MIJRD Multidisciplinary International Journal of Research and Development

Volume: 05 / Issue: 04 / 2026 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

Privacy-Preserving Federated Transformer for IoT Anomaly Detection

Henal Patel

Department of Computer Science & Engineering

Uka Tarsadia University, India

Abstract— The rapid expansion of the Internet of Things (IoT) has significantly transformed modern digital infrastructures by enabling seamless communication among interconnected devices. However, this growth has also introduced serious security challenges, particularly in the form of cyberattacks, data breaches, and anomalous activities within IoT networks. Anomaly detection has emerged as a critical approach for identifying such threats by analyzing patterns and deviations in network behavior.

This review paper provides a comprehensive analysis of existing anomaly detection techniques in IoT systems, focusing on machine learning, deep learning, and hybrid approaches. It examines the evolution of traditional methods toward advanced intelligent models capable of handling large-scale and dynamic IoT environments. The study also explores emerging technologies such as federated learning, blockchain integration, and edge–cloud architectures, which enhance privacy, scalability, and real-time processing capabilities.

Furthermore, the paper identifies key challenges, including data heterogeneity, resource constraints, lack of standardized datasets, and limited model interpretability. A critical comparison of different methodologies is presented to highlight their strengths and limitations. Based on the analysis, the review emphasizes the importance of integrated and lightweight frameworks that balance accuracy, efficiency, and security.

Finally, future research directions are proposed, focusing on adaptive learning models, privacy-preserving mechanisms, and cross-domain applicability. This work aims to serve as a valuable reference for researchers and practitioners seeking to develop robust and scalable anomaly detection systems in IoT environments.

Keywords— IoT Security, Anomaly Detection, Machine Learning, Deep Learning, Federated Learning, Blockchain, Edge Computing, Cybersecurity.

1. INTRODUCTION

Background / Context

The rapid growth of the Internet of Things (IoT) has transformed modern digital ecosystems by enabling interconnected devices to communicate, collect, and exchange data in real time. IoT applications are widely used in domains such as smart homes, healthcare, industrial automation, and smart cities, making them a critical component of contemporary technology infrastructures [1]–[4]. However, the increasing number of connected devices has also expanded the attack surface, exposing IoT systems to various cyber threats, including intrusion attacks, malware, and data breaches [5]–[8].

Anomaly detection has emerged as a crucial technique for identifying abnormal patterns in IoT network behavior that may indicate potential security threats. Traditional rule-based systems are often insufficient due to the dynamic and heterogeneous nature of IoT environments [9]–[12]. As a result, machine learning and deep learning approaches have gained significant attention for their ability to automatically learn patterns and detect anomalies with higher accuracy [13]–[16].

Recent advancements have introduced sophisticated techniques such as federated learning, blockchain-based security mechanisms, and edge intelligence to enhance privacy and real-time detection capabilities in IoT systems [17]–[20]. Additionally, explainable artificial intelligence (XAI) has been integrated into anomaly detection models to improve transparency and trust in decision-making processes [21]–[23].

Despite these advancements, challenges such as resource constraints, data heterogeneity, scalability, and lack of standardized datasets continue to hinder the effective deployment of anomaly detection systems in IoT environments [24]–[27].

Earlier foundational studies laid the groundwork for anomaly detection and IoT security by exploring network behavior analysis, intrusion detection techniques, and machine learning-based approaches [28]–[32]. These contributions have been instrumental in shaping current research trends and highlighting the importance of robust and scalable anomaly detection frameworks.

Furthermore, surveys and conceptual studies have provided insights into the evolution, architecture, and challenges of IoT systems, emphasizing the need for advanced security solutions [33]–[35].

Rationale / Objectives

With the exponential growth of IoT devices and the increasing sophistication of cyberattacks, there is a pressing need to develop efficient and scalable anomaly detection techniques tailored for IoT environments. Although numerous studies have proposed various machine learning and deep learning models, there is still a lack of comprehensive understanding regarding their effectiveness, limitations, and applicability in real-world scenarios [1]–[10].

The primary objective of this review is to systematically analyze existing anomaly detection techniques in IoT systems, focusing on their methodologies, performance, and security implications. This review aims to answer the following research questions:

- What are the most effective machine learning and deep learning techniques for IoT anomaly detection?
- How do emerging technologies such as federated learning and blockchain enhance security and privacy?
- What are the key challenges and limitations in current anomaly detection approaches?
- What future directions can improve the robustness and scalability of IoT security systems?

By addressing these questions, this study seeks to provide a comprehensive understanding of the current state of research and identify potential areas for improvement [11]–[20].

Volume: 05 / Issue: 04 / 2026 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

Scope of the Review

This review focuses on anomaly detection techniques applied to IoT environments, particularly those leveraging machine learning, deep learning, and hybrid approaches. It includes studies related to intrusion detection, cyberattack detection, and behavior analysis in IoT networks [21]–[25].

The scope of this review covers:

- Machine learning and deep learning-based anomaly detection models
- Federated learning and blockchain-based security approaches
- Edge and cloud-based IoT architectures
- Explainable AI techniques for improving model transparency

However, this review excludes:

- Non-IoT-specific anomaly detection systems
- Purely hardware-based security mechanisms
- Studies without experimental validation or practical implementation

The selected references span from foundational research to recent advancements, providing a comprehensive overview of the evolution of anomaly detection techniques in IoT systems [26]–[35].

2. METHODOLOGY / SEARCH STRATEGY

Databases / Search Terms

A systematic search strategy was adopted to identify relevant literature on anomaly detection in IoT environments. Multiple well-known academic databases and digital libraries were used to ensure comprehensive coverage of high-quality research articles. These databases include IEEE Xplore, Scopus, ScienceDirect, SpringerLink, and Google Scholar, which are widely recognized for indexing peer-reviewed journals and conference proceedings in the fields of computer science, cybersecurity, and IoT research [1]–[5].

To retrieve relevant studies, a combination of keywords and Boolean operators was employed. The primary search terms included:

- “IoT anomaly detection”
- “intrusion detection in IoT”
- “machine learning for IoT security”
- “deep learning anomaly detection IoT”
- “federated learning IoT security”
- “blockchain-based IoT security”
- “edge computing anomaly detection”

These keywords were combined using Boolean operators such as AND, OR, and NOT to refine the search results and improve relevance. For example, queries such as “IoT anomaly detection AND deep learning” and “IoT security AND blockchain AND federated learning” were used to capture recent advancements in the field [6]–[10].

Volume: 05 / Issue: 04 / 2026 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

Additionally, backward and forward citation tracking techniques were applied to identify influential studies and ensure that no significant contributions were overlooked. This approach helped in capturing both foundational research and recent developments in IoT anomaly detection [11]–[15].

Inclusion / Exclusion Criteria

To ensure the quality and relevance of the selected studies, specific inclusion and exclusion criteria were defined.

Inclusion Criteria

The following criteria were used to include studies in this review:

- Peer-reviewed journal articles and conference papers
- Studies focusing on IoT anomaly detection, intrusion detection, or cybersecurity
- Research utilizing machine learning, deep learning, or hybrid approaches
- Papers published between 2010 and 2025 to cover both foundational and recent advancements
- Articles written in the English language
- Studies with experimental validation, datasets, or real-world applications

These criteria ensured that the selected literature provides both theoretical insights and practical implementations relevant to IoT security [16]–[22].

Exclusion Criteria

The following types of studies were excluded:

- Articles not related to IoT or anomaly detection
- Studies focusing only on traditional networks without IoT context
- Non-peer-reviewed content such as blogs, tutorials, and opinion articles
- Papers lacking sufficient methodological details or experimental evaluation
- Duplicate studies across multiple databases

This filtering process helped eliminate irrelevant and low-quality studies, ensuring the reliability and credibility of the review [23]–[28].

After applying these criteria, a final set of 35 relevant studies was selected for detailed analysis. These studies include foundational works on IoT architecture and anomaly detection, as well as recent advancements involving federated learning, blockchain integration, and explainable AI techniques [29]–[35].

3. MAIN BODY

Machine Learning and Deep Learning-Based Anomaly Detection

Overview and Current Findings

Machine learning (ML) and deep learning (DL) techniques have become the foundation of modern IoT anomaly detection systems. Early approaches primarily relied on supervised learning algorithms such as Support Vector

Volume: 05 / Issue: 04 / 2026 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

Machines (SVM), Decision Trees, and Random Forests to classify normal and abnormal network behavior [1]–[5]. However, these approaches required labeled datasets, which are often scarce in IoT environments.

To address this limitation, researchers have explored unsupervised and semi-supervised learning methods such as autoencoders and clustering algorithms. These models can detect anomalies without requiring labeled data, making them suitable for dynamic IoT scenarios [6]–[10].

Recent advancements have introduced deep neural networks, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Graph Neural Networks (GNNs), which provide improved accuracy by capturing complex temporal and spatial patterns in IoT data [11]–[15].

Critical Analysis and Comparison

While ML/DL models demonstrate high detection accuracy, they also present several challenges. Supervised models suffer from overfitting and poor generalization in unseen environments, whereas unsupervised models may produce higher false-positive rates [16]–[18]. Deep learning models, although powerful, require significant computational resources, making them less suitable for resource-constrained IoT devices [19]–[20].

Federated Learning and Blockchain-Based Approaches

Overview and Current Findings

Federated learning (FL) has emerged as a promising approach for privacy-preserving anomaly detection by enabling decentralized model training without sharing raw data. This is particularly useful in IoT environments where data privacy is critical [21]–[23]. Additionally, blockchain technology has been integrated with FL to ensure secure data sharing, integrity, and trust among distributed IoT devices [24]–[26].

Recent studies propose hybrid frameworks combining FL and blockchain to enhance both privacy and security. These approaches reduce the risk of data leakage while maintaining high detection accuracy [27]–[28].

Methodological Differences and Contradictions

Despite their advantages, FL-based models face challenges such as communication overhead, non-IID data distribution, and synchronization issues across devices. Similarly, blockchain integration introduces latency and scalability concerns due to consensus mechanisms [29]–[30]. Some studies report improved security but at the cost of increased computational complexity, highlighting a trade-off between efficiency and robustness.

Edge–Cloud and Hybrid Architectures

Overview and Current Findings

Edge computing has gained popularity as a solution to reduce latency and enable real-time anomaly detection in IoT systems. By processing data closer to the source, edge-based models minimize response time and bandwidth usage [31]–[32]. Hybrid edge–cloud architectures further enhance performance by distributing computational tasks between edge devices and cloud servers.

Critical Comparison

While edge computing improves real-time detection, it is limited by device constraints such as memory and processing power. Cloud-based approaches, on the other hand, offer scalability but introduce latency and privacy concerns. Hybrid architectures attempt to balance these trade-offs, but optimal task allocation remains a challenge [33]–[35].

Critical Discussion and Synthesis

A comprehensive analysis of the selected studies reveals that no single approach can fully address the challenges of IoT anomaly detection. Traditional ML methods provide simplicity and interpretability but lack scalability, while deep learning models offer higher accuracy at the expense of computational cost.

Emerging techniques such as federated learning and blockchain improve privacy and security but introduce new challenges related to communication overhead and system complexity. Similarly, edge–cloud architectures enhance real-time processing but require careful optimization to balance performance and resource usage.

Overall, the research indicates a growing trend toward hybrid and integrated solutions that combine multiple techniques to overcome individual limitations. Future research should focus on developing lightweight, scalable, and privacy-preserving models that can operate efficiently in real-world IoT environments.

Tables (Comparative Summary)

Study Ref	Technique Used	Advantages	Limitations
[1]–[5]	Traditional ML (SVM, RF)	Simple, interpretable	Requires labeled data
[6]–[10]	Unsupervised Learning (Autoencoders)	No labeling needed	High false positives
[11]–[15]	Deep Learning (CNN, RNN, GNN)	High accuracy	High computational cost
[21]–[23]	Federated Learning	Privacy-preserving	Communication overhead
[24]–[26]	Blockchain Integration	Secure and decentralized	Scalability issues
[31]–[35]	Edge–Cloud Systems	Real-time detection	Resource constraints

Table: Comparison of Anomaly Detection Techniques in IoT

4. DISCUSSION / EXPERT OPINION

Synthesis and Interpretation

The comprehensive analysis of the selected studies reveals that anomaly detection in IoT systems has evolved significantly from traditional machine learning approaches to more advanced deep learning and hybrid frameworks. Early research primarily focused on rule-based and classical machine learning techniques, which provided a foundation for identifying anomalous behavior in network traffic [1]–[5]. However, these approaches were limited in handling the dynamic and heterogeneous nature of IoT environments.

With the advancement of deep learning, models such as CNNs, RNNs, and autoencoders have demonstrated improved capability in capturing complex temporal and spatial patterns, resulting in higher detection accuracy [6]–[12]. Furthermore, the integration of emerging technologies such as federated learning and blockchain has

Volume: 05 / Issue: 04 / 2026 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

enhanced privacy preservation and data security, addressing critical concerns in distributed IoT systems [13]–[18].

Edge computing and hybrid edge–cloud architectures have further improved real-time anomaly detection by reducing latency and optimizing resource utilization [19]–[23]. Additionally, explainable AI techniques have been introduced to improve transparency and interpretability, which are essential for building trust in automated security systems [24]–[27].

Overall, the synthesis of these studies indicates a clear shift toward integrated, intelligent, and privacy-aware anomaly detection frameworks, combining multiple technologies to achieve better performance and scalability [28]–[35].

Limitations and Research Gaps

Despite significant advancements, several limitations and research gaps remain in the field of IoT anomaly detection.

One of the primary challenges is the lack of standardized and high-quality datasets, which makes it difficult to evaluate and compare different models fairly [1]–[5]. Many studies rely on simulated or outdated datasets that do not accurately represent real-world IoT environments.

Another limitation is the resource constraint of IoT devices, which restricts the deployment of computationally intensive deep learning models [6]–[10]. While edge computing partially addresses this issue, optimal distribution of tasks between edge and cloud layers remains an open problem.

Privacy and security challenges also persist. Although federated learning and blockchain-based approaches improve data privacy, they introduce communication overhead, latency, and scalability issues [11]–[16]. Additionally, non-IID data distribution in federated settings can negatively impact model performance.

Furthermore, many existing models lack interpretability and explainability, which limits their adoption in critical applications such as healthcare and industrial systems [17]–[20]. There is also a lack of research focusing on real-time adaptive models that can dynamically respond to evolving cyber threats.

Finally, most studies focus on specific IoT scenarios (e.g., smart homes), leading to limited generalization across diverse IoT domains [21]–[25]. This highlights the need for more robust and universally applicable solutions [26]–[35].

Expert Opinion and Future Perspectives

Based on the analysis of the reviewed literature, it is evident that the future of IoT anomaly detection lies in the development of lightweight, scalable, and intelligent hybrid models. No single technique is sufficient to address all challenges; therefore, integrating machine learning, federated learning, blockchain, and edge computing is essential for building robust systems.

From an expert perspective, future research should focus on the following directions:

- **Lightweight Deep Learning Models:** Designing resource-efficient models suitable for deployment on edge and IoT devices without compromising accuracy [1]–[8].
- **Standardized Benchmark Datasets:** Developing realistic, large-scale IoT datasets to enable fair comparison and evaluation of models [9]–[14].
- **Adaptive and Self-Learning Systems:** Creating models that can continuously learn and adapt to new types of cyberattacks in real time [15]–[20].
- **Explainable AI Integration:** Enhancing transparency and interpretability to improve trust and usability in critical applications [21]–[25].
- **Secure and Scalable Frameworks:** Improving federated learning and blockchain mechanisms to reduce overhead while maintaining security and privacy [26]–[30].
- **Cross-Domain Generalization:** Developing models that can perform effectively across multiple IoT domains, such as healthcare, smart cities, and industrial IoT [31]–[35].

In conclusion, while significant progress has been made, IoT anomaly detection remains an evolving field with numerous opportunities for innovation. Future solutions must strike a balance between accuracy, efficiency, scalability, and privacy to ensure secure and reliable IoT ecosystems.

5. CONCLUSIONS AND FUTURE DIRECTIONS

Summary of Key Findings

This review provides a comprehensive analysis of anomaly detection techniques in IoT environments, highlighting the evolution from traditional machine learning methods to advanced deep learning and hybrid frameworks. Early approaches based on classical machine learning algorithms laid the foundation for anomaly detection but were limited in handling the dynamic and large-scale nature of IoT systems [1]–[5].

With the advancement of deep learning, models such as autoencoders, CNNs, RNNs, and GNNs have significantly improved detection accuracy by capturing complex data patterns and temporal dependencies [6]–[12]. Furthermore, emerging paradigms such as federated learning and blockchain have enhanced privacy and security by enabling decentralized and secure data processing [13]–[18].

The integration of edge computing and hybrid edge–cloud architectures has addressed latency and real-time processing challenges, making anomaly detection more efficient in practical IoT deployments [19]–[23]. Additionally, explainable AI techniques have contributed to improving the transparency and interpretability of anomaly detection models, which is crucial for critical applications [24]–[27].

Overall, the findings indicate a clear trend toward integrated and intelligent frameworks that combine multiple technologies to overcome the limitations of individual approaches. Despite these advancements, challenges such as scalability, resource constraints, and lack of standardized datasets continue to persist [28]–[35].

Future Directions

Based on the identified gaps and limitations, several promising directions for future research are proposed:

Volume: 05 / Issue: 04 / 2026 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

- **Development of Lightweight Models:** Future work should focus on designing computationally efficient deep learning models that can operate on resource-constrained IoT devices without compromising performance [1]–[6].
- **Standardized and Realistic Datasets:** There is a strong need for publicly available, large-scale, and real-world IoT datasets to ensure fair evaluation and benchmarking of anomaly detection models [7]–[12].
- **Adaptive and Real-Time Detection Systems:** Research should aim to develop adaptive models capable of continuous learning and real-time response to evolving cyber threats in dynamic IoT environments [13]–[18].
- **Enhanced Privacy-Preserving Techniques:** Improving federated learning and blockchain-based approaches to reduce communication overhead and latency while maintaining strong security guarantees remains a critical research area [19]–[24].
- **Explainable and Trustworthy AI Models:** Future systems should integrate explainable AI techniques to improve interpretability, enabling better decision-making and trust in automated security systems [25]–[29].
- **Cross-Domain Generalization:** Developing models that can generalize across different IoT domains, such as healthcare, industrial IoT, and smart cities, is essential for broader applicability [30]–[35].

In conclusion, while significant progress has been made in IoT anomaly detection, the field continues to evolve with emerging technologies and increasing security demands. Future research must focus on achieving a balance between accuracy, efficiency, scalability, and privacy to build robust and reliable IoT security solutions.

REFERENCES

[1] Y. Yuan, "Research on anomaly detection and privacy protection of network security data based on machine learning," J. Phys.: Conf. Ser., vol. 2892, no. 1, p. 012003, 2025.

[2] D. Cejudo, F. Tavares, and A. M. Cabrera, "Smart home-assisted anomaly detection system for older adults," Sensors, vol. 25, no. 5, p. 2231, 2025.

[3] R. Alam, S. Nasrin, and F. Rahman, "Federated deep learning for secure IoT anomaly detection using blockchain-enhanced privacy," IEEE Internet Things J., vol. 12, no. 3, pp. 18342–18356, 2025.

[4] L. Q. Wang, J. H. Xu, and C. K. Lee, "Explainable deep hybrid model for human-centric smart home security," IEEE Access, vol. 13, pp. 55710–55725, 2025.

[5] A. Basu and N. R. Patra, "Lightweight federated transformer network for real-time IoT anomaly detection," Future Gener. Comput. Syst., vol. 161, pp. 227–239, 2025.

[6] A. S. Abhishek and P. Kumar, "Blockchain-based federated learning for IoT anomaly detection," Future Gener. Comput. Syst., vol. 150, pp. 320–332, 2024.

[7] X. Liu, L. Li, and W. Wang, "Hybrid edge–cloud architecture for real-time IoT anomaly detection using deep reinforcement learning," IEEE Internet Things J., vol. 11, no. 2, pp. 2441–2452, 2024.

[8] S. Alghamdi and F. Hussain, "Explainable AI-based intrusion detection for smart homes," IEEE Trans. Emerg. Topics Comput. Intell., vol. 8, no. 1, pp. 178–190, 2024.

[9] J. I. Araya, "Anomaly-based cyberattack detection for smart homes: A systematic literature review," Internet Things, vol. 22, p. 100792, 2023.

[10] R. M. Abolhasanzadeh and M. Conti, "Lightweight intrusion detection for IoT devices using autoencoders," Ad Hoc Netw., vol. 136, p. 103086, 2023.

[11] P. Zhang, L. Qian, and D. Chen, "A lightweight blockchain-based anomaly detection model for IoT networks," IEEE Trans. Inf. Forensics Secur., vol. 18, pp. 2356–2369, 2023.

[12] D. Nguyen, T. Hoang, and P. Nguyen, "Edge intelligence for IoT anomaly detection: A survey," IEEE Internet Things Mag., vol. 6, no. 2, pp. 112–118, 2023.

[13] J. Brown, D. Wu, and T. Zhang, "Semi-supervised learning for IoT anomaly detection using graph neural networks," IEEE Internet Things J., vol. 10, no. 12, pp. 10245–10256, 2023.

[14] K. DeMedeiros, A. Hendawi, and M. Alvarez, "A survey of AI-based anomaly detection in IoT and sensor networks," Sensors, vol. 23, no. 3, p. 1352, 2023.

[15] A. Chatterjee, "IoT anomaly detection methods and applications: A survey," Internet Things, vol. 19, p. 100568, 2022.

[16] S. K. Singh and R. Goyal, "A machine learning-based approach for IoT device anomaly detection," IEEE Internet Things J., vol. 9, no. 16, pp. 14589–14597, 2022.

[17] Y. Zhang, Y. Chen, and M. Li, "Federated deep learning for anomaly detection in IoT systems," IEEE Trans. Ind. Informat., vol. 18, no. 8, pp. 5184–5192, 2022.

[18] T. Kim, J. Park, and S. Kim, "Unsupervised learning-based anomaly detection in smart home IoT networks," IEEE Access, vol. 10, pp. 47650–47662, 2022.

[19] A. H. Lashkari, Y. Zang, and A. Ghorbani, "A comprehensive review of network traffic datasets for IoT anomaly detection," IEEE Access, vol. 10, pp. 45553–45574, 2022.

[20] C. Zhang, J. Li, and Y. Liu, "Federated learning for smart home IoT devices: A privacy-preserving anomaly detection framework," IEEE Trans. Netw. Serv. Manag., vol. 19, no. 4, pp. 4003–4015, 2022.

[21] A. Diro, N. Chilamkurti, V. D. Nguyen, and W. Heyne, "A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms," Sensors, vol. 21, no. 24, p. 8320, 2021.

[22] I. H. Sarker, "Deep learning: A comprehensive overview on techniques, taxonomy, applications, and research directions," SN Comput. Sci., vol. 2, no. 6, p. 420, 2021.

[23] F. Hussain et al., "Machine learning in IoT security: Current solutions and future challenges," IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 1686–1721, 2020.

[24] M. A. Ferrag et al., "A systematic review of data-driven intrusion detection in smart grids," IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1143–1176, 2019.

[25] R. Doshi, N. Apthorpe, and N. Feamster, "Characterizing IoT device behavior and detecting anomalies using machine learning," in ACM SIGCOMM Workshop, pp. 123–129, 2019.

[26] M. Conti et al., "Internet of Things security and forensics: Challenges and opportunities," Future Gener. Comput. Syst., vol. 78, pp. 544–546, 2018.

[27] H. HaddadPajouh et al., "A deep recurrent neural network-based approach for IoT malware threat hunting," Future Gener. Comput. Syst., vol. 85, pp. 88–96, 2018.

[28] R. Doshi et al., "Machine learning DDoS detection for consumer IoT devices," in IEEE SPW, pp. 29–35, 2018.

Volume: 05 / Issue: 04 / 2026 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

[29] S. Meidan et al., "Detection of unauthorized IoT devices using machine learning techniques," arXiv:1709.04647, 2017.

[30] P. K. Sharma et al., "DistBlockNet: A distributed blockchain-based secure SDN architecture for IoT networks," IEEE Commun. Mag., vol. 55, no. 9, pp. 78–85, 2017.

[31] M. Ahmed et al., "A survey of network anomaly detection techniques," J. Netw. Comput. Appl., vol. 60, pp. 19–31, 2016.

[32] A. Javaid et al., "A deep learning approach for network intrusion detection system," in EAI Conference, pp. 21–26, 2016.

[33] S. Suthaharan, "Big data classification: Problems and challenges in network intrusion prediction," ACM SIGMETRICS, vol. 41, no. 4, pp. 70–73, 2014.

[34] J. Gubbi et al., "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[35] L. Atzori et al., "The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.