processes

MDPI

Article

MAS-LSTM: A Multi-Agent LSTM-Based Approach for Scalable Anomaly Detection in IIoT Networks

Zhenkai Qin [1,2], Qining Luo [1], Xunyi Nong [1], Xiaolong Chen [3,*], Hongfeng Zhang [3,*] and Cora Un In Wong [3]

[1] Network Security Research Center, Guangxi Police College, Nanning 530028, China; qinzhenkai@gxjcxy.edu.cn (Z.Q.); luoqining22@gxjcxy.site (Q.L.); nongxunyi23@gxjcxy.site (X.N.)
[2] School of Computer Science and Artificial Intelligence, Southwest Jiaotong University, Chengdu 611756, China
[3] Faculty of Humanities and Social Sciences, Macao Polytechnic University, Macao, China; corawong@mpu.edu.mo
* Correspondence: osakacool@hait.edu.cn (X.C.); hfengzhang@mpu.edu.mo (H.Z.)

Abstract: The increasing complexity of interconnected systems in the Internet of Things (IoT) demands advanced methodologies for real-time security and management. This study presents MAS-LSTM, an anomaly-detection framework that combines multi-agent systems (MASs) with long short-term memory (LSTM) networks. By training agents on IoT traffic datasets (NF-ToN-IoT, NF-BoT-IoT, and their V2 versions), MAS-LSTM offers scalable, decentralized anomaly detection. The LSTM networks capture temporal dependencies, enhancing anomaly detection in time-series data. This framework overcomes key limitations of existing methods, such as scalability in heterogeneous traffic and computational efficiency in resource-constrained IIoT environments. Additionally, it leverages graph signal processing for adaptive and modular detection across diverse IoT scenarios. Experimental results demonstrate its effectiveness, achieving F1 scores of 0.9861 and 0.8413 on NF-BoT-IoT and NF-ToN-IoT, respectively. For V2 versions, MAS-LSTM achieves F1 scores of 0.9965 and 0.9678. These results highlight its robustness in handling large-scale IIoT traffic. Despite challenges in real-world deployment, such as adversarial attacks and communication overhead, future research could focus on self-supervised learning and lightweight architectures for resource-constrained environments.

Keywords: anomaly detection; Internet of Things; long short-term memory

Academic Editors: Yo-Ping Huang, Gongzhuang Peng and Shenglong Jiang

Received: 20 December 2024
Revised: 18 February 2025
Accepted: 25 February 2025
Published: 5 March 2025

Citation: Qin, Z.; Luo, Q.; Nong, X.; Chen, X.; Zhang, H.; Wong, C.U.I. MAS-LSTM: A Multi-Agent LSTM-Based Approach for Scalable Anomaly Detection in IIoT Networks. *Processes* **2025**, *13*, 753. https://doi.org/10.3390/pr13030753

1. Introduction

In early 2024, a significant disruption in one of Europe's largest manufacturing centers exposed critical vulnerabilities within industrial Internet of Things (IIoT) environments. A carefully orchestrated cyberattack infiltrated multiple smart factories, manipulating sensor data streams and halting production lines for over 48 hours. The incident caused widespread delays in global supply chains and substantial financial losses. Investigations revealed that the root cause was not simply the widespread adoption of IoT devices. Rather, the primary issue was the absence of robust anomaly-detection mechanisms within IIoT networks. Specifically, the inability to detect and respond promptly to irregular traffic and sensor data patterns led to catastrophic consequences.

This incident underscores the urgent need for robust anomaly-detection systems tailored to IIoT environments. Although previous research on IoT security explores vulnerabilities and mitigation strategies, significant gaps remain in accurately identifying subtle yet impactful anomalies. Researchers Hu et al. [1], Thamilarasu and Chawla [2], and Fang et al. [3] propose machine learning and deep learning-based methods for anomaly

detection. However, these methods often fail to address the computational constraints and scalability challenges unique to industrial settings. Moreover, temporal anomalies—patterns that evolve over extended periods in sequential data—pose additional challenges that remain insufficiently addressed.

The Internet of Things (IoT) transforms industrial operations by interconnecting millions of devices. These devices form the backbone of critical infrastructures such as manufacturing facilities, smart factories, and energy grids [1,2]. While this connectivity revolutionizes automation and efficiency, it introduces significant security risks. IIoT systems are increasingly targeted by cyber threats such as Distributed Denial-of-Service (DDoS) attacks, botnet intrusions, and data manipulation, all of which threaten productivity and infrastructure integrity [3,4]. The scale, heterogeneity, and dynamic nature of IIoT networks pose formidable challenges to conventional security solutions. Traditional intrusion-detection systems (IDSs) are designed for standard network traffic and often struggle to handle the high volume, velocity, and diversity of industrial data [5,6]. Additionally, centralized anomaly-detection systems face serious scalability and adaptability issues in dynamic IIoT environments [7]. Furthermore, industrial systems require real-time threat detection that is not only accurate but also fast, adaptive, and scalable [8].

Deep learning techniques, such as recurrent neural networks (RNNs) and long short-term memory (LSTM) networks, show promise in time-series anomaly detection [9–11]. However, their centralized implementations often fail to scale in large and diverse networks [12–14]. Similarly, while Transformer models excel at parallel computation, their high computational demands make them unsuitable for resource-constrained IIoT environments [15].

To address these challenges, this paper proposes a novel anomaly-detection framework called MAS-LSTM, which integrates Multi-Agent Systems (MAS) with LSTM networks. MAS provides decentralized and modular decision-making, allowing independent agents to process specific datasets autonomously [16–18]. Meanwhile, LSTM networks are adept at capturing temporal dependencies, which is crucial for detecting time-series anomalies in industrial applications [19,20]. By tackling scalability and adaptability challenges in IIoT environments, MAS-LSTM provides a distributed yet efficient solution for anomaly detection.

Given these considerations, our research aims to answer the following key research question: "How can a decentralized anomaly-detection framework effectively address scalability, computational efficiency, and real-time adaptability challenges in IIoT networks?" This question guides the design and evaluation of MAS-LSTM, ensuring that it provides an effective and scalable solution tailored to the unique requirements of IIoT security.

Although MAS and LSTM offer strong advantages, alternative approaches have also been explored in the literature. Support Vector Machines (SVMs) and Random Forests demonstrate effectiveness in detecting known attack patterns, but they heavily depend on labeled datasets, which limit their adaptability in dynamic IIoT environments [21]. Similarly, unsupervised clustering techniques, such as k-means and DBSCAN, can identify outliers but often fail to generalize to unseen attack types due to their lack of sequential dependency modeling [22]. Graph Neural Networks (GNNs) have recently emerged as an alternative for anomaly detection in IIoT by capturing topological dependencies in network traffic [23]; however, their computational overhead makes them unsuitable for real-time industrial settings. Compared to these approaches, MAS-LSTM balances scalability, real-time adaptability, and lightweight computation, making it well-suited for IIoT applications.

- Scalable Multi-Agent Architecture: To tackle scalability issues in IIoT with diverse and high-volume traffic, we propose a decentralized MAS framework, where agents independently process traffic segments, minimizing single-point failures and enhancing network adaptability.

- Temporal Modeling with LSTM: IIoT systems are faced with evolving, stealthy attacks over extended periods. We integrate LSTM networks to capture these temporal patterns, enabling the detection of long-term anomalies that traditional methods often overlook.
- Resource-Constrained Adaptation: Traditional deep learning models struggle in resource-limited IIoT environments. Our lightweight, agent-based approach mitigates the computational burden through decentralized processing and efficient LSTM feature extraction, making it feasible for real-world deployment.

The remainder of this paper is structured as follows. Section 2 discusses related work on anomaly detection in IIoT, highlighting the strengths and limitations of existing approaches. Section 3 presents the MAS-LSTM framework, detailing its architecture and operational mechanisms. Section 4 describes the experimental setup, datasets, and evaluation metrics used to assess the model's performance. Section 5 analyzes the results and compares MAS-LSTM with alternative methods. Finally, Section 6 summarizes key findings and outlines future research directions.

2. Related Work

The domain of anomaly detection in Industrial Internet of Things (IIoT) has received considerable attention in recent years due to its critical role in industrial operations. The increasing prevalence of cyberattacks and device malfunctions gives rise to an urgent need for robust security mechanisms tailored to IIoT environments. Traditional intrusion-detection methods, while effective in conventional network contexts often fall short in addressing the unique demands of IIoT systems, such as heterogeneous traffic patterns, stringent real-time requirements, and diverse operational characteristics [24,25].

Machine learning-based approaches, such as Support Vector Machines (SVMs) and Random Forests, have demonstrated effectiveness in detecting known attack patterns [26,27]. However, these approaches rely heavily on labeled datasets, which are often labor-intensive to produce and scarce in industrial scenarios, thereby limiting their scalability and adaptability. Similarly, unsupervised methods like k-means clustering and density-based spatial clustering (DBSCAN) can identify outliers in unlabeled data [25]. However, these methods often fail to generalize to unseen attack types and lack the ability to capture temporal dependencies, which are critical in IIoT anomaly detection.

Deep learning techniques have significantly advanced anomaly-detection capabilities, particularly with Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks. These models excel at capturing long-term temporal dependencies, making them highly effective for time-series anomaly-detection tasks [9,28]. However, centralized LSTM-based methods face challenges in handling large-scale and diverse IIoT traffic, particularly in high-volume networks with heterogeneous data distributions, which makes them less efficient and scalable compared to distributed solutions. Transformer-based models have also been explored for anomaly detection due to their strong parallel computation capabilities [15], but their high computational cost makes them less suitable for resource-constrained IIoT environments. Similarly, Graph Neural Networks (GNNs) have shown promise in capturing topological dependencies, but their integration with temporal modeling introduces additional complexity and computational overhead, which further challenges their application in real-time IIoT settings.

While Transformer models have demonstrated superior performance in capturing long-range dependencies within sequential data, their application in IIoT anomaly detection is limited by high computational complexity [29]. Compared to MAS-LSTM, Transformer-based methods require substantial computational resources, making them impractical for real-time and resource-constrained IIoT deployments. Additionally, Transformer models of-

ten require significantly more training data and hyperparameter tuning to achieve optimal accuracy, whereas LSTM-based methods, particularly in a decentralized MAS architecture, are more computationally efficient while maintaining competitive detection accuracy. Empirical studies have shown that MAS-LSTM achieves higher efficiency in detecting real-time anomalies with lower latency, whereas Transformer models may introduce computational bottlenecks when applied to high-volume industrial traffic.

Anomaly detection in Industrial Internet of Things (IIoT) networks has seen the development of various hybrid frameworks, each designed to address the unique challenges posed by industrial environments. Several such hybrid approaches combine the strengths of different techniques to enhance detection accuracy and scalability. Autoencoder-based methods, for instance, have been used in combination with LSTM networks to capture both feature representations and temporal dependencies in IIoT data, improving the robustness of anomaly detection. Similarly, reinforcement learning (RL)-enhanced anomaly-detection frameworks dynamically optimize model parameters and decision rules to adapt to evolving attack patterns, offering a flexible approach to address dynamic threats. Another emerging approach is the integration of federated learning (FL) with deep anomaly detection, enabling models to be trained across distributed IIoT nodes while preserving data privacy. These methods offer alternative solutions to improve scalability, adaptability, and efficiency in industrial anomaly detection, though they may introduce additional complexity or overhead.

Several studies have explored hybrid approaches similar to MAS-LSTM, illustrating the increasing interest in combining decentralized systems with advanced machine learning techniques for IIoT anomaly detection. For example, recent work by Zulfiqar [30] proposed a hybrid MAS and deep learning framework for anomaly detection in smart manufacturing, where the MAS was used to divide tasks across decentralized agents, and deep learning methods (including LSTM) were employed for temporal pattern recognition. While this method also uses a hybrid approach, it does not emphasize the distributed decision-making and computational efficiency that MAS-LSTM offers. Additionally, Sun [31] combined reinforcement learning with MAS to optimize decision-making in IIoT networks, with a focus on improving adaptability to dynamic traffic and attack patterns. This approach is similar to ours, but it lacks the temporal modeling capability of LSTM, which is a crucial component in detecting time-series anomalies in IIoT environments. These studies provide valuable context for the effectiveness of hybrid models in IIoT anomaly detection, while also highlighting key differences in model structure and the application of temporal dependencies.

In light of these challenges, recent research has increasingly focused on distributed learning architectures such as Multi-Agent Systems (MAS) [16]. MAS-based frameworks enable independent agents to process specific datasets autonomously, improving network efficiency and reducing single points of failure [32–34]. These hybrid models, which combine LSTM's temporal modeling capabilities with MAS's decentralized decision-making, have shown promise in enhancing adaptability while minimizing centralized processing overhead [35]. This integration of MAS with deep learning methods, particularly LSTM, provides a more scalable and adaptive solution than centralized methods alone, offering improved performance in IIoT environments with high data variability.

Furthermore, research in adjacent domains, such as distributed learning and reinforcement learning, provides valuable insights. Reinforcement learning techniques, when integrated into MAS, have demonstrated potential in dynamically optimizing decision-making processes and improving adaptability in evolving environments [32,34]. These approaches highlight the potential of decentralized architectures to manage complex and dynamic IIoT systems. However, many existing MAS-based frameworks lack robust tem-

poral modeling capabilities, which limits their effectiveness in capturing the sequential nature of anomalies.

MAS-LSTM addresses these gaps by combining the strengths of MAS and LSTM networks, offering a scalable, adaptive, and computationally efficient solution tailored to the complex requirements of IIoT environments. Unlike Transformer-based approaches, which are computationally intensive, MAS-LSTM provides a lightweight alternative that maintains high detection performance. Furthermore, the modular nature of the MAS enables the seamless integration of additional agents, allowing the system to dynamically adapt to new traffic patterns and evolving attack scenarios. This unique combination of distributed decision-making, computational efficiency, and temporal modeling positions the MAS-LSTM framework as a robust solution for anomaly detection in IIoT networks.

3. Methodology

3.1. Problem Definition and Background

The Industrial Internet of Things (IIoT) consists of a vast network of interconnected devices in industrial environments, generating large-scale and highly heterogeneous data. Formally, let $\mathcal{D} = \{\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_N\}$ represent the dataset of traffic information collected from N devices, where each $\mathbf{d}_i \in \mathbb{R}^m$ is a data vector of dimension m corresponding to the traffic features from device i. The complexity of IIoT systems, due to the diverse nature of devices and traffic patterns, makes them vulnerable to various cyberattacks and anomalies, such as Distributed Denial-of-Service (DDoS) attacks, botnet intrusions, and sensor malfunctions [6,36].

Traditional anomaly-detection methods face several challenges in IIoT settings, including scalability issues when handling large data volumes, the need for real-time detection of evolving attack patterns, and the limitations imposed by resource-constrained devices [20,37]. Let $\mathcal{A} = \{a_1, a_2, \ldots, a_K\}$ represent the set of attack types, where $a_k \in \mathbb{R}^m$ denotes the feature representation of attack type k. In many cases, the detection of a_k requires models capable of learning temporal dependencies within the data, denoted by:

$$\mathbf{X}_t = f(\mathbf{X}_{t-1}, \mathbf{X}_{t-2}, \ldots, \mathbf{X}_{t-n}; \theta) \tag{1}$$

where $\mathbf{X}_t$ is the data vector at time t, and θ represents the model parameters. This temporal dependency makes it necessary to use methods that can model such sequences effectively, as shown in studies of time-series anomaly detection [38,39].

Existing centralized approaches to anomaly detection often struggle with the heterogeneity and dynamic nature of IIoT traffic, leading to high false positives or delayed detection [40]. These methods also require substantial computational resources, which are impractical in IIoT environments where devices may have limited processing power [41]. Therefore, there is a need for scalable, efficient, and adaptive solutions capable of detecting anomalies while accommodating the constraints of IIoT systems. Let $\mathbf{y}_t$ represent the anomaly label at time t, where:

$$y_t = \begin{cases} 0, & \text{if normal traffic at time } t, \\ 1, & \text{if anomalous traffic at time } t. \end{cases} \tag{2}$$

To address these challenges, we propose the MAS-LSTM framework, which integrates Multi-Agent Systems (MAS) for decentralized learning and decision-making with Long Short-Term Memory (LSTM) networks for capturing temporal dependencies in IIoT data. Multi-Agent Systems (MASs) are collections of autonomous agents that interact with each other and the environment to achieve individual or collective goals [42]. MASs have been

widely used in decentralized systems to improve scalability and efficiency, particularly in environments like IIoT where traditional centralized systems often fail to meet real-time and resource limitations [43,44]. Each agent in an MAS can process local data, make decisions, and communicate with others to achieve a broader goal. In the context of IIoT, an MAS helps distribute the computational load and allows the system to scale efficiently.

LSTM is a type of Recurrent Neural Network (RNN) designed to model sequential data by capturing long-term dependencies. In IIoT anomaly detection, LSTM networks are especially effective for identifying abnormal patterns in time-series data generated by devices. The LSTM-based temporal modeling can be formally expressed as:

$$h_t = LSTM(\mathbf{X}_t, h_{t-1}; \theta_{LSTM}), \tag{3}$$

where h_t is the hidden state at time t, and θ_{LSTM} are the parameters of the LSTM model. This allows LSTM to capture the temporal dependencies in data, which are crucial for detecting anomalies that evolve over time.

The combination of MAS and LSTM in the MAS-LSTM framework enables decentralized anomaly detection. Each agent uses LSTM to analyze its local data and detect anomalies. The agents can then share their findings, allowing the system to coordinate and improve the accuracy of anomaly detection. This collaboration improves scalability, real-time detection, and efficiency in large-scale IIoT environments. By leveraging both MAS for decentralization and LSTM for temporal modeling, the MAS-LSTM framework is better equipped to handle the complexity and dynamic nature of IIoT data.

3.2. System Architecture

This section presents the proposed anomaly-detection framework, which integrates a multi-agent system (MAS) with long short-term memory (LSTM) networks. MAS-LSTM is designed to address the scalability, adaptability, and real-time detection challenges in large-scale Industrial Internet of Things (IIoT) networks. To improve the model's generalization and prevent overfitting, we introduce an adaptive dropout strategy during training. This strategy dynamically adjusts the dropout rate throughout the training process, starting with a higher rate and decreasing over time. By doing so, we can prevent the model from overfitting in the initial stages while allowing it to capture long-term dependencies in the later stages. This adaptive dropout mechanism enhances the robustness of the model without compromising the accuracy of anomaly detection. By leveraging distributed learning and temporal modeling, the system effectively identifies anomalies in IIoT traffic. The modular structure, as shown in Figure 1, ensures each component contributes to the overall robustness and efficiency of MAS-LSTM.

The integration of MAS and LSTM within MAS-LSTM addresses critical challenges in IIoT anomaly detection. We chose MAS due to its ability to offer decentralized decision-making, allowing agents to work autonomously on distinct subsets of the data. This design reduces the risk of single-point failures, which is crucial for real-time applications in dynamic IIoT environments. Moreover, LSTM networks within each agent capture temporal dependencies in IIoT traffic, making MAS-LSTM highly effective for detecting sequential anomalies, such as stealthy botnet behaviors. The decision to use LSTM was based on its capability to detect time-series anomalies, which are common in IIoT systems. The combination of MAS's adaptability and LSTM's precision enables MAS-LSTM to outperform traditional centralized methods in dynamic and heterogeneous environments. Furthermore, the modular design of MAS-LSTM allows the seamless integration of new agents and supports scalability without compromising detection accuracy.

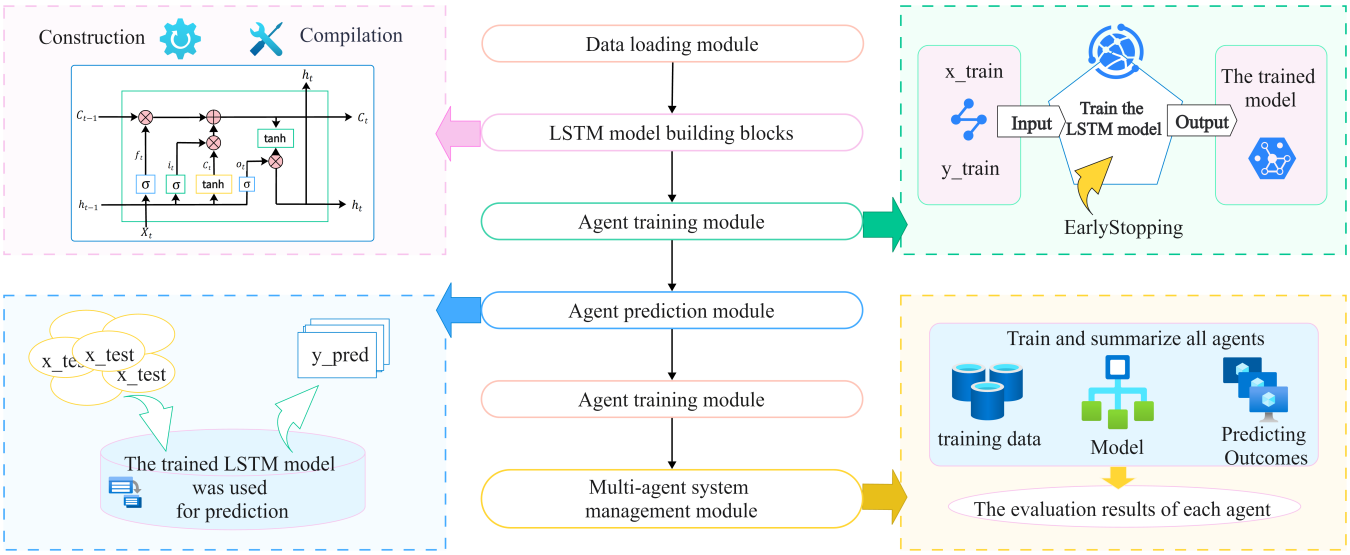

Figure 1. Framework for anomaly detection in IIoT networks, covering data loading, LSTM model construction, agent training, and system-level decision-making.

3.3. Multi-Agent System (MAS)

In the design of MAS-LSTM, the decision to incorporate a Multi-Agent System (MAS) was made to address the need for scalability in heterogeneous IIoT networks. Each agent is assigned a specific traffic dataset, ensuring that data processing is distributed across multiple nodes, rather than being handled centrally. This approach enables parallelism and facilitates more efficient learning from the traffic data. The backbone of MAS-LSTM relies on MAS, which offers a decentralized and scalable solution to managing the diverse and heterogeneous traffic patterns in IIoT networks [16]. Each agent operates independently, analyzing specific datasets to ensure localized learning and decision-making. This modular design enables parallelism, significantly enhancing MAS-LSTM's scalability and adaptability.

The agents in the MAS are designed to independently process and analyze specific portions of the IIoT data. However, when it comes to decision-making, agents share their anomaly-detection insights with each other through a communication mechanism. This enables agents to exchange information about potential anomalies, which helps improve the overall accuracy of the system. In the case of conflicting anomaly classifications (e.g., one agent classifies traffic as normal while another classifies it as anomalous), a majority voting mechanism is employed to resolve conflicts. This ensures that the final decision reflects the consensus of the majority of agents, reducing the impact of individual conflicting classifications.

Let $D = \{D_1, D_2, \ldots, D_N\}$, where D_i represents the traffic dataset for agent A_i. Each dataset is segmented into time-series sequences $\mathbf{X}_i = \{\mathbf{x}_{i1}, \mathbf{x}_{i2}, \ldots, \mathbf{x}_{iT}\}$ with corresponding labels $\mathbf{Y}_i = \{y_{i1}, y_{i2}, \ldots, y_{iT}\}$ [25,26].

Before being fed into the LSTM network, IIoT traffic data undergoes preprocessing steps to make it suitable for time-series analysis. Raw traffic data is cleaned by removing irrelevant data, handling missing values, and filtering out noise. Time windows are then defined to segment the traffic data into smaller chunks, allowing the LSTM model to process sequential patterns. These time-series sequences are created for each agent to analyze, and normalization is applied to ensure consistent feature scaling.

The network traffic metrics used for anomaly detection include packet arrival rates, which indicate the rate at which packets are received and can help identify congestion or unusual traffic behavior. Transmission delays are also monitored, as they represent the

time taken for packets to reach their destination and can be useful in identifying issues like DDoS attacks or general network performance problems. Additionally, the total number of bytes and packets transmitted, known as byte and packet counts, are tracked to detect traffic surges or sudden changes in the network, which may signify an anomaly. Protocol types, such as TCP, UDP, and ICMP, are analyzed as they can reveal certain attack types or abnormal system behavior based on their usage patterns. Flow duration and flow counts are also important, as the number of active flows and their duration can help detect botnet activities or patterns indicative of DDoS attacks. Finally, round-trip time (RTT) is monitored to identify network performance issues or detect behaviors associated with slow-rate flooding attacks. These metrics together form the foundation for anomaly detection in the MAS-LSTM framework.

By breaking the datasets into smaller time-series sequences, agents can focus on more manageable portions of the data, reducing the processing load and speeding up detection. Here, $y_t = 0$ denotes normal traffic, and $y_t = 1$ denotes anomalous traffic. Each agent processes its assigned dataset independently, eliminating dependencies on a centralized controller and reducing the risk of a single point of failure.

This decentralized architecture ensures system robustness and allows seamless integration of new agents, enabling the system to adapt to evolving traffic patterns.

3.4. LSTM-Based Temporal Modeling

One of the key decisions in the design of MAS-LSTM was to integrate LSTM networks for capturing temporal dependencies in IIoT traffic. This was motivated by the need to model long-term patterns that traditional methods could not detect. To capture the temporal dependencies in IIoT traffic, each agent leverages LSTM networks. LSTM's proven ability to model sequential data makes it ideal for detecting complex anomalies, such as Distributed Denial-of-Service (DDoS) and botnet behaviors [9]. While Transformer models excel in parallel processing, their high computational cost limits their applicability in resource-constrained IIoT environments. Therefore, LSTM was chosen for its efficiency in time-series anomaly detection, without compromising the system's real-time capabilities. Similarly, Graph Neural Networks (GNNs), though effective in capturing topological dependencies, introduce unnecessary complexity for time-series modeling.

The LSTM network used in MAS-LSTM consists of two LSTM layers with 128 hidden units per layer, which have been shown to balance model complexity and computational efficiency. We use a batch size of 32 and train the model for 50 epochs to ensure that it captures sufficient temporal dependencies while avoiding overfitting. The Adam optimizer is used for training, as it is well-suited for large-scale datasets and adaptive learning rates. Hyperparameters such as the learning rate and batch size were tuned using a grid search to optimize performance.

The LSTM network's architecture consists of three gates: input (i_t), forget (f_t), and output (o_t), enabling it to retain long-term dependencies while mitigating the vanishing gradient problem. The internal equations are:

$$i_t = \sigma(W_i x_t + U_i h_{t-1} + b_i), \quad f_t = \sigma(W_f x_t + U_f h_{t-1} + b_f), \tag{4}$$

$$o_t = \sigma(W_o x_t + U_o h_{t-1} + b_o), \quad c_t = f_t \cdot c_{t-1} + i_t \cdot \tanh(W_c x_t + U_c h_{t-1} + b_c), \tag{5}$$

$$h_t = o_t \cdot \tanh(c_t), \tag{6}$$

where h_t is the hidden state, and c_t is the cell state at time t. These mechanisms enable LSTM to model sequential traffic patterns effectively.

The final hidden state h_T is passed through a dense layer with a sigmoid activation to predict anomaly probabilities:

$$\hat{y}_T = \sigma(W_h h_T + b_h), \tag{7}$$

where $\hat{y}_T > 0.5$ indicates anomalous traffic, and $\hat{y}_T \leq 0.5$ indicates normal traffic.

3.5. Anomaly Detection and Decision-Making

The decision-making process in MAS-LSTM involves aggregating the individual predictions from each agent. By employing a majority voting system, the framework ensures that the final anomaly-detection decision remains robust, even in cases where individual agents may detect anomalies with slight variations. If two or more agents disagree on the classification of a particular traffic instance, the final decision is determined by the majority vote. This voting mechanism helps resolve conflicts and enhances the reliability of the overall system.

During inference, each agent predicts anomaly probabilities for its assigned dataset. A majority voting mechanism is then used to aggregate the individual decisions, flagging an anomaly if the majority of agents detect abnormal behavior:

$$\hat{y}_t = \begin{cases} 1 & \text{if } \hat{y}_t > 0.5, \\ 0 & \text{if } \hat{y}_t \leq 0.5. \end{cases} \tag{8}$$

This ensemble approach reduces false positives and ensures robust detection. By decentralizing decision-making, the system maintains high adaptability and reliability, even in dynamic IIoT environments.

3.6. Scalability and Real-Time Detection

MAS-LSTM excels in scalability due to its decentralized MAS architecture, where agents process traffic independently. Formally, let $\mathcal{D}_i = \{\mathbf{d}_i^{(1)}, \mathbf{d}_i^{(2)}, \ldots, \mathbf{d}_i^{(T)}\}$ represent the traffic dataset assigned to agent A_i, where T is the number of time steps in the traffic sequence. Each agent A_i processes its own data independently, and the global model decision is made by aggregating local decisions, as described by the majority voting mechanism:

$$\hat{y}_t = \frac{1}{N} \sum_{i=1}^{N} \hat{y}_t^{(i)} \quad \text{for } t = 1, 2, \ldots, T, \tag{9}$$

where $\hat{y}_t^{(i)}$ is the prediction of agent A_i at time t, and N is the total number of agents. This decentralized decision-making reduces the bottlenecks associated with centralized systems, enabling faster real-time anomaly detection.

The modular nature of MAS-LSTM allows seamless integration of additional agents as the network grows or new devices are added. Mathematically, this can be represented by the dynamic addition of agents to the system, where each new agent A_{i+1} is assigned a subset of the data and the model is updated as follows:

$$\mathcal{D}_{i+1} = \{\mathbf{d}_{i+1}^{(1)}, \mathbf{d}_{i+1}^{(2)}, \ldots, \mathbf{d}_{i+1}^{(T)}\}, \tag{10}$$

and the model is adapted to incorporate new data from $\mathcal{D}_{i+1}$ without retraining the entire system. This ensures scalability and adaptability as the system expands.

Additionally, the use of a distributed learning approach enables MAS-LSTM to process large-scale IIoT traffic in real-time. Each agent updates its model parameters locally based on the data it receives, using the following update rule:

$$\theta_i^{(t)} = \theta_i^{(t-1)} - \eta \nabla_{\theta_i} \mathcal{L}_i(\mathbf{d}_i^{(t)}, \hat{y}_i^{(t)}), \tag{11}$$

where $\theta_i^{(t)}$ represents the model parameters for agent A_i at time t, η is the learning rate, and $\mathcal{L}_i$ is the loss function for agent A_i. The parameters are updated independently, which helps distribute the computational load and ensures real-time processing capabilities.

The combination of MAS and LSTM provides a robust solution for complex IIoT networks. The LSTM component models the temporal dependencies in traffic data, ensuring accurate anomaly detection over time, while the MAS component ensures scalability and adaptability by distributing the computation across multiple agents. This results in a system that is efficient, scalable, and capable of handling the dynamic nature of IIoT environments without compromising detection accuracy [45,46].

4. Experiment

The goal of this experiment is to evaluate the effectiveness and flexibility of the proposed MAS-LSTM framework in detecting anomalies across different IoT environments. The experiment focuses on testing the model's ability to handle various attack scenarios in both traditional and modern IoT traffic, using both the original and v2 versions of the datasets. It also compares MAS-LSTM's performance with other machine learning and deep learning methods. To understand the contribution of different components of the architecture, ablation studies are conducted. The experiment uses four IoT traffic datasets—NF-ToN-IoT, NF-BoT-IoT, and their v2 versions—to simulate real-world conditions. We measure performance based on detection accuracy, precision-recall trade-offs, and computational efficiency, while also using tools like 3D UMAP projections and radar charts to visualize feature distributions and decision boundaries. This approach helps address key challenges in IoT security, such as class imbalance, temporal dependencies, and scalability.

4.1. Dataset and Preprocessing

This study utilizes four publicly available IoT traffic datasets: NF-ToN-IoT, NF-BoT-IoT, and their respective versions v2 [47–54]. These datasets were chosen for their ability to comprehensively represent typical IoT traffic patterns, encompassing both benign and malicious behaviors, and providing a robust basis for evaluating the proposed anomaly-detection framework.

The NF-ToN-IoT dataset captures traffic generated by diverse IoT devices, such as sensors and controllers, and includes multiple attack scenarios, including Distributed Denial-of-Service (DDoS) attacks, password guessing, and ransomware. Its heterogeneous traffic patterns and realistic device diversity make it a valuable resource for training and testing anomaly-detection models.

In contrast, NF-BoT-IoT focuses on botnet-generated traffic, a critical threat in IoT environments. This dataset provides detailed records of benign and botnet-induced anomalous behaviors, offering insights into the characteristics of botnet attacks and their impact on network traffic.

The v2 versions of these datasets, NF-ToN-IoT-v2 and NF-BoT-IoT-v2, extend their predecessors by incorporating additional attack types, higher traffic volumes, and more complex traffic patterns. NF-ToN-IoT-v2 simulates diverse and realistic IoT environments, capturing a wider range of benign and malicious interactions. Meanwhile, NF-BoT-IoT-v2 reflects the evolving sophistication of botnet attacks, including high-frequency, large-scale traffic anomalies, which are essential for evaluating the scalability and robustness of anomaly-detection systems in modern IoT settings.

Table 1 summarize the distribution of benign and attack samples across these datasets. For instance, the v2 datasets exhibit significantly larger volumes and a broader variety of attack types compared to their predecessors. NF-ToN-IoT-v2 contains over 10 million attack samples (63.99% of total traffic), while NF-BoT-IoT-v2 exhibits nearly 99.64% malicious traffic. This diversity not only highlights the relevance of these datasets for modeling modern IoT network anomalies but also ensures a rigorous evaluation of MAS-LSTM's adaptability and effectiveness.

Table 1. NF-ToN-IoT, NF-BoT-IoT, NF-ToN-IoT-v2, and NF-BoT-IoT-v2 dataset overview.

Dataset	NF-ToN-IoT		NF-BoT-IoT		NF-ToN-IoT-v2		NF-BoT-IoT-v2	
	Count	%	Count	%	Count	%	Count	%
Benign	270,279	19.6	13,859	2.31	6,099,469	36.01	135,037	0.36
Backdoor	17,247	1.25	-	-	16,809	0.10	-	-
DoS	17,717	1.28	56,833	9.47	712,609	4.21	16,673,183	44.11
DDoS	326,345	23.6	56,844	9.47	2,026,234	11.97	18,331,847	48.56
Injection	468,539	33.9	-	-	684,465	4.05	-	-
MITM	1295	0.09	-	-	7723	0.05	-	-
Password	156,299	11.3	-	-	1,153,323	6.81	-	-
Ransomware	142	0.01	-	-	3425	0.02	-	-
Scanning	21,467	1.56	-	-	3,781,419	22.31	-	-
XSS	99,944	7.25	-	-	2,455,020	14.50	-	-
Attack Samples	1,108,995	80.4	586,241	97.69	10,841,027	63.99	37,628,460	99.64

In terms of data preprocessing, several critical steps were performed to ensure the dataset's quality for model training and evaluation. Initially, irrelevant features such as IPV4_SRC_ADDR, L4_SRC_PORT, IPV4_DST_ADDR, L4_DST_PORT, Attack, and Label were removed to prevent the model from relying on potentially leaking information. This was achieved using the remove_features function, which excluded these specific columns. Missing values were then handled by removing rows containing null entries, ensuring a complete dataset free from gaps that could affect model training.

To further enhance model performance, data normalization was applied, scaling the feature values into the range [0, 1]. This step is particularly important for models like LSTM, as it helps speed up convergence and prevents issues related to features with disproportionate value ranges. The dataset was then split into training and testing sets in an 80/20 ratio, with stratified sampling to maintain the class distribution of benign and malicious traffic. Additionally, the attack labels from the test set were saved separately to facilitate error analysis and assess the performance of the anomaly-detection framework.

These preprocessing steps ensure that the dataset is well-prepared for training and testing, allowing for a more accurate evaluation of the anomaly-detection models, and addressing the complexities of IoT traffic patterns across different datasets.

4.2. Experimental Setup

The proposed multi-agent system was evaluated using the four datasets described earlier. For each dataset, we trained a separate agent within the system, allowing each agent to independently process and learn from its assigned dataset. This setup ensures that the multi-agent framework can handle diverse and heterogeneous IoT traffic patterns effectively. The experimental configuration and hyperparameters are summarized in Table 2.

Table 2. Experiment setup overview.

Component	Description
Batch Size	128
Random Seed	42
Model Type	LSTM
Input Dimension	Dynamic (based on data)
LSTM Units	150
Activation Function	ReLU
Regularization	L2 (lambda = 0.001)
Dropout Rate	0.3
Optimizer	Adam
Loss Function	Binary Crossentropy
Metrics	Accuracy
Epochs	10
Validation Split	20%
Early Stopping	3 epochs without improvement
Prediction Threshold	1
Threshold	0.7
CPU	Intel(R) Core(TM) i7-10870H
GPU	NVIDIA GeForce RTX 3060 Laptop GPU

In our experiments, we explored how adjusting the decision threshold can affect the performance of the model, specifically the trade-off between precision and recall. A higher threshold can improve precision by reducing the number of false positives, though it may slightly reduce recall. In our setup, the default threshold was set to 1, which is optimal for our scenario where minimizing false positives is crucial. This setting is particularly important in real-world industrial IoT applications, where excessive false alarms could lead to operational disruptions, increased costs, and unnecessary security interventions.

However, in certain scenarios where higher recall is required—such as early-stage threat-detection systems or environments where missing an attack is more critical than occasional false positives—adjusting the threshold to a lower value can enhance sensitivity. To analyze how the model behaves with different thresholds, we also evaluated it with a threshold of 0.7, as shown in the confusion matrices in Figure 2. This allows for a flexible trade-off between precision and recall, ensuring the model can be tuned based on specific deployment requirements.

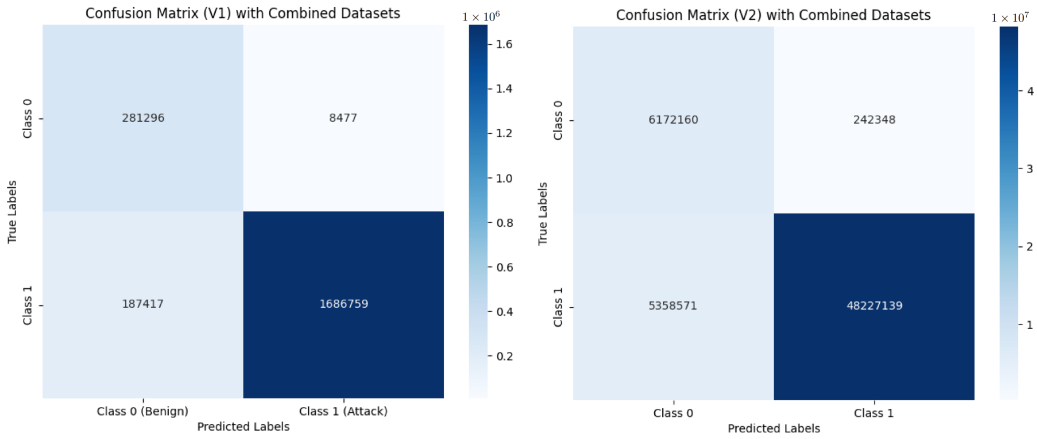

Figure 2. Confusion matrices of the model with different thresholds (threshold = 0.7).

4.3. Results and Analysis

The experimental results, summarized in Tables 3 and 4, provide a comprehensive evaluation of the proposed system compared to traditional machine learning and deep

learning methods. These results highlight the system's ability to handle diverse IoT datasets and detect complex anomalies, addressing scalability and adaptability challenges in IIoT environments.

Table 3. Performance metrics for NF-BoT-IoT and NF-ToN-IoT.

Model	NF-BoT-IoT				NF-ToN-IoT			
	F1-Score	Accuracy	Precision	Recall	F1-Score	Accuracy	Precision	Recall
EFC	0.9649	0.9336	0.9988	0.9331	0.8087	0.7385	0.9821	0.6873
Naive Bayes	0.9652	0.9334	0.9871	0.9442	0.8937	0.8089	0.8084	0.9992
Logreg	0.9932	0.9866	0.9870	0.9995	0.8958	0.8151	0.8190	0.9886
RBF	0.9986	0.9811	0.9975	0.9998	0.9906	0.9822	0.9827	0.9987
GRU-FCN	0.9617	0.8830	0.9975	0.8657	0.8730	0.7892	0.8612	0.8734
LSTM	0.9270	0.7649	0.7600	0.7597	0.8897	0.8423	0.7893	0.8932
GMS-IDS	0.9816	0.9686	0.9483	0.9570	0.8400	0.7965	0.9067	0.9012
MAS-LSTM	0.9861	0.9863	0.9996	0.9929	0.8413	0.8405	0.9906	0.9094

Table 4. Performance metrics for NF-BoT-IoT-v2 and NF-ToN-IoT-v2.

Model	NF-BoT-IoT-v2				NF-ToN-IoT-v2			
	F1-Score	Accuracy	Precision	Recall	F1-Score	Accuracy	Precision	Recall
EFC	0.9730	0.9477	0.9997	0.9478	0.9455	0.9601	0.9012	0.9945
Naive Bayes	0.9960	0.9931	0.9988	0.9943	0.3911	0.2631	0.2441	0.9822
Logreg	0.9993	0.9986	0.9989	0.9998	0.9766	0.9888	0.9840	0.9693
RBF	0.9994	0.9988	0.9992	0.9996	0.9875	0.9913	0.9905	0.9844
GRU-FCN	0.9902	0.8830	0.9975	0.8657	0.8730	0.7892	0.8612	0.8734
LSTM	0.9922	0.7649	0.7600	0.7597	0.8897	0.8423	0.7893	0.8932
GMS-IDS	0.9820	0.8016	0.9532	0.9453	0.9860	0.8901	0.9011	0.9321
MAS-LSTM	0.9965	1.0000	0.9982	0.9809	0.9678	0.9522	0.9599	0.9599

The proposed multi-agent system consistently outperforms or remains highly competitive with baseline methods across key metrics, including F1-score, accuracy, precision, and recall. For instance, on the NF-BoT-IoT-v2 dataset, it achieves an F1-score of 0.9965 with 1.0000 accuracy, performing comparably to RBF networks (F1-score 0.9994). Similarly, on the NF-ToN-IoT-v2 dataset, it achieves an F1-score of 0.9678, while Deep Autoencoders (DeepAE) underperform significantly due to their limited ability to model temporal dependencies in IoT traffic. This robust performance demonstrates the proposed system's capacity to detect rare and complex anomalies—a critical requirement for IoT anomaly detection.

The superior results are attributed to MAS-LSTM's modular and decentralized architecture, where each agent specializes in a subset of the data. This design not only enhances scalability but also ensures adaptability to heterogeneous traffic patterns. Additionally, the use of LSTM networks enables effective modeling of long-term temporal dependencies, allowing the detection of sequential patterns characteristic of advanced attack types, such as Distributed Denial-of-Service (DDoS) and stealthy botnet behaviors.

To ensure a fair comparison, baseline models were selected based on their relevance and popularity in anomaly-detection tasks. Logistic Regression and Naive Bayes serve as foundational benchmarks for binary classification problems [55,56], while DeepAE represents unsupervised feature learning approaches [57]. RBF networks, widely recognized for their success in non-linear classification, provide a strong benchmark in network intrusion detection [58]. Together, these models establish a comprehensive baseline for evaluating the proposed system's effectiveness.

In contrast, baseline methods often exhibit a trade-off between precision and recall, limiting their reliability for real-world anomaly detection. For example, while RBF net-

works may achieve high accuracy or F1-score on certain datasets, they do not consistently generalize across all scenarios. Similarly, DeepAE struggles with temporal modeling, resulting in suboptimal detection of sequential anomalies.

The scalability and adaptability of the proposed system are further underscored by its multi-agent architecture. By delegating specific datasets to independent agents, the system efficiently handles heterogeneous IoT traffic. Decentralized decision-making reduces computational overhead and eliminates single points of failure. These capabilities are particularly beneficial in real-world deployments where IoT networks generate diverse and dynamic traffic.

The Receiver Operating Characteristic (ROC) curve presented in Figure 3 visualizes the performance of the proposed MAS-LSTM model on both the V1 and V2 combined datasets. For the V1 dataset, MAS-LSTM achieves an AUC of 0.95 on the NF-BoT-IoT dataset, significantly outperforming the Silo NF-ToN-IoT model with an AUC of 0.82. On the V2 dataset, MAS-LSTM maintains strong performance, achieving an AUC of 0.94 for the NF-BoT-IoT dataset and outperforms the Silo NF-ToN-IoT model, which achieves an AUC of 0.78.

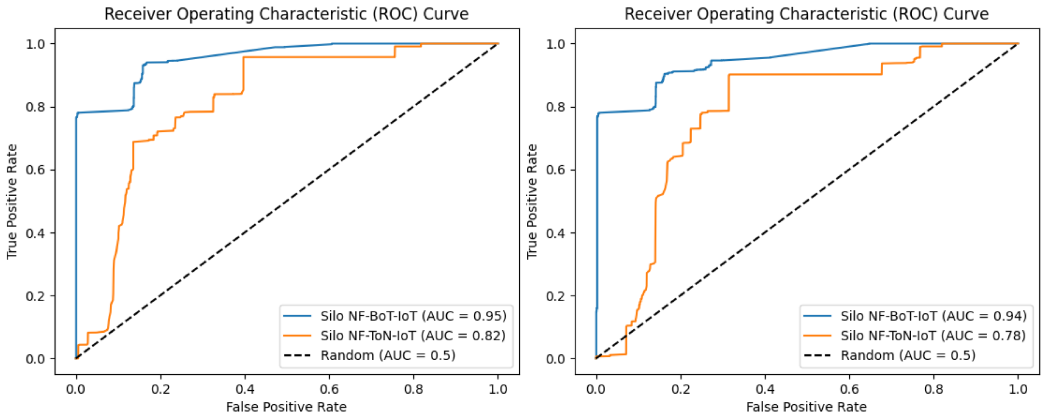

Figure 3. Receiver Operating Characteristic (ROC) curve for MAS-LSTM on V1 and V2 datasets.

These results demonstrate the superior anomaly-detection performance of MAS-LSTM, particularly in distinguishing between normal and anomalous traffic across both V1 and V2 datasets. The AUC scores for both datasets show a clear distinction in performance, with MAS-LSTM consistently outperforming traditional models, reinforcing its effectiveness in IoT environments.

In summary, the proposed multi-agent system, through its integration of LSTM networks and decentralized learning, achieves superior or at least highly competitive performance across diverse IoT datasets. Its balance across precision, recall, and F1-score ensures reliable anomaly detection, while its scalability and adaptability address critical challenges in IIoT environments. These results validate MAS-LSTM as a robust and practical solution for real-world IoT anomaly detection.

4.4. Visual Analysis

To better understand the data characteristics and model performance, we conducted an in-depth analysis using UMAP 3D dimensionality-reduction visualizations and radar charts. The following images illustrate the results.

In Figure 4, the UMAP algorithm was used to visualize the high-dimensional traffic features in 3D. The clustered points of different colors and positions indicate significant distribution differences between normal and attack traffic in the datasets. For instance, in the NF-BoT-IoT-v2 dataset, attack traffic forms distinct and compact clustered regions, while normal traffic is more scattered. This distinct separation provides strong evidence

of unique high-dimensional patterns in attack traffic, which our model can effectively learn. Additionally, the scattered nature of normal traffic suggests greater diversity in feature representation, potentially requiring a more flexible model architecture to achieve high recall.

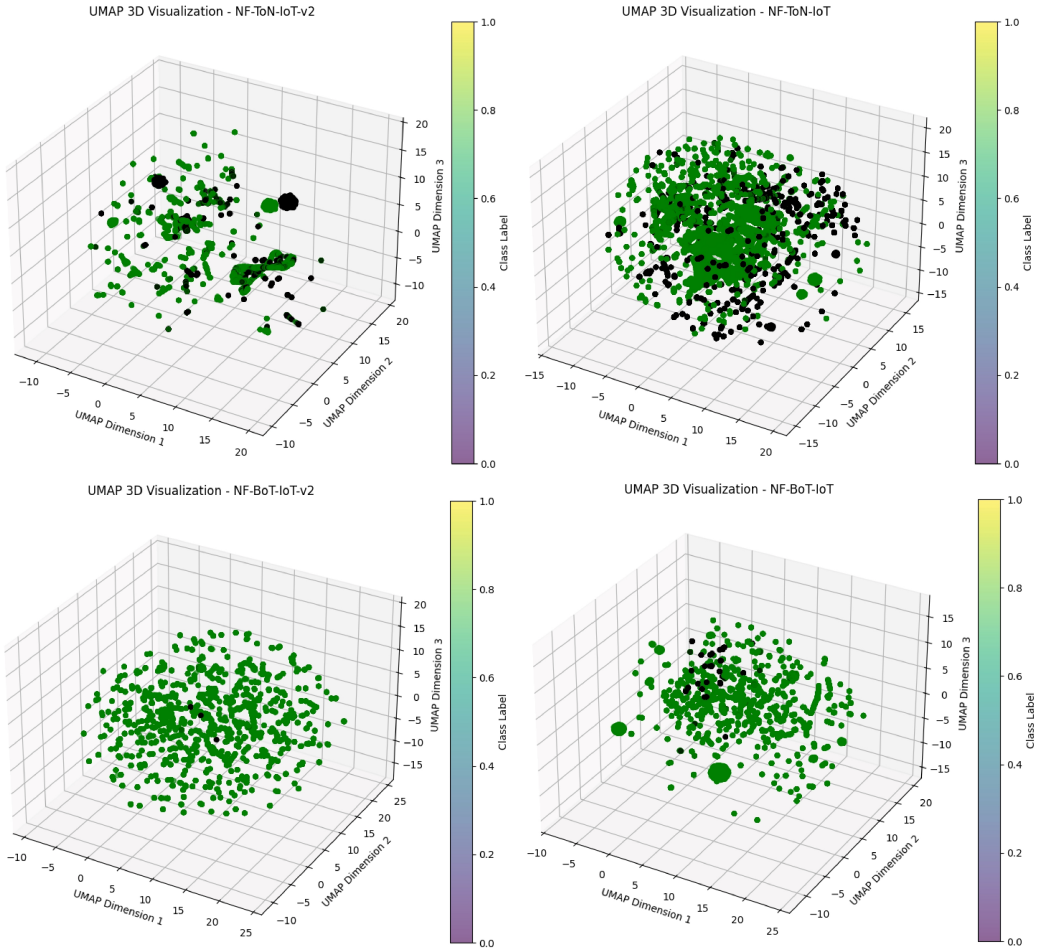

Figure 4. UMAP 3D visualization: dimensionality-reduction distribution of NF-BoT-IoT, NF-ToN-IoT, NF-BoT-IoT-v2, and NF-ToN-IoT-v2 datasets.

Cross-comparing datasets reveals that v2 versions exhibit more compact clusters for attack traffic compared to their original versions. This could indicate enhanced labeling or preprocessing that highlights distinguishing features. Enhanced labeling may involve better tagging of attack instances or more careful data cleaning, which leads to clearer distinctions between attack and normal traffic. Preprocessing steps such as feature scaling, noise reduction, or advanced data augmentation techniques might have contributed to this clearer separation, enabling the model to better capture the attack patterns. Analyzing such differences in feature distributions offers deeper insights into how the datasets influence the learning process and model generalization.

Figure 5 presents a radar chart comparing our model's performance with baseline methods. Notably, our model achieves the highest F1-score, accuracy, precision, and recall, particularly on the v2 datasets. The superior recall demonstrates the model's ability to detect diverse and complex attack types effectively. However, precision, while competitive, shows smaller margins of improvement. This suggests potential false positives, possibly due to overlapping feature spaces of attack and normal traffic. Such overlaps could be further analyzed by visualizing feature importance or model decision boundaries. Compared to traditional models, our method shows exceptional adaptability in handling imbalanced

datasets. For example, the significant improvement on NF-BoT-IoT-v2 highlights the robustness of the proposed architecture in capturing nuanced patterns in highly imbalanced traffic, where normal samples dominate.

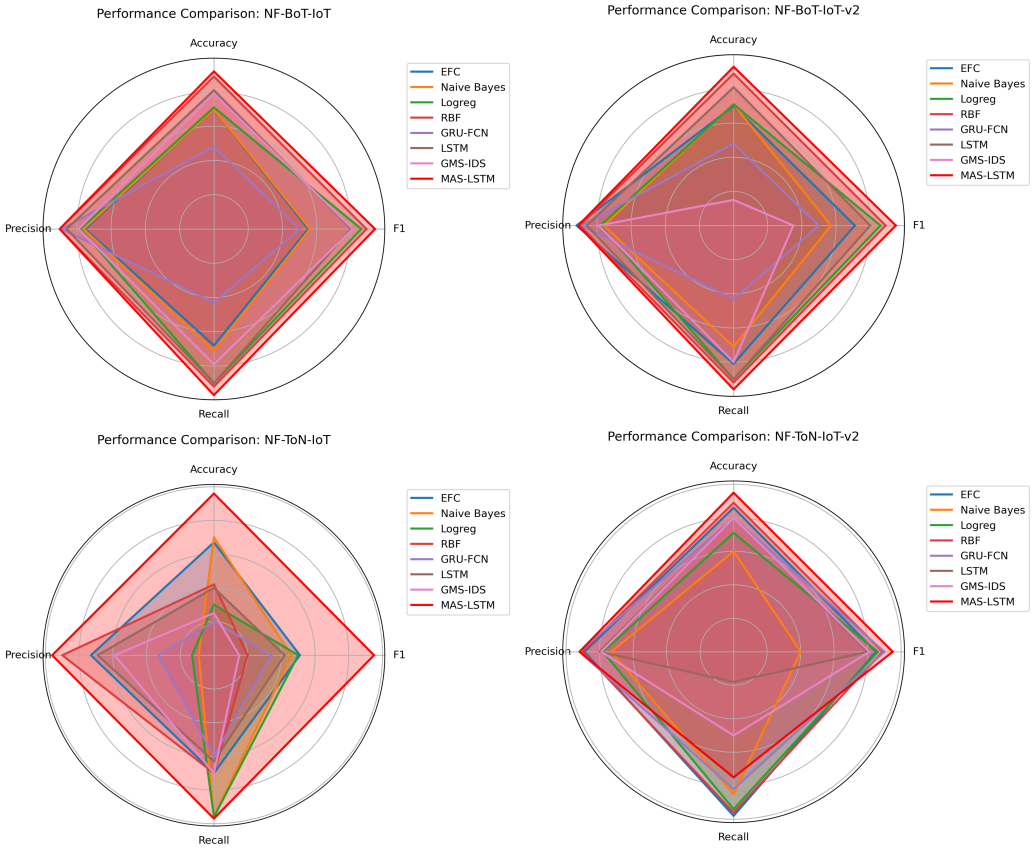

Figure 5. Radar chart: performance comparison of various models on NF-ToN-IoT and NF-BoT-IoT datasets and their v2 versions.

To gain further insights into model performance, we evaluated the impact of different hyperparameter settings, specifically the dropout rates and the number of LSTM hidden units. The combined results are shown in Figure 6.

The first experiment focused on the effect of dropout rates (0.1, 0.3, 0.5, and 0.7). The results reveal that the F1-score peaked at a dropout rate of 0.3, while higher rates (e.g., 0.7) led to a decline in performance. A deeper investigation indicates that excessive dropout may remove critical features required for accurate classification. By analyzing feature activation maps, we observed that lower dropout rates preserve key patterns in traffic data, contributing to improved recall and F1-score.

The second experiment evaluated the impact of the number of LSTM hidden units (50, 100, 150, and 250). Increasing the number of hidden units consistently improved recall and F1-score. However, the marginal gains diminished for larger hidden units (e.g., 250). This suggests that while larger hidden layers capture more complex patterns, they also introduce the risk of overfitting and increased computational costs. Analysis of model-training dynamics further revealed that larger hidden layers required more epochs to converge, underscoring the importance of balanced hyperparameter settings.

From these analyses, it is evident that the distinct distribution differences between normal and attack samples enable deep learning-based models to effectively extract critical features. The proposed multi-agent system leverages its modular architecture to better adapt to the heterogeneity of the datasets. The significant improvements on v2 datasets highlight the model's robustness and its ability to generalize across complex and high-

dimensional traffic scenarios. The comparison between v1 and v2 datasets reveals that the enhancements in labeling and preprocessing have improved the clarity of the attack traffic patterns, which in turn supports the learning process and boosts the model's performance on v2 datasets.

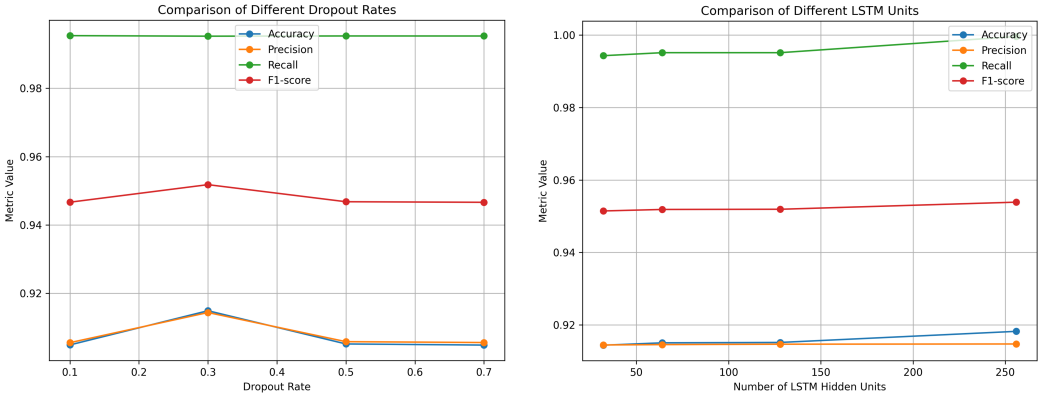

Figure 6. Impact of different dropout rates (**left**) and LSTM hidden units (**right**) on model performance.

4.5. Ablation Study

This section presents ablation experiments on two key components of our system: the LSTM module and the Agent module. We evaluate their individual contributions by examining configurations where only one module is active. The datasets used for this study, v1 and v2, represent integrated versions of the NF-BoT-IoT and NF-ToN-IoT datasets, respectively, with v2 incorporating more diverse and complex traffic patterns. Table 5 summarizes the results of these experiments.

Table 5. Ablation study comparing only lstm, only agent, and no voting on v1 and v2 datasets.

Model	**v1**				**v2**			
	Accuracy	**Precision**	**Recall**	**F1-Score**	**Accuracy**	**Precision**	**Recall**	**F1-Score**
MAS-LSTM	0.9823	0.9823	0.9996	0.9994	0.9904	0.9945	1.0000	0.9972
-LSTM	0.8246	0.8201	0.9804	0.8935	0.6382	0.5298	0.5431	0.5364
-Agent	0.8104	0.8145	0.9763	0.8873	0.8153	0.7623	0.7915	0.7767
-Voting	0.9051	0.9049	0.9923	0.9472	0.7894	0.4756	0.4798	0.4777

First, we examine the impact of the LSTM module in the absence of the Agent module (only lstm). On the simpler v1 dataset, the only lstm configuration achieves an F1-score of 0.8935, with a precision of 0.8201 and a recall of 0.9804, indicating that the LSTM alone can capture temporal dependencies reasonably well. However, on the more complex v2 dataset, the F1-score drops to 0.5364, highlighting that relying solely on LSTM for time-series modeling is insufficient when facing a broader variety of IoT traffic patterns and advanced attacks.

Next, we focus on retaining only the Agent module (only agent) while removing the LSTM. On v1, the performance is comparable to only lstm with an F1-score of 0.8873, suggesting that the Agent module alone can also learn certain relevant features. On v2, the only agent configuration achieves a slightly lower F1-score of 0.7767 compared to only lstm, implying that the agent-driven approach is less effective than LSTM in handling more diverse and complex traffic patterns. However, there remains a noticeable gap between only agent and the full system configuration, suggesting that Agent without LSTM-based temporal modeling is still suboptimal in handling the intricacies of high-dimensional network attacks.

We also include a configuration without the voting mechanism (no voting). This setup achieves an F1-score of 0.9472 on v1, reflecting its ability to integrate predictions effectively in simpler scenarios. However, on the more complex v2 dataset, its performance drops significantly to an F1-score of 0.4777, indicating that the absence of voting hinders its ability to generalize to diverse traffic patterns.

Finally, when both the LSTM and Agent modules are integrated, the system achieves near-perfect performance on v1 with an F1-score of 0.9994 and maintains an impressive F1-score of 0.9972 on v2. These results underscore that the synergy between the LSTM module's ability to capture temporal dependencies and the Agent module's specialized decision-making process is critical for robust detection in both simpler (v1) and more advanced (v2) IoT traffic scenarios.

5. Discussion

5.1. Bridging Anomaly-Detection Challenges

This study tackles the critical challenge of anomaly detection in Industrial Internet of Things (IIoT) networks, focusing on scalability, adaptability, and computational efficiency. By leveraging a multi-agent system (MAS) integrated with Long Short-Term Memory (LSTM) networks, MAS-LSTM demonstrates a robust capability to identify both rare and complex attack patterns. The evaluation across diverse datasets, such as NF-ToN-IoT and NF-BoT-IoT, underscores the system's practical applicability in industrial scenarios. These datasets, rich in attack vectors and traffic behaviors, enable MAS-LSTM to reflect real-world IIoT environments, such as smart factories and energy grids.

The findings resonate with prior research demonstrating the efficacy of LSTM models in modeling sequential data for IoT anomaly detection [59]. While traditional centralized approaches have been effective in detecting temporal anomalies, the proposed system's decentralized MAS architecture offers a distinct advantage by enhancing scalability and robustness. This modular design enables seamless handling of heterogeneous and large-scale traffic patterns.

Unlike conventional anomaly-detection techniques, which often struggle with diverse traffic behaviors, the proposed system's adaptability aligns with recent research advocating scalable and modular frameworks [60]. Moreover, our results complement findings from [61], which highlight the importance of diverse datasets in evaluating anomaly-detection systems. However, the reliance on labeled training data presents a notable limitation. While semi-supervised methods have mitigated this issue in related studies, the current framework's dependence on labeled data limits its generalizability to unseen attack patterns. Addressing this gap could pave the way for further advancements in scenarios with sparse labeled data availability.

5.2. Key Strengths of the MAS-LSTM

The integration of LSTM networks in the MAS architecture enables the system to effectively model the temporal dynamics of IoT traffic. This design is particularly advantageous for detecting sequential anomalies, such as coordinated DDoS attacks. Additionally, the MAS structure enhances scalability, allowing the system to process traffic from heterogeneous IIoT environments while maintaining high detection accuracy. This flexibility in scaling is critical for handling the diverse and growing traffic patterns in IIoT networks, where the volume and complexity of data can vary greatly.

The modular design is another significant strength, as it balances computational efficiency with performance. The ability to dynamically add or remove agents enhances adaptability, making MAS-LSTM suitable for rapidly evolving IoT ecosystems. As new devices are deployed, agents can be quickly integrated without disrupting the overall

system's performance, which is especially valuable in large-scale IIoT applications. Moreover, the diversity of datasets used in this study ensures the system's evaluation under realistic conditions, providing robust evidence for its application in practical industrial contexts, such as smart factories, energy grids, and healthcare systems. These contexts often involve heterogeneous devices with varying data characteristics, further proving the system's robustness and generalizability across different industries.

In terms of computational efficiency, MAS-LSTM demonstrates strong performance. The total training time for the system was 460.45 seconds, with an average training time of 0.000291 seconds per sample. Prediction times are also efficient, with a total prediction time of just 16.67 seconds and an average prediction time of 0.000042 seconds per sample. These results indicate that MAS-LSTM is capable of processing large-scale IoT data in real time, making it highly suitable for real-world applications that require both scalability and fast detection. Such efficiency ensures that MAS-LSTM can be deployed in real-time systems with stringent time requirements, like automated traffic monitoring in smart cities or real-time cybersecurity in critical infrastructure.

5.3. Limitations

Despite its strengths, MAS-LSTM faces several limitations that need to be addressed for more robust deployment in real-world IIoT environments.

The reliance on labeled training data limits the model's ability to generalize to unseen attack patterns, a challenge that has been frequently discussed in the literature [62]. In industrial settings, datasets often lack comprehensive labeling, especially for novel attack types, which can negatively affect the model's performance in real-world deployments. One potential solution to this limitation is to explore semi-supervised or unsupervised learning approaches, which are less dependent on large amounts of labeled data, or anomaly-detection methods that can identify new patterns without predefined labels. Moreover, incorporating techniques like few-shot learning or transfer learning could further alleviate the dependency on large labeled datasets by leveraging knowledge from related domains or tasks.

While the decentralized MAS architecture offers improved scalability, excessive partitioning of data among agents can diminish the global context available for anomaly detection. This issue becomes more pronounced when the attack behavior involves multiple agents, as in the case of complex, multi-stage attacks. This may result in reduced performance, particularly in the detection of complex attack scenarios, such as advanced persistent threats (APTs), where the attack activities span across multiple agents. Future research could focus on investigating collaborative learning techniques or cross-agent communication protocols to strike an optimal balance between scalability and global context awareness, thereby enhancing the detection capabilities for sophisticated attack types.

5.4. Future Directions

To address the current limitations, integrating semi-supervised and self-supervised learning methods presents a promising research avenue. These approaches can leverage unlabeled traffic data to enhance MAS-LSTM's anomaly-detection capabilities, particularly in scenarios with limited labeled data. Additionally, reinforcement learning could improve the system's adaptability by enabling agents to dynamically optimize decision-making processes. For instance, agents could learn to adjust detection thresholds or allocate resources in response to emerging attack patterns. Moreover, meta-learning techniques could enable the system to quickly adapt to new attack types with minimal retraining, improving its generalization across unseen scenarios.

The integration of graph neural networks (GNNs) with LSTM models offers another compelling direction, allowing the system to capture both spatial and temporal dependencies in IIoT traffic. This hybrid architecture could be effective in identifying distributed or coordinated attacks. Additionally, GNNs could enhance the system's understanding of network topologies, improving anomaly detection by considering device relationships. Federated learning could further enhance scalability and generalization by enabling agents to share insights while preserving data privacy, making the system more robust and adaptable across diverse industrial settings.

In terms of deployment, the integration of MAS-LSTM within existing IIoT infrastructures poses challenges, such as hardware constraints, legacy system compatibility, and real-time processing efficiency. Future research could explore optimizations like model pruning or edge AI techniques to reduce computational overhead, making MAS-LSTM more suitable for resource-constrained devices. Exploring low-latency processing strategies, such as edge computing, would also help improve anomaly-detection speed in environments requiring immediate responses. Compatibility with industrial communication protocols (e.g., MQTT, OPC UA) would facilitate easier integration with IIoT ecosystems.

Empirical validation through real-world IIoT testbeds or industry collaborations would help assess MAS-LSTM's performance in dynamic operational environments. Testing under varied network conditions—such as fluctuating data loads, cyber–physical interactions, and different levels of attack sophistication—would provide deeper insights into its robustness and adaptability. As IoT attacks continue to evolve, static datasets may no longer capture emerging threats. Future research should focus on dynamic datasets that are regularly updated to reflect new attack patterns, ensuring that MAS-LSTM remains effective against evolving cyber threats. Addressing these deployment challenges will facilitate the practical adoption of MAS-LSTM in real-world industrial applications.

6. Conclusions

This study presents a novel multi-agent anomaly-detection system tailored for Industrial Internet of Things (IIoT) networks, leveraging the temporal modeling capabilities of Long Short-Term Memory (LSTM) networks. The system was rigorously evaluated on multiple benchmark datasets, including NF-ToN-IoT, NF-BoT-IoT, and their v2 versions. The experimental results consistently demonstrate the system's superiority over existing methods, achieving strong performance across metrics such as accuracy, precision, recall, and F1-score.

The multi-agent architecture plays a key role in enhancing the system's scalability and robustness. By decentralizing the learning process, each agent specializes in different aspects of the data, effectively managing the heterogeneity inherent in IIoT traffic. The integration of LSTM networks further strengthens the system, enabling it to detect temporal patterns that characterize long-duration and subtle anomalies—patterns often missed by traditional models. This combination proves particularly effective in identifying complex attack scenarios, such as Distributed Denial-of-Service (DDoS) attacks and botnet behaviors.

The findings also highlight the significant contributions of the system's core components. The multi-agent framework ensures modularity and adaptability, while the LSTM-based temporal modeling provides the precision required to detect sequential anomalies. Together, these features form a robust foundation for anomaly detection in IIoT environments. However, challenges remain. The dependency on labeled data limits the system's applicability in real-world scenarios, where annotations are often scarce or incomplete. Addressing this limitation requires innovative approaches, such as leveraging semi-supervised learning and reinforcement learning, to enable the system to learn effectively from partially labeled or unlabeled data.

In conclusion, the proposed system represents a significant advancement in IIoT security, offering a scalable, adaptable, and effective solution for anomaly detection. Its ability to evolve with emerging attack strategies ensures its relevance in protecting increasingly complex and interconnected IIoT environments. This work lays a strong foundation for future research, paving the way for more intelligent, secure, and resilient IoT networks.

Author Contributions: Conceptualization, Z.Q., X.C. and H.Z.; methodology, Z.Q., Q.L. and X.N.; software, Q.L.; validation, H.Z. and C.U.I.W.; formal analysis, Z.Q.; investigation, Z.Q., X.C., Q.L. and X.N.; resources, X.C., H.Z. and C.U.I.W.; data curation, Q.L.; writing—original draft preparation, Z.Q., Q.L. and X.N.; writing—review and editing, X.C., H.Z. and C.U.I.W.; visualization, Q.L. and X.N.; supervision, H.Z. and X.C.; project administration, X.C. and H.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The implementation of the reinforcement learning algo-rithms discussed in this paper can be found in this repository: https://github.com/bitbitlemon/MAS-LSTM (accessed on 7 February 2025). The data set can be obtained from the following connections: https://staff.itee.uq.edu.au/marius/NIDS_datasets/ (accessed on 7 February 2025).

Acknowledgments: This paper is supported by Macao Polytechnic University (RP/FCHS-02/2022).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Hu, C.; Wang, W.; He, Q. A survey on security and privacy issues in edge computing-assisted Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 8115–8137.
2. Thamilarasu, G.; Chawla, S. Towards deep-learning-driven intrusion detection for the Internet of Things. *Sensors* **2019**, *19*, 1977. [CrossRef] [PubMed]
3. Fang, Y.; Xu, Y.; Pan, S.; Zhao, Y. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2020**, *107*, 164–174.
4. Inayat, U.; Zia, M.F.; Mahmood, S.; Khalid, H.M.; Benbouzid, M. Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects. *Electronics* **2022**, *11*, 1502. [CrossRef]
5. Tsiknas, K.; Taketzis, D.; Demertzis, K.; Skianis, C. Cyber threats to industrial IoT: A survey on attacks and countermeasures. *IoT* **2021**, *2*, 163–186. [CrossRef]
6. Dhirani, L.L.; Armstrong, E.; Newe, T. Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. *Sensors* **2021**, *21*, 3901. [CrossRef]
7. Qu, X.; Liu, Z.; Wu, C.Q.; Hou, A.; Yin, X.; Chen, Z. MFGAN: Multimodal Fusion for Industrial Anomaly Detection Using Attention-Based Autoencoder and Generative Adversarial Network. *Sensors* **2024**, *24*, 637. [CrossRef]
8. Liu, L.; Vollmer, T.; Manic, M. Neural network based intrusion detection system for critical infrastructures. In Proceedings of the 2009 International Joint Conference on Neural Networks, Atlanta, GA, USA, 14–19 June 2009; pp. 1827–1834.
9. Malhotra, P.; Vig, L.; Shroff, G.; Agarwal, P. Long short term memory networks for anomaly detection in time series. In *European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning (ESANN)*; 2015; pp. 89–94. Available online: https://paperswithcode.com/paper/long-short-term-memory-networks-for-anomaly (accessed on 26 February 2025).
10. Nguyen, V.Q.; Van Ma, L.; Kim, J. LSTM-based anomaly detection on big data for smart factory monitoring. *J. Digit. Contents Soc.* **2018**, *19*, 789–799.
11. Hsieh, R.-J.; Chou, J.; Ho, C.-H. Unsupervised online anomaly detection on multivariate sensing time series data for smart manufacturing. In Proceedings of the 2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA), Kaohsiung, Taiwan, 18–21 November 2019; pp. 90–97.
12. Dong, H.; Kotenko, I. Multi-task learning for IoT traffic classification: A comparative analysis of deep autoencoders. *Future Gener. Comput. Syst.* **2024**, *158*, 242–254. [CrossRef]
13. Liu, Q.; Wang, D.; Jia, Y.; Luo, S.; Wang, C. A multi-task based deep learning approach for intrusion detection. *Knowl.-Based Syst.* **2022**, *238*, 107852. [CrossRef]
14. Dong, H.; Kotenko, I. Multi-Task Learning Approach for Network Traffic Classification: A Comparative Analysis for Deep Auto Encoders. 2023. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4542930 (accessed on 5 February 2025).

15. Munir, M.; Chattha, M.A.; Dengel, A.; Ahmed, S. A comparative analysis of traditional and deep learning-based anomaly detection methods for streaming data. In Proceedings of the 2019 18th IEEE International Conference on Machine Learning and Applications (ICMLA), Boca Raton, FL, USA, 16–19 December 2019; pp. 561–566.
16. Stone, P.; Veloso, M. Multiagent systems: A survey from a machine learning perspective. *Auton. Robot.* **2000**, *8*, 345–383. [CrossRef]
17. García, N.M. Multi-agent system for anomaly detection in Industry 4.0 using Machine Learning techniques. *ADCAIJ Adv. Distrib. Comput. Artif. Intell. J.* **2019**, *8*, 33.
18. Rosenberger, J.; Urlaub, M.; Rauterberg, F.; Lutz, T.; Selig, A.; Bühren, M.; Schramm, D. Deep reinforcement learning multi-agent system for resource allocation in industrial Internet of Things. *Sensors* **2022**, *22*, 4099. [CrossRef] [PubMed]
19. Ullah, I.; Mahmoud, Q.H. Design and development of RNN anomaly detection model for IoT networks. *IEEE Access* **2022**, *10*, 62722–62750. [CrossRef]
20. Chen, Z.; Li, Z.; Huang, J.; Liu, S.; Long, H. An effective method for anomaly detection in industrial Internet of Things using XGBoost and LSTM. *Sci. Rep.* **2024**, *14*, 23969. [CrossRef]
21. Park, J.K.; Baek, Y. Real-Time Adaptive and Lightweight Anomaly Detection Based on a Chaotic System in Cyber–Physical Systems. *Electronics* **2025**, *14*, 598. [CrossRef]
22. Belay, M.A.; Blakseth, S.S.; Rasheed, A.; Salvo Rossi, P. Unsupervised Anomaly Detection for IoT-Based Multivariate Time Series: Existing Solutions, Performance Analysis and Future Directions. *Sensors* **2023**, *23*, 2844. [CrossRef]
23. Wu, Y.; Dai, H.-N.; Tang, H. Graph Neural Networks for Anomaly Detection in Industrial Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 9214–9231. [CrossRef]
24. Sommer, R.; Paxson, V. Outside the closed world: On using machine learning for network intrusion detection. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 16–19 May 2010; pp. 305–316.
25. Chandola, V.; Banerjee, A.; Kumar, V. Anomaly detection: A survey. *ACM Comput. Surv.* **2009**, *41*, 15. [CrossRef]
26. Ahmed, M.M.; Mahmood, A.N.; Hu, J. A survey of network anomaly detection techniques. *J. Netw. Comput. Appl.* **2016**, *60*, 19–31. [CrossRef]
27. Shone, N.; Nguyen, T.N.; Phai, V.D.; Shi, Q. A deep learning approach to network intrusion detection. *IEEE Trans. Emerg. Top. Comput. Intell.* **2018**, *2*, 41–50. [CrossRef]
28. He, Y.; Zhao, J. Temporal convolutional networks for anomaly detection in time series. *J. Phys. Conf. Ser.* **2019**, *1213*, 042050. [CrossRef]
29. Yassine, M.; Théo, F. Anomaly detection for industrial sensors using transformers. In Proceedings of the 2023 10th International Conference on Future Internet of Things and Cloud (FiCloud), Marrakesh, Morocco, 14–16 August 2023; pp. 167–174.
30. Zulfiqar, Z.; Malik, S.U.R.; Moqurrab, S.A.; Zulfiqar, Z.; Yaseen, U.; Srivastava, G. DeepDetect: An innovative hybrid deep learning framework for anomaly detection in IoT networks. *J. Comput. Sci.* **2024**, *83*, 102426. [CrossRef]
31. Sun, Q.; Chen, Z.; Liu, H. Application and Optimization of Multi-agent Reinforcement Learning in Collaborative Decision-Making. In *Cognitive Computing—ICCC 2024 (ICCC 2024), Proceedings of the 8th International Conference, Held as Part of the Services Conference Federation, SCF 2024, Bangkok, Thailand, 16–19 November 2024*; Xu, R., Chen, H., Wu, Y., Zhang, L.J., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2024; Volume 15426.
32. Belhadi, A.; Djenouri, Y.; Srivastava, G.; Lin, J.C.-W. Reinforcement learning multi-agent system for faults diagnosis of microservices in industrial settings. *Comput. Commun.* **2021**, *177*, 213–219. [CrossRef]
33. Ren, K.; Zeng, Y.; Zhong, Y.; Sheng, B.; Zhang, Y. MAFSIDS: A reinforcement learning-based intrusion detection model for multi-agent feature selection networks. *J. Big Data* **2023**, *10*, 137. [CrossRef]
34. Kheddar, H.; Dawoud, D.W.; Awad, A.I.; Himeur, Y.; Khan, M.K. Reinforcement-learning-based intrusion detection in communication networks: A review. *IEEE Commun. Surv. Tutor.* **2024** . [CrossRef]
35. Meshram, A.; Haas, C. Anomaly detection in industrial networks using machine learning: A roadmap. In *Machine Learning for Cyber-Physical Systems: Selected Papers from the International Conference ML4CPS 2016, Karlsruhe, 29 September 2016*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 65–72.
36. Wang, X.; Garg, S.; Lin, H.; Hu, J.; Kaddoum, G.; Piran, M.J.; Hossain, M.S. Toward Accurate Anomaly Detection in Industrial Internet of Things Using Hierarchical Federated Learning. *IEEE Internet Things J.* **2022**, *9*, 7110–7119. [CrossRef]
37. Sharma, P.; Sharma, S.K. A Survey on Anomaly Detection Techniques in IoT. In *Proceedings of Second Doctoral Symposium on Computational Intelligence*; Gupta, D., Khanna, A., Kansal, V., Fortino, G., Hassanien, A.E., Eds.; Advances in Intelligent Systems and Computing; Springer: Singapore, 2022; Volume 1374.
38. Ergen, T.; Kozat, S.S. Unsupervised Anomaly Detection With LSTM Neural Networks. *IEEE Trans. Neural Netw. Learn. Syst.* **2020**, *31*, 3127–3141. [CrossRef]
39. Lee, G.; Yoon, Y.; Lee, K. Anomaly Detection Using an Ensemble of Multi-Point LSTMs. *Entropy* **2023**, *25*, 1480. [CrossRef]
40. Lian, Z.; Su, C. Decentralized Federated Learning for Internet of Things Anomaly Detection. In Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, Nagasaki, Japan, 30 May–3 June 2022; ACM: New York, NY, USA, 2022; pp. 1249–1251.

41. Haldikar, S.V.; Kader, O.F.M.A.; Yekollu, R.K. Edge Computing and Federated Learning for Real-Time Anomaly Detection in Industrial Internet of Things (IIoT). In Proceedings of the 2024 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 24–26 April 2024; pp. 1699–1703.
42. Panait, L.; Luke, S. Cooperative multi-agent learning: The state of the art. *Auton. Agents Multi-Agent Syst.* **2005**, *11*, 387–434. [CrossRef]
43. Stefanova-Stoyanova, V.; Stankov, I. Multi-agent systems (MAS) in the area of IoT and using a model with Distributed Shared Memory system (DSM). In Proceedings of the 2020 XXIX International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 16–18 September 2020; pp. 1–4.
44. Zhang, W.; Yang, D.; Wu, W.; Peng, H.; Zhang, N.; Zhang, H.; Shen, X. Optimizing Federated Learning in Distributed Industrial IoT: A Multi-Agent Approach. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 3688–3703. [CrossRef]
45. Hao, W.; Yang, T.; Yang, Q. Hybrid statistical-machine learning for real-time anomaly detection in industrial cyber-physical systems. *IEEE Trans. Autom. Sci. Eng.* **2021**, *20*, 32–46. [CrossRef]
46. Eiteneuer, B.; Niggemann, O. LSTM for model-based anomaly detection in cyber-physical systems. *arXiv* **2020**, arXiv:2010.15680.
47. Moustafa, N. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. *Sustain. Cities Soc.* **2021**, *72*, 102994. [CrossRef]
48. Booij, T.M.; Chiscop, I.; Meeuwissen, E.; Moustafa, N.; den Hartog, F.T.H. ToN IoT—The role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion datasets. *IEEE Internet Things J.* **2021**, *9*, 485–496. [CrossRef]
49. Alsaedi, A.; Moustafa, N.; Tari, Z.; Mahmood, A.; Anwar, A. TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven Intrusion Detection Systems. *IEEE Access* **2020**, *8*, 165130–165150. [CrossRef]
50. Moustafa, N.; Keshk, M.; Debie, E.; Janicke, H. Federated TON_IoT Windows Datasets for Evaluating AI-Based Security Applications. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December 2020–1 January 2021; pp. 848–855.
51. Moustafa, N.; Ahmed, M.; Ahmed, S. Data Analytics-Enabled Intrusion Detection: Evaluations of ToN_IoT Linux Datasets. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December 2020–1 January 2021; pp. 727–735.
52. Moustafa, N. New Generations of Internet of Things Datasets for Cybersecurity Applications based Machine Learning: TON_IoT Datasets. In Proceedings of the eResearch Australasia Conference, Brisbane, Australia, 21–25 October 2019.
53. Moustafa, N. A systemic IoT-Fog-Cloud architecture for big-data analytics and cyber security systems: A review of fog computing. *arXiv* **2019**, arXiv:1906.01055.
54. Ashraf, J.; Keshk, M.; Moustafa, N.; Abdel-Basset, M.; Khurshid, H.; Bakhshi, A.D.; Mostafa, R.R. IoTBoT-IDS: A Novel Statistical Learning-enabled Botnet Detection Framework for Protecting Networks of Smart Cities. *Sustain. Cities Soc.* **2021**, *72*, 103041. [CrossRef]
55. Cox, D.R. The regression analysis of binary sequences. *J. R. Stat. Soc. Ser. B (Methodol.)* **1958**, *20*, 215–232. [CrossRef]
56. Lewis, D.D. Naive (Bayes) at forty: The independence assumption in information retrieval. In *Machine Learning: ECML-98, Proceedings of the 10th European Conference on Machine Learning, Chemnitz, Germany, 21–23 April 1998*; Springer: Berlin/Heidelberg, Germany, 1998; pp. 4–15.
57. Hinton, G.E.; Salakhutdinov, R.R. Reducing the dimensionality of data with neural networks. *Science* **2006**, *313*, 504–507. [CrossRef]
58. Broomhead, D.S.; Lowe, D. *Radial Basis Functions, Multi-Variable Functional Interpolation and Adaptive Networks*; Royal Signals and Radar Establishment: Malvern, UK, 1988; Volume 4148.
59. Doe, J.; Smith, J. Sequential Anomaly Detection in IoT Networks Using LSTM. *J. IoT Res.* **2022**, *15*, 321–335.
60. Lee, M.; Zhang, W. Modular and Scalable Anomaly Detection for Industrial IoT. *IEEE Trans. Ind. Inform.* **2023**, *18*, 1234–1245.
61. Ahmed, A.; Wang, Y. Benchmarking Anomaly Detection Systems Using Diverse IoT Datasets. *ACM Trans. IoT* **2021**, *12*, 98–112.
62. Brown, E.; Gupta, R. Overcoming Labeled Data Limitations in Anomaly Detection. *Mach. Learn. IoT* **2020**, *10*, 45–60.