IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Comprehensive Review of Machine Learning and Deep Learning Approaches for Medical IOT and Threat Detection

Suman Kumari
Student- M Tech, 4th Semester
Branch- CSE
Lakshmi Narain College of Technology,
Kalchuri nagar, Raisen Road Bhopal, India .

Anju Singh
Professor
Department of CSE
Lakshmi Narain College of Technology,
Kalchuri nagar, Raisen Road Bhopal, India.

***Abstract*—** The increasing reliance on Medical Internet of Things (MIoT) devices for patient monitoring and healthcare delivery has introduced significant security challenges, necessitating advanced threat detection mechanisms. This review provides a comprehensive analysis of deep learning approaches for MIoT threat detection, while also considering complementary techniques such as machine learning, anomaly detection, blockchain-based security, hybrid models, and cloud–edge integration. Traditional machine learning methods like SVM, Decision Trees, Random Forests, and k-NN are effective for structured data but struggle with complex healthcare datasets, whereas deep learning models such as CNNs, RNNs, and LSTMs excel in feature extraction and sequential data analysis, achieving higher accuracy in detecting malicious activities. Anomaly detection techniques, including autoencoders and clustering methods, offer the ability to identify zero-day attacks but often suffer from false-positive rates. Blockchain integration enhances trust, transparency, and data integrity, though at the cost of latency and energy efficiency. Hybrid frameworks that combine ML/DL with anomaly detection or blockchain provide a balanced approach to security, and cloud–edge computing synergy further improves scalability and real-time responsiveness. Collectively, these approaches highlight the growing importance of deep learning in enabling secure, reliable, and intelligent threat detection in Medical IoT environments.

Keywords— MIoT, Deep Learning, Accuracy, Security.

I. INTRODUCTION

The rapid evolution of the Internet of Things (IoT) has revolutionized the healthcare sector, giving rise to what is widely referred to as the Medical Internet of Things (MIoT). By interconnecting a wide range of medical devices, sensors, applications, and cloud-based platforms, MIoT enables seamless patient monitoring, accurate diagnostics, efficient treatment, and real-time data-driven decision-making [1]. Devices such as wearable heart rate monitors, glucose sensors, implantable pacemakers, infusion pumps, and even connected hospital infrastructure systems are now integrated into a digital healthcare ecosystem. This integration not only enhances medical outcomes but also promotes accessibility, efficiency, and cost-effectiveness in healthcare delivery[2].

However, as with any connected digital infrastructure, MIoT faces critical cybersecurity challenges. The sensitive nature of medical data and the life-critical functions of healthcare devices make them prime targets for cyberattacks[3]. A successful breach can result in unauthorized access to confidential patient records, manipulation of medical devices, interruption of healthcare services, or even direct harm to patients. Unlike traditional IT systems, where downtime may cause financial loss, the stakes in MIoT are significantly higher, as compromised devices can put human lives at risk[4].

The threat landscape in Medical IoT is broad and continually expanding. Attackers exploit vulnerabilities such as weak authentication mechanisms, outdated firmware, insecure communication channels, and inadequate encryption practices[5]. Threats may range from simple data theft and ransomware attacks to highly sophisticated exploits like device hijacking, distributed denial of service (DDoS), or malicious tampering with real-time medical signals. Moreover, the interconnected nature of MIoT means that a single compromised device can serve as an entry point to an entire healthcare network, amplifying the severity of cyber risks[6].

An additional layer of complexity arises from the resource constraints of medical IoT devices. Many of these devices have limited computing power, storage, and energy capacity, making it difficult to implement traditional heavyweight security solutions[7]. At the same time, regulatory compliance requirements—such as HIPAA (Health Insurance Portability and Accountability Act) in the United States or GDPR (General Data Protection Regulation) in Europe—demand strict protection of medical data privacy and integrity. These constraints highlight the urgent need for specialized threat detection mechanisms tailored to the healthcare domain[8].

Medical IoT threat detection involves the application of advanced techniques to monitor, analyze, and identify malicious activities within healthcare networks and connected devices[9]. Unlike preventive security measures that focus on building barriers, threat detection emphasizes real-time identification of anomalies, suspicious behaviors, or intrusions before they escalate into critical security breaches. Modern approaches employ a variety of strategies, including machine learning, deep learning, artificial intelligence (AI), blockchain-based verification, and anomaly detection algorithms. These methods help differentiate between normal operational patterns and potentially harmful activities, ensuring proactive responses to cyber risks[10].

The significance of medical IoT threat detection extends beyond data confidentiality to patient safety, healthcare trust, and system resilience. With the increasing adoption of remote patient monitoring, telemedicine, and smart hospitals, the volume of medical data transmitted over wireless networks has surged. As a result, cybercriminals gain more opportunities to launch sophisticated attacks. Timely detection mechanisms not only protect patients but also help maintain the integrity of the healthcare infrastructure, thereby fostering confidence among practitioners, patients, and regulatory authorities[11].

The growing dependency on Medical IoT highlights both immense opportunities and pressing challenges. While these technologies have transformed healthcare by enabling connected and intelligent care delivery, they also open the door to new categories of threats. Therefore, developing robust and efficient Medical IoT threat detection frameworks is not just a technological necessity but also a moral and ethical responsibility to ensure the safety and well-being of patients in an increasingly digital healthcare environment[12].

II. BACKGROUND

The A. K. Kumar et al., [1] proposed an enhanced hybrid deep learning approach for botnet detection in IoT environments. Their framework combined CNN and LSTM networks to capture both spatial and temporal dependencies in traffic patterns. The method was evaluated on benchmark IoT datasets and showed improved accuracy and reduced false-positive rates compared to traditional ML models. The hybrid approach demonstrated robustness against complex and evolving IoT botnet attacks, making it suitable for real-time detection. However, scalability to resource-constrained IoT devices remains a challenge.

M. Alshehri et al., [2] developed SkipGateNet, a lightweight hybrid CNN-LSTM model with learnable skip connections for efficient botnet attack detection in IoT systems. The skip connections helped in preserving crucial features while reducing computational overhead. Experimental analysis highlighted that SkipGateNet achieved high detection accuracy with lower latency, making it adaptable to real-time IoT scenarios. The proposed method outperformed existing models in terms of precision and recall while

maintaining computational efficiency. This makes it suitable for practical deployment in IoT networks with limited resources.

M. Al-Fawa'reh et al., [3] introduced MalbotDRL, a malware botnet detection framework using deep reinforcement learning (DRL) in IoT networks. Unlike supervised approaches, MalbotDRL continuously learns and adapts to new threat behaviors without requiring large labeled datasets. The model demonstrated superior detection performance across multiple datasets by dynamically adjusting detection policies. Their work highlighted the importance of reinforcement learning in evolving IoT security landscapes. However, the training process is computationally intensive, raising concerns for large-scale deployment.

R. Kalakoti et al., [4] explored IoT botnet detection using explainable AI (XAI) to enhance transparency and trust in security systems. Their study quantitatively evaluated the explainability of different AI models and demonstrated how interpretable frameworks can help security experts understand decision-making in botnet detection. The integration of explainability improved stakeholder confidence in automated security decisions. Although effective, balancing model accuracy and interpretability remains an open challenge in XAI-based IoT security solutions.

X. Yan et al., [5] presented a domain embedding model integrated with blockchain technology for botnet detection in IoT networks. Their framework leveraged smart blockchain mechanisms to ensure secure, tamper-proof feature extraction and classification processes. The proposed approach enhanced detection accuracy while ensuring decentralized security management. This integration also provided resistance against data manipulation attacks. While innovative, blockchain adoption raises concerns related to high computational costs and energy consumption in IoT environments.

S. Saravanan and U. M. Balasubramanian [6] proposed an adaptive scalable data pipeline for multiclass attack classification in large-scale IoT networks. Their system was designed to handle massive amounts of IoT traffic data while ensuring real-time processing and classification. The pipeline demonstrated strong scalability and efficiency in detecting multiple types of IoT attacks simultaneously. Experimental validation showed superior performance compared to existing systems, making it well-suited for complex IoT infrastructures. However, deployment in highly resource-constrained IoT devices remains a limitation.

P. V. Dinh et al., [7] proposed a constrained twin variational auto-encoder (CT-VAE) model for intrusion detection in IoT systems. The twin architecture enabled the system to effectively capture hidden representations of normal and malicious traffic while reducing reconstruction errors. Their experiments demonstrated superior performance compared to traditional autoencoders, particularly in detecting sophisticated and low-frequency attacks. The model also proved effective in handling imbalanced datasets, which is a common issue in intrusion detection. However, the computational requirements of the CT-VAE may limit its deployment on highly resource-constrained IoT devices.

J. Kabdjou and N. Shinomiya [8] introduced a cyber-deception based architecture for improving Quality of Service (QoS) and detecting HTTPS DDoS attacks in Mobile Edge Computing (MEC) environments. Their model leveraged decoy mechanisms to mislead attackers while simultaneously collecting useful information about malicious behaviors. Experimental results showed significant improvements in detecting encrypted DDoS traffic without compromising QoS in edge networks. The proposed approach enhanced resilience against large-scale attacks, but scalability and adaptability across different IoT domains remain open challenges.

A. A. Mohammed and A. A. Ibrahim [9] explored malware detection in Ad-hoc E-Government networks using machine learning techniques. Their approach applied classification models to identify malware in decentralized and dynamic government communication infrastructures. The study demonstrated that ML models could detect malicious traffic patterns effectively, thereby improving network resilience against cyber threats. The proposed framework provided an efficient solution for governmental IoT deployments where data integrity and availability are critical. However, the work did not extensively address zero-day attack detection or real-time adaptability.

T. Hasan et al., [10] presented a hybrid deep learning model for securing Industrial IoT (IIoT) systems against botnet attacks. Their architecture combined CNNs and RNNs to capture both spatial and sequential dependencies in IIoT traffic data. Results indicated significant improvements in detection accuracy, recall, and F1-score compared to conventional ML models. The proposed solution addressed large-scale industrial

IoT vulnerabilities where botnets can cause severe disruptions in production. While effective, the approach required high computational resources, making it less suitable for lightweight industrial IoT devices.

P. Saxena and R. B. Patel [11] developed an efficient hybrid machine learning model for IoT botnet detection. Their method combined supervised learning classifiers with feature engineering techniques to improve detection precision. The framework achieved enhanced detection performance across diverse IoT traffic datasets while maintaining low false-positive rates. The hybrid approach demonstrated practical utility for scalable IoT deployments. Nevertheless, its reliance on labeled datasets limits adaptability to unknown attack types and dynamic IoT environments.

F. Sattari et al., [12] proposed a hybrid deep learning approach for bottleneck detection in IoT networks. Their model integrated CNNs and LSTMs to identify congestion and malicious traffic that could degrade IoT performance. The proposed approach achieved high detection accuracy in identifying both security threats and network performance bottlenecks. By addressing performance and security jointly, the method offered a holistic solution for IoT systems. However, computational efficiency and real-time adaptability in large-scale networks remain areas for further research.

Review of State-of-the-Art Techniques

2.1 Machine Learning–based Techniques

Machine learning (ML) has emerged as a cornerstone in healthcare IoT security, offering automated methods to detect anomalies and potential cyber threats. ML algorithms such as Decision Trees, Random Forests, Support Vector Machines (SVM), and K-Nearest Neighbors (KNN) are commonly applied to analyze large-scale medical data and identify unusual patterns that may indicate attacks. These methods can handle high-dimensional data from wearable devices, sensors, and hospital networks to predict intrusions or failures.

In addition to classical algorithms, deep learning (DL) models like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have been increasingly adopted for their capability to process complex, sequential, and temporal data in IoT networks. CNNs are particularly effective in recognizing spatial patterns in imaging or sensor data, while RNNs and Long Short-Term Memory (LSTM) networks excel in capturing temporal dependencies in time-series health signals. These models enhance predictive accuracy and allow real-time threat detection.

Despite their effectiveness, ML-based techniques face challenges in IoMT environments. Issues such as imbalanced datasets, noisy data, and heterogeneous device communication can reduce detection accuracy. Moreover, many ML models require centralized processing, which may introduce latency and privacy concerns. Consequently, ongoing research focuses on optimizing ML models for distributed, lightweight, and privacy-preserving IoT applications in healthcare.

2.2 Blockchain-enabled Healthcare Data Systems

Blockchain technology offers a decentralized and secure approach to managing healthcare data, addressing concerns related to privacy, tampering, and unauthorized access. By leveraging distributed ledger technology, blockchain ensures that every transaction or data entry is immutable and traceable. In medical IoT systems, this allows secure storage of patient records, device logs, and sensor data without relying on a centralized authority, reducing the risk of data breaches.

Smart contracts, a key feature of blockchain, automate verification and authentication processes within healthcare networks. For instance, access permissions, data sharing between hospitals, and logging of IoT device activity can be handled automatically, ensuring compliance with regulations like HIPAA. Blockchain also facilitates secure audit trails, enabling healthcare providers to track data access and modifications in real time.

However, blockchain implementation in IoMT faces challenges related to scalability, latency, and energy consumption. Consensus mechanisms like Proof-of-Work (PoW) or Proof-of-Stake (PoS) can introduce delays that are critical in real-time medical applications. Hybrid approaches combining blockchain with edge computing or cloud integration are being explored to overcome these limitations while maintaining data integrity, security, and accessibility.

2.3 Hybrid AI–Blockchain Approaches

Hybrid AI–Blockchain approaches combine the predictive power of artificial intelligence with the security features of blockchain to provide robust healthcare IoT solutions. In such systems, AI models analyze incoming medical data for anomalies or predictive insights, while blockchain ensures secure, immutable storage of the processed data. This integration enhances trust in the data, enabling accurate decision-making without compromising patient privacy.

For example, AI can detect irregularities in patient vitals collected from wearable sensors and automatically trigger alerts or interventions. Blockchain simultaneously records these events in a decentralized ledger, ensuring transparency and tamper-proof logging. This combination also supports collaborative healthcare, where multiple institutions can share insights without compromising sensitive patient information.

Despite its potential, hybrid AI–Blockchain systems must address issues of computational overhead, latency, and interoperability. Training AI models on encrypted or distributed datasets can be resource-intensive, and integrating blockchain with real-time IoT systems requires efficient communication protocols. Current research emphasizes lightweight blockchain frameworks, federated learning, and edge-based AI processing to mitigate these challenges.

2.4 Comparative Analysis of Techniques

Machine learning, blockchain, and hybrid AI–Blockchain approaches each offer unique benefits and trade-offs in healthcare IoT security. ML-based techniques excel in anomaly detection and predictive analytics but often struggle with privacy, centralized processing, and heterogeneous IoT environments. Blockchain provides robust data integrity and privacy but can be limited by latency and computational demands.

Hybrid AI–Blockchain systems aim to combine the strengths of both approaches, offering predictive capabilities alongside secure, tamper-proof storage. These systems are particularly useful for collaborative healthcare networks, IoMT devices, and sensitive medical records. However, they require careful optimization to balance computational efficiency, real-time performance, and scalability.

Overall, comparative studies suggest that no single technique suffices for all IoMT security challenges. The choice of approach depends on factors such as the application scenario, data sensitivity, device capabilities, and latency requirements. Future research is focusing on adaptive, lightweight, and scalable frameworks that integrate AI and blockchain to provide comprehensive, real-time threat detection in healthcare IoT environments.

Table 1: Summary

Re. No.	Author (Year)	Work	Method	Outcome
1	A. K. Kumar et al. (2024)	Enhanced Hybrid Deep Learning Approach for Botnet Attacks Detection in IoT Environment	Hybrid deep learning combining CNN and RNN layers	Achieved higher detection accuracy and reduced false alarms for IoT botnet detection
2	M. Alshehri et al. (2024)	SkipGateNet: A Lightweight CNN-LSTM Hybrid Model with Learnable Skip Connections	CNN-LSTM hybrid with skip connections	Provided efficient botnet attack detection with lightweight model suitable for IoT devices
3	M. Al-Fawa'reh et al. (2023)	MalbotDRL: Malware Botnet Detection using Deep Reinforcement Learning in IoT Networks	Deep Reinforcement Learning (DRL)	Demonstrated adaptive learning to evolving threats, improving detection over static models
4	R. Kalakoti et al. (2024)	Improving IoT Security with Explainable AI: Quantitative Evaluation of Explainability for IoT Botnet Detection	Explainable AI with quantitative metrics	Enhanced transparency in model decisions, balancing detection accuracy with

				interpretability
5	X. Yan et al. (2024)	A Domain Embedding Model for Botnet Detection Based on Smart Blockchain	Domain embedding + blockchain integration	Strengthened trust and decentralization in botnet detection with improved scalability
6	S. Saravanan et al. (2024)	Adaptive Scalable Data Pipeline for Multiclass Attack Classification in Large-Scale IoT Networks	Scalable data pipeline with ML classifiers	Enabled efficient multiclass attack detection in large-scale IoT networks with reduced latency
7	P.V. Dinh et al. (2024)	Constrained Twin Variational Auto-Encoder for Intrusion Detection in IoT Systems	Variational Auto-Encoder (VAE)	Improved intrusion detection accuracy with constrained twin architecture on IoT datasets
8	J. Kabdjou et al. (2024)	Improving QoS and HTTPS DDoS Detection in MEC Environment with Cyber-Deception Based Architecture	Cyber-deception based MEC architecture	Enhanced QoS and successfully mitigated HTTPS DDoS attacks in IoT-MEC environments
9	A.A. Mohammed et al. (2024)	Malware Detection in Adhoc E-Government Network using Machine Learning	ML-based classification algorithms	Achieved reliable malware detection in e-Government Adhoc networks with low resource use
10	T. Hasan et al. (2022)	Securing Industrial IoT Against Botnet Attacks Using Hybrid Deep Learning Approach	Hybrid CNN-LSTM deep learning model	Secured Industrial IoT by detecting botnet attacks with high precision and robustness
11	P. Saxena et al. (2024)	Efficient Hybrid Model for Botnet Detection using Machine Learning	Hybrid machine learning classifiers	Improved detection speed and accuracy in IoT environments with computational efficiency
12	F. Sattari et al. (2023)	Hybrid Deep Learning Approach for Bottleneck Detection in IoT	Hybrid deep learning framework	Enhanced detection of IoT bottlenecks and reduced misclassification rate

III. CHALLENGES

The rapid integration of IoT in healthcare has brought significant benefits, but it also introduces a wide range of challenges that complicate the detection and prevention of security threats. One of the primary challenges is device heterogeneity. Medical IoT systems consist of a diverse range of devices such as wearable sensors, infusion pumps, imaging equipment, and cloud-based monitoring platforms. Each of these devices may have different hardware configurations, operating systems, and communication protocols. This diversity makes it difficult to design a single security framework that is compatible with all devices.

Another major challenge is resource constraints. Many IoMT devices have limited processing power, memory, and battery life, making it impractical to implement complex security algorithms or real-time threat detection techniques. Deploying deep learning models, which often require significant computational resources, becomes particularly challenging in such constrained environments. Lightweight models may help but often compromise on detection accuracy.

Data security and privacy present additional obstacles. Medical IoT devices constantly collect sensitive patient data, including personal health records, biosignals, and real-time monitoring information. Any security breach could lead not only to unauthorized access but also to the misuse of critical patient information. Ensuring compliance with regulations such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation) adds another layer of complexity in designing secure IoMT systems.

Another critical challenge is real-time threat detection. In healthcare, even a slight delay in detecting or responding to a security threat could endanger patient lives. Designing systems that can perform efficient, accurate, and timely detection while balancing computational overhead is extremely difficult. Furthermore, the dynamic and evolving nature of cyber threats poses continuous difficulties. Attackers constantly develop new methods such as zero-day attacks, ransomware, and adversarial attacks that exploit vulnerabilities in IoMT systems. This makes it necessary to update security models frequently, which is not always feasible in healthcare infrastructure.

Finally, lack of standardized security frameworks and interoperability issues create further challenges. Different manufacturers develop IoMT devices with proprietary technologies, resulting in compatibility issues when integrating security solutions across systems. Without standardization, it becomes difficult to implement a unified and scalable threat detection approach.

The challenges in Medical IoT threat detection lie at the intersection of technical, regulatory, and operational concerns. Overcoming these challenges requires the development of lightweight yet powerful deep learning models, real-time detection mechanisms, standardized security frameworks, and privacy-preserving techniques that safeguard sensitive health data while ensuring system efficiency.

IV. CONCLUSION

Medical IoT is transforming healthcare through continuous monitoring and personalized care, but it also introduces serious security risks that can compromise patient safety and data privacy. Deep learning offers powerful capabilities for detecting anomalies and mitigating advanced threats, yet challenges such as limited device resources, absence of standards, and constantly evolving attacks still hinder real-world adoption. To build a secure and reliable IoMT ecosystem, future research must emphasize lightweight, explainable, and scalable deep learning models. Strengthening these areas will ensure better protection of sensitive health information and support safe, trustworthy medical IoT systems in the digital era.

REFERENCES

1. A. K. Kumar et al., "Enhanced Hybrid Deep Learning Approach for Botnet Attacks Detection in IoT Environment," 2024 7th International Conference on Signal Processing and Information Security (ICSPIS), Dubai, United Arab Emirates, 2024, pp. 1-6, doi: 10.1109/ICSPIS63676.2024.10812621.
2. M. Alshehri J. Ahmad, S. Almakdi, M. Qathrady, Y. Ghadi and w. Buchanan, “SkipGateNet: A Lightweight CNN-LSTM hybrid model with learnable skip connections for efficient botnet attack detection in IoT,” IEEE Access, vol. 12, pp. 35521–35538, March 2024 https://doi.org/10.1109/access 3371992.
3. M. Al-Fawa’reh, J. Abu-Khalaf, P. Szewczyk, and J.J Kang, MalbotDRL: Malware botnet detection using deep reinforcement learning in IOT Networks. IEEE Internet of Things Journal, vol. 11, no. 6, pp. 9610–9629, October 2023, https://doi.org/10.1109/jiot.2023.3324053
4. R. Kalakoti, H. Bahsi, and S. No mm (2024). Improving IOT security with explainable AI: Quantitative evaluation of explainability for IOT botnet detection. IEEE Internet of Things Journal, vol. 11, no. 10, pp. 18237–18254. January 2024, https://doi.org/10.1109/jiot.2024.3360626
5. X. Yan, X. Yu, S. Yao, and Y. Sun (2024). A domain embedding model for botnet detection based on Smart Blockchain. IEEE Internet of Things Journal, vol. 11, no. 5, pp. 8005–8018, February 2024, https://doi.org/10.1109/jiot.2023.3320046
6. S. Saravanan, and U.M. Balasubramanian, “An adaptive scalable data pipeline for multiclass attack classification in large-scale IOT Networks ”. Big Data Mining and Analytics, vol. 7, no. 2, pp. 500–511, April 2024, https://doi.org/10.26599/bdma.2023.9020027
7. P.V. Dinh, Q.U. Nguyen, D.T Hoang, D.N. Nguyen, S.P. Bao and E. Dutkiewicz, “Constrained twin variational auto-encoder for intrusion detection in IOT Systems ”. IEEE Internet of Things Journal, vol. 11, no. 8, pp. 14789–14803,2024, https://doi.org/10.1109/jiot.2023.3344842

8. J. Kabdjou, and N. Shinomiya, “Improving quality of service and HTTPS DDoS detection in MEC environment with a cyber-deception based architecture,” IEEE Access, vol. 12, pp. 23490–23503,2024, https://doi.org/10.1109/access.2024.3361476
9. A.A. Mohammed, and A.A. Ibrahim, “Malware detection in Adhoc EGovernment Network using machine learning,” 5 th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 20 24, https://doi.org/10.1109/hora58378.2023.10156724
10. T. Hasan, J. Malik, I. Bibi, W.U. Khan, F. N. Al-Wesabi, K. Dev and G. Huang, “Securing Industrial Internet of Things Against botnet attacks using hybrid deep learning approach,” IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, pp. 2952–2963, April 2022, https://doi.org/10.1109/tnse.2022.3168533
11. P. Saxena, and R.B. Patel, “Efficient hybrid model for botnet detection using machine learning,” 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM), 2024, https://doi.org/10.1109/iccakm58659.2023.10449643
12. F. Sattari, A.H. Farooqi, Z. Qadir, B. Raza, H. Nazari and M. Almutiry. A hybrid deep learning approach for bottleneck detection in IOT. IEEE Access, vol. 10, pp. 77039–77053,2023, https://doi.org/10.1109/access.2022.