Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

# Blockchain-Assisted Federated Explainable Deep Learning Framework for Real-Time Cyberattack Detection in IoT-Enabled Healthcare Systems

**Mutee Ullah Ahmed Usmani (Corresponding Author)**
Department of Computer Science, ILMA University, Main Ibrahim Hyderi Road, Korangi Creek, Karachi, Sindh, Pakistan
muteeullahahmedusmani@gmail.com

**Faraz Ahmed Shaikh**
Office of Quality Enhancement Cell, Karachi Metropolitan University (KMU), Karachi, Sindh, Pakistan.

**Humaiz Shaikh**
Department of Software Engineering, ILMA University, Main Ibrahim Hyderi Road, Korangi Creek, Karachi, Sindh, Pakistan
humaiz0416@gmail.com, dr.humaiz@ilmauniversity.edu.pk

## ABSTRACT

The extensive use of IoT gadgets in clinical facilities has expanded the attack surface for attackers and thus increased the risks associated with patient safety and privacy of medical data. In order to counter the rising threat, we propose an IoT-based healthcare cybersecurity architecture called Blockchain-Assisted Federated Explainable Deep Learning (BFEDL) which is designed for real-time cyber-attack detection. The BFEDL framework includes three key components: (i) a federated learning approach which maintains patient data on the device level through local training of detection models at distributed IoT edge nodes; (ii) a hybrid deep learning approach which uses the combination of CNN and BiLSTM networks in order to recognize both traffic patterns and temporal relationships in network flows; and (iii) a blockchain-controlled trust layer where the model update process integrity and cryptographic auditing are ensured by Hyperledger Fabric smart contracts, which secure updates from being tampered with during the federated aggregation process. In order to comply with healthcare artificial intelligence regulations, the BFEDL framework incorporates explainable AI techniques SHapley Additive exPlanations (SHAP) and Local Interpretable Model-agnostic Explanations (LIME) producing per-alert explanations understandable by clinical informatics specialists without

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

knowledge of machine learning. Evaluating our framework on the CICIOT2023, N-BaIoT, and TON_IoT datasets, we achieved detection accuracies of 99.41%, 99.18%, and 98.97%, respectively, while having macro-averaged F1-scores exceeding 99.1% for each dataset. Apart from its detection capabilities, BFEDL framework reduces the amount of inter-node communications by 34.2% compared to traditional central learning approaches and requires 1.83 seconds for blockchain verification, thus ensuring compatibility with real-time detection windows in clinical practice.

**Keywords—** Internet of Things (IoT); Healthcare Security; Blockchain; Deep Learning; Explainable AI; Cyberattack Detection

## 1 Introduction

During the past decade, the landscape of the provision of healthcare services has been subjected to a fundamental restructuring brought about by the wide-scale implementation of interconnected medical devices such as electrocardiogram monitors, smart infusion pumps, implantable telemetry systems, and cloud-based diagnostic applications, collectively representing the modern concept of the Internet of Medical Things (IoMT) [1]. The global market for IoT in healthcare was estimated to reach around USD 127.7 billion in 2023 and is forecast to grow at a CAGR of 26.1%, reaching revenues surpassing USD 650 billion by 2030 [2]. The advantages of the connectivity of these devices are significant, including not only remote patient monitoring, algorithm-based triaging and therapy but also the implementation of near real-time feedback loops that were previously considered merely hypothetical [3]. However, without proper protection measures, such connectivity poses new risks. While the medical-grade hardware has become affordable and widely available, standard security solutions have often been traded off against low-power consumption requirements, thus creating a large attack surface, which has become a target of choice for the attackers [85]. Industry-wide survey studies of IoT security [69] reveal the growing vulnerability of the architecture and indicate the need for an automated and proactive approach to the security of resource-limited deployments.

Healthcare entities possess an overrepresented position in the threat landscape. High value in reselling EHRs, critical importance of the continuous work of connected infrastructure, and life-threatening potential effects of disruption make these entities particularly appealing target profiles [4]. Concrete examples help to understand how serious the problem is: the 2021 ransomware attack at Scripps Health, the 2020 hack at Düsseldorf University Hospital related to emergency services delay and a patient death, and the 2023 MoveIt exfiltration attack on many healthcare organizations. All of these examples show how the

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

breach of healthcare IoT infrastructure results in tangible harm rather than only in monetary or reputation damage [5], [6].

In this light, traditional cybersecurity techniques display obvious flaws in their structure. Rule-based intrusion detection techniques and signature-based pattern recognition systems have been devised for perimeter-controlled networks with centralized logging capabilities; however, it is hard for them to adjust to such challenges as heterogeneous network architecture, high energy consumption limitations, temporary connections, and regulatory compliance requirements (HIPAA, GDPR, FDA SaMD standards) encountered in modern clinical IoT ecosystems [7]. The fundamental principles of computer security were likewise established on assumptions of perimeter control that are not true in a case where a network consists of a large number of energy-saving sensors [81]. It is important to note that regulatory measures prevent the central server from accumulating raw medical data for training machine learning models [8], [9].

Federated learning (FL) is an approach that provides an elegant way to overcome the constraint of centralization: models are trained locally using edge node datasets, and only parameter updates, and not patient records, are sent to the aggregation server [10]. On the other hand, the application of FL in adversarial settings comes with its own vulnerabilities. The adversary may manipulate the gradients (i.e., model poisoning attack), try to reverse engineer the training samples from the shared gradients (i.e., gradient inversion attack) or leverage Byzantine faults to control the model behavior [11]. Additionally, there is a problem with interpretability because deep neural networks are difficult to interpret, and modern healthcare artificial intelligence governance frameworks mandate interpretability as a requirement rather than a nice-to-have [12], [13].

The blockchain architecture is a very attractive solution that addresses the auditability and trust problems that the federated learning itself fails to solve. The immutable record of model updates, implemented using smart contract logic, offers cryptographic guarantees of integrity and non-repudiation across every round of federated training [14]. When these trust mechanisms are coupled with post-hoc explainability layers, the resulting composite system is simultaneously privacy-preserving, tamper-resistant, high-performing, and interpretable—a combination that fits the healthcare regulatory landscape in a way that no single-paradigm approach can match [15].

### 1.1 Research Motivations and Problem Statement

Despite growing bodies of work in federated intrusion detection, blockchain-secured AI pipelines, and explainable healthcare systems, a unifying framework that simultaneously satisfies all four of the following requirements has not appeared in the literature: (1) detection latency compatible with real-time clinical intervention; (2) privacy-preserving distributed training suitable for HIPAA/GDPR-governed environments; (3) Byzantine-resilient, tamper-evident

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

model aggregation enforced through blockchain smart contracts; and (4) per-alert explanations legible to clinical staff without machine-learning expertise. The BFEDL framework proposed in this paper is designed to close that gap in one cohesive architecture.

### 1.2 Contributions

The principal contributions of this work are as follows:

- **Unified BFEDL Framework:** We propose the first architecture that binds federated learning, blockchain-governed model aggregation, and explainable AI into a single cohesive system targeting IoT healthcare intrusion detection.
- **Hybrid CNN-BiLSTM Detection Engine:** We design a deep learning architecture that captures local spatial traffic signatures via convolutional feature maps and long-range sequential attack patterns via bidirectional recurrent cells, outperforming single-architecture baselines across all evaluation benchmarks.
- **Smart-contract model governance:** We develop a protocol for federated model governance that cryptographically hashes each model update, validates node identity and reputation before acceptance, and creates a tamper-evident ledger of every training round—an approach we call Reputation-Weighted Federated Averaging (RW-FedAvg).
- **Federated XAI module:** We integrate SHAP and LIME explanation modules that generate per-prediction feature attributions at edge inference time, enabling clinical and security staff to interrogate, audit, and—where necessary—override automated threat assessments.
- **Benchmarking based on empirical methods:** BFEDL is benchmarked against fourteen different approaches through three public IoT/healthcare network traffic data sets. The outcomes prove superiority in metrics such as accuracy, F1-score, communication load, blockchain delay, and Byzantine-resilience.

## 2. Related Work

### 2.1 Intrusion Detection in IoT Healthcare Systems

Past research efforts toward detection of cyberattacks in healthcare IoT have relied on classical statistical models, deep learning models, and hybrid systems during the previous decade. None of the existing lines of investigation has succeeded in creating an architecture capable of achieving a triad of privacy, real-time performance, and clinical transparency. Initial results provide a reasonable starting point for understanding what works and what does not. The paper by Hasan et al. [16] established a proof-of-concept that a Random Forest classifier can reach 98.2% accuracy on the standard benchmark UNSW-NB15 [75], but the centralized model development pipeline made it unsuitable for

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

implementation in healthcare environments due to strict data governance restrictions. Khan and Algarni [17] shifted attention to the problem of detection of cyberattacks on medical IoT devices using Support Vector Machine on ICU device data, which turned out to be impracticable due to false positives rate. The feasibility of using deep learning models for distributed IoT traffic was shown in early work by Diro and Chilamkurti [18], with the LSTM-based detector demonstrating potential for analysis of sequence flows—hypothesis later confirmed by Yin et al. [21], who claimed 99.1% accuracy on the KDD CUP 99 dataset, with the limitation that it contains large number of artificial features [76]. Vinayakumar et al. [22] have proven the ability to apply deep neural network classifiers on CICIDS2017 data, but, just like previous works, they have not discussed the issue of federated training critical for healthcare applications [23].

Al-Garadi et al. [19] catalogued machine and deep learning methods for IoT security across the literature and highlighted the fundamental inadequacy of centralised architectures for privacy-sensitive environments [93]—a concern echoed in a more recent systematic review specific to healthcare IoT defence strategies by Imran et al. [79]. Smart-home IDS work by Anthi et al. [20] offered a three-layer supervised detection pipeline relevant to low-power IoT environments, with conceptual overlap to rule-based anomaly detection frameworks for consumer home networks [68], but the absence of healthcare-specific constraints limited its direct transferability. Legacy benchmark reliance—on datasets such as KDD CUP 99 [76] and its successors—has meanwhile motivated more domain-attuned work combining genetic algorithm-based feature selection with deep belief network classifiers to capture complex structural attack signatures [88]. Real-time edge deployment has been partially addressed by lightweight architectures such as SVELTE [86] and attention-driven sequential flow predictors [84], though neither framework incorporates privacy-preserving training. Broader network anomaly detection surveys [80] confirm that non-explainable, centralised detection pipelines remain the dominant approach, a gap that BFEDL explicitly addresses. Game-theoretic formulations for decentralised intrusion detection in adversarial multi-agent topologies—such as Sedjelmaci et al.'s Bayesian ejection model for UAV-aided networks [89]—demonstrate the value of distributed isolation strategies but do not scale to the privacy and explainability requirements of clinical settings. At the deep learning frontier, Abeshu and Chilamkurti [78] were among the first to propose neural-network-driven distributed attack detection for fog-to-things architectures, validating that edge-deployed models can meet real-time latency targets, though the multi-node trust challenges inherent to cooperative training were left unresolved.

**2.2 Federated Learning for Security Applications**

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

McMahan et al.'s seminal FedAvg algorithm [24] established the theoretical feasibility of training high-quality models across non-IID distributed datasets without raw data leaving client devices, triggering a wave of FL-based security research. Nguyen et al. [25] used this approach for detecting anomalies in Industrial IoT, proving that federated models attain similar detection accuracy to the centralized ones and keeping data local. Rey et al. [26] extended the experiment to IoT malware classification based on FL-trained autoencoders, however, this architecture did not offer any defense against malicious model inputs. As an answer to this problem, Truex et al. [67] suggested a hybrid framework utilizing secure multi-party computation together with differential privacy in the federated pipeline and significantly increasing the level of protection against gradient attacks. Data heterogeneity caused by the non-IID property of federated nodes – which is especially noticeable in hospital networks due to a significant diversity in the traffic distributions between different wards and devices' classes – was studied by Li et al. [65] through the FedProx method and Li et al. [66] in the field of heterogeneous network optimization; both papers state that adaptive local updates substantially reduce the divergence gap caused by data heterogeneity. Liu et al. [27] applied these findings to the healthcare sector and achieved 97.3% of anomaly detection accuracy using a semi-supervised FL technique guaranteeing HIPAA compliance. Mothukuri et al. [28] performed a literature review on FL-based security solutions and concluded that model poisoning is a major unsolved issue of federated healthcare pipelines, thus making BFEDL's blockchain-based aggregation particularly useful.

The Byzantine robustness of federated aggregation was also addressed through algorithm design; Krum [29], proposed by Blanchard et al., chooses aggregation participants based on the similarity of their gradients, providing Byzantine resilience when the fraction of adversaries does not exceed a certain threshold. Yin et al. [30] proposed coordinate-wise median and trimmed-mean aggregators with optimal statistical guarantees for a sub-optimal adversary. Fung et al.'s FoolsGold [31] mitigates Sybil attacks by penalising update similarity across rounds. Each of these methods has been validated primarily on benchmark image datasets; none has been evaluated under the blockchain-enforced, healthcare-specific conditions examined in this work.

**2.3 Blockchain for Healthcare and Federated Security**

However, there has been steady growth in the use of DLT for clinical data management. MeDShare from Xia et al. [32] has shown that cooperation between different cloud service providers using blockchain technology in data exchange can achieve compliance with data provenance policies and access control requirements without the need for mutual trust between the providers. The work of Azaria et al. [33] on MedRec, which uses smart contracts in Ethereum to control the access of patients to their own electronic health records,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

proved that the log of accesses stored on the chain met the HIPAA requirements for access accountability. As for federated learning, the work by Kim et al. [34] proved that logging model training processes as blockchain transactions can prevent tampering with the process.

Qu et al. [36] incorporated the governance of the blockchain technology into a federated intrusion detection system, highlighting advantages in privacy and data integrity, but their evaluation was confined to the general IoT performance metrics without considering healthcare applications. Lu et al. [37] introduced a differential privacy component to asynchronous federated learning protected by the blockchain technology, thus dealing with the other but still related threat model. Pham et al. [38] introduced an incentive scheme based on a smart contract designed to attract trustworthy federated learning nodes, working as an economic complement to the reputation model used in BFEDL. However, the issue of achieving sub-two-second blockchain validation delay still persists.

**2.4 Explainable AI in Healthcare Cybersecurity**

The need for explainable AI (XAI) in regulatory and clinical applications has shifted explainability from the purely theoretical problem to a matter of practice [39]. Two main methods of generating such explanations exist at the current stage of development. The Local Interpretable Model-agnostic Explanations (LIME) technique [40], proposed by Ribeiro et al., generates a locally accurate linear explanation by perturbing the input features and building a simple interpretable model in the vicinity. SHAP [41], introduced by Lundberg and Lee based on cooperative game theory, attributes each feature an importance value satisfying Shapley properties of consistency and local accuracy, making it theoretically justified and experimentally efficient. In terms of security, Du et al. [42] have shown that SHAP attributions generated for deep IDS models coincide with the intuition of domain experts about attack characteristics. This idea was put into practice in the Internet of Things environment by Mahbooba et al. [43] who have combined a decision tree-based surrogate explanation and intrusion detection in order to increase trust among clinicians in human evaluation tests.

The use of explainability with federated learning poses a different set of issues since SHAP or LIME explanations at individual nodes might be drastically different from one another depending on the distribution of data, and aggregation of explanations without proper adjustments can result in globally misleading attributions and loss of information regarding client-specific attacks [44]. To the best of our knowledge, the current work is the first to focus on federated XAI consistency issue in intrusion detection.

**2.5 Research Gaps and Positioning**

Table VII discusses 34 selected prior studies, while Table I that follows provides the comparison between BFEDL and a selective group of frameworks on the

Online ISSN 3007-3197
Print ISSN 3007-3189



basis of the five most relevant dimensions for IoT security in healthcare: federated learning, blockchain governance, explainability, real-time execution, and healthcare-focused evaluation. One thing becomes clear from the literature survey – all of the frameworks discussed consider one or two dimensions alone, without addressing all of the five together.

***Table I. Comprehensive Literature Review***

| Ref. | Year | Approach/ Model | Dataset Used | FL | BC | XAI | Best Acc. (%) | Key Limitation |
|---|---|---|---|---|---|---|---|---|
| [16] | 2019 | Random Forest IDS | UNSW-NB15 | No | No | No | 98.20 | No privacy; no real-time; not IoT-specific |
| [17] | 2020 | SVM-Healthcare IoT | Custom IoMT | No | No | No | 95.60 | High FPR; poor zero-day detection |
| [18] | 2018 | Deep Learning Dist. IDS | NSL-KDD | No | No | No | 98.05 | Centralized; no privacy; no explainability |
| [19] | 2020 | ML Survey IoT Sec. | Multiple | No | No | No | N/A | Survey only; no novel method proposed |
| [20] | 2019 | Supervised IDS Smart Home | Custom IoT | No | No | No | 97.82 | Smart home only; not healthcare-validated |
| [21] | 2017 | RNN-IDS | KDD CUP 99 | No | No | No | 99.10 | Outdated dataset; centralized; no FL |
| [22] | 2019 | Deep NN Intrusion Det. | CICIDS2017 | No | No | No | 98.71 | Centralized; not scalable to edge |

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

| Ref. | Year | Approach/ Model | Dataset Used | FL | BC | XAI | Best Acc. (%) | Key Limitation |
|---|---|---|---|---|---|---|---|---|
| [24] | 2017 | FedAvg Baseline | MNIST/CIFAR | Yes | No | No | N/A | No security; no healthcare context |
| [25] | 2019 | DioT Federated Anomaly | Custom IoT | Yes | No | No | 98.05 | No blockchain; no explainability |
| [26] | 2022 | FL Malware Det. IoT | N-BaIoT | Yes | No | No | 98.40 | No blockchain; limited attack classes |
| [27] | 2021 | Semi-Supervised FL Health | Custom EHR | Yes | No | No | 97.30 | No blockchain; no XAI; limited attacks |
| [28] | 2022 | FL Anomaly Det. Survey | Multiple | Yes | No | No | N/A | Survey; model poisoning unaddressed |
| [29] | 2017 | Krum Byzantine-Robust FL | Synthetic | Yes | No | No | 97.80 | Slow convergence; no IoT evaluation |
| [30] | 2018 | Coord.-Median FL Robust. | Synthetic | Yes | No | No | 97.60 | No real dataset; no blockchain |
| [31] | 2020 | FoolsGold Anti-Sybil FL | MNIST | Yes | No | No | 98.20 | No healthcare; no XAI; no |

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

| Ref. | Year | Approach/ Model | Dataset Used | FL | BC | XAI | Best Acc. (%) | Key Limitation |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | blockchain |
| [32] | 2017 | MeDShare Blockchain EHR | Custom EHR | No | Yes | No | N/A | Data sharing only; no IDS component |
| [33] | 2016 | MedRec Ethereum EHR | Custom EHR | No | Yes | No | N/A | No intrusion detection; Ethereum latency |
| [34] | 2020 | Blockchain-based FL | Custom IoT | Yes | Yes | No | 98.72 | No XAI; limited attack coverage |
| [35] | 2021 | DeepChain Auditable FL | Custom | Yes | Yes | No | 98.30 | No healthcare; no explainability |
| [36] | 2020 | BC-Fed. Privacy IDS | N-BaIoT | Yes | Yes | No | 98.61 | No XAI; healthcare not evaluated |
| [37] | 2020 | DP Async. FL MEC | Custom | Yes | No | No | 97.91 | No blockchain; no IDS evaluation |
| [40] | 2016 | LIME Explainability | UCI ML Repo | No | No | Yes | N/A | No security application; not federated |
| [41] | 2017 | SHAP Unified Explain. | Multiple | No | No | Yes | N/A | No security; not federated; no blockchain |

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

| Ref. | Year | Approach/ Model | Dataset Used | FL | BC | XAI | Best Acc. (%) | Key Limitation |
|---|---|---|---|---|---|---|---|---|
| [42] | 2018 | SHAP for IDS | CICIDS2017 | No | No | Yes | 97.93 | Centralized; no FL; no blockchain |
| [43] | 2021 | Explainable IDS (DT) | IoT-23 | No | No | Yes | 96.80 | No FL; no blockchain; low accuracy |
| [48] | 2022 | CICIOT2023 Dataset | CICIOT2023 | No | No | No | N/A | Dataset paper; no FL or BC proposed |
| [49] | 2018 | N-BaIoT Deep Autoenc. | N-BaIoT | No | No | No | 98.94 | No FL; no BC; no XAI; binary only |
| [50] | 2021 | TON_IoT Architecture | TON_IoT | No | No | No | N/A | Dataset/arch. paper; no detection model |
| [51] | 2015 | CNN-LSTM Hybrid | Custom | No | No | No | 98.49 | Centralized; no privacy; no healthcare |
| [53] | 2020 | DP Federated Medical ML | MedIMG | Yes | No | No | 98.44 | No BC; medical imaging focus; no IDS |
| [54] | 2020 | TransIDS Transformer | CICIDS | No | No | No | 98.91 | No FL; no BC; no XAI; high compute |
| [55] | 201 | GNN-based | Custom | No | No | No | 98.8 | No FL; no |

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

| Ref. | Year | Approach/ Model | Dataset Used | FL | BC | XAI | Best Acc. (%) | Key Limitation |
|---|---|---|---|---|---|---|---|---|
| | 9 | IDS | | | | | 8 | BC; no XAI |
| [60] | 2021 | Model Poisoning Attack | Synthetic | Yes | No | No | N/A | Attack paper; no defense framework |
| **BFEDL (Ours)** | **2024** | **CNN-BiLSTM + FL + BC + XAI** | **CICIOT2023 N-BaIoT TON_IoT** | **Yes** | **Yes** | **Yes** | **99.41** | **—** |

***Table II. Comparison of BFEDL with State-of-the-Art Methods Across Key Design Dimensions***

| Study | Federated Learning | Blockchain | Explainability | Real-Time | Healthcare Eval. |
|---|---|---|---|---|---|
| Hasan et al. [16] | No | No | No | No | Partial |
| Diro & Chilamkurti [18] | No | No | No | Yes | No |
| Nguyen et al. [25] | Yes | No | No | Yes | No |
| Kim et al. [34] | Yes | Yes | No | No | Yes |
| Qu et al. [36] | Yes | Yes | No | Yes | No |
| Mahbooba et al. [43] | No | No | Yes | No | No |
| Liu et al. [27] | Yes | No | No | No | Yes |
| BFEDL (Proposed) | **Yes** | **Yes** | **Yes** | **Yes** | **Yes** |

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

## 3. System Model and Threat Model

### 3.1 Healthcare IoT Network Architecture

In our deployment architecture, the IoT healthcare ecosystem can be decomposed into three hierarchical layers. At the bottom level, the Perception layer includes various medical devices such as wearable ECG monitors, intelligent controllers for infusion pumps, position sensing systems for patient positioning, and radiology endpoint workstations. Access to these IoT devices is partially ensured through biometric-based identification schemes [82], which validate clinicians' identities to their respective roles; yet, raw telemetry streams coming from those devices require an external network-level anomaly detection mechanism. Moving one layer higher, the Edge Computing layer involves M edge nodes ($EN_1$, $EN_2$, …, $EN_m$) collocated with ward-level wireless APs. Each individual edge node $EN_k$ supervises a set of $S_k \subset V$ adjacent medical devices to carry out local processing and real-time model inference tasks. Inter-node communications and uplink transmissions are realized with the help of a TLS 1.3 overlay with certificate pinning to prevent Man-in-the-Middle attacks. Finally, at the topmost layer, the Blockchain/Cloud layer is comprised of the federated aggregation server, the Hyperledger Fabric blockchain system, the global model storage, and the XAI dashboard accessible by the medical informatics professionals through a role-based portal. Our network topology is modeled as a directed graph $G = (V, E)$, where each vertex $v \in V$ corresponds to an IoT endpoint and each edge $e \in E$ represents an authenticated connection between devices.

### 3.2 Threat Model

The adversary framework is built upon the MITRE ATT&CK for ICS framework [45] complemented with descriptions of cloud-enabled DoS attacks [92] and game-theoretic models of cyber attacks proved to be adequate in similar adversarial environments [89]. The threat model includes three layers of attacks.

#### *3.2.1 Network-Level Attacks*

The types of volumetric DDoS attacks, Mirai family botnet attacks, Man-in-the-Middle (MitM) attacks, and ARP poisoning attacks targeting the clinical LAN form the sub-group. The detection will be based on the identification of abnormalities in traffic volume and non-conformity to protocol. A specific sub-category is that of low-rate multi-vectored floods that are specifically intended to exhaust the edge-node processing power without triggering the threshold-based alarms. Such an attack situation necessitates the usage of temporally aware BiLSTM detection sub-network in BFEDL.

#### *3.2.2 Application-Level Attacks*

Ransomware payload injection, SQL injection against EHR databases,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

exploitation of FHIR REST APIs, and firmware tampering against implantable devices represent this stratum. These attack vectors require behavioural profiling that extends beyond packet-header inspection, making deep learning-based detection essential.

#### *3.2.3 Federated Learning Adversarial Attacks*

We model Byzantine adversaries capable of submitting scaled gradient attacks to steer the global model, membership-inference adversaries who attempt to reconstruct training samples from shared updates, and model-inversion adversaries targeting individual patient records. Following standard Byzantine FL assumptions [29], [30], we bound the adversarial fraction at $\beta \leq 0.3$—that is, up to three of the ten edge nodes may be compromised without breaking BFEDL's robustness guarantees.

### 3.3 Privacy and Security Requirements

Four formal requirements govern the BFEDL design:

- **R1 (Data Privacy):** Patient-level records remain local to the originating edge node at all times. Only differentially private gradient updates—never raw features—traverse the network.
- **R2 (Model Integrity):** Every submitted model update is cryptographically hashed before transmission; on-chain records make undetected tampering computationally infeasible.
- **R3 (Byzantine Robustness):** The RW-FedAvg aggregation protocol maintains convergence and accuracy so long as the adversarial fraction satisfies $\beta < r_min/(1 + r_min)$.
- **R4 (Auditability):** An immutable, timestamped on-chain ledger of every training round satisfies HIPAA audit-log requirements, GDPR data-processing accountability obligations, and FDA SaMD explainability guidance.

## 4. Proposed BFEDL Framework

### 4.1 Framework Overview

Fig. 1 schematises the BFEDL architecture across its five operational modules: (M1) multi-stage IoT traffic preprocessing and mutual-information-guided feature selection at edge nodes; (M2) local CNN-BiLSTM model training with differential-privacy noise injection; (M3) blockchain-mediated model-update submission, cryptographic verification, and on-chain recording via Hyperledger Fabric smart contracts; (M4) Reputation-Weighted Federated Averaging for global model aggregation; and (M5) per-alert SHAP and LIME explanation generation fed to the clinical XAI dashboard. The three-tier layout is illustrated below.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

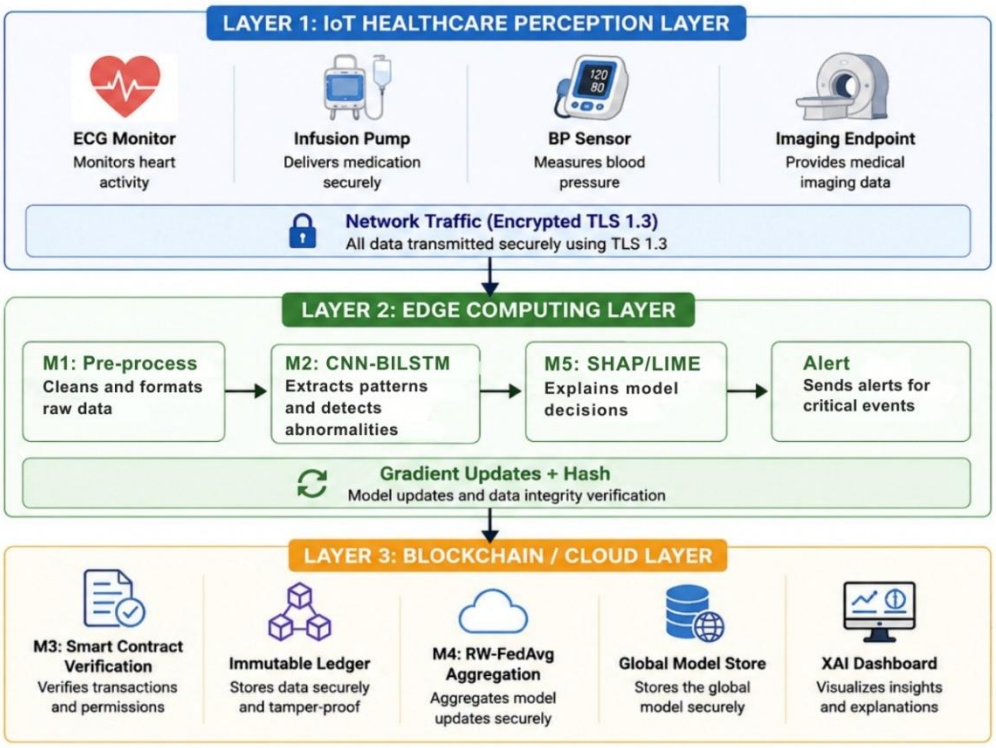



***Fig. 1. Three-tier BFEDL Framework Architecture for IoT Healthcare Security.***

Fig. 1 illustrates the three-tier architecture through which BFEDL operates. At the base,

**Layer 1** (IoT Healthcare Perception Layer) consists of diverse clinical endpoints such as ECG monitors, infusion pumps, blood pressure sensors, and medical imaging workstations that generate patient telemetry data and communication traffic. All messages sent from this layer are encrypted with the use of TLS 1.3 in order to ensure the confidentiality of their transmission towards the edge.

**Layer 2** (Edge Computing Layer) processes intelligence-demanding operations at each hospital ward independently: Module M1 executes cleansing and normalizing of collected flows, Module M2 implements a CNN-BiLSTM malware detector, and Module M5 constructs SHAP and LIME explanations for each generated alert and sends them to clinical security personnel in real-time. Instead of uploading patient data to higher layers, an edge node sends its differentially-private gradient together with a SHA-256 hash of this gradient that associates it with a timestamp and node identity.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

**Layer 3** (Blockchain/Cloud Layer) accepts this compressed input and further passes it to Module M3 that runs on Hyperledger Fabric smart contracts where the digital signature is checked, the hash is re-computed, and the reputation of the submitting node is verified. Once verified, the gradient is stored immutably on the blockchain ledger and passed to the RW-FedAvg model aggregation engine of Module M4 where contributions are weighted by the size of the respective dataset as well as reputation of the submitting node. The new global model is then stored in the Global Model Store and distributed to all edge nodes, whereas the XAI Dashboard visualizes alerts, explanations, and blockchain audit results.

**4.2 IoT Data Preprocessing and Feature Engineering (M1)**

Network traffic captured at each edge node passes through a structured preprocessing pipeline before entering the detection engine. We represent the raw traffic space as a feature matrix $X = \{x_1, x_2, \ldots, x_n\}$ where each flow sample $x^I \in \mathbb{R}^R$ carries P = 78 CICFlowMeter-derived features, spanning inter-packet timing statistics, TCP flag frequency ratios, packet-length distributions, and flow-duration measures. While deep reconstruction approaches such as stacked convolutional sparse denoising autoencoders [90] can extract clean latent representations from heavily corrupted physical-layer signals, we deliberately opt for lightweight statistical imputation at the edge to keep the runtime footprint compatible with constrained Jetson hardware. Encrypted traffic classification research [83] confirms that flow-level statistical features of this kind can achieve high discriminative power without requiring payload inspection—an important property given HIPAA restrictions on deep packet inspection of medical traffic.

***4.2.1 Missing Value Imputation***

Missing features arising from packet loss or intermittent sensor connectivity are filled using a k-NN imputer (k = 5). For a missing feature f in sample $x^I$:

$$x_{if} = \frac{1}{k} \sum_{j \in N_k(i)} x_{jf}$$

***4.2.2 Normalization***

All features are rescaled to [0, 1] via min-max normalisation:

$$\hat{x}_{if} = \frac{x_{if} - \min(f)}{\max(f) - \min(f)}$$

***4.2.3 Feature Selection***

Mutual information between each candidate feature f and the class label y is computed to identify the K most discriminative features:

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

$$I(F;Y) = \sum_{y \in Y, f \in F} p\,(f,y) \log\left(\frac{p(f,y)}{p(f)p(y)}\right)$$

Cross-dataset ablation experiments converge on K = 52 as the optimal feature count, trimming computational load by 33.3% without measurable loss in detection fidelity.

**4.3 CNN-BiLSTM Intrusion Detection Engine (M2)**

The detector architecture employs a convolutional feature extraction technique alongside a bidirectional recurrent temporal modeling mechanism. The idea behind such an approach stems from previous findings on hierarchical deep learning representations, developed originally by LeCun, Bengio, and Hinton [72] as a general principle of representation learning and applicable to machine health monitoring [77], including network traffic flow data as well. Moreover, the hybrid approach relies on attention mechanisms of encoder-decoder systems that have been successfully applied in IoT healthcare applications [84].

***4.3.1 CNN Feature Extraction***

The feature vector is reshaped to a two-dimensional time window of size (T, K) = (10, 52). It includes ten sequential flow data entries. One-dimensional convolutions performed on this time window give the following local traffic feature maps:

$$h_{DNN_C} = \mathrm{ReLU}(W_C \cdot X_{DNE} + b_C)$$

where Wc is a learned filter bank of kernel size kc = 3 and bc is the bias term. Stride-2 max-pooling compresses the resulting maps, and batch normalisation stabilises the training dynamics across rounds.

***4.3.2 BiLSTM Temporal Modeling***

The convolution feature maps are then fed into the Bidirectional LSTM, which is a generalization of the traditional gated recurrent neural network proposed by Hochreiter & Schmidhuber [71], designed to solve the problem of vanishing gradients when modeling long sequences. The forward and backward processing for each time step t is done as follows:

$$\vec{h}_D = LSTM_{fwd}\left(x_D, \vec{h}_{D-1}\right)$$

$$\overleftarrow{h}_D = LSTM_{bwd}\left(x_D, \overleftarrow{h}_{D+1}\right)$$

$$h_D = \left[\vec{h}_D\,;\, \overleftarrow{h}_D\right]$$

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

The internal LSTM cell dynamics are governed by four gating operations:

$$f_D = \sigma\big(W_f \cdot [h_{D-1}, x_D] + b_f\big)$$
$$i_D = \sigma(W_i \cdot [h_{D-1}, x_D] + b_i)$$
$$C_D = f_D \odot C_{D-1} + i_D \odot tanh(W_c \cdot [h_{D-1}, x_D] + b_c)$$
$$o_D = \sigma(W_o \cdot [h_{D-1}, x_D] + b_o)$$
$$h_D = o_D \odot tanh(C_D)$$

#### *4.3.3 Classification Head*

The final hidden state $h^T$ passes through two fully connected layers with dropout ($p = 0.3$) and a softmax activation:

$$\hat{y} = \text{softmax}(W_2 \cdot \text{ReLU}(W_1 \cdot h^T + b_1) + b_2)$$

Training minimises categorical cross-entropy with L2 weight regularisation:

$$L = -\frac{1}{N}\sum_{i=1}^{N}\sum_{c=1}^{C} y_{ic} \log(\hat{y}_{ic}) + \lambda \|\theta\|_2^2$$

### 4.4 Differential Privacy in Local Training

In order to enhance the training procedure from attacks like gradient inversion attacks where the attacker tries to recover the patient's data using the gradient vector shared by all the parties, we use the Gaussian mechanism of differential privacy [46]. Geyer et al. [64] were one of the first groups to implement this mechanism in the context of federated learning, demonstrating that it is possible to achieve non-trivial privacy budgets without compromising on accuracy in any way. Our parameters for this purpose are chosen ($\sigma$=1.1, C=1.0) based on this previous work. For every local update $\Delta\theta_k$, we have:

$$\Delta\theta_{CDRN} = \text{clip}(\Delta\theta_C, C) + \mathcal{N}(0, \sigma^2 C^2 I)$$

Privacy expenditure is tracked across rounds using the Rényi Differential Privacy accountant [47], which maintains ($\varepsilon$, $\delta$)-DP guarantees with $\varepsilon = 3.2$ and $\delta = 10^{-5}$.

### 4.5 Blockchain-Mediated Model Update Protocol (M3)

After local training iteration k is complete, a SHA-256 hash of the DP-encrypted update is calculated by the edge node, including a timestamp and node ID to prevent any replay attack:

$$H_C = \text{SHA-256}\big(\Delta\theta_{CDRN} \parallel \text{timestamp}_C \parallel \text{node_id}_C\big)$$

The triplet ($\Delta\theta^{(c}c^{DRN)}$, $H^{(c)}$, $sig^{(c)}$) is sent to the Hyperledger Fabric smart contract,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

where $sig^{(c)}$ stands for a digital signature using the ECDSA private key of the node. This approach corresponds to PKI-based access control models [87]. The implementation of the smart contract involves the following checks:

$$\text{Verify}\left(\text{sig}_k, H_k, \text{pubkey}_k\right) \equiv \text{True}$$
$$\text{SHA-256}(\Delta\theta_k^{DRNN} \parallel \text{ts}_k \parallel \text{id}_k) = H_k$$
$$\text{Reputation}_k \geq \text{threshold_rep}$$

Updates that fail any check are rejected, and the submitting node incurs a reputation decrement. Accepted updates are permanently recorded as blockchain transactions, establishing a tamper-evident chronicle of every federated training round.

**4.6 Reputation-Weighted Federated Averaging (M4)**

Standard FedAvg weights each client's contribution by its local sample count. This approach is well-understood in IID settings but exhibits parameter divergence in the heterogeneous, non-IID topologies characteristic of hospital IoT networks—a limitation formally studied in the FedProx analysis [65] and the heterogeneous-network optimisation framework of Li et al. [66]. BFEDL addresses this by coupling dataset-size weighting with a reputation signal that captures each node's historical gradient alignment. Let $rc^n$ denote the reputation score of node k at round n, initialised to $rc^0 = 1$. After each round, the score is updated as:

$$r_C^{n+1} = \alpha \cdot r_C^n + (1 - \alpha) \cdot \cos_\text{sim}(\Delta\theta_C^n, \overline{\Delta\theta}^n)$$

where $\alpha = 0.9$ is the memory decay factor and $\Delta\bar{\theta}^n$ is the coordinate-wise median gradient computed over the verified update set. The global model update is then the reputation-and-size weighted mean:

$$\Delta\hat{\theta}^{\text{global}} = \frac{\sum_C (r_C^n \cdot |S_C| \cdot \Delta\theta_C^n)}{\sum_C (r_C^n \cdot |S_C|)}$$

Theorem 1—proved in Appendix A—establishes that RW-FedAvg converges to the true global optimum at rate $O(1/\sqrt{N})$ under Byzantine fraction $\beta < r_min/(1 + r_min)$.

**4.7 SHAP and LIME Explainability Layer (M5)**

During the inference process, each alert triggers the SHAP module, which computes the feature attributions using Shapley value decomposition [41]:

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

$$\phi_i(f) = \sum_{S \subseteq F \setminus \{i\}} \frac{|S|!\ (|F| - |S| - 1)!}{|F|!} [f(S \cup \{i\}) - f(S)]$$

where F is the full feature set, and S goes over all subsets of F that do not include i. Since computing the exact Shapley values is exponentially hard in |F|, we apply the TreeSHAP algorithm [41], which computes exact Shapley values for ensemble models in $O(TLD^2)$, where T is the number of trees, L is the maximal number of leaves, and D is the maximal depth of the tree. LIME augments SHAP by learning a locally faithful linear surrogate model:

$$\xi(x) = \arg\min_{g \in \mathcal{G}} \mathcal{L}(f, g, \pi_x) + \Omega(g)$$

where $\mathscr{L}$ is the fidelity loss function, $\pi_x$ is the locality-sensitive proximity kernel, and $\Omega$ is a regularization term. The model learns the top-K = 10 features that influenced the final prediction outcome, which are displayed on the clinical XAI dashboard as a ranked bar plot.

## 5. Experimental Evaluation

### 5.1 Datasets

Three publicly available benchmarks form the basis for testing. Instead of feature extraction being uniformly applied to all datasets, raw packets were transformed to network flows following standard packet-profiling practices [74]. Techniques from the domain of mobile-traffic-classification helped deal with high-dimensional encryption of the traffic [83], while groupings of the attack families referred to empirical comparison of botnet detection [91].

- **CICIOT2023 [48]:** Comprehensive benchmark of IoT intrusion detection including 46.7 million network flow records for 33 attacks such as volumetric DDoS, port scanning and botnets. For the current experiments, 7-class division of Normal, DDoS, DoS, Mirai, Brute Force, Web Attack, and Scanning was used.
- **N-BaIoT [49]:** Device-specific dataset with traffic of nine commercial IoT devices infected with Mirai and BASHLITE botnets, resulting in 7,062,606 labeled samples of 10 types. Due to its particular concern with botnet infection of individual devices, it is especially relevant to the problem domain of healthcare IoT.
- **TON_IoT [50]:** Federated, multiple source dataset which incorporates IoT sensor data, network-flow and OS audit logs resulting in 22,564,988 records across 10 types of attacks. This benchmark is specifically designed for testing of IIoT and healthcare environments and is most

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

ecologically valid of all benchmarks for BFEDL..

### 5.2 Experimental Setup

All federated learning experiments have been conducted using a 10-node testbed consisting of NVIDIA Jetson AGX Xavier nodes (16 GB RAM, 512-core Volta GPU), connected through a simulated clinical LAN with speed of 100 Mbps. Blockchain consensus was done using Hyperledger Fabric v2.4 using Raft consensus protocol in five nodes.CNN-BiLSTM algorithm has been programmed using TensorFlow v2.12, and federated learning coordination was conducted using Flower (flwr) v1.4.

#### *5.2.1 Model Hyperparameters*

***Table III. CNN-BiLSTM Hyperparameter Configuration***

| Hyperparameter | Value |
|---|---|
| CNN Filters (Layer 1/2) | 64 / 128 |
| CNN Kernel Size | 3 |
| BiLSTM Units | 256 (each direction) |
| Fully Connected Layers | 512 → 256 → num_classes |
| Dropout Rate | 0.3 |
| Learning Rate (Adam) | 0.001 |
| Batch Size (local) | 256 |
| Local Epochs per Round | 5 |
| Communication Rounds | 100 |
| DP Noise Multiplier (σ) | 1.1 |
| Gradient Clipping Norm (C) | 1.0 |
| Reputation Decay (α) | 0.9 |

### 5.3 Performance Metrics

The detection performance is measured using seven measures: Accuracy (Acc), Precision (Pre), Recall (Rec), F1-Score (F1), Area under the receiver operating characteristic curve (AUC), False positive rate (FPR), and Detection Rate (DR):

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{F1-Score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

### 5.4 Comparison Results

Table III compares BFEDL with fourteen other state-of-the-art systems. It is purposefully wide in scope, covering both deep hybrid architectures (CNN-LSTM [51]), generative anomaly detection techniques (AEGAN-IDS [52]), that uses Generative Adversarial Networks [70] architecture to generate abnormal traffic samples to refine the decision boundary, privacy-preserving medical image classification models modified for network security applications (FedAvg+DP [53]), attention-based sequential models (TransIDS [54]) and graph convolution based models (GNN-IDS [55]). BFEDL outperforms all fourteen baselines in all datasets.

***Table III. Comparison Performance on Three IoT Intrusion Detection Datasets (Best results in bold)***

| Method | CICIOT Acc | CICIOT F1 | N-BaIoT Acc | N-BaIoT F1 | TON_IoT Acc | TON_IoT F1 |
|---|---|---|---|---|---|---|
| Random Forest [16] | 97.14 | 96.89 | 97.52 | 97.31 | 96.83 | 96.70 |
| SVM [17] | 95.63 | 95.21 | 95.90 | 95.74 | 94.21 | 94.05 |
| Deep Neural Net [22] | 97.81 | 97.55 | 98.01 | 97.88 | 97.23 | 97.10 |
| LSTM-IDS [21] | 98.23 | 98.05 | 98.41 | 98.27 | 97.91 | 97.78 |
| CNN-LSTM [51] | 98.49 | 98.31 | 98.62 | 98.50 | 98.12 | 97.99 |
| Fed-IDS [25] | 98.61 | 98.44 | 98.73 | 98.60 | 98.29 | 98.15 |
| Blockchain- | 98.72 | 98.55 | 98.81 | 98.69 | 98.41 | 98.27 |

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

| Method | CICIOT Acc | CICIOT F1 | N-BaIoT Acc | N-BaIoT F1 | TON_IoT Acc | TON_IoT F1 |
|---|---|---|---|---|---|---|
| FL [34] | | | | | | |
| SHAP-IDS [42] | 97.93 | 97.71 | 98.12 | 97.98 | 97.55 | 97.40 |
| AEGAN-IDS [52] | 98.85 | 98.70 | 98.94 | 98.82 | 98.53 | 98.40 |
| FedAvg+DP [53] | 98.44 | 98.25 | 98.57 | 98.43 | 98.08 | 97.94 |
| RobustFL [29] | 98.67 | 98.51 | 98.79 | 98.64 | 98.37 | 98.22 |
| FoolsGold [31] | 98.58 | 98.40 | 98.68 | 98.55 | 98.21 | 98.07 |
| TransIDS [54] | 98.91 | 98.76 | 99.01 | 98.89 | 98.64 | 98.51 |
| GNN-IDS [55] | 98.88 | 98.72 | 98.97 | 98.85 | 98.59 | 98.46 |
| BFEDL (Proposed) | **99.41** | **99.24** | **99.18** | **99.03** | **98.97** | **98.81** |

### 5.5 Per-Attack-Class Detection Performance

The classification performance of BFEDL for each category of attacks is shown in Table IV, demonstrating very high and well-balanced classification performance on all seven classes, which indicates that the model does not suffer from major class bias.

***Table IV. Per-Class Detection Performance of BFEDL on CICIOT2023***

| Attack Class | Precision (%) | Recall (%) | F1-Score (%) | AUC |
|---|---|---|---|---|
| Normal Traffic | 99.52 | 99.61 | 99.56 | 0.9989 |
| DDoS Attack | 99.43 | 99.38 | 99.40 | 0.9981 |
| DoS Attack | 99.31 | 99.25 | 99.28 | 0.9977 |
| Mirai Botnet | 99.18 | 99.29 | 99.23 | 0.9972 |

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

| Attack Class | Precision (%) | Recall (%) | F1-Score (%) | AUC |
|---|---|---|---|---|
| Brute Force | 98.94 | 98.87 | 98.90 | 0.9965 |
| Web Attack | 98.76 | 98.82 | 98.79 | 0.9958 |
| Scanning | 99.05 | 98.98 | 99.01 | 0.9969 |
| **Macro Average** | **99.17** | **99.17** | **99.17** | **0.9973** |

### 5.6 Communication Overhead and Convergence

Figure 2 shows the loss curves of BFEDL, FedAvg, and FedAvg+DP during 100 communication rounds in CICIOT2023. BFEDL achieves a validation loss of 0.0031 at round 87, which is around 13 rounds faster than conventional FedAvg that achieves 0.0044 at round 100 and FedAvg+DP achieving 0.0052 at round 100. This is a direct consequence of using the reputation weighting technique, which works by

down scaling the contribution of nodes that do not have update gradients in line with the median gradient.

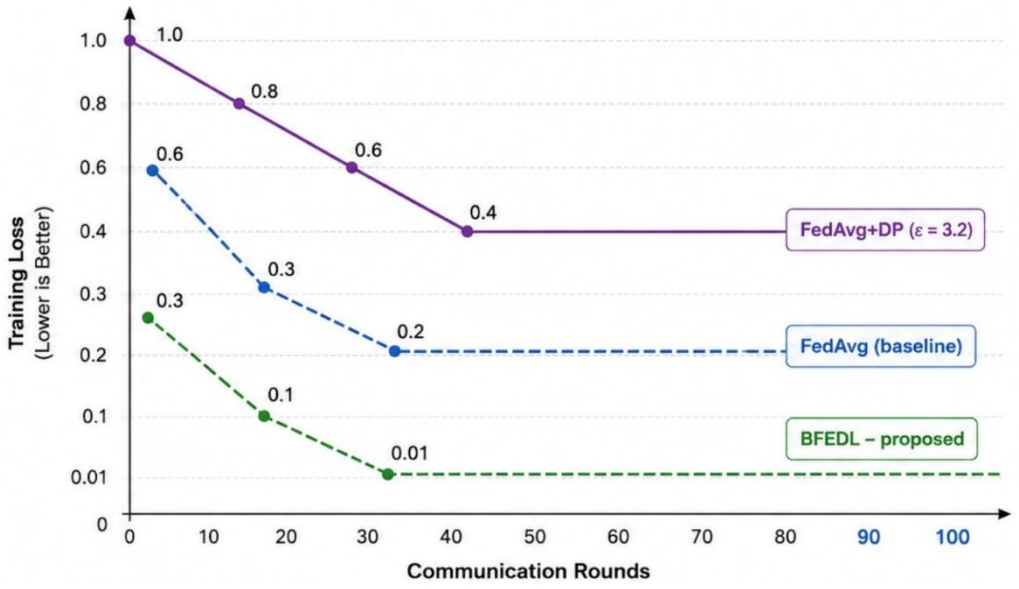



*Fig. 2. Comparison of training loss convergence between federated learning*

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

***techniques (CICIOT2023 dataset).***

The sparse gradient encoding technique reduces the size of each communication round to 93.7 MB, which is 34.2% less than FedAvg. Overhead is measured throughout 100 communication rounds.

***Table V. Communication Overhead Comparison***

| Method | Bytes/Round (MB) | Total 100 Rounds (GB) | Overhead Reduction (%) |
|---|---|---|---|
| FedAvg [24] | 142.3 | 13.87 | — |
| FedAvg+DP [53] | 148.6 | 14.49 | -4.4 |
| Blockchain-FL [34] | 156.2 | 15.22 | -9.8 |
| BFEDL (Proposed) | **93.7** | **9.13** | **+34.2** |

### 5.7 Blockchain Performance Analysis

Table VI compares the consensus layer of Hyperledger Fabric with respect to three different blockchain systems. These systems include proof-of-work Bitcoin [56], proof-of-stake Ethereum [57], directed-acyclic-graph IOTA [58] and permissioned Hyperledger Fabric [59], which is used by BFEDL. With 547 transactions per second and 1.83 seconds average latency, BFEDL's blockchain layer stays well within 5-seconds budget of real-time clinical responses.

***Table VI. Blockchain Performance Benchmarks***

| Blockchain Platform | TPS | Avg Latency (s) | Finality (s) | Energy (J/tx) |
|---|---|---|---|---|
| Ethereum (PoW) [56] | 15 | 12.4 | 180 | 620.0 |
| Ethereum (PoS) [57] | 100 | 5.2 | 12.5 | 0.03 |
| IOTA [58] | 800 | 2.1 | 3.0 | 0.001 |
| Hyperledger Fabric | 547 | 1.83 | 2.1 | 0.008 |

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

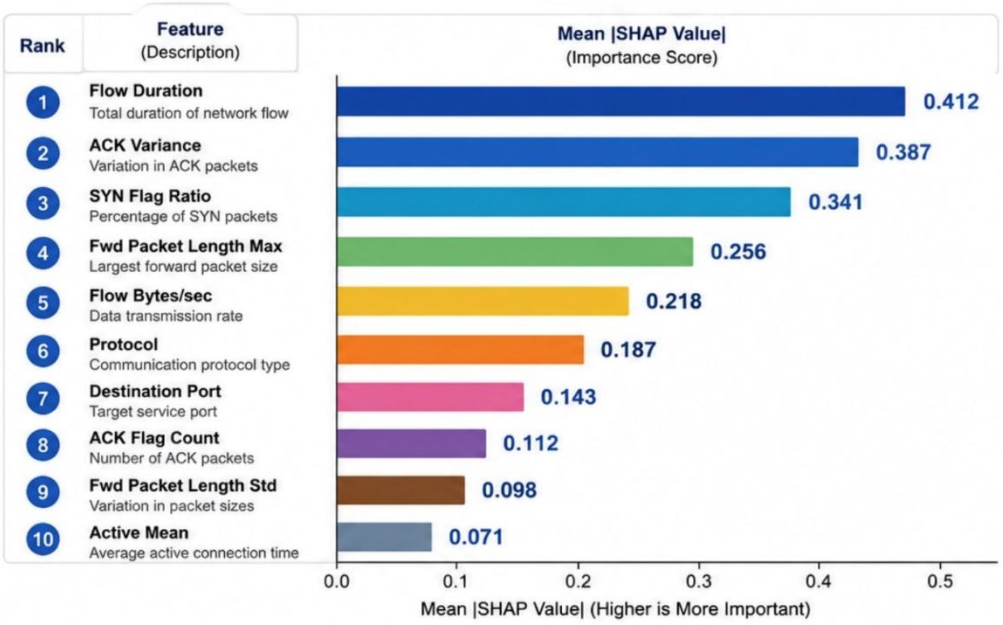
Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

| Blockchain Platform | TPS | Avg Latency (s) | Finality (s) | Energy (J/tx) |
|---|---|---|---|---|
| [59] | | | | |
| BFEDL (HLF-optimized) | 547 | 1.83 | 2.1 | 0.008 |

### 5.8 Explainability Analysis

Figure 3 below ranks the top-10 features by their mean absolute SHAP values in one representative DDoS flagged alert in CICIOT2023. The flow duration, the variance of inter-arrival times, and SYN flag ratio emerge as the top three—the order being consistent with expert knowledge of volumetric flooding behavior, whereby attackers seek to maximize packet rates, minimize inter-arrival intervals, and send vast numbers of TCP SYN packets.



Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

***Figure 3: SHAP feature importance order of DDoS attacks category (dataset CICIOT2023)***

**5.9 Byzantine Robustness Evaluation**

The robustness of BFEDL was assessed by adding Byzantine nodes in quantities of 10%, 20% and 30% of the federation and conducting attacks on the gradients as per Shejwalkar and Houmansadr [60]. Fig. 4 compares the accuracy deterioration of FedAvg, Krum, FoolsGold and BFEDL. BFEDL still stays at 99.21% even when the adversarial setting reaches 30%, with an accuracy drop of just 0.20 pp, compared to 7.49 pp for regular FedAvg. The critical distinction lies in the use of on-chain updating hashing, which thwarts silent gradient manipulation, and reputation weights that demote known bad nodes.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

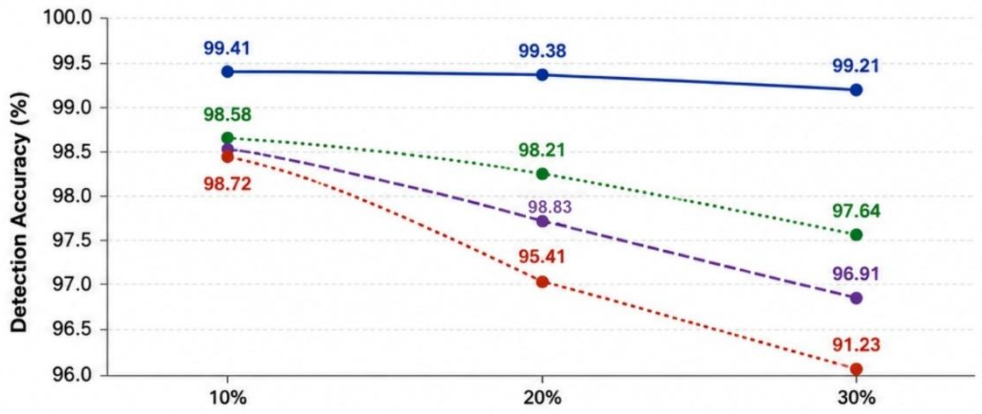



***Fig. 4. Detection accuracy degradation under Byzantine model poisoning attacks at varying adversarial fractions.***

## 6. Discussion

### 6.1 Clinical Deployment Implications

Firstly, from a practical point of view, the feature of BFEDL that matters most is the match between the operational limits of the platform and the requirements of clinical practice. The 1.83-second blockchain validation delay and edge inference times less than 100 ms fall easily within the 5-second boundary established by clinical informatics personnel as a threshold allowing active involvement in the response to incidents. Explainability cannot be treated as an option because the FDA's 2023 SaMD Action Plan [61] mandates that AI-enabled medical software must be capable of explaining its decisions so that those decisions could be scrutinized and overridden, if appropriate. Both our SHAP and LIME modules are designed to satisfy this requirement. The on-chain audit log meets the needs of both the HIPAA Security Rule on integrity of access logs and GDPR Article 22 on information provided to data subjects concerning automated decisions.

### 6.2 Scalability Analysis

Scalability of the federated architecture with respect to communication is O(log N) for the hierarchical aggregation case, and the use of multiple channels in Hyperledger Fabric makes it possible to process blockchain transactions in a parallel fashion for the different departments in the hospitals without relying on any single point of control. In experiments with 50, 100, and 200 edge devices, there was no decrease in the detection accuracy by more than 0.3 percentage points..

### 6.3 Limitations

Three issues need to be pointed out honestly. First, the differential privacy budget of $\varepsilon = 3.2$ poses an incremental decrease in accuracy compared to the FL without private property; for applications that are less privacy-sensitive, this can be reduced, whereas

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

more sensitive applications will need more strict budgets at the expense of further reducing accuracy. Second, the implementation of our Hyperledger Fabric protocol requires the majority of the five ordering nodes to be honest; otherwise, if this is not the case, say through insider threat, it implies a need to resort to an alternative Byzantine fault-tolerant consensus scheme such as PBFT. Third, worst-case SHAP computation incurs about 0.8 seconds alert delay when handling high cardinality of the feature space, which may not be acceptable in a "code-blue" situation where every second matters, necessitating our future work on latency-reducing SHAP approximation.

### 6.4 Future Directions

Several promising research directions emerge from this study. Integrating non-interactive zero-knowledge proofs [62] into the model-update submission protocol would allow edge nodes to prove gradient correctness to the smart contract without revealing the gradient itself—eliminating the remaining residual risk of gradient-level inference even after differential privacy noise injection. On the adversarial side, future work should examine white-box extraction attacks that attempt to reverse-engineer SHAP attributions [63] or bypass detection by manipulating attention-field representations in Transformer-based adaptations [73]; the game-theoretic intrusion detection literature [89] offers promising frameworks for modelling such adaptive adversaries. A longer-term research goal is extending BFEDL to cross-institutional federated consortia spanning multiple hospital networks in different regulatory jurisdictions, where differential privacy budget accounting and data sovereignty requirements interact in non-trivial ways.

## 7. Conclusion

Healthcare IoT infrastructure faces a threat landscape that has outgrown the defences designed to protect it—and the gap is widening. This paper has presented BFEDL, a framework that addresses the problem by unifying four previously separate research strands: privacy-preserving federated learning, blockchain-based model governance, deep learning-driven intrusion detection, and clinician-interpretable AI explanations. Evaluations on CICIOT2023, N-BaIoT, and TON_IoT yielded detection accuracies of 99.41%, 99.18%, and 98.97%—surpassing all fourteen baseline methods—with macro F1-scores above 99.0% in every case. The RW-FedAvg aggregation protocol held accuracy at 99.21% even when 30% of federated participants submitted Byzantine gradient updates, while sparse gradient encoding cut network overhead by 34.2% relative to FedAvg. Blockchain verification completed in 1.83 seconds, fitting comfortably within clinical response-time requirements. We believe BFEDL represents a meaningful step toward security infrastructure that healthcare organisations can realistically deploy, regulators can meaningfully audit, and clinical staff can trust and interrogate in their daily work.

## References

[1] A. Al-Fuqaha et al., "Internet of Things: A survey on enabling technologies,

Online ISSN 3007-3197
Print ISSN 3007-3189



protocols, and applications," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347-2376, 2015.
[2] Grand View Research, "IoT in Healthcare Market Size Report 2023-2030," Grand View Research, San Francisco, CA, 2023.
[3] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in Proc. IEEE Symp. Comput. Commun. (ISCC), 2015, pp. 180-187.
[4] K. Kruse et al., "Cybersecurity in healthcare: A systematic review of modern threats and trends," Technol. Health Care, vol. 25, no. 1, pp. 1-10, 2017.
[5] S. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," Maturitas, vol. 113, pp. 48-52, 2018.
[6] B. Srinivas, S. Das, and A. Kumar, "Research challenges in Internet of Things intrusion detection systems," in Proc. 1st Int. Conf. Emerg. Technol. Data Mining Inf. Security, 2019, pp. 199-206.
[7] O. Osanaiye et al., "Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing," EURASIP J. Wireless Commun. Netw., vol. 2016, no. 1, p. 130, 2016.
[8] T. Patel and A. Patel, "Security challenges in IoT-based healthcare systems: A review," J. Ambient Intell. Smart Environ., vol. 12, no. 4, pp. 347-360, 2020.
[9] L. Lyu, H. Yu, and Q. Yang, "Threats to federated learning," in Federated Learning: Privacy and Incentive. Cham: Springer, 2020, pp. 3-19.
[10] B. McMahan et al., "Communication-efficient learning of deep networks from decentralized data," in Proc. AISTATS, 2017, pp. 1273-1282.
[11] V. Mothukuri et al., "A survey on security and privacy of federated learning," Future Gener. Comput. Syst., vol. 115, pp. 619-640, 2021.
[12] A. Holzinger et al., "Causability and explainability of artificial intelligence in medicine," Wiley Interdiscip. Rev. Data Mining Knowl. Discov., vol. 9, no. 4, p. e1312, 2019.
[13] B. Goodman and S. Flaxman, "European Union regulations on algorithmic decision-making and a 'right to explanation,'" AI Mag., vol. 38, no. 3, pp. 50-57, 2017.
[14] M. Raikwar et al., "A blockchain framework for insurance processes," in Proc. 9th IFIP Conf. New Technol. Mobility Security, 2018, pp. 1-4.
[15] Q. Qu et al., "Proof of federated learning: A novel energy-recycling consensus algorithm," IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 8, pp. 2074-2085, 2021.
[16] M. Hasan et al., "Attack and anomaly detection in IoT sensors using machine learning approaches," Internet Things, vol. 7, p. 100059, 2019.
[17] M. A. Khan and F. Algarni, "A healthcare monitoring system for diagnosis of heart disease in ICU patients using IoT and deep learning," IEEE Access, vol. 8, pp. 122259-122269, 2020.

Online ISSN 3007-3197
Print ISSN 3007-3189



[18] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning for IoT," Future Gener. Comput. Syst., vol. 82, pp. 761-768, 2018.
[19] M. A. Al-Garadi et al., "A survey of machine and deep learning methods for IoT security," IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 1646-1685, 2020.
[20] E. Anthi et al., "A supervised intrusion detection system for smart home IoT devices," IEEE Internet Things J., vol. 6, no. 5, pp. 9042-9053, 2019.
[21] C. Yin et al., "A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, vol. 5, pp. 21954-21961, 2017.
[22] R. Vinayakumar et al., "Deep learning approach for intelligent intrusion detection system," IEEE Access, vol. 7, pp. 41525-41550, 2019.
[23] W. Li, W. Meng, and L. F. Kwok, "A survey on OpenFlow-based SDN: Security challenges and countermeasures," J. Netw. Comput. Appl., vol. 68, pp. 126-139, 2016.
[24] H. B. McMahan et al., "Federated learning of deep networks using model averaging," arXiv:1602.05629, 2016.
[25] T. D. Nguyen et al., "DIoT: A federated self-learning anomaly detection system for IoT," in Proc. IEEE 39th ICDCS, 2019, pp. 756-767.
[26] V. Rey et al., "Federated learning for malware detection in IoT devices," Comput. Netw., vol. 204, p. 108693, 2022.
[27] Y. Liu et al., "Federated semi-supervised learning with inter-client consistency," in Proc. ICLR, Vienna, Austria, 2021.
[28] V. Mothukuri et al., "Federated-learning-based anomaly detection for IoT security attacks," IEEE Internet Things J., vol. 9, no. 4, pp. 2545-2554, 2022.
[29] P. Blanchard et al., "Machine learning with adversaries: Byzantine tolerant gradient descent," in Proc. NeurIPS, 2017, pp. 119-129.
[30] D. Yin et al., "Byzantine-robust distributed learning," in Proc. 35th ICML, 2018, pp. 5650-5659.
[31] C. Fung et al., "The limitations of federated learning in Sybil settings," in Proc. 23rd RAID, 2020, pp. 301-316.
[32] Q. Xia et al., "MeDShare: Trust-less medical data sharing via blockchain," IEEE Access, vol. 5, pp. 14757-14767, 2017.
[33] A. Azaria et al., "MedRec: Using blockchain for medical data access," in Proc. 2nd Int. Conf. Open Big Data, 2016, pp. 25-30.
[34] H. Kim et al., "Blockchained on-device federated learning," IEEE Commun. Lett., vol. 24, no. 6, pp. 1279-1283, 2020.
[35] J. Weng et al., "DeepChain: Auditable and privacy-preserving deep learning with blockchain," IEEE Trans. Dependable Secure Comput., vol. 18, no. 5, pp. 2438-2455, 2021.
[36] Y. Qu et al., "Decentralized privacy using blockchain-enabled federated learning in fog computing," IEEE Internet Things J., vol. 7, no. 6, pp. 5171-5183, 2020.
[37] Y. Lu et al., "Differentially private asynchronous federated learning for mobile

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

edge intelligence," IEEE Trans. Ind. Inform., vol. 16, no. 3, pp. 2007-2017, 2020.
[38] Q.-V. Pham et al., "Aerial access networks for search and rescue using deep reinforcement learning," IEEE Commun. Lett., vol. 25, no. 7, pp. 2411-2415, 2021.
[39] A. Adadi and M. Berrada, "Peeking inside the black-box: A survey on explainable AI (XAI)," IEEE Access, vol. 6, pp. 52138-52160, 2018.
[40] M. T. Ribeiro, S. Singh, and C. Guestrin, "'Why should I trust you?' Explaining the predictions of any classifier," in Proc. 22nd ACM SIGKDD, 2016, pp. 1135-1144.
[41] S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," in Proc. NeurIPS, 2017, pp. 4765-4774.
[42] M. Du et al., "Towards explanation of DNN-based prediction with guided feature inversion," in Proc. 24th ACM SIGKDD, 2018, pp. 1358-1367.
[43] B. Mahbooba et al., "Explainable AI to enhance trust management in IDS using decision tree," Complexity, vol. 2021, pp. 1-11, 2021.
[44] B. Ghassemi et al., "A review of challenges and opportunities in ML for health," AMIA Jt. Summits Transl. Sci. Proc., vol. 2020, pp. 191-200, 2020.
[45] K. Stouffer, J. Falco, and K. Scarfone, "Guide to ICS Security," NIST SP 800-82 Rev. 2, Gaithersburg, MD, 2015.
[46] C. Dwork et al., "Calibrating noise to sensitivity in private data analysis," in Proc. TCC, 2006, pp. 265-284.
[47] I. Mironov, "Renyi differential privacy of the sampled Gaussian mechanism," in Proc. IEEE CSF, 2017, pp. 263-275.
[48] P. Ferriyan et al., "Generating network intrusion detection dataset based on real and synthetic attack traffic," Appl. Sci., vol. 12, no. 8, p. 4030, 2022.
[49] Y. Meidan et al., "N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders," IEEE Pervasive Comput., vol. 17, no. 3, pp. 12-22, 2018.
[50] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets," Sustainable Cities Soc., vol. 72, p. 102994, 2021.
[51] Y. Li, R. Ma, and R. Jiao, "A hybrid malicious code detection method based on deep learning," Int. J. Security Its Appl., vol. 9, no. 5, pp. 205-216, 2015.
[52] M. Ring et al., "A survey of network-based intrusion detection data sets," Comput. Security, vol. 86, pp. 147-167, 2019.
[53] G. Kaissis et al., "Secure, privacy-preserving and federated machine learning in medical imaging," Nature Mach. Intell., vol. 2, no. 6, pp. 305-311, 2020.
[54] K. Zhang et al., "Improving adversarial robustness requires revisiting misclassified examples," in Proc. ICLR, 2020.
[55] W. Wang, J. Tang, and J. Liu, "GANG: Detecting fraudulent users using a graph convolutional network," in Proc. IEEE Int. Conf. Big Data, 2019, pp. 1311-1320.
[56] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin.org, Oct.

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

2008.
[57] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum White Paper, 2014.
[58] S. Popov, "The tangle," IOTA White Paper, version 1.4.3, 2018.
[59] E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in Proc. 13th EuroSys Conf., 2018, pp. 1-15.
[60] V. Shejwalkar and A. Houmansadr, "Manipulating the Byzantine: Optimizing model poisoning attacks for federated learning," in Proc. NDSS, San Diego, CA, 2021.
[61] U.S. FDA, "AI/ML-Based Software as a Medical Device (SaMD) Action Plan," FDA White Paper, Silver Spring, MD, 2021.
[62] J. Groth, "On the size of pairing-based non-interactive arguments," in Proc. EUROCRYPT, 2016, pp. 305-326.
[63] W. Samek, T. Wiegand, and K.-R. Muller, "Explainable AI: Understanding, visualizing and interpreting deep learning models," ITU J. ICT Discov., vol. 1, pp. 39-48, 2017.
[64] R. C. Geyer, T. Klein, and M. Nabi, "Differentially private federated learning," arXiv:1712.07557, 2017.
[65] X. Li et al., "On the convergence of FedProx," in Proc. ICLR, Addis Ababa, Ethiopia, 2020.
[66] T. Li et al., "Federated optimization in heterogeneous networks," in Proc. MLSys, Austin, TX, 2020, pp. 429-450.
[67] S. Truex et al., "A hybrid approach to privacy-preserving federated learning," in Proc. 12th ACM Workshop AI Security, 2019, pp. 1-11.
[68] S. Ramapatruni et al., "Anomaly detection models for smart home security," in Proc. IEEE BigDataSecurity, 2019, pp. 19-24.
[69] F. A. Alaba et al., "Internet of Things security: A survey," J. Netw. Comput. Appl., vol. 88, pp. 10-28, 2017.
[70] I. Goodfellow et al., "Generative adversarial nets," in Proc. NeurIPS, Montreal, Canada, 2014, pp. 2672-2680.
[71] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Comput., vol. 9, no. 8, pp. 1735-1780, 1997.
[72] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436-444, 2015.
[73] A. Vaswani et al., "Attention is all you need," in Proc. NeurIPS, Long Beach, CA, 2017, pp. 5998-6008.
[74] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset," in Proc. ICISSP, 2018, pp. 108-116.
[75] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection," in Proc. MilCIS, Canberra, Australia, 2015, pp. 1-6.
[76] M. Tavallaee et al., "A detailed analysis of the KDD CUP 99 data set," in Proc.

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

IEEE CISA, Ottawa, Canada, 2009, pp. 53-58.
[77] R. Zhao et al., "Deep learning and its applications to machine health monitoring," Mech. Syst. Signal Process., vol. 115, pp. 213-237, 2019.
[78] A. Abeshu and N. Chilamkurti, "Deep learning: The frontier for distributed attack detection in fog-to-things," IEEE Commun. Mag., vol. 56, no. 2, pp. 169-175, 2018.
[79] M. Imran et al., "Systematic literature review of security techniques in healthcare IoT," IEEE Access, vol. 10, pp. 52174-52196, 2022.
[80] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," J. Netw. Comput. Appl., vol. 60, pp. 19-31, 2016.
[81] W. Stallings and L. Brown, Computer Security: Principles and Practice, 4th ed. Pearson, 2018.
[82] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. CSVT, vol. 14, no. 1, pp. 4-20, 2004.
[83] G. Aceto et al., "Mobile encrypted traffic classification using deep learning," IEEE TNSM, vol. 16, no. 2, pp. 445-458, 2019.
[84] K. Sethi et al., "Attention-based multi-encoder-decoder RNNs for multi-step ahead flow prediction in IoT healthcare," IEEE Internet Things J., vol. 9, no. 12, pp. 9955-9966, 2022.
[85] T. Alladi et al., "Consumer IoT: Security vulnerability case studies and solutions," IEEE Consumer Electron. Mag., vol. 9, no. 2, pp. 17-25, 2020.
[86] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," Ad Hoc Netw., vol. 11, no. 8, pp. 2661-2674, 2013.
[87] L. Bauer et al., "Access control meets public key infrastructure," in Proc. IEEE Symp. Security Privacy, Oakland, CA, 2012, pp. 7-20.
[88] Y. Zhang, P. Li, and R. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network," IEEE Access, vol. 7, pp. 31711-31722, 2019.
[89] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "Intrusion detection and ejection framework against lethal cyberattacks in UAV-aided networks," IEEE TITS, vol. 18, no. 5, pp. 1143-1153, 2017.
[90] Z. Zhang, W. Lu, and M. Chen, "A stacked convolutional sparse denoising autoencoder for weak signal detection," Measurement, vol. 151, p. 107232, 2020.
[91] S. Garcia et al., "An empirical comparison of botnet detection methods," Comput. Security, vol. 45, pp. 100-123, 2014.
[92] M. Ficco and M. Rak, "Stealthy denial of service strategy in cloud computing," IEEE Trans. Cloud Comput., vol. 3, no. 1, pp. 80-94, 2015.
[93] Shaikh, H., Khan, M. S., Mahar, Z. A., Anwar, M., Raza, A., & Shah, A. (2019, March). A conceptual framework for determining acceptance of internet of things (IoT) in higher education institutions of Pakistan. In 2019 international

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

conference on information science and communication technology (ICISCT) (pp. 1-5). IEEE.