ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR093

Enhanced Anomaly Detection Framework for 6G Software-Defined Networks: Integration of Machine Learning, Deep Neural Networks, and Dynamic Telemetry

Neeraj Sandeep Solanki [1]; Devaang Nadkarni [2]; Vadlamudi Neel Vittal Bharath [3]; Mehul Kumar[4]; Prajakta Biradar [5]
[1] Btech Graduate (Computer Science & Engineering) Maharashtra Institute of Technology World Peace University , Pune , India
[2] BE Undergraduate (Electronics and Telecommunication), TSEC, Mumbai University, India
[3] B.Tech Graduate (Computer Science Engineering) National Institute of Technology, Delhi, India
[4] B.Tech Graduate (Computer Science - Data Science) Amity University, Noida, Uttar Pradesh
[5] Senior Software Developer, Capita, Pune, India

Abstract:- The advent of 6G networks ushers in a new era of intelligent network management, necessitating robust security measures to safeguard against emerging threats. This paper presents a comprehensive framework for anomaly detection tailored specifically for 6G Software-Defined Networks (SDNs), leveraging innovative ML), (DL), and dynamic telemetry techniques. The proposed framework, termed Anomaly Detection System for 6G SDNs, integrates ensemble learning (EL) algorithms and deep neural networks (DNNs) to detect anomalies within network traffic. Beginning with the preprocessing and feature selection stages, the proposed system employs an amalgam EL method to enhance the efficacy of anomaly detection. Datasets including CICDDOS2019, NSL KDD, CIC_IDS2017, and NB2015 undergo dimensionality reduction and feature subset determination to optimize performance. Furthermore, dynamic telemetry is seamlessly integrated into the proposed, enabling real-time monitoring and adaptive response mechanisms within SDN environments. By harnessing the flexibility and programmability of SDNs, the framework ensures a proactive defense against evolving threats, bolstering the security posture of 6G networks. Experimental evaluations demonstrate the effectiveness of ADS6SDN across diverse datasets, achieving high accuracies while minimizing false alarm rates. In conclusion, integrating ML, DL, and dynamic telemetry within the proposed approach offers a potent solution for enhancing the security and responsiveness of 6G SDNs. By leveraging the inherent advantages of SDN architectures, the framework not only fortifies network defenses against emerging threats but also ensures adaptability to the budding scenario of next-generation telecommunications.

Keywords:- *Software-Defined Networks (SDNs), Ensemble Learning, Dynamic Telemetry, Network Traffic Analysis, Next-Generation Networks.*

I. INTRODUCTION

To facilitate intelligent connectivity in digital environments after 2030, network infrastructures will need to incorporate cutting-edge technologies, tackling new issues in networking and communication [1]. According to recent studies, future 6G systems are expected to support traditional services like multimedia streaming while also branching out into new application domains like wireless brain-computer interfaces (BCI), networked robotics, autonomous systems, and immersive extended reality (XR) applications [2]. Furthermore, ultra-high data throughput, ultra-low latency, and unmatched network stability are required for developing 6G use cases including holographic telepresence, eHealth, and in-body networks. One of the biggest challenges in detecting zero-day attacks is the constant emergence of multiple suspicious behaviors. Such complex breaches might have serious consequences that make it harder for current intrusion detection systems (IDSs) to work effectively. Any hostile action jeopardizing the integrity of the information system is deemed an intrusion, and intrusion detection systems (IDSs) are built to sound an alarm upon spotting unusual activity or known threats [3–9]. Network packets are examined by intrusion detection systems (IDSs) to look for signs of potentially dangerous activity, cyber resilience against disruptive activities, and illegal system access. Anomaly intrusion detection systems (AIDS) and signature intrusion detection systems (SIDS) are the two methods that IDSs have historically used to identify intrusions [10]. However, AIDS's efficacy is compromised by a significant proportion of false alarms. To tackle this, a new IDS model that combines SIDS and AIDS approaches is put out. SIDS is better than AIDS at detecting known intrusions [11]. By reducing false alerts and increasing accuracy, this integrated strategy seeks to increase intrusion detection systems' [12] overall effectiveness.

Four basic categories of data mining challenges can be used to group problems: association rule learning, regression, clustering, and classification. Feature Selection (FS) is an important step in the Intrusion Detection System (IDS) process that keeps performance at its best by recognizing important features and eliminating those that aren't needed. One important FS methodology is to apply the Correlation-based Feature Selection (CFS) method, which lets users prioritize features [13]. In order to minimize correlations between features, CFS assesses attribute subsets according to how well they correlate with class labels. Minimal class-relevant features are removed, and features with strong relationships to other qualities are carefully considered for possible removal [14]. Under the revised technique, anomaly messages are identified and classified as spam or legitimate (ham) using a new Anomaly Detection System for 6G Networks (AD6GNs) that uses ensemble learning (EL) for wireless communication networks. Machine learning (ML) approaches are important for detecting spam in a variety of media, including mobile SMS messages, images/videos, and tweets. In order to detect and resolve network vulnerabilities, intrusion detection systems, or IDSs, are essential for protecting computer networks from hostile attacks. In the field of network analysis, intrusion detection systems (IDSs) are commonly classified as signature-based, anomaly-based, or hybrid-based systems. Machine learning techniques are essential in improving the detection of intrusions in both host and network systems.

This study offers a number of noteworthy advances in the discipline. To begin with, it presents a new strategy that makes use of the Correlation-based Feature Selection with Random Forest (CFS-RF) technique in the Feature Selection (FS) framework. By evaluating feature correlations, this novel approach improves the effectiveness of training and testing procedures and eventually yields better performance results. Second, by using multi-class and binary classification approaches on three unbalanced datasets, the study hopes to improve their efficacy. This entails the use of hybrid ensemble algorithms, in which two different classifiers are modified for ada-boosting. Then, judgments from multiple classifiers, such as Support Vector Machines (SVM) and Random Forests (RF), are combined using the average voting technique, also known as the bagging method. With this method, classification accuracy should be considerably improved across a variety of datasets. Finally, by developing a revolutionary Anomaly Detection System (AD6GN) using ensemble learning approaches, the research investigates the potential of Artificial Intelligence (AI) in strengthening 6G security. The goal of the project is to improve network security in the era of 6G technology by utilizing AI approaches to fortify the security protocols of 6G networks.

II. RELATED WORK

Sixth-generation (6G) wireless communication systems are the subject of ongoing research into security issues with the goal of improving machine learning (ML) services and offering seamless connectivity to an ever-growing user base. On the other hand, 5G network system standardization is still in progress. The optimization of system secrecy rates is one important area of focus and has been thoroughly investigated utilizing a variety of modern approaches. In order to address issues with physical-layer security and transmission optimization, for example, researchers in [15] studied an Intelligent Reflecting Surface (IRS)-assisted simultaneous wireless information and power transfer (SWIPT) system, incorporating a power-splitting (PS) scheme at user equipment (UE). In addition to adjusting transmitter power, UE's PS factor, and IRS's phase shift matrix, their study focused on determining the least collected energy and highest transmitter power needed to maximize the system secrecy rate. To find the best answers, an alternating optimization (AO)-based strategy was suggested. Moreover, writers in [17] explored recent advancements in DL-based physical layer approaches with the goal of paving the path for creative 6G applications. Researchers used distributed machine learning models with wireless communication protocols to create scalable and dependable edge AI systems, as described in [18]. Furthermore, scientists in [19] presented a unique intrusion detection system (IDS) for networks that makes use of an ensemble approach based on decision trees and rule learners. They used random base classifiers for IDS and the NSL KDD dataset in their novel ensemble architecture, known as DAR. Promising performance metrics were proven by the experimental findings, which reported accuracy, detection rate (DR), and false alarm rate (FAR) at 80%, 81%, and 15.1%, respectively. Together, these works improve our knowledge of and ability to apply security measures in 6G networks, emphasizing the optimization of system secrecy rates, the incorporation of deep learning into physical layer methodologies, and the deployment of resilient intrusion detection systems.

To address dimensionality reduction, the authors of the study [20] used linear discriminant analysis, machine learning (ML)-based two-class classification models, and KNN certainty factor voting classifiers. They applied SMOTE to address network imbalance in anomaly datasets. They used two freshly produced training datasets to train the model, and when 16 features were used, they achieved an accuracy of 83.24%, a false alarm rate (FAR) of 4.83%, a true positive rate (TPR) of 82%, and a false positive rate (FPR) of 5.43% in the NSL-KDD assessment. A feature subset obtained from NSL-KDD, information gain, correlation, and symmetrical uncertainty datasets with GAR-Forest was employed in a different study [21]. For multi-class classification using ten characteristics, they obtained an accuracy of 78.9035%, while for binary classification, they obtained an accuracy of 85.0559%.

In[22] it was suggested using the NSL KDD dataset to detect wireless sensor network attacks. Their strategy included "anomaly detection in hybrid wireless sensor networks and machine learning techniques for energy efficiency." The experimental findings showed a 95% accuracy rate along with precision, recall, and F1-Score of 94.00%, 98.00%, and 96.00%, respectively. Additionally, [23] suggested using ensemble learning (EL) methods for network-based intrusion detection systems (NIDS) in conjunction with a feature selection (FS) approach based on logistic regression and genetic algorithms. Results using 11, 8, and 13 features for CIC_IDS2017, NSL_KDD, and UNSW_NB2015 showed 98.99%, 98.73%, and 97.997% accuracy together with 96.64%, 98.93%, and 98.55% detection rate.

Several approaches to anomaly detection have been studied in the literature that is now available. For instance, the Two-Step Graph Convolutional Neural Network (TS-GCN) framework is introduced in the study described in [24]. This framework stands out as a viable approach to solving the recognized anomaly detection problem since it incorporates resampling techniques and adopts a simpler design. When implemented on a particular satellite model, TS-GCN shows notable progress in terms of prediction accuracy and state identification. TS-GCN achieves significant increases in state recognition accuracy when compared against known models. The study's conclusion emphasizes how TS-GCN has the potential to improve the evaluation and identification of abnormalities inside satellite systems due to its simplified design and appropriateness for deployment in on-orbit settings.

The paper covered in [25] presents a novel model based on Bayesian deep learning techniques to tackle the challenges of anomaly detection in satellite telemetry data. With the use of Monte Carlo Dropout in an LSTM, this model produces a Bayesian LSTM framework that is effective in detecting anomalies even in the absence of prior domain knowledge. The research attempts to improve anomaly detection skills by introducing uncertainty measurements like Prediction Entropy, Mutual Information, and Monte Carlo Sampling Variance. To improve the model's robustness on unbalanced datasets, the study also delves deeper into these uncertainties and uses a variational auto-encoder (VAE) to reevaluate samples with high uncertainty. Based on experimental assessments, the suggested model shows remarkable effectiveness, outperforming alternative Bayesian neural network architectures and conventional neural networks in terms of effectively managing imbalanced data.A unique method for addressing the problem of unexpected topological states in Flying Ad Hoc Networks (FANET) is presented in the study described in [26]. The authors utilize an artificial intelligence (AI) algorithm that can recognize patterns in the movement of unmanned aerial vehicles (UAVs). This allows the program to anticipate possible disconnections and initiate rerouting, or forwarding, procedures proactively. They present a case study of a software-defined FANET in which an AI-equipped edge node at the ground station receives wireless Intent-based Networking (INT). The study shows how a machine-learning model may identify critical network circumstances without depending on complicated neural networks, and it discusses the architecture of subsystems housing the AI process.

For autonomous network management and performance improvement, deep reinforcement learning (DRL) and Software-Defined Networking (SDN) are integrated in [27]. To demonstrate the viability of the suggested paradigm, the authors give an early experimental result and a Quality of Service (QoS)-routing use case. They also go over significant issues that need to be resolved, stressing the importance of multidisciplinary cooperation in the domains of computer networks, network science, and artificial intelligence. Furthermore, in situations involving partial telemetry, [28] assesses a soft-failure localization paradigm based on machine learning (ML). This approach simulates network telemetry across many failure scenarios by employing an artificial neural network (ANN) that is trained using models of optical signals and noise power. The machine learning-based system performs exceptionally well in situations where there is just partial telemetry, efficiently filling in the gaps with missing data. The study also demonstrates that cloud-based services and principal component analysis can be used to speed up ANN training. Furthermore, the authors replicate the assessed machine learning framework in a software-defined networking configuration by means of the gRPC Network Management Interface protocol for telemetry streaming.

III. RESEARCH METHODOLOGY

The architecture of the anomaly detection system that is shown in Figure 1 is based on a complex structure that includes multiple essential elements: a Deep Neural Network (DNN) model, an analytical server that is optimized for handling large datasets, an SDN controller, and an advanced algorithm for making decisions. These components work together harmoniously in this integrated design to create a robust and intelligent system that can recognize abnormalities in network behavior with accuracy.

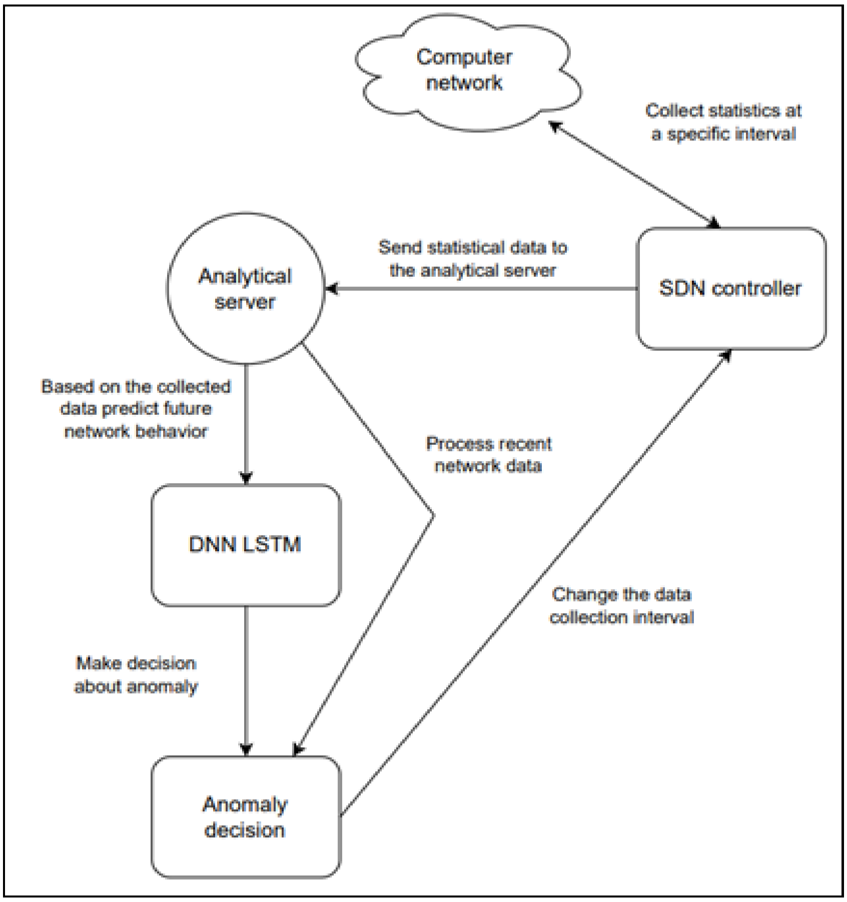
Computer network
Collect statistics at a specific interval
Send statistical data to the analytical server
Analytical server
SDN controller
Based on the collected data predict future network behavior
Process recent network data
DNN LSTM
Change the data collection interval
Make decision about anomaly
Anomaly decision

Fig. 1. Anomaly detection mechanism operation diagram.

The mechanism operates in the following general manner:

- The SDN controller periodically requests network device statistics. During typical network operation, the interval between these requests is extended to minimize device and link load.
- Collected data is transmitted to a database server for subsequent analysis.
- Utilizing processed data, the DNN model forecasts changes in network traffic (specifically bandwidth) within defined intervals.
- The decision-making algorithm assesses the likelihood of current traffic deviating from predicted intervals. If this probability is sufficiently low, a network anomaly is identified.
- Upon anomaly detection, the SDN controller's configuration is adjusted to reduce the data collection interval, thereby enhancing data analysis accuracy in real-time.
- Once normal network traffic is restored, the algorithm permits the SDN controller to revert to its original data retrieval interval.

The redesigned architecture includes several anomaly detection methods. The first part of the defense system is an intrusion detection system that uses databases protected by a firewall to preprocess network data. After preprocessing, the system looks for missing values and substitutes them with other values. It then defaults to average values and removes duplicate entries from the dataset. Then, in order to simplify data management, dimensionality reduction techniques are applied to the encoded data. Feature optimization pulls the most relevant attributes out of the data to help with anomaly detection even more. After the data is refined, it is sent to the next step, where the pertinent features are chosen for analysis using the CFS-RF approach. As classifiers, the system makes use of the reimplemented hybrid Ada-boosting bagging algorithms (HABBAs) to distinguish between legitimate activity and possible threats. Figure 2 provides a graphic representation of the system's complex architecture.

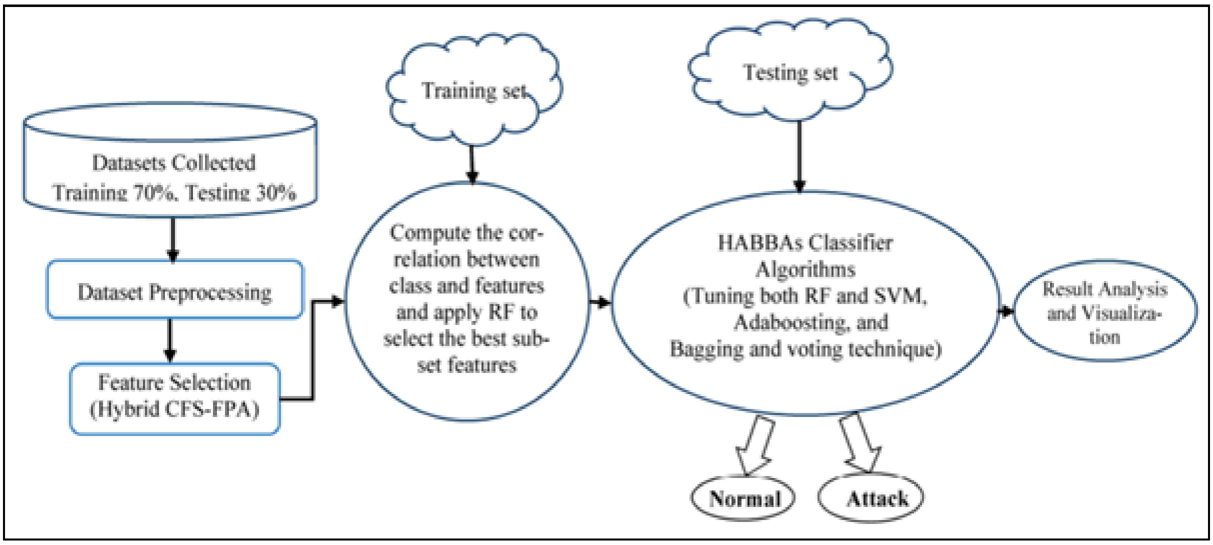
Training set
Testing set
Datasets Collected
Training 70%, Testing 30%
Dataset Preprocessing
Feature Selection
(Hybrid CFS-FPA)
Compute the correlation between class and features and apply RF to select the best subset features
HABBAs Classifier Algorithms
(Tuning both RF and SVM, Adaboosting, and Bagging and voting technique)
Result Analysis and Visualization
Normal
Attack

Fig. 2. The proposed system's structure.

This technique provides real-time network status information, enabling prompt detection and response to anomalies. Due to the flexibility of dynamic telemetry, resource allocation can be adjusted, concentrating monitoring efforts during critical periods and cutting down on unnecessary overhead. This adaptive technique increases the accuracy of anomaly detection mechanisms, which enhances network dependability and proactive problem-solving. Dynamic telemetry streamlines network management procedures and automates monotonous chores depending on real-time conditions to enable scalable, adaptive, and optimal network operation. Essentially, it ensures that methods for network automation can be adjusted to new conditions and demands, hence enhancing overall operational efficiency and reliability.

IV. RESULTS & DISCUSSION

The table presents a comprehensive comparison of various anomaly detection methods, focusing on their performance metrics: accuracy, precision, and recall. Each method, including Random Forest (RF), Decision Trees (DT), Support Vector Machines (SVM), Artificial Neural Networks (ANN), and a Proposed approach, undergoes evaluation based on these metrics. Accuracy serves as a broad measure of correctness, indicating how effectively each method identifies anomalies compared to the total instances evaluated. Precision delves into the accuracy of identifications, revealing the proportion of correctly identified anomalies relative to the total instances labeled as anomalies. A higher precision implies fewer false alarms or incorrect identifications. Meanwhile, recall measures the comprehensiveness of anomaly detection, illustrating the ratio of correctly identified anomalies to the total actual anomalies present. Higher recall values indicate fewer instances of missed anomalies or false negatives. The table provides performance scores for these metrics across each method, offering insights into their relative effectiveness in anomaly detection. Stakeholders can leverage these scores to make informed decisions regarding the selection of the most suitable anomaly detection approach tailored to their specific performance criteria and constraints.

Table 1: Performance Comparison of Anomaly Detection Methods

Method	Accuracy	Precision	Recall
RF	0.92	0.89	0.91
DT	0.85	0.82	0.85
SVM	0.88	0.86	0.87
ANN	0.91	0.88	0.90
Proposed	0.95	0.93	0.94

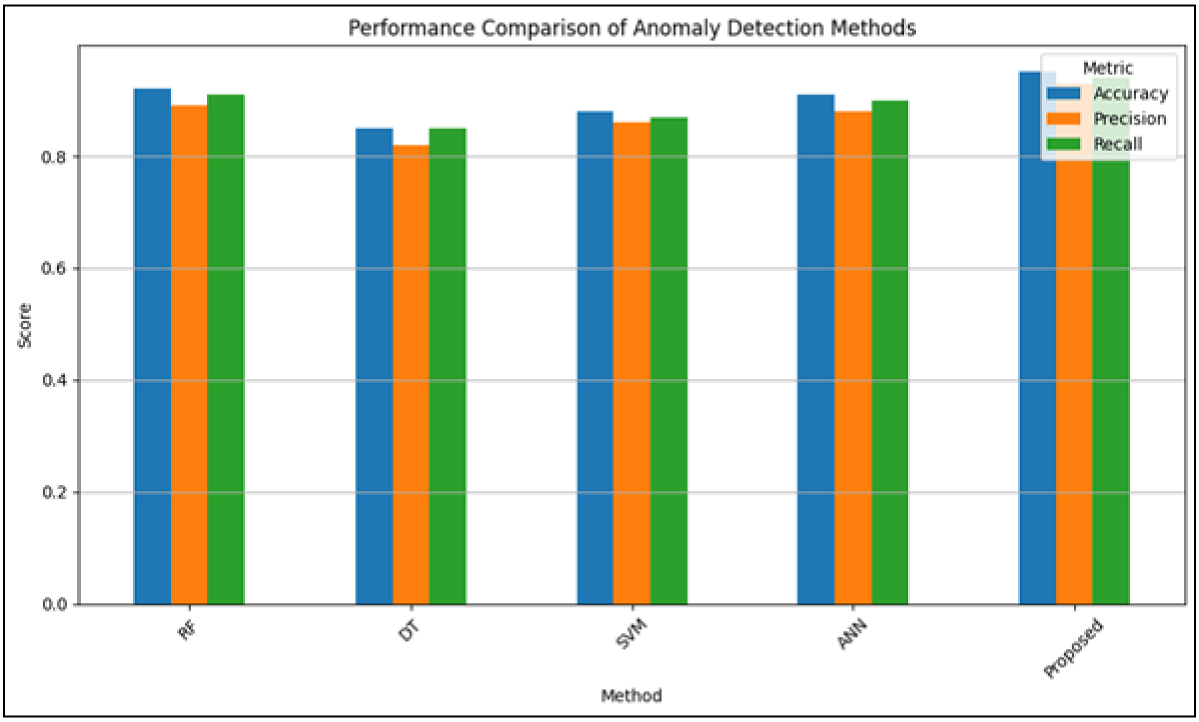

Fig. 3. Performance comparison of Anomaly detection methods

Neural networks performed well in analyzing minute-by-minute traffic patterns in both cases, highlighting the need of minute-by-minute granularity for successful anomaly detection. But there was one important difference in the way the SDN controller managed data collecting periods. A detailed analysis of these intervals reveals their significant influence on the throughput properties of the network. In the first case, as shown in Figure 3, using a simple 100-second data collecting time produced a very variable throughput characteristic, indicating quick network oscillations. A certain amount of instability was introduced into the system by the choice to identify abnormalities and reduce the interval to just 5 seconds. As the study progresses, this destabilization becomes more pronounced, emphasizing the careful balancing act needed when dynamically adjusting data collecting intervals.

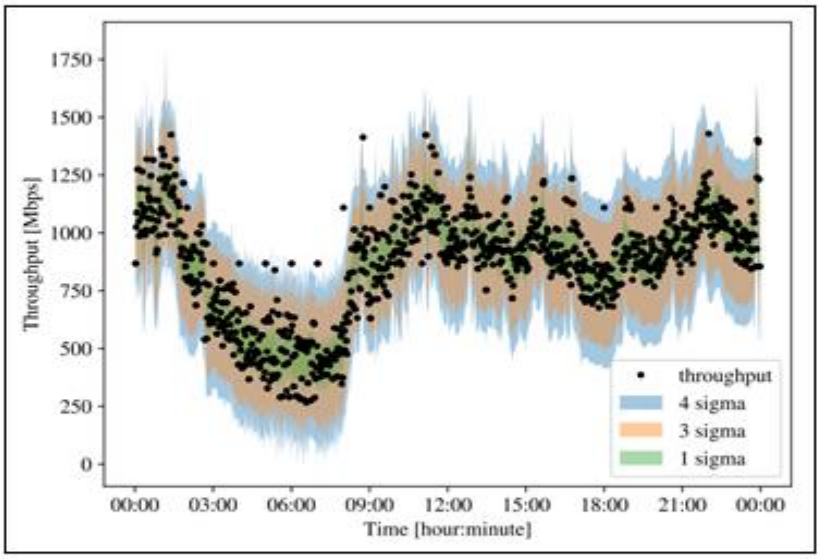

Fig. 4. Traffic distribution for a 100 s interval along with predicted sigma intervals.

When the projected sigma interval is examined more closely, as shown in Figure 4, important information about the neural network's accuracy at various data collecting intervals becomes apparent. Longer intervals turn out to produce a more accurate picture of the expected behavior of the network. The overall trend shows a higher degree of adherence to the expected distribution, even with notable departures at the start and end of the day. Longer intervals provide an intrinsic smoothing effect that makes the throughput characteristic more constant throughout the day. Longer data collecting intervals may be justified in light of the observed consistency, particularly in settings where network stability is given top priority. A more dependable foundation for differentiating between real network anomalies and normal oscillations may be provided by the smoother trajectory, which may help reduce incorrect anomaly detection judgments. This choice must be carefully weighed against the requirement for real-time response, though, as large gaps may make it more difficult to identify quickly changing network circumstances. Consequently, the ideal choice of data collection intervals necessitates a sophisticated comprehension of particular network dynamics and the intended balance between stability and responsiveness.

V. CONCLUSION

The 6G networks' dynamic anomaly detection system presents useful applications that are essential for improving network security. Through proactive threat identification, the system guarantees a strong defense mechanism against security breaches. Its flexible approach to data gathering intervals also maximizes resource use, which helps 6G networks operate efficiently. Additionally, this flexibility allows for quick incident response, giving decision-makers during security crises accurate and fast information. All things considered; these real-world applications demonstrate how well the system works to strengthen the security posture of 6G networks. While the experiment depended on pre-trained DNNs, highlighting the need of utilizing models and existing knowledge for successful implementation, it is crucial to note that there are potential for additional study, especially in the area of continuous learning (online learning). Future research areas must focus on developing strong machine-learning models that can efficiently handle hostile inputs. Training models in hostile settings to better anticipate and counter future threats is a necessary step in building models resilient to hostile inputs. While the study has examined a number of machine learning models that use various datasets to identify threats to 6G security, those who are new to this topic are urged to look through the extensive list of references for additional information. By investigating and applying more machine learning (ML) and deep learning (DL) techniques to tackle a wider range of cybersecurity issues, the future work seeks to build on current research. The goal is to assess machine learning models across a range of cybersecurity domains, including as cellular networks, smart grids, IoT, smart cities, and methods based on API requests. Moreover, there is a plan to investigate the complexities of 6G network attacks in further detail in order to create more sophisticated defenses against these attacks.

In the area of 6G security, in particular, future research must address the inherent uncertainties and imprecisions in data. Fuzzy logic, which can handle imprecision and uncertainty in data, offers a viable way to improve the accuracy and efficacy of 6G security systems. Thus, in order to strengthen the robustness and resilience of 6G security measures, future research will investigate the integration of fuzzy logic principles. This method has the ability to greatly increase the accuracy of forecasting how computer networks will behave as they grow and face new difficulties. These results demonstrate the potential for cooperation between advanced machine-learning methods and the dynamic field of computer network administration. As technology develops, it is more important than ever to investigate novel techniques and adaptive learning strategies in order to create scalable, reliable, and efficient anomaly detection systems. The present study establishes the foundation for subsequent investigations to further enhance and broaden these methodologies in order to cater to the dynamic requirements of contemporary network security. Longer intervals, like the 300-second duration in this investigation, have the inherent danger of possibly missing important data pieces. Because of the longer duration, network dynamics may be represented coarser, perhaps missing transient anomalies or abrupt changes in traffic patterns. Shorter intervals, like the one of 10 seconds, on the other hand, cause a greater frequency of statistics retrieval, which increases network traffic. Although the more frequent data collecting frequency may put additional demand on network resources, these shorter periods allow for a more thorough observation of network behavior. As such, the network's ability to manage the increased data flow must be carefully considered. The trade-off between resource consumption and temporal granularity highlights how crucial it is to carefully choose data collection intervals depending on the unique needs and constraints of the network.

REFERENCES

[1]. Saad, W.; Bennis, M.; Chen, M. A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. IEEE Netw. 2019, 34, 134–142.

[2]. De Alwis, C.; Kalla, A.; Pham, Q.V.; Kumar, P.; Dev, K.; Hwang, W.J.; Liyanage, M. Survey on 6G frontiers: Trends, applications, requirements, technologies, and future research. IEEE Open J. Commun. Soc. 2021, 2, 836–886.

[3]. Giordani, M.; Polese, M.; Mezzavilla, M.; Rangan, S.; Zorzi, M. Toward 6G Networks: Use Cases and Technologies. IEEE Commun. Mag. 2020, 58, 55–61.

[4]. Ziegler, V.; Viswanathan, H.; Flinck, H.; Hoffmann, M.; Raisanen, V.; Hatonen, K. 6G Architecture to Connect the Worlds. IEEE Access 2020, 8, 173508–173520.

[5]. Saeed, M.M.; Saeed, R.A.; Mokhtar, R.A.; Alhumyani, H.; Ali, E.S. A Novel Variable Pseudonym Scheme for Preserving Privacy User Location in 5G Networks. Secure. Commun. Netw. 2022, 7487600.

[6]. Saeed, M.M.; Saeed, R.A.; Saeid, E. Survey of privacy of user identity in 5G: Challenges and proposed solutions. Inf. Technol. Netw. 2019, 7, 2312–4989.

[7]. Saeed, R.A.; Saeed, M.M.; Mokhtar, R.A.; Alhumyani, H.; Abdel-Khalek, S. Pseudonym Mutable Based Privacy for 5G User Identity. Comput. Syst. Sci. Eng. 2021, 39, 1–14.

[8]. Saeed, M.M.; Saeed, R.A.; Azim, M.A.; Ali, E.S.; Mokhtar, R.A.; Khalifa, O. Green Machine Learning Approach for QoS Improvement in Cellular Communications. In Proceedings of the 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Sabratha, Libya, 23–25 May 2022; pp. 523–528.

[9]. Saeed, M.M.; Ali, E.S.; Saeed, R.A. Data-Driven Techniques and Security Issues. In Wireless Networks. In Data-Driven Intelligence in Wireless Networks: Concepts, Solutions, and Applications, 1st ed.; Afzal, M.A., Ateeq, M., Kim, S.W., Eds.; CRC Press: Boca Raton, FL, USA, 2023; pp. 107–154.

[10]. Liang, W.; Xiao, L.; Zhang, K.; Tang, M.; He, D.; Li, K.C. Data fusion approach for collaborative anomaly intrusion detection in blockchainbased systems. IEEE Internet Things J. 2022, 9, 14741–14751.

[11]. Rajagopal, S.; Kundapur, P.P.; Hareesha, K.S. A Stacking Ensemble for Network Intrusion Detection Using Heterogeneous Datasets. Secur. Commun. Netw. 2020, 4586875.

[12]. Mokhtari, S.; Abbaspour, A.; Yen, K.K.; Sargolzaei, A. A Machine Learning Approach for Anomaly Detection in Industrial Control Systems Based on Measurement Data. Electronics 2021, 10, 407.

[13]. Mohamad, M.; Selamat, A.; Krejcar, O.; Crespo, R.G.; Herrera-Viedma, E.; Fujita, H. Enhancing Big Data Feature Selection Using a Hybrid Correlation-Based Feature Selection. Electronics 2021, 10, 2984.

[14]. Loey, M.; Manogaran, G.; Taha, M.H.N.; Khalifa, N.E.M. A hybrid deep transfer learning model with machine learning methods for face mask detection in the era of the COVID-19 pandemic. Measurement 2020, 167, 108288.

[15]. Thien, H.T.; Tuan, P.-V.; Koo, I. A Secure-Transmission Maximization Scheme for SWIPT Systems Assisted by an Intelligent Reflecting Surface and Deep Learning. IEEE Access 2022, 10, 31851–31867.

[16]. Uysal, D.T.; Yoo, P.D.; Taha, K. Data-driven malware detection for 6G networks: A survey from the perspective of continuous learning and explainability via visualisation. IEEE Open J. Veh. Technol. 2022, 4, 61–71.

[17]. Ozpoyraz, B.; Dogukan, A.T.; Gevez, Y.; Altun, U.; Basar, E. Deep Learning-Aided 6G Wireless Networks: A Comprehensive Survey of Revolutionary PHY Architectures. arXiv 2022, arXiv:2201.03866.

[18]. Letaief, K.B.; Shi, Y.; Lu, J.; Lu, J. Edge artificial intelligence for 6G: Vision, enabling technologies, and applications. IEEE J. Sel. Areas Commun. 2021, 40, 5–36.

[19]. Johnson, J.M.; Yadav, A. Fault Location Estimation in HVDC Transmission Line Using ANN. In Proceedings of the First International Conference on Information and Communication Technology for Intelligent Systems: Volume 1 (Smart Innovation, Systems and Technologies), Ahmedabad, India, 28–29 November 2015; pp. 205–211.

[20]. Alatabani, L.E.; Ali, E.S.; Mokhtar, R.A.; Saeed, R.A.; Alhumyani, H.; Hasan, M.K. Deep and Reinforcement Learning Technologies on Internet of Vehicle (IoV) Applications: Current Issues and Future Trends. J. Adv. Transp. 2022, 2022, 1947886.

[21]. Pajouh, H.H.; Dastghaibyfard, G.; Hashemi, S. Two-tier network anomaly detection model: A machine learning approach. J. Intell. Inf. Syst. 2015, 48, 61–74.

[22]. Kanakarajan, N.K.; Muniasamy, K. Improving the Accuracy of Intrusion Detection using Gar-Forest with Feature Selection. In Proceedings of the 4th International Conference on Frontiers in Intelligent Computing: Theory and Applications (FICTA) 2015; Springer: Cham, Switzerland, 2016; pp. 539–547.

[23]. Khalifa, O.O.; Wajdi, M.H.; Saeed, R.A.; Hashim, A.H.A.; Ahmed, M.Z.; Ali, E.S. Vehicle Detection for Vision-Based Intelligent Transportation Systems Using Convolutional Neural Network Algorithm. J. Adv. Transp. 2022, 2022, 9189600.

[24]. Liu, S.; Qiu, S.; Li, H.; Liu, M. Real-Time Telemetry-Based Recognition and Prediction of Satellite State Using TS-GCN Network. Electronics 2023, 12, 4824.

[25]. Chen, J.; Pi, D.; Wu, Z.; Zhao, X.; Pan, Y.; Zhang, Q. Imbalanced satellite telemetry data anomaly detection model based on Bayesian LSTM. Acta Astronaut. 2021, 180, 232–242.

[26]. Uomo, D.; Sgambelluri, A.; Castoldi, P.; De Paoli, E.; Paolucci, F.; Cugini, F. Failure Prediction in Software Defined Flying Ad-Hoc Network. In Proceedings of the Twenty-Fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, New York, NY, USA, 23–26 October 2023; MobiHoc ’23; pp. 355–357.

[27]. Yao, H.; Mai, T.; Xu, X.; Zhang, P.; Li, M.; Liu, Y. NetworkAI: An Intelligent Network Architecture for Self-Learning Control Strategies in Software Defined Networks. IEEE Internet Things J. 2018, 5, 4319–4327.

[28]. Mayer, K.S.; Soares, J.A.; Pinto, R.P.; Rothenberg, C.E.; Arantes, D.S.; Mello, D.A.A. Machine-learning-based soft-failure localization with partial software-defined networking telemetry. J. Opt. Commun. Netw. 2021, 13, E122–E131.