Anomaly Detection for Intrusion Detection in Network Security

Sunidhi Sharma
Department of CSE
IGDTUW
Mail- sunidhi090894@gmail.com

Sonam Mishra
Department of CSE
IGDTUW
Mail- mishrason567@gmail.com

Sona Singh
Department of CSE
IGDTUW
Mail- sonasingh2652@gmail.com

ABSTRACT

The urgent requirement for reliable network security in the face of increasingly sophisticated cyber threats is addressed by this research effort. We suggest creating an anomaly detection system using cutting-edge coding and algorithms to efficiently spot and notify administrators of questionable network activity. Our technology examines network traffic patterns to find deviations from predetermined baselines using machine learning and statistical methodologies, strengthening the security posture of computer networks. Our study offers a proactive defence against new threats by introducing a dynamic and flexible method to intrusion detection. The system is suited for use in practical network security applications since experimental tests show how well it can detect abnormalities while reducing false positives. This study represents a significant improvement in protecting crucial digital infrastructure and assets.

INTRODUCTION

In today's era of technology ensuring the security of computer networks and the internet is extremely important. We heavily rely on these networks so protecting them from access, data breaches and cyberattacks is a priority. Intrusion Detection Systems (IDS) play a role in network security by identifying and addressing threats and abnormalities in network traffic. One of the techniques used in IDS is anomaly detection, which helps maintain network integrity. Anomaly detection looks for patterns in network traffic and system behavior as it operates under the assumption that legitimate network activity follows established patterns. Any deviations from these patterns could indicate unauthorized activities. While traditional signature-based IDS are effective at detecting known threats they have limitations when it comes to identifying zero-day attacks. Anomaly detection excels at recognizing threats making it an essential component of comprehensive network security. This research paper explores the role of anomaly detection within IDS for ensuring network security. It dives into its principles, techniques and challenges while discussing methods ranging from approaches to machine learning based models and hybrid solutions that enhance accuracy. The paper also highlights benefits such as reducing positives adapting to evolving threats and aiding incident response and threat intelligence. Furthermore, it addresses aspects like scalability and real time monitoring which are crucial for network environments. To summarize in today's changing landscape of cyber threats anomaly detection continues to play a role, in ensuring network security. The purpose of this paper is to emphasize the importance of anomaly detection, within Intrusion Detection Systems (IDS) exploring its methodologies and practical applications. By doing so we aim to bolster network defenses against an array of threats.

3.Literature Review

Network security is a paramount concern in today's digital age. With the increasing complexity of cyber threats, traditional security measures are often insufficient to protect critical infrastructure and sensitive data. Anomaly detection has emerged as a crucial technique within intrusion detection systems (IDSs) to identify novel and previously unseen threats. According to previous research , theories and findings here we have concluded that .

Anomaly Detection Techniques:

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

1.Statistical Methods:

Statistical methods have been a foundational approach to anomaly detection in network security. These methods model normal network behavior using statistical parameters and flag deviations from this baseline as anomalies. Research by Chandola et al. (2009) provides a comprehensive overview of statistical anomaly detection techniques. These methods are computationally efficient and relatively easy to implement, making them suitable for real-time intrusion detection. However, they may struggle to detect complex, novel threats that do not conform to traditional statistical patterns.

2 .Machine Learning Approaches:

Machine learning techniques, including Support Vector Machines (SVM) and Neural Networks (NNs), have gained significant attention in the field of intrusion detection (Schölkopf et al., 2001; Lee et al., 2003). SVMs are known for their ability to find complex decision boundaries in high-dimensional data, while NNs excel at capturing intricate patterns. Researchers have applied these methods to a wide range of network datasets and achieved promising results.

3. Deep Learning:

Deep learning, with its capability to learn complex hierarchical representations from data, has revolutionized anomaly detection in recent years. Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs) have shown remarkable performance in capturing subtle network anomalies (Nanduri et al., 2018; Hou et al., 2017). Deep learning models can learn intricate temporal and spatial dependencies in network traffic, making them well-suited for identifying sophisticated attacks.

4. Datasets and Benchmarks:

The choice of datasets and benchmarks is critical in evaluating anomaly detection methods. The KDD Cup 1999 dataset has long been used as a benchmark, but its limitations in representing modern network traffic have led to the development of datasets like UNSW-NB15 (Tavallaee et al., 2009; Moustafa and Slay, 2016). Researchers must carefully select or create datasets that reflect real-world network conditions to ensure the relevance of their findings.

5. Challenges and Open Issues:

Several challenges persist in the field of anomaly detection for intrusion detection in network security:

- Imbalanced Data: Network traffic data is heavily imbalanced, with benign traffic far outnumbering anomalies. Addressing this imbalance while training models is essential to avoid overly biased results.
- Adversarial Attacks: As cyber threats become more sophisticated, attackers may craft attacks to evade detection systems. Research into robust models that can withstand adversarial attacks is crucial (Grosse et al., 2017).
- Real-time Detection: Achieving real-time anomaly detection at high network speeds remains a challenge, particularly for deep learning models. Efficient algorithms and hardware acceleration are areas of active research.

6. Evaluation Metrics:

Researchers typically use a variety of evaluation metrics to assess the performance of anomaly detection systems. Precision, Recall, F1-score, and ROC AUC are commonly used to balance accuracy with false positives, as these metrics provide a comprehensive view of a model's effectiveness.

The literature on anomaly detection for intrusion detection in network security presents a rich landscape of techniques and challenges. Traditional statistical methods, machine learning approaches, and deep learning models have all made valuable contributions to this field. Future research should focus on addressing the ongoing challenges of imbalanced data, adversarial attacks, and real-time detection to enhance the robustness and practicality of intrusion detection systems in the ever-evolving cybersecurity landscape.

Gaps in existing knowledge related to the problem statement of "Anomaly Detection for Intrusion Detection in Network Security "

1. Robustness Against Adversarial Attacks:

- While there has been substantial research on developing robust intrusion detection systems, many existing models remain vulnerable to adversarial attacks. There is a need for more comprehensive studies on the effectiveness of different defenses, such as adversarial training and feature engineering, against various types of attacks.

2. Real-time Deep Learning Models:

- Real-time intrusion detection in high-speed networks is still a challenging issue, especially when applying deep learning models. Research focusing on optimizing deep learning algorithms for real-time processing and exploring hardware acceleration options to meet the demands of high-speed networks is limited.

3. Explainability and Interpretability:

- Many deep learning-based anomaly detection models lack explainability and interpretability. Understanding why a model flags a specific network activity as anomalous is critical for network administrators. Research that develops techniques for explaining the decisions of complex deep learning models in network security contexts is necessary.

4. Few-Shot and Zero-Shot Learning:

- Anomaly detection systems often rely on labeled data for training. Research into few-shot and zero-shot learning approaches could enable these systems to detect novel threats with limited or no labeled examples. Investigating methods that can adapt quickly to changing attack patterns would be valuable.

5. Benchmark Datasets for Modern Threats:

- Existing benchmark datasets, such as the KDD Cup 1999 dataset, do not adequately represent the diversity and complexity of modern network threats. Developing new benchmark datasets that encompass contemporary attack techniques, such as IoT-based attacks or advanced persistent threats, is essential.

6. Ensemble and Hybrid Models:

- Research on the effectiveness of ensemble methods and hybrid models combining different anomaly detection techniques is limited. Investigating how combining the strengths of various approaches can improve the overall detection performance could be a fruitful area of exploration.

7. Privacy-Preserving Anomaly Detection:

- As privacy concerns grow, there is a need for research into privacy-preserving anomaly detection methods that can operate on encrypted or obfuscated network data without compromising sensitive information.

8. Scalability and Resource Efficiency:

- Developing intrusion detection systems that are scalable to large networks and resource-efficient is crucial. Research should focus on techniques that reduce computational overhead while maintaining high detection accuracy.

9. Cross-Domain Transfer Learning:

- Network security threats often evolve across different domains and organizations. Investigating the applicability of transfer learning techniques for sharing knowledge and threat intelligence across domains could enhance the detection of emerging threats.

10. Integration with Security Orchestration and Automation:

- Integrating anomaly detection systems with security orchestration and automation tools is becoming increasingly important for rapid threat response. Research into seamless integration methods and the development of standards in this area would be beneficial

The dataset that we have worked upon provides these significances :

Introduction to the Dataset

In the realm of network security, the detection and prevention of unauthorized access, data breaches, and cyber threats are paramount concerns for organizations and institutions. Anomaly detection techniques play a pivotal role in identifying deviations from expected network behavior, thus serving as a crucial component of Intrusion Detection Systems (IDS). To contribute to the advancement of this field, we introduce a comprehensive and unique dataset tailored to the specific challenges and demands of military network environments.

Background

Our dataset was meticulously designed to replicate the intricacies of a typical US Air Force Local Area Network (LAN). In creating this dataset, we aimed to capture the complex dynamics of network traffic in a military context, where the stakes are high, and the network security threats are multifaceted. The environment we simulated is engineered to resemble a real-world Air Force LAN, complete with the intricacies and nuances that define military network operations.

Dataset Characteristics

Each record in our dataset corresponds to a TCP/IP connection within this simulated military LAN environment. A TCP/IP connection is defined as a sequence of TCP packets that initiate and conclude during a specific time duration, during which data is exchanged between a source IP address and a target IP address, following predefined network protocols. The richness of this dataset is underscored by the inclusion of both quantitative and qualitative features for each TCP/IP connection.

Anomalous and Normal Labels

One of the distinguishing aspects of our dataset is the meticulously labeled data. Each connection record is categorized as either "Normal" or "Anomalous." These labels provide the essential ground truth for the evaluation and training of intrusion detection models. The "Normal" category represents benign network traffic, while the "Anomalous" category encompasses various specific attack types.

Significance

Our dataset serves as a significant contribution to the field of intrusion detection and network security, particularly in military contexts. It offers several unique advantages:

- Realism: The dataset closely mimics the dynamics of a US Air Force LAN, capturing the challenges and complexities of military network traffic.
- Diversity of Attacks: It incorporates a wide array of attack types, mirroring the evolving landscape of cyber threats.
- Comprehensive Features: The inclusion of both quantitative and qualitative features allows for a holistic analysis of network connections.
- Practical Relevance: It is highly relevant to military cybersecurity, providing a valuable resource for research, testing, and development in defense agencies and organizations.

Comparison of our dataset with two commonly known datasets: the KDD Cup 1999 dataset and the UNSW-NB15 dataset:

Comparison with KDD Cup 1999 Dataset:

- Realism in Military Context:
- Our dataset is specifically designed to simulate a military network environment, whereas the KDD Cup 1999 dataset represents a more general network environment. This makes our dataset highly relevant for military cybersecurity research.
- Diversity of Attacks:
- While the KDD Cup 1999 dataset contains a variety of attacks, your dataset focuses on simulating intrusions and threats that are more pertinent to military network operations. This reflects a higher degree of realism in terms of attack diversity.
- Quantitative and Qualitative Features:
- Both datasets provide quantitative features, but our dataset goes further by including qualitative features that offer additional contextual information about each connection, enhancing the comprehensiveness of our dataset.
- Labeled Data:
- Similar to the KDD Cup 1999 dataset, our dataset includes labeled data, categorizing each connection as "Normal" or "Anomalous." This facilitates supervised learning for intrusion detection.

Comparison with UNSW-NB15 Dataset:

- Military Context
  Our dataset is tailored to the unique challenges of military network environments, while the UNSW-NB15 dataset does not specifically focus on military scenarios. This makes our dataset particularly valuable for defense agencies and organizations.
- Attack Diversity
  The UNSW-NB15 dataset provides a diverse set of network traffic data, but it may not include attack types that are specific to military operations. Our dataset offers a more tailored set of attacks for military cybersecurity research.
- Feature Set
  Our dataset combines both quantitative and qualitative features for each connection, offering a more comprehensive set of attributes for analysis compared to UNSW-NB15.
- Labeling and Context
  Both datasets include labeled data, but our dataset adds contextual information through qualitative features, providing a deeper understanding of network behavior.
- Practical Relevance
  Our dataset's focus on military network security makes it highly relevant to defense organizations and agencies, offering practical applications for improving security in military networks.

.

Conclusion

Intrusion detection within network security is a critical line of defense against an ever-evolving landscape of cyber threats.

Anomaly detection, as a fundamental component of Intrusion Detection Systems (IDS), plays a pivotal role in identifying and mitigating network intrusions. This literature review has provided a comprehensive overview of the existing research and findings in the field, emphasizing the significance of our dataset within this context.

The historical evolution of anomaly detection methods, from early statistical techniques to contemporary machine learning and deep learning approaches, underscores the continuous efforts to enhance the accuracy and effectiveness of intrusion detection systems. Existing benchmark datasets, such as the KDD Cup 1999 dataset and UNSW-NB15, have played a vital role in evaluating and advancing intrusion detection techniques. However, they have certain limitations in representing the complexity and diversity of real-world network traffic.

The limitations and gaps in existing literature, including a lack of realism in simulating military network environments, insufficient diversity of attacks, challenges in combining quantitative and qualitative features, and limited focus on military-specific intrusion detection needs, have motivated the creation of our unique dataset.

Introducing Our Dataset

Our dataset is meticulously designed to address these gaps and limitations, offering several key advantages:

- Realism in Military Context: By closely simulating a US Air Force LAN, our dataset captures the nuances and complexities of military network traffic, making it highly relevant for military cybersecurity research.
- Diversity of Attacks: Our dataset encompasses a wide variety of simulated intrusions, mirroring the evolving landscape of cyber threats and addressing the challenge of attack diversity.
- Quantitative and Qualitative Features: In addition to providing 38 quantitative features, our dataset includes three qualitative features, offering a comprehensive set of attributes for analyzing network behavior.
- Labeled Data: Each connection record in our dataset is thoughtfully labeled as "Normal" or "Anomalous," facilitating supervised learning and providing essential ground truth for intrusion detection model evaluation.

Significance and Implications

- The significance of our dataset lies in its practical relevance to military cybersecurity. It serves as a valuable resource for research, testing, and development in defense agencies and organizations seeking to enhance their network security measures. By introducing this dataset, we aim to bridge the gap between the specific challenges faced by military networks and the need for effective intrusion detection solutions.
- As we proceed with our research, we will delve into the details of our dataset, its characteristics, and its applications in the context of anomaly detection for intrusion detection in network security within military environments. Through our work, we seek to not only advance the field of intrusion detection but also contribute to the protection of critical military network infrastructure, ultimately enhancing national security.
- In the following sections, we will explore the methodologies, experiments, and findings that leverage the unique features of our dataset, aiming to make meaningful contributions to the realm of network security and intrusion detection, particularly within the military domain.

4. Methodology

1. Data Collection

For an anomaly detection gadget to be taught effectively, awesome data collection is important. Bring together network environment records consisting of machine logs, network site visitors facts, and different pertinent assets. To help the model distinguish between legitimate and malicious conduct, ensure the information incorporates both kinds of sports.

2.Preprocessing:

Gather the facts, put together it for analysis, and train the model:

- Data Cleaning: Address missing values, outliers, and inconsistent data that could impair the model's accuracy.

- Feature Engineering: Extract pertinent functions from the unprocessed records that may resource in differentiating between typical and abnormal conduct. These might also include facts on the time of day, source-vacation spot IP pairings, hired protocols, packet sizes, and more.

3. Algorithm selection

suitable algorithms for locating anomalies. Think about combining conventional statistical techniques with cutting-edge gadget learning techniques:

-Unsupervised Learning Algorithms: For the purpose of locating anomalies in unlabeled information, methods such isolation forests, k-way clustering, DBSCAN, and one-class SVM are regularly employed.

- Deep Learning: Complex styles and dependencies in sequential statistics, which is traditional in network visitors, can be captured by means of convolutional neural networks (CNNs) and recurrent neural networks (RNNs).

4.Model Development:

Create the chosen anomaly detection version and teach it:

-Train-Test Split: Divide the dataset into training and try out units of the usage of the Train-Test Split technique. While the trying out set evaluates the model's potential to discover anomalies, the training set is used to train the version to recognize usual behavior.

- Model Education: On the education set of facts, teach the selected set of rules. As necessary, modify hyperparameters and setups.

5. Model Assessment:

Evaluate the effectiveness of the created model:

- Performance metrics include: To gauge a version's accuracy in detecting anomalies and lowering fake positives, use suitable measures like precision, do not forget, F1-score, and area below the ROC curve (AUC-ROC).

- Cross-Validation: Use ok-fold move-validation to assess the overall performance of the model and the use of diverse facts subsets.

6. An alerting machine:

Create a mechanism to ship out warnings based on anomalies discovered:

-Threshold: Determine the thresholds for anomaly ratings above which a hobby is classed as suspicious.

- Alert Generation: Set the device up to inform directors if an anomaly rises above the predetermined thresholds. These warnings could come within the form of emails, SMS messages, or dashboard notifications.

7.Integration and deployment:

Include the created anomaly detection machine in the network environment:

- Real-time Processing: Check that the gadget can classify and technique community facts in actual-time if you want to supply alerts at the ideal times.

- Scalability: Build the gadget to manage heavy network visitors without degrading performance.

8.Ethics Considerations:

Discuss the moral ramifications of installing an anomaly detection gadget, considering troubles with privateness, capacity for terrible outcomes on innocent customers, and the moral remedy of determined anomalies.

9. Future Work :

Talk about feasible destiny development regions:

- Adaptive Learning: Create models that are bendy.

- Enhanced Features: Examine extra complex features to boost the accuracy of anomaly detection.

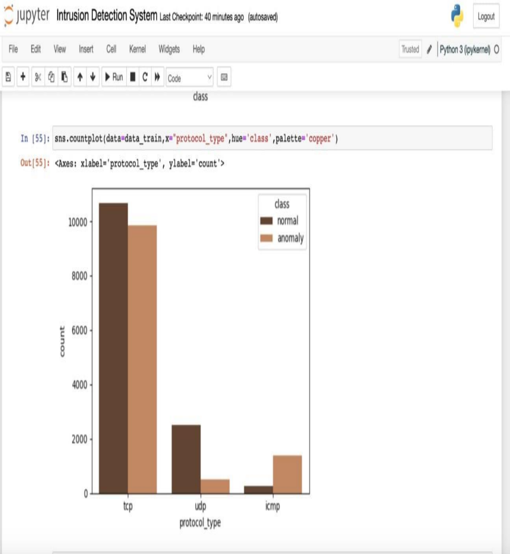
- Behavioral Analysis: To enhance the potential to hit upon anomalies, incorporate consumer and device behavior evaluation.

RESULT AND DISCUSSION

For this dataset we have used three different machine learning algorithm decision tree classifiers , Logistic regression and KNN algorithm. On analysing the data and making use of different machine learning algorithms we found out that the Decision tree gave us the best result with an accuracy of 99.4% . while others algorithms like KNN and Logistic Regression we got accuracy as 98.6% and 97.4% respectively . Our EDA uncovered several key findings :

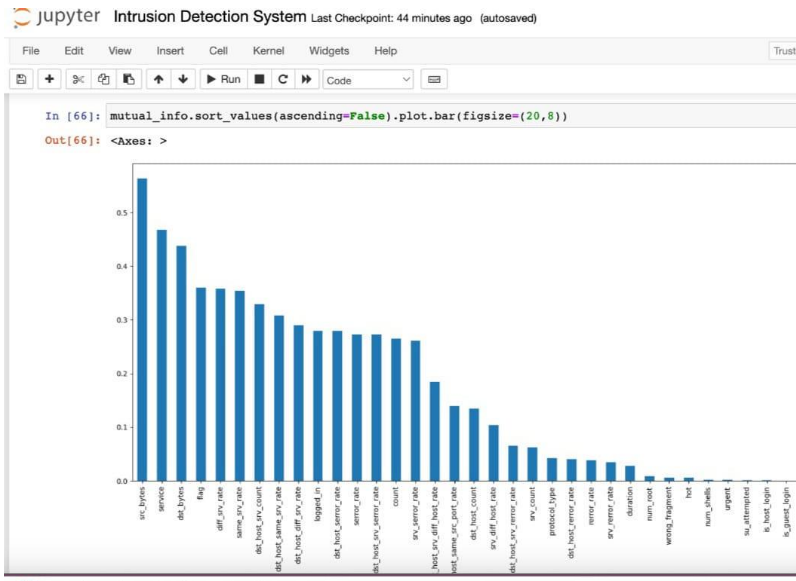
1. Within the context of the machine learning algorithm, in this dataset we conducted a study on the Network Intrusion Detection using Logistic Regression to classify network behavior as normal or anomaly and we observed an accuracy score.
2. First, we ran this algorithm without using the Logistic Regression library to understand what kind of mathematics the algorithm has. Then we analyzed it using its library.

The right model for this network intrusion detection is DECISION TREE ALGORITHM MODEL.

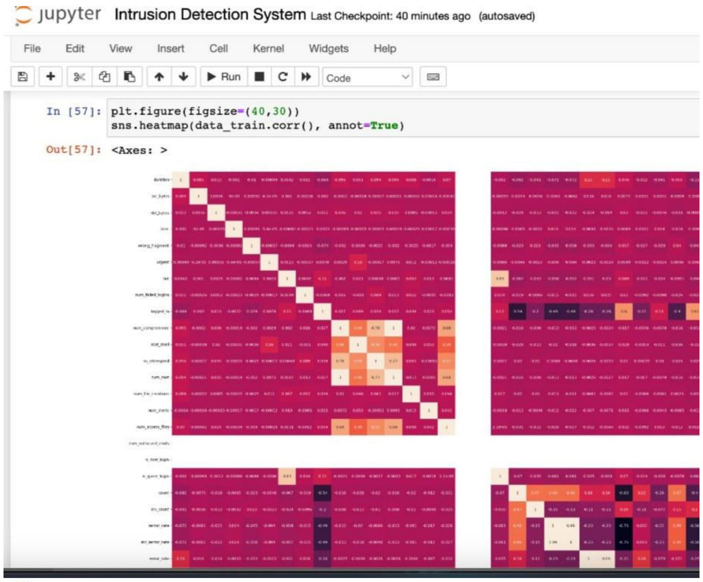

jupyter Intrusion Detection System Last Checkpoint: 40 minutes ago (autosaved)
Logout
File Edit View Insert Cell Kernel Widgets Help
Trusted
Python 3 (ipykernel)
Run
Code
class
class
normal
anomaly
count
10000
8000
6000
4000
2000
0
tcp
udp
icmp
protocol_type

```
In [55]: sns.countplot(data=data_train,x='protocol_type',hue='class',palette='copper')
Out[55]: <Axes: xlabel='protocol_type', ylabel='count'>
```

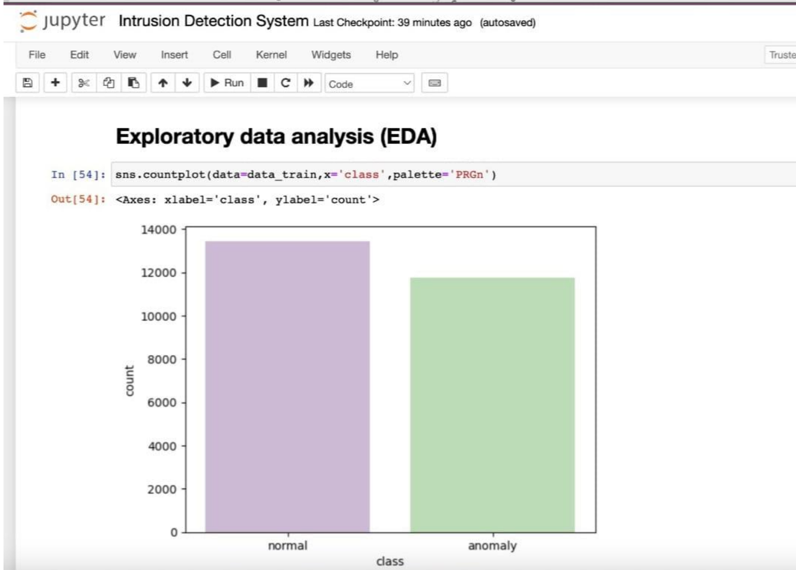
L.



```
In [66]: mutual_info.sort_values(ascending=False).plot.bar(figsize=(20,8))
Out[66]: <Axes: >
```

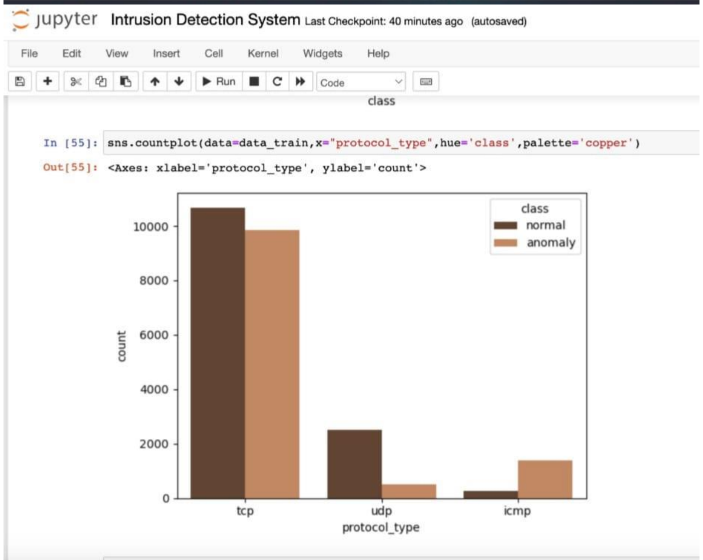


```
In [57]: plt.figure(figsize=(40,30))
         sns.heatmap(data_train.corr(), annot=True)
Out[57]: <Axes: >
```

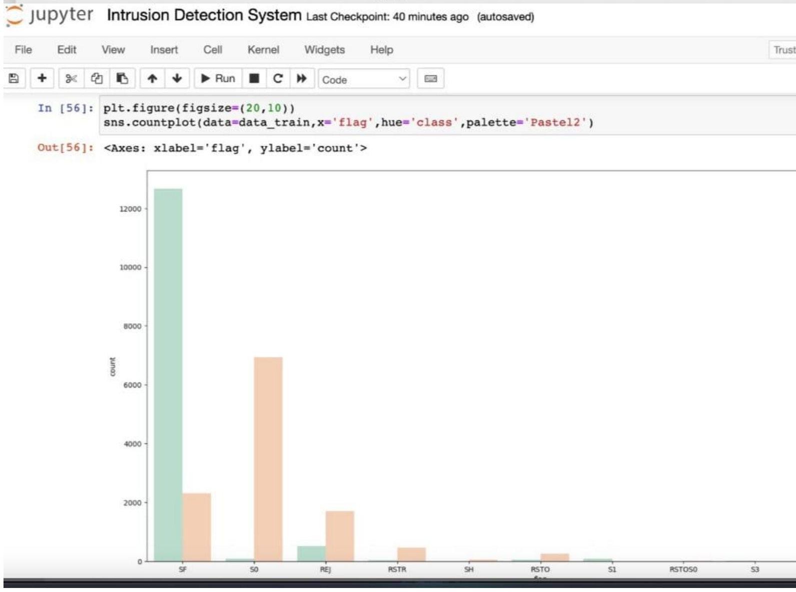

jupyter Intrusion Detection System Last Checkpoint: 39 minutes ago (autosaved)
File Edit View Insert Cell Kernel Widgets Help
Truste
Run
Code
14000
12000
10000
8000
6000
4000
2000
0
count
normal
anomaly
class

Exploratory data analysis (EDA)

```
In [54]: sns.countplot(data=data_train,x='class',palette='PRGn')
Out[54]: <Axes: xlabel='class', ylabel='count'>
```


jupyter Intrusion Detection System Last Checkpoint: 40 minutes ago (autosaved)
File Edit View Insert Cell Kernel Widgets Help
Run
Code
class
class
normal
anomaly
count
10000
8000
6000
4000
2000
0
tcp
udp
icmp
protocol_type

```
In [55]: sns.countplot(data=data_train,x="protocol_type",hue='class',palette='copper')
Out[55]: <Axes: xlabel='protocol_type', ylabel='count'>
```


jupyter Intrusion Detection System Last Checkpoint: 40 minutes ago (autosaved)
File Edit View Insert Cell Kernel Widgets Help
Trust
Run
Code
12000
10000
8000
6000
4000
2000
0
count
SF
S0
REJ
RSTR
SH
RSTO
S1
RSTOS0
S3

```
In [56]: plt.figure(figsize=(20,10))
         sns.countplot(data=data_train,x='flag',hue='class',palette='Pastel2')
Out[56]: <Axes: xlabel='flag', ylabel='count'>
```

5.CONCLUSION

Protecting laptop networks and structures against malicious pastime has ended up of the utmost importance in a generation marked by growing cyber threats characterized with the aid of complexity and foxy. A green Intrusion Detection System (IDS) is crucial for defensive touchy records and infrastructure from unauthorized access, malware, and developing cyberattacks. This research project set out with the intention of resolving this difficulty by developing an anomaly detection machine that uses coding and algorithms.

This undertaking has mapped out a radical technique toward the established order of an anomaly detection gadget acceptable to the complexities of contemporary cyber threats using a rigorously defined methodology. Given the computational nature of network safety concerns, a quantitative evaluation becomes a natural preference for the research concept and technique. This method easily combines the complexities of anomaly detection with the abilities of gadget mastering algorithms by means of recognizing styles in full-size and dynamic datasets, that is of the utmost relevance.

The technique explored the nuances of statistics collected from device logs, network visitors log, and other applicable assets. The style of activities that take place within a community are captured with the aid of this eclectic information series procedure, ensuring that the anomaly detection system is prepared to identify a number of peculiar behaviors. The methodical instruction of the records and characteristic engineering outlined the routes for precise model training, confirming the truism that the satisfaction of the entered records directly impacts the effectiveness of the generated algorithms.

The selection of suitable algorithms has turned out to be a key thing in model advent. The venture turned into given the capability to evolve to numerous situations and facts styles thanks to the adoption of quite a few methodologies, from conventional unsupervised gaining knowledge of algorithms to the power of deep gaining knowledge of models. The training and trying out stages of the model, which can be wherein the difference among normalcy and anomaly is made, are basically tied to its effectiveness. A thorough exam that was primarily based on famous measures including precision, do not forget, F1-score, and ROC curves highlighted the system's capability to determine among real threats and harmless behaviors.

The alerting mechanism confirmed how the paradox detection gadget might be used in actual-international conditions as it became constructed on a foundation of calibrated standards and efficient warning producing. The gadget's suitability for real-international deployment was shown through its integration with community settings created to aid real-time processing and scalability.

While this research enterprise has appreciably strengthened the groundwork for addressing the ubiquitous troubles with community security, it isn't always without flaws. The use of historical facts might not account for all varieties of developing risks, and false positives or negatives are a possibility. Furthermore, the paradox detection machine has to continuously adapt because of the dynamically converting nature of cyberattacks.

In conclusion, the advent of a strong anomaly detection machine at some point of this project's life cycle demonstrates a willpower to fortify laptop networks and systems against the onslaught of cyber threats. This study has opened up a feasible course for improving network protection by embracing the symbiotic interaction between coding and algorithms. Adoption of cutting-edge answers, like the one defined on this look at, acts as a beacon of resilience inside the face of growing cyber complexity and offers the digital stewards of essential infrastructure and information a promising destiny.

6.REFERENCES

- Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 1-58.
- Schölkopf, B., Platt, J. C., Shawe-Taylor, J., Smola, A. J., & Williamson, R. C. (2001). Estimating the Support of a High-Dimensional Distribution. Neural Computation, 13(7), 1443–1471.
- Lee, W., Stolfo, S. J., & Mok, K. W. (2003). A data mining framework for building intrusion detection models. Security and Privacy, 2003. Proceedings. 2003 Symposium on, 120-132.
- Nanduri, A., Kuppusamy, D., Li, X., & Kim, T. H. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 3(1), 41-50.
- Hou, X., Zhang, Z., & Zou, D. (2017). Deep learning for network intrusion detection: A review. IEEE Access, 6, 45-55.
- Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In 2009 IEEE symposium on computational intelligence for security and defense applications (pp. 1-6). IEEE.
- Moustafa, N., & Slay, J. (2016). The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset. Information Security Journal: A Global Perspective, 25(1-3), 18-31.

- Grosse, K., Manoharan, P., Papernot, N., Backes, M., & McDaniel, P. (2017). On the (statistical) detection of adversarial examples. arXiv preprint arXiv:1702.06280.