Designing a Machine Learning-Based Framework for Anomaly-based Network Intrusion Detection

Created by
Ayushman Singh
Raghav

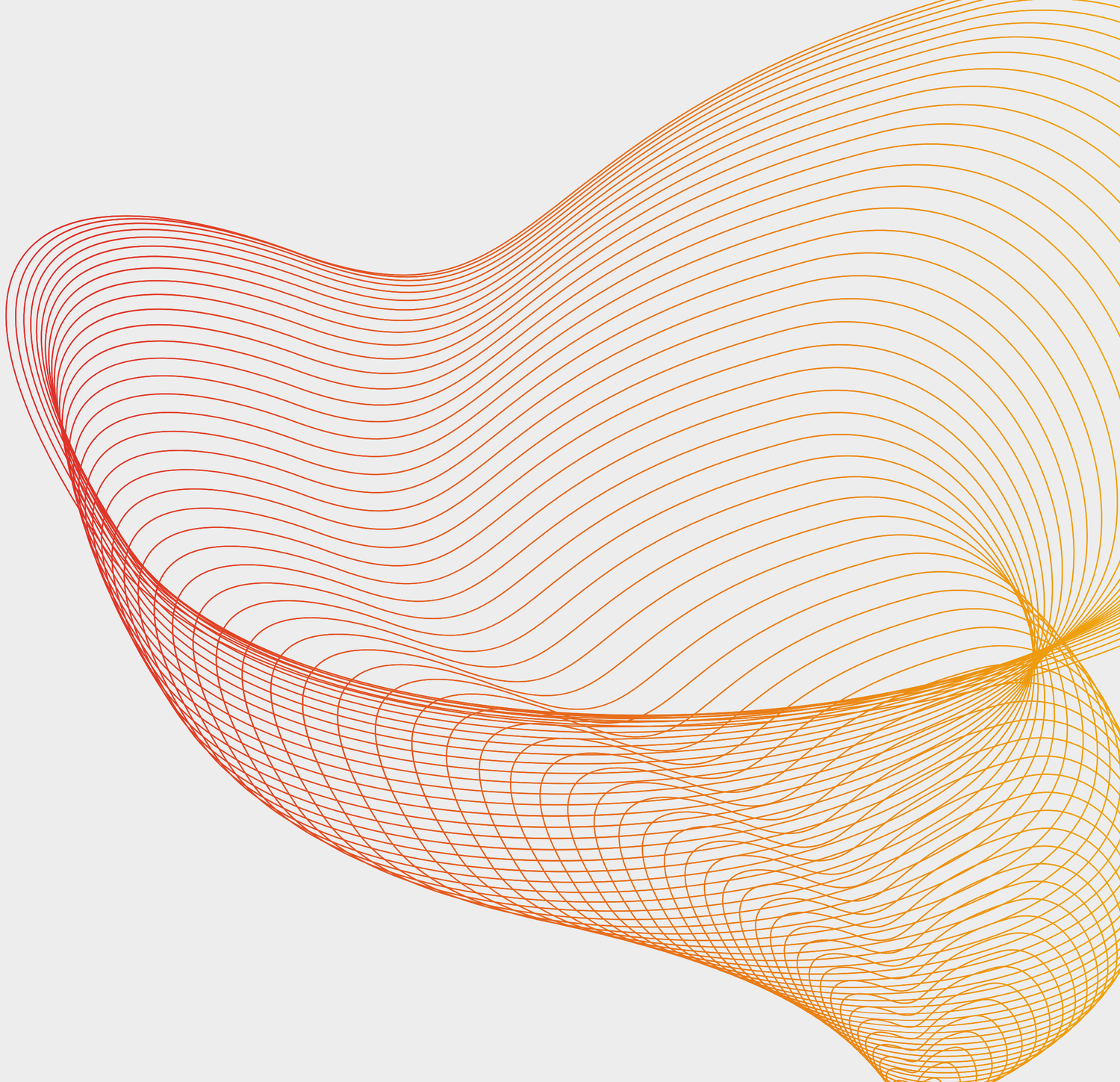


Table of Content

Introduction

Good Evening Everyone

Welcome to "Designing a Machine Learning-Based Framework for Anomaly-based Network Intrusion Detection." Today, we'll explore network security and anomaly detection. This research attempts to improve classification models under data imbalance conditions. Explore how we may solve this problem and improve network security

Research Objective

This approach involves monitoring network traffic and system behaviour to detect deviations from established baselines or normal patterns of activity. The study investigated and optimized three powerful algorithms: Random Forest, SVC, and XGBoost. The main goal was to create models that accurately identify positive cases, especially in anomaly detection where false negatives are critical. The study also investigated methods for achieving these to detect deviations from established baselines or normal patterns of activity.

Dataset:

The dataset was created based on 9 types of cyber attacks These attacks are used to target surveillance cameras and related systems.

Reconnaissance:

- **OS Scan:** The attacker uses the Network mapper tool to scan the network for hosts and their operating systems to identify potential vulnerabilities.
- **Fuzzing:** The attacker employs the S-Fuzz tool to search for vulnerabilities in the camera's web servers by sending random commands to their Common Gateway Interfaces (CGIs).

Man in the Middle:

- **Video Injection:** The attacker, using Video Jack, injects a recorded video clip into a live video stream, potentially compromising the integrity and authenticity of the video feed.
- **ARP MitM (Address Resolution Protocol):** The attacker utilizes Ettercap to intercept all LAN traffic through an ARP poisoning attack, potentially compromising confidentiality and integrity.
- **Active Wiretap:** The attacker employs an R.PI (Raspberry PI) 3B device to covertly intercept all LAN traffic by installing an active wiretap (network bridge) on an exposed cable, potentially compromising confidentiality.

Denial of Service (DoS):

- **SSDP Flood (Simple Service Discovery Protocol):** The attacker, using Saddam, overloads the DVR by causing cameras to spam the server with UPnP advertisements, potentially affecting availability.
- **SYN DoS (TCP SYN flood) :** The attacker, with Hping3, disables a camera's video stream by overloading its web server, impacting availability.
- **SSL Renegotiation (Secure Sockets Layer) :** The attacker uses THC to disable a camera's video stream by sending numerous SSL renegotiation packets to the camera, affecting availability.

Dataset:

Botnet Malware:

- **Mirai:** The attacker exploits default credentials to infect IoT devices with the Mirai malware via Telnet. Once infected, the malware scans for new vulnerable victims in the network, potentially compromising confidentiality, integrity, and availability.

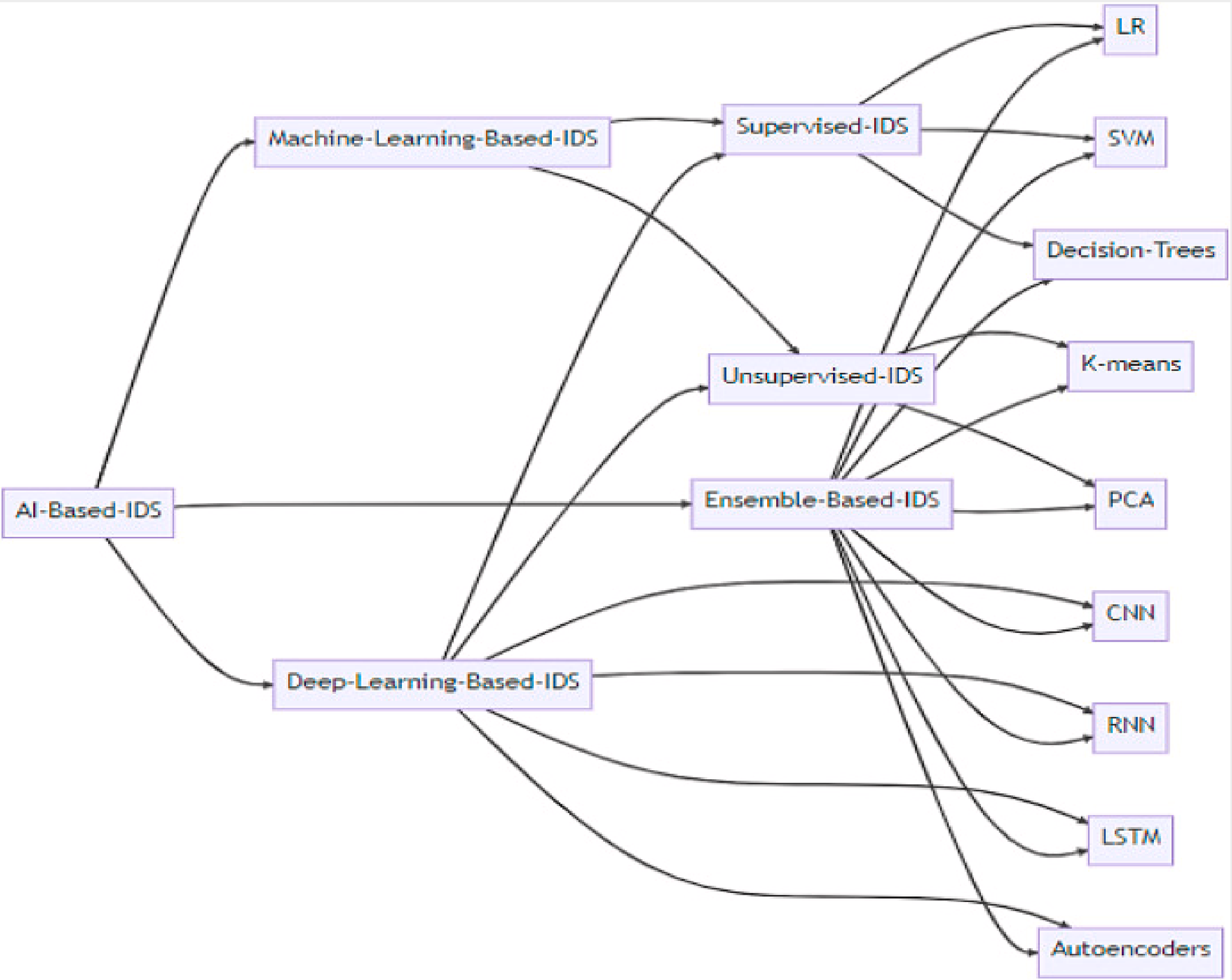
A network connection or activity is represented by each row in the dataset, which is organized as a CSV. Multiple properties or columns in the dataset capture various facets of network relationships. The following standout properties are among the prominent ones: "Duration," "protocol_type," "service," "flag," "src_bytes," "dst_bytes," and numerous others. These characteristics reveal details on the properties of network traffic.

Types of Network Traffic: The dataset seems to encompass different types of network traffic, such as **"TCP"** (Transmission Control Protocol), **"ICMP"**(Internet Control Message Protocol), and **"UDP"**(User datagram protocol) which are captured in the "protocol_type" column. Each type of traffic may have different characteristics and behaviours.

Network Features: Features like **"src_bytes"** and **"dst_bytes"** likely represent the number of source and destination bytes in the network connection. Other features like **"serror_rate"** and **"rerror_rate"** denotes error rates in the network communication.

Labels: The last column, labelled **"class"** specifies each network connection's class or category. It likely indicates whether a particular connection is considered **"normal"** or an **"anomaly".** This is essential for network intrusion detection or anomaly detection tasks.

AI-based intrusion detection techniques



Methodology Overview

Key Steps

- **Algorithm Selection**: Choose Random Forest, SVC, and XGBoost for their unique characteristics and strengths in handling imbalanced datasets.
- **Hyperparameter Tuning**: Systematically optimized hyperparameters to maximize model performance.
- **Data Preprocessing**: Prepared data for modeling through cleaning, normalization, and addressing missing values.

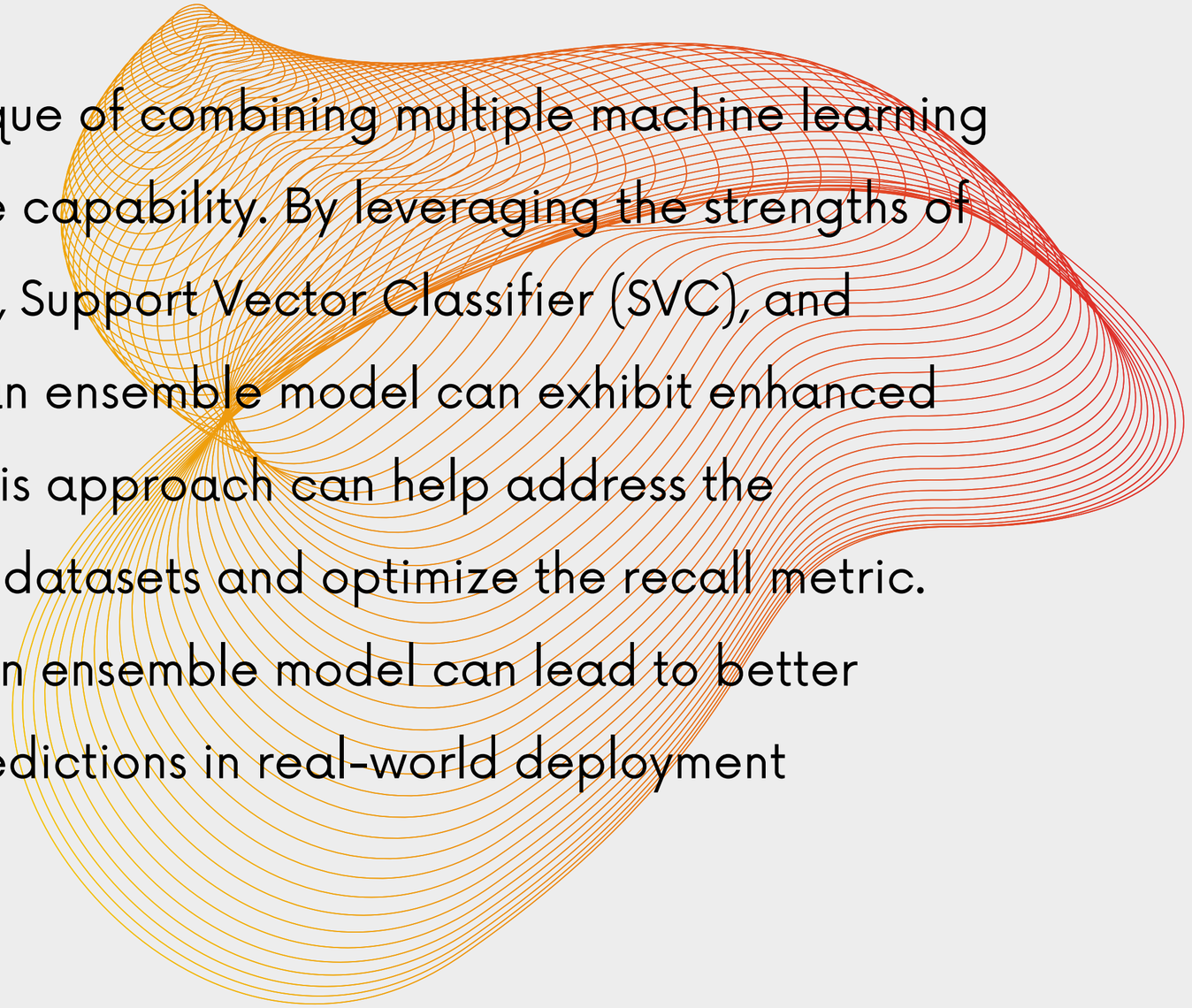
This comprehensive approach aimed to extract the best performance from each algorithm while mitigating the impact of class imbalance.

Model Performance

- **Random Forest Classifier** - This was assessed based on its recall metric, which assesses the model's ability to detect positive cases. The best classifier setup used 100 estimators and had a recall score of 0.958. The attribute 'flag_SF' has the most weight, suggesting its importance in class differentiation.
- **The Support Vector Classifier (SVC)** - This was constructed using sci-kit-learn and the hyperparameter tweaking was done using Grid Search and cross-validation. A pipeline method was used, incorporating SMOTE for class imbalance. The experimental configuration in this study resulted in a notable recall score of approximately 0.958.
- **The Extreme Gradient Boosting (XGBoost)** - This approach has been shown to effectively optimize recall and solve imbalanced datasets.The XGBoost Classifier was optimized with a learning rate of 0.1 and 130 boosting rounds. This configuration outperformed previous models, achieving a recall score of approximately 0.959.

Ensemble of Models

Ensemble of models refers to the technique of combining multiple machine learning models to improve the overall predictive capability. By leveraging the strengths of different models, such as Random Forest, Support Vector Classifier (SVC), and Extreme Gradient Boosting (XGBoost), an ensemble model can exhibit enhanced performance across diverse contexts. This approach can help address the challenges associated with imbalanced datasets and optimize the recall metric. The integration of diverse classifiers in an ensemble model can lead to better decision-making and more accurate predictions in real-world deployment scenarios.



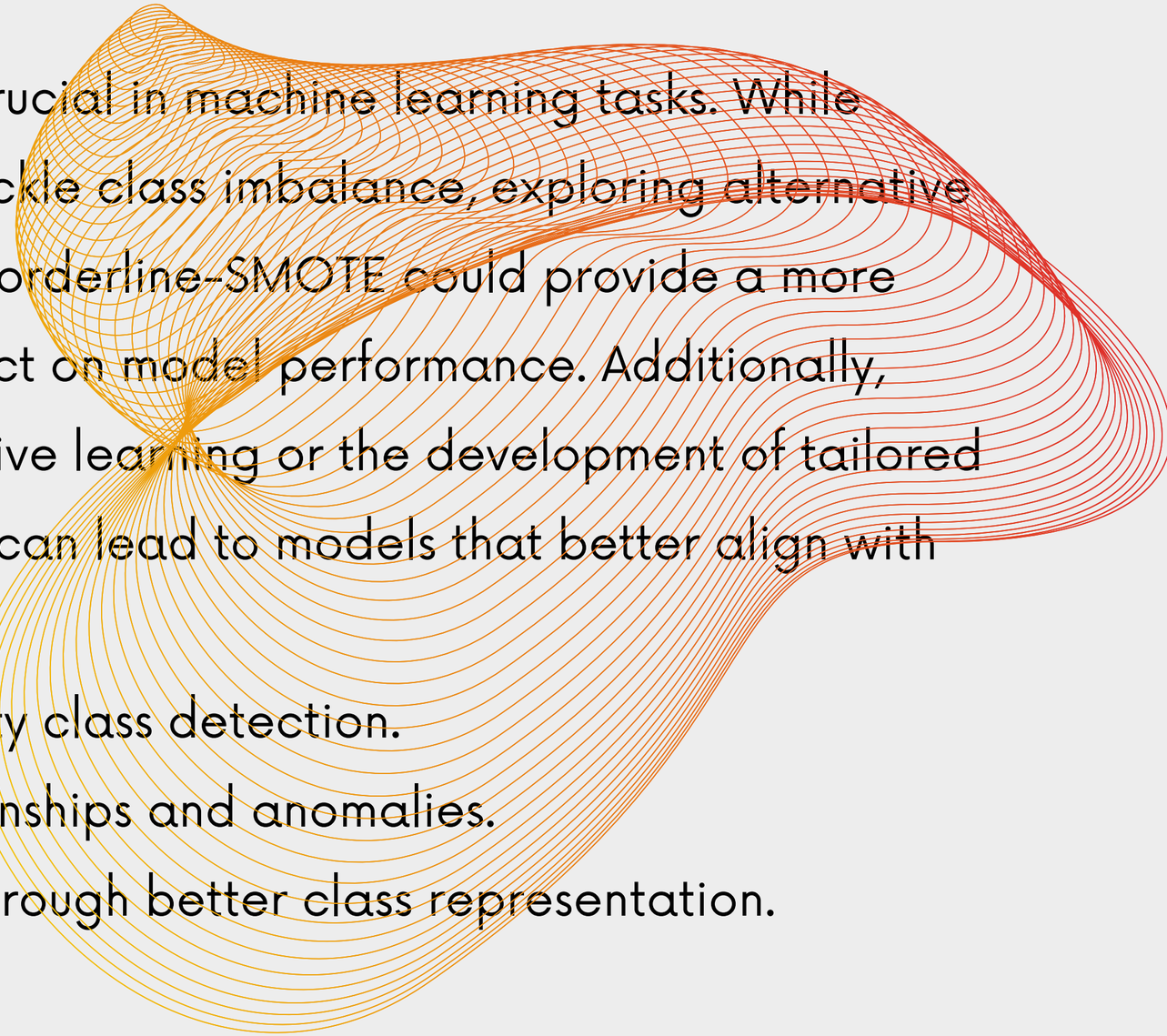
Feature engineering

Feature engineering is an important aspect of machine learning that involves transforming and selecting relevant features from the dataset to improve the performance of a model. In the present study, the focus was primarily on model selection and hyperparameter tuning. However, it is worth noting that feature engineering could be a potential area of investigation in future research endeavors. By exploring feature transformations, aggregations, or interactions specific to a certain domain, latent information can be unveiled and the performance of a model can be enhanced. Additionally, the application of dimensionality reduction techniques in feature engineering can help mitigate the impact of high dimensionality and potentially improve the efficacy of models.

Handling Class Imbalance

Addressing the issue of class imbalance is crucial in machine learning tasks. While SMOTE was employed in this research to tackle class imbalance, exploring alternative resampling techniques such as ADASYN or Borderline-SMOTE could provide a more comprehensive understanding of their impact on model performance. Additionally, investigating methodologies like cost-sensitive learning or the development of tailored loss functions specific to the given problem can lead to models that better align with real-world requirements.

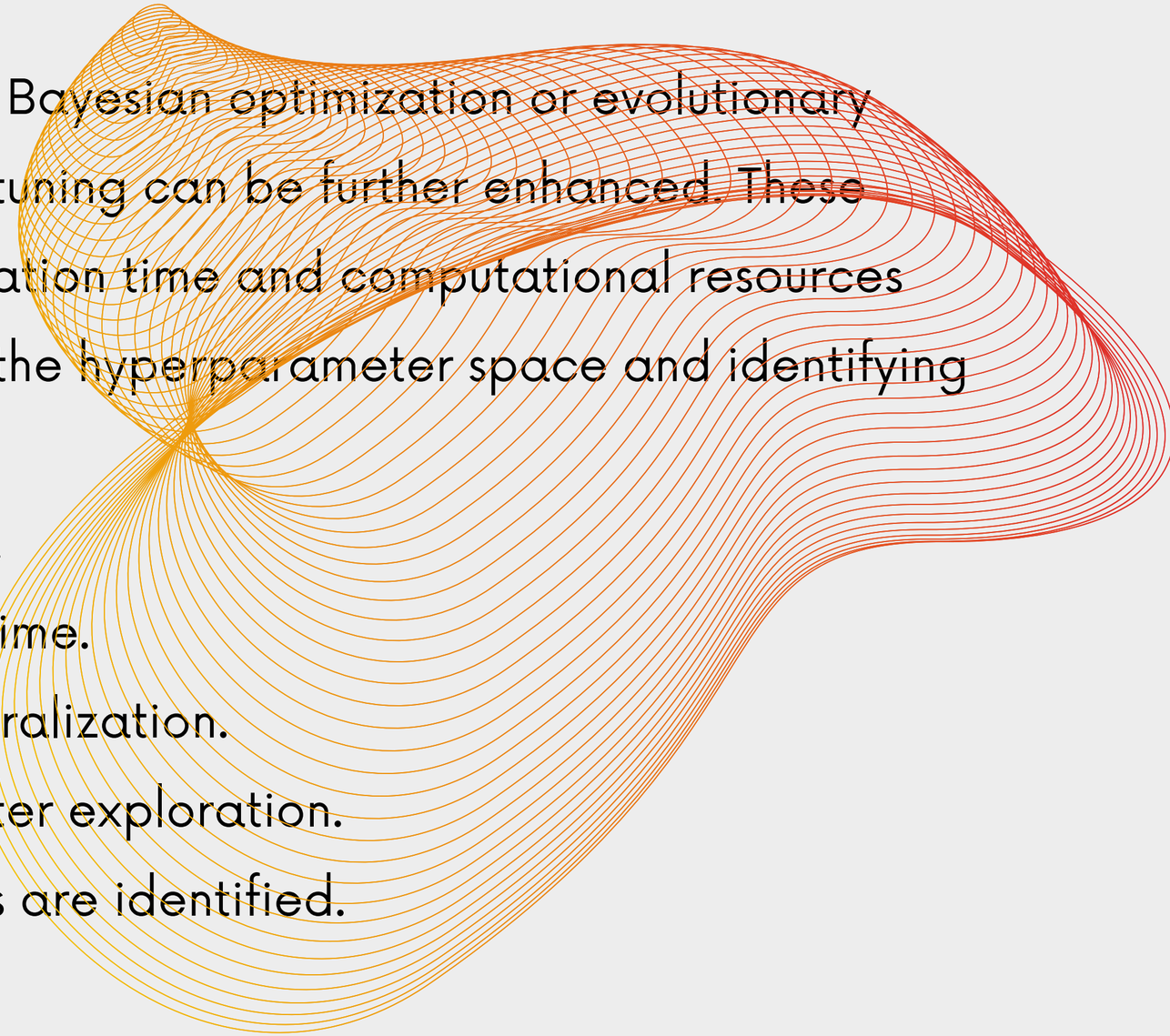
- Improved model performance on minority class detection.
- Enhanced understanding of class relationships and anomalies.
- Real-world implementation alignment through better class representation.



Advanced Hyperparameter Tuning

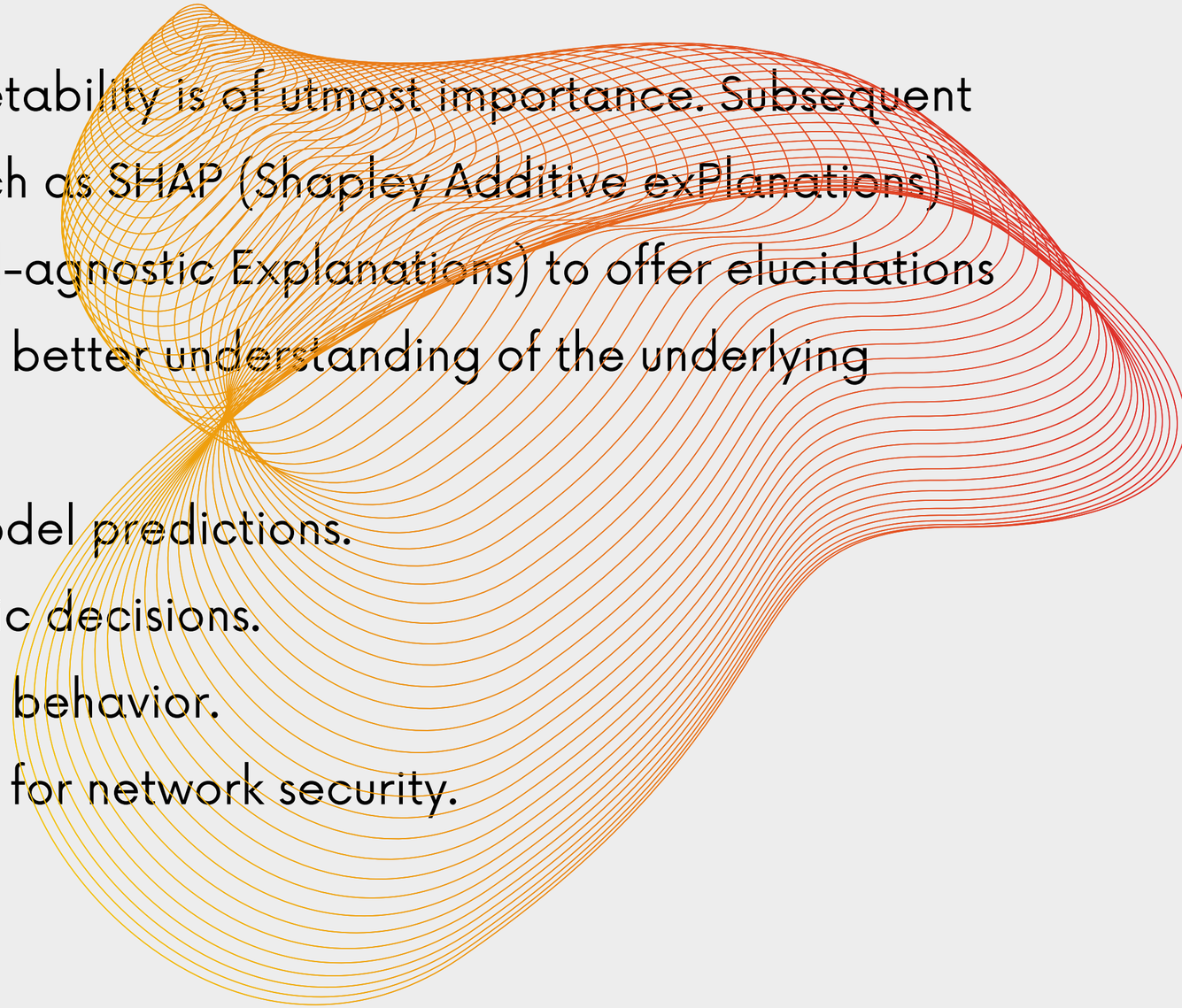
By employing advanced techniques such as Bayesian optimization or evolutionary algorithms, the process of hyperparameter tuning can be further enhanced. These strategies have the potential to reduce iteration time and computational resources while improving the efficiency of exploring the hyperparameter space and identifying optimal configurations.

- Faster convergence to optimal solutions.
- Reduced computational resources and time.
- Improved model performance and generalization.
- Boosting the efficiency of hyperparameter exploration.
- Ensuring the best possible configurations are identified.



Explainability and Interpretability

Ensuring model transparency and interpretability is of utmost importance. Subsequent investigations could employ strategies such as SHAP (Shapley Additive exPlanations) values or LIME (Local Interpretable Model-agnostic Explanations) to offer elucidations for model predictions and contribute to a better understanding of the underlying rationale behind a particular prediction.



- Enhanced trust and acceptance of model predictions.
- Insights into the reasons behind specific decisions.
- Identifying features driving anomalous behavior.
- Facilitating informed decision-making for network security.

Key Takeaways

1. Research Achievements

- Improved recall performance in network anomaly detection.
- Addressed class imbalance using SMOTE and alternative techniques.
- Explored various classification models and hyperparameter tuning.

2. Significance of Recall

- Critical in network security for identifying true positives and minimizing false negatives.
- Enables timely response to potential threats and intrusions.

3. Future Research Directions

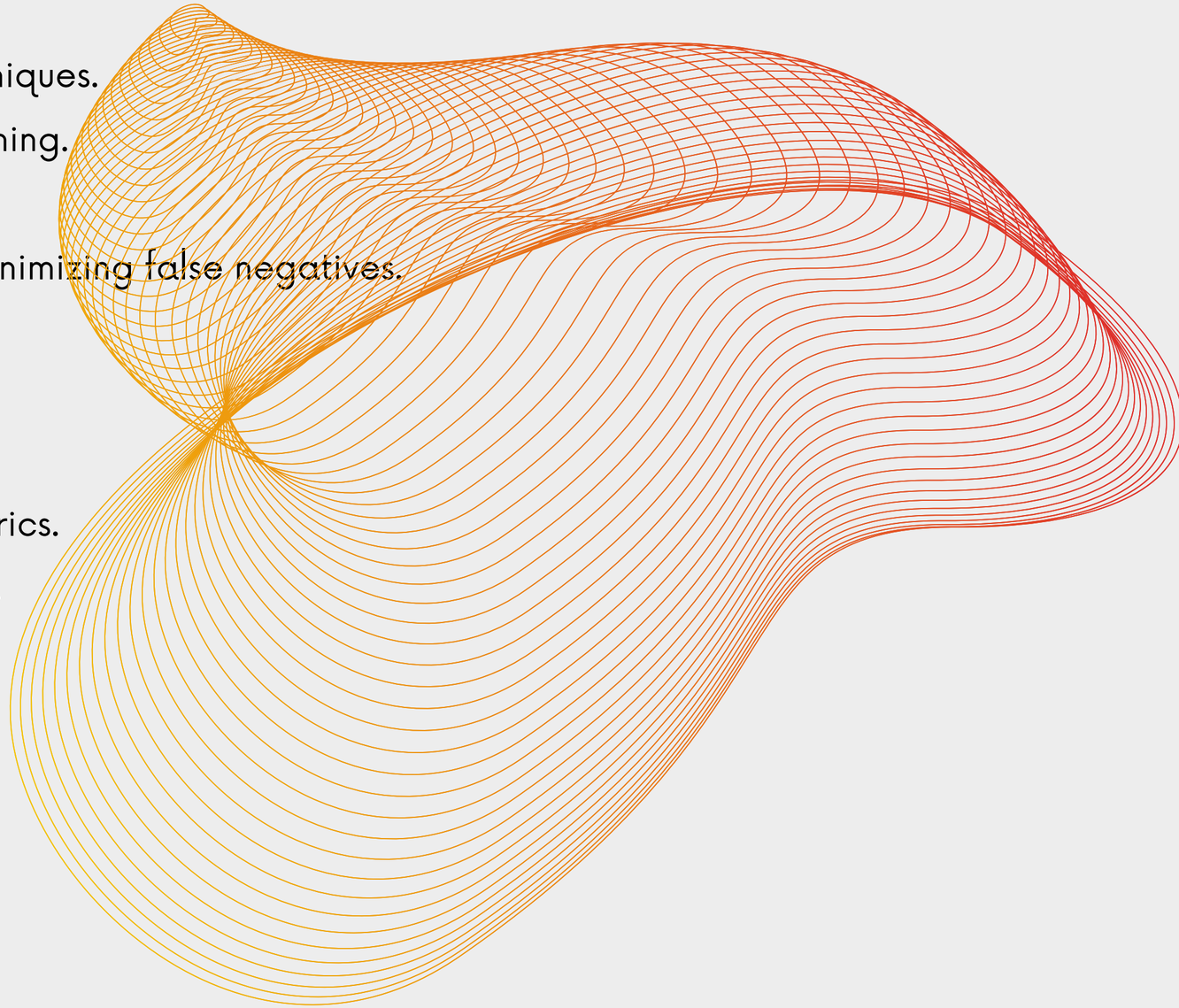
- Ensembling diverse models for enhanced performance.
- Further exploration of feature engineering and evaluation metrics.
- Advancing explainability and interpretability for transparency.

4. Real-World Impact

- Facilitates informed decision-making for network security.
- Enhances model adoption and trust in practical applications.

5. Ongoing Inquiry

- Continual research for improved anomaly detection models.
- Aligning models with real-world requirements and challenges.



Thank You