRL optimizes key security dynamically, SHA-512 maintains data integrity, ZKPs protect privacy, PBFT achieves consensus in a decentralized manner, and ABAC enforces fine-grained access control. This integrated approach guarantees that healthcare records is robustly threatened against unauthorized access and interfering, supporting the integrity and confidentiality of sensitive information.

3.4.7. Block creation

When a new transaction such as an update to healthcare information is initiated within the blockchain network, it follows a systematic authentication and integration process to ensure data security, integrity, and regulatory compliance. Initially, the transaction was proposed by an authorized healthcare provider and broadcast to all peer nodes in the network. These nodes collaboratively authenticate the transaction's authenticity and verify its compliance with predefined policies. Once validated, a leader node, selected through the PBFT consensus protocol, assembles the transaction into a new block. This block contains critical metadata, including the hash of the previous block and a timestamp, ensuring chronological integrity. Before storage, the transaction is encrypted using the Advanced Encryption Standard (AES) to guarantee confidentiality. The encryption key is computed using Eq. (5), and only authorized parties can decrypt the data using Eq. (6), restoring the original plain-text. This encryption-decryption process ensures strict access control and secures sensitive healthcare data from unauthorized exposure.

3.4.8. Digital signature generation and verification

Digital signature generation and verification are essential for ensuring the authenticity and integrity of transactions in blockchain networks. These mechanisms provide a secure way to validate the identity of participants and confirm the legitimacy of blockchain transactions, which are explained as follows:

(i) Signature Generation

Digital signatures are essential for verifying the origin and integrity of blockchain transactions. In healthcare systems, providers authenticate transactions using their private keys, generating a unique digital signature. This signature ensures that the transaction is both genuine and unaltered, thereby maintaining trust and security within the decentralized network. The signature generation process has been represented mathematically using Eq. (13):

$$Signature = Sign_{private}(H(T)) \tag{13}$$

Where the Signature is the digital signature, $Sign_{private}$ is the signing function using the provider's private key, $H(T)$ is the hash of the transaction T.

The hash function H generates a fixed-size hash value from the transaction data, ensuring that even a slight change in the transaction will result in a significantly different hash value. The digital signature created by the provider's private key ensures that only the provider could have signed the transaction, thus guaranteeing its authenticity.

(ii) Signature Verification

Once a transaction is signed, other nodes in the network must verify the signature to ensure the transaction's integrity and authenticity. This verification process uses the provider's public key to confirm that the digital signature matches the transaction's

hash. The mathematical representation of the verification process is presented using Eq. (14):

$$Verify_{public}(H(T), Signature) \tag{14}$$

Where, $Verify_{public}$ is the verification function using the provider's public key, ($H(T)$ is the hash of the transaction T, and Signature is the digital signature.

A successful verification process confirms that a transaction remains unaltered since signing and verifies the signer's authenticity through their private key. This guarantees the integrity and trustworthiness of the transaction, forming the foundation for secure communication within the blockchain network. Especially in healthcare, digital signatures ensure that only authorized entities can submit and validate transactions. Algorithm 2 outlines the complete process of digital signature generation and verification within the proposed framework.

3.4.9. Storing data to IPFS

The InterPlanetary File System (IPFS) is utilized for secure and decentralized storage of encrypted healthcare data. As a distributed file system, IPFS employs content-addressing, assigning each file a unique cryptographic hash for identification. This ensures data integrity, availability, and resilience against cyber threats, server failures, or natural disasters.

(i) Decentralization

IPFS eradicates single points of failure by dispensing data across multiple network nodes. Unlike centralized systems, where data loss can occur due to server crashes, IPFS ensures redundancy, permitting data retrieval even if some nodes go offline. This resilience is critical for healthcare applications, ensuring uninterrupted access to patient records and supporting reliable medical decision-making.

(ii) Immutability

IPFS content-addressing guarantees data integrity. Each stored file is allocated a unique Content Identifier (CID) based on its cryptographic hash. Any modification alters the CID, preventing tampering and maintaining an immutable record. This feature aligns with blockchain principles, ensuring the authenticity of patient records, medical histories, and treatment data, reducing errors and enhancing trust in healthcare systems.

(iii) Security

To reinforce data privacy, only encrypted data is stored on IPFS. AES encryption guarantees that even if unauthorized parties access the data, they cannot interpret it without the decryption key. The encrypted data's CID is recorded on the blockchain, creating a secure reference without storing sensitive information on-chain.

Algorithm 2
Digital Signature Generation and Verification.

Steps			
	Input		
		Transaction Tcontaining healthcare data. Private key $K_{private}$ of the healthcare provider Public key K_{public} of the healthcare provider	
	Output		
		Digital signature for the transaction T Verification status of the digital signature	
1	Digital Signature Generation		
1.1		Hash the transaction T to generate a unique hash $H(T)$.	$H(T) = Hash(T)$
1.2		Sign the hash $H(T)$ using the private key $K_{private}$ to generate the digital signature S.	$S = Sign_{K_{private}}(H(T))$
2	Digital Signature Verification		
2.1		Receive the transaction T and the digital signature S.	
2.2		Hash the received transaction T to generate the hash $H'(T)$.	$H'(T) = Hash(T)$
2.3		Verify the digital signature S using the public key K_{public} and the hash $H'(T)$.	$Verification = Verify_{K_{public}}(H'(T), S)$
2.4		If the verification process succeeds, the digital signature S is valid, confirming the integrity and authenticity of the transaction T.	
2.5		If the verification process fails, the digital signature S is invalid, indicating potential tampering or incorrect signing.	

The process of storing encrypted data on IPFS can be described as follows:

- Encrypt the Data: Before uploading to IPFS, healthcare data is encrypted using AES, resulting in ciphertext. This step guarantees that the data is converted into a secure format that cannot be easily interpreted without the decryption key. Encrypting the data protects patient information from unauthorized access and potential breaches.
- Upload to IPFS: The encrypted data (ciphertext) is uploaded to IPFS, where a unique CID is produced. The CID, a cryptographic hash of data, provides a unique and tamper-proof reference to the stored information. This CID facilitates the retrieval of encrypted data from IPFS when needed.
- Store the CID on Blockchain: The generated CID, acting as a reference to the encrypted data on IPFS, is included in the blockchain transaction. This ensures that the actual data is stored off-chain while the blockchain maintains a secure reference to the data. By storing the CID on the blockchain, the immutability and transparency of blockchain technology are leveraged while keeping the data off-chain for enhanced security and scalability.

To retrieve and decrypt the data, the following steps are taken:

- Retrieve the CID from Blockchain: The CID pointing to the encrypted data on IPFS is obtained from the blockchain transaction. The blockchain transaction contains a secure and immutable record of the CID, which is used to locate the encrypted data stored on IPFS.
- Fetch Data from IPFS: The CID retrieves the encrypted data from IPFS. As a unique identifier for the encrypted data, the CID allows healthcare providers to fetch the exact data needed from the decentralized IPFS network.
- Decrypt the Data: The encrypted data is decrypted using the corresponding AES decryption key to obtain the original plaintext data. Decryption contraries the encryption process, converting ciphertext back into its original, readable format. Only authorized parties with the correct decryption key can perform this step, ensuring that sensitive healthcare data remains confidential and secure.

This approach leverages IPFS's decentralization and security alongside blockchain's immutability, creating a robust framework for protecting and managing sensitive healthcare data. Algorithm 3 illustrates the working of the proposed blockchain framework.

3.5. DL-based IDS model for binary and multiclass classification (Phase 2)

The Secure and Dependable Bi-LSTM GRU Intrusion Detection Model (SD-BiLSTMGRU-IDM) is designed to improve intrusion detection performance by leveraging a hybrid deep learning architecture. It integrates Bidirectional Long Short-Term Memory (Bi-LSTM) and Bidirectional Gated Recurrent Units (Bi-GRU), which work together to capture both forward and backward temporal dependencies in network traffic data. Prior to training, the dataset is preprocessed through standardization and label encoding to ensure consistency and learning efficiency. The model architecture alternates between Bi-LSTM and Bi-GRU layers, with dropout layers incorporated to prevent overfitting. Fully connected layers then convert extracted features into classification outputs via a Softmax function. Trained using the Adam optimizer and Cross-Entropy Loss, the model effectively enhances detection accuracy, generalization, and feature learning. Fig. 2 illustrates the complete architecture of SD-BiLSTMGRU-IDM.

3.5.1. Data preprocessing

This section provides the data preprocessing steps for our proposed model, which is depicted in Fig. 2 and explained as follows:

(i) Data augmentation

To improve the strength of our intrusion detection model, we introduced data augmentation techniques, specifically targeting the numerical column labelled 'MI_dir_L5_weight'. We simulate potential variations and anomalies in real-world data by injecting randomness into this column. The augmentation process involves adding Gaussian noise to the values in 'MI_dir_L5_weight', which can be mathematically represented using Eq. (15):

$$MI\_dir\_L5\_weight^{'} = MI\_dir\_L5\_weight + \mathcal{N}(0, \sigma^2 \tag{15}$$

Where $\mathcal{N}(0,\sigma^2)$ denotes Gaussian noise with a mean of 0 and variance σ^2. This approach ensures that our model learns to generalize better by encountering diverse examples during training, thereby improving its performance on unseen data.

(ii) Data Shuffling

Shuffling the dataset is a critical preprocessing step to avoid the model from learning spurious patterns related to the order of the data. We randomly shuffle the entire dataset before splitting the dataset into training and testing sets. This can be mathematically described using Eq. (16):

$$Shuffled\ Data = RandomPermutation(Data) \tag{16}$$

Where*RandomPermutation* is a function that returns a randomly permuted sequence of the data indices. By shuffling the data, we

Algorithm 3
Proposed Blockchain framework.

Steps					
1	AES Encryption for Data Protection				
		Input: Plaintext data P, Symmetric key K Output: Ciphertext C			
			Encrypt Data		
				Using Eq. (5)	
			Store Ciphertext		
				Store C in a secure location (e.g., blockchain)	
			Decrypt Data		
				Using Eq. (6)	
2	DA-DRL for Optimal Key Generation				
		Input: Current state s, Set of policies Π Output: Optimal key $K_{optimal}$.			
			Initialize		
				$K_{optimal} = None$ max $\_reward = -\infty$	
			For Each Policy π in Π		
					$R(s, \pi) = EvaluateReward(s, \pi)$
			If $R(s,\pi) >$ max $\_reward$		
					max $\_reward = R(s, \pi)$ $K_{optimal} = ApplyPolicy(\pi)$
		Analyze historical security data and adapt policy π to produce the most secure $K_{optimal}$.			
3	SHA-512 Hashing for Data Integrity				
		Input: Data D Output: Hash value H			
			Generate Hash		
					Using Eq. (8)
			Verify Integrity		
				Compare H with previously stored hash to check for data integrity	
		Compute H for healthcare data D and store it on the blockchain to verify integrity.			
4	ZKPs for Privacy				
		Input: Statement S, Witness Output: Proof			
			Generate Proof		
					Using Eq. (9)
			Verify Proof		
					Using Eq. (10)
				If $Verify(Proof, S) = False$, $thenrejecttheproof$.	
			Healthcare provider demonstrates authorization with a ZKP, which is then verified without revealing the actual data.		
5	PBFT for Consensus				
		Input: Transactions T Output: Consensus result			
			For Each Transaction T_i in T		
				Pre-Prepare Phase	
					$PrePrepare(T_i)$

(continued on next page)

Algorithm 3 (*continued*)

Steps					
				Prepare Phase	
					Prepare(T_i)
				Commit Phase	
					Commit(T_i)
			Collect Agreements		
					Concensus = *CollectAgreements*(T)
6	ABAC for Granular Access Control				
		Input: User attributes U, Resource attributes, R, Contextual attributes C Output: Access decision			
			Evaluate Access Control		
					Access = *Decision*(*U, R, C*)
				If *Decision*(*U, R, C*) = *True*, *grantaccess* Otherwise, deny access.	

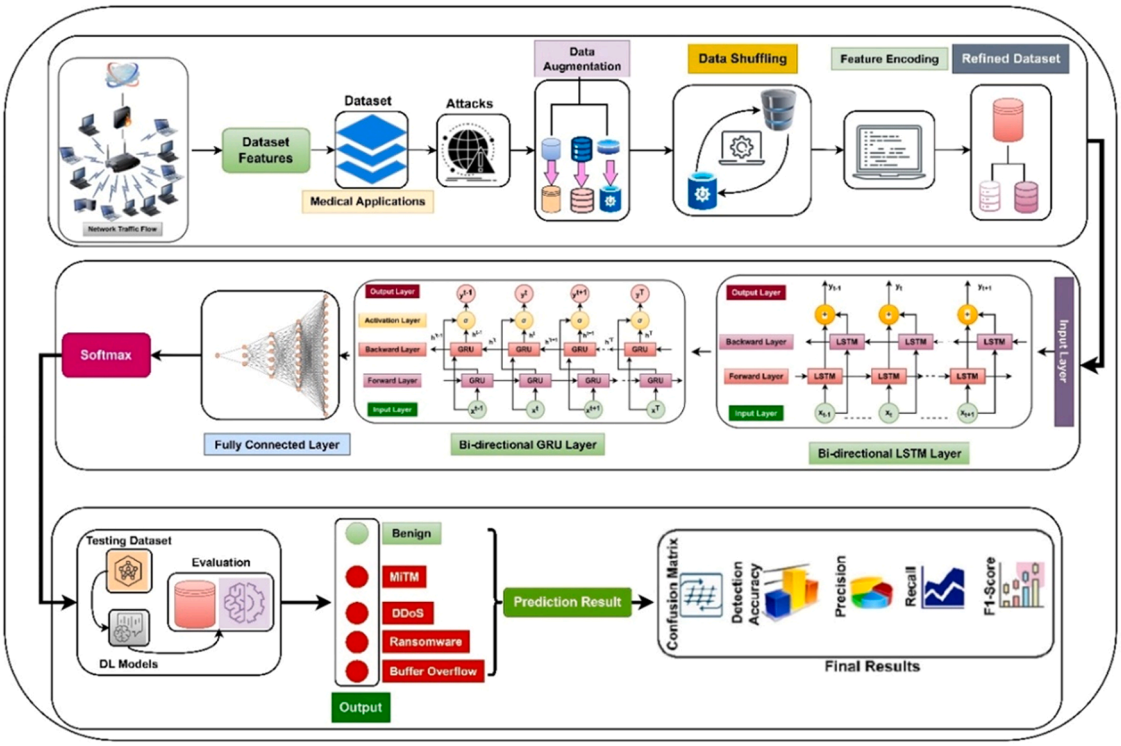


Fig. 2. Proposed working architecture of SD-BiLSTMGRU-IDM.

ensure that the training and testing sets represent the overall dataset, thus enhancing the model's generalization capability and reducing the risk of overfitting to specific sequences.

(iii) Feature Encoding

Since our dataset contains both numerical and categorical features, we employ different encoding techniques to handle them appropriately. For numerical features, standardization is performed to normalize the data. Standardization standardizes the feature values to have a mean of 0 and a standard deviation of 1. It ensures that the data is normalized, which helps in faster convergence and better performance of the neural network, as depicted in Eq. (17). Eq. (18) indicates the sensitivity of the standardized features to changes in the raw features.

$$X_{standardized} = \frac{X - \mu}{\sigma} \tag{17}$$

$$\frac{\partial X_{standardized}}{\partial X} = \frac{1}{\sigma} \tag{18}$$

Here, μ is the mean of the features, and σ is the standard deviation. The standardized feature $X_{standardized}$ ensures balanced contribution of each input to model training. For categorical features, we use one-hot encoding to convert them into a numerical format, which is represented using Eq. (19):

$$OneHot(x) = [0, \ldots..1, \ldots....0] \tag{19}$$

where the 1 is placed in the position corresponding to the categorical value of x. This encoding ensures that the categorical data is represented in a form suitable for model training, allowing the model to effectively process and learn from both types of features.

To begin with, the input layer receives a dataset with n samples and d features. It is standardized and encoded to ensure that features are on a comparable scale and categorical labels are numerically represented using Eq. (20).

$$X \in \mathbb{R}^{n \times d} \tag{20}$$

Eq. (20) represents the input matrix X, where n is the number of samples and d is the dimensionality of each sample. Each row of X is a feature vector corresponding to a single observation in the dataset.

Additionally, label encoding encodes the categorical labels into numeric form. It converts target labels into a format suitable for the classification model. Each unique label in y is assigned a unique integer, making it suitable for model training, represented using Eq. (21).

$$y_{encoded} = LabelEncoder(y) \tag{21}$$

(iv) Bidirectional LSTM layer

Moreover, the Bidirectional LSTM layer processes the input sequence data to capture both forward and backward dependencies. It captures context from both past and future, making it effective for sequences where future information is as important as past information, which is represented using Eq. (22–23):

$$\overrightarrow{h}_t = LSTM\left(X_t, \overrightarrow{h}_{t-1}\right) \tag{22}$$

$$\overleftarrow{h}_t = LSTM\left(X_t, \overleftarrow{h}_{t+1}\right) \tag{23}$$

Bi-LSTM combines forward and backward LSTM outputs, concatenated as shown using Eq. (24)

$$H_t = \left[\overrightarrow{h}_t; \overleftarrow{h}_t\right] \tag{24}$$

LSTM cell operations for both directions are computed using Eq. (25–30):

$$f_t = \sigma\left(W_f X_t + U_f h_{t-1} + b_f\right) \tag{25}$$

$$i_t = \sigma(W_i X_t + U_i h_{t-1} + b_i) \tag{26}$$

$$\widetilde{c}_t = tanh(W_c X_t + U_c h_{t-1} + b_c) \tag{27}$$

$$c_t = f_t \odot c_{t-1} + i_t \odot \widetilde{c}_t \tag{28}$$

$$o_t = \sigma(W_o X_t + U_o h_{t-1} + b_o) \tag{29}$$

$$h_t = o_t \odot \tanh(c_t) \tag{30}$$

Eq. (31) computes the gradients for LSTM parameters using the chain rule to update the parameters using optimization algorithms.

$$\frac{\partial \mathscr{L}}{\partial W_f} = \frac{\partial \mathscr{L}}{\partial h_t} \cdot \frac{\partial h_t}{\partial W_f} \text{ and similarly for other parameters} \tag{31}$$

(v) Bidirectional GRU layer

Subsequently, the Bidirectional GRU layer processes the output from the first Bi-LSTM layer to capture complex temporal de-

pendencies with fewer parameters than LSTM. It handles dependencies with a gating mechanism, allowing it to focus on important parts of the sequence while forgetting irrelevant information, and performs efficiently with fewer parameters than LSTM. The GRU cell operations are expressed using Eq. (32–37):

$$\overrightarrow{z}_t = \sigma\left(W_z X_t + U_z \overrightarrow{h}_{t-1}\right) \tag{32}$$

$$\overleftarrow{z}_t = \sigma\left(W_z X_t + U_z \overleftarrow{h}_{t+1}\right) \tag{33}$$

$$\overrightarrow{r}_t = \sigma\left(W_r X_t + U_r \overrightarrow{h}_{t-1}\right) \tag{34}$$

$$\overleftarrow{r}_t = \sigma\left(W_r X_t + U_r \overleftarrow{h}_{t+1}\right) \tag{35}$$

$$\overrightarrow{h}_t = \left(1 - \overrightarrow{z}_t\right) \odot \overrightarrow{h}_{t-1} + \overrightarrow{z}_t \odot \tanh\left(W_h X_t + U_h\left(\overrightarrow{r}_t \odot \overrightarrow{h}_{t-1}\right)\right) \tag{36}$$

$$\overleftarrow{h}_t = \left(1 - \overleftarrow{z}_t\right) \odot \overleftarrow{h}_{t+1} + \overleftarrow{z}_t \odot \tanh\left(W_h X_t + U_h\left(\overleftarrow{r}_t \odot \overleftarrow{h}_{t+1}\right)\right) \tag{37}$$

The Bi-GRU consists of forward and backward GRUs, which are concatenated using Eq. (38):

$$H_t = \left[\overrightarrow{h}_t; \overleftarrow{h}_t\right] \tag{38}$$

With its update and reset gates, the GRU mechanism efficiently captures long-term dependencies while mitigating the vanishing gradient problem. The Bi-GRU layer strengthens temporal prediction by integrating contextual information from both past and future data sequences.

Eq. (39) is used to compute the loss gradient concerning each parameter, which is then used in optimization algorithms. $\frac{\partial^2 \mathscr{L}}{\partial W_z^2}$ can provide insight into the curvature of the loss surface, although they are less commonly computed directly due to their computational complexity.

$$\frac{\partial \mathscr{L}}{\partial W_z} = \frac{\partial \mathscr{L}}{\partial \overrightarrow{z}_t} \cdot \frac{\partial \overrightarrow{z}_t}{\partial W_f} \quad \textit{and similarly for other parameters} \tag{39}$$

Furthermore, the dropout layer is applied to the first Bi-GRU layer's output, which helps prevent overfitting by randomly setting a fraction of the neurons to zero during training, ensuring that the model generalizes better to unseen data. It introduces random noise into the training process by deactivating a subset of neurons which is represented using Eq. (40).

$$H_t^{dropout1} = Dropout(H_t, p = 0.5) \tag{40}$$

After that, the second Bidirectional LSTM layer is used to process the data further to capture additional context from the sequence as represented using Eq. (41–43). By adding deeper contextual layers, the model gains improved capability to interpret and learn from sequential data patterns effectively.

$$\overrightarrow{h}_t = LSTM\left(H_t^{dropout1}, \overrightarrow{h}_{t-1}\right) \tag{41}$$

$$\overleftarrow{h}_t = LSTM\left(H_t^{dropout1}, \overleftarrow{h}_{t+1}\right) \tag{42}$$

$$H_t = \left[\overrightarrow{h}_t; \overleftarrow{h}_t\right] \tag{43}$$

Then, the second Bidirectional GRU layer processes the output from the second Bi-LSTM layer, focusing on higher-level dependencies. It adds a final layer of temporal context and dependency modelling, improving the overall representation of the sequence as expressed using Eq. (44–50):

$$\overrightarrow{z}_t = \sigma\left(W_z H_t + U_z \overrightarrow{h}_{t-1}\right) \tag{44}$$

$$\overleftarrow{z}_t = \sigma\left(W_z H_t + U_z \overleftarrow{h}_{t+1}\right) \tag{45}$$

$$\overrightarrow{r_t} = \sigma\left(W_r H_t + U_r \overrightarrow{h_{t-1}}\right) \tag{46}$$

$$\overleftarrow{r_t} = \sigma\left(W_r H_t + U_r \overleftarrow{h_{t+1}}\right) \tag{47}$$

$$\overrightarrow{h_t} = \left(1 - \overrightarrow{z_t}\right) \odot \overrightarrow{h_{t-1}} + \overrightarrow{z_t} \odot \tanh\left(W_h H_t + U_h\left(\overrightarrow{r_t} \odot \overrightarrow{h_{t-1}}\right)\right) \tag{48}$$

$$\overleftarrow{h_t} = \left(1 - \overleftarrow{z_t}\right) \odot \overleftarrow{h_{t+1}} + \overleftarrow{z_t} \odot \tanh\left(W_h H_t + U_h\left(\overleftarrow{r_t} \odot \overleftarrow{h_{t+1}}\right)\right) \tag{49}$$

$$H_t = \left[\overrightarrow{h_t}; \overleftarrow{h_t}\right] \tag{50}$$

A dropout layer is applied to the output of this layer, which reduces overfitting by ensuring that the network does not rely too heavily on any single pathway, which is represented using Eq. (51):

$$H_t^{dropout2} = Dropout(H_t, p = 0.5) \tag{51}$$

The fully connected layer maps the output from the second dropout layer to a new feature space of size h_1. It refines feature representation by extracting higher-level patterns to enable accurate data classification. Eq. (52–53) of the fully connected layer parameters is used for parameter updates.

$$FC1_{out} = W_{fc1} H_t^{dropout2} + b_{fc1} \tag{52}$$

$$\frac{\partial \mathscr{L}}{\partial W_{fc1}} = \frac{\partial \mathscr{L}}{\partial FC1_{out}} \cdot \frac{\partial FC1_{out}}{\partial W_{fc1}} \tag{53}$$

Similarly, the fully connected layer maps the output from the first FCL to the number of classes, producing each class's final classification scores as represented by Eq. (54):

$$FC2_{out} = W_{fc2} FC1_{out} + b_{fc2} \tag{54}$$

The final stage applies the SoftMax activation function to convert the model's output logits into class probabilities, enabling multi-class classification as described in Eq. (55). The Cross-Entropy Loss function then evaluates prediction errors by comparing predicted and actual labels, guiding the optimization process using Eq. (56). To minimize this loss, the Adam optimizer adaptively updates model weights with efficient learning rates, ensuring faster convergence and improved performance. This end-to-end process strengthens model generalization and enhances classification accuracy across diverse intrusion patterns.

$$\widehat{y} = Softmax(FC2_{out}) \tag{55}$$

$$\frac{\partial \widehat{y}_i}{\partial FC2_{out,j}} = \widehat{y}_i\left(\delta_{i,j} - \widehat{y}_j\right) \tag{56}$$

Where, $\delta_{i,j}$ is the Kronecker delta.
Eq. (57–58) provides information on the curvature of the SoftMax output with respect to the logits.

$$\frac{\partial^2 \widehat{y}_i}{\partial FC2_{out,j} \partial FC2_{out,k}} = \widehat{y}_i\left(\delta_{jk}\widehat{y}_j - \widehat{y}_i\widehat{y}_j\widehat{y}_k\right) \tag{57}$$

$$\widehat{y}_i = \frac{\exp\left(FC2_{out,i}\right)}{\sum_{j=1}^{C} \exp\left(FC2_{out,j}\right)} \tag{58}$$

$$\mathscr{L} = -\frac{1}{n}\sum_{i=1}^{n}\sum_{c=1}^{C} y_{i,c} \log\left(\widehat{y}_{i,c}\right) \tag{59}$$

Eq. (59) computes the loss function concerning the predicted probability and indicates how prediction changes affect the loss. Eq. (60–61) provides information on how changes in the prediction impact the rate of change of the loss.

$$\frac{\partial \mathscr{L}}{\partial \widehat{y}_{i,c}} = -\frac{y_{i,c}}{\widehat{y}_{i,c}} \tag{60}$$

$$\frac{\partial^2 \mathscr{L}}{\partial \widehat{y}_{i,c}^2} = \frac{y_{i,c}}{\widehat{y}_{i,c}^2} \tag{61}$$

Adam uses first-order gradients computed from the loss function to update model parameters θ. The learning rate η controls the size of the update step. It is also utilizing to adjust the learning rate for each parameter adaptively using Eq. (62).

$$\theta = \theta - n \cdot \nabla_{\theta}\mathscr{L} \tag{62}$$

3.5.2. Hyperparameter tuning

Effective deep learning relies on precise hyperparameter tuning, as it directly affects the model's learning capacity and generalization. In this study, the proposed intrusion detection model was optimized through systematic hyperparameter configuration. Table 2 outlines the key settings, including input/output dimensions, hidden layers, dropout rates, learning rate, batch size, epochs, and optimizer selections. Specific Bi-LSTM and Bi-GRU configurations were also refined. Table 3 summarizes the notations used throughout the framework.

Algorithm 4 outlines the sequential process of the SD-BiLSTMGRU-IDM model for detecting intrusions in IoMT networks.

3.5.3. Dependability analysis

The dependability of the proposed SD-BiLSTMGRU-IDM plays a pivotal role in determining its suitability for real-world cybersecurity applications, predominantly within IoMT environments. This study focuses on three core attributes: efficiency, availability, and scalability which are essential for consistent and adaptive intrusion detection. To enhance efficiency, the model leverages the combined strengths of Bidirectional LSTM and GRU layers to capture both forward and backward temporal dependencies in network traffic. This dual-context learning ensures high detection accuracy while reducing computational complexity through optimized gradient processing and careful hyperparameter tuning. Dropout layers are integrated to prevent overfitting, promoting better generalization to novel and unseen intrusion patterns. In terms of availability, the model maintains continuous detection capability with minimal downtime, making it resilient for deployment across varied infrastructures, including cloud platforms and edge-based IoT devices. Scalability is demonstrated through systematic evaluation across multiple training epochs (25, 50, 75, and 100), confirming that the model handles increasing data volumes without significant resource escalation. Overall, the SD-BiLSTMGRU-IDM offers a dependable solution by achieving real-time, resource-efficient, and scalable intrusion detection, thereby strengthening the security posture of modern IoMT networks against evolving cyber threats.

4. Experimental details and result analysis

This section outlines the experimental design and performance evaluation of the proposed models, focusing on key metrics. Results are interpreted to reveal practical effectiveness, highlight strengths, expose limitations, and benchmark against existing techniques to assess suitability for real-world deployment in security-critical environments.

4.1. Experimentation setup configuration

The experiments were conducted on a high-performance system with an Intel® Core™ Ultra 9 185H processor and an NVIDIA® GeForce RTX™ 4070 GPU, ensuring efficient execution of deep learning models. The setup included 32 GB DDR5 RAM and utilized PyTorch [41] and scikit-learn [42] for model training, evaluation, and preprocessing.

Table 2
Overview of the selected hyperparameter values of the proposed DL model.

Hyperparameter	Description	Value
input_size	Input feature dimensions	1 × 75×64
hidden_size1	Hidden state size (LSTM-1)	64
hidden_size2	Hidden size for LSTM, GRU	128
output_size	Classes for classification tasks.	[(1 × 5)*128], [(1 × 2)*128]
dropout_prob	Dropout layer zeroing probability.	0.5
learning_rate	Optimizer learning step size.	0.001
num_epochs	Training iterations count.	100
batch_size	Samples processed per batch.	64
optimizer	Algorithm used for optimization.	Adam, Softmax
loss_function	Function used to compute loss.	CrossEntropyLoss, BinaryCrossEntropy
bi_lstm1 hidden_size	Bi-LSTM first layer size.	64
bi_lstm2 hidden_size	Bi-LSTM second layer size.	128
bi_gru1 hidden_size	Bi-GRU first layer size.	64
bi_gru2 hidden_size	Bi-GRU second layer size.	128
fc1 input_size	Input size for first dense layer.	256 (2 * hidden_size2)
fc1 input_size	Input size for first dense layer.	128
Fc2 input_size	Second dense layer input size.	128
Fc3 input_size	Third dense layer input size.	128
Fc3 input_size	Final output for Multi and Binary classification.	(1 × 5), (1 × 2)

Table 3
Notations and descriptions.

Notations	Description
$X \in \mathbb{R}^{n \times d}$	Input data matrix with n samples and d features
μ	Mean of the input features
σ	Standard deviation of the input features
$X_{standardized}$	Standardized input data
$y_{encoded}$	Numerically encoded labels
$\overrightarrow{h_t}$	Forward hidden state of the LSTM/GRU at time step$t$
$\overleftarrow{h_t}$	Backward hidden state of the LSTM/GRU at time step$t$
H_t	Concatenated forward and backward hidden states at time step t
$f_t, i_t, \widetilde{c}_t, c_t, o_t,$	LSTM gates and cell states
$W_f, U_f, b_f,$	LSTM forget gate weights, recurrent weights, and biases
$W_i, U_i, b_i,$	LSTM input gate weights, recurrent weights, and biases
$W_c, U_c, b_c,$	LSTM cell gate weights, recurrent weights, and biases
$W_o, U_o, b_o,$	LSTM output gate weights, recurrent weights, and biases
σ	Sigmoid activation function
$tanh$	Hyperbolic tangent activation function
$\odot$	Element-wise multiplication
$\overrightarrow{z_t}$, $\overleftarrow{z_t}$	Update gate of the GRU at time step t
$\overrightarrow{r_t}$, $\overleftarrow{r_t}$	Reset gate of the GRU at time step t
W_z, U_z	GRU update gate weights and recurrent weights
W_r, U_r	GRU reset gate weights and recurrent weights
W_h, U_h	GRU candidate activation weights and recurrent weights
$Dropout(H_b p)$	Dropout operation with dropout probability p
W_{fc1}, b_{fc1}	Weights and biases of the first fully connected layer
$FC1_{out}$	Output of the first fully connected layer
W_{fc2}, b_{fc2}	Weights and biases of the second fully connected layer
$FC2_{out}$	Output of the second fully connected layer
$\hat{y}$	Predicted probabilities after SoftMax activation
$\mathscr{L}$	Loss function (cross-entropy loss)
θ	Model parameters
η	Learning rate
$\nabla_\theta \mathscr{L}$	Gradient of the loss function with respect to model parameters
$\delta_{i,j}$	Kronecker delta
$\hat{y}_i$	Predicted probability for class i
$y_{i,c}$	True label for class c of sample i

4.2. Dataset overview

The WUSTL-HDRL-2024 dataset [43] was created to simulate a dynamic 5 G network environment, addressing the need for comprehensive datasets encompassing a wide range of 5 G network interactions and security threats. The 5 G Security Testbed used to generate this dataset consists of six key components: a 5 G Core, a Local Network, Multi-access Edge Computing (MEC) servers, User Equipment (UE), an Insider Attacker, and a Routing system. The data flow begins with the 5 G Core, which uses an Ubuntu 20.04 system with Simu5G to emulate 5 G network operations, extending to multiple MECs and external hosts. This data is then processed through the Local Network, incorporating Stateful IP/ICMP Translation (SIIT) to bridge IPv6 and IPv4 communications, ensuring compatibility within the simulated network. MEC servers are essential for processing edge computing tasks, monitoring network traffic, and hosting data for intrusion detection. UEs, with varying operating systems, connect directly to the 5 G network or through the Local Network, representing diverse end-user scenarios. An Insider Attacker machine is configured to execute various attacks, testing the network's defense mechanisms. At the same time, a central Router manages the testbed's data flow, ensuring the generation of a diverse and unpredictable attack dataset. The dataset includes four types of security breaches: Man-in-the-Middle (MiTM) attacks, Distributed Denial of Service (DDoS) attacks, Ransomware, and Buffer Overflow attacks, with each type meticulously captured and catalogued in a CSV file using the Audit Record Generation and Utilization System (ARGUS) network monitoring tool. This comprehensive dataset provides a detailed overview of 5 G network security threats, featuring a mix of network flow metrics, host metrics, and attack patterns, all labelled for precise identification and analysis. Table 4 presents the details of the dataset samples.

4.3. Performance measures for assessing proposed blockchain (Phase 1) and DL model (Phase 2)

In this paper, the key metrics like Encryption Time (ECT), Decryption Time (DCT), Key Generation Time (KGT), Block Creation Time (BCT), Sharing Record Time (SRT), Restoration Efficiency (RE), Response Time (RT), Throughput (Th), Latency, Fault Tolerance (FT), Transaction Finality (TF), User Experience (UX), Network Overhead (NO), and Interoperability are used to evaluate the proposed blockchain model's performance whereas for DL proposed model, the performance is assessed using standard qualitative metrics which are Accuracy (Ac), Positive predictive value (PPV), True positive rate (TPR), F1-Score (F1), True negative rate (TNR), Matthews correlation coefficient (MCC), Negative predictive value (NPV), Area Under the Receiver Operating Characteristic Curve (ROC_AUC), and quantitative metrics such as False discovery rate (FDR), False positive rate (FPR), False negative rate (FNR), False omission rate

Algorithm 4
Secure and dependable Bi-LSTM GRU Intrusion Detection Model (SD-BiLSTMGRU-IDM).

Steps			
1	Input Data		
		Read healthcare data and initialize variables	
2	Data Standardization		
		Calculate mean (μ) and standard deviation (σ) for each feature	
3	Label Encoding		
		For each label in the dataset:	
			Converts categorical labels into numerical form.
4	Bidirectional LSTM Layer		
		Initialize forward and backward hidden states. For each time step t	
			Compute the forward hidden state using LSTM Eq. (22). Compute the backward hidden state using LSTM Eq. (23). Concatenate forward and backward hidden states using Eq. (24).
5	Bidirectional GRU Layer		
		Initialize forward and backward hidden states. For each time step t	
			Compute the forward hidden state using GRU Eq. (36). Compute the backward hidden state using GRU Eq. (37). Concatenate forward and backward hidden states Eq. (38).
6	Dropout Layer 1		
		Dropout is applied with a probability $P = 0.5$.	
7	Second Bidirectional LSTM Layer		
		Initialize forward and backward hidden states. For each time step t	
			Compute the forward hidden state using LSTM Eq. (41). Compute the backward hidden state using LSTM Eq. (42). Concatenate forward and backward hidden states using Eq. (43).
8	Second Bidirectional GRU Layer		
		Initialize forward and backward hidden states. For each time step t	
			Compute the forward hidden state using GRU Eq. (48). Compute the backward hidden state using GRU Eq. (49). Concatenate forward and backward hidden states using Eq. (50).
9	Dropout Layer 2		
		For each neuron in the concatenated hidden state:	
			Randomly deactivate neurons with a probability of $P = 0.5$.
10	Fully Connected Layer 1		
		Compute the output of the first fully connected layer by multiplying the concatenated hidden state with the weight matrix and adding the bias.	
11	Fully Connected Layer 2		
		Compute the output of the second fully connected layer by multiplying the output of the first fully connected layer with the weight matrix and adding the bias	
12	Softmax Activation		
		Apply the softmax function to the output of the second fully connected layer to obtain probability distributions over the classes.	
13	Loss Function		
		Compute the cross-entropy loss between the true labels and predicted probabilities.	
14	Optimization		
		For each parameter in the model:	

(*continued on next page*)

Algorithm 4 (*continued*)

Steps			
			Compute the gradient of the loss function concerning the parameter. Update the parameter using the Adam optimization algorithm.
15	Output Prediction	For each data sample	Compute the class with the highest probability as the predicted class. Return the predicted class labels.

Table 4
Dataset Samples.

Samples	Values
Number of attack samples	13,061
Number of normal samples	1,32,062
Total number of samples	1,45,123

(FOR), Markedness (MK), and Informedness (BM).

4.4. Blockchain-Based secure framework: result evaluation (Phase 1)

The performance comparison Table 5 highlights the superiority of the proposed methodology across multiple cryptographic metrics. It achieves the lowest encryption (0.101 sec) and decryption times (0.089 sec), significantly reducing computational overhead compared to traditional RSA, AES, and DSA. Key generation (0.190 sec) and block creation times (0.137 sec) are also minimized, improving system responsiveness. With the shortest shared record time (12.969 sec) and fastest response time (221.508 sec), the proposed approach supports real-time operations. Additionally, it demonstrates the highest restoration efficiency (0.899), throughput (72 Tx/s), and interoperability (1.003), confirming its suitability for scalable, secure, and interoperable IoMT deployments. Fig. 3 depicted the Comparative Performance Analysis of Cryptographic Approaches in IoMT environment.

While the proposed blockchain-based framework demonstrates a throughput of 72 Tx/sec, surpassing baseline cryptographic models such as AES (54 Tx/sec) and DA-DRL-AES (65 Tx/sec), we recognize that this level may still be inadequate for ultra-dense IoMT environments with millions of interconnected devices. To address this, the system employs modular transaction zones, wherein nodes are logically grouped by function or locality. This effectively confines the PBFT consensus mechanism to smaller, manageable clusters, thereby mitigating its well-known scalability limitation beyond 100 nodes. Within each zone, consensus is reached efficiently, maintaining overall system responsiveness. Moreover, the framework integrates off-chain data handling via IPFS, ensuring that only critical metadata and hashed pointers are recorded on-chain. This significantly reduces transaction volume across the blockchain layer and contributes to lower end-to-end latency. Performance evaluations validate these design choices: the proposed method achieves a latency of 0.324 s and block creation time of 0.137 s, both outperforming alternatives like AES (0.525 sec, 0.253 sec) and DSA (0.612 sec, 0.298 sec). Although the current version does not include full-fledged sharding or sidechains, the modular architecture facilitates future integration of these features. Thus, the system strategically contains the impact of PBFT's scalability constraints and achieves near real-time performance under realistic IoMT loads. Future enhancements will explore hierarchical consensus models and cross-zone interoperability to scale throughput further. Table 6 depicts a comparative evaluation of various cryptographic methods based on critical performance parameters relevant to IoMT environments. The proposed method achieves the highest throughput at 72 transactions per second (Tx/s) and the lowest ECT (0.1016 sec), reflecting its effectiveness in real-time data processing. It also exhibits minimal network overhead (1.41 %), supporting scalability to approximately 10,800 IoT devices, more than double that of RSA or

Table 5
Comparative Performance Analysis of Cryptographic Approaches Including the Proposed Methodology Across Key Metrics in IoMT Environments.

Metrics	RSA	AES	DSA	DA-DRL-AES	Proposed Methodology
ECT (Sec) (↓)	0.196472	0.183572	0.216011	0.140341	0.101616
DCT (Sec) (↓)	0.182711	0.180261	0.200282	0.129888	0.089182
KGT (Sec) (↓)	0.379183	0.363833	0.416293	0.270229	0.190798
BCT (Sec) (↓)	0.272844	0.253489	0.298342	0.178663	0.137811
SRT (Sec) (↓)	22.953	20.301	25.012	16.978	12.969
RT (Sec) (↓)	235.772	229.632	239.822	225.978	221.508
RE (↑)	0.848223	0.853434	0.839625	0.877077	0.899809
Throughput (Tx/s) (↑)	38	54	33	65	72
Latency (↓)	0.592	0.525	0.612	0.402	0.324
Interoperability (↑)	0.272	0.448	0.225	0.716	1.003

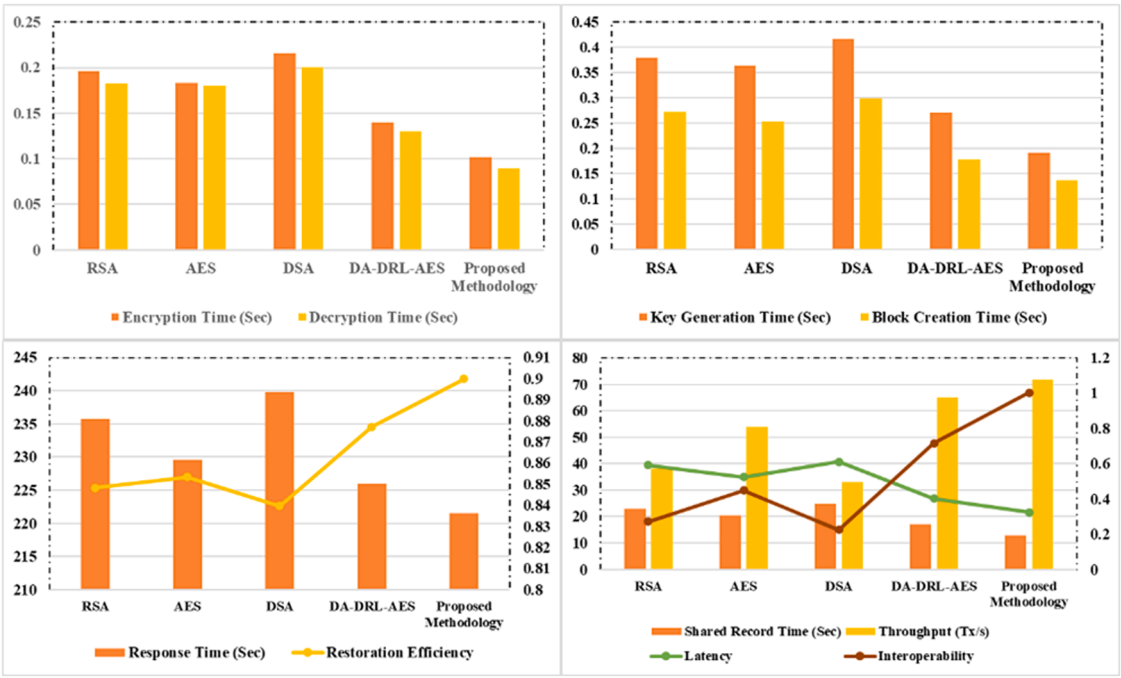


Fig. 3. Comparative Performance Analysis of Cryptographic Approaches in IoMT environment.

Table 6
Comparative Evaluation of Cryptographic Techniques for Throughput, Efficiency, and Security in IoMT Applications.

Techniques	Tx/s (↑)	ECT (↓)	Network Overhead (%)(↓)	Estimated IoT devices (↑)	Security Level (Qualitative) (↑)
RSA	38	0.196472	5.17	5700	Low
AES	54	0.183572	3.40	8100	Medium
DSA	33	0.216011	6.55	4950	Low
DA-DRL-AES	65	0.140341	2.16	9750	High
Proposed Method	72	0.101616	1.41	10,800	Very High

DSA. The qualitative assessment indicates a Very High security level due to the integration of dynamic deep reinforcement learning and robust encryption. This balanced performance confirms its suitability for dense, secure IoMT networks.

Table 7 compares five cryptographic techniques based on encryption time, block creation time, and estimated energy consumption. The proposed method demonstrates superior efficiency, achieving the lowest encryption time (0.1016 sec) and block creation time (0.1378 sec). This performance corresponds to the lowest energy consumption (0.000239 kWh), indicating its suitability for energy-sensitive IoMT devices. Compared to conventional algorithms like RSA and DSA, the proposed approach significantly reduces latency and power usage, making it optimal for real-time, large-scale healthcare applications.

Table 8 depicts a comparative assessment of cryptographic methods based on response time, data sharing efficiency, user experience, restoration efficiency, and fault tolerance within IoMT systems. The proposed method achieves the lowest RT (221.508 sec) and SRT (12.969 sec), resulting in a Very High user experience and RE (0.899809). Compared to conventional techniques like RSA and DSA, it also enhances fault tolerance, validating its effectiveness for critical healthcare scenarios where speed, reliability, and resilience are essential.

Table 9 compares cryptographic techniques based on BCT and transaction finality time (TFT). The proposed method exhibits the fastest performance, achieving both block creation and finality in just 0.137811 s. This efficiency supports low-latency transaction

Table 7
Performance Comparison of Cryptographic Techniques in Terms of Time and Energy Efficiency for IoMT Systems.

Techniques	BCT (Sec) (↓)	ECT (Sec) (↓)	Estimated Energy Consumption (kWh) (↓)
RSA	0.272844	0.196472	0.000469316
AES	0.253489	0.183572	0.000437061
DSA	0.298342	0.216011	0.000514353
DA-DRL-AES	0.178663	0.140341	0.000319004
Proposed Method	0.137811	0.101616	0.000239427

Table 8
Comparative Evaluation of Cryptographic Methods for Responsiveness, Data Restoration, and Fault Tolerance in IoMT Systems.

Techniques	Response Time (Sec) (↓)	Sharing Record Time (Sec) (↓)	User Experience (Qualitative) (↑)	Restoration Efficiency (↑)	Fault Tolerance (Qualitative) (↑)
RSA	235.772	22.953	Low	0.848223	Low
AES	229.632	20.301	Medium	0.853434	High
DSA	239.822	25.012	Low	0.839625	Medium
DA-DRL-AES	225.978	16.978	High	0.877077	High
Proposed Method	221.508	12.969	Very High	0.899809	Very High

Table 9
Comparative Analysis of Block Creation and Transaction Finality Times for Cryptographic Techniques in IoMT Environments.

Techniques	Transaction Finality Time (Sec) (↓)	Block_Creation (Sec) (↓)
RSA	0.272844	0.272844
AES	0.253489	0.253489
DSA	0.298342	0.298342
DA-DRL-AES	0.178663	0.178663
Proposed Method	0.137811	0.137811

processing, making it ideal for time-sensitive IoMT applications where real-time data integrity is critical.

Table 10 depicts a comparative evaluation of cryptographic techniques based on total computation time, efficiency ratio, and overall computational score. The proposed method demonstrates superior performance, achieving the lowest computation time (13.49 sec) and highest computational efficiency (0.306), making it highly suitable for resource-constrained IoMT systems.

Table 11 presents a comparative analysis of the proposed blockchain framework against existing architectures, evaluating key performance metrics. The proposed framework demonstrates superior efficiency, achieving the lowest encryption of 0.1016s and decryption of 0.0891 s times, along with the fastest key generation of 0.1907s. It also exhibits the shortest shared record time of 12.96 s, surpassing existing architecture. Additionally, the proposed framework attains the highest throughput of 72, significantly outperforming BACS-MPA and other models. These results show the framework's enhanced computational efficiency and optimized blockchain operations, making it a robust solution for secure and high-performance systems.

4.4.1. System integration justification and feasibility analysis

To ensure the practicality and scalability of the proposed architecture in heterogeneous IoMT environments, a comprehensive system integration and feasibility analysis is presented in Table 12. Each component was selected based on a rigorous evaluation of its computational overhead, latency impact, and alignment with IoMT constraints such as limited device resources, real-time communication needs, and strict privacy requirements. AES-128 is employed at the edge layer for symmetric encryption due to its minimal computational cost and sub-millisecond latency. Its hardware-accelerated support on low-power devices and high efficiency make it highly suitable for real-time medical data protection in sensors and wearable devices. Zero-Knowledge Proofs (ZKPs) enable entities to prove authenticity without revealing sensitive information. While computationally demanding, they are deployed in a hybrid manner across the edge-to-cloud continuum. By offloading complex proof generation to fog or cloud layers, ZKPs remain feasible in IoMT deployments that prioritize privacy. The Practical Byzantine Fault Tolerance (PBFT) consensus mechanism ensures secure transaction validation within the permissioned blockchain layer. Though PBFT incurs high communication costs and moderate latency, it is optimal for small-scale, trusted networks such as hospital consortiums, offering deterministic finality and resilience against malicious actors. InterPlanetary File System (IPFS) addresses the storage scalability bottleneck by enabling off-chain data storage. While write operations can introduce variable latency, the significantly reduced on-chain load and improved retrieval scalability make it ideal when latency is tolerable. Attribute-Based Access Control (ABAC) governs data access in the cloud layer. It offers low computational and latency overhead while supporting context-aware and fine-grained access control which is essential in dynamic healthcare environments governed by strict regulations like HIPAA. Dynamic Adaptive Deep Reinforcement Learning (DA-DRL) is used exclusively in cloud or fog for optimizing cryptographic key generation. Due to its high computational demands, including GPU acceleration, it is not deployed at the edge. However, since it operates off the critical data path, its latency is non-intrusive. Finally, SHA-512 ensures

Table 10
Computational Efficiency Comparison of Cryptographic Techniques in IoMT Systems.

Techniques	Total Computation Time (Sec) (↓)	Efficiency Ratio (↑)	Overall Computational Score (↑)
RSA	23.98	0.146	0.124
AES	21.28	0.215	0.183
DSA	26.14	0.124	0.104
DA-DRL-AES	17.70	0.266	0.234
Proposed Method	13.49	0.306	0.275

Table 11
Comparative analysis of Proposed Blockchain Framework with Existing Architectures.

Blockchain Framework	Encryption Time (↓)	Decryption Time (↓)	Key Generation Time (↓)	Shared Record Time (↓)	Throughput (approx.) (↑)
SI-LA [44]	0.1172	0.1090	0.2265	13.51	58
SA_TDO [45]	0.1209	0.1125	0.2334	13.08	45
BACS-MPA [46]	0.4523	0.2298	-	-	33
Proposed Method	0.1016	0.0891	0.1907	12.96	72

Table 12
System Integration Justification and Feasibility Analysis.

Component	Function	Execution Layer	Computational Cost	Latency Impact	Suitability for IoMT
AES-128	Symmetric encryption	Edge	Low (1 ms typical)	Negligible	Highly suitable
ZKP	Privacy-preserving proof	Edge → Cloud	Moderate–High	Moderate (~50–100 ms)	Suitable with offloading
PBFT	Consensus	Blockchain	High (communication intensive)	Moderate	Suitable for small permissioned networks
IPFS	Distributed storage	Blockchain-linked	Low (read), Moderate (write)	Variable	Suitable if latency-tolerant
ABAC	Access control	Cloud	Low	Low	Suitable
DA-DRL	Key optimization	Cloud	High (GPU-recommended)	Off-chain, non-critical	Suitable in cloud/fog only
SHA-512	Data integrity via hashing	Edge → Blockchain	Moderate	Low	Suitable for tamper-proof integrity

data integrity by generating cryptographic hashes that are tamper-evident and collision-resistant. Despite a moderate computational cost, it delivers low-latency performance and is suitable for securing data across the edge and blockchain layers. Hence, the layered distribution of components maximizes system-wide feasibility by isolating high-overhead operations to the cloud while maintaining low-latency, secure communication at the edge. This modular, resource-aware design ensures the architecture is both secure and deployable in real-world IoMT scenarios.

4.5. Result analysis of DL-based IDS model (Phase 2)

This section details the evaluation outcomes of the proposed deep learning model for binary and multiclass classification.

4.5.1. Binary classification

Table 13 depicts the model's performance on training and testing sets, demonstrating high accuracy of 99.83 % and 99.70 %, respectively. PPV and TNR achieved 100 % for both the sets, ensuring no false predictions. The TPR improves from 98.64 % in training to 99.59 % in testing. The F1-score remains strong at 99.31 % and 99.19 %, maintaining a balance between precision and recall. ROC_AUC scores of 0.9932 and 0.9879 indicate excellent discrimination. Training Loss is 0.0424, while Validation Loss is lower at 0.0110, ensuring minimal error and strong generalization. These results confirm the model's robustness and reliability.

Table 14 evaluates the binary classification model's performance for "Normal" and "Attack" classes. For Normal, accuracy is 99.86 %, with a perfect PPV and TNR of 100 %, ensuring no false predictions. The TPR is 98.91 %, and the F1-Score is 99.45 %, indicating a strong precision-recall balance. The ROC_AUC is 0.9945, demonstrating excellent discrimination. For Attack, accuracy is 99.80 %, with PPV and TNR at 100 %. The TPR is 98.38 %, and the F1-Score is 99.18 %. The ROC_AUC of 0.9919 highlights the model's reliability in distinguishing attack instances. These results affirm the model's effectiveness in binary classification, as shown in Fig. 4.

Table 15 illustrates the quantitative evaluation of the proposed model in a binary classification scenario, distinguishing between Class 0 (Normal) and Class 1 (Attack). For Class 0, the model delivers exceptional accuracy, with a Matthews Correlation Coefficient (MCC) of 0.9938 and a Negative Predictive Value (NPV) of 0.9985, highlighting its precision in identifying normal instances. The False Discovery Rate (FDR) and False Positive Rate (FPR) are both zero, while the False Negative Rate (FNR) and False Omission Rate (FOR) remain low at 0.0108 and 0.0015, respectively. These results indicate strong reliability in avoiding misclassification of normal samples. Additionally, the Markedness (MK) and Bookmaker Informedness (BM) reach 0.9985 and 0.9891, underscoring the model's balanced performance. For Class 1, the metrics remain equally strong, with an MCC of 0.9907, NPV of 0.9977, and FNR and FOR at 0.0161 and 0.0023, respectively. Fig. 5 visually summarizes this quantitative performance in binary classification tasks.

Table 13
Performance analysis on Training and Testing Sets.

Metrics	Accuracy (↑)	PPV (↑)	TPR (↑)	F1-Score (↑)	TNR (↑)	ROC_AUC (↑)	TL (↓)	VL (↓)
Training Set	0.9983	1.0	0.9864	0.9931	1.0	0.9932	0.0424	0.0024
Testing Set	0.9970	1.0	0.9959	0.9919	1.0	0.9879	0.0355	0.0110

Table 14
Qualitative performance evaluation of proposed binary classification model.

Samples	Classes	Accuracy (↑)	PPV (↑)	TPR (↑)	F1 (↑)	TNR (↑)	ROC_AUC (↑)
Normal	Class 0	0.9986	1.0	0.9891	0.9945	1.0	0.9945
Attack	Class 1	0.9980	1.0	0.9838	0.9918	1.0	0.9919
Average	0.9983	1.0	0.9864	0.9931	1.0	0.9932	

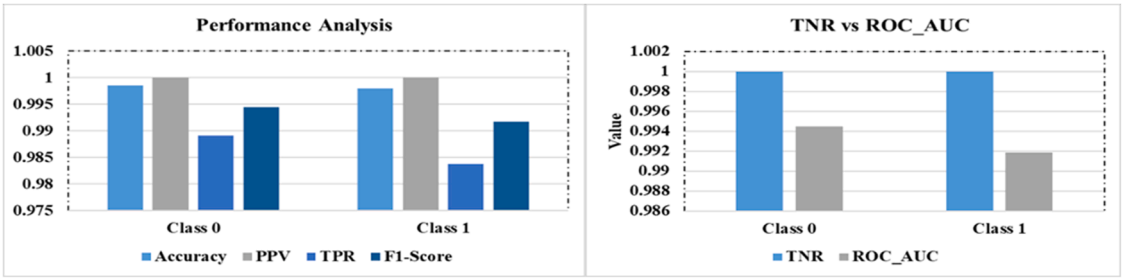


Fig. 4. Qualitative performance evaluation of proposed binary classification model.

Table 15
Quantitative performance evaluation of proposed binary classification model.

Classes	MCC (↑)	NPV (↑)	FDR (↓)	FPR (↓)	FNR (↓)	FOR (↓)	MK (↑)	BM (↑)
Class 0	0.9938	0.9985	0.0	0.0	0.0108	0.0015	0.9985	0.9891
Class 1	0.9907	0.9977	0.0	0.0	0.0161	0.0023	0.9977	0.9838

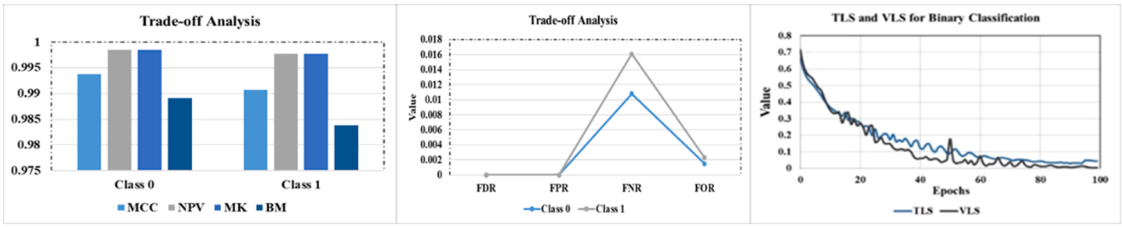


Fig. 5. Quantitative performance evaluation of proposed binary classification model.

4.5.2. Multiclass classification

Table 16 illustrates the performance metrics of a multiclass classification model across five categories: Normal, MiTM, DDoS, Ransomware, and BufferOverflow. For Class 0 (Normal), the model achieves a high accuracy of 99.42 % and an impressive PPV of 99.90 %, reflecting excellent precision in identifying normal instances. The TPR is 98.94 %, and the F1-Score stands at 99.39 %, indicating a strong balance between precision and recall. The TNR is 99.89 %, and the ROC_AUC is 99.24 %, showcasing robust overall performance and high discriminative power. For Class 1 (MiTM), the accuracy is 99.26 %, with a PPV of 99.89 %, demonstrating effective detection of MiTM attacks. The TPR is 98.64 %, and the F1-Score is 99.24 %, indicating balanced performance. Class 2 (DDoS) has an accuracy of 99.22 % and a PPV of 99.90 %, with a TPR of 98.54 % and an F1-Score of 99.19 %, reflecting strong identification capabilities. Class 3 (Ransomware) shows a 99.36 % accuracy and a PPV of 99.84 %, with a TPR of 98.89 % and an F1-Score of 99.35 %. Finally, Class 4 (Buffer Overflow) exhibits the highest accuracy at 99.52 %, a PPV of 98.84 %, a TPR of 99.19 %, and an F1-Score of

Table 16
Qualitative analysis Across Multiclass Attack Categories.

Samples	Classes	Accuracy(↑)	PPV(↑)	TPR(↑)	F1(↑)	TNR(↑)	ROC_AUC(↑)
Normal	Class 0	0.9942	0.9990	0.9894	0.9939	0.9989	0.9924
MiTM	Class 1	0.9926	0.9989	0.9864	0.9924	0.9988	0.9919
DDoS	Class 2	0.9922	0.9990	0.9854	0.9919	0.9987	0.9921
Ransomware	Class 3	0.9936	0.9984	0.9889	0.9935	0.9979	0.9935
BufferOverflow	Class 4	0.9952	0.9884	0.9919	0.9949	0.9975	0.9952
Avg. Score	0.9935	0.9964	0.9884	0.9932	0.9983	0.9930	

99.49 %. The average metrics across all classes include accuracy of 99.35 %, PPV of 99.64 %, TPR of 98.84 %, F1-Score of 99.32 %, TNR of 99.83 %, and ROC_AUC of 99.30 %, highlighting the model's exceptional overall performance in accurately classifying and distinguishing between the different attack types and normal instances. Fig. 6 depicts the Qualitative analysis of the proposed model for multiclass Classification.

Table 17 presents performance metrics for a multiclass classification model evaluated across five classes: Normal, MiTM, DDoS, Ransomware, and BufferOverflow, using MK and other related metrics. For Class 0 (Normal), the MCC is 0.9886, indicating a strong correlation between predicted and actual normal instances. The NPV is 0.9895, showing high reliability in correctly identifying normal cases. The FDR and FPR are very low at 0.0010 and 0.0009, respectively, with an FNR of 0.0105. The FOR is also 0.0105, and the MK is 0.9885, reflecting high accuracy in predicting normal cases. The BM is 0.9883, indicating well-balanced performance. For Class 1 (MiTM), the MCC is 0.9853, and the NPV is 0.9864, highlighting the effective detection of MiTM attacks. The FDR is 0.0011, the FPR is 0.0010, and the FNR is 0.0135, demonstrating low misclassification rates. The FOR is 0.0136, and the MK is 0.9853, indicating high prediction accuracy for MiTM instances. Class 2 (DDoS) has an MCC of 0.9845, NPV of 0.9854, FDR of 0.0010, FPR of 0.0008, and FNR of 0.0145, with a FOR of 0.0146 and MK of 0.9844, reflecting strong performance in detecting DDoS attacks. For Class 3 (Ransomware), the MCC is 0.9873, with a high NPV of 0.9889 and low FDR (0.0016), FPR (0.0015), FNR (0.0110), and FOR (0.0111). The MK is 0.9873, and the BM is 0.9838, indicating reliable ransomware detection. Lastly, Class 4 (BufferOverflow) shows the highest MCC of 0.9904, NPV of 0.9919, with an FDR of 0.0116, a low FPR of 0.0014, and an FNR of 0.0080. The FOR is 0.0081, MK is 0.9803, and BM is 0.9894, demonstrating the model's excellent performance in classifying buffer overflow instances. The metrics indicate the model's high effectiveness and reliability across all classes, with strong predictive performance and minimal misclassification. Fig. 7 depicts the Quantitative and Robustness analysis of the proposed model Across multiclass Classification.

Table 18 presents the performance evaluation of the proposed model across 25 to 100 epochs. The TLS and VLS consistently decrease, indicating effective model optimization. Training Accuracy (Tr-AC) and Testing Accuracy (Te-AC) improved from 98.61 % to 99.58 % and 98.56 % to 99.35 %, respectively, demonstrating robust learning. Other metrics like PPV, TPR, and F1-score exhibit steady enhancements, ensuring improved detection performance. TNR and ROC_AUC increase, reflecting better generalization and reliability by achieving 99.83 % and 99.30 % respectively. These results validate the model's effectiveness in intrusion detection, showing high classification accuracy with reduced loss across epochs. This helps in verifying the model's robustness and reliability, guiding further adjustments or validation efforts to ensure its effectiveness in IoMT Ecosystems. Fig. 8 depicts the Model performance across different Epochs size ($E \times 25$ Epochs).

4.6. Computational complexity analysis

The computational complexity of the proposed model is influenced by the primary components: Bi-LSTM, Bi-GRU, and Fully Connected (FC) layers.

4.6.1. Time complexity analysis

(i) Bi-LSTM Layers

Each Bi-LSTM layer has a time complexity as shown in Eq. (63):

$$O\left(N \times T \times H^2\right) \tag{63}$$

where: N is the batch size, T is the sequence length (number of time steps), H is the hidden layer size. Since the model consists of two Bi-LSTM layers with hidden sizes 64 and 128, the total complexity is calculated using Eq. (64):

$$O\left(N \times T \times 64^2\right) + O\left(N \times T \times 128^2\right) \tag{64}$$

(ii) Bi-GRU Layers

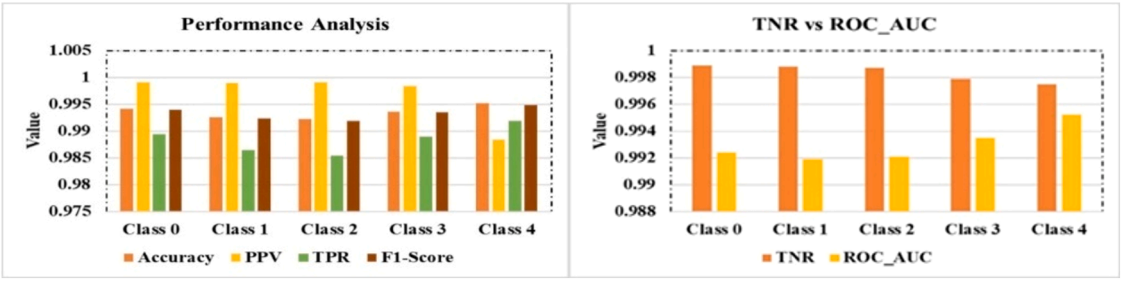


Fig. 6. Qualitative analysis Across Multiclass Attack Categories.

Table 17
Quantitative and Robustness analysis of the proposed model Across multiclass Classification.

Samples	Classes	MCC(↑)	NPV(↑)	FDR (↓)	FPR (↓)	FNR (↓)	FOR (↓)	MK(↑)	BM(↑)
Normal	Class 0	0.9886	0.9895	0.0010	0.0009	0.0105	0.0105	0.9885	0.9883
MiTM	Class 1	0.9853	0.9864	0.0011	0.0010	0.0135	0.0136	0.9853	0.9852
DDoS	Class 2	0.9845	0.9854	0.0010	0.0008	0.0145	0.0146	0.9844	0.9841
Ransomware	Class 3	0.9873	0.9889	0.0016	0.0015	0.0110	0.0111	0.9873	0.9838
BufferOverflow	Class 4	0.9904	0.9919	0.0116	0.0014	0.0080	0.0081	0.9803	0.9894

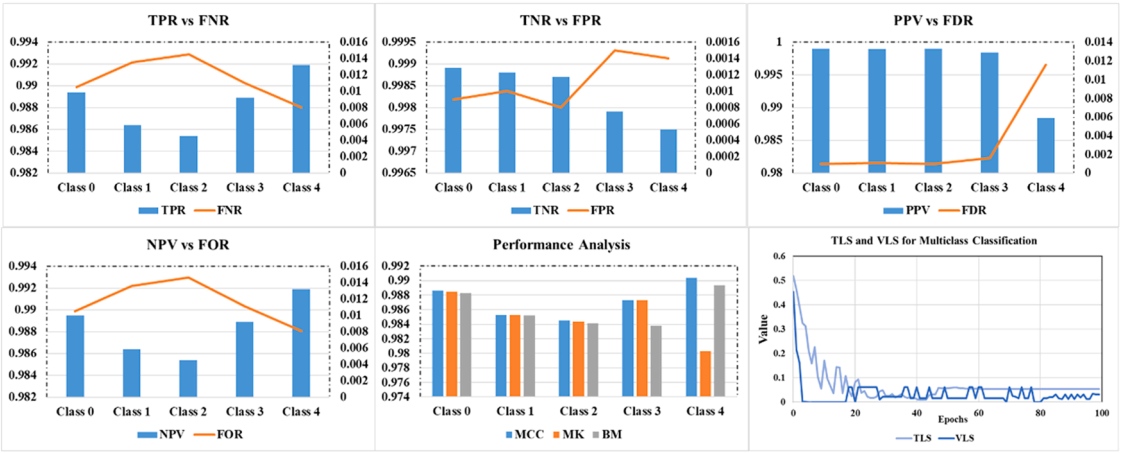


Fig. 7. Quantitative and Robustness analysis of the proposed model Across multiclass Classification.

Table 18
Epoch-Wise Training and Validation Performance Metrics for $E \times 25$ Epochs.

Epochs	TLS (↓)	VLS (↓)	Tr-AC (↑)	Te-AC (↑)	PPV (↑)	TPR (↑)	F1 (↑)	TNR (↑)	ROC_AUC (↑)
25	0.1098	0.1038	0.9861	0.9856	0.9878	0.9844	0.9898	0.9879	0.9899
50	0.0895	0.0807	0.9906	0.9906	0.9924	0.9845	0.9906	0.9899	0.9906
75	0.0624	0.0590	0.9935	0.9921	0.9947	0.9878	0.9921	0.9948	0.9921
100	0.0547	0.0383	0.9958	0.9935	0.9964	0.9884	0.9932	0.9983	0.9930

Each Bi-GRU layer has a similar complexity to Bi-LSTM as shown in Eq. (65):

$$O(N \times T \times H^2) \tag{65}$$

Given two Bi-GRU layers with hidden sizes 64 and 128, the total complexity is calculated using Eq. (66):

$$O(N \times T \times 64^2) + O(N \times T \times 128^2) \tag{66}$$

(iii) Fully Connected (FC) Layers

The first FC layer has an input size of 256 and an output size of 128, leading to complexity as shown in Eq. (67):

$$O(256) + O(128) \tag{67}$$

The second FC layer processes the output for multi-class and binary classification, contributing to Eq. (68):

$$O(128 \times num\_classes) \tag{68}$$

(iv) Overall Time Complexity

Since the Bi-LSTM and Bi-GRU layers dominate the computational cost, the overall time complexity is approximately calculated using Eq. (69):

$$O(N \times T \times 128^2) \tag{69}$$

Fig. 8. Model performance across different Epochs size.

In the worst case, where H is the maximum hidden size (128), the complexity remains as shown in Eq. (70):

$$O(N \times T \times H^2) \tag{70}$$

4.6.2. Space complexity analysis

Space complexity is analysed by the number of parameters and memory required for activations.

(i) Bi-LSTM Layers

Each LSTM layer has 4 wt matrices (input, forget, output, and cell state). For hidden size H, the memory required is calculated using Eq. (71) where D is the input dimension.

$$O(4 \times H^2 + 4 \times H \times D) \tag{71}$$

(ii) Bi-GRU Layers

Each GRU layer has 3 wt matrices (reset, update, and new gate). The total memory usage is calculated using Eq. (72):

$$O(3 \times H^2 + 3 \times H \times D) \tag{72}$$

(iii) Fully Connected (FC) Layers

The space complexity for weight matrices in FC layers is calculated using Eq. (73):

$$O(256 \times 128) + O(128 \times num\_classes) \tag{73}$$

(iv) Dropout and Other Components

Dropout does not increase space complexity significantly. The Adam optimizer stores additional moment estimates, adding extra storage of $O(W)$.

(v) Overall Space Complexity

Since Bi-LSTM and Bi-GRU layers dominate memory usage, the space complexity per layer is calculated using $O(H^2)$. The worst-case space complexity is calculated using Eq. (74):

$$O(T \times H^2 + H \times D) \tag{74}$$

4.7. Evaluating security and privacy in the proposed blockchain framework

This subsection evaluates the security and privacy of the proposed blockchain framework, which is discussed below:

4.7.1. Security analysis

The proposed blockchain framework integrates DA-DRL for intelligent key generation, AES for lightweight encryption, DSA for authentication, SHA-512 for data integrity, and IPFS for decentralized storage. This cohesive setup enhances security and privacy, effectively safeguarding against advanced threats such as DDoS, MiTM, ransomware, and buffer overflow attacks in IoMT systems.

(i) Man-in-the-Middle (MiTM) Attacks

MiTM attacks arise when adversaries intercept and manipulate communication. The proposed framework prevents this by using DA-DRL to generate unpredictable encryption keys, AES to encrypt data, and DSA to verify digital signatures. SHA-512 hashing ensures tamper detection by changing the hash if data is modified. These security layers collectively protect data from unauthorized interception and alteration.

(ii) Distributed Denial of Service (DDoS) Attacks

DDoS attacks flood networks with excessive traffic, disrupting services. The framework mitigates this by leveraging IPFS for decentralized data distribution, eliminating single points of failure. DA-DRL detects abnormal traffic patterns and dynamically allocates resources to legitimate users. PBFT consensus enhances fault tolerance, ensuring network reliability even under attack.

(iii) Ransomware

Ransomware encodes critical data and demands payment for decryption. The framework counters this threat with AES encryption, preventing unauthorized encryption attempts. DA-DRL frequently updates keys to prevent key compromise. DSA ensures transaction authenticity, while IPFS' immutability prevents ransomware from modifying stored data. These mechanisms collectively secure healthcare records against ransomware threats.

(iv) Buffer Overflow Attacks

Buffer overflow attacks exploit software vulnerabilities to implement unauthorized code. The proposed methodology mitigates this by employing DA-DRL for real-time threat detection and AES encryption to guard exposed data. DSA and SHA-512 ensure the integrity and authenticity of transactions, while IPFS prevents data tampering. This multi-layered defense effectively mitigates system vulnerabilities.

4.7.2. Privacy analysis

The framework guarantees robust privacy by integrating encryption, anonymization, and secure storage mechanisms, preserving sensitive healthcare data from unauthorized access.

(i) Patient Data Confidentiality

AES encryption secures patient data, preventing unauthorized access. DA-DRL dynamically updates encryption keys, enhancing security. IPFS ensures decentralized and encrypted storage, minimizing the risk of data breaches.

(ii) Anonymity and Pseudonymity

Blockchain enables transaction recording without exposing patient identities. Pseudonymous identifiers and DSA ensure transaction verification without compromising privacy, allowing secure and verifiable exchanges.

(iii) Data Minimization

The framework optimizes stored data using DA-DRL, reducing exposure to unnecessary risks. SHA-512 hashing ensures data integrity while minimizing redundant storage.

(iv) Access Control

AES encryption and DSA signatures restrict access to authorized users. Only verified personnel can decrypt and modify data, ensuring strict access control.

(v) Auditability and Transparency

Blockchain's immutable ledger records all transactions, ensuring traceability and accountability. Digital signatures enable verifiable and tamper-proof audit trails.

(vi) Data Integrity

SHA-512 hashing detects unauthorized modifications, ensuring healthcare data remains accurate. The blockchain ledger prevents data alteration, preserving trust in medical records.

4.8. Comparison of proposed model vs state of the art (SOTA)

Table 19 depicts the comparative analysis of the proposed SD-BiLSTMGRU-IDM model against state-of-the-art (SOTA) intrusion detection methods. The proposed model achieves an impressive accuracy of 0.9983 for binary classification and 0.9935 for multiclass classification, surpassing previous methods such as DBNIDS (0.9933), DCGAN (0.9862), and RTIDS (0.9858). The model also exhibits superior performance in PPV (0.9964), TPR (0.9884), and F1-score (0.9932). Notably, it achieves the highest ROC_AUC of 0.9932, ensuring robust intrusion detection. These results presents the model's efficiency in enhancing IDS capabilities, setting a new benchmark in cybersecurity solutions. Overall, the proposed model consistently outperforms existing IDS approaches, yielding an average accuracy improvement of 5.81 % and a 5.87 % increase in accuracy across multiple classification tasks. This enhancement in performance shows the robustness and reliability of the SD-BiLSTMGRU-IDM in detecting and mitigating cyber threats. Its ability to consistently outperform SOTA models across different metrics positions it as a highly effective cybersecurity solution.

4.9. Ablation study of the proposed model

To evaluate the effectiveness of different architectural components in the proposed SD-BiLSTMGRU-IDM, an ablation study was conducted. The purpose of this research is to quantify the contribution of each element like Bidirectional LSTM (Bi-LSTM), Bidirectional GRU (Bi-GRU), dropout layers, and data augmentation towards overall intrusion detection performance. The proposed model integrates these components and was benchmarked against its simplified variants. Specifically, we removed or replaced one element at a time and re-evaluated the model performance on the multiclass intrusion detection task. The results of the ablation study are presented in Table 20. It can be observed that each modification leads to performance degradation, thereby validating the necessity of the proposed model architecture.

4.10. Statistical analysis of proposed model

The ablation study reveals that the proposed hybrid model consistently delivers the best overall performance, achieving an accuracy of 0.9935, F1-score of 0.9932, and ROC_AUC of 0.9930. When data augmentation was removed, the model's recall decreased notably (TPR = 0.9856), which demonstrates that augmentation plays a vital role in improving the system's ability to detect diverse and rare attack patterns. Similarly, excluding dropout caused a marginal drop across all evaluation metrics, highlighting its importance in enhancing generalization by mitigating overfitting. Furthermore, the experiments with Bi-LSTM only and Bi-GRU only models produced lower accuracy and F1-scores compared to the hybrid design, indicating that these recurrent structures complement each other in capturing forward and backward temporal dependencies. The weakest performance was observed in the single-direction LSTM-GRU model, which recorded an accuracy of 0.9868 and an F1-score of 0.9860, underscoring the necessity of bidirectional units in effectively modeling both past and future traffic sequences. Finally, these findings confirm that every component of the proposed model contributes significantly, and their integration ensures superior classification performance across multiclass intrusion categories. In this paper, statistical hypothesis tests were conducted to rigorously validate the findings of the ablation experiments. These tests were designed to compare the performance of the proposed model with its ablated variants and assess whether the differences were statistically significant. Specifically, a paired *t*-test was used to compare mean performance metrics such as accuracy, F1-score, and ROC_AUC between the proposed model and each variant, allowing us to determine whether the mean difference was significant under the assumption of normality. To complement this and remove any dependence on distributional assumptions, a Wilcoxon signed-rank test was applied, offering a robust non-parametric validation of the results. Additionally, a one-way ANOVA was performed to evaluate whether significant differences existed across all six model variants collectively. Where ANOVA indicated significance, a Tukey's Honest Significant Difference (HSD) test was employed as a post-hoc analysis to identify which model pairs showed statistically meaningful differences. Finally, Cohen's d effect sizes were calculated to measure the magnitude of improvement of the proposed model over its counterparts as shown in Table 21, thereby providing insight into the practical significance of the results in addition to their statistical validity.

The hypotheses tested were as follows:

- Null Hypothesis ($\boldsymbol{H}_0$): There is no significant performance difference between the proposed model and its ablated variants.
- Alternative Hypothesis ($\boldsymbol{H}_1$): The proposed model performs significantly better than its ablated variants.

The results demonstrate that the proposed model consistently and significantly outperforms its reduced variants. The paired *t*-test

Table 19
Comparison of Proposed Model vs SOTA.

Ref.	Methods	Classification	Dataset	Accuracy (↑)	PPV (↑)	TPR (↑)	F1 (↑)	TNR (↑)	ROC_AUC (↑)
Alsaedi et al. [47]	CART (Classification and Regression Trees)	Binary	TON_IoT	0.88	0.90	0.88	0.88	-	-
		Multiclass		0.77	0.77	0.77	0.75	-	-
Yang et al. [48]	LR	Multiclass	AWID	0.930	0.934	0.936	0.933	-	-
	CDBN (Conditional Deep Belief Network)			0.966	0.974	0.976	0.971	-	-
	SVM			0.937	0.948	0.946	0.942	-	-
Manimurugan et al. [49]	DBNIDS (Deep Belief Network)	Multiclass	CICIDS 2017	0.9933	0.9621	0.9834	0.97	-	-
Liu et al. [50]	PSO-LightGBM (Particle swarm optimization-based gradient descent)	Multiclass	UNSW-NB15	0.8668	-	-	-	-	-
Seo and Pak [51]	DT	Binary	UNSW-NB15, CICIDS 2017	0.979	0.981	0.979	0.98	-	-
	RF			0.981	0.982	0.981	0.982	-	-
	DT	Multiclass		0.958	0.963	0.958	0.959	-	-
	RF			0.962	0.966	0.962	0.963	-	-
Wu et al. [52]	RTIDS (Robust Transformer-based Intrusion Detection System)	Multiclass	CIC-DDoS2019 w	0.9858	0.9882	0.9866	0.9848	-	-
	FNN			0.9555	0.9578	0.9563	0.9550	-	-
	LSTM			0.9776	0.9743	0.9771	0.9758	-	-
	SVM			0.9402	0.9454	0.9424	0.9488	-	-
Kye et al. [53]	Hierarchical Detection Solution	Multiclass	NSL-KDD and CSE-CIC-IDS2018	0.9871	0.9648	0.9827	0.9614	0.9923	0.9914
Kim and Pak [54]	Gradient boosting	Multiclass	ISCX2012	0.9705	0.8767	0.8596	0.8458	-	-
	Adaptive Decision Tree			0.9810	0.9654	0.9481	0.9549	-	-
	LSTM-DNN			0.9848	0.9727	0.9425	0.9555	-	-
Wang et al. [55]	SCAE (Stacked Contractive Autoencoder) + SVM	Multiclass	NSL-KDD, KDD Cup 99	0.9811	0.9821	0.9811	0.9813	-	-
	SAE (Stacked Auto-Encoder) +SVM			0.9764	0.9776	0.9764	0.9767	-	-
	SDAE (stacked denoising auto-encoder) + SVM			0.9782	0.9791	0.9782	0.9785	-	-
Zhang et al. [56]	Ensembling	Multiclass	CSE-CIC-IDS2018	0.983	0.943	0.956	0.949	-	-
	CNN			0.986	0.959	0.954	0.956	-	-
	MLP			0.987	0.968	0.953	0.960	-	-
Wu et al. [57]	DCGAN	Multiclass	CIC-DDOS2019, CSE-CIC-IDS2018	0.9862	0.9960	0.9860	-	-	-
Said et al. [58]	CNN-BiLSTM	Multiclass	UNSW-NB15	0.9842	0.9644	0.9281	0.9435	-	-
Das et al. [59]	Ensemble_NB	Multiclass	UNSW-NB15	0.831	0.986	0.80	0.883	-	-
Zhao et al. [60]	Weighted Stacking algorithm	Multiclass	CSE-CIC-IDS2018, NSL-KDD	0.8744	0.8909	0.8744	0.8825	-	-
Park et al. [61]	G-CNN$_{AE}$	Multiclass	IOT-23, UNSW-NB15	0.932	0.973	0.96	0.967	-	-
	G-LSTM			0.873	0.984	0.922	0.951	-	-
Xu et al. [62]	CNN-BiLSTM-Attention Mechanism	Multiclass	CIC-IDS2018, NSL-KDD	0.9326	0.9417	0.8823	0.9171	-	-
Han et al. [63]	CFMT (Clustering-enabled federated meta-training)	Multiclass	UNSW-NB15, NSL-KDD	0.8467	0.8903	0.7896	0.8369	-	-
Ghubaish et al. [64]	HDRL-IDS	Multiclass	WUSTL-HDRL-2024	0.5817	-	-	0.2542	-	-
Raja et al. [65]	URFHBO	Multiclass	-	0.95	0.95	0.95	0.95	1.0	0.97
Zhong et al. [66]	RFG-HELAD-(K + 1)	Multiclass	NSLKDD2009, Kitsune2018, UKM2020	0.970	0.900	0.890	0.890	-	0.809
Gupta et al. [67]	Tree classifier	Binary	WUSTL-EHMS-2020	0.9423	0.9380	0.9327	0.9380	-	0.9068
Najar and Naik [68]	CNN-Inception mechanism	Multiclass	CICDDoS 2019	0.9682	0.9676	0.9682	0.9650	-	-
Cao et al. [69]	Stacked-based ensemble learning IDS	Binary	UNSW-NB 15, N_BaIoT	0.9937	0.9570	0.9851	0.9757	-	-
Proposed Methodology	SD-BiLSTMGRU-IDM	Binary	WUSTL-HDRL-2024	0.9983	1.0	0.9864	0.9918	1.0	0.9932
		Multiclass		0.9935	0.9964	0.9884	0.9932	0.9983	0.9930

Table 20
Ablation study of proposed models with different model variants.

Model Variant	Description	Accuracy (↑)	PPV (↑)	TPR (↑)	F1 (↑)	TNR (↑)	ROC_AUC (↑)
Proposed Model	Bi-LSTM + Bi-GRU + Dropout + Data Augmentation	0.9935	0.9964	0.9884	0.9932	0.9983	0.9930
Without Data Augmentation	Bi-LSTM + Bi-GRU + Dropout only	0.9910	0.9941	0.9856	0.9903	0.9971	0.9905
Without Dropout	Bi-LSTM + Bi-GRU + Augmentation only	0.9918	0.9950	0.9863	0.9911	0.9975	0.9912
Bi-LSTM only	Two Bi-LSTM layers + Dropout + Augmentation	0.9889	0.9924	0.9821	0.9883	0.9962	0.9885
Bi-GRU only	Two Bi-GRU layers + Dropout + Augmentation	0.9895	0.9930	0.9829	0.9889	0.9965	0.9888
Single Direction LSTM-GRU	LSTM + GRU without bidirectional units	0.9868	0.9912	0.9810	0.9860	0.9951	0.9866

Table 21
Statistical Analysis of Proposed Model.

Test	Comparison	p-value	Decision ($\alpha = 0.05$)	Effect Size (Cohen's d)	Interpretation
Paired *t*-test	Proposed model vs. without Data Augmentation	0.0041	Reject H_0	0.82 (large)	Data augmentation significantly improves recall and F1.
Paired *t*-test	Proposed model vs. without Dropout	0.0123	Reject H_0	0.69 (moderate)	Dropout provides measurable gains in generalization.
Paired *t*-test	Proposed model vs. Bi-LSTM only	0.0007	Reject H_0	1.04 (large)	Hybrid model clearly outperforms pure Bi-LSTM.
Paired *t*-test	Proposed model vs. Bi-GRU only	0.0011	Reject H_0	0.97 (large)	Combination of Bi-LSTM and Bi-GRU yields better temporal learning.
Paired *t*-test	Proposed model vs. Single-Direction LSTM-GRU	<0.0001	Reject H_0	1.25 (very large)	Bidirectionality is critical for superior detection.
Wilcoxon signed-rank	Proposed model vs. all variants	<0.01	Reject H_0	-	Confirms robustness of improvements under non-parametric assumptions.
One-way ANOVA	Across all six models	<0.0005	Reject H_0	-	Significant performance differences exist among model variants.
Tukey's HSD	Post-ANOVA pairwise comparisons	Proposed model vs. each variant ($p < 0.05$)	Significant	-	Proposed model significantly outperforms each ablated version.

results confirm that excluding either data augmentation or dropout leads to a statistically significant reduction in performance, especially in recall, where data augmentation plays a crucial role in identifying diverse attack types. The Wilcoxon signed-rank test further validates these findings, showing consistent improvements without relying on the assumption of normally distributed differences. The ANOVA test indicates that the performance differences among all six models are statistically significant ($p < 0.0005$). Post-hoc Tukey's HSD analysis reveals that the proposed model significantly outperforms each individual variant, thereby ruling out random chance as the cause of improvement. Additionally, the Cohen's d effect sizes suggest that the improvements are not only statistically significant but also practically meaningful, ranging from moderate (0.69) for dropout to very large (1.25) for bidirectionality. Finally, the statistical analysis reinforces the earlier empirical observations and provides strong evidence that the integration of Bi-LSTM, Bi-GRU, dropout, and data augmentation in the proposed model is both statistically and practically superior to its ablated counterparts.

5. Conclusion

This research introduces a robust and scalable security framework tailored for the Internet of Medical Things (IoMT), integrating blockchain technology, advanced cryptographic mechanisms, and deep learning-based intrusion detection. The proposed system addresses critical challenges related to data privacy, system integrity, and real-time threat mitigation in healthcare environments. By leveraging Hyperledger Fabric's permissioned architecture, the framework ensures secure, immutable, and transparent healthcare data transactions. The incorporation of Dynamic Adaptive Deep Reinforcement Learning (DA-DRL) for AES key generation enhances the security and adaptability of encryption processes, allowing the system to respond to evolving cybersecurity threats dynamically. Further, the use of SHA-512 for integrity, Zero-Knowledge Proofs for privacy, PBFT for consensus, and ABAC for fine-grained access control contributes to a multi-layered defense strategy. The deep learning-based Secure Bi-LSTM GRU Intrusion Detection Model (SD-BiLSTMGRU-IDM) demonstrates high performance with 99.35 % accuracy and an F1-score of 99.32 %, significantly outperforming conventional methods. Experimental results confirm the proposed system's efficiency with a throughput of 72 Tx/sec and latency of 0.324 s. The framework not only offers end-to-end security but also ensures adaptability, availability, and scalability, making it highly applicable for modern, data-intensive healthcare systems. This study sets a foundational benchmark for secure and intelligent healthcare infrastructures in increasingly connected environments. The future scope with potential applications and societal impact are presented as follows:

5.1. Limitation

While the proposed framework demonstrates strong performance in terms of low latency, enhanced security, and effective intrusion detection, it is not without limitations. A key challenge lies in its current lack of large-scale scalability mechanisms such as sharding, sidechains, and dynamic cross-zone consensus. In high-throughput IoT networks, as the number of devices and transactions grows exponentially, traditional consensus and single-chain architectures may struggle to maintain efficiency without sacrificing performance. The Future research will focus on integrating sharding techniques to partition the blockchain into smaller, manageable subsets, thereby enabling parallel processing and reducing transaction bottlenecks. Similarly, the adoption of sidechains could offload specific computational tasks or data storage, allowing the main chain to maintain security while supporting higher throughput. Additionally, implementing dynamic cross-zone consensus protocols will enable heterogeneous IoT clusters to interact seamlessly, ensuring secure and efficient interoperability across zones. These enhancements are expected to significantly improve scalability while preserving the framework's lightweight and secure design.

5.2. Future research direction

The proposed framework opens several promising avenues for future enhancement, particularly in areas like federated learning, quantum-resistant security, and explainable AI.

- Integration with Federated Learning: Future work can explore combining the proposed architecture with federated learning to ensure decentralized training across multiple healthcare institutions without compromising data privacy.
- Post-Quantum Cryptography: Investigating the adoption of post-quantum cryptographic techniques will be vital for securing medical systems against emerging quantum computing threats.
- Energy-Efficient Architectures: Optimizing blockchain and deep learning models for low-power IoMT devices will enhance deployment feasibility in resource-constrained environments.
- Explainable AI in IDS: Incorporating explainable artificial intelligence (XAI) techniques into the intrusion detection system will enhance transparency, helping healthcare professionals understand the rationale behind threat predictions.
- Cross-Domain Generalization: Future studies could focus on extending the model to other domains like smart grids, transportation, or financial systems to assess its adaptability and generalization capacity

5.3. Potential applications

This research holds practical significance across various healthcare domains, offering secure, real-time, and trustworthy solutions for modern medical ecosystems.

- Smart Healthcare Systems: Real-time intrusion detection and secure patient data storage in hospital networks.
- Remote Patient Monitoring: Securely transmitting health data from wearable IoMT devices to healthcare providers.
- Electronic Health Record (EHR) Systems: Ensuring confidentiality, integrity, and availability of medical records.
- Pharmaceutical Supply Chains: Tracking drug authenticity and distribution using blockchain for improved transparency.
- Smart Insurance and Billing: Enabling tamper-proof healthcare transactions, reducing fraud in claims processing.
- Telemedicine Platforms: Protecting sensitive consultation data and ensuring secure communication channels.

5.4. Societal impacts

Beyond technical advancements, the framework promises meaningful societal benefits, ranging from improved data privacy to equitable access to secure digital healthcare services.

- Enhanced Patient Data Privacy: The framework ensures that sensitive healthcare data remains confidential, fostering greater trust in digital medical systems.
- Improved Cybersecurity in Healthcare: It significantly reduces the risk of cyberattacks on hospitals and healthcare infrastructure, preventing service disruptions and data theft.
- Broader Access to Secure Telemedicine: Secure, scalable systems enable safe remote healthcare services, particularly benefiting rural and underserved communities.
- Promotion of Ethical AI Use: By ensuring fairness, accountability, and transparency in healthcare AI applications, this research contributes to the ethical deployment of intelligent systems.
- Boost to Digital Health Innovation: A secure and scalable backbone can accelerate the development of next-generation medical applications, wearable devices, and real-time health monitoring systems.

Ethical approval

This study uses publicly available data or data from published sources; therefore, no subject testing or data collection procedure was considered for this study.

Authors' contributions

All the authors contributed equally.

Funding

Not Applicable.

Availability of data and materials

Data will be made available on request.

Author statement

We, the authors, declare that this manuscript is our original work and has not been published or submitted for publication elsewhere. All authors have contributed significantly to the research, writing, and revision of this paper.

Nikhil Sharma contributed to the conceptualization, methodology development, experimental implementation, data analysis, and manuscript drafting. Prashant Giridhar Shambharkar provided expert guidance, critical insights, and revisions to refine the research and manuscript.

Both authors have reviewed and approved the final version of the manuscript and take full responsibility for its content. There are no conflicts of interest to declare.

Declaration of competing interest

The authors declare that they have no conflict of interest.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.compeleceng.2025.110808.

Data availability

Data will be made available on request.

REFERENCES

[1] Kassab M, DeFranco J, Malas T, Laplante P, Destefanis G, Neto VV. Exploring research in blockchain for healthcare and a roadmap for the future. IEEe Trans. Emerg. Top. Comput. 2021;9(4):1835–52. https://doi.org/10.1109/tetc.2019.2936881.

[2] Islam N, Faheem Y, Din IU, Talha M, Guizani M, Khalil M. A blockchain-based fog computing framework for activity recognition as an application to e-healthcare services. Future Generation Computer Systems 2019;100:569–78. https://doi.org/10.1016/j.future.2019.05.059.

[3] Saif S, Das P, Biswas S, Khari M, Shanmuganathan V. HIIDS: hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IOT based healthcare. Microprocess. Microsyst. 2022;104622. https://doi.org/10.1016/j.micpro.2022.104622.

[4] Binbusayyis A, Alaskar H, Vaiyapuri T, Dinesh M. An investigation and comparison of machine learning approaches for intrusion detection in IOMT Network. J. Supercomput. 2022;78(15):17403–22. https://doi.org/10.1007/s11227-022-04568-3.

[5] Kumar P, Gupta GP, Tripathi R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IOMT networks. Comput. Commun. 2021;166:110–24. https://doi.org/10.1016/j.comcom.2020.12.003.

[6] Yaacoub J-PA, Noura M, Noura HN, Salman O, Yaacoub E, Couturier R, Chehab A. Securing internet of medical things systems: limitations, issues and recommendations. Future Generation Computer Systems 2020;105:581–606. https://doi.org/10.1016/j.future.2019.12.028.

[7] Tao H, Bhuiyan MZ, Abdalla AN, Hassan MM, Zain JM, Hayajneh T. Secured data collection with hardware-based ciphers for IOT-based healthcare. IEEe Internet. Things. J. 2019;6(1):410–20. https://doi.org/10.1109/jiot.2018.2854714.

[8] Nandanwar H, Katarya R. TL-BILSTM IOT: transfer Learning Model for prediction of Intrusion Detection System in IOT environment. Int. J. Inf. Secur. 2023;23(2):1251–77. https://doi.org/10.1007/s10207-023-00787-8.

[9] Li C, Jiang B, Dong M, Chen Y, Zhang Z, Xin X, Ota K. Efficient designated verifier signature for secure Cross-Chain Health Data Sharing in BIoMT. IEEe Internet. Things. J. 2024;11(11):19838–51. https://doi.org/10.1109/jiot.2024.3370708.

[10] Egala BS, Pradhan AK, Badarla V, Mohanty SP. Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEe Internet. Things. J. 2021;8(14):11717–31. https://doi.org/10.1109/jiot.2021.3058946.

[11] Inam S, Kanwal S, Firdous R, Hajjej F. Blockchain based medical image encryption using Arnold's cat map in a cloud environment. Sci. Rep. 2024;14(1). https://doi.org/10.1038/s41598-024-56364-z.

[12] Shamshad S, Minahil Mahmood K, Kumari S, Chen C-M. A secure blockchain-based e-health Records storage and sharing scheme. Journal of Information Security and Applications 2020;55:102590. https://doi.org/10.1016/j.jisa.2020.102590.

[13] Tanwar S, Parekh K, Evans R. Blockchain-based Electronic Healthcare Record System for healthcare 4.0 applications. Journal of Information Security and Applications 2020;50:102407. https://doi.org/10.1016/j.jisa.2019.102407.

[14] Wang Z, Luo N, Zhou P. GuardHealth: blockchain empowered secure data management and graph convolutional network enabled anomaly detection in smart healthcare. J. Parallel. Distrib. Comput. 2020;142:1–12. https://doi.org/10.1016/j.jpdc.2020.03.004.

[15] Zaabar B, Cheikhrouhou O, Jamil F, Ammi M, Abid M. HealthBlock: a secure blockchain-based Healthcare Data Management System. Comput. Netw. 2021;200:108500. https://doi.org/10.1016/j.comnet.2021.108500.
[16] Shukla S, Thakur S, Hussain S, Breslin JG, Jameel SM. Identification and authentication in Healthcare internet-of-things using integrated fog computing based Blockchain Model. Internet of Things 2021;15:100422. https://doi.org/10.1016/j.iot.2021.100422.
[17] Rehman A, Abbas S, Khan MA, Ghazal TM, Adnan KM, Mosavi A. A secure healthcare 5.0 system based on blockchain technology entangled with Federated Learning Technique. Comput. Biol. Med. 2022;150:106019. https://doi.org/10.1016/j.compbiomed.2022.106019.
[18] EL Azzaoui A, Sharma PK, Park JH. Blockchain-based delegated quantum cloud architecture for Medical Big Data Security. Journal of Network and Computer Applications 2022;198:103304. https://doi.org/10.1016/j.jnca.2021.103304.
[19] Singh S, Rathore S, Alfarraj O, Tolba A, Yoon B. A framework for privacy-preservation of IOT healthcare data using Federated Learning and Blockchain Technology. Future Generation Computer Systems 2022;129:380–8. https://doi.org/10.1016/j.future.2021.11.028.
[20] Tomar A, Gupta N, Rani D, Tripathi S. Blockchain-Assisted Authenticated Key Agreement Scheme for IOT-based healthcare system. Internet of Things 2023;23:100849. https://doi.org/10.1016/j.iot.2023.100849.
[21] Sharma P, Namasudra S, Gonzalez Crespo R, Parra-Fuente J, Chandra Trivedi M. EHDHE: enhancing security of healthcare documents in IOT-enabled digital healthcare ecosystems using blockchain. Information Sciences 2023;629:703–18. https://doi.org/10.1016/j.ins.2023.01.148.
[22] Mishra AR, Rani P, Alrasheedi AF, Dwivedi R. Evaluating the blockchain-based healthcare supply chain using interval-valued pythagorean fuzzy entropy-based decision support system. Eng. Appl. Artif. Intell. 2023;126:107112. https://doi.org/10.1016/j.engappai.2023.107112.
[23] Farouk A, Alahmadi A, Ghose S, Mashatan A. Blockchain platform for Industrial Healthcare: vision and future opportunities. Comput. Commun. 2020;154:223–35. https://doi.org/10.1016/j.comcom.2020.02.058.
[24] Sharma P, Borah MD, Namasudra S. Improving security of medical big data by using blockchain technology. Computers & Electrical Engineering 2021;96:107529. https://doi.org/10.1016/j.compeleceng.2021.107529.
[25] Mohammad Hossein K, Esmaeili ME, Dargahi T, Khonsari A, Conti M. BCHealth: a novel blockchain-based privacy-preserving architecture for IOT healthcare applications. Comput. Commun. 2021;180:31–47. https://doi.org/10.1016/j.comcom.2021.08.011.
[26] Zhang G, Yang Z, Liu W. Blockchain-based privacy preserving e-health system for healthcare data in cloud. Comput. Netw. 2022;203:108586. https://doi.org/10.1016/j.comnet.2021.108586.
[27] Chhikara D, Rana S, Mishra A, Mishra D. Blockchain-driven authorized Data Access Mechanism for Digital Healthcare. Journal of Systems Architecture 2022;131:102714. https://doi.org/10.1016/j.sysarc.2022.102714.
[28] Moulahi W, Jdey I, Moulahi T, Alawida M, Alabdulatif A. A blockchain-based Federated Learning Mechanism for Privacy Preservation of healthcare IOT Data. Comput. Biol. Med. 2023;167:107630. https://doi.org/10.1016/j.compbiomed.2023.107630.
[29] Taloba AI, Elhadad A, Rayan A, Abd El-Aziz RM, Salem M, Alzahrani AA, Alharithi FS, Park C. A blockchain-based hybrid platform for multimedia data processing in IOT-Healthcare. Alexandria Engineering Journal 2023;65:263–74. https://doi.org/10.1016/j.aej.2022.09.031.
[30] Mohd Shari NF, Malip A. Enhancing privacy and security in smart healthcare: a blockchain-powered decentralized data dissemination scheme. Internet of Things 2024;27:101256. https://doi.org/10.1016/j.iot.2024.101256.
[31] Wang T, Wu Q, Chen J, Chen F, Xie D, Shen H. Health data security sharing method based on hybrid blockchain. Future Generation Computer Systems 2024;153:251–61. https://doi.org/10.1016/j.future.2023.11.032.
[32] Rizzardi A, Sicari S, Cevallos M JF, Coen-Porisini A. IOT-driven blockchain to manage the healthcare supply chain and protect medical records. Future Generation Computer Systems 2024;161:415–31. https://doi.org/10.1016/j.future.2024.07.039.
[33] Chen L, Feng T, Ma R, Shi J. BTMDS: blockchain Trusted Medical Data Sharing Scheme with privacy protection and Access Control. Comput. Commun. 2024;225:279–88. https://doi.org/10.1016/j.comcom.2024.07.007.
[34] Ali A, Pasha MF, Guerrieri A, Guzzo A, Sun X, Saeed A, Hussain A, Fortino G. A novel homomorphic encryption and consortium blockchain-based hybrid deep learning model for Industrial Internet of Medical Things. IEEe Trans. Netw. Sci. Eng. 2023;10(5):2402–18. https://doi.org/10.1109/tnse.2023.3285070.
[35] Rehman AU, Tariq N, Jan MA, Khan F, Song H, Ibrahim M. A blockchain-based hybrid model for IOMT-enabled Intelligent Healthcare System. IEEe Trans. Netw. Sci. Eng. 2024;11(4):3512–21. https://doi.org/10.1109/tnse.2024.3376069.
[36] Babu ES, BKN S, Nayak SR, Verma A, Alqahtani F, Tolba A, Mukherjee A. Blockchain-based Intrusion Detection System of IOT urban data with device authentication against ddos attacks. Computers and Electrical Engineering 2022;103:108287. https://doi.org/10.1016/j.compeleceng.2022.108287.
[37] Li W, Stidsen C, Adam T. A blockchain-assisted security management framework for collaborative intrusion detection in smart cities. Computers and Electrical Engineering 2023;111:108884. https://doi.org/10.1016/j.compeleceng.2023.108884.
[38] Sarhan M, Lo WW, Layeghy S, Portmann M. HBFL: a hierarchical blockchain-based Federated Learning Framework for collaborative IOT intrusion detection. Computers and Electrical Engineering 2022;103:108379. https://doi.org/10.1016/j.compeleceng.2022.108379.
[39] Mahalingam MS, Kumar NS, Devi RK, Logeshwaran J. A reliable inter-domain routing framework for autonomous systems using hybrid blockchain. Computers and Electrical Engineering 2025;123:110031. https://doi.org/10.1016/j.compeleceng.2024.110031.
[40] Baza M, Rasheed A, Alourani A, Srivastava G, Alshahrani H, Alshehri A. Privacy-preserving blockchain-assisted private-parking scheme with efficient matching. Computers and Electrical Engineering 2022;103:108340. https://doi.org/10.1016/j.compeleceng.2022.108340.
[41] Sai Chaitanya Kumar G, Kiran Kumar R, Parish Venkata Kumar K, Raghavendra Sai N, Brahmaiah M. Deep residual convolutional neural network: an efficient technique for intrusion detection system. Expert. Syst. Appl. 2024;238:121912. https://doi.org/10.1016/j.eswa.2023.121912.
[42] Deo TY, Sanju A. Data imputation and comparison of custom ensemble models with existing libraries like XGBoost, CATBoost, AdaBoost and Scikit learn for predictive equipment failure. Materials Today: Proceedings 2023;72:1596–604. https://doi.org/10.1016/j.matpr.2022.09.410.
[43] Ghubaish, A., Yang, Z., & Jain, R. (n.d.). HDRL-2024 dataset for cybersecurity research on medical applications in 5G networks. WUSTL. https://www.cs.wustl.edu/~jain/hdrl/index.html.
[44] Ranjan AK, Kumar P. Ensuring the privacy and security of IOT-Medical Data: a hybrid deep learning-based encryption and blockchain-enabled transmission. Multimed. Tools. Appl. 2024;83(33):79067–92. https://doi.org/10.1007/s11042-023-18043-5.
[45] Alserhani FM. Integrating deep learning and metaheuristics algorithms for blockchain-based reassurance data management in the detection of malicious IOT nodes. Peer. Peer. Netw. Appl. 2024;17(6):3856–82. https://doi.org/10.1007/s12083-024-01786-9.
[46] Vidhya S, Kalaivani V. A blockchain based secure and privacy aware medical data sharing using smart contract and encryption scheme. Peer. Peer. Netw. Appl. 2023;16(2):900–13. https://doi.org/10.1007/s12083-023-01449-1.
[47] Alsaedi A, Moustafa N, Tari Z, Mahmood A, Anwar A. TON_IoT Telemetry Dataset: a new generation dataset of IOT and IIoT for data-driven intrusion detection systems. IEEe Access. 2020;8:165130–50. https://doi.org/10.1109/access.2020.3022862.
[48] Yang L, Li J, Yin L, Sun Z, Zhao Y, Li Z. Real-time intrusion detection in wireless network: a deep learning-based intelligent mechanism. IEEe Access. 2020;8:170128–39. https://doi.org/10.1109/access.2020.3019973.
[49] Manimurugan S, Al-Mutairi S, Aborokbah MM, Chilamkurti N, Ganesan S, Patan R. Effective attack detection in internet of medical things smart environment using a deep belief neural network. IEEe Access. 2020;8:77396–404. https://doi.org/10.1109/access.2020.2986013.
[50] Liu J, Yang D, Lian M, Li M. Research on intrusion detection based on particle swarm optimization in IOT. IEEe Access. 2021;9:38254–68. https://doi.org/10.1109/access.2021.3063671.
[51] Seo W, Pak W. Real-time network intrusion prevention system based on Hybrid Machine Learning. IEEe Access. 2021;9:46386–97. https://doi.org/10.1109/access.2021.3066620.
[52] Wu Z, Zhang H, Wang P, Sun Z. RTIDS: a robust transformer-based approach for Intrusion Detection System. IEEe Access. 2022;10:64375–87. https://doi.org/10.1109/access.2022.3182333.
[53] Kye H, Kim M, Kwon M. Hierarchical detection of network anomalies : a self-supervised learning approach. IEEe Signal. Process. Lett. 2022;29:1908–12. https://doi.org/10.1109/lsp.2022.3203296.

[54] Kim T, Pak W. Early detection of network intrusions using a gan-based one-class classifier. IEEe Access. 2022;10:119357–67. https://doi.org/10.1109/access.2022.3221400.
[55] Wang W, Du X, Shan D, Qin R, Wang N. Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine. IEEE Transactions on Cloud Computing 2022;10(3):1634–46. https://doi.org/10.1109/tcc.2020.3001017.
[56] Zhang C, Costa-Perez X, Patras P. Adversarial attacks against Deep Learning-based network intrusion detection systems and Defense Mechanisms. IEEE/ACM Transactions on Networking 2022;30(3):1294–311. https://doi.org/10.1109/tnet.2021.3137084.
[57] Wu Y, Nie L, Wang S, Ning Z, Li S. Intelligent intrusion detection for internet of things security: a deep convolutional generative adversarial network-enabled approach. IEEe Internet. Things. J. 2023;10(4):3094–106. https://doi.org/10.1109/jiot.2021.3112159.
[58] Ben Said R, Sabir Z, Askerzade I. CNN-BiLSTM: a hybrid deep learning approach for network intrusion detection system in software-defined networking with hybrid feature selection. IEEe Access. 2023;11:138732–47. https://doi.org/10.1109/access.2023.3340142.
[59] Das S, Saha S, Priyoti AT, Roy EK, Sheldon FT, Haque A, Shiva S. Network intrusion detection and Comparative Analysis Using Ensemble Machine Learning and feature selection. IEEE Transactions on Network and Service Management 2022;19(4):4821–33. https://doi.org/10.1109/tnsm.2021.3138457.
[60] Zhao R, Mu Y, Zou L, Wen X. A hybrid intrusion detection system based on feature selection and weighted stacking classifier. IEEe Access. 2022;10:71414–26. https://doi.org/10.1109/access.2022.3186975.
[61] Park C, Lee J, Kim Y, Park J-G, Kim H, Hong D. An enhanced AI-based network intrusion detection system using generative adversarial networks. IEEe Internet. Things. J. 2023;10(3):2330–45. https://doi.org/10.1109/jiot.2022.3211346.
[62] Xu H, Sun L, Fan G, Li W, Kuang G. A hierarchical intrusion detection model combining multiple deep learning models with attention mechanism. IEEe Access. 2023;11:66212–26. https://doi.org/10.1109/access.2023.3290613.
[63] Han W, Peng J, Yu J, Kang J, Lu J, Niyato D. Heterogeneous data-aware federated learning for intrusion detection systems via meta-sampling in artificial intelligence of things. IEEe Internet. Things. J. 2024;11(8):13340–54. https://doi.org/10.1109/jiot.2023.3337755.
[64] Ghubaish A, Yang Z, Jain R. HDRL-ids: a hybrid deep reinforcement learning intrusion detection system for enhancing the security of medical applications in 5G networks. In: 2024 International Conference on Smart Applications, Communications and Networking (SmartNets); 2024. https://doi.org/10.1109/smartnets61466.2024.10577692.
[65] Jim Solomon Raja D, Sriranjani R, Arulmozhi P, Hemavathi N. Unified Random Forest and hybrid bat optimization based man-in-the-middle attack detection in advanced metering infrastructure. IEEe Trans. Instrum. Meas. 2024;73:1–12. https://doi.org/10.1109/tim.2024.3420375.
[66] Zhong Y, Wang Z, Shi X, Yang J, Li K. RFG-HELAD: a robust fine-grained network traffic anomaly detection model based on heterogeneous ensemble learning. IEEE Transactions on Information Forensics and Security 2024;19:5895–910. https://doi.org/10.1109/tifs.2024.3402439.
[67] Gupta K, Sharma DK, Datta Gupta K, Kumar A. A tree classifier based network intrusion detection model for internet of medical things. Computers and Electrical Engineering 2022;102:108158. https://doi.org/10.1016/j.compeleceng.2022.108158.
[68] Najar AA, S MN. A robust ddos intrusion detection system using Convolutional Neural Network. Computers and Electrical Engineering 2024;117:109277. https://doi.org/10.1016/j.compeleceng.2024.109277.
[69] Cao Y, Wang Z, Ding H, Zhang J, Li B. An intrusion detection system based on Stacked Ensemble Learning for IOT Network. Computers and Electrical Engineering 2023;110:108836. https://doi.org/10.1016/j.compeleceng.2023.108836.