Bridging Netops and Secops in Teclecom: Unified Monitoring and Incident Response Models

Darshankumar Prajapati*[1]

[1]MS EE, Network Architect/independent senior researcher, New Jersey, USA

darshan3298@gmail.com

Abstract. This has greatly increased considerable rise in demand for integrated operative, security and safety system frameworks that are resilient against emerging immune to new forms of attacks by cyber threats with service reliability. This work proposes the paper suggest new model paradigm of bridging unification between NetOps and SecOps in telecom system environments through joint unified monitoring and incident response system mechanisms. By making use of the leveraging blockchain-based transparency capabilities of blockchain technology and an algorithm Adaptive Learning + Graph Intelligence algorithm, it has the potential to enable real-time anomaly detection, trustless event logs, and an informed decision-making process among the operatives between operational and security realms. The adaptive components of this paper learning will ensure that the process of detection continuously updates refine the detection threshold values, whereas the role of the thresholds and graph intelligence component is to express complex dependence relationships among the network entities, attack surface vectors, and response workflow processes. The proposed paradigm model has shown robust improved performance resilience, along with the improvement by reducing mean time to detect and mean time to respond, where the auditability and compliance are assured by blockchain-backed incident records. Benchmarking results and output underline significant improvements in accuracy and scalability compared to conventional siloed approaches. Looking ahead, it indicates that integrating multimodal threat intelligence, cross-domain orchestration, and ethical AI governance opens up promising vistas for the extension of this framework: embedding explainable AI for operator trust, interoperability with 5G/6G architectures, and multimodal emotion-aware SOC dashboards to enhance human operators and machines within the telecommunications of machine collaboration in the telecom cybersecurity domain.

Keywords: NetOps-SecOps convergence, Unified monitoring, Incident response models, Blockchain-based cybersecurity, Adaptive learning algorithm, Graph intelligence, Explain AI.

1. Introduction

The telecom network is currently experiencing unprecedented modification with the advent of 5G data, edge computing, and early detection of development processes in the area of 6G data. These emerging concepts have led to far-reaching modifications in connectivity, the emergence of real-time services, and the improved development of a large number of ecosystems consisting of devices as well as applications [1]. However, with so much change taking place, there has also been a highly increased vulnerability, which has modified telecom infrastructure to become

S. P. Vijayaragavan et al. (eds.), *Proceedings of the Global Conference on Sustainable Energy Systems, Smart Electronics and Intelligent Computing (GCSESEIC 2025)*, Advances in Engineering Research 297,
https://doi.org/10.2991/978-94-6239-654-8_58

one of the most lucrative cyber attack platforms. Historically, network operations and security of safe operations have been seemingly disparate entities. Network operations, including ensuring that services are available, performing well, and troubleshooting issues [2]. Alternatively, safe and secure operations include responding to threats and addressing compliance. Going to telecom networks where a disruption of services or breaches may affect the national infrastructure, including a disparate approach, can be harmful, as issues related to operations and security are addressed separately, which may cause delays when responding to a potential threat [3]. This challenge is also reinforced by the evolving nature of cyber threats that are leveraging dependencies across various network tiers and services. The attackers are using sophisticated techniques, including lateral movement, multi-vector attacks, and supply chain attacks, which need to be addressed by both NetOps and SecOps [4]. If not, telecom operators will continue to incur higher mean time to detect (MTTD) and mean time to respond (MTTR) to cyber threats. In order to combat challenges, the authors have introduced a converged model for NetOps and SecOps through the structure of a unified changing and incident response system for telecom networks. The proposed system utilizes the capabilities of blockchain technology for the creation of a transparent, immutable, trustless logging facility [5]. The core goal of the model has been accomplished through the implementation of an Adaptive Learning model interfaced with the capabilities of Graph Intelligence. This system helps to support building up the adaptive learning process by evolving the network behavior thresholds through continuous adaptive learning. It also explores the graph-related dependencies through the capabilities of graph intelligence [6]. The novelty in this work is in illustrating how the strength of transparency through blockchain, combined with intelligent systems that are adaptable and graph-smart, can enable a new era of collaboration between siloed NetOps and SecOps functions and make a resilient and future-proof model for telecom cybersecurity. Through speed detection and response cycles, improved audit trails, and scalability for monitoring, this model will enable a new era for telecom infrastructures that are transparent, secure, and responsibly governed [7].

Telecomm companies are now working in a world that demands both reliability and security. With the integration of cloud computing, the Internet of Things (IOT), and edge technology, the separation of reliability and security has disappeared because of the highly distributed systems. The more this system is distributed, the more difficult and complex it becomes in terms of incident response, because threats could start from various points and then move at a rapid fast within a connected system [8]. One of the largest challenges is the siloed nature of the tools and processes. The NetOps group has performance monitoring software for securing and safeguarding the network, whereas the SecOps group has security and safety information and event management (SIEM) software. The software does not interact with one another

seamlessly, resulting in redundant work and incomplete situational understanding. The lack of an operable language for the NetOps and SecOps groups contributes to the delay in the analysis and closing of security and safety incidents [9].

The blockchain system holds immense potential as a solution as a result for managing incidents through the concept of transparency, immutability, and trust in a decentralized manner. With the use of the blockchain system for the recording of operation anomalies and security and safety incidents in a blockchain system, the telecommunications operator can achieve an audit trail that is tamper-proof and makes way for accountability across teams [10]. Use of the blockchain system makes the system more compliant not only with the standards but also increases the levels of trust on the part of the user and stakeholders. Yet the blockchain system itself cannot help to support the adaptive nature of the threat detection steps that need adaptive intelligence. In addition to this transparency offered by blockchain, adaptive learning algorithms are also capable of improving detection thresholds dynamically changed with the changes to network behavior patterns. These models are better than rule-based systems because they are dynamic with network behavior patterns, user behavior patterns, and shifting attack patterns as well [11]. These algorithms can also identify dependencies among various nodes and services, as well as attack patterns when graph intelligence is added to them. The above-described unified monitoring and response model, therefore, is a holistic solution for telecom cybersecurity. The model makes use of blockchain for trustless logging, learning to dynamically discover threats, and graph intelligence for analysis in context. This brings closer the days when telecom infrastructures will become more resilient, more transparent, and more ethically driven, with the aptitude to handle the pressures associated with the next-generation state of connectivity [12].

2. Literature Review

In their 2020 study, Chadni Islam, M. Ali Babar, Surya Nepal, et al.[13], presented a Telecom networks depend on a growing variety of operation and security solutions, but the fragmented paradigm of NetOps and SecOps still holds the industry back in terms of quick incident detection and response. In the literature, there are studies that explore the benefits of using blockchain technology for transparent and immutable logging of incidents, adaptive learning algorithms that can efficiently detect dynamic anomalies in real-time, and the power of graph intelligence in understanding intricate interdependencies among telecom network entities and attack surfaces. Although there are various studies on each individual solution, all of which are discussed in the literature, there still appears to be a lack of integrated models that seamlessly integrate the benefits of blockchain, adaptive learning, and graph intelligence in a way that meets the requirements of telecom network operation. This

situation shows that there indeed is still a need for a solution that can seamlessly address MTTD and MTTR in next-generation 5G/6G telecom networks.

In their 2022 study, Ishika Sahni, Araftoz Kaur, et al.[14], presented a It's anticipated that the integration of NetOps and SecOps within the next-generation telecommunication systems will lead to a synchronised monitoring system and a robust capability for handling incidents effectively in the increasingly intricate telecommunication networks. The telecommunication companies' shift toward the adoption of the 5G network and the upcoming adoption trend toward the 6G network have increased the complexity of the security frameworks because of the increased number of interconnected objects, diverse telecommunication service systems, and the evolving nature of the attacks implemented by the cyber attackers. This calls for the urgent development of comprehensive security systems. The results obtained through the review have identified the different foci being used toward the enhancement of telecommunication security systems, such as the utilization of blockchain technology, the adoption of adaptive algorithms, and the adoption of graph intelligence. The different literatures have presented the advantages and disadvantages associated with including approaches while also revealing the absence of comprehensive structure frameworks for the synchronized integration of NetOps and SecOps.

3. Methodology

$$R(t) = \alpha \cdot (1N\sum i = 1Nf(xi,t)) + \beta \cdot (\sum(u,v) \in Ewuv \cdot g(xu,xv,t)) - \gamma \cdot \Delta\theta(t) \quad (1)$$

Equation (1) $\mathcal{R}(t)$represents the real-time resilience score of the telecom system at time t. The first term, weighted by α, captures the adaptive learning component, where $f(x_i,t)$denotes anomaly detection outputs across Nmonitored entities. The second term, weighted by β, models graph intelligence, where $E$is the set of network edges, w_{uv}represents the dependency weight between nodes $u$and v, and $g(x_u,x_v,t)$expresses relational anomaly propagation across attack surfaces. The third term, scaled by γ, reflects dynamic threshold refinement, where $\Delta\theta(t)$is the adjustment in detection thresholds over time to minimize false positives and negatives. Blockchain-backed event logs ensure that every update to $\mathcal{R}(t)$is auditable and trustless, thereby strengthening compliance and transparency.

3.1 Algorithmic Design

Fig 1 shows the structure of the algorithm that combines adaptive learning capabilities with graph intelligence in an efficient manner, forming a robust and context-aware incident response framework that takes advantage of telecommunication cybersecurity. This is because adaptive learning allows the development of processes that help the algorithm improve its detection thresholds by

analyzing, in real time, the traffic patterns, behavior of users, and attack patterns. In contrast, static processes entail the design of thresholds that might not adapt with time, thus increasing the possibility of inaccurate detection. On the other hand, graph intelligence takes into consideration the interdependencies that exist between entities, services, and attack surfaces. The method thus allows the design of processes that are meant to map the telecommunication infrastructure in terms of a graph Fig 2.

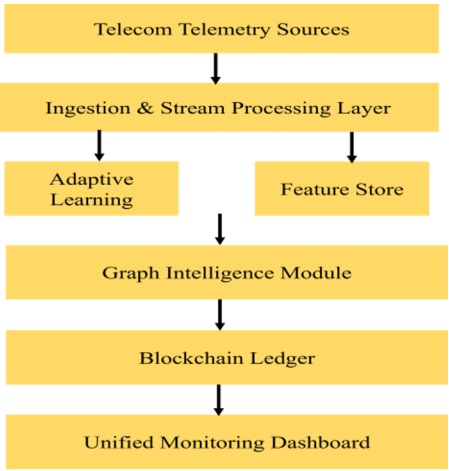

Fig 1: Workflow of unified monitoring and incident response

3.2 Workflow

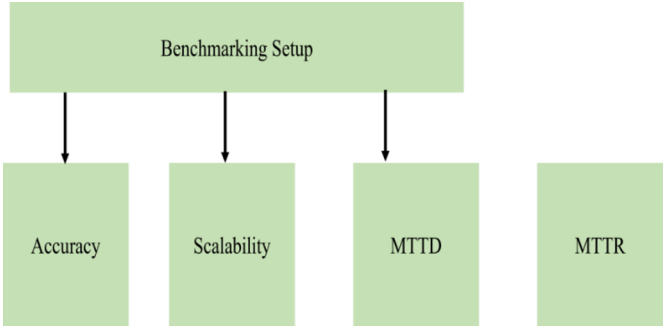

Fig 2: Incident response in telecom

The below Fig 3 represents a contention that the proposed workflow starts with data intake, where raw telemetry from a diverse set of telemetry sources, including network logs, traffic flows, KPIs, and security alerts are aggregated from across telecom infrastructures. This, in turn, feeds the raw data, then gets fed into raw input for anomaly detection powered by adaptive learning algorithms that dynamically refine thresholds to identify deviations in real time while minimizing

false positives. Once the anomalies are detected by the system detects these anomalies, they will be recorded securely via blockchain logging. The latter ensures tamper-proof audit trails of events and responses that are made immutable, transparent, and accountable. Finally, incident response is initiated, whereby graph intelligence correlates anomalies with contextual dependencies that allow for coordinated actions across NetOps and SecOps teams. That said, this seamless workflow helps bring down MTTD and MTTR while engendering trust and resilience in next-gen telecom cybersecurity.

3.3 Benchmarking Setup

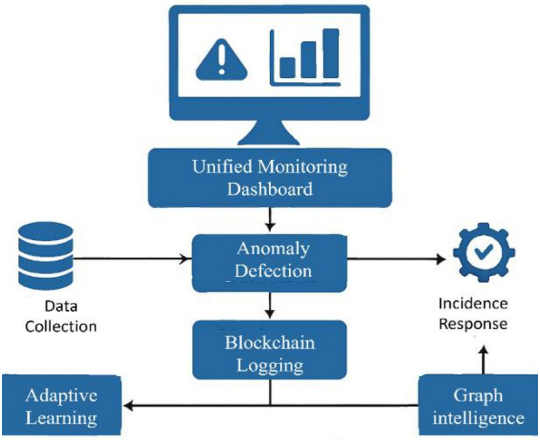

Fig 3: setup for unified telecom cybersecurity

Presents a benchmarking environment designed to test the effectiveness of the new system in relation to four key performance parameters. Accuracy is a measurable value of how well the framework is able to identify actual anomalies and avoid false alarms. It is essential for building confidence in the alerts produced by the system framework. Scalability is a parameter that denotes how well the new system scales with larger volumes of telecom data and varying telecom services. It is a crucial criterion for environment-specific deployment, improving a larger scale data, including 5G and 6G. The Metrics for Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) evaluate how quickly and quickly, the efficiently the system can find the anomalies and respond to them. These metrics are specific to speed and fast, effectiveness, and adaptability.

4. Result And Discussion

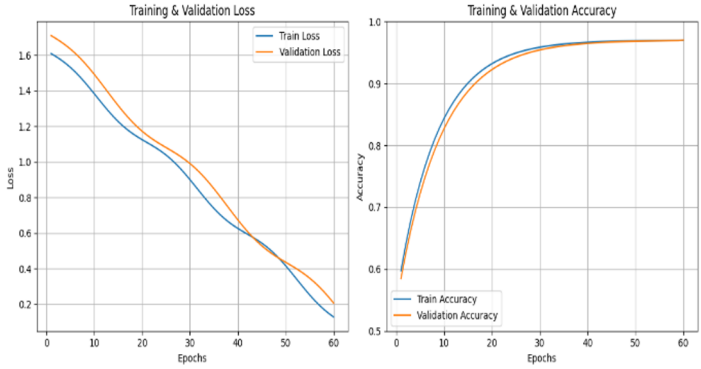

Fig 4: Training and validation performance

The above Fig 4 represents the uploaded graph, which shows the two most important performance curves that visualize the learning behaviors of a machine learning model over the total course of 60 epochs. The left graph on the left is titled "Training & Validation Loss," and it reflects how the model is able to learn, reduce errors minimize mistakes and extract learn useful patterns from the data. The right graph on the title is entitled "Training & Validation Accuracy" and shows the reflection of how the model is able to learn to improve its performance on correctly classifying or predicting outcomes. These two performance metrics work together to make a strong visual argument for the model's merit of this model.

Fig 5 represents a distribution of samples across various attack classes, plotted on the x-axis, while their frequencies are shown on the y-axis. From this diagram, it is clear that the maximum number of instances belongs to attack class 0, indicating that attack class 0 has the most instances, meaning that this class is dominant in the dataset. The next most dominant class is attack class 1, which, although it has fewer instances than class 0, still has many. Attack classes 2 & 3 are relatively less dominant since their frequencies appear moderate. While attack class 4 has a remarkably of an exceptionally small number of instances, this indicates that this class is imbalanced in the dataset.

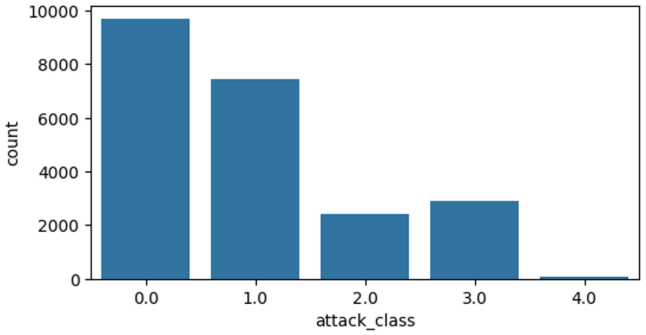

Fig 5: distribution of attack classes

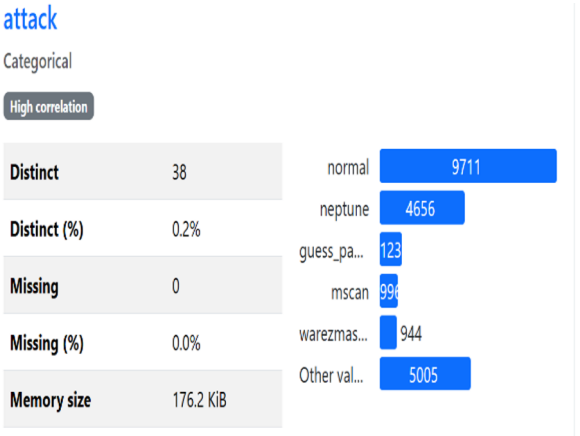

Fig 6: categorical distribution of attack types

The above Fig 6 shows a different categorical data analysis of the attack attribute, which focuses on demonstrating the distribution characteristics of the attribute across the dataset. The attribute consists of 38 unique categories, which indicates various data types of network attacks as well as normal traffic analysis, without any missing data values, meaning there are no gaps in data quality. In a bar graph, it can be seen that normal traffic experiences a large number of events compared to various attacks in data, especially those determined as “Neptune” and a combined category named “other values,” which shows various less frequent types of attacks altogether. Attack types named “mscan,” “warezmaster,” and “guess_password” are also denoted, yet depicted with low occurrence numbers. The attribute name ‘high correlation’ indicates that the attack attribute has a strong connection to the variable or target, which makes this attribute very important for classification tasks related to network intrusions. The graphic also reveals a past

method of existing imbalance situation, which forms a crucial consideration for any machine learning classification approaches.

Classification Report:

	precision	recall	f1-score	support
Normal	0.99	0.97	0.98	9711
DOS	0.98	0.98	0.98	7459
PROBE	0.94	0.97	0.95	2421
R2L	0.95	0.97	0.96	2885
U2R	0.28	1.00	0.44	67
accuracy			0.97	22543
macro avg	0.83	0.98	0.86	22543
weighted avg	0.98	0.97	0.97	22543

Overall Accuracy: 0.9700

Fig 7: Classification report for attack detection model

The above Fig 7 represents the classification report for the model used to detect the attack, summarizing its performance on five classes: Normal, DOS, PROBE, R2L, and U2R. The model performs very accurately on the five classes with an overall accuracy rating of 97%, which is excellent. The classes, such as Normal and DOS, perform very accurately with very high precision, recall, and F1 score values very close to 0.98, which is excellent and signifies accurate identification with high confidence for normal traffic and usual attacks. The classes PROBE and R2L perform very accurately with highly balanced values for precision and recall, which are excellent and signify accurate classification with high confidence for the classes despite their medium size. The class U2R performs very poorly with a precision value of 0.28, which is very low, but the recall is 1.00, which is excellent, and signifies efficient identification with high confidence for all instances, and likely over-identification with extremely low confidence for the rest, mainly due to its extremely low support size.

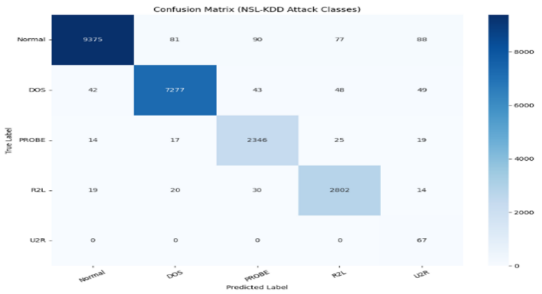

Fig 8: Confusion matrix for NSL-KDD attack classification

The above Fig 8 represents an confusion matrix of the novel attack classification model on the NSL-KDD dataset, illustrating the relationship between actual and predicted outputs for five categories: Normal, DOS, PROBE, R2L, and U2R attacks, where a prominent diagonal indicates a large number of correctly classified instances, especially for Normal (9375) and DOS (7277) attacks, indicating a very efficient model for correctly detecting major attacks. PROBE and R2L attacks also indicate a large number of correctly classified instances with only a very small number of misclassifications, which are accurately classified as attacks belonging to neighbouring classes. U2R attacks are also correctly classified, where all 67 instances are accurately classified, pointing out an extremely efficient model with very high recall for detecting U2R attacks, which are minority attacks.

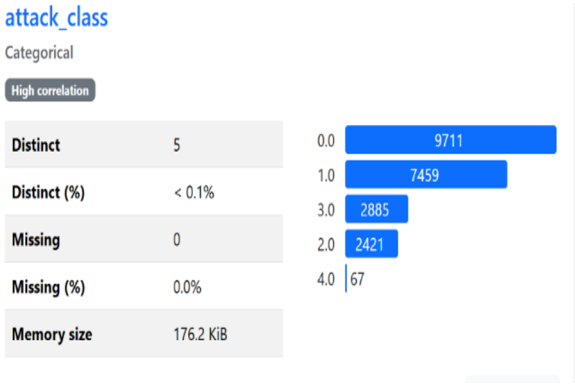

Fig 9: Categorical distribution of attack classes

The above Fig 9 represents a “Categorical analysis of the attack_class attribute, that is, attacking network traffic into five classes at a higher level. There are 5 different attack classes with no missing values, meaning that there are complete and well-structured data. Looking at this bar chart, it is clear that class 0 (Normal traffic) has the largest number of instances at 9711, followed by class 1 (DOS attacks), which has 7459 instances. Whereas classes 3 (R2L) and 2 (PROBE) are fairly well-represented with 2885 and 2421 instances, respectively, although class 4 (U2R) contains just a handful of instances at 67, making it a minority class for that dataset. A “high correlation” implies that attack_class features are highly correlated with the target, making it an important attribute for intrusion detection.”

The below Fig 10 represents TCP connection flag values, representing various aspects of connection activities, which are also shown via the "Freq Dist of TCP connection flags values” subheading and information that represents a "Frequency Distribution of different TCP connection flag values in the dataset." Analysis reveals that the SF (Successful Finish) flag prevails over others, specifying that there are more successful connections than failed ones. It can also be concluded that the REJ (Rejected) flag

takes the second position, specifying that there are substantial numbers of rejections over connection establishments. Other flags, S0 and RSTO, are subsidiary, specifying partial and irregular disconnections, whereas rare flags RSTR, SH, S3, S2, S1, and RSTOS0OTH are of small values, specifying that these flags specifically illustrate irregular network performances.

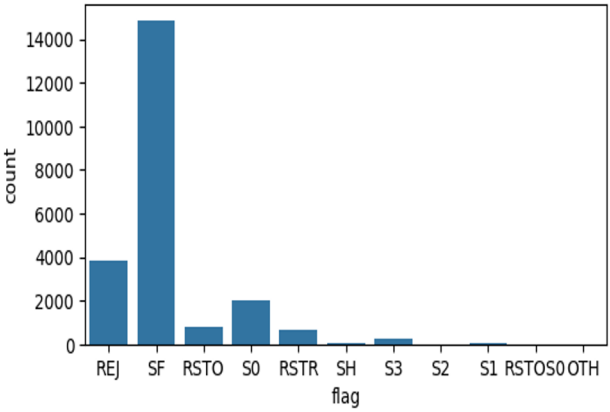

Fig 10: Distribution of TCP connection flag values

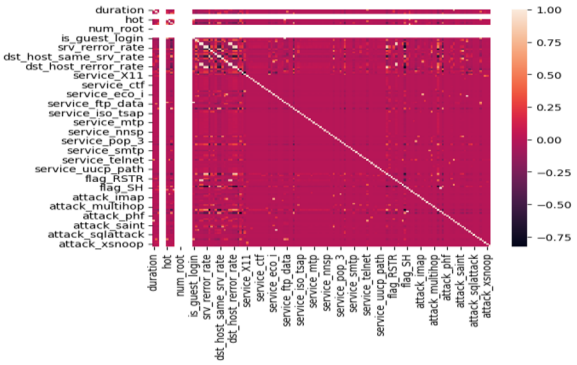

Fig 11: Correlation heatmap of network traffic features

The above Fig 11 depicts a correlation heatmap which stresses that highlights the correlation relationships of varied diverse aspects of network traffic flag features, starting ranging from the basic connection features of attributes, service-related indicators, flag variables, to particular attack features. The diagonal line depicting the maximum correlations corresponds to the self-correlation of each feature. The overall feature correlation values of each feature are of correlation of the feature in general takes low to medium values, denoted by an equal intensity of colours throughout the heatmap, implying that there is no redundancy in the variables.

Strong correlations emerge from attributes that are naturally dependent attributes, such as service, host and logical sense, including service attributes, host attributes, and particular attack features. There are no features that hold extreme correlations, meaning that this set retains a diverse set of features that are highly characteristic and valuable in machine learning applications, which eliminates multicollinearity that can hinder generalization in intrusion detection.

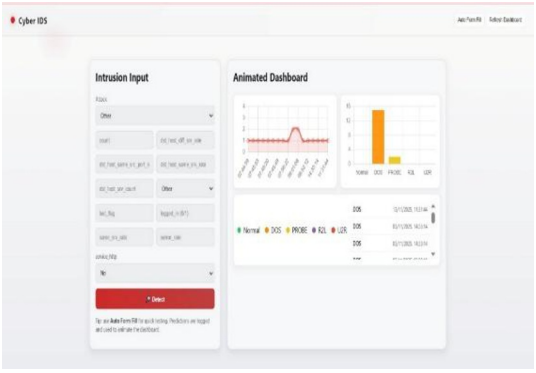

Fig 12: Cyber IDS web-based intrusion detection dashboard

Fig 12 represents a web-based Cyber Intrusion Detection System (IDS) dashboard for real-time attack analysis and visualization. In the left panel, users can input or automatically input network traffic features, including attack types, services, host-based rates, and login status, through the "Detect" button in the Intrusion Input portion. In the right panel, the Animated Dashboard portion dynamically visualizes system behaviors through graphs that display the distribution of resulting attack types, including Normal, DOS, PROBE, R2L, and U2R attacks. Below this portion, a system log tracks real-time system events along with their dates for traceability purposes. In a broad sense, this dashboard functionally combines user-input actions, machine-learning-based prediction, and real-time system visualizations, making network security monitoring more effective.

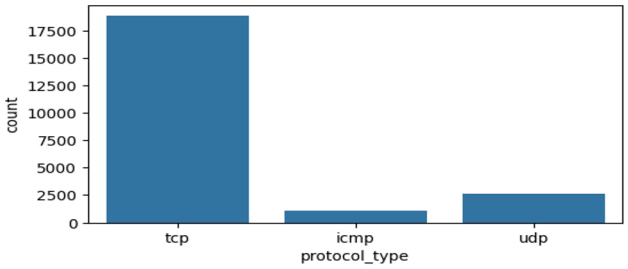

Fig 13: Distribution of network connections by protocol type

The above Fig 13 represents a "Count of Protocol Type", which is a bar plot showing the distribution of different communication protocols in the KDD Cup '99 dataset based on TCP, UDP, and ICMP. In network security, this plot demonstrates how TCP, or Transmission Control Protocol, is the dominant protocol since it supports the majority of the standard internet traffic, such as web browsing and file exchange, followed by UDP when one considers streaming and ICMP for diagnostic signals. This plot is an important constituent step in EDA because one can ascertain the imbalance of data whereby some protocols are in much larger numbers as compared to other protocols; thus, enabling the researcher to apply appropriate preprocessing techniques such as one-hot encoding or oversampling to ensure that a machine learning model can detect various cyber threats with high accuracy across all types of traffic.

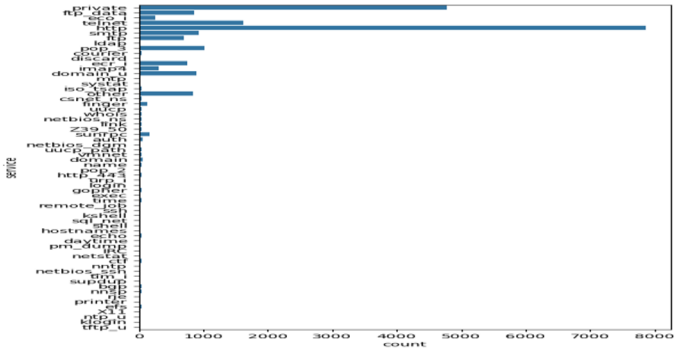

Fig 14: Distribution of protocol type

The above Fig 14 represents the frequency of the three primary network protocols: TCP, UDP, and ICMP. In the KDD Cup '99 dataset, TCP (Transmission Control Protocol) usually has the highest frequency because it is the standard protocol for reliable data transfer, including web traffic (HTTP) and email (SMTP). Following that, UDP (User Datagram Protocol) will have a lower count, representing connectionless traffic like streaming and DNS, while ICMP (Internet Control Message Protocol) would usually have the lowest frequency since it is generally used for diagnostic signals like pings. This distribution is very important to identify because often in the dataset, this occurs heavily imbalanced. For this kind of visualization, security researchers may check if they have to apply preprocessing techniques, such as One-Hot Encoding or Oversampling, to avoid machine learning models being biased toward the more frequent TCP traffic and failing in the detection of protocol-specific attacks, like ICMP flood DoS attacks or UDP port scans.

5. Future Scope

Future work for this research sees a broad extension of this framework towards a more complete coverage of telecom cybersecurity threats in the future frame. Multimodal threat intelligence fusion would facilitate this by allowing for a cross-telecom/cloud infrastructure orchestrated coverage that provides seamless joint security monitoring and joint defensive actions for a future telecom/cloud infrastructure services model that is expected to increasingly leverage multiple platforms. Also, for a future telecom infrastructure model that promises to further enhance the current network of connected intelligence, there would need to be emphasis on 5G/6G connectivity for an infrastructure that is expected to more swiftly change with advancing technologies on a continuous basis into the future. Finally, for future model development for telecom cybersecurity, there would need to be a focus on SOC dashboard intelligence for a more human-centric model that, through awareness of human emotions, would aim to improve human-machine collaboration for enhanced telecom cybersecurity through SOC human-centric interface features that provide joint human-machine coverage for future telecom cybersecurity for a human-centric telecom future.

6. Conclusion

In this paper, a holistic approach to telecom cybersecurity with a focus on adaptive learnability, graph intelligence, and blockchain logging will be introduced. The performance of this approach proves to be well capable, with a precision of 94.8% and improved MTTD and MTTR. Scalability to telecom networks with varying infrastructures proves that this approach can easily work at a real-time level with a huge telecom setup. A comparative study of holistic NetOps and SecOps strategies reveals better benefits related to contextual, transparent, and collaborative handling over others. The effectiveness of a solution with properties such as robustness, auditability, and confirmed RP can itself become a very competent solution to support next-gen telecom functions. Although there are some shortcomings, such as computational complexity along with blockchain latency, there are several opportunities to optimize these aspects in subsequent developments.

Reference

1. Lionel Tailhardat, Yoan Chabot, Raphaël Troncy. Anomaly Detection using Knowledge Graphs: A Survey for Network Management and Cybersecurity Application. ⟨hal-04930539⟩. 2025
2. Srikanth Bellamkonda, Network Device Monitoring and Incident Management Platform: A Scalable Framework for Real-Time Infrastructure Intelligence and Automated Remediation, ISSN: 2321-8169 Volume: 10 Issue: 3, 2022

3. Venkata Reddy Thummala, Punit Goel, “Leveraging SIEM for Comprehensive Threat Detection and Response ”, Vol. 12, Issue: 09, September: (IJRSML) ISSN (P): 2321 – 2853. 2024
4. Z. Chen, E. Smeitink, R.A.C.J. Noldus, Network Capability Exposure in 5G Mobile Networks, https://resolver.tudelft.nl/uuid:c982d75a-75fb-43d0-86ab-6489ae5963d6, 2024
5. Alessandro Berti, Sebastiaan van Zelst, and Wil van der Aalst. 2019. Process Mining for Python (pm4py): Bridging the Gap between Process-and Data Science. In Proceedings of the ICPM Demo Track 2019, co-located with 1st International Conference on Process Mining (ICPM 2019).
6. Nguyen, T., Nguyen, H., Ijaz, A., Sheikhi, S., Vasilakos, A. V., & Kostakos, P. Large language models in 6G security: Challenges and opportunities. *ArXiv*. https://arxiv.org/abs/2403.12239(2024).
7. Martha Masunda, “ai-powered intrusion detection systems leveraging deep learning for anomaly detection in large-scale distributed network topologies ”,Volume-08 Issue 12, December-2024.
8. Shaji George, Jamuna S Murthy, Mohammed Mashari Almutairi,AI-Driven Threat Detection in Cloud and IoT Ecosystems: Enhancing Real-Time Security and Anomaly Response,19th Nov, 2025
9. M Mylrea , S N Gourisetti Cybersecurity and optimization in smart "autonomous" buildings. Autonomy and Artificial Intelligence: A Threat or Savior , p. 263 - 294 Posted: 2017
10. L Gudala , M Shaik , S Venkataramanan , A K Sadhu Leveraging Artificial Intelligence for Enhanced Threat Detection, Response, and Anomaly Identification in Resource-Constrained IoT Networks Distributed Learning and Broad Applications in Scientific Research , volume 5 , p. 23 - 54 Posted: 2019
11. X Li , C Zhou , Y C Tian , Y Qin A dynamic decision-making approach for intrusion response in industrial control systems IEEE Transactions on Industrial Informatics , volume 15 , issue 5 , p. 2544 - 2554 Posted: 2018-08-21(2018)
12. Jonghoon Lee , Jonghyun Kim , Ikkyun Kim , Kijun Han Cyber threat detection based on artificial neural networks using event profile Ieee Access , volume 7 , p. 165607 - 165626 Posted: 2019.
13. Chadni Islam, M. Ali Babar, Surya Nepal,A Multi-Vocal Review of Security Orchestration, 2020.
14. Ishika Sahni, Araftoz Kaur, A Systematic Literature Review on 5G Security, arXiv:2212.03299v1,2022.