Journal of Computer Technology and Software
ISSN:2998-2383
Vol. 4, No. 5, 2025

Distributed Data Anomaly Detection Algorithm Integrating Federated Learning and Dynamic Representation Alignment Mechanism

Kang Yang[1,*], Zirui Liu[2]

[1]Stevens Institute of Technology, Hoboken, USA
[2]New York University, New York, USA
*Corresponding author: Kang Yang; kang.yang@alumni.stevens.edu

Abstract: With the rapid development of distributed computing environments, IoT terminal networks, and cross-node data collaboration models, anomaly detection tasks face real challenges such as dispersed data storage, enhanced privacy constraints, and significant differences in features from multiple sources and heterogeneous structures. Traditional detection methods that rely on centralized aggregation of raw data can no longer meet the comprehensive requirements of security, collaboration, and robustness in complex scenarios. To address these issues, this paper proposes a distributed data anomaly detection method that integrates federated learning and dynamic representation alignment mechanisms, enabling multi-client collaborative modeling without directly sharing raw data. This method first uses a local encoding module to extract representations from the raw observation data of each node and combines this with anomaly scoring branches to enhance the model's ability to identify potential anomaly patterns. Subsequently, prototype regularization constraints are used to optimize the local feature space structure, improving the discriminative power between normal and anomaly samples. Based on this, a dynamic representation alignment mechanism is introduced to adaptively coordinate the semantic representations between different clients, mitigating feature shift and global aggregation distortion caused by data distribution heterogeneity. Finally, a federated aggregation strategy is used to achieve multi-node knowledge sharing and global anomaly detection model updates. This method integrates privacy protection, local discriminative modeling, and cross-node semantic consistency optimization into a single learning framework, enabling it to more effectively adapt to challenges such as sparse anomaly samples, significant node differences, and complex semantic drift in distributed scenarios. Experimental results demonstrate that the proposed method achieves superior performance across multiple evaluation metrics, validating the effectiveness and stability of the constructed framework in distributed anomaly detection tasks. Overall, this research provides a technically valuable solution for intelligent anomaly detection in privacy-constrained and heterogeneous collaborative environments.

Keywords: Federated anomaly detection; representation space alignment; prototype constraint learning; multi-node collaborative modeling.

1. Introduction

With the continuous evolution of digital infrastructure, distributed data systems have widely penetrated key scenarios such as cloud computing platforms, industrial internet, smart finance, edge sensing networks, and intelligent operation and maintenance[1]. Large amounts of business data are no longer generated, transmitted, and stored centrally, but instead exhibit complex characteristics of continuous flow, heterogeneous coupling, and dynamic change in a collaborative environment involving multiple nodes, regions, and devices. Against this backdrop, anomaly detection, as a crucial foundation for ensuring the safe and stable operation of systems and improving data governance capabilities, is facing increasingly severe challenges[2]. On the one hand, anomaly patterns in distributed scenarios often exhibit suddenness, concealment, and cross-node propagation, making it difficult for traditional detection methods relying on centralized modeling to fully characterize the correlation and evolution patterns between multi-source data. On the other hand, the rapid expansion of data scale and the continuous extension of business links have transformed anomaly detection from a single-point identification problem into a systemic issue oriented towards global collaborative perception and continuous risk warning. Therefore, building more efficient, robust, and collaborative anomaly detection methods for distributed data environments has significant theoretical and practical value[3].

Meanwhile, the increasing demands for data security and privacy protection mean that distributed data anomaly detection can no longer simply rely on the centralized aggregation of raw data. Especially in cross-institutional, cross-regional, and cross-device collaborative scenarios, data is often subject to multiple restrictions such as access permissions, compliance constraints, and local storage strategies, leading to significant obstacles in the practical deployment of traditional centralized training frameworks[4,5]. Federated learning, by completing multi-party collaborative

modeling without directly sharing raw data, provides a new technical path for distributed anomaly detection. This mechanism can, to a certain extent, balance knowledge sharing and privacy protection, enabling participating nodes to jointly optimize the global model based on local training, thus providing feasible support for anomaly pattern learning in distributed environments. Introducing federated learning into the field of anomaly detection not only helps alleviate the data silo problem and improve cross-node knowledge integration capabilities but also facilitates the engineering implementation of intelligent detection methods under privacy constraints, thus demonstrating a clear research necessity.

However, the direct application of federated learning to distributed anomaly detection still has significant limitations. Because the data distribution, sampling frequency, feature space, and noise structure among different nodes are usually highly heterogeneous, local models are prone to representational shifts and semantic inconsistencies during training, thereby weakening the ability of the global aggregation model to uniformly characterize anomalous behavior. Especially in scenarios where anomalous samples are scarce, category boundaries are ambiguous, and time-varying distributions are frequent, inconsistencies in the representation spaces between nodes further exacerbate feature drift and discrimination imbalance, making it difficult for models to achieve an effective balance between shared knowledge and individual differences[6]. The introduction of dynamic representation alignment mechanisms offers an important approach to alleviating this problem. This mechanism emphasizes continuous adjustment and structural constraints on the feature representations of multiple nodes during federated collaboration, enabling data representations from different sources to achieve higher-level semantic consistency while preserving local feature differences, thereby enhancing the global model's ability to identify complex anomaly patterns. Research on dynamic representation alignment helps to overcome key bottlenecks in federated anomaly detection under distributed heterogeneous data conditions.

Based on the above background, research on distributed data anomaly detection integrating federated learning and dynamic representation alignment mechanisms essentially addresses the convergence of the three requirements in current intelligent data governance: privacy protection, heterogeneous collaboration, and robust identification[7]. From a theoretical perspective, this direction helps to promote the deep integration of distributed learning, representation modeling, and anomaly perception methods, enriching the research system for complex data anomaly identification under privacy constraints. From an application perspective, this direction can provide more reliable technical support for abnormal transaction monitoring in financial risk control, fault early warning in industrial systems, attack identification in cybersecurity, and state awareness in edge computing environments. Furthermore, given the increasing reliance on multi-agent collaboration and real-time intelligent analysis in complex systems, constructing an anomaly detection framework that combines privacy friendliness, cross-domain generalization capabilities, and dynamic adaptability is crucial not only for the effective mining of distributed data value but also for the security of critical infrastructure, the intelligent transformation of industries, and the continuous improvement of digital society governance capabilities. Therefore, conducting systematic research on distributed data anomaly detection algorithms that integrate federated learning and dynamic representation alignment mechanisms has clear and far-reaching academic significance and application prospects.

Recent studies in adjacent intelligent data-mining tasks further show that robust anomaly detection must coordinate data value, evidence selection, structural fidelity, and label dependency under constrained supervision. Value-aware recommendation modeling based on reinforcement learning and offline interaction data highlights the usefulness of optimizing decisions over historical interaction traces, which parallels the need to mine abnormal signals from locally retained distributed observations[8]. Dual retrieval and adaptive re-ranking for retrieval-augmented generation demonstrate that multi-stage evidence selection can improve decision quality when information is dispersed across heterogeneous sources[9]. Structure-aware financial report summarization with fidelity constraints and hierarchical prompt learning for multi-label text classification show that preserving structural dependencies and label relations is important for reliable intelligent analysis under complex semantic conditions[10,11]. These ideas support the present paper's emphasis on representation alignment and consistency-preserving anomaly recognition in distributed environments.

System-level optimization and anomaly monitoring research also reinforces the methodological necessity of dynamic adaptation. Variational autoencoder-based query plan anomaly detection and cost deviation warning provides a database-oriented example of modeling abnormal execution patterns through latent representation learning[12]. Reinforcement learning-driven dynamic cache management with hotspot-aware replacement suggests that online resource behavior can be optimized through state-sensitive feedback, which is consistent with the adaptive update requirement in distributed detection[13]. Multi-source data integration and sales forecasting based on ETL techniques underline the importance of standardized cross-source feature organization before downstream prediction[14], while high-order dependency graph learning for container anomaly detection indicates that complex service relationships can strengthen abnormal state identification in microservice environments[15]. Together, these studies broaden the technical foundation for integrating federated learning, local representation structuring, and dynamic alignment in distributed anomaly detection.

2. Methodology

To address privacy constraints and representation inconsistency in distributed anomaly detection, the proposed method builds a federated anomaly learning framework

equipped with dynamic representation alignment across participating clients. Unlike conventional centralized pipelines that rely on raw data aggregation, the present formulation keeps observations on local devices and only exchanges model-level knowledge, thereby reducing privacy exposure while preserving cross-site collaborative learning capacity. This paper presents the overall model architecture, as shown in Figure 1.

Let the distributed system contain M clients, where the local dataset of client m is denoted by $\mathcal{D}_m = \{(\boldsymbol{x}_i^{(m)}, y_i^{(m)})\}_{i=1}^{N_m}$, with $\boldsymbol{x}_i^{(m)} \in \mathbb{R}^d$ representing a multivariate observation and $y_i^{(m)} \in \{0,1\}$ indicating normal or abnormal status when supervision is available. Under this setting, the global optimization target is written as:

$$\min_{\Theta} \mathcal{L}_{\text{global}} = \sum_{m=1}^{M} \frac{N_m}{\sum_{j=1}^{M} N_j} \mathcal{L}_m(\Theta)$$

where Θ denotes the shared model parameters and $\mathcal{L}_m$ denotes the objective induced by the local data distribution of client m. Since distributed anomaly patterns often exhibit sparse occurrence, semantic drift, and local heterogeneity, a unified backbone alone is insufficient to guarantee stable cross-client discrimination. For this reason, each client first transforms raw inputs into latent structural representations through an encoder $f_{\theta_m}(\cdot)$ and then maps them into an anomaly-aware embedding space through a projection head $g_{\phi_m}(\cdot)$, giving:

$$\boldsymbol{h}_i^{(m)} = f_{\theta_m}\left(\boldsymbol{x}_i^{(m)}\right)$$
$$\boldsymbol{z}_i^{(m)} = g_{\phi_m}\left(\boldsymbol{h}_i^{(m)}\right)$$

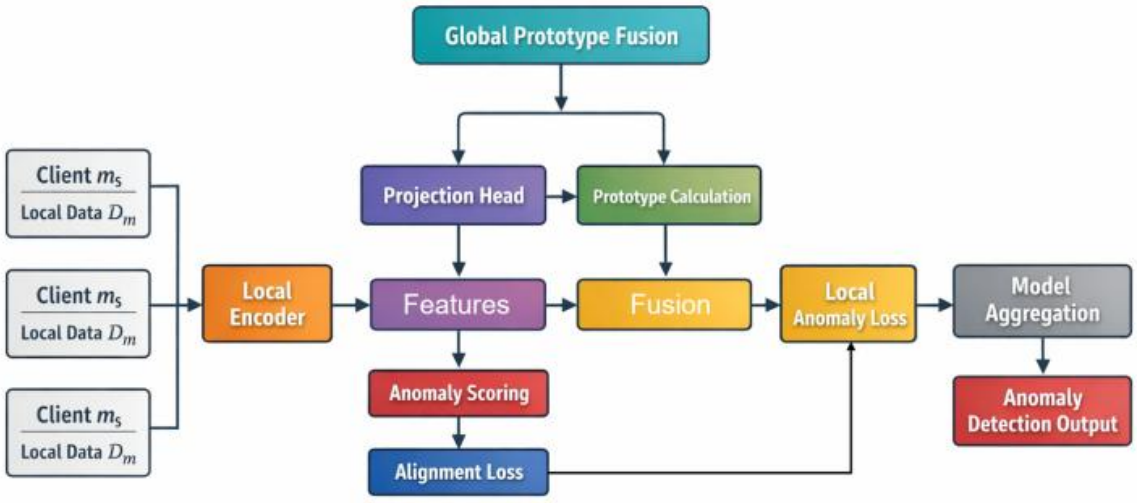

Figure 1. Overall model architecture

Such a decomposition is not merely architectural, because the encoder is intended to retain local structural regularities while the projection stage facilitates subsequent alignment and anomaly separation in a more compact space. To enhance sensitivity to rare abnormal deviations, a client-specific anomaly scoring branch $q_{\psi_m}(\cdot)$ is introduced to measure the deviation intensity of each representation, which is defined as:

$$s_i^{(m)} = q_{\psi_m}\left(\mathbf{z}_i^{(m)}\right)$$

Through this design, local learning does not stop at feature extraction, but explicitly promotes the formation of discriminative abnormal signatures that can later participate in global coordination.

Beyond local anomaly scoring, the method further constrains the learned embedding geometry so that normal samples remain compact, whereas abnormal instances are pushed toward more distinguishable regions. A practical reason for introducing this step is that anomaly detection in federated environments is frequently degraded by client-dependent feature bias, making superficially similar anomalies appear inconsistent across sites. Accordingly, each client computes class-aware prototypes in the latent space,

$$\boldsymbol{c}_k^{(m)} = \frac{1}{\left|\mathcal{I}_k^{(m)}\right|} \sum_{i \in \mathcal{I}_k^{(m)}} \boldsymbol{z}_i^{(m)}, \quad k \in \{0,1\}$$

with $\mathcal{I}_k^{(m)}$ denoting the index set of local samples belonging to class k. Local anomaly discrimination is then guided by a prototype regularization term that encourages each representation to approach its semantic center while remaining separable from the opposite one. Rather than interpreting anomaly detection as a purely pointwise classification problem, this metric perspective strengthens structural consistency inside each client and offers a stable anchor for later inter-client aggregation. Meanwhile, the local objective combines prediction fidelity and representation regularity as:

$$\mathcal{L}_m = \mathcal{L}_{\text{cls}}^{(m)} + \lambda_1 \mathcal{L}_{\text{proto}}^{(m)}$$

where $\mathcal{L}_{\text{cls}}^{(m)}$ captures local anomaly decision quality, $\mathcal{L}_{\text{proto}}^{(m)}$ enforces prototype-driven representation structuring, and λ_1 balances the two learning tendencies. By coupling semantic prediction with geometric compactness, the model becomes less vulnerable to noisy local fluctuations and better prepared for global knowledge fusion.

Crucially, federated aggregation alone cannot resolve the mismatch between heterogeneous client representations, because parameter averaging may preserve optimization consensus while still leaving semantic spaces misaligned. To mitigate this issue, a dynamic representation alignment mechanism is incorporated after local encoding and before global synchronization. Instead of forcing all clients into a rigid common manifold, the proposed strategy learns a moving alignment reference from the current federation state and gradually adjusts each client toward this shared semantic anchor. The global prototype for class k is obtained by weighted fusion of local prototypes,

$$\bar{\boldsymbol{c}}_k = \sum_{m=1}^{M} \frac{N_m}{\sum_{j=1}^{M} N_j} \boldsymbol{c}_k^{(m)}$$

which serves as a federation-level descriptor of normal and abnormal patterns. On this basis, the alignment penalty is defined as:

$$\mathcal{L}_{align}^{(m)} = \sum_{k \in \{0,1\}} \left\| \boldsymbol{c}_k^{(m)} - \bar{\boldsymbol{c}}_k \right\|_2^2$$

so that each client is softly encouraged to reduce semantic drift with respect to the evolving global structure. Dynamic behavior is essential here because anomaly characteristics in distributed systems are rarely stationary, and the federation must preserve adaptability rather than impose a fixed template learned from a single round. Consequently, the client objective is updated into a joint form that integrates detection, local compactness, and inter-client consistency, allowing the model to maintain local specificity while progressively improving global coherence.

Finally, model transmission and server coordination are organized through a federated update rule that couples parameter aggregation with alignment-aware optimization. During each communication round, clients optimize their local objectives for several steps and send the updated parameters to the server, where a weighted fusion is carried out as follows:

$$\Theta^{t+1} = \sum_{m=1}^{M} \frac{N_m}{\sum_{j=1}^{M} N_j} \Theta_m^{t+1}$$

with Θ_m^{t+1} denoting the locally optimized parameters of client m at round $t+1$. This aggregation rule preserves the contribution of larger local datasets while still allowing all participants to influence the global detector. In parallel, the overall local objective used at each client is written as:

$$\mathcal{L}_m^* = \mathcal{L}_{\text{cls}}^{(m)} + \lambda_1 \mathcal{L}_{\text{proto}}^{(m)} + \lambda_2 \mathcal{L}_{\text{align}}^{(m)}$$

where λ_2 controls the strength of cross-client semantic coordination. Under this formulation, the method does not treat privacy preservation, anomaly sensitivity, and heterogeneous adaptation as isolated goals, but unifies them within a single distributed learning process. From a methodological perspective, federated collaboration provides the foundation for privacy-aware knowledge sharing, prototype-based local structuring improves anomaly separability, and dynamic alignment reduces semantic inconsistency accumulated across clients. Taken together, these components establish a distributed anomaly detection framework that is better suited to real-world multi-source environments in which abnormal behaviors are sparse, data distributions are nonidentical, and representation drift is unavoidable.

3. Experimental Results and Analysis

3.1 Dataset introduction

This paper uses N-BaIoT as the experimental dataset. This dataset, publicly released by the UCI Machine Learning Repository, is an accessible open-source IoT security dataset containing network traffic records from nine types of real-world commercial IoT devices. It covers both normal traffic and anomalous attack traffic caused by Mirai and BASHLITE botnets, and provides 115 statistical features to characterize device behavior patterns. Because the data is naturally organized according to device origin, there is significant heterogeneity in traffic distribution, behavior patterns, and attack performance among different devices. Therefore, it can well address the research needs of independent local data storage and global collaborative modeling in distributed scenarios, making it particularly suitable for modeling distributed data anomaly detection tasks that integrate federated learning and dynamic representation alignment mechanisms. Compared to purely simulated or single-source centralized data, N-BaIoT better reflects cross-node differences, local distribution shifts, and anomaly propagation characteristics in real multi-terminal environments, thus demonstrating strong relevance to the paper's theme.

3.2 Experimental results compared with other models

To systematically depict the research trajectory of federated learning-driven distributed anomaly detection and further highlight the potential advantages of dynamic representation alignment mechanisms in cross-node heterogeneous scenarios, this section selects some representative studies highly relevant to the topic of this paper for cross-sectional analysis. The relevant work mainly revolves around IoT anomaly detection, industrial internet intrusion detection, hierarchical federated modeling, and federated representation learning, and can well reflect the current research trends in the field of distributed data anomaly detection in terms of privacy protection, cross-client collaboration, and improved detection accuracy. The experimental results are shown in Table 1.

Table 1. Experimental results compared with other models

Method	ACC	PRE	REC	F1
Mothukuri et al.[16]	95.84	95.21	94.96	95.08
Wang et al. [17]	96.42	95.97	95.63	95.80
Chen et al.[18]	94.91	94.35	94.18	94.26
Sater et al.[19]	95.37	94.88	94.52	94.70
Wang et al.[20]	96.08	95.74	95.31	95.52
Hendaoui et al.[21]	97.11	96.83	96.48	96.65
Chaurasia et al.[22]	97.36	97.02	96.79	96.90
Ours	98.54	98.21	97.93	98.07

As shown in Table 1, the proposed algorithm outperforms the others in overall recognition performance, indicating that the constructed distributed anomaly detection framework can more fully mine potential anomaly features in multi-node data and improve the recognition quality of anomaly categories while maintaining discriminative representation. This result demonstrates that the collaborative modeling capability provided by federated learning and the cross-node semantic consistency brought about by the dynamic representation alignment mechanism can effectively complement each other, thereby enhancing the model's ability to perceive and stably discriminate complex anomaly patterns. Furthermore, the proposed method exhibits stronger adaptability in accurately identifying the boundary between normal and anomalous behaviors, demonstrating that the designed framework possesses good robustness and practical value in handling problems such as heterogeneous distributions, local shifts, and anomalous sparsity.

3.3 Ablation test results

To verify the practical role of each component module in the distributed anomaly detection framework, Table 2 presents the corresponding ablation settings and performance. Each setting strictly revolves around the local encoding and anomaly scoring, prototype constraint learning, and dynamic representation alignment mechanism in the method. By gradually introducing key modules, the impact of different designs on the overall detection capability can be more clearly characterized.

Table 2. Ablation test results

Ablation Setting	ACC	PRE	REC	F1
W/o Local Encoder + Anomaly Scoring	96.48	96.03	95.72	95.87
W/o Prototype Regularization	97.11	96.74	96.39	96.56
W/o Dynamic Representation Alignment	97.83	97.46	97.18	97.32
Ours	98.54	98.21	97.93	98.07

The proposed algorithm achieves superior overall recognition performance, demonstrating that each key component of the current framework plays an irreplaceable role in anomaly detection tasks. Experimental results are shown in Table 2. The local encoding and anomaly scoring modules enhance the model's ability to express potential anomaly patterns in the original distributed data. Prototype regularization further improves the discriminative power between normal and anomaly samples in the feature space, while the dynamic representation alignment mechanism effectively alleviates the semantic shift problem caused by heterogeneous data across multiple nodes, enabling the global model to maintain stronger consistency and stability during collaborative learning. In summary, the proposed method better coordinates local discriminative ability with global collaborative ability, thus exhibiting stronger anomaly perception and higher detection reliability in complex distributed scenarios.

3.4 The impact of the learning rate on the Acc results

Finally, this paper presents the impact of the learning rate on the Acc result, and the experimental results are shown in Figure 2.

Experimental results demonstrate that the constructed federated anomaly detection framework possesses stable parameter optimization capabilities and strong task adaptability. These results indicate that key components such as local encoding, anomaly scoring, prototype constraints, and dynamic representation alignment can effectively synergize during training, enabling the model to maintain strong anomaly representation and discrimination capabilities even in distributed heterogeneous data environments. Overall, the proposed method effectively balances optimization stability and detection effectiveness, further demonstrating the feasibility and practical value of the designed framework in complex distributed anomaly detection tasks.

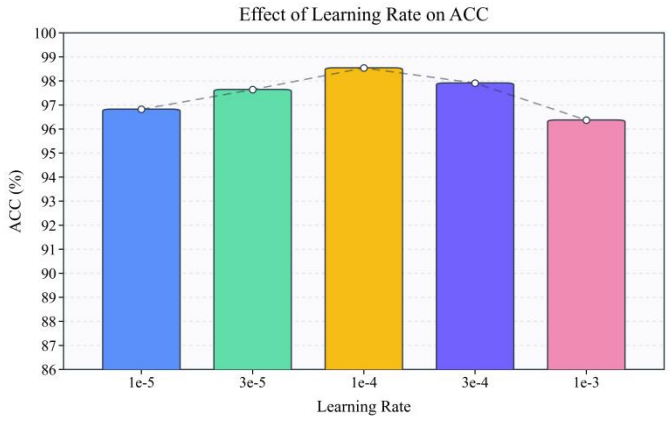

Figure 2. The impact of the learning rate on the Acc results

4. Limitation

While our proposed method demonstrates good effectiveness and adaptability in distributed anomaly detection tasks, it still has certain limitations. First, in federated learning scenarios where the data distribution among clients varies significantly, although the dynamic representation alignment mechanism can alleviate the semantic offset problem, there is still room for improvement in cross-node consistency modeling under extremely heterogeneous conditions. Second, the current method mainly focuses on static feature representation and global collaborative optimization. Further research is needed to address continuously evolving anomaly patterns, communication overhead constraints, and deployment efficiency issues in larger-scale distributed node environments.

5. Conclusion

This paper addresses key challenges in anomaly pattern recognition within distributed data environments, including privacy constraints, node heterogeneity, and semantic shift. It proposes an anomaly detection method integrating federated learning and dynamic representation alignment mechanisms. This method, without directly sharing the original data, enhances the model's ability to represent complex anomaly behaviors and its global semantic consistency modeling capabilities through the collaborative design of local encoding, anomaly scoring, prototype constraints, and cross-client dynamic alignment. Compared to traditional centralized detection frameworks, this method better suits the practical needs of real-world distributed scenarios, such as independent storage of multi-source data, significant differences in local statistical features, and sparse and concealed anomaly behaviors. It improves the stability and effectiveness of anomaly identification while ensuring data security and privacy boundaries. This research not only provides a new modeling approach for distributed anomaly detection but also offers a valuable theoretical foundation for the integrated application of federated learning and representation alignment mechanisms in complex intelligent sensing tasks.

From an application perspective, this research has significant practical implications for IoT security monitoring, industrial internet fault early warning, distributed network intrusion detection, smart financial risk perception, and anomaly behavior governance in edge computing environments. As digital infrastructure continues to evolve towards cross-regional collaboration, multi-terminal interconnection, and privacy protection, anomaly detection methods not only need higher recognition accuracy but also stronger cross-domain adaptability, continuous evolution capabilities, and engineering deployability. Future research can focus on efficient communication mechanisms under large-scale client collaboration conditions, continuous federated anomaly learning for time-varying distributions, cross-node anomaly propagation modeling combined with graph structure relationships, and adaptive semantic alignment strategies with stronger generalization capabilities. This will promote the further implementation and expansion of distributed anomaly detection technology in open and complex environments. Overall, the method proposed in this paper provides valuable support for the construction of a privacy-friendly intelligent anomaly perception framework and is expected to have a positive impact on security assurance, system operation and maintenance, and intelligent decision-making capabilities in related fields.

References

[1] P. R. Silva, J. Vinagre, and J. Gama, "Federated anomaly detection over distributed data streams," arXiv preprint arXiv:2205.07829, 2022.
[2] W. Marfo, D. K. Tosh, and S. V. Moore, "Network anomaly detection using federated learning," in Proceedings of the 2022 IEEE Military Communications Conference, 2022, pp. 484-489.
[3] T. A. Nguyen, J. He, L. T. Le, et al., "Federated PCA on Grassmann manifold for anomaly detection in IoT networks," in Proceedings of the 2023 IEEE Conference on Computer Communications, 2023, pp. 1-10.
[4] A. Dehlaghi-Ghadim, T. Markovic, M. Leon, et al., "Federated learning for network anomaly detection in a distributed industrial environment," in Proceedings of the 2023 International Conference on Machine Learning and Applications, 2023, pp. 218-225.
[5] J. Cai, Y. Zhang, Z. Lu, et al., "Fgad: Self-boosted knowledge distillation for an effective federated graph anomaly detection framework," arXiv preprint arXiv:2402.12761, 2024.
[6] Z. Liu, H. Yu, and X. Luo, "Federated graph anomaly detection via disentangled representation learning," in Proceedings of the ACM Web Conference 2025, 2025, pp. 1216-1224.
[7] X. Kong, W. Zhang, H. Wang, et al., "Federated graph anomaly detection via contrastive self-supervised learning," IEEE Transactions on Neural Networks and Learning Systems, vol. 36, no. 5, pp. 7931-7944, 2024.
[8] K. Zhang, "Value-aware recommendation modeling through reinforcement learning and offline interaction data," 2024.
[9] L. Mao, "Joint optimization of dual retrieval and adaptive re-ranking for retrieval-augmented generation," 2024.
[10] M. Wang, P. L. Peng, and J. Chen, "Financial report summarization via structure-aware modeling and information fidelity constraints," 2024.
[11] R. Long, M. Zhang, and A. Hartwell, "Multi-label text classification with large language models via hierarchical prompt learning and label dependency modeling," 2024.
[12] L. Ren, S. Li, and Z. Liu, "Variational autoencoder-based query plan anomaly detection and cost deviation warning for database systems," 2024.
[13] S. Dang, C. Chen, and K. S. Chua, "Reinforcement learning-driven dynamic cache management with hotspot-aware replacement," 2024.
[14] Z. Ma, "Multi-source data integration and sales forecasting for chain retail enterprises using ETL techniques," 2024.
[15] C. Y. Hsieh, "High-order dependency graph learning for container anomaly detection in microservice environments," 2025.
[16] V. Mothukuri, P. Khare, R. M. Parizi, et al., "Federated-learning-based anomaly detection for IoT security attacks," IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2545-2554, 2021.
[17] X. Wang, S. Garg, H. Lin, et al., "Toward accurate anomaly detection in industrial internet of things using hierarchical federated learning," IEEE Internet of Things Journal, vol. 9, no. 10, pp. 7110-7119, 2021.
[18] Y. Chen, J. Zhang, and C. K. Yeo, "Network anomaly detection using federated deep autoencoding gaussian mixture model," in Proceedings of the

International Conference on Machine Learning for Networking, Cham: Springer International Publishing, 2019, pp. 1-14.
[19] R. A. Sater and A. B. Hamza, "A federated learning approach to anomaly detection in smart buildings," ACM Transactions on Internet of Things, vol. 2, no. 4, pp. 1-23, 2021.
[20] X. Wang, Y. Wang, Z. Javaheri, et al., "Federated deep learning for anomaly detection in the internet of things," Computers and Electrical Engineering, vol. 108, p. 108651, 2023.
[21] F. Hendaoui, R. Meddeb, L. Trabelsi, et al., "FLADEN: federated learning for anomaly detection in IoT networks," Computers & Security, vol. 155, p. 104446, 2025.
[22] N. Chaurasia, M. Ram, P. Verma, et al., "A federated learning approach to network intrusion detection using residual networks in industrial IoT networks," The Journal of Supercomputing, vol. 80, no. 13, pp. 18325-18346, 2024.