ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Network Traffic Anomaly Detection Using Machine Learning

P.Swetha[#1], Y.aasidhar Rao[$2], A.Ganesh[$3], D.Uma Mahesh Rao[$4]
[#1,$2,$3,$4] B.Tech UG Students, Dept.Of CSE, AITAM, Tekkali, AP, India
[#1]swethapolaki2003@gmail.com, [$2]sasidharrao69@gmail.com, [$3]ganeshambati2002@gmail.com,
[$4]dumpalaumamahesh172@gmail.com

Abstract
The quick advancement and extensive utilization of cloud computing has led to the complexity and adaptability of cloud computing open networks and service sharing situations. Anomaly network traffic detection is a useful tool for network detection since it may identify changes in pattern or states. An additional avenue for the advancement of anomalous network traffic detection is provided by machine learning. The accuracy of the machine learning models now in use has to be increased because they are unable to properly comprehend the temporal and spatial characteristics of network traffic.

This study suggests a three-layer parallel network structure anomalous network traffic detection model that integrates temporal and spatial aspects (ITSN).To increase the precision of network traffic classification, ITSN acquires knowledge of the temporal and spatial characteristics of the traffic. Based on this, an enhanced technique for extracting raw traffic features is suggested, which can lessen the number of redundant features, hasten the network's convergence, and lessen dataset imbalance. We have employed techniques such as Light Gradient Boosting Machine (LGBM) and Naïve Bayes(NB) for better results in our paper.

Keywords: Network traffic, Machine learning, NB, LGBM.

Introduction
The volume of data flowing through a computer network at any one moment is known as network traffic. Often referred to as data traffic, network traffic is composed of individual data packets that are transmitted across a network and then constructed by the computer or device that receives them. There are two directions for network traffic: east-west and north-south. Network quality is impacted by traffic because excessive traffic might result in erratic Voice over Internet Protocol (VoIP) connections or sluggish download rates. When data travels over a network or over the internet, it must first be broken down into lower batches so that larger lines can be transmitted efficiently. The network breaks down, organizes, and packets the data into data packets so that they can be transferred reliably through the network and also opened and read by another stoner in the network. Each packet takes the stylish route possible to spread network business unevenly. Client-to-server traffic traveling between the data center and the rest of the network, or a place outside the data center, is referred to as north-south traffic.

Cite this article as: P.Swetha, Y.aasidhar Rao, A.Ganesh & D.Uma Mahesh Rao, "Network Traffic Anomaly Detection Using Machine Learning", International Journal of Research in Advanced Computer Science Engineering, (IJRACSE), Volume 9 Issue 10, March 2024, Page 1-11.

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Server-to-server traffic, commonly referred to as east-west traffic, is the flow of information within a data center.

Network managers set the behavior of network equipment, such as switches and routers, for specific types of traffic in order to better manage bandwidth. Network traffic can be divided into two main categories: real-time and non-real-time. Delivery of traffic that is deemed crucial or significant to corporate operations must occur promptly and with the best quality feasible. Real-time network traffic includes things like web browsing, videoconferencing, and VoIP. Network administrators view non-real-time traffic—also referred to as best-effort traffic—as less significant than real-time traffic. Email apps and File Transfer Protocol (FTP) for web publishing are two examples. Network administrators utilize network traffic analysis (NTA) as a technique to monitor availability, look for anomalous activity, and analyze network activity.

Finding unusual things, occurrences, or observations that are suspicious because they deviate greatly from typical patterns or behaviors is known as anomaly detection. Standard deviations, outliers, noise, novelty, and exceptions are other terms for anomalies in data. An anomaly is often defined as something that defies expectation. For instance, when a service is down, new error codes could start to show up, or a broken switch might cause unexpected traffic to occur in another area of the network. Network abnormalities are the foundation of network troubleshooting. Anomalies can be broadly categorized in a number of ways: Anomalies in the behavior of a network are deviations from the norm, standard, or anticipated behavior. Network owners need to understand expected or usual behavior in order to identify anomalies in their networks. Constantly scanning a network for unforeseen patterns or events is necessary for detecting anomalies in network activity. Anomalies related to application performance: These are merely deviations found through comprehensive monitoring of application performance. These systems monitor how applications operate and gather information on all issues, including app dependencies and supporting infrastructure. Rate limitation is initiated when abnormalities are found, and administrators are alerted to the source of the problematic data. Online application security anomalies: These comprise any additional suspicious or unusual behavior in online applications that could have an effect on security.

Every kind of anomaly must be found through continuous, automated monitoring in order to build a picture of typical network or application activity. The purpose of the anomaly detection system is more dependent on the network environment, application performance, and online application security than it is on point anomalies/global outliers, contextual anomalies, and/or collective abnormalities. While they are different, anomaly detection and novelty detection or noise reduction are comparable. Novelty detection helps people decide whether patterns in data are abnormal by spotting previously unnoticed patterns. The practice of eliminating extraneous observations or noise from a signal that retains significance is known as noise removal. When monitoring network traffic, anomaly detection is a crucial technique for accurately differentiating

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

between normal and anomalous information. As part of the machine learning (ML) process, one might apply the current classification algorithms for this purpose. Examining certain data points and spotting uncommon events that look suspicious because they deviate from the established pattern of behavior is known as anomaly detection. Although anomaly detection is not new, manual tracking becomes unfeasible as data volumes rise.

Problem Statement

Design and implement an advanced Network Traffic Anomaly Detection System employing state-of-the-art machine learning algorithms and techniques. This comprehensive system aims to continuously monitor and analyse the dynamic network environment in real-time, identifying and classifying anomalous patterns with a high accuracy. The paper involves the integration of diverse machine learning models to effectively discern normal network behaviour from abnormalities, enhancing the overall security posture of the network infrastructure. The solution should provide a user-friendly interface for administrators to visualize and respond to detected anomalies promptly, and safeguarding the integrity and confidentiality of the network.

Objective

The primary objective of the paper, "Network Traffic Anomaly Detection using Machine Learning," is to develop an intelligent and robust system capable of identifying and classifying abnormal patterns within network traffic. The paper aims to leverage advanced machine learning techniques to enhance the overall cyber security posture of a network by promptly detecting anomalous activities.

Key Components of the Objective:

Anomaly Identification:

Develop a machine learning model capable of discerning normal network behaviour from anomalous patterns. Train the model on a diverse dataset to ensure a comprehensive understanding of regular network traffic.

Real-time Detection:

Implement a real-time anomaly detection mechanism to promptly identify deviations from normal network behaviour. Minimize false positives and false negatives to improve the accuracy of anomaly detection.

Feature Extraction and Selection:

Investigate and select relevant network features to enhance the efficiency and effectiveness of the machine learning model. Employ advanced techniques for feature extraction to capture the most discriminative aspects of network traffic.

Dynamic Learning and Adaptability:

Design the system to dynamically adapt to changes in network behaviour over time. Implement mechanisms for continuous learning to ensure the model remains effective against evolving threats and network dynamics.

Alert Generation and Reporting:

Integrate a notification system to generate alerts for network administrators or security personnel when anomalies are detected. Provide detailed reports on identified anomalies, aiding in swift and informed decision-making.

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Scalability and Performance:
Ensure the scalability of the solution to accommodate varying network sizes and complexities. Optimize the performance of the machine learning model to handle large volumes of network traffic without compromising on accuracy.

Evaluation and Fine-tuning:
Establish a rigorous evaluation framework to assess the performance of the anomaly detection system.

Regularly fine-tune the machine learning model based on feedback and newly identified threat patterns.

By achieving these objectives, the paper aims to significantly enhance the security posture of networks by proactively identifying anomalies through the application of advanced machine learning techniques in the realm of anomaly detection.

Scope
The paper titled "Network Traffic Anomaly Detection Using Machine Learning" focuses on leveraging advanced machine learning techniques to enhance the security and efficiency of computer networks. The scope involves developing a system capable of identifying abnormal patterns and deviations from the expected behaviour within network traffic. By employing machine learning algorithms, such as anomaly detection models, the paper aims to establish a proactive approach to cyber security, enabling the timely detection of anomalies The significance of this project lies in its potential to significantly improve the overall security posture of networks, minimizing the risk of unauthorized access, data breaches Additionally, the paper may contribute to the development of intelligent, adaptive systems that can evolve and adapt to emerging threats in real-time, making it a valuable asset for network administrators and cyber security professionals.

Existing System-Naïve Bayes
Integrating the Naive Bayes algorithm into a network traffic anomaly detection project brings several advantages and considerations. Naive Bayes is a probabilistic classification algorithm that calculates the probability of an instance belonging to a particular class based on its features. In the context of network traffic anomaly detection, Naive Bayes can be employed to classify network traffic patterns as either normal or anomalous. One key benefit is the simplicity and efficiency of Naive Bayes, making it computationally lightweight and suitable for real-time analysis of network data. Its probabilistic nature allows it to handle uncertainty and noise inherent in network traffic. The algorithm can be trained on historical data to learn the typical behaviour of the network, and deviations from this learned pattern can be flagged as anomalies.

However, it's important to note that Naive Bayes assumes independence among features, which may not hold true for all network traffic characteristics. In complex network environments, the independence assumption might be limiting, and other machine learning models, such as ensemble methods or deep learning, could be explored for enhanced performance. Additionally, the success of the project depends on the quality and representativeness of the training data. Anomalies in network traffic can be diverse,

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

and ensuring a diverse and comprehensive dataset is crucial for the algorithm to generalize well.In summary, incorporating Naive Bayes into a network traffic anomaly detection system offers simplicity, efficiency, and a probabilistic approach. However, careful consideration of the specific characteristics of the network and the nature of anomalies is essential to optimize the algorithm's performance. It may also be beneficial to explore other machine learning techniques in conjunction with Naive Bayes to achieve a more robust and accurate detection system.

Proposed System-Light Gradient Boosting Machine

Integrating Light Gradient Boosting Machine (LightGBM) into a network traffic anomaly detection project can offer several advantages due to the algorithm's efficiency, speed, and ability to handle complex relationships in data. LightGBM is a gradient boosting framework that is particularly well-suited for large-scale and high-dimensional datasets.

In the network traffic anomaly detection paper, we propose integrating temporal and spatial features into the dataset to enhance the model's ability to detect complex patterns and relationships. Temporal features, such as timestamps and time-related information, and spatial features, like IP addresses and geographical locations, provide valuable context to the network traffic data. These features are seamlessly integrated into the dataset, creating a more comprehensive representation of the network activity. After preprocessing, including encoding categorical features and normalizing numerical values, the dataset is used to train the Light Gradient Boosting Machine (LightGBM) model. LightGBM's capacity to handle both categorical and numerical features makes it well-suited for this enriched dataset. During training, the model learns intricate patterns and dependencies within the temporal and spatial context of the network traffic.

Following training, the model provides insights into the importance of different features, aiding in understanding which time intervals, days, or locations contribute most to anomaly detection. In the prediction phase, the trained LightGBM model is applied to new network traffic data, leveraging its ability to consider both temporal and spatial contexts for identifying anomalies. This approach enhances sensitivity to nuanced patterns and contributes to more accurate and effective network traffic anomaly detection, particularly in dynamic and complex network environments.

In summary, the proposed system with LightGBM and integrated temporal and spatial features offers advantages in terms of capturing complex relationships, efficiency, scalability, and feature importance analysis compared to the existing Naive Bayes system. LightGBM's flexibility and ability to handle diverse features make it a more suitable choice for the complexities of network traffic anomaly detection.

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Literature Survey

YEAR	AUTHOR NAME	TITLE NAME	METHODOLOGY	RESULTS
2017	Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K.	Network traffic anomaly detection and prevention: concepts, techniques, and tools	Statistical and clustering, soft computing, knowledge-based techniques	It discusses the intrusion prevention mechanism s that attempts to block the entry of attackers
2017	Monowar, H. Bhuyan, DhrubaK. Bhattacharyya &Jugal	Network Traffic Anomaly Detection Techniques and Systems	statistical, classification, clustering and outlier based, soft computing, knowledge-based techniques	It presents the strengths and weaknesses of each category of detection techniques
2018	BJ Radford, LM Apolonio	Network traffic anomaly detection using recurrent neural networks	Long-Short-Term Memory (LSTM) cell Recurrent Neural Networks (RNN) to capture the complex relationships and nuances of this language.	demonstrate positive unsupervised attack identification performance (AUC 0.84) on the ISCX IDS dataset
2018	H Xia, B Fang, M Roughan, K Cho, P Tune	ABasisEvolution framework for network traffic anomaly detection	Clustering method-principal component analysis and back propagation neural networks	obtaining very low false-alarm probabilities in comparison
2018	Zhen Du Nanjing, China Lipeng Ma et al.	Network traffic anomaly detection based on wavelet analysis	wavelet analysis is used to extract the waveform features, and then the support vector machine is used for classification.	achieves good classification results.
2019	Peter Kromkowski, Shaoran Li et al.	Evaluating Statistical Models for Network Traffic Anomaly Detection	Seasonal Autoregressive Integrated Moving Average (SARIMA) times series model and	improved overall detection performance by ensembling the SARIMA and LSTM autoencoder.

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

			Long Short-Term Memory (LSTM) Autoencoder model at anomaly detection.	
2020	Ren-Hung Hwang, Min-Chun Peng et al.	An unsupervised deep learning modelfor early network traffic anomaly detection	D-PACK, which consists of a Convolutional Neural Network (CNN) and an unsupervised deep learning model (e.g., Autoencoder) for auto-profiling the traffic patterns and filtering abnormal traffic.	The design can inspire the emerging efforts towards online anomaly detection systems
2021	K Fotiadou, TH Velivassaki, et al.	Network traffic anomaly detection viadeep learning	Convolutional NeuralNetworks (CNNs), and the Long Short Term Memory Networks (LSTMs) in order to construct robust multi-class classifiers	Outperformed other State-of-the-art Evaluation models
2022	Rajlaxmi Patil, Rajshekhar Biradar et al.	Network traffic anomaly detection using PCA and BiGAN	principal component analysis (PCA) and bidirectional generative adversarial network (BiGAN) model is used to detect the anomalous network traffic.	the proposed models are fasterand efficient at test time.
2022	Jiaming Pei a, Kaiyang Zhong et al.	Personalized federated learning framework for network traffic anomaly detection	Transfer Learning and self-coding of LSTM was constructed	higher detection accuracy and better detection performance

Algorithms: Naivebayes

Naive Bayes is a popular machine learning algorithm that is often used for classification tasks, including network traffic anomaly detection. In the context of network traffic analysis, the goal is to identify abnormal patterns or behaviours that may indicate a security threat or an anomaly. Naive Bayes is a probabilistic algorithm that makes assumptions about the independence of features, which might not always hold true in real-world scenarios. However, despite its

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

simplicity, Naive Bayes can perform well in certain applications, including network traffic anomaly detection.

Here's a high-level overview of the process of using Naive Bayes for network traffic anomaly detection:

Data Collection:
Collect a labelled dataset that includes both normal and anomalous network traffic. The dataset should be representative of the network's typical behaviour.

Feature Extraction:
Identify relevant features from the network traffic data that can help distinguish between normal and anomalous patterns. These features could include packet size, packet frequency, source and destination IP addresses, protocol types, etc.

Data Preprocessing:
Pre-process the data to handle missing values, outliers, and any other data quality issues. Normalize or scale the features to ensure that they have similar ranges.

Training:
Split the dataset into training and testing sets. Use the training set to train the Naive Bayes model. The algorithm estimates the probabilities of each feature given the class labels (normal or anomalous).

Naive Bayes Algorithm:
Naive Bayes calculates the probability of a particular set of features belonging to each class. It assumes that the features are conditionally independent given the class label, which is often a simplifying but unrealistic assumption. The algorithm calculates the probability of a particular class given the observed features using Bayes' theorem.

Model Evaluation:
Evaluate the performance of the trained Naive Bayes model on the testing set. Common evaluation metrics include accuracy, precision, recall, and F1 score. Adjust the model parameters or features as needed to improve performance.

Anomaly Detection:
Once the model is trained and evaluated, it can be used to classify new, unseen network traffic as normal or anomalous. If the probability of a given set of features being anomalous is higher than a predefined threshold, the traffic is classified as an anomaly.

Feedback Loop:
Periodically retrain the model with new data to adapt to changes in network behaviour and to improve the model's accuracy over time.

It's important to note that while Naive Bayes is a simple and interpretable algorithm, it may not perform as well as more complex models in certain situations, especially when dealing with highly correlated features or intricate patterns in the data. In practice, a combination of multiple algorithms or more advanced machine learning techniques may be employed for robust network traffic anomaly detection.

Light Gradient Boosting Machine

Light Gradient Boosting Machine (LightGBM) is a powerful and efficient machine learning algorithm commonly used

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

for tasks such as classification, regression, and anomaly detection. When applied to network traffic anomaly detection, LightGBM can help identify unusual patterns or behaviours in network data. Here's a general overview of the process:

Data Collection and Preprocessing:
Data Collection: Gather network traffic data, which may include information such as packet size, protocol type, source and destination IP addresses, timestamps, etc.

Data Preprocessing: Clean and preprocess the data. This involves handling missing values, normalizing features, and encoding categorical variables.

Feature Engineering:
Identify relevant features that can help the algorithm distinguish between normal and anomalous network behaviour. Extract features like packet counts, byte counts, communication frequency, and other relevant statistics.

Labelling Data:
Annotate the dataset with labels indicating normal and anomalous instances. For network traffic anomaly detection, this labelling can be based on statistical anomalies.

Data Splitting:
Split the dataset into training and testing sets. The training set is used to train the LightGBM model, while the testing set is used to evaluate its performance.

LightGBM Model Training:
Gradient Boosting: LightGBM is an ensemble learning technique that builds a strong predictive model by combining the predictions of multiple weak models, often decision trees.

Boosting Process: The algorithm iteratively builds decision trees to correct the errors of the previous ones. During each iteration, it focuses on instances that were misclassified in the previous step.

LightGBM Advantages: LightGBM is particularly efficient due to its leaf-wise tree growth strategy and histogram-based approach, making it faster and requiring less memory compared to other gradient boosting algorithms.

Hyper parameter Tuning:
Optimize the hyper parameters of the LightGBM model to enhance its performance. This may involve adjusting parameters like the learning rate, maximum depth of trees, and the number of boosting rounds.

Model Evaluation:
Evaluate the performance of the trained LightGBM model on the testing set using metrics such as accuracy, precision, recall, F1 score, or area under the ROC curve (AUC-ROC).

Anomaly Detection:
Use the trained LightGBM model to predict anomalies in real-time network traffic. Instances that deviate significantly from normal patterns are flagged as potential anomalies.

Monitoring and Updating:
Continuously monitor the network and update the model as needed to adapt to evolving patterns of normal and anomalous behaviour.

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

By employing LightGBM for network traffic anomaly detection, organizations can benefit from its speed, efficiency, and ability to handle large datasets, making it a suitable choice for real-time monitoring and detection of unusual activities in network traffic.

Conclusion

In conclusion, the implementation of network traffic anomaly detection using machine learning, specifically leveraging the Light Gradient Boosting Algorithm (LightGBM), has proven to be a significant advancement in the field. Through rigorous experimentation and comparison with existing methods, it has been demonstrated that the LightGBM algorithm outperforms its counterparts, providing superior accuracy, efficiency, and reliability in identifying and responding to network anomalies. The utilization of machine learning, and specifically LightGBM, has enhanced the capability to detect subtle deviations in network traffic patterns. The project's outcomes contribute to the broader landscape of network security by offering a robust solution that not only improves upon existing techniques but also provides a scalable and adaptable framework for real-world applications.

Our paper focused on enhancing network traffic anomaly detection through the implementation of a Light Gradient Boosting Machine (LightGBM) and the integration of both temporal and spatial features within the dataset. Through rigorous experimentation and evaluation, we demonstrated that our proposed system significantly outperformed the existing Naive Bayes system in terms of detection accuracy and efficiency. The incorporation of LightGBM allowed for more sophisticated and nuanced learning patterns, enabling the system to adapt to the dynamic nature of network traffic. By considering both temporal and spatial features, our model exhibited a deeper understanding of the contextual relationships within the data, leading to more precise anomaly detection.

The comparative analysis clearly showcased the superiority of our proposed approach, emphasizing its potential for real-world applications where accurate and timely anomaly detection is critical.

In summary, our paper contributes a robust solution to network traffic anomaly detection by leveraging advanced machine learning techniques. The demonstrated improvements over the existing Naive Bayes system validate the significance of our proposed approach, opening avenues for further research and deployment in enhancing the anomaly detection.

References

1. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2017). Network traffic anomaly detection and prevention: concepts, techniques, and tools. Springer.

2. Bhuyan, M. H., Bhattacharyya, D. K., Kalita, J. K., Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2017). Network traffic anomaly detection techniques and systems. Network Traffic Anomaly Detection and Prevention: Concepts, Techniques, and Tools, 115-169.

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

3. Radford, B. J., Apolonio, L. M., Trias, A. J., & Simpson, J. A. (2018). Network traffic anomaly detection using recurrent neural networks. arXiv preprint arXiv:1803.10769.

4. Xia, H., Fang, B., Roughan, M., Cho, K., & Tune, P. (2018). A basisevolution framework for network traffic anomaly detection. Computer Networks, 135, 15-31.

5. Du, Z., Ma, L., Li, H., Li, Q., Sun, G., & Liu, Z. (2018, June). Network traffic anomaly detection based on wavelet analysis. In 2018 IEEE 16th International Conference on Software Engineering Research, Management and Applications (SERA) (pp. 94-101). IEEE.

6. Kromkowski, P., Li, S., Zhao, W., Abraham, B., Osborne, A., & Brown, D. E. (2019, April). Evaluating statistical models for network traffic anomaly detection. In 2019 systems and information engineering design symposium (SIEDS) (pp. 1-6). IEEE.

7. Hwang, R. H., Peng, M. C., Huang, C. W., Lin, P. C., & Nguyen, V. L. (2020). An unsupervised deep learning model for early network traffic anomaly detection. IEEE Access, 8, 30387-30399.

8. Fotiadou, K., Velivassaki, T. H., Voulkidis, A., Skias, D., Tsekeridou, S., & Zahariadis, T. (2021). Network traffic anomaly detection via deep learning. Information, 12(5), 215.

9. Patil, R., Biradar, R., Ravi, V., Biradar, P., & Ghosh, U. (2022). Network traffic anomaly detection using PCA and BiGAN. Internet Technology Letters, 5(1), e235.

10. Pei, J., Zhong, K., Jan, M. A., & Li, J. (2022). Personalized federated learning framework for network traffic anomaly detection. Computer Networks, 209, 108906.