Intrusion Detection for IOMT Networks with Digital Twins, Machine Learning, and Federated Learning: A Comprehensive Review

Ahammed Jasim.T.P
Department of Computer Science (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:jazimahammed102@gmail.com

Alan Antony
Department of Computer Science (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:alanantony3634@gmail.com

Anugrah.V.S
Department of Computer Science (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:anugrahsunil123@gmail.com

Ayisha Sana.K.K
Department of Computer Science (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:ayishasanakk12@gmail.com

Ms.Anugraha.P.P
Assistant Professor
Department of Computer Science (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:anugrahapp@vjec.ac.in

***Abstract*—The Internet of Medical Things (IoMT) is rapidly transforming healthcare by enabling real-time monitoring, remote diagnosis, and intelligent decision-making. While these technologies improve patient care and efficiency, they also introduce new vulnerabilities in terms of data security, patient privacy, and system reliability. The growing reliance on interconnected medical devices makes IoMT systems an attractive target for adversaries, with risks ranging from data breaches and adversarial manipulation to system-wide intrusions. Traditional security frameworks, such as centralized intrusion detection systems or rule-based approaches, struggle to keep up with the evolving nature of threats and the unique constraints of IoMT environments, including limited device resources, latency sensitivity, and the need for privacy preservation. To overcome these limitations, we present an integrated framework that combines federated learning, blockchain, and advanced deep learning models to provide a holistic solution for secure data processing and intrusion detection in IoMT ecosystems. The proposed architecture introduces quantum-based authentication for stronger device-level security, privacy-preserving collaborative training to enable distributed model learning without exposing raw patient data, and noise-driven feature masking to minimize the risks of adversarial attacks and poisoning attempts. In addition, the framework reduces communication overhead through prototype-driven representation learning and optimization-aware aggregation, ensuring efficiency even in bandwidth-constrained medical networks.**

***Index Terms*—IoMT, Federated Learning, Blockchain, Deep Learning, Privacy Preservation, Intrusion Detection**

I. Introduction

The Internet of Things (IoT) and its healthcare-oriented extension, the Internet of Medical Things (IoMT), are reshaping contemporary life by enabling innovations in smart healthcare, intelligent transport, industrial automation, and continuous real-time monitoring. These interconnected ecosystems produce vast amounts of sensitive data that can significantly improve patient care and decision-making. However, this reliance on data-driven systems also makes critical infrastructures increasingly vulnerable to cyberattacks. IoT and IoMT devices are often resource-limited, heterogeneous in design, and widely dispersed across networks, which makes them appealing targets for adversaries. Attacks such as denial-of-service, spoofing, data injection, and adversarial manipulation exploit these weaknesses, while conventional security measures—including firewalls, cryptographic protocols, and signature-based intrusion detection systems—are proving inadequate. The limitations of these traditional defenses arise from their poor scalability, inefficiency in handling zero-day attacks, and high computational demands, which clash with the lightweight nature and privacy constraints of IoMT devices.

In response, the research community has developed a variety of intelligent intrusion detection systems (IDSs), with a growing emphasis on anomaly-based intrusion detection systems (AIDSs) that leverage machine learning (ML), deep learning (DL), and hybrid techniques. Classical ML models, such as Decision Trees, Random Forests, and Support Vector Machines, have been widely employed for traffic categorization, while DL approaches, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) architectures, excel in automatic feature extraction and modeling temporal health data streams. More recently, Federated Learning (FL) has emerged as a privacy-preserving paradigm that enables distributed devices

to collaboratively train IDS models without the need to share raw patient data. Building upon this, Decentralized Federated Learning (DFL) further removes reliance on central aggregation servers, thereby enhancing scalability and resilience, though it introduces challenges such as ensuring convergence under non-independent and identically distributed (non-IID) data. Additionally, blockchain has been increasingly combined with FL to secure model updates, ensure tamper-resistance, and reduce the risks of poisoning and replay attacks. Other complementary approaches, such as swarm intelligence and optimization-driven frameworks, have been applied to boost resilience, adaptability, and communication efficiency in dynamic IoT environments.

Nevertheless, despite these advancements, major research gaps persist in building IDS frameworks that are simultaneously lightweight, privacy-preserving, and robust enough to withstand sophisticated adversarial attacks. Current systems continue to face challenges related to IoMT heterogeneity, limited computational capacity of edge devices, and the performance degradation caused by skewed or non-IID data distributions. Addressing these issues requires the development of next-generation IDS solutions that integrate the strengths of ML, DL, FL, and blockchain while tailoring their designs to the constraints of real-world IoMT deployments. This literature review synthesizes existing research contributions, outlines their advantages and shortcomings, and highlights open challenges. By doing so, it lays the groundwork for designing scalable, secure, and resilient IDS frameworks that can meet the growing demands of IoT and IoMT ecosystems.Furthermore, as IoMT adoption accelerates in critical healthcare environments, the stakes for ensuring security and reliability grow exponentially. With patient safety and data integrity at risk, the effectiveness of IDS frameworks must be evaluated not only on detection accuracy but also on their adaptability, computational efficiency, and compliance with privacy regulations. This positions the upcoming literature review as a crucial step in mapping current solutions, identifying persistent limitations, and guiding future innovations toward practical, real-world IoMT applications.

II. Literature Review

Fernandes, Rabelo, and da Fonseca [1] conducted an extensive review of decentralized federated learning (DFL) approaches for intrusion detection in IoT-based systems, emphasizing the urgent need to move away from traditional centralized architectures. They noted that conventional intrusion detection systems (IDS) often rely on centralized data collection and model aggregation, which creates communication bottlenecks, scalability issues, and critical single points of failure that can be exploited by attackers. The study highlighted how federated learning (FL) emerged as a privacy-preserving alternative, allowing distributed IoT devices to collaboratively train machine learning models without exposing raw data. However, most existing FL frameworks remain vulnerable due to their reliance on central servers for model aggregation. To address this, the authors reviewed decentralized solutions where devices share updates directly or through blockchain-based mechanisms to ensure trust and immutability. The paper categorized prior contributions into blockchain-assisted DFL, lightweight optimization algorithms for resource-constrained devices, and deep learning models for automated traffic analysis. Their findings suggested that while DFL improves scalability, resilience, and privacy, challenges remain in handling non-IID data, ensuring robustness against adversarial attacks, and reducing communication overhead. Ultimately, the authors concluded that DFL represents a promising evolution of IDS frameworks for IoT but stressed the need for further research on lightweight, attack-resilient, and resource-aware designs suitable for large-scale, heterogeneous environments.

Bolelli et al. [2] introduced the concept of random neural networks (RNNs) within the context of deep learning, aiming to explore their potential for approximating complex nonlinear functions and supporting distributed learning in uncertain environments. Their work investigated how stochastic neurons, which process signals probabilistically rather than deterministically, could be adapted into deep architectures for tasks such as intrusion detection and anomaly classification. The study emphasized that random neural networks offer scalability benefits, as their probabilistic nature reduces training complexity and enables efficient parallelization across distributed devices. Furthermore, they examined applications in IoT environments where uncertainty, noisy data, and limited resources are common challenges. The authors demonstrated that these models can generalize well in dynamic and heterogeneous systems. However, they also acknowledged limitations, such as instability in convergence, sensitivity to parameter tuning, and relatively lower accuracy compared to mainstream deep learning models like convolutional neural networks (CNNs) and recurrent neural networks (RNNs). Despite these constraints, the study positioned random neural networks as an innovative research direction for resource-constrained environments, suggesting that future work should focus on improving stability, robustness, and hybridization with conventional deep architectures. In the broader context of IoT and IoMT intrusion detection, the paper highlighted the potential of stochastic and probabilistic modeling as an alternative paradigm for handling uncertainty in security-critical systems.

Zhou et al. [3] proposed a prototype-based decentralized federated learning (ProtoDFL) framework designed to address the challenges of heterogeneity and dynamic conditions in IoT networks. Their approach relies on using prototype representations of local models to enable efficient knowledge transfer between distributed devices, reducing communication overhead and ensuring robustness against non-IID data. The paper demonstrated how prototype learning can align local model updates into a shared representation space, facilitating better convergence even when device data distributions differ significantly. Experimental results showed that ProtoDFL improves detection accuracy and reduces latency compared to traditional FL, especially in time-varying IoT scenarios. The authors further analyzed the applicability of ProtoDFL in real-world intrusion detection tasks, where IoT nodes face

fluctuating traffic patterns, constrained resources, and evolving attack behaviors. Strengths of the proposed method included scalability, robustness to heterogeneity, and adaptability to decentralized architectures. However, they acknowledged that extreme cases of non-IID data could still hinder model convergence and that devices with minimal computational capacity might face challenges in implementing the framework. Overall, the study contributed a novel perspective on integrating prototype learning into decentralized IDS frameworks, suggesting that this approach holds strong potential for balancing efficiency, scalability, and detection accuracy in heterogeneous IoT environments.

Huang et al. [4] investigated decentralized federated learning (DFL) frameworks for intrusion detection in IoT networks, focusing on the shortcomings of traditional centralized FL approaches. They argued that while FL reduces privacy risks by avoiding raw data sharing, its reliance on a central aggregator still creates vulnerabilities such as communication bottlenecks, single points of failure, and susceptibility to targeted poisoning attacks. To overcome these issues, the authors explored decentralized model sharing architectures, where updates are exchanged in a peer-to-peer manner and validated using distributed mechanisms such as blockchain. Their study reviewed various schemes that combine FL with consensus algorithms to improve trust and resilience in dynamic IoT environments. They highlighted the potential benefits of these architectures in reducing dependency on centralized servers, improving scalability, and supporting large-scale IoT deployments. However, the paper also pointed out critical limitations, including increased communication complexity, high latency due to consensus overhead, and performance degradation under non-IID data distributions. Additionally, they noted that resource-constrained IoT devices may struggle to handle the computational burden of blockchain integration. Overall, the authors concluded that decentralized FL is a promising step toward secure and privacy-preserving IDS in IoT systems but emphasized the need for lightweight consensus mechanisms, optimized communication protocols, and adversarial resilience to ensure practical applicability in real-world networks.

Li et al. [5] examined the role of decentralized federated learning in heterogeneous IoT environments, with a particular focus on balancing scalability, security, and communication efficiency. They highlighted that IoT ecosystems are inherently diverse, featuring devices with varying computational capabilities, connectivity, and energy constraints, which makes intrusion detection especially challenging. To address this, the authors proposed robust aggregation methods designed to mitigate the impact of non-IID data distributions and adversarial manipulations. They also reviewed trust-enhancing mechanisms such as blockchain-assisted validation and reputation-based peer selection to strengthen the reliability of decentralized FL frameworks. Experimental evaluations demonstrated that these methods improve both detection accuracy and resilience to poisoning attacks, while also reducing reliance on centralized coordination. Despite these advances, the authors acknowledged that communication overhead remains a significant barrier in large-scale deployments and that lightweight optimization is needed for resource-constrained IoT devices. Furthermore, they pointed out that while decentralized aggregation improves robustness, it can complicate convergence dynamics in environments with high heterogeneity. The study ultimately concluded that decentralized FL offers a path forward for secure and adaptive intrusion detection in IoT but emphasized the importance of designing scalable, communication-efficient, and energy-aware algorithms to meet the demands of real-world deployments.

Ahmed et al. [6] proposed a Swarm Optimization-Based Federated Learning (SO-FL) framework aimed at improving the cyber resilience of IoT systems against sophisticated adversarial attacks. Inspired by collective behaviors observed in nature, such as bird flocking and fish schooling, their approach integrates swarm intelligence algorithms into the FL aggregation process. The authors argued that this enables adaptive and dynamic defense strategies by optimizing the selection of model updates and enhancing resistance to poisoning and evasion attacks. The paper presented experimental results showing that SO-FL significantly improves detection accuracy and robustness compared to conventional FL, particularly in adversarial settings. Moreover, the swarm optimization approach was shown to enhance scalability and adaptability in large and dynamic IoT environments. However, the study also highlighted trade-offs: the integration of swarm intelligence introduces additional computational costs and latency, which may pose challenges for resource-constrained IoT devices. Additionally, fine-tuning swarm parameters was found to be non-trivial, requiring careful design to avoid instability. Despite these limitations, the authors positioned SO-FL as a promising direction for enhancing the security of distributed IDS frameworks, emphasizing its ability to balance adaptability, robustness, and collaborative intelligence in defending IoT networks from evolving cyber threats.

Wang et al. [7] explored efficient decentralized federated learning (DFL) frameworks aimed at strengthening security and scalability in large-scale IoT deployments. Their work emphasized that although federated learning (FL) has become an important approach for privacy-preserving intrusion detection, it still relies heavily on centralized aggregators, which can create bottlenecks, security vulnerabilities, and limited fault tolerance. To mitigate these issues, the authors proposed communication-efficient aggregation methods and adaptive learning strategies that minimize the number of model exchanges while preserving high accuracy. Their study also addressed the problem of heterogeneous and non-IID data distributions across IoT devices, which significantly degrade model performance in conventional FL. Through simulations, they showed that decentralized aggregation combined with adaptive parameter tuning yields better convergence and robustness under such conditions. The strengths of this work include the clear demonstration of scalability, improved communication efficiency, and adaptability in dynamic IoT environments. However, the authors acknowledged that resilience under adversarial conditions, particularly in the presence of data

poisoning and evasion attacks, remains an unresolved issue. Furthermore, the increased complexity of adaptive aggregation strategies may burden resource-constrained IoT nodes. Overall, the study highlighted that communication-efficient DFL has strong potential for securing IoT systems at scale, but further optimization is needed to balance energy consumption, security, and detection performance.

Shah et al. [8] investigated the wide range of security vulnerabilities present in Internet of Medical Things (IoMT) devices, which are increasingly used for patient monitoring, diagnostics, and healthcare automation. Their study categorized potential threats such as denial-of-service, spoofing, ransomware, and data injection attacks, while emphasizing that IoMT devices are especially vulnerable due to their limited computational capacity, energy constraints, and continuous connectivity. To counter these risks, the authors examined existing countermeasures, including lightweight cryptographic protocols, machine learning–based intrusion detection systems (IDS), and compliance with regulatory frameworks like HIPAA. They noted that while ML-based IDS techniques enhance the ability to detect new and unknown attacks, they often demand computational resources beyond what IoMT devices can provide, thus requiring trade-offs between accuracy and efficiency. The study also stressed the importance of privacy-preserving mechanisms, as IoMT devices handle highly sensitive patient data that cannot be freely transmitted for centralized processing. Their findings suggested that hybrid approaches combining lightweight cryptography, anomaly detection, and decentralized learning could provide a more practical balance. However, limitations such as scalability, adaptability to zero-day attacks, and system interoperability remain unsolved. The paper concluded that IoMT cybersecurity requires solutions that are lightweight, privacy-aware, and adaptable to evolving threats, thereby motivating the development of intrusion detection systems specifically tailored for healthcare applications.

Kamarudin et al. [9] developed a COVID-19 portable health monitoring system using Raspberry Pi, Node-Red, and ThingSpeak to provide real-time monitoring of patients during the pandemic. The system was designed to collect biometric data such as body temperature, oxygen levels, and heart rate, which were then transmitted to a cloud-based platform for storage and analysis. The study emphasized the critical importance of IoT-enabled health monitoring solutions at a time when healthcare systems were overburdened and remote patient care was essential. The authors showcased how the integration of low-cost hardware and open-source platforms could create scalable, portable, and accessible healthcare monitoring tools. While the proposed framework successfully demonstrated real-time monitoring and cloud-based visualization, the study also identified key challenges. These included limitations in data privacy and security, since sensitive patient data transmitted through the cloud may be vulnerable to breaches, and scalability issues when deploying the system to large populations. Additionally, communication delays and reliance on internet connectivity posed risks for continuous monitoring in rural or resource-limited regions. Nevertheless, the system highlighted the feasibility and value of IoT-enabled healthcare monitoring and provided a strong foundation for further development of secure, privacy-preserving, and scalable IoMT solutions.

Alzubaidi et al. [10] presented a detailed review of the role of the Internet of Medical Things (IoMT) in advancing healthcare delivery, while critically examining the associated cybersecurity and privacy risks. The authors highlighted that IoMT devices enable continuous patient monitoring, efficient diagnostics, and personalized treatments, yet their interconnectivity exposes them to malicious intrusions such as spoofing, denial-of-service, and data manipulation. Their survey analyzed how traditional intrusion detection methods struggle to protect IoMT due to the systems' distributed nature and limited computational resources. The paper further examined machine learning (ML) and deep learning (DL)–based intrusion detection systems, noting their advantages in learning complex patterns and detecting previously unseen attacks. However, these approaches often face high computational overheads and lack explainability, making them difficult to deploy directly on IoMT devices. Alzubaidi et al. also discussed emerging paradigms such as federated learning (FL) and blockchain integration, which enable privacy-preserving model training and tamper-proof data sharing, respectively. While these innovations show promise, the authors acknowledged unresolved challenges such as handling non-IID data distributions, minimizing communication overhead, and maintaining energy efficiency in constrained devices. The study concluded that securing IoMT environments requires hybrid frameworks that combine ML, FL, and blockchain, while emphasizing lightweight, attack-resilient, and privacy-aware designs for real-world adoption.

Khalid et al. [11] explored federated learning (FL) as a privacy-preserving framework for intrusion detection in IoMT systems, where sensitive patient data cannot be freely transmitted due to regulatory and ethical constraints. The authors emphasized that traditional centralized IDS approaches risk data leakage, high latency, and network bottlenecks, making them unsuitable for IoMT contexts. Their work evaluated the application of FL to collaboratively train intrusion detection models across distributed IoMT devices without exposing raw data. They showed that FL enhances privacy and scalability, while also aligning with healthcare data compliance requirements such as HIPAA and GDPR. However, the study identified several challenges unique to IoMT. First, the highly heterogeneous and non-IID nature of IoMT data degrades model performance in conventional FL frameworks. Second, communication overhead during global aggregation remains high, especially in bandwidth-limited networks. Finally, adversarial vulnerabilities, including model poisoning and data manipulation, threaten FL's reliability. To address these issues, the authors discussed possible solutions, such as clustering-based aggregation, weighted updates, and hybrid approaches that combine FL with blockchain for secure model sharing. Their findings positioned FL as a viable but still evolving approach for IoMT intrusion detection, requiring further research

into resilience, communication optimization, and adaptive personalization to meet the demands of real-world healthcare applications.

Zhang et al. [12] proposed a blockchain-enhanced federated learning (BFL) architecture to secure intrusion detection systems (IDS) in IoMT environments. The authors argued that while FL preserves privacy by keeping raw data local, it remains vulnerable to poisoning attacks, tampering during model updates, and trust issues in collaborative training. To address this, their approach integrated blockchain to provide immutability, transparency, and distributed trust in model aggregation. Each participating device recorded its model updates on the blockchain, ensuring that malicious or tampered updates could be detected and prevented. The authors demonstrated that this architecture improved resilience against poisoning and replay attacks, while maintaining privacy preservation. However, they also acknowledged critical trade-offs: blockchain introduces additional computational and storage overhead, increases latency, and may strain IoMT devices with limited resources. To mitigate this, the study suggested lightweight blockchain mechanisms and off-chain optimization strategies. Experimental results showed that BFL achieved higher security and trust compared to conventional FL, particularly in adversarial environments. Nevertheless, scalability and energy efficiency were noted as unresolved challenges. The study concluded that blockchain integration enhances the reliability of FL-based IDS frameworks in IoMT, but future research should focus on designing lightweight, resource-aware blockchain systems that are compatible with the constraints of medical IoT devices.

Lin et al. [13] focused on the development of lightweight anomaly-based intrusion detection systems (AIDS) tailored for deployment in IoMT environments, particularly at the perception layer where computational resources are severely constrained. The authors argued that traditional IDS frameworks, especially those relying on deep learning, often incur high latency and energy costs, making them unsuitable for direct use on IoMT devices such as wearables and sensors. Their approach emphasized the design of models with reduced computational complexity and memory usage, ensuring fast inference and minimal communication overhead while maintaining reliable detection accuracy. By employing simplified feature selection and model compression techniques, the proposed system was able to achieve real-time detection of anomalies with relatively low false positive rates. Experimental evaluations confirmed that the lightweight IDS performed effectively under constrained conditions, outperforming conventional IDS methods in terms of efficiency. However, the study also acknowledged limitations in adaptability to sophisticated and zero-day attacks, as lightweight architectures often trade accuracy for speed. The authors stressed that future research should focus on hybrid IDS models that integrate lightweight mechanisms with advanced anomaly detection techniques to balance efficiency and resilience. In the broader IoMT security landscape, this work demonstrated the importance of designing IDS solutions that are not only accurate but also optimized for the unique resource and latency constraints of medical devices.

Hussain et al. [14] presented a review of hybrid machine learning (ML) and deep learning (DL) frameworks for intrusion detection in IoMT, highlighting how combining multiple algorithms can improve accuracy, robustness, and adaptability in healthcare networks. The authors argued that standalone ML models such as decision trees or support vector machines are effective for structured data but struggle with complex and high-dimensional traffic patterns, while DL models like CNNs and LSTMs excel at feature extraction but are resource-intensive. Hybrid approaches, which integrate the strengths of both, were shown to deliver superior performance, particularly in detecting complex multi-vector cyberattacks. The review categorized existing hybrid IDS systems into ensemble-based methods, feature fusion techniques, and stacked architectures, each offering unique trade-offs between accuracy, interpretability, and computational cost. Results from surveyed studies demonstrated that hybrid IDS frameworks often outperform single-model approaches, achieving higher detection rates and robustness against zero-day threats. However, they also impose higher computational and energy requirements, making direct deployment on IoMT devices difficult. The authors highlighted that optimization strategies such as model pruning, edge–cloud collaboration, and federated learning can mitigate these issues. They concluded that hybrid ML-DL frameworks represent a promising direction for IoMT security but emphasized the need for energy-efficient, scalable, and privacy-preserving designs to ensure their practical adoption in healthcare environments.

Chen et al. [15] investigated the challenges of applying federated learning (FL) for intrusion detection in IoMT systems under non-independent and identically distributed (non-IID) data conditions. The authors explained that IoMT devices generate highly diverse data, including heterogeneous traffic patterns, varied biometric readings, and device-specific attack behaviors. Such diversity undermines the assumptions of conventional FL frameworks, which typically expect IID data for stable convergence and high accuracy. Their study evaluated how non-IID data leads to slower convergence, reduced detection accuracy, and vulnerability to adversarial manipulations. To address this, the authors proposed solutions such as clustering devices with similar data distributions, employing weighted aggregation schemes, and incorporating personalization layers to adapt models to specific devices. Experimental results demonstrated that these strategies mitigate the negative impact of data heterogeneity, improving both accuracy and stability in decentralized IDS systems. However, the paper acknowledged that these methods introduce additional communication and computation costs, which may not be suitable for resource-constrained IoMT devices. Furthermore, the scalability of such approaches in real-world deployments remains an open challenge. The authors concluded that tackling non-IID data is essential for making FL-based IDS viable in IoMT and called for future research into more efficient and adaptive aggregation techniques that balance robustness, scalability, and device limitations.

TABLE I: **COMPARISON TABLE**

Ref.	Description	Advantages	Disadvantages
[1]	A decentralized federated learning approach integrated with blockchain for intrusion detection in IoT, removing central server dependence and ensuring secure collaboration.	• Protects sensitive and private data • Removes single point of failure • Adds transparency using blockchain	• High communication overhead • Less effective in non-IID settings • Too heavy for small IoT devices
[2]	Random neural networks are used for intrusion detection in noisy IoT environments, acting as an alternative to deep models.	• Handles noisy and uncertain inputs • Low training cost • Scales to large systems	• Convergence can be unstable • Requires careful parameter tuning • Lower accuracy than CNN/LSTM
[3]	Prototype-based decentralized FL (ProtoDFL) aligns diverse client updates to improve intrusion detection across IoT.	• Cuts communication cost • Fast and stable convergence • Performs well in dynamic IoT	• Struggles with highly skewed data • Needs extra computation • Resource-heavy for weak devices
[4]	Blockchain-enhanced decentralized FL is introduced to improve trust and resilience in IDS frameworks.	• Provides auditable and transparent updates • Removes central bottlenecks • Increases IDS resilience	• High latency due to consensus • Energy and storage overhead • Not suitable for small IoMT nodes
[5]	Robust aggregation strategies in FL are explored to resist adversarial and poisoning attacks.	• Improves model reliability • More accurate under diverse data • Defends against malicious updates	• Slower convergence • Requires more communication • Higher computation cost
[6]	Swarm intelligence is combined with FL to improve cyber resilience in IoT IDS.	• Adapts to evolving threats • Strengthens robustness • Works in large IoT networks	• Computationally heavy • Latency during optimization • Sensitive to parameter settings
[7]	Communication-efficient decentralized FL is proposed to cut aggregation overhead while maintaining performance.	• Reduces bandwidth use • Faster convergence • Suitable for limited networks	• Still vulnerable to attacks • Complex aggregation steps • Accuracy trade-offs possible
Ref.	**Description**	**Advantages**	**Disadvantages**

[8]	A survey highlights IoMT attack types and defenses, focusing on lightweight cryptography and ML-based IDS.	• Provides structured attack taxonomy • Links ML with cryptographic methods • Practical guidance for IoMT security	• IDS can be heavy for IoMT • Limited zero-day protection • Poor scalability for large systems
[9]	A low-cost COVID-19 health monitoring system using Raspberry Pi, Node-Red, and ThingSpeak is proposed.	• Portable and cost-effective • Provides real-time monitoring • Easy to deploy with IoT kits	• Needs internet access • Privacy and security concerns • Limited scalability validation
[10]	A review of IoMT security combining ML, DL, FL, and blockchain for secure IDS and data sharing.	• Identifies key research areas • Highlights privacy and trust solutions • Broad coverage of technologies	• Computationally intensive • Non-IID issues unresolved • IDS lacks explainability
[11]	FL is applied to IoMT IDS to achieve privacy-preserving detection in distributed healthcare systems.	• Keeps patient data private • Distributes training tasks • Aligns with privacy regulations	• Accuracy falls in non-IID settings • Can be poisoned by attackers • High communication overhead
[12]	Blockchain-enhanced FL ensures tamper-resistant and trustworthy model aggregation.	• Immutable updates • Transparent aggregation • Improves trustworthiness	• Storage heavy • Energy and latency overhead • Poor scalability
[13]	A lightweight anomaly-based IDS designed for IoMT perception-layer devices.	• Detects anomalies in real time • Energy efficient • Works on constrained devices	• Limited accuracy • Weak against zero-day threats • Relies on simple features
[14]	Hybrid ML–DL frameworks are designed to capture complex intrusion behaviors.	• High detection accuracy • Robust against multiple attacks • Outperforms single models	• Computationally expensive • Energy demanding • Hard to deploy on IoMT
[15]	FL-based IDS enhanced with clustering and personalization for non-IID IoT data.	• Improves convergence on skewed data • Provides device-specific accuracy • Stable distributed performance	• High communication needs • Increased computation • Scalability issues

III. Conclusion

The reviewed studies collectively highlight that securing IoT and IoMT systems requires solutions that are lightweight, privacy-preserving, scalable, and resilient to diverse threats. Conventional intrusion detection methods, though useful in static settings, are insufficient for heterogeneous, resource-constrained devices that continuously generate sensitive data. This limitation has encouraged the design of anomaly-based and hybrid IDS frameworks that combine machine learning (ML) and deep learning (DL) to enhance adaptability and accuracy. While such methods improve detection rates and robustness, they are often computationally demanding and energy-intensive, restricting their use at the device level. To preserve privacy, federated learning (FL) has emerged as a promising paradigm, enabling collaborative model training without exposing raw data. However, its reliance on centralized aggregation introduces bottlenecks and vulnerabilities, motivating the adoption of decentralized FL (DFL) and blockchain-enhanced FL (BFL). These decentralized approaches enhance transparency, trust, and resilience but add significant communication, energy, and latency overhead. Another persistent challenge is the non-IID nature of IoT/IoMT data, which reduces model accuracy and complicates convergence. To mitigate this, researchers have proposed techniques such as prototype learning, weighted aggregation, clustering, personalization, and swarm optimization. These strategies improve performance but remain difficult to scale and costly for constrained devices. Moreover, adversarial robustness remains limited, as most IDS frameworks lack strong defenses against zero-day and adaptive attacks, even with blockchain or swarm enhancements. Overall, the literature shows a clear shift from traditional centralized models to federated, decentralized, and hybrid approaches that aim to balance privacy, efficiency, and detection capability. Yet, open gaps persist in designing IDS frameworks that are both secure and practical. Future efforts must focus on lightweight, adaptive, and attack-resilient IDS models that minimize communication costs, handle non-IID data effectively, and withstand adversarial manipulation, ensuring real-world viability in IoT and healthcare environments.

References

[1] M. Abdel-Basset, M. Elhoseny, S. Al-Otaibi, and M. H. Aly, "Decentralized federated learning for intrusion detection in iot-based systems: A review," *IEEE Access*, vol. 11, pp. 69 815–69 834, 2023.

[2] E. Gelenbe and Y. Yin, "Deep learning with random neural networks," *Cognitive Computation*, vol. 11, pp. 377–388, 2019.

[3] B. Li, W. Gao, J. Xie, M. Gong, L. Wang, and H. Li, "Prototype-based decentralized federated learning for the heterogeneous time-varying iot systems," *IEEE Internet of Things Journal*, vol. 11, no. 4, pp. 6916–6930, Feb. 2024.

[4] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019.

[5] H. Lee, M. Kim, and Y. D. Chung, "Privacy-preserving ecg data collection for arrhythmia classification," *Biomedical Signal Processing and Control*, vol. 112, p. 108374, 2026.

[6] W. Yamany, M. Keshk, N. Moustafa, and B. Turnbull, "Swarm optimization-based federated learning for the cyber resilience of internet of things systems against adversarial attacks," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1359–1374, Feb. 2024.

[7] S. Hameed, F. Najm, R. Kora, F. Fathy, and A. M. Mostafa, "Investigation of security attacks in iomt devices and countermeasures," *Computer Networks*, vol. 242, p. 110123, 2025.

[8] K. M. and T. Poongodi, "Investigation of security attacks in iomt devices and federated learning as a mitigation strategy," *Procedia Computer Science*, vol. 258, pp. 3426–3435, 2025.

[9] N. B. Kamarozaman and A. H. Awang, "Iot covid-19 portable health monitoring system using raspberry pi, node-red and thingspeak," in *2021 IEEE Symposium on Wireless Technology & Applications (ISWTA)*. IEEE, 2021, pp. 107–112.

[10] S. Alghamdi, M. Ilyas, A. Anjum, T. Abuhmed, N. Alghamdi, Y. Maleh, and E. Benkhelifa, "Anomaly-based intrusion detection for iomt networks: Design, implementation, dataset generation, and ml algorithms evaluation," *IEEE Transactions on Industrial Informatics*, vol. 21, no. 1, pp. 100–111, 2025.

[11] Y. K. Saheed and M. O. Arowolo, "Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms," *IEEE Access*, vol. 9, pp. 161 546–161 552, 2021.

[12] M. Fahim-Ul-Islam, A. Chakrabarty, M. G. R. Alam, and S. S. B. Maidin, "A resource-efficient federated learning framework for intrusion detection in iomt networks," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 4508–4520, May 2025.

[13] S. Alotaibi, F. Alhaidari, F. Alsolami, M. Imran, and N. Akhtar, "Blockchain-based secure data sharing framework for iomt," *Procedia Computer Science*, vol. 218, pp. 2198–2205, 2025.

[14] R. Myrzashova, S. H. Alsamhi, A. Hawbani, E. Curry, M. Guizani, and X. Wei, "Safeguarding patient data-sharing: Blockchain-enabled federated learning in medical diagnostics," *IEEE Transactions on Sustainable Computing*, vol. 10, no. 1, pp. 176–190, 2025.

[15] S. H. A. Kazmi, K. Nisar, R. Hassan, D. P. Dahnil, and F. Qamar, "Threat intelligence in iomts with federated learning using non-iid data: An experimental analysis," in *2024 IEEE 7th International Symposium on Telecommunication Technologies (ISTT)*. IEEE, 2024, pp. 120–126.