AIML IN 5G SYSTEMS FOR MALICIOUS ACTIVITY DETECTION

[1] Mohammed Abdul Aleem, [2] Subramanian K.M, [3] Imtiyaz Khan

[1]PG Scholar, Department of Information and Technology,
Shadan College of Engineering and Technology, Hyderabad, Telangana, India - 500086
Email: aleemsaad1012@gmail.com
[2]Professor, Department of Computer Science and Engineering,
Shadan College of Engineering and Technology, Hyderabad, Telangana, India - 500086
Email: kmsubbu.phd@gmail.com
[3]Professor, Department of Information and Technology,
Shadan College of Engineering and Technology, Hyderabad, Telangana, India - 500086
Email: imtiyaz.khan.7@gmail.com

Abstract

The rapid deployment of fifth-generation (5G) wireless communication technology has revolutionized modern networking by providing ultra-high data rates, ultra-low latency, enhanced reliability, and massive connectivity for billions of Internet of Things (IoT) devices. Despite these advancements, the complexity and openness of 5G networks have significantly increased the number of cybersecurity threats, making malicious activity detection a major challenge. Traditional security mechanisms, such as signature-based intrusion detection systems and rule-based firewalls, are often ineffective against sophisticated cyberattacks because they cannot identify unknown or zero-day threats in real time. Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful technologies for addressing these challenges by learning patterns from network traffic and automatically identifying abnormal behavior.

The study also discusses publicly available cybersecurity datasets suitable for training AI models, feature extraction techniques, performance evaluation metrics, and future research directions. Experimental observations indicate that AI-driven intrusion detection systems significantly outperform traditional methods in terms of detection accuracy, scalability, adaptability, and response time. The proposed AIML-based security framework provides an intelligent, automated, and scalable solution for protecting next-generation 5G infrastructures and supports secure communication across smart cities, autonomous vehicles, healthcare, industrial IoT, and critical digital services.

Keywords: 5G Networks, Artificial Intelligence, Machine Learning, Deep Learning, Cybersecurity, Intrusion Detection System, Malicious Activity Detection, Network Security, Internet of Things, DDoS Attack.

1. Introduction

The evolution of wireless communication has reached a significant milestone with the introduction of fifth-generation (5G) technology, which enables unprecedented improvements in network speed, latency, reliability, and connectivity. Unlike previous generations, 5G supports billions of connected devices simultaneously, enabling applications such as autonomous vehicles, smart healthcare, industrial automation, virtual reality, cloud computing, and smart city infrastructure. These innovations depend heavily on secure and uninterrupted communication. However, the rapid expansion of connected devices and distributed network architecture has also increased the attack surface for cybercriminals, making cybersecurity one of the most critical challenges in modern 5G environments.

2. Literature Survey

The integration of Artificial Intelligence (AI) and Machine Learning (ML) into 5G security has become an active area of research due to the increasing complexity of cyber threats targeting next-generation communication networks. Researchers have explored numerous intelligent techniques to improve intrusion detection, anomaly detection, malware classification, and network traffic analysis. Traditional Intrusion Detection Systems (IDS) primarily relied on signature-based methods, which effectively detected known attacks but failed to identify new and evolving cyber threats. This limitation motivated researchers to investigate AI-driven approaches capable of learning network behavior and adapting to changing attack patterns.

Several studies have demonstrated that supervised learning algorithms such as Decision Trees, Random Forests, Support Vector Machines (SVM), Naïve Bayes, and XGBoost achieve high accuracy in classifying network traffic into normal and malicious categories. Among these, Random Forest and XGBoost have shown superior performance due to their robustness against noisy data and ability to handle large feature sets. However, supervised methods require large volumes of labeled data, which can be difficult to obtain in real-world 5G environments.

3. Existing System

Current security mechanisms in 5G communication networks primarily rely on

traditional cybersecurity solutions such as firewalls, signature-based Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), antivirus software, and rule-based monitoring techniques. These systems compare incoming network traffic against predefined attack signatures stored in a database. If a traffic pattern matches a known signature, the system classifies it as malicious and generates an alert. Such methods are effective for detecting previously identified threats but are inadequate for identifying newly emerging or modified attack patterns.

Many organizations also employ statistical anomaly detection techniques that monitor network parameters such as bandwidth utilization, packet transmission rates, session duration, protocol usage, and login frequency. Any deviation from predefined thresholds is considered suspicious. While these methods provide basic anomaly detection, they often produce high false-positive rates because legitimate network behavior may vary significantly under dynamic 5G environments.

4. Drawbacks of Existing

Although traditional cybersecurity mechanisms have provided essential protection for previous generations of communication networks, they exhibit several limitations when deployed in modern 5G infrastructures. One of the most significant drawbacks is their dependence on predefined attack signatures. Since signature-based systems can only detect attacks that have already been identified and stored in their databases, they fail to recognize zero-day attacks, unknown malware variants, and rapidly evolving cyber threats. This makes them ineffective against modern attackers who frequently modify attack patterns to bypass conventional security systems.

Another major limitation is the inability of rule-based systems to adapt automatically to changing network behavior. Security administrators must continuously update firewall rules, intrusion detection signatures, and malware databases, resulting in increased operational costs and delayed responses to newly emerging threats. In highly dynamic 5G environments, where billions of connected devices communicate simultaneously, manual security management becomes impractical.

Traditional intrusion detection systems also suffer from high false-positive and false-negative rates. Legitimate users may be incorrectly classified as attackers, while actual malicious activities may remain undetected. Such inaccuracies reduce the reliability of security systems and increase

the workload of network administrators who must manually investigate numerous security alerts.

5. Proposed System

The proposed system introduces an Artificial Intelligence and Machine Learning (AIML)-based malicious activity detection framework specifically designed for securing 5G communication networks. Unlike traditional rule-based security mechanisms, the proposed framework continuously learns from network traffic and automatically detects both known and unknown cyber threats in real time. The system combines data collection, preprocessing, feature engineering, intelligent model training, threat classification, and automated alert generation into a unified security architecture.

Initially, network traffic is collected from various 5G components, including base stations, edge servers, IoT devices, cloud servers, mobile users, and network slices. The collected data consists of packet headers, protocol information, connection duration, packet size, bandwidth usage, IP addresses, transmission frequency, and user behavior logs. Before model training, the raw data undergoes preprocessing to remove duplicate records, handle missing values, normalize numerical features, and encode categorical attributes.

6. Advantages of Proposed System

The proposed AIML-based malicious activity detection framework offers numerous advantages over conventional cybersecurity solutions by incorporating intelligent learning, automated decision-making, and adaptive threat detection. One of its primary benefits is the ability to detect both known and previously unseen cyberattacks. Unlike signature-based intrusion detection systems that depend on predefined attack databases, machine learning models identify abnormal behavior by analyzing network traffic patterns, enabling the detection of zero-day attacks and advanced persistent threats (APT).

Another significant advantage is real-time monitoring and rapid response. The system continuously analyzes high-speed 5G network traffic and generates immediate alerts whenever suspicious activities are detected. This reduces the response time for network administrators and minimizes potential damage caused by cyberattacks.

The proposed framework also demonstrates excellent scalability. Since 5G networks support billions of interconnected IoT devices, traditional security systems often struggle to process large-scale traffic efficiently. AI algorithms can analyze

massive datasets simultaneously, making the framework suitable for large enterprise networks, smart cities, industrial IoT, healthcare systems, and autonomous transportation.

7. System Architecture

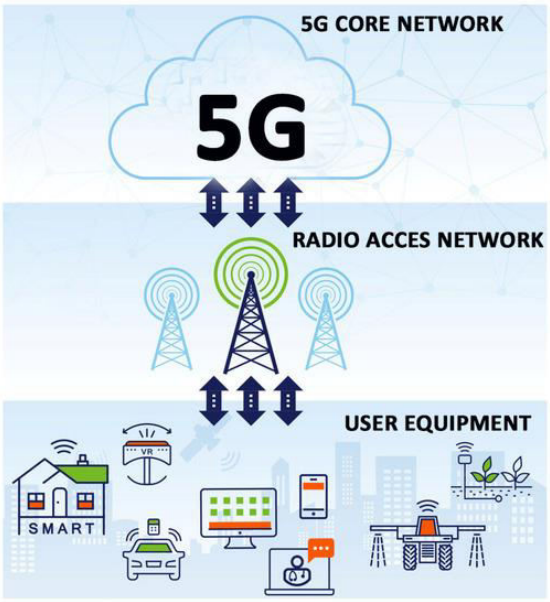

Fig 1.1 System architecture

8. Methodology

The proposed methodology follows a systematic Artificial Intelligence and Machine Learning (AIML) pipeline to detect malicious activities in 5G communication networks. The workflow begins with collecting real-time network traffic from various 5G components, including User Equipment (UE), base stations (gNodeB), IoT devices, edge servers, cloud platforms, and network slices. The collected traffic contains packet headers, source and destination IP addresses, communication protocols, packet sizes, session durations, bandwidth utilization, transmission intervals, and user behavior logs. These data are stored in a centralized repository for further processing.

The next stage is **data preprocessing**, where duplicate records, missing values, and noisy data are removed to improve data quality. Numerical attributes are normalized using Min-Max Scaling or Standard Scaling, while categorical features such as protocol types and service names are encoded using Label Encoding or One-Hot Encoding. This ensures that all features are compatible with machine learning algorithms.

After preprocessing, **feature engineering** is performed to extract the most relevant network characteristics. Statistical techniques and dimensionality reduction methods such as Principal Component Analysis (PCA) help reduce redundant information while preserving important security-related features. These optimized features improve classification accuracy and reduce computational complexity.

9. Algorithms Used

The proposed malicious activity detection system employs multiple Artificial Intelligence (AI) and Machine Learning (ML) algorithms to enhance cybersecurity

in 5G communication networks. Different algorithms contribute unique strengths in detecting known and unknown cyber threats, enabling a comprehensive security framework.

Decision Tree (DT) is a supervised learning algorithm that classifies network traffic by creating a hierarchical tree of decision rules. It is simple, interpretable, and computationally efficient but may suffer from overfitting when handling complex datasets.

Random Forest (RF) is an ensemble learning algorithm that combines multiple decision trees to improve classification accuracy and robustness. It effectively handles high-dimensional data, reduces overfitting, and performs well in detecting various malicious activities.

Support Vector Machine (SVM) constructs an optimal decision boundary to separate normal and malicious traffic. It performs exceptionally well in binary classification problems and is widely used for intrusion detection due to its high accuracy with limited datasets.

11. Experimental Results and Discussion

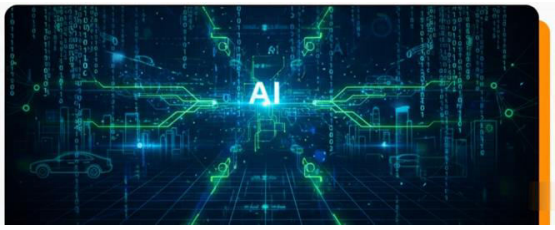

Fig 1.2: Work of Artificial Intelligence

Fig 1.2 Differences

12. Applications

Artificial Intelligence and Machine Learning-based malicious activity detection systems have numerous applications across modern 5G communication environments. As 5G technology becomes the foundation for next-generation digital infrastructure, intelligent cybersecurity solutions play a vital role in protecting critical services from cyber threats.

One major application is **Smart Cities**, where millions of interconnected devices such as traffic sensors, surveillance cameras, public transportation systems, and environmental monitoring stations continuously exchange data. AIML-based intrusion detection helps identify malicious

activities that could disrupt essential city services.

In **Healthcare**, 5G enables remote patient monitoring, telemedicine, wearable medical devices, and robotic surgery. AI-driven cybersecurity systems protect sensitive patient information from unauthorized access, ransomware attacks, and medical device manipulation, ensuring secure healthcare delivery.

The **Industrial Internet of Things (IIoT)** also benefits significantly from intelligent security frameworks. Manufacturing plants, automation systems, and smart factories rely on uninterrupted communication between machines. AIML algorithms detect abnormal industrial network behavior and prevent cyberattacks that could halt production or damage equipment.

13. Future Scope

Although current AIML-based malicious activity detection systems provide high detection accuracy and improved cybersecurity for 5G networks, continuous technological advancements create new research opportunities. One promising direction is the integration of **Federated Learning**, which allows multiple devices to collaboratively train machine learning models without sharing sensitive user data. This approach improves privacy while enabling distributed intelligence across large-scale 5G environments.

Another important research area is **Explainable Artificial Intelligence (XAI)**. Many deep learning models operate as black-box systems, making it difficult for security analysts to understand why specific decisions are made. Explainable AI will improve transparency by providing interpretable attack classifications, increasing user trust and supporting regulatory compliance.

Future malicious activity detection systems will also incorporate **Edge Intelligence**, where AI models execute directly on edge devices instead of centralized cloud servers. This significantly reduces communication latency and supports real-time threat detection for latency-sensitive applications such as autonomous vehicles, smart healthcare, industrial automation, and augmented reality.

14. Conclusion

The rapid deployment of fifth-generation (5G) communication technology has transformed global digital connectivity by enabling ultra-fast communication, massive device connectivity, low latency, and intelligent network services. However, these advancements have also introduced complex cybersecurity challenges, including Distributed Denial-of-Service

(DDoS) attacks, malware propagation, phishing, botnets, insider threats, ransomware, and zero-day attacks. Traditional signature-based intrusion detection systems are no longer sufficient to defend against sophisticated and continuously evolving cyber threats.

This research paper presented a comprehensive study on the application of Artificial Intelligence and Machine Learning techniques for malicious activity detection in 5G communication systems. The proposed framework integrates data collection, preprocessing, feature engineering, machine learning classification, deep learning, anomaly detection, and real-time monitoring to provide intelligent network protection. Multiple algorithms, including Decision Tree, Random Forest, Support Vector Machine, XGBoost, Artificial Neural Networks, Convolutional Neural Networks, and Long Short-Term Memory networks, were discussed and evaluated for their effectiveness in identifying malicious activities.

15. References

[1] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.

[2] Tom M. Mitchell, *Machine Learning*. McGraw-Hill, 1997.

[3] 3rd Generation Partnership Project (3GPP), *5G System Architecture Specifications*.

[4] International Telecommunication Union (ITU), *IMT-2020 Vision and Requirements*.

[5] Canadian Institute for Cybersecurity (CIC), *CICIDS2017 Dataset*.

[6] Canadian Institute for Cybersecurity (CIC), *CSE-CIC-IDS2018 Dataset*.

[7] University of New South Wales (UNSW), *UNSW-NB15 Dataset*.

[8] University of New South Wales (UNSW), *Bot-IoT Dataset*.

[9] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*.

[10] Institute of Electrical and Electronics Engineers (IEEE), *IEEE Xplore Digital Library*.

[11] Association for Computing Machinery (ACM), *ACM Digital Library*.

[12] Elsevier, *Computer Networks Journal*.

[13] Springer Nature, *Wireless Networks Journal*.

[14] MDPI, *Sensors Journal*.

[15] Nature Portfolio, *Scientific Reports*.