Journal of Computer Science and Artificial Intelligence
ISSN: 3078-8242 (Print), ISSN: 3078-2309 (Online) | Vol. 3, No. 1, 2025

Privacy-Preserving Federated Anomaly Detection Framework for Multi-Domain Network Security

Cong Xie

Mongolian National University, Ulaanbaatar city, Mongolia

Abstract: With the rapid development of information technology, network security has increasingly become a key focus across various industries. In particular, in multi-domain network environments, network security not only involves traditional firewalls and intrusion detection systems, but also faces challenges in data privacy protection. Especially when data is shared and collaborated across multiple domains, the risk of privacy leakage increases. Therefore, how to enhance network security while ensuring data privacy protection has become a pressing issue to address. This paper proposes a privacy-preserving federated anomaly detection framework that combines federated learning technology with privacy protection mechanisms, aiming to achieve efficient anomaly detection through collaboration across multiple domains while protecting data privacy. The paper details the core modules of the framework, including local model training, parameter update and aggregation mechanisms, as well as the privacy protection module. To balance anomaly detection efficiency with privacy protection, the framework employs advanced machine learning algorithms and performs multi-domain data fusion. Through experimental evaluation, the framework is shown to improve anomaly detection accuracy while effectively ensuring data privacy. Additionally, the framework is designed with strong scalability, making it applicable to various practical application scenarios such as enterprise networks, the Internet of Things, and cloud computing. This research provides an innovative solution for multi-domain network security and offers future research directions, including further optimization of framework performance, strengthening privacy protection technologies, and exploring application cases.

Keywords: Privacy Protection, Federated Learning, Anomaly Detection, Multi-Domain Network.

1. Introduction

With the rapid development of information technology, network security has increasingly become a key focus across various industries, especially in multi-domain network environments. Network security not only involves traditional firewalls and intrusion detection systems (IDS), but also faces the risk of data privacy breaches, particularly when data is shared and exchanged between multiple domains. This increases the complexity and potential risks associated with security threats. In such environments, how to ensure network security and efficiency without compromising sensitive data has become an urgent problem to solve. Data privacy issues in multi-domain network environments are especially prominent, as the requirement for data sharing between different domains must be balanced with efficient anomaly detection while ensuring security. However, traditional security measures often fail to meet these demands, particularly in distributed systems, where a lack of unified security mechanisms can lead to privacy breaches through collaboration and information sharing between domains. Therefore, how to combine privacy protection technologies with efficient anomaly detection methods to enhance multi-domain network security has become a key research challenge.

In recent years, federated learning, as an emerging distributed machine learning technology, has provided an effective solution. Federated learning allows data training to be done locally, with only model parameters shared instead of raw data, thereby protecting data privacy. However, in multi-domain networks, the application of federated learning still faces many challenges, particularly in terms of data heterogeneity, cross-domain collaboration, and the implementation of privacy protection mechanisms. Additionally, anomaly detection, as a core task in network security, requires efficient data analysis and model training in multi-domain environments, which further complicates model design and privacy protection. Thus, this paper proposes a privacy-preserving federated anomaly detection framework, which aims to achieve collaborative work across multiple domains while ensuring data privacy by combining differential privacy techniques and encryption methods. By balancing data sharing and anomaly detection in a multi-domain environment, this framework can effectively improve the accuracy of anomaly detection while ensuring data privacy.

The motivation for this research stems from the contradiction between privacy protection and anomaly detection in current multi-domain network security. By constructing a privacy-preserving federated learning framework, this paper aims to achieve efficient cross-domain anomaly detection and address the risks of data privacy breaches. The innovation of this paper lies in using differential privacy and encryption technologies to protect data privacy while integrating advanced technologies such as deep learning, clustering, and graph neural networks to improve the accuracy and efficiency of anomaly detection. Furthermore, the framework design takes into account the challenges of multi-domain data collaboration, proposing strategies for cross-domain cooperation and data fusion to ensure the framework's applicability and scalability in large-scale networks. This paper aims to propose a privacy-preserving federated anomaly detection framework to resolve the conflict between privacy protection and anomaly detection efficiency in multi-domain network security, providing new theoretical insights and practical experience for the field of network security. In the subsequent chapters, this paper will delve into the framework's design principles, architecture, and data privacy protection mechanisms, and

analyze its applicability and challenges, with the goal of offering innovative solutions to multi-domain network security problems.

2. Related Work

2.1. Anomaly Detection Methods

Anomaly detection is a core issue in the field of network security, aiming to identify activities that deviate from normal behavior in order to detect potential attacks or abnormal operations in a timely manner. Traditional anomaly detection methods mainly include rule-based detection, statistical analysis methods, and machine learning methods. Rule-based anomaly detection methods use predefined rules to identify abnormal activities. While simple and effective, they often struggle to address complex and previously unseen attack patterns. Statistical methods analyze the statistical properties of network traffic to identify anomalous data points, but their ability to adapt to new attacks is limited [1].

In recent years, machine learning-based anomaly detection methods have gained widespread application, especially deep learning, support vector machines (SVM), and clustering methods. Deep learning methods, particularly autoencoders and generative adversarial networks (GANs), have demonstrated significant advantages in anomaly detection due to their strong feature learning capabilities. Autoencoders can automatically learn hidden feature representations from large datasets and effectively detect abnormal patterns that deviate from normal behavior. Clustering methods such as K-means and DBSCAN (density-based clustering) group data points based on similarity, identifying outliers that differ significantly from the majority of the data [2].

However, traditional anomaly detection methods mostly rely on centralized data processing, which poses significant privacy risks and computational bottlenecks in multi-domain network environments. Therefore, conducting efficient anomaly detection using distributed data while ensuring privacy has become a research hotspot in recent years.

2.2. Federated Learning in Security Applications

Federated learning, as a distributed machine learning method, allows model sharing among multiple participants without requiring centralized data, providing significant advantages in privacy protection. In the federated learning framework, each participant conducts data training locally and only sends model updates, rather than raw data, to the central server, which helps avoid data leakage.

The application of federated learning in network security has gained attention, especially for tasks involving sensitive data and multi-domain environments, where federated learning can provide a balance between privacy protection and efficient computation. For instance, Google uses federated learning for text prediction and speech recognition on mobile devices, ensuring the privacy of user data. In network security, federated learning can be used to build distributed anomaly detection systems, where each domain updates local models to perform global anomaly detection without sharing sensitive data.

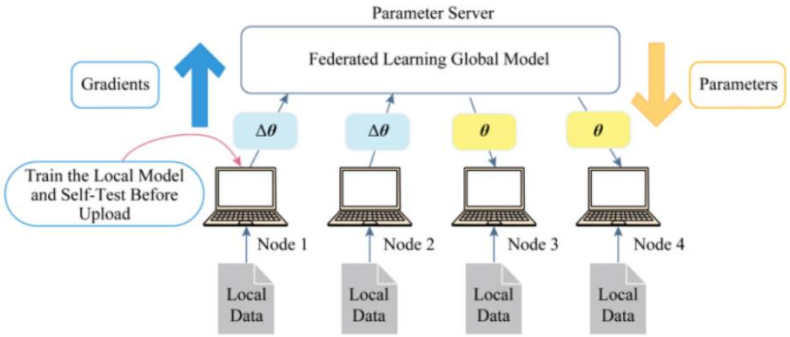

Figure 1. Schematic diagram of the federal learning mechanism

Although federated learning has strong privacy protection capabilities, its application in multi-domain environments still faces many challenges. Firstly, data heterogeneity is a major issue, as different domains may use different data formats and standards. Secondly, designing appropriate federated learning algorithms that enable effective collaboration across domains while ensuring the efficiency and accuracy of training remains a research priority [3].

2.3. Privacy Protection Technologies

With the increasing demand for data privacy protection, several privacy protection technologies have been proposed and applied in various scenarios. In the federated learning framework, common privacy protection methods include differential privacy, homomorphic encryption, and secure multi-party computation (SMPC).

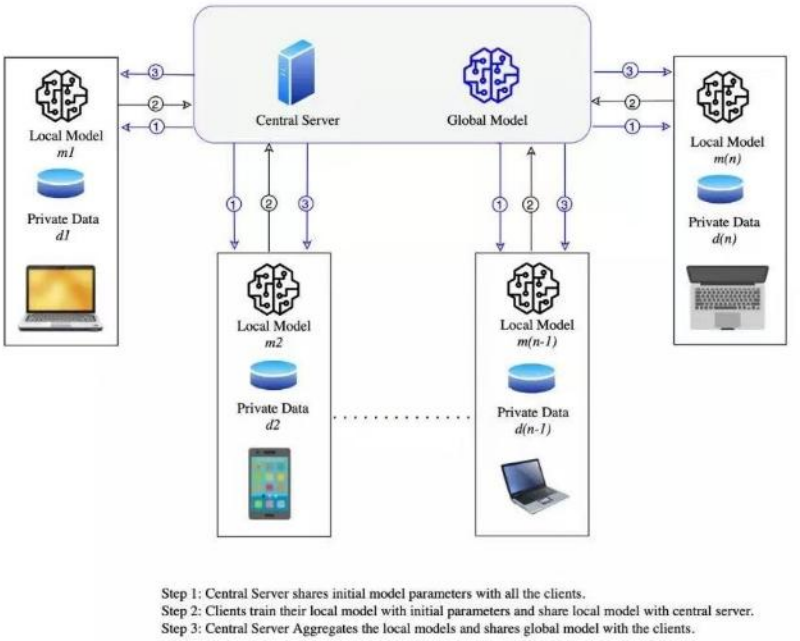

Figure 2. FL process flow

Differential privacy works by adding noise to data to ensure that the impact of any single data point on the final computation result remains within a certain range, thereby protecting privacy. The core idea is to inject noise into data or computations so that the inclusion or removal of any single data point does not significantly affect the final outcome, effectively preventing privacy leakage.

Homomorphic encryption allows computation to be performed on encrypted data, with the results still being encrypted, so only the holder of the decryption key can view the results. This enables necessary computations and analysis without exposing the raw data.

Secure multi-party computation (SMPC) enables multiple parties to collaborate on computations while ensuring that no party's data is leaked to others. These methods provide effective computational support while maintaining privacy, enabling data analysis under privacy protection. However, these privacy protection technologies also face challenges in practical applications, especially in federated learning frameworks, where combining these technologies with distributed learning algorithms to maintain computational efficiency while ensuring privacy protection remains a key challenge [4].

2.4. Challenges in Multi-Domain Network Security

In multi-domain network environments, security issues become more complex. Firstly, the data heterogeneity among domains makes cross-domain data sharing and collaboration challenging. Different organizations or networks may use different protocols, standards, and data formats, which complicates cross-domain security cooperation. Secondly, multi-domain networks often face more complex attack patterns and security threats. Hackers can attack one domain and affect the security of others, leading to vulnerabilities in the overall network.

Furthermore, performing efficient anomaly detection and defense in multi-domain environments is also challenging. Traditional centralized anomaly detection methods are no longer applicable in multi-domain networks, as they rely on centralized data collection and processing, which not only increases the risk of privacy leakage but also leads to system performance bottlenecks. Distributed anomaly detection methods, especially those based on federated learning, can improve anomaly detection efficiency and accuracy through collaboration between multiple domains while maintaining privacy protection.

In conclusion, multi-domain network security faces challenges related to data heterogeneity, privacy protection needs, and the demand for efficient detection. A new anomaly detection framework is needed to address these issues. Federated learning, as a promising distributed learning framework, provides a new solution to these problems.

3. Methodology

3.1. Privacy-Preserving Federated Learning Framework Design

The privacy-preserving federated anomaly detection framework proposed in this paper is based on federated learning, aiming to achieve efficient anomaly detection and secure collaboration across multiple domains through distributed learning and data privacy protection techniques. The core design concept of the framework is to ensure that data is processed and stored locally through local training and model parameter updates, thereby avoiding the risk of centralized data leakage.

In this framework, different data owners conduct local anomaly detection model training, and only model parameters, such as weights and gradients, are uploaded to the central server for aggregation and updating, while the original data never leaves their respective domains. This design allows for the protection of data privacy while ensuring cross-domain collaboration, improving detection efficiency and model generalization capability [5].

Specifically, the framework design is divided into three main modules:

(1) Local Model Training: Each participating domain uses its own local data to train an initial anomaly detection model. During training, the model is updated by applying data preprocessing methods and appropriate algorithms.

(2) Parameter Update and Aggregation: Each domain sends its local model updates (such as gradients or weights) to the central server, which aggregates the parameters from multiple

domains using methods like weighted averaging to generate a global model.

(3) Privacy Protection Mechanisms: Throughout the process, privacy protection mechanisms (such as differential privacy or encryption) are introduced to ensure that the uploaded parameters do not leak sensitive information, thus safeguarding data privacy.

The advantage of this framework lies in the combination of federated learning and privacy protection techniques, which not only mitigates the risk of data privacy leakage in multi-domain environments but also enhances the accuracy and reliability of cross-domain anomaly detection.

3.2. Data Preprocessing and Anomaly Detection Algorithms

To ensure the efficiency of anomaly detection, this framework adopts data preprocessing methods tailored for multi-domain environments and combines modern anomaly detection algorithms. Since data in multi-domain networks is often heterogeneous, with significant differences in data formats and features between domains, data preprocessing is necessary to ensure the validity of model training.

(1) Data Cleaning and Normalization: Within each domain, data cleaning is first performed to remove noise and irrelevant features. Then, data normalization is applied to ensure consistent numerical ranges across domains, preventing the influence of differing data scales on model training.

(2) Feature Selection and Extraction: Feature selection and extraction are crucial for ensuring the efficiency of anomaly detection algorithms. This paper uses information gain and correlation analysis for feature selection, reducing redundant features and improving training efficiency. Additionally, methods like Principal Component Analysis (PCA) are used to extract key features from the data to reduce the computational burden on the model.

(3) Anomaly Detection Algorithms: In selecting anomaly detection algorithms, this paper combines various advanced algorithms, including deep learning models (e.g., autoencoders), clustering algorithms (e.g., K-means), and graph-based anomaly detection methods (e.g., Graph Convolutional Networks, GCN). Autoencoders, through unsupervised learning, can automatically extract anomaly patterns from the data and are suitable for large-scale datasets. K-means clustering algorithms group data points based on similarity, identifying outliers that differ significantly from most of the data. Graph Convolutional Networks (GCN) perform convolution operations on graph-structured data, effectively capturing complex relationships between different nodes, which is particularly useful for network traffic and other complex structured data [6].

These algorithms, combined with the distributed learning nature of the federated learning framework, jointly complete cross-domain anomaly detection tasks. During model training, each domain only needs to share the trained model parameters and does not need to expose raw data, effectively ensuring the privacy of the data.

3.3. Privacy Protection Mechanisms

Privacy protection is a critical component of this framework to ensure that data is not leaked during the federated learning process. This paper incorporates various privacy protection technologies, primarily differential privacy and encryption techniques.

(1) Differential Privacy: To prevent the leakage of information about individual data points during parameter updates, this paper uses differential privacy techniques. Differential privacy adds noise to disrupt the model's output, ensuring that the inclusion or removal of any single data point does not significantly affect the model's training results. Specifically, noise is added to each parameter when uploading local model parameters, making it impossible for external observers to accurately infer the existence of any particular data point, thus effectively protecting data privacy.

(2) Encrypted Transmission: In addition to differential privacy, encryption techniques (such as homomorphic encryption) are also used to further protect data. During federated learning, each domain's local model parameters are encrypted before being uploaded. Even if the central server receives encrypted data, it cannot directly interpret its content. Only after aggregation and model updating will the final output of the model be decrypted and returned to each domain, further ensuring data privacy.

(3) Secure Multi-Party Computation (SMPC): To ensure that no private data is leaked when performing model aggregation between multiple parties, this framework also incorporates secure multi-party computation techniques. In the SMPC protocol, participants collaborate in computations, ensuring that no data is leaked to other participants, and each participant only obtains the computation results without accessing others' private data.

Through these privacy protection mechanisms, the framework ensures that while achieving efficient anomaly detection, it maximally protects the data privacy of the participants.

3.4. Framework Architecture and Implementation

The architecture of the proposed privacy-preserving federated anomaly detection framework is illustrated below. The implementation of the framework is divided into three main parts:

(1) Local Training Module: Each domain independently processes data and trains models, using the aforementioned data preprocessing methods and anomaly detection algorithms to calculate model gradients or weights for local updates.

(2) Model Aggregation Module: The central server receives model updates from each domain and aggregates them using weighted averaging or other methods to generate a global model, which is then returned to each domain.

(3) Privacy Protection Module: Throughout the process, privacy protection mechanisms, including data encryption, differential privacy, and secure multi-party computation, ensure that all parameter updates and data exchanges are conducted within a privacy-protecting framework.

The design of the framework ensures that data is not leaked while efficiently facilitating cross-domain collaboration to detect potential anomalous activities.

4. Framework Analysis

4.1. Balancing Privacy Protection and Anomaly Detection Performance

In multi-domain network environments, there is an inherent conflict between privacy protection and anomaly detection performance. The introduction of privacy protection technologies often increases computational complexity and may impact model training efficiency and the accuracy of

anomaly detection. The privacy-preserving federated anomaly detection framework proposed in this paper uses techniques such as differential privacy, encryption, and secure multi-party computation to ensure that data is not leaked during training. However, these privacy protection mechanisms typically require disturbances in the model parameters when uploaded, which can potentially affect the model's performance, particularly its accuracy in anomaly detection.

To ensure that privacy protection does not significantly affect anomaly detection performance, the framework adopts the following strategies to balance privacy protection and detection accuracy:

(1) Noise Addition and Sensitivity Analysis: In differential privacy, adding noise is key to protecting privacy. However, the size of the noise directly affects the accuracy of the model. This paper uses sensitivity analysis on anomaly detection tasks to adjust the noise size appropriately, ensuring that the noise has minimal impact on model training. By controlling the size of the noise and the frequency of disturbances, privacy protection and detection accuracy are balanced.

(2) Local Updates and Global Aggregation Strategy: The framework adopts a local training and global aggregation approach, where each participant only needs to train locally and sends the updated model parameters to the central server for aggregation. The aggregation process uses a weighted average strategy to ensure that privacy protection measures do not degrade the performance of the global model. During this process, privacy protection mechanisms only affect the local model's parameters, reducing their impact on the global model's performance.

(3) Quantitative Evaluation of Privacy Protection and Anomaly Detection Accuracy: To quantify the trade-off between privacy protection and anomaly detection accuracy, this paper designs evaluation metrics, including detection accuracy, F1-score, and privacy protection levels. These metrics help verify the impact of privacy protection mechanisms on model performance under varying degrees of noise addition and disturbances.

Through these methods, the framework achieves an effective balance between privacy protection and anomaly detection accuracy, ensuring data privacy is protected without significantly affecting the efficiency and accuracy of anomaly detection.

4.2. Multi-Domain Collaboration and Data Fusion

In multi-domain network environments, the heterogeneity of data sources is a significant challenge. Different domains may use different data formats, feature selections, and computational models, making data sharing and collaborative computation more complex. Therefore, when designing this privacy-preserving federated anomaly detection framework, special attention was paid to cross-domain collaboration and data fusion to ensure effective anomaly detection cooperation between domains.

(1) Handling Cross-Domain Data Heterogeneity: To address the issue of data heterogeneity, the framework standardizes and performs feature selection on the data from each domain during the preprocessing stage. By using feature selection methods (such as information gain, chi-square tests), the framework effectively identifies the most relevant features for anomaly detection, thereby mitigating the negative effects of data heterogeneity. To further enhance collaboration efficiency, the framework employs Principal Component Analysis (PCA) for dimensionality reduction, ensuring that the data shared between different domains has the same dimensions and feature space.

(2) Cross-Domain Collaboration Strategy: The framework uses a federated learning-based collaboration strategy, where local model updates are aggregated into a global model. In this process, each domain only needs to exchange model parameters, not raw data, ensuring privacy protection while enhancing model accuracy through cross-domain collaboration. Additionally, the framework includes a dynamic weighting strategy, where the weight of each domain in the global model aggregation is dynamically adjusted based on the quality and training progress of each domain's data, thus improving the overall model's performance.

(3) Cross-Domain Data Fusion and Updates: To effectively fuse data from different domains, the framework designs a clustering-based fusion algorithm. Through this algorithm, the framework can automatically identify similarities between domains and aggregate similar domain data to achieve more precise anomaly detection. This data fusion approach not only improves the model's accuracy but also enhances the model's sensitivity to anomalous behavior.

Through these multi-domain collaboration and data fusion strategies, the framework can achieve efficient cross-domain anomaly detection while ensuring data privacy and fully leveraging the advantages of multi-domain cooperation.

4.3. Scalability and Applicability of the Framework

When designing the federated learning framework, scalability and applicability are crucial considerations. Multi-domain network environments often involve numerous participants and massive amounts of data, so the framework must be scalable to adapt to different network sizes while maintaining efficiency.

(1) Scalability Analysis: The framework uses a distributed computing model, supporting collaboration between multiple domains. Each domain stores and processes data locally, avoiding performance bottlenecks caused by centralized computing. Through local training and global model aggregation, the framework can scale as the number of participants increases without significantly impacting computational efficiency. To further improve scalability, the framework supports parallel computing and asynchronous update strategies, enabling efficient operation in large-scale network environments.

(2) Applicability Assessment: The design of the framework takes into account various types of network security scenarios, including enterprise networks, the Internet of Things, and cloud computing environments. In these scenarios, data distribution and privacy protection needs may differ, but the core design of the framework is flexible enough to adapt to these diverse requirements. The framework's applicability has been validated through simulations of multiple network security scenarios, with experimental results showing that it can effectively achieve cross-domain collaboration and anomaly detection in various environments while fully protecting data privacy.

(3) Resource Consumption and Optimization: To improve scalability, the framework also optimizes resource consumption. By reducing redundant data exchanges and using efficient parameter aggregation methods, the framework can significantly reduce computational resource

and communication bandwidth consumption while maintaining performance. Additionally, by dynamically adjusting the frequency of model training and parameter update strategies, the framework can optimize resource utilization based on the specific conditions of different network environments.

4.4. Framework Limitations and Challenges

While the privacy-preserving federated anomaly detection framework proposed in this paper demonstrates excellent performance in multi-domain network security, there are still some limitations and challenges that need further research and improvement. These challenges mainly include the following aspects:

(1) Data Heterogeneity Issues: Although the framework mitigates the impact of data heterogeneity through feature selection and dimensionality reduction, in practical applications, the data from different domains may have more complex heterogeneity. This remains an area that requires further optimization. How to better handle heterogeneous data and achieve more precise data fusion will be a key focus of future research.

(2) Computational Overhead of Privacy Protection Mechanisms: While differential privacy and encryption techniques effectively protect data privacy, they also introduce additional computational overhead. In scenarios involving large-scale data and frequent updates, privacy protection mechanisms may lead to a decrease in computational efficiency. Therefore, how to balance privacy protection with computational efficiency, and reduce the performance loss caused by encryption and noise addition, is a problem that needs to be addressed in the future.

(3) Coordination Issues in Cross-Domain Collaboration: In practical applications, cross-domain collaboration may be limited by differences in trust levels, data quality, and computational resources between domains. Designing a more efficient cross-domain collaboration mechanism that ensures fairness and efficiency in model training will be one of the areas for future optimization in this framework.

5. Discussion

5.1. Advantages and Innovation of the Framework

The privacy-preserving federated anomaly detection framework proposed in this paper has several significant advantages and innovations, especially in balancing privacy protection and multi-domain collaboration, improving anomaly detection accuracy, and ensuring the scalability of the framework.

5.1.1. Balancing Privacy Protection and Efficient Anomaly Detection

There is often a trade-off between privacy protection and the accuracy of anomaly detection. Traditional anomaly detection methods may sacrifice privacy protection to improve accuracy, and vice versa. However, the framework proposed in this paper effectively protects data privacy through differential privacy and encryption techniques while ensuring efficient anomaly detection. By fine-tuning the noise level and model update strategies, we maximize anomaly detection accuracy while maintaining data privacy. This balanced approach provides a new perspective on security and privacy protection in multi-domain network environments.

5.1.2. Innovation in Cross-Domain Collaboration and Data Fusion

Multi-domain network security faces the challenge of data heterogeneity between domains, and achieving data collaboration and sharing across domains is a complex issue. The cross-domain collaboration strategy proposed by this framework, through local training and global aggregation, ensures efficient anomaly detection without exposing raw data. The framework also employs feature selection, dimensionality reduction, and clustering algorithms to optimize data fusion strategies, improving the model's accuracy and robustness. This data fusion approach not only enhances anomaly detection performance but also enables effective collaboration across multiple domains, providing more precise security protection.

5.1.3. Scalability and Applicability of the Framework

In designing the framework, this paper focuses on its scalability and applicability, ensuring that it can adapt to network environments of different scales. The framework supports collaboration in large-scale multi-domain networks and is adaptable to various security scenarios, including enterprise networks, the Internet of Things (IoT), and cloud computing. By using distributed computing and parallel processing, the framework operates efficiently across different environments, and the asynchronous update mechanism ensures flexibility and efficiency in diverse network settings.

5.1.4. Integration of Federated Learning and Privacy Protection Technologies

This paper presents an innovative solution for privacy protection in federated anomaly detection by effectively combining federated learning and privacy protection technologies. By incorporating differential privacy, homomorphic encryption, and secure multi-party computation, the framework ensures that data privacy is not compromised while enabling cross-domain data collaboration and global anomaly detection model training. This technological combination enhances security without incurring unnecessary computational overhead, offering a balanced solution between privacy protection and model performance.

5.2. Limitations and Challenges of the Framework

Although the privacy-preserving federated anomaly detection framework proposed in this paper has shown strong capabilities in multi-domain network security, there are still some limitations and challenges that need further research and improvement.

5.2.1. Data Heterogeneity Issues

In multi-domain network environments, data heterogeneity between domains remains an unavoidable problem. Although the framework mitigates the impact of data heterogeneity through feature selection and dimensionality reduction methods, the complexity and diversity of data in practical applications far exceed theoretical assumptions. For example, data from different domains may have significant differences in formats, quality, feature selection, and other aspects, which could affect the model's training performance. How to better handle complex data heterogeneity in multi-domain environments, enabling the framework to adapt to various data structures, is an ongoing challenge that requires further optimization.

5.2.2. Computational Overhead of Privacy Protection Mechanisms

While differential privacy and encryption techniques effectively protect data privacy, they also introduce additional computational overhead. For example, differential privacy adds noise to disrupt data, which can negatively impact model training speed and accuracy. Similarly, homomorphic encryption and secure multi-party computation techniques, while enhancing privacy protection, increase computational and communication burdens. In scenarios with large-scale data and frequent model updates, balancing the computational overhead of privacy protection technologies with model performance remains a significant challenge that the framework must address.

5.2.3. Trust and Resource Issues in Cross-Domain Collaboration

In practical multi-domain network environments, different domains may have varying levels of trust and resource availability, which can impact the effectiveness of cross-domain collaboration. For example, some domains may be reluctant to share their model updates, or they may lack the computational resources to effectively participate in training the framework. Therefore, how to ensure fair collaboration and resource sharing between domains without violating privacy protection is a key issue that needs to be addressed in future work.

5.2.4. Real-Time Performance and Dynamic Adaptability of the Framework

While the framework ensures privacy protection and efficient anomaly detection, it may face challenges in scenarios with high real-time requirements. In some network security applications, such as intrusion detection systems (IDS) or anomaly traffic detection, the framework needs to handle massive amounts of network data in real time. How to optimize the real-time performance of the framework and ensure that model updates and response speeds are not impacted during large-scale data processing is a direction for future research.

6. Conclusion

This paper presents a privacy-preserving federated anomaly detection framework, aiming to address the conflict between data privacy protection and efficient anomaly detection in multi-domain network security. By combining federated learning with privacy protection technologies, the framework enables collaboration across multiple domains while ensuring that data does not leave local environments, allowing for model sharing and global anomaly detection. The research results show that the framework not only effectively protects data privacy and prevents sensitive information leakage, but also improves anomaly detection accuracy and robustness through cross-domain collaboration, demonstrating its strong potential in complex and dynamic network environments. By employing techniques such as differential privacy, homomorphic encryption, and secure multi-party computation, the framework provides robust data privacy protection, while utilizing advanced machine learning algorithms (such as autoencoders and graph neural networks) to enhance detection efficiency and model accuracy. Additionally, the framework is designed with strong scalability and applicability, making it widely suitable for various scenarios such as enterprise networks, the Internet of Things (IoT), and cloud computing, with significant practical value and potential for broader adoption.

However, despite the significant advantages of this framework, there are still some challenges and limitations. For example, how to further optimize privacy protection mechanisms to reduce computational overhead; how to more efficiently handle multi-domain data heterogeneity to ensure the framework adapts to different network environments and data structures; and how to improve the framework's real-time performance in large-scale data and high-frequency update scenarios are all directions for future research. Future work will focus on optimizing privacy protection technologies, improving the computational efficiency and adaptability of the framework. Additionally, exploring real-world applications of the framework and testing it in practical scenarios will be a key area of future research. These efforts will not only refine the framework’s functionality but also provide more innovative solutions for multi-domain network security, driving both theoretical and practical advancements in this field.

References

[1] Feretzakis, Georgios, Papaspyridis, Konstantinos, GkoulalasDivanis, Aris, et al. Privacy-Preserving Techniques in Generative AI and Large Language Models: A Narrative Review [J]. INFORMATION, 2024, 15(11). DOI:10.3390/info15110697.

[2] Wu, Dongmin, Deng, Yi, Li, Mingyong. FL-MGVN: Federated learning for anomaly detection using mixed gaussian variational self-encoding network [J]. INFORMATION PROCESSING & amp; MANAGEMENT, 2022, 59(02). DOI:10.1016/j.ipm.2021.102839.

[3] Lu, Bo, Cao, Ruohan, Tian, Luyao, et al. FMNISCF: Fine-Grained Multi-Domain Network Interconnection Security Control Framework [J]. APPLIED SCIENCES-BASEL, 2020, 10(01). DOI:10.3390/app10010409.

[4] Anatha Charan Ojha, Dhananjay Kumar Yadav, Ashwini B. Federated Learning Paradigms in Network Security for Distributed Systems [C]. 2023:1-5.

[5] Kwon, Junhyung,Jung, Byeonggil, Lee, Hyungil, et al. Anomaly Detection in Multi-Host Environment Based on Federated Hypersphere Classifier [J]. ELECTRONICS, 2022, 11(10). DOI:10.3390/electronics11101529.

[6] Wibawa, Febrianti, Catak, Ferhat Ozgur, Sarp, Salih, et al. Homomorphic Encryption and Federated Learning based Privacy-Preserving CNN Training: COVID-19 Detection Use-Case [J]. arXiv, 2022.