2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS) | 979-8-3503-6118-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/INCOS59338.2024.10527501

Real-time Anomaly Detection in 5G Networks through Edge Computing

Riaz Shaik
Department of CSE
KL University,
Vaddeswaram, Andhra Pradesh, India.
sheikriaz@gmail.com

Dara Raju
Dept.,of Computer Science &Engineering,
Vignana Bharathi Institute and Technology,
Aushapur, Ghatkesar, India.
rajurdara@gmail.com

Prakash Chandra Behera
Department of Science,
St. Claret College,
Bangalore, India.
prakash@claretcollege.edu.in

Ravindra Changala
Department of Information Technology
Guru Nanak Institutions Technical Campus,
Hyderabad, India.
changalaravindra@gmail.com

S. Suma Christal Mary,
Department of Information Technology,
Panimalar Engineering College,
Poonamalle, Chennai.
sumasheyalin@gmail.com

A.Balakumar
Department of ECE
K.Ramakrishnan College Of Engineering,
samayapuram, Trichy,India.
balakumar2712@gmail.com

***Abstract*—Strong anomaly detection techniques are becoming more and more necessary as 5G networks develop in order to maintain network performance, security, and dependability. This study leverages the capabilities of Mobile Edge Computing (MEC) to present a novel method for anomaly detection in 5G networks. By processing data closer to the network edge, the integration of MEC offers an efficient and decentralized architecture that lowers latency and improves real-time detection capabilities. The distributed module takes advantage of its close proximity to network devices by using sophisticated algorithms for anomaly detection, which are implemented at the mobile edge. The system can quickly detect abnormalities from typical network activity by utilizing capabilities including Flow Collection, Anomaly Symptom Detection, and Network Anomaly Detection. The distributed module provides anomalous information to the centralized decision-making module for thorough examination. It takes into account variables like resource use and network traffic and integrates this data with metrics gathered from monitoring modules. Because of its adaptive characteristics, the system may expand anomaly detection components, enhance detection functions, and modify virtualized resources in response to shifting network circumstances. The evaluation findings reveal that the suggested anomaly detection method performs well in 5G networks, with decreased false positives, increased responsiveness, and better flexibility to changing network conditions. Using MEC not only makes anomaly detection more effective, but it also fits in with the 5G design, which makes it a viable option for protecting the upcoming generation of communication networks. It obtains 95% accuracy in classification. The suggested approach has proven to be resilient in handling security issues by producing outcomes that are either comparable to or better than those attained by other techniques that have been previously presented in the study literature. This demonstrates the model's dependability and effectiveness in handling security-related problems.**

Keywords—Anomaly Detection; Mobile Edge Computing (MEC); 5G Networks; Decentralized Architecture; Real-time Detection

I. INTRODUCTION

The introduction of 5G networks has completely changed the telecom landscape by providing previously unheard-of connection and data rates[1]. In a 5G environment, the sheer amount of data produced by numerous devices and apps calls for creative solutions for network management and security. Because they frequently depend on centralized processing, traditional anomaly detection techniques would find it difficult to keep up with 5G networks' rapid changes[2]. This problem is most noticeable in situations when making decisions quickly is essential, such in driverless cars or vital infrastructure[3].The limits of centralized processing in 5G networks are being addressed by edge computing, which is developing as a game-changing technology[4].Edge computing lowers latency and improves the network's capacity to handle information in real-time by allocating computer resources closer to the location of data creation. This closeness to the edge facilitates faster data processing in the context of anomaly detection, allowing for immediate discovery and reaction to unusual patterns or behaviors[5].In 5G networks, real-time anomaly detection is mostly dependent on advanced machine learning techniques[6]. Large datasets are used to train machine learning models, which then allow them to independently understand the typical behavior patterns of the network and the devices linked to it[7]. When one of these established patterns deviates from the norm, it is immediately investigated or mitigated[8]. The incorporation of machine learning into edge computing settings improves anomaly detection systems' flexibility and reactivity, guaranteeing precise identification of known and unknown dangers. Given that 5G networks offer essential services, its security implications go beyond traditional worries[9]. In addition to strengthening the network against cyberattacks, real-time anomaly detection at the edge also increases the network's overall resilience[10]. Quick detection and reaction to irregularities reduce the possible effect of security breaches, preserving data integrity and the availability of services that depend on 5G connection. Although there is potential to improve 5G network security with the integration of edge computing and real-time anomaly detection, there are still obstacles to overcome[11]. Careful thought must be given to matters like the scalability of edge computing infrastructure, the creation of robust yet lightweight machine learning models, and the standardization of anomaly detection protocols[12]. The goal of this domain's future research should be to solve these issues in order to fully realize the promise of real-time anomaly detection in 5G networks. In conclusion, a critical component

979-8-3503-6118-6/24/$31.00 ©2024 IEEE

of protecting 5G networks from new attacks is the convergence of edge computing and real-time anomaly detection[13]. In the face of changing problems, the telecom sector can guarantee the security, dependability, and performance of 5G networks by utilizing cutting-edge machine learning techniques and pushing computing power to the edge[14].With the incorporation of edge computing technologies, anomaly detection—a crucial component in the field of cyber security and network management is becoming even more important. Edge computing lowers latency and improves the ability to make decisions in real time by processing data closer to the point of generation. Edge computing combined with advanced algorithms has shown to be a potent method for handling anomalies and security risks in a variety of systems when it comes to anomaly identification. Edge computing makes it possible to run anomaly detection algorithms directly at the edge servers or on the edge devices, allowing for quick data analysis without transferring the data to a centralized cloud or data center. This is especially helpful in situations where minimal latency is essential, such autonomous systems, industrial automation, and vital infrastructure. The use of anomaly detection techniques at the edge enhances the efficiency, responsiveness, and timeliness of the detection process.

The capabilities of anomaly detection are further improved by the incorporation of AI and ML algorithms into edge computing. These algorithms are able to quickly detect deviations from the norm that can point to possible security breaches or anomalies in operation, and they can also adjust to changing patterns of typical activity. With processing power and AI capabilities, the edge devices become intelligent endpoints that can identify abnormalities on their own and take the necessary action. Furthermore, situations involving the Internet of Things make the combination of anomaly detection and edge computing very pertinent (IoT). A distributed and cooperative approach to security can be facilitated by the active participation of edge devices in an IoT ecosystem, such as sensors and actuators, in anomaly detection procedures.

This improves the network's overall resiliency while also lessening the strain on centralized systems. Nonetheless, there are still issues to be solved, such as the restricted processing power at the edge and the requirement for effective algorithms that strike a compromise between precision and resource efficiency. Furthermore, protecting the edge computing environment from hostile assaults is crucial for preventing anomaly detection process intrusions. To sum up, combining anomaly detection with edge computing offers a potential new direction for improving the security of contemporary systems. Anomaly detection at the edge is made possible by the convergence of distributed intelligence, real-time processing, and adaptive algorithms, which makes it essential for defending networks, systems, and vital infrastructures from new threats.

The key contributions are as follows:

- ➢ The study harnesses the capabilities of MEC to process data closer to the network edge, enhancing efficiency and reducing latency in anomaly detection.
- ➢ Introduces a decentralized system architecture with a centralized decision-making module and a distributed anomaly detection module, leveraging the advantages of both for real-time detection
- ➢ Utilizes advanced algorithms at the mobile edge for anomaly detection, taking advantage of the close proximity to network devices for swift identification of abnormalities.
- ➢ expanding anomaly detection components, enhancing detection functions, and modifying virtualized resources in response to changing network circumstances
- ➢ Evaluation results demonstrate reduced false positives, increased responsiveness, and improved flexibility, showcasing the efficacy of the proposed method in enhancing the security and performance of 5G

The rest of this study is systematized as follows. Section II includes extensive earlier research on the work scheduling problem using various optimization strategies. Section III discussed about the proposed technique. Section IV presents the investigational setup, the outcomes, and discussion of findings. Finally, section V carries conclusion of the paper.

II. Related works

The potential of MEC to alleviate data transfer issues in 5G scenarios has drawn interest. A survey of research emphasizes that one possible option for MEC is the deployment of computer resources in telecom operators' Centralized Radio Access Networks (C-RAN). The IoT front-end of the C-RAN network is formed by a combination of smart street lighting with 5G base stations, which facilitates effective data collecting. To ensure the integrity of 5G networks of communication, an adaptive rules engine has been suggested for quick identification of anomalies and normal information monitoring. The research supports the idea that this integrated strategy offers a comprehensive solution for creating robust and responsive 5G networks, highlighting the practical benefits and demonstrating its potential for use in the industry and medicine domains. The strategy including combined MEC, C-RAN, and smart street lighting may encounter difficulties because of high installation costs, intricate logistics, scalability problems, and the requirement for ongoing rule engine service. Furthermore, it's critical to provide strong security protocols and respect for privacy for data collecting using IoT front-end components[3].

Santos et al.[15]suggests a minimal latency, scalable detection of anomalies solution for Smart City presentations. Low-power Fog computing technologies were the primary objective of the assessment, which is carried out inside the Antwerp City of Things test bed. A substantial data set is used to look into which low-power Wide Area Network technologies are most suited for the Smart City use case. This study advances the investigation of modern methods for effective anomaly detection in the context of IoT utilization in smart city settings. The chosen LPWAN technology will be implemented in the near future, along with techno economic analyses.

In this paper Fog intelligence solves scalability issues, guarantees security for privacy, and is well-suited for the difficulties of managing dispersed wireless links by fusing edge processing with centralize cloud computing. This method is in line with the larger body of research, which highlights the need

979-8-3503-6118-6/24/$31.00 ©2024 IEEE

for innovative, scalable, and private-preserving anomaly detection systems in the dynamic field of wireless communication networks. Utilizing fog intelligence to build distributed machine learning models for smart network administration may be very effective in reducing processing delays, decreasing data transmission, and safeguarding privacy[5].

Zhang et al.[16]A block chain-powered mobile edge computing strategy for effective and secure data sharing and storage. The exclusive signing secret key of a region is divided into several secret shares in our system. All that is needed from IoT devices is the data and the arbitrary token sharing that is assigned to the edge node. The edge node applies holomorphic encryption of passwords and information signature using the recovered verified private key. After processing current data concurrently, the edge node will re-establish a connection with the client. When sending data to the internet for processing, we use standby uploading to avoid information floods. After analysis, it became clear that our system could provide low-latency communication answers for terminal users while maintaining confidentiality and authenticity and enabling anonymized identity identification.

Wang [17]give a full examination of MEC security and privacy from an AI perspective. The) has integrated its NFV and SDN technologies into the MEC standard architecture in an effort to further demonstrate a workable MEC platform. However, the other side concentrates on new privacy and security issues along with potential AI-based solutions. Finally, discuss the benefits and drawbacks of employing AI to enhance MEC safety and secrecy as possible directions for future study While AI has the potential to significantly increase safety and secrecy in MEC settings, it also has its own unique set of challenges. Subsequent research should focus on developing AI systems that are cost-effective, safe from attacks, and private in addition to addressing the ethical and legal concerns surrounding MEC.

The associated studies demonstrate how several technologies, including blockchain, IoT, 5G networks, and fog intelligence, may be used to solve problems with anomaly detection, effective data interchange, and privacy protection. The promise of these integrated techniques is demonstrated by the literature, which stresses practical applications in smart cities, healthcare, and industrial domains. Nonetheless, difficulties are recognized, including the high cost of deployment, scalability problems, security issues, and the requirement for ongoing rule engine maintenance. Furthermore, the research acknowledges the constraints pertaining to the intricacy of extensive dispersed networks and the possible hazards linked to the integration of innovative technologies like as blockchain and artificial intelligence inside the MEC framework. MEC-oriented architecture for network anomaly detection.

III. Proposed MEC-focused Design for Detecting Anomalies in Networks

A. *Data collection*

IoT-23 is the data set that was used in this study. It is made up of network data that was taken from 20 sick Raspberry Pis and three secure IoT devices. The Stratosphere Center at the Czech University of Technology in the Czech Republic supplied the Internet of Things' internet traffic. An Amazon Echo smart speaker, a Philips HUE smart LED light, and an intuitive smart door lock were the three different IoT devices utilized to track the online activity. The suitable circumstances were identified using these three Internet of Things devices. It's crucial to remember that each of these three Internet of Things, or IoT, gadgets is a real, functional device. More than 325 million traffic flow statistics that were made available in 2020 are also included in the collection. Initially, the node's acquired data from the connection is manually analyzed. Cap file. After that, the suspicious flows are detected and given the proper designations. A tagged document in comma-separated value (.csv) format is then produced by the expert. A Python script processes the individually labeled.csv files, adding tags to each flow as it goes. Additional log data was analyzed by a second Python script, which compared its patterns to those of correctly labeled.csv files. Additionally, it labeled each file it examined according to its proper order[18].

1) Feature Selection Engine: Two modules make up the proposed feature selection engine: one includes selectors for data gain and gain ratio in order to assess features based on gain ratio and information gain. Better identification outcomes are indicated by higher scores, whereas worse identification outcomes are suggested by lower scores. Using a combining key, the second module, a combined feature choice module, chooses and refines pertinent features to find the majority of relevant features (MR Feature). A Random Forest machine learning technique is used to process and analyze the final collection of the top twenty rated attributes[19]. InfoG is given in (1)

$$\text{InfoG}\ (T', X') = (E'\ (T') - E'\ (T' | X')) \tag{1}$$

(Gainer) in relation is given in (2)

$$\text{Gainer}\ (T', X') = (E'\ (T') - E'\ (T' | X'))\ /\ E'\ (X') \tag{2}$$

B. *Proposed MEC-focused Design for Detecting Anomalies in Networks*

For network anomaly detection in 5G networks, a decentralized strategy based on distributed computing and virtualization is emphasized in the suggested Mobile Edge Computing (MEC)-oriented design. With a high-level design influenced by the ETSI NFV architecture, the architecture is divided into functional planes to take advantage of the versatility of 5G networks. In order to enable the execution of Mobile Edge Applications and Services, the design includes a Virtualization Infrastructure (VI) within the Mobile Edge Host, which operates at both the Mobile Edge System and Mobile Edge Host levels. One important aspect is the convergence of MEC with NFV, which allows Virtual Network Functions (VNF) and MEC applications to share a similar platform. By separating the software implementation of Virtual Network Functions from the underlying hardware, the design makes use of Software-Defined Networking (SDN) and Network Function Virtualization (NFV) approaches to improve flexibility in network resource management. At the highest level of the

979-8-3503-6118-6/24/$31.00 ©2024 IEEE

architecture, the Mobile Edge Orchestrator regulates the behavior of the infrastructure according to regulations specified by Virtual Network Operators, while the OSS controls the logic of the Anomaly Detection (AD) system.

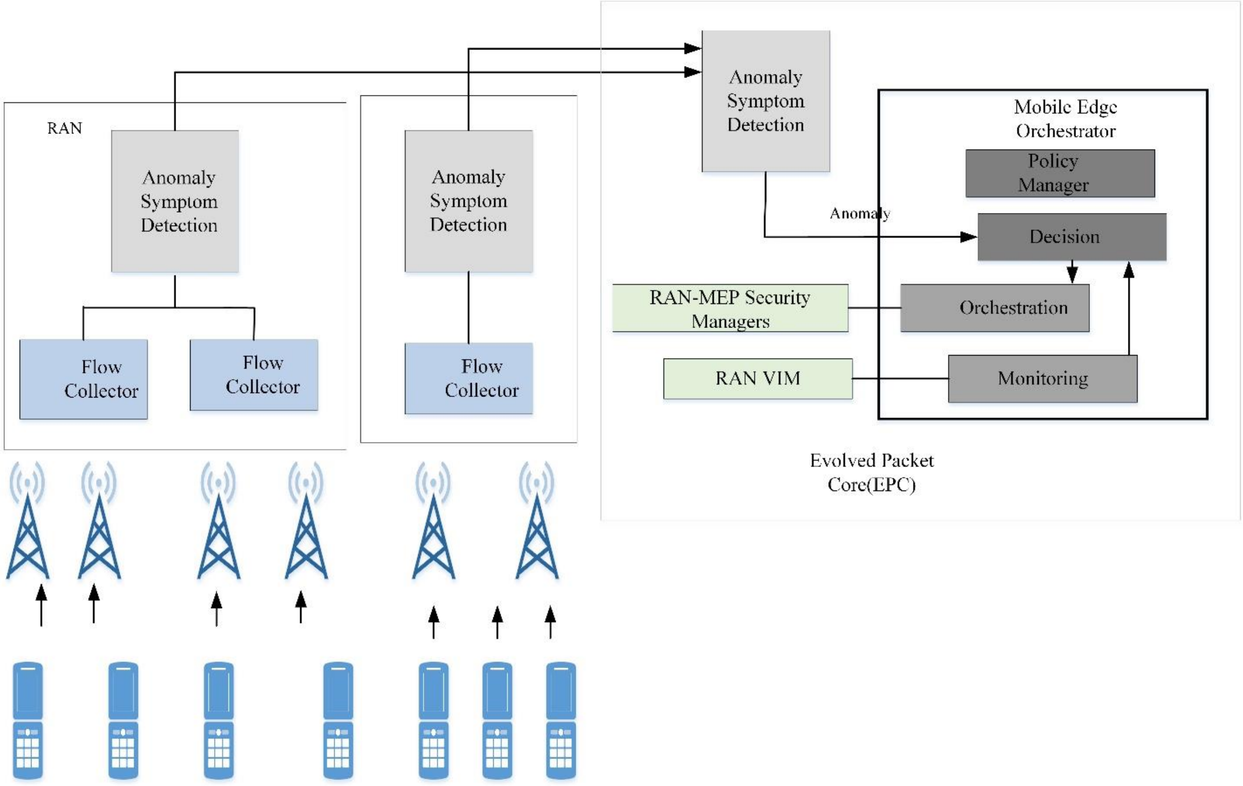

Fig.1. Architecture of Network Anomaly detection

Fig.1 demonstrates Architecture of Network Anomaly detection. Anomaly Symptom Detection and Intrusion Detection Systems are two examples of Mobile Edge Applications that are instantiated on the Virtual Infrastructure and are controlled by requests or settings that are verified by the management and orchestration plane. In order to satisfy the dynamic demands of contemporary networks, the suggested architecture successfully integrates virtualization and decentralized computing to offer a flexible and responsive framework for network anomaly detection in 5G. Anomaly Symptom Detection (ASD), Network Anomaly Detection (NAD), and Flow Collection (FC) are three virtualized components that are used in the proposed distributed system for 5G network anomaly detection. Network anomalies are found via FC collecting and storing network flows, ASD quickly identifying anomaly symptoms, and NAD analyzing time stamped symptoms. The Decision module of the system, which is shown in Fig. 1, enables the prompt notification of identified anomalies to the Mobile Edge (ME) Orchestrator. This module takes network flow data and resource utilization into account when combining anomaly information with metrics from the Monitoring module. The Policy Manager provides contextual information to direct the best course of action while storing and upholding policy consistency. The Decision module ensures flexibility, extensibility, and real-time adaptability to dynamic network circumstances by optimizing detection algorithms, extending capabilities, and adapting virtualized resources in reaction to abnormalities [20].

C. An application for 5G networks

This use case emphasizes how crucial it is to effectively manage anomaly detection and response capabilities in 5G networks, especially when it comes to Mobile Edge Computing (MEC). It highlights factors including user mobility, communication latency, and the quantity of concurrent users. In this scenario, virtual machines (VMs) are hosted on generic hardware and mobile users utilize a range of network services offered by a Radio Access Network (RAN). For anomaly identification, a deep learning-based Anomaly Symptom identification (ASD) module is used.

An effective and self-regulating system for managing physical resources is needed when the number of users rises and the ASD module becomes overloaded. The suggested method effectively manages ASD services and resolves issues with upgrading detection models by allocating resources in real-time and dynamically. In order to identify new kinds of network abnormalities, deep learning techniques must be continuously trained, which calls for retraining on separate machines on a regular basis. The use case goes on to handle issues with the ASD module's overload, which calls for the management of ASD services and the associated virtual machines (VMs) at the network's edge by an automated system. Various solutions are suggested, such as allocating more resources to already-existing virtual machines (VMs) or deploying new VMs with more processing power.

979-8-3503-6118-6/24/$31.00 ©2024 IEEE

The last issue is the necessity of using Deep Packet Inspection (DPI) tools in conjunction with Virtual Network Functions (VNFs) to thoroughly examine suspicious network traffic. In order to solve this issue, the suggested method shows how to install and set up a Snort tool in an already-existing VM1 of the RAN. In summary, the use case presents a thorough management strategy that utilizes specialized tools, updates detection models, and adjusts to network circumstances in order to handle changing security threats in a 5G network environment[21].

IV. Results and Discussion

Notable performance gains are seen when the suggested anomaly detection technique is evaluated on 5G networks using Mobile Edge Computing (MEC). Reduced false positives, greater responsiveness, and more adaptability to changing network circumstances are all displayed by the system. The use of MEC not only makes anomaly detection more effective, but it also fits in well with the 5G network's architectural principles, making it a workable option for guaranteeing the security and functionality of the next communication networks. Below Table I provides Histogram values.

Accuracy: The suggested method successfully classifies data with a high accuracy rate of 95%, demonstrating its efficacy in precisely identifying network anomalies.

Flexibility: The system exhibits greater adaptability to shifting network conditions, enabling dynamic modification of resource allocation and anomaly detection components in response to changing network conditions.

Responsiveness: The approach shows improved real-time anomaly detection responsiveness, facilitating quicker anomaly identification and remediation.

Table I. Histogram values

Data Value	Frequency
0	65
9	9.5
53	48
60	15

Fig.2 shows graphical representation of histogram values a histogram is a visual representation of a dataset's distribution, displaying the frequency of data values within specific intervals through adjacent bars. While typically discrete, a smooth curve (e.g., probability density function) can be overlaid for a continuous representation.

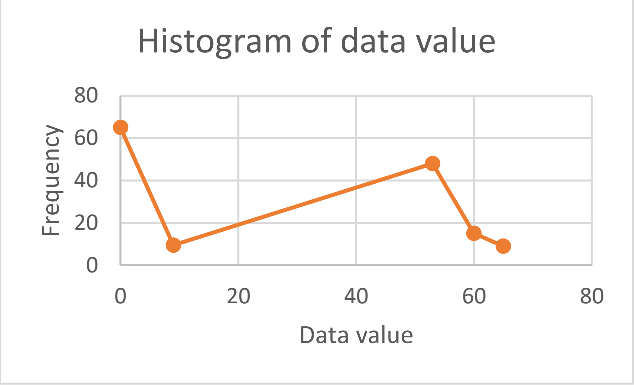

Fig.2 graphical representation of histogram values

This graphical approach helps identify data patterns and central tendencies, providing insights into the dataset's overall shape and density. The combination of bars and curves in a histogram enhances the visualization for effective statistical analysis. Location Distribution values are given in Table.II

Table II. Location Distribution

Location	Distribution
Room A	20.6
Room B	24.8
Room C	26.6
Outdoor	30.0

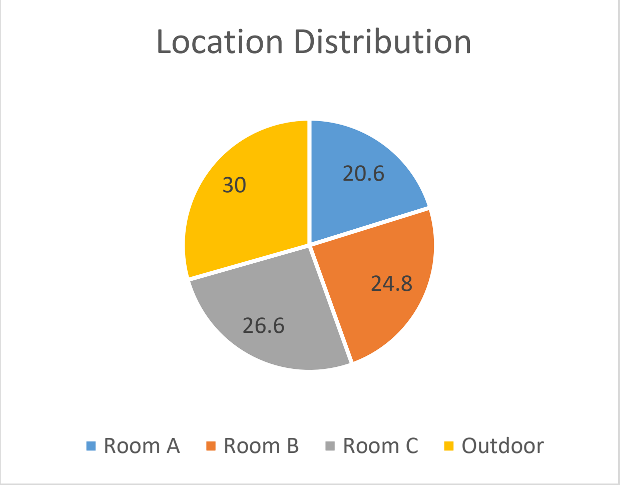

Fig.3 graphic depiction of Distribution of locations

Distribution of locations a pie chart is a graphic depiction that shows how different components, data points, or products are distributed or allocated among several areas or geographical places. This kind of picture offers a simple and quick method to comprehend how a dataset is distributed geographically or how common certain features are in various locations.

A. Discussions

The integration of MEC for anomaly detection in 5G networks represents a promising advancement by minimizing latency and enabling real-time detection. The decentralized nature of the anomaly detection module at the mobile edge

979-8-3503-6118-6/24/$31.00 ©2024 IEEE

enhances responsiveness, making it well-suited for applications with stringent latency requirements. The proposed adaptive rule engine adds a dynamic element to routine data monitoring, contributing to timely anomaly identification with potential applications in critical sectors. However, challenges such as high implementation costs, logistical complexities, scalability issues, and the necessity for continuous rule engine maintenance should be acknowledged. Security and privacy considerations remain crucial, demanding robust measures to protect sensitive data and user confidentiality. The recommended method's increased accuracy boosts trust in its efficacy for network security by reliably and precisely finding anomalies in the network. Furthermore, the system's adaptability to shifting network conditions suggests a strong ability to sustain peak performance and change course in response to new threats, strengthening the security posture and overall resilience of the network. Looking forward, future research should focus on refining anomaly detection algorithms, addressing implementation challenges, and exploring synergies with emerging technologies to further enhance the effectiveness of abnormality recognition in 5G networks through MEC.

V. Conclusion and Future works

The incorporation of MEC for anomaly detection in 5G networks emerges as a promising approach, offering real-time detection and reduced latency for applications with stringent requirements. The decentralized architecture at the mobile edge enhances responsiveness, showcasing potential applications in critical sectors. Despite its promise, challenges such as implementation costs, logistical complexities, and scalability issues must be addressed, emphasizing the need for robust security measures. The adaptive rule engine augments routine monitoring, contributing to timely anomaly identification. Future research should focus on refining algorithms, mitigating implementation challenges, exploring synergies with emerging technologies, and enhancing security measures. Standardized frameworks for MEC integration and investigations into real-world impact across industries will be instrumental in advancing the efficacy and scalability of anomaly detection in the dynamic landscape of 5G networks.

References

[1] X. Wang, W. Wu, Y. Du, J. Cao, Q. Chen, and Y. Xia, "Wireless IoT Monitoring System in Hong Kong–Zhuhai–Macao Bridge and Edge Computing for Anomaly Detection," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 4763–4774, Feb. 2024, doi: 10.1109/JIOT.2023.3300073.

[2] W. Xu, Z. Yang, D. W. K. Ng, M. Levorato, Y. C. Eldar, and M. Debbah, "Edge Learning for B5G Networks with Distributed Signal Processing: Semantic Communication, Edge Computing, and Wireless Sensing," *IEEE J. Sel. Top. Signal Process.*, vol. 17, no. 1, pp. 9–39, Jan. 2023, doi: 10.1109/JSTSP.2023.3239189.

[3] P. Sun, L. Luo, S. Liu, and W. Wu, "Adaptive rule engine for anomaly detection in 5g mobile edge computing," in *2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, IEEE, 2020, pp. 690–691.

[4] A. El Sayed, M. Ruiz, H. Harb, and L. Velasco, "Deep Learning-Based Adaptive Compression and Anomaly Detection for Smart B5G Use Cases Operation," *Sensors*, vol. 23, no. 2, Art. no. 2, Jan. 2023, doi: 10.3390/s23021043.

[5] K. Yang, H. Ma, and S. Dou, "Fog intelligence for network anomaly detection," *IEEE Network*, vol. 34, no. 2, pp. 78–82, 2020.

[6] A. De GAETANO, "Trusted virtual switching in 5G MEC for critical systems: implementation and performance evaluation," 2019.

[7] O. R. Devi *et al.*, "The Future Development Direction of Cloud-Associated Edge-Computing Security in the Era of 5G as Edge Intelligence," *Scientific Programming*, vol. 2022, 2022.

[8] SongPei-Cheng, PanJeng-Shyang, ChaoHan-Chieh, and ChuShu-Chuan, "Collaborative Hotspot Data Collection with Drones and 5G Edge Computing in Smart City," *ACM Transactions on Internet Technology*, Nov. 2023, doi: 10.1145/3617373.

[9] A. Feriani, A. Refaey, and E. Hossain, "Tracking pandemics: A MEC-enabled IoT ecosystem with learning capability," *IEEE Internet of Things Magazine*, vol. 3, no. 3, pp. 40–45, 2020.

[10] B. Deebak, "Cooperative Mobile Traffic Offloading in Mobile Edge Computing for 5G HetNet IoT Applications," *Real-Time Intelligence for Heterogeneous Networks: Applications, Challenges, and Scenarios in IoT HetNets*, pp. 43–58, 2021.

[11] Z. Zhou *et al.*, "Secure and latency-aware digital twin assisted resource scheduling for 5G edge computing-empowered distribution grids," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4933–4943, 2021.

[12] J. Santos, T. Wauters, B. Volckaert, and F. De Turck, "Towards delay-aware container-based service function chaining in fog computing," in *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*, IEEE, 2020, pp. 1–9.

[13] Z. Bing, X. Wang, Z. Dong, L. Dong, and T. He, "A novel edge computing architecture for intelligent coal mining system," *Wireless Netw*, vol. 29, no. 4, pp. 1545–1554, May 2023, doi: 10.1007/s11276-021-02858-x.

[14] J. Lam and R. Abbas, "Machine learning based anomaly detection for 5g networks," *arXiv preprint arXiv:2003.03474*, 2020.

[15] J. Santos, P. Leroux, T. Wauters, B. Volckaert, and F. De Turck, "Anomaly detection for smart city applications over 5g low power wide area networks," in *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, IEEE, 2018, pp. 1–9.

[16] L. Zhang, M. Peng, W. Wang, Z. Jin, Y. Su, and H. Chen, "Secure and efficient data storage and sharing scheme for BLOCKCHAIN-BASED MOBILE-EDGE computing," *Trans Emerging Tel Tech*, vol. 32, no. 10, p. e4315, Oct. 2021, doi: 10.1002/ett.4315.

[17] Y. Wu, H.-N. Dai, and H. Wang, "Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2300–2317, Feb. 2021, doi: 10.1109/JIOT.2020.3025916.

[18] S. A. Bhat, I. B. Sofi, and C.-Y. Chi, "Edge computing and its convergence with blockchain in 5G and beyond: Security, challenges, and opportunities," *IEEE Access*, vol. 8, pp. 205340–205373, 2020.

[19] R. Pietrantuono, M. Ficco, and F. Palmieri, "Testing the resilience of MEC-based IoT applications against resource exhaustion attacks," *IEEE Transactions on Dependable and Secure Computing*, 2023.

[20] L. Fernández Maimó, A. Huertas Celdrán, M. Gil Pérez, F. J. García Clemente, and G. Martínez Pérez, "Dynamic management of a deep learning-based anomaly detection system for 5G networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 3083–3097, 2019.

[21] H. Zhao *et al.*, "Application of 5G communication technology in ubiquitous power internet of things," in *2020 Asia Energy and Electrical Engineering Symposium (AEEES)*, IEEE, 2020, pp. 618–624.

979-8-3503-6118-6/24/$31.00 ©2024 IEEE