Efficient Approaches for Detecting Denial of Service (DoS) Attacks in 5G Networks: A Review

Kajal[1], Krishan Kumar Ranga[2]
[1]*Research Scholar Department of Computer Science and Engineering, Guru Jambheshwar University of Science and Technology, Hisar, Haryana (India)*
[2]*Assistant Professor, Department of Computer Science and Engineering, Guru Jambheshwar University of Science and Technology, Hisar, Haryana (India)*

***Abstract*—Digital communications have been revolutionized by the deployment of 5G networks, which offer incredibly fast speeds, low latency, and the capacity to link a large number of devices. These enhancements do, however, also introduce additional security threats, particularly those associated with Distributed Denial of Service (DDoS) and Denial of Service (DoS) attacks. Both conventional and modern techniques for detecting DoS attacks in 5G environments are thoroughly examined in this paper. It examines the aspects of DoS attacks that are specific to 5G, such as the abuse of big bandwidth, widespread exposure of IoT, and protocol flaws.**

The study compares several detection strategies, such as rule-based, machine learning, and deep learning methods, highlighting the advantages of AI-driven solutions in terms of accuracy and flexibility. The potential for context-aware detection through network slicing is also explored. In order to address the growing complexity and dangers associated with 5G networks, the results emphasize the need for resource-efficient, scalable, and intelligent solutions.

***Index Terms*—5g, DoS attacks, machine learning, artificial learning etc.**

I. INTRODUCTION

The development of 5G technology, the most recent generation of mobile networks, has provided notable improvements over earlier generations such as 2G, 3G, and 4G/LTE-A. Faster routing speeds during upstream and downstream services, reduced latency, increased bandwidth size, enabling new applications such as the Internet of Things (IoT), and enhanced reliability are a few of the enhancements [1]. Nevertheless, there are other problems that still pose a risk to 5G networks' overall quality of service. There are numerous challenges that 5G networks must overcome today in order to deliver high-quality service. Network congestion, interference, security vulnerabilities, and high deployment costs are a few of these Issues that lead to poor coverage, low routing speeds, decreased dependability, low throughput, vulnerable to cyber-attacks, and general performance degradation that affects user experience [2]. The paradigm transition from traditional physical network resources to dynamic virtualization, software-defined networking, and cloud computing has been brought about by 5G's software-dependent characteristics, which has also given cybercriminals/cyber threats numerous options[3].Networks have grown significantly in recent years, mostly due to the extensive use of Internet of Things (IoT) devices [4]. These gadgets frequently manage sensitive data, such as real-time photos, location data, and financial information, despite typically having minimal processing capability. This feature makes IoT devices easy targets for assaults because successful breaches result in high-value data, which raises the number of cyber security incidents significantly [5]. Numerous businesses and organizations are battling this illegal behaviour, creating new methods to stop attacks, and publishing papers, evaluations, studies, and articles to expose hacker flaws in an attempt to lessen their tactics [6]. Additionally, legislative actions are part of the commitment to cyber security. By taking advantage of weaknesses, digital bandits have also demonstrated their ability to breach even the most protected and encrypted networks. Data theft, cyber-attacks, infrastructure damage, ransom demands, blackmail, interruption of vital services, dangers to democracy, and fatalities are all consequences of such vulnerabilities that are frequently covered by

breaking news. Consequently, there is a greater need to invest in techniques that facilitate safer and more secure communications through open user policies, trust models, and End-to-End (E2E) visibility. Furthermore, the idea of dedicated network resources for dedicated network functions has given way to more dynamic virtualization, cloudification, orchestration, automation, and softwareization of network functions from common/shared network resources in 5G and beyond [7].

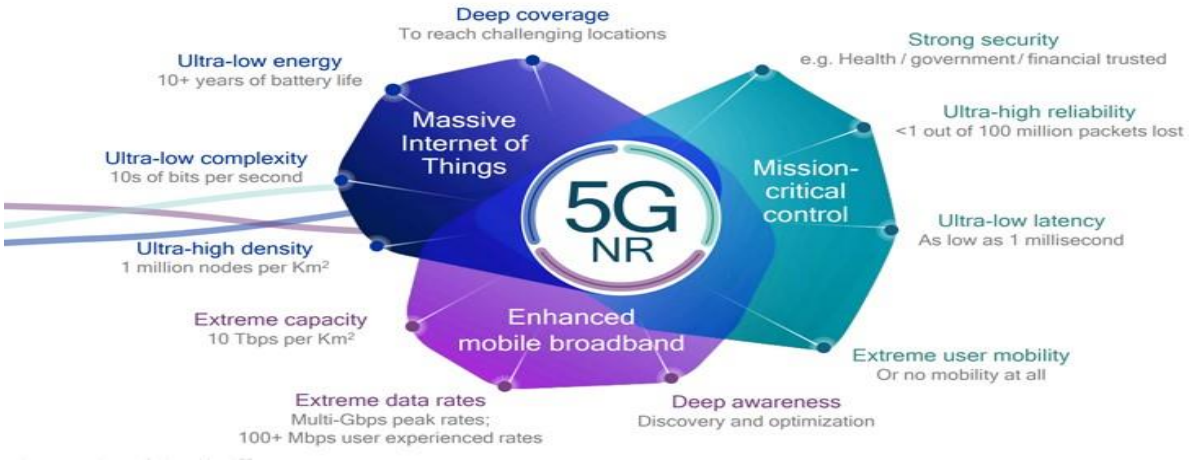

Figure1 the image showcases 5G NR's capabilities, highlighting.

II. DOS ATTACK

This type of attack overloads the target (host or network) by impairing the services it provides, either temporarily or permanently, rendering it unavailable to its intended users. When a hacker successfully uses up all of the system's resources or network bandwidth, the server may crash or perform worse [8].

Because it prevents authorized users from accessing the system, the hack disrupts regular operations and costs the company money. Attacks of this type can take many different forms, from flooding a server with too many requests to slow it down, making requests using fake IP addresses or overloading a server with a large amount of incorrect data [9].

DoS assaults often fall into one of four main categories, each with unique traits

• Volumetric: These are flood-based assaults that overwhelm the target with asymmetric data flows by flooding it with a large volume of packets.

• Computational: The goal of these attacks is to deplete computational resources by using up CPU and memory resources.

• Vulnerability-based: It involves taking advantage of software systems' flaws. These attacks aim to weaken the target's security posture by focusing on known flaws.

When a host or network is subjected to a denial-of-service attack, the attack can show up as a number of symptoms, including: poor victim performance, network connectivity issues, low network communication, high CPU usage, a large volume of packets flooding the network, and slowed accessibility, unresponsiveness, or total server shutdown [10].

The assault method is referred to as DoS when it is carried out by a single source. However, the attack is referred to as a Distributed Denial of Service (DDoS) when several different sources work together to carry it out. Using a network of devices that the attacker controls remotely, known as a "botnet," DDoS attacks use a number of devices to transmit harmful traffic in the direction of their target [11]. More advanced tactics must be used to counteract this kind of attack because blocking a single source is usually ineffective because there are so many sources involved.

Typical DoS Attack Features in 5G Networks: In a 5G network, a denial of service (DoS) attack

aims to overload or interfere with network functions, rendering them inaccessible to authorized users. The main features of DoS attacks in the context of 5G are as follows:

1. High Bandwidth Exploitation: Attackers can use 5G's huge bandwidth and lightning-fast speeds to execute high-volume attacks, which rapidly deplete the network's available resources.
2. Massive Connectivity Target: 5G enables millions of linked devices per square kilometer (Massive IoT), raising the number of possible targets, particularly low-power IoT devices with inadequate protection.

3. Exploitation of Protocols 5G brings new service-based architecture (SBA), network slicing, and virtualization (NFV).
• These intricate systems have flaws that hackers can take advantage of to interfere with services.

4. Risk of Denial of Service (DDoS) Exposure Large-scale DDoS assaults might cause more damage because of the large number of endpoints that are linked.
• Botnets composed of compromised Internet of Things devices, similar to those in 4G, are considerably more potent in 5G.

5. Attacks Targeting Control and User Planes: Attacks may target either the user plane (data floods, for example) or the control plane (signaling storms).
• Control plane DoS can interfere with crucial network administration tasks.

6. Patterns of Smart Attacks: the ability of AI-driven attacks to dynamically alter behavior to evade conventional detection techniques makes them more difficult to anticipate and stop.
More difficult to identify and prevent
• The window for detection is shortened by 5G's low latency and rapid speed; conventional defenses might not be able to keep up. [12]

III. ATTACK ARCHITECTURE

Architecture of Attack DDoS assaults are planned using a set of procedures that call for particular roles and equipment. They are frequently planned using amplification methods or device-based botnets. Attackers can readily use these devices, which frequently lack strong security measures, to produce large volumes of traffic data. A DDoS attack is demonstrated in Figure 2, where the attacker controls several agents using handlers.
Once compromised, the victim is directed to receive attack traffic from these agents [13]:
• Handler: This is the host that is executing the tool that the attacker uses to initiate and manage a DDoS assault. In order to manage compromised agents and plan the attack, the handler acts as the attacker's main command center.
Agent: The agent is a hacked host that is in charge of executing a daemon process that carries out the handler's directives. Because malicious software has been installed on these compromised hosts, the attacker can take control of them from a distance. They use a daemon process to receive and carry out handler tasks. DDoS attacks are launched against the victim site using this daemon process.

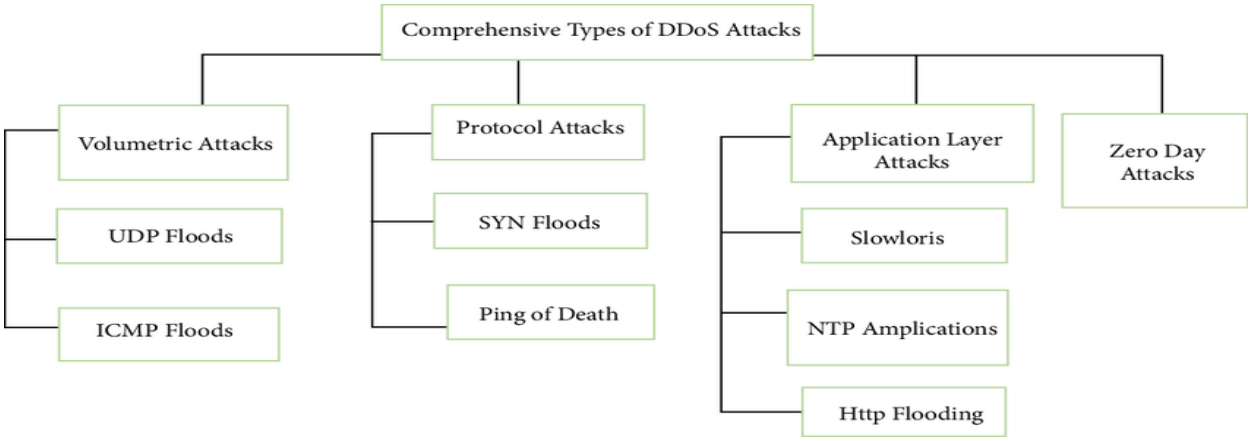

Figure3. Denial of service attack classification

IV. LITERATURE REVIEW

Fang, *et al.* [15] conducted a comprehensive survey of 5G wireless network security, highlighted how advanced features of 5G introduced new security requirements and challenges compared to traditional cellular networks. The review began by outlining the unique characteristics and motivations behind 5G securities, then summarized potential attacks and required security services-such as authentication, availability, data confidentiality, key management, and privacy-within the context of new 5G use cases. It also assessed recent developments and existing
Security schemes, particularly in relation to emerging technologies like heterogeneous networks, device-to-device communications, massive MIMO, software-defined networking, and the Internet of Things. The authors proposed new security architecture for 5G, analyzed identity management and flexible authentication, and illustrated the benefits through a handover case study. The review concluded by identifying ongoing challenges and future research directions, emphasized the need for robust, adaptive security solutions in the evolving 5G landscape.

Park *et al.* [16] reviewed the evolution of mobile communication security from 2G to 5G, emphasized the increased complexity and new security challenges introduced by 5G's architecture and services. The literature highlighted that while 5G offered ultra-fast speeds, low latency, and supported massive device connectivity, these advances also expanded the attack surface and introduced vulnerabilities not present in previous generations. The authors discussed how traditional security approaches were insufficient for 5G due to its use of software-defined networking (SDN), decentralized core networks, and dedicated protocols like NGAP and GTP. Prior studies identified that the non-standalone (NSA) 5G architecture, which integrated LTE and 5G components, inherited security weaknesses from both networks. However, most existing research focused on theoretical or simulated environments rather than real-world deployments. The author addressed this gap by assessing actual 5G NSA networks, identified and validated vulnerabilities, and proposed practical countermeasures. Their review underscored the urgent need for ongoing security assessments and the development of dedicated 5G security technologies to protect user privacy and network integrity in real-world scenarios.

Dolente, *et al.* [17]. Reviewed on 5G network security increasingly focused on the unique challenges introduced by the adoption of open-source platforms and network function virtualization. Prior studies highlighted that while 5G standards, such as those set by 3GPP, introduced stronger security constraints than previous generations, the responsibility for effective implementation fell on vendors and mobile network operators (MNOs). Researchers assessed vulnerabilities in 5G core architectures, especially in service-based interfaces (SBIs) and network functions like AMF and NRF/NEF, and showed that traditional security mechanisms were inadequate for these new paradigms. Formal verification and fuzz testing uncovered protocol flaws in open-source 5G frameworks, such as Open5GS and OAI, but most work focused on simulated or controlled environments rather than real-world deployments.

Pascale *et al.* [18] developed an embedded Intrusion Detection System (IDS) for the automobile sector. It analyzed CAN bus traffic to detect potential hacks. The authors concentrated on the deployment and effectiveness of their suggested IDS, but did not provide a complete analysis of the cyber security landscape or how to integrate developing standards and laws.

Ahmad *et al.* [19] have monitored advancements in network intrusion detection systems (NIDS) with particular focus on ML and DL techniques. Their research showed that while ML and DL approaches were achieving better accuracy and adaptability, conventional IDS systems were struggling with recognizing new attempts at intrusion while maintaining low false alarm rates. The authors performed a critical analysis of recent research publications (2017–2020) and provided taxonomy of techniques based on ML and DL used in NIDS along with discussion of their methodology, pros, and cons the study also compared available datasets and evaluation metrics that are commonly used in the industry. The authors noted that there is significant progress made, but some gaps still need to be resolved, such as more accurate detection of zero-day attacks, reduction of false positives, and development of dependable, scalable, real-time NIDS. The conclusion of the study proposed new directions of

research to address these gaps and improve NIDS with AI capabilities.

Pascale *et al.* [20] proposed an automotive cyber security increasingly addressed the growing risks associated with the connectivity of modern vehicles, especially as they became integral parts of the Internet of Things (IoT) and smart city ecosystems. Researchers highlighted that traditional automotive network, such as the CAN-Bus, were vulnerable to a range of cyber-attacks due to their lack of encryption and increasing exposure through new communication interfaces. Previous approaches to securing in-vehicle networks included redesigning hardware and software or implementing intrusion detection systems (IDS), but many solutions faced challenges related to computational constraints and real-time performance. In this context, the author proposed an embedded IDS for connected vehicles that used a two-step algorithm-combining spatial-temporal analysis and Bayesian networks-to detect anomalies in CAN-Bus traffic. Their work built on existing research by providing efficient, experimentally validated IDS that demonstrated promising results against common automotive cyber-attacks, while also acknowledging the need for ongoing adaptation to evolving threats and standards in the automotive domain.

Chaganti *et al.* [21] reviewed on block-chain security increasingly addressed the growing threat of Denial of Service (DoS) attacks within block-chain ecosystems, especially as block-chain technology was adopted across diverse sectors such as finance, healthcare, and supply chain management. While block-chain's decentralized and cryptographically secured architecture offered inherent security advantages, researchers highlighted that it remained vulnerable to various attacks, including DoS, eclipse, double-spending, and 51% attacks Prior studies primarily focused on leveraging block-chain to mitigate DoS threats in conventional networks, but comprehensive surveys specifically addressing DoS attacks targeting block-chain systems were limited. Author addressed this gap by systematically analyzed and categorized state-of-the-art DoS attack methods, detection strategies, and mitigation solutions within block-chain peer-to-peer networks and crypto exchanges. Their review also discussed the application of machine learning and deep learning techniques for attack detection, and identified open challenges and future research directions, emphasized the urgent need for robust, adaptive security mechanisms to protect the evolving block-chain infrastructure.

Aslam *et al.* [22] provided on securing Internet of Things (IoT) networks increasingly explored the integration of Software Defined Networking (SDN) and machine learning to address the growing threat of Distributed Denial-of-Service (DDoS) attacks. Traditional network security solutions often proved too costly and lacked scalability for IoT environments, which were highly vulnerable due to numerous resource-constrained devices. Prior studies proposed SDN-based frameworks and machine learning-driven intrusion detection systems to enhance network protection, but many existing solutions either relied on single classifiers, lacked adaptiveness, or did not efficiently mitigate diverse DDoS attack types. The author addressed these gaps by introducing an Adaptive Machine Learning based SDN-enabled DDoS Detection and Mitigation (AMLSDM) framework. Their approach leveraged a multilayered ensemble of machine learning classifiers and real-time traffic analysis to improve detection accuracy and reduce false alarms. Experimental results demonstrated that the AMLSDM framework outperformed existing methods, offering a more robust and adaptive solution for safeguarding SDN-enabled IoT networks against evolving DDoS threats.

Amponis *et al.* [23] provided an in-depth examination of security vulnerabilities in 5G core networks, with a particular focus on the risks posed by Denial of Service (DoS) attacks targeting the Packet Forwarding Control Protocol (PFCP). The authors reviewed the landscape of 5G security, highlighted how the increased complexity and modularity of 5G core architecture, while enabling advanced features and new IoT and industrial use cases, also introduced new attack surfaces and protocol-specific weaknesses. Prior research largely concentrated on threats at the radio access network (NG-RAN) level or on use-case-specific vulnerabilities, whereas this study differentiated itself by experimentally demonstrated and analyzed five distinct PFCP-based DoS attacks within the 5G core, including unauthorized session deletion and modification, session establishment flooding, misconfiguration of forwarding rules, and user traffic eavesdropping. The paper not only evaluated the impact of these attacks-showing that they could

disrupt UAV communications without affecting radio connectivity-but also discussed potential mitigation strategies and the need for robust intrusion detection datasets to support AI-driven security solutions. This work advanced the literature by shifting focus to core-level vulnerabilities and provided practical insights for enhancing the resilience of 5G-enabled UAV and IoT applications.

Kumari and Mrunalini [23] provided on Distributed Denial of Service (DDoS) attacks highlighted their growing sophistication and the significant threat they posed to networked systems, particularly in terms of resource exhaustion and service disruption. Early studies developed detection methods using classification trees, deep neural networks, and autonomous infrastructures like SDN-based frameworks to counter DDoS threats. Machine learning approaches-including Support Vector Machines, Artificial Neural Networks, Decision Trees, and Naive Bayes-were widely investigated for their effectiveness in distinguishing between normal and attack traffic, with several works demonstrating improved detection accuracy and reduced false alarm rates. Other studies explored Botnets detection, flow-table sharing in SDN to prevent overload, and domain-based anomaly detection. Kumari and Mrunalini (2022) contributed to this body of work by proposing a mathematical model for bandwidth depletion and throughput analysis, and by applying machine learning algorithms such as Logistic Regression and Naive Bayes to the CAIDA 2007 dataset. Their results, implemented using the Weka platform, were compared with existing methods, demonstrating the continued relevance and advancement of machine learning techniques in mitigating DDoS attacks.

Fang, *et al.* [24] provided a comprehensive overview of security challenges and solutions for 5G mobile wireless networks. The paper began by outlining the unique features and advanced service requirements of 5G, such as ultra-low latency, massive device connectivity, and support for IoT, which introduced new security challenges compared to previous generations. The authors summarized potential attacks and necessary security services-including authentication, confidentiality, key management, and privacy-while they reviewed recent developments and existing security schemes. The study further discussed security implications of enabling technologies like heterogeneous networks, device-to-device communication, massive MIMO, software-defined networking, and network slicing. Motivated by current research, the authors proposed a flexible 5G security architecture and analyzed its effectiveness in identity management and authentication through a handover case study. They concluded by highlighting ongoing challenges and future research directions for robust 5G security.

Kifor and Popescu [25] present in depth the picture of present day automotive cyber security. We see that modern cars are getting to be more complex and connected which in turn presents them with new security and vulnerability issues which is what the research reports. Through extensive literature review and bibliometric analysis, the authors identified forth the4 main study areas which are -- frameworks and technologies, standards and regulations, monitoring and vulnerability management, and testing and validation. They also went into how automotive cyber security standards which include SAE J3061, UN Regulation No. 155, and ISO/SAE 20434 have grown over time and also he issues Oems and engineers have in- incorporation cyber security into the full vehicle life cycle. In order to provide more realistic and efficient cyber security solutions for the automobile sector, the evaluation also identified research gaps and recommended future approaches.

Benlloch-Caballero *et al.* [26] addressed the growing challenge of safeguarding massive 5G and 6G IoT networks from DDoS attacks. Recognizing that manual management isn't practical at such scale, they introduced an innovative, distributed, dual-layer self-defense system that operates autonomously. This system empowers both digital service providers and infrastructure providers to detect and counter DDoS attacks quickly and efficiently, even across different administrative domains. Their experiments showed the system was over 78% effective and responded to attacks more than three times faster than traditional methods. The study highlights how automation, collaboration, and distributed defenses are essential for keeping future IoT infrastructures resilient.

Akhtar *et al.* [27] developed a smart detection and mitigation approach using a deep learning model called ACGRU, fine-tuned with a novel optimization algorithm. Their method not only improved the

security and reliability of data in 5G-IoT networks but also delivered faster and more accurate DDoS detection. The results outperformed several existing techniques, underscoring the value of combining advanced AI and optimization methods to strengthen IoT network defenses as technology evolves.

Cetinkaya *et al.* [28] took a broad look at DoS attacks in networked control systems, such as those found in industrial and critical infrastructure. Their review covered how these attacks disrupt feedback control, state estimation, and coordination among multiple agents. They discussed different ways to model and understand attack strategies, from probabilistic to game-theoretic approaches, and reviewed recent progress in designing communication and control protocols that can withstand attacks. Their work is notable for bridging the gap between cyber security and control theory, offering a comprehensive guide for securing both industrial and social systems.

Salim *et al.* [29] provided an in-depth overview of DDoS attacks in the IoT world, especially as insecure devices like webcams and smart appliances become more common. These devices are easy targets for attackers, who use them to build massive botnets capable of launching powerful DDoS attacks on cloud and IoT services. The authors explored why IoT devices are targeted, how attack tactics are evolving, and what tools and techniques are being used. They also reviewed detection and mitigation strategies, presenting a well-rounded taxonomy of DDoS threats and countermeasures. Their work calls for robust, multi-layered defenses as IoT adoption and attack sophistication continue to rise.

Kumari and Mrunalini [30] focused on how machine learning can help detect DDoS attacks more accurately. Their research showed that approaches like classification trees, deep neural networks, and logistic regression are much better at distinguishing between legitimate and malicious traffic compared to older methods. By testing these algorithms on real-world data, they demonstrated significant improvements in detection accuracy and reliability, supporting the ongoing move toward AI-driven cyber security solutions.

Syed et al. [31] addressed the growing threat of Denial of Service (DoS) attacks in Internet of Things (IoT) environments, focusing on the widely used MQTT protocol. Their study highlighted that as MQTT adoption increased for IoT communications, so did its security vulnerabilities, particularly to application-layer DoS attacks that could disrupt critical services. The authors reviewed prior research, noting that most existing works either focused on performance evaluation or offered only limited security analysis for MQTT, often lacked real-world attack datasets. To bridge this gap, they proposed a machine learning-based detection framework specifically for MQTT DoS attacks, identified protocol-specific features that improved detection accuracy and reduced false positives. Their experimental results, conducted on physical IoT deployments, demonstrated that the proposed framework effectively detected DoS attacks, even when attackers attempted to mimic legitimate traffic. This research advanced the field by providing a practical, protocol-aware approach to securing IoT infrastructures against evolving DoS threats.

Haider, *et al.* [32] provided a comprehensive review of the opportunities and challenges of applying artificial intelligence (AI) and machine learning (ML) in 5G network securities. The paper highlighted how the rapid evolution of 5G-driven by softwareization, virtualization, and cloudification-increased both performance and security risks across all network domains, from end devices to the core. The authors discussed a wide range of threats and vulnerabilities in 5G, including device-level attacks, edge and radio access network threats, and core network risks such as DoS and DDoS attacks. They emphasized that traditional security methods were insufficient for the dynamic and data-intensive environment of 5G, and demonstrated how AI and ML enabled real-time threat detection, anomaly classification, and adaptive security protocol design. The article also reviewed the taxonomy of AI/ML technologies, their use cases in 5G security, and outlined future research directions, such as the development of autonomous, fully automated security mechanisms for next-generation networks.

Ala Mughaid *et al.* [33] reviewed on highlighted the growing threat of cyber-attacks in 5G wireless networks, particularly due to the expanded attack surface introduced by new technologies like Non-

Orthogonal Multiple Access (NOMA). Prior studies focused on simulating 5G environments and evaluated the effectiveness of various intrusion detection systems (IDS) using both traditional and machine learning-based approaches. Simulation platforms such as OMNeT++ were widely used to model wireless DoS attacks and assessed IDS performance, while deep learning models, including multilayer neural networks, demonstrated high accuracy in detecting network threats-though often on outdated datasets like KDD99. Other researchers explored machine learning-based authentication and anomaly detection, leveraged both supervised and unsupervised learning to enhance 5G security. Despite these advances, the literature noted a lack of up-to-date datasets and the need for robust, adaptive detection methods tailored to the unique characteristics of 5G and NOMA. The reviewed paper built on this foundation by proposing and evaluating a range of machine learning and deep learning techniques-including Decision Trees, KNN, Decision Forests, and Neural Networks-for detecting dropping attacks in simulated 5G NOMA environments, and demonstrated superior accuracy compared to previous methods.

Alashhab *et al.* [35] provided a comprehensive overview of Distributed Denial of Service (DDoS) attacks within cloud computing environments. The authors surveyed the evolution of DDoS attack techniques, highlighted how the scalability, multi-tenancy, and resource-sharing features of cloud platforms made them attractive and vulnerable targets. They examined existing research on DDoS attack vectors, tools, and methodologies used to compromise cloud services, as well as the unique challenges posed by the dynamic and distributed nature of cloud infrastructure. The review also covered various detection, prevention, and mitigation strategies proposed in the literature, identified gaps such as the need for more adaptive and intelligent defense mechanisms tailored to cloud-specific architectures. By synthesizing prior work, the authors laid the groundwork for their own taxonomy and emphasized unresolved Issues and emerging trends in cloud DDoS research.

Mikail Mohammed Salim *et al.* [36] distributed denial of service attacks and its defenses in IoT: a survey" surveyed the evolution of DDoS attacks in IoT environments and highlighted the proliferation of insecure IoT devices that made them prime targets for attackers. The authors reviewed how attackers exploited the constant connectivity and weak security of IoT devices to form large-scale botnets, which launched sophisticated multi-vector and volumetric DDoS attacks against both IoT and cloud platforms. They examined various attack motivations, tools, and infection methods used in the IoT context, and analyzed state-of-the-art detection, prevention, and mitigation strategies. The review compared prior surveys, identified the unique vulnerabilities of IoT systems, and emphasized the urgent need for robust, multi-layered defenses as DDoS attack sophistication increased with IoT adoption.

V. OPTIMIZATION TECHNIQUES

When it comes to optimizing Denial of Service (DoS) detection, traditional methods like rule-based systems, signature-based detection, and anomaly detection with set thresholds are the go-to strategies. They're quick and straightforward, but they often struggle to adapt to new or evolving attack patterns. In contrast, machine learning techniques such as Support Vector Machines (SVM), Random Forests, and Neural Networks offer a more flexible approach by learning from traffic patterns, which helps in identifying more sophisticated DoS attacks. On the cutting edge, advanced artificial intelligence (AI) and deep learning (DL) methods, especially Convolution Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, take detection accuracy to the next level through automatic feature extraction and scalability. Plus, with 5G's network slicing, we can achieve context-aware detection by isolating virtual network slices and applying analytics specific to each slice. When these techniques are combined with AI-driven methods, they can effectively pinpoint and mitigate attacks in the intricate 5G landscape.

VI. COMPARATIVE ANALYSIS

the reviewed techniques based on criteria such as detection accuracy, computational efficiency, scalability, and adaptability. AI and ML-based methods generally outperform traditional techniques but require significant computational resources and training data.

VII. PROBLEM STATEMENT

5G networks, like the expansion of, have witnessed rapid development because they enable wireless high-speed communication. Attacks on 5G networks are also on the rise. DDoS attacks decrease the availability of network resources. Furthermore, these assaults have the potential to degrade CPU performance. Inefficient data transmission channels waste time and energy. As a result, numerous researchers developed algorithms for detecting DDoS attacks. Nonetheless, current techniques face fewer difficulties, as seen below:

1) DDoS impact: Because of the shared virtualized architecture, DDoS assaults on 5G networks can target several resources at the same time, reducing overall network performance.
2) Evolving Attacks: Traditional security solutions struggle to keep up with the increasing sophistication and variety of DDoS attack strategies, necessitating a more advanced detection mechanism.
3) Emergence of 5G Networks: The rollout of 5G networks has introduced ultra-fast speeds, low latency, and massive device connectivity, but these advancements have also created new and significant security vulnerabilities.
4) Increased Attack Surface: The extensive use of IoT devices in 5G, many of which have minimal security, has expanded the potential targets for cyber-attacks, especially DoS and DDoS attacks.
5) Complex Network Architecture: 5G's reliance on dynamic virtualization, software-defined networking, and cloudification has increased the complexity of network management and introduced new opportunities for attackers.
6) Advanced DoS/DDoS Attack Techniques: Attackers exploit 5G's high bandwidth, protocol vulnerabilities, and massive device connectivity to launch more powerful and sophisticated DoS/DDoS attacks.
7) Limitations of Traditional Detection Methods: Existing rule-based and signature-based detection mechanisms are often inadequate for the high speed, low latency, and adaptive nature of 5G networks.
8) Need for Intelligent Solutions: There is a critical need for intelligent, scalable, and resource-efficient detection and mitigation solutions, such as those based on AI, machine learning, and context-aware mechanisms.
9) Real-Time Detection Challenge: The rapid data flow and low-latency requirements of 5G networks make real-time detection and response to DoS/DDoS attacks more challenging.
10) Evolving Attack Patterns: Attackers increasingly use AI-driven and adaptive strategies, making attacks harder to predict, detect, and block with conventional methods.
11) Impact on Service and Security: Successful DoS/DDoS attacks can lead to service outages, financial loss, data breaches, infrastructure damage, and threats to critical services and user privacy.
12) Urgent Research Need: There is an urgent need for ongoing research and development of advanced, adaptive, and area.

VIII. CONCLUSION

The review highlights that while 5G networks bring transformative advances in speed, connectivity, and flexibility, they also introduce new and significant security challenges-particularly in the form of DoS and DDoS attacks. The unique features of 5G, such as massive IoT connectivity, network slicing, and virtualization, create a broader attack surface and more complex vulnerabilities than previous generations. Traditional detection and mitigation strategies are often inadequate for the dynamic, high-speed, and low-latency environment of 5G. The comparative analysis of detection methods demonstrates that AI-driven and context-aware approaches, especially those leveraging machine learning and deep learning, offer superior adaptability and accuracy for identifying and mitigating DoS attacks in 5G settings. However, the ongoing evolution of attack techniques and the increasing complexity of network architectures underscore the urgent need for intelligent, scalable, and resource-efficient security solutions. Continued research and innovation are essential to ensure robust, real-time protection for 5G networks against ever-evolving cyber threats.

REFERENCES

[1] Manbayev, A. S. Imangaliyev, A. Y. Turlybekov, N. S. Sarsembayeva, and A. M. Aitmagambetov, (2022) "Research ofmachine learning algorithms for the development of intrusion detection systems in 5G mobile networks and beyond", Journal Sensors (Vol. 22, Issue 24, Article 9957, ISSN NO. no. 1424-8220), December 14, 2022, DOI: https://DOI.org/10.3390/s22249957.

[2] A. Yadav, N. Kumar, S. K. Gupta, and S. Tanwar (2022) "Intrusion detection system on IoT with 5G network using deep learning", Journal Wireless Communication and Mobile Computing (Article 9304689, ISSN NO. 1530-8669). July 19, 2022, DOI: https://DOI.org/10.1155/2022/9304689.

[3] P. Kumari and A. K. Jain (2023) "A comprehensive study of DDoS attacks over IoT networks" and their countermeasures, Journal Computers & Security (vol. 127, Article 103096, ISSN NO. 0167-4048), March 1,2023, DOI: https://DOI.org/10.1016/j.cose.2023.103096.

[4] S. Capusneanu, D. I. Topor, I. S. Rakos, C. O. Tenovici, and M. S. Hint (2023) "The main aspects of the impact of cybercrimes on the business environment in the digital era: Literature review", Journal Contributions to Finance and Accounting (F1313, pp. 151–171, ISSN NO. 2730-6038) date: March 5, 2025, DOI: https://DOI.org/10.1007/978-3-031-34082-6_7

[5] Khan et al. (2020) "5G security and privacy, published in IEEE Communications Surveys & Tutorials", vol. 22, Issue 1, pp. 196–248, August 8, 2019, March 11, 2020. ISSN NO.: 1553-877X, DOI: https://doi.org/10.1109/COMST.2019.2953364.

[6] R. Chaganti, R. V. Boppana, V. Ravi, K. Munir, M. Almutairi, F. Rustam, et al. "A Comprehensive Review of Denial-of-Service Attacks in Blockchain Ecosystem and Open Challenges," IEEE Access, vol. 10, pp. 96538-96562, 2022, ISSN NO.: 2169-3536, DOI: https://doi.org/10.1109/ACCESS.2022.3205019.

[7] Aslam, M., Ye, D., Tariq, A., et al. "Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT," journal in 2022. Sensors is an open access, peer-reviewed MDPI, with the ISSN NO. 1424-8220. Vol. 22, Issue 7, on pp 2697. Date: April 2022, DOI: https://doi.org/10.3390/s22072697

[8] Kimmi Kumari and M. Mrunalini et al. "Application of machine learning algorithms for detection of distributed denial-of-service attacks" Journal of Big Data in 2022. Vol. 9, article number 56, pp 1–17. ISSN NO. is 2196-1115. March 24, 2022.DOI: 10.1186/s40537-022-00616-0.

[9] U. Islam, A. Muhammad, R. Mansoor, M. S. Hossain, I. Ahmad, E. T. Eldin, J. A. Khan, A. U. Rehman, and M. Shafiq, "Detection of distributed denial of service (DDoS) attacks in IoT based monitoring system of banking sector using machine learning models," Sustainability, vol. 14, no. 14, Art. no. 8374, pp. 1–19, July 2022, ISSN NO.: 2071-1050. DOI: https://doi.org/10.1186/s40537-022-00616-0.

[10] Ortega-Fernandez, Ines, and Francesco Liberati 2023 "Denial of service (DoS) attacks and mitigation strategies in the smart grid, specifically focusing on the application of reinforcement learning techniques". Journal Energies, vol. 16, Issue 2, in 2023. page 635. ISSN NO. 1996-1073. DOI: https://doi.org/10.3390/s22072697

[11] Cloudflare, "How to DDoS | DoS and DDoS attack tools" Cloudflare Learning Center section, which provides educational resources on cybersecurity topics. The article discusses various DoS and DDoS attack tools, their mechanisms, and how organizations can defend against such threats using modern security solutions. As this is a web article and not a journal or conference paper, it does not have an ISSN NO., page numbers, or a DOI. on March 22, 2024.DOI: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/how-to-ddos/.

[12] Mishra, Anupama, Brij B. Gupta, and Ramesh Chandra Joshi "A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques," 2011 European Intelligence and Security Informatics Conference (EISIC), organized by IEEE. pp 286-289, September 12 to 14, 2011. ISSN NO. no.

2167-4961. The DOIhttps://doi.org/10.1109/EISIC.2011.15

[13] "DDoS Resources - How DDoS Attacks Work" Advanced Network Management Lab (ANML), Indiana University. http://anml.iu.edu/ddos/how to work.html July 9, 2010. Accessed on March 11, 2024.DOI: https://web.archive.org/web/20100709203549/http://anml.iu.edu/ddos/howtowork.html.

[14] Imperva, Inc. "DDoS Attack Types & Mitigation Methods" March 22, 2024. DOI: https://www.imperva.com/learn/ddos/ddos-attacks/

[15] Fang, Zhang, and Wang et al., "Security for 5G Mobile Wireless Networks" peer-reviewed journal IEEE Access, Vol. 6, pp 4850–4874, in 2017. ISSN NO. is 2169-3536. December 4, 2017, DOI: https://doi.org/10.1109/ACCESS.2017.2779140.

[16] Seongmin Park, Daeun Kim, Youngkwon Park, Hyungjin Cho, Dowon Kim, and Sungmoon Kwon et al. "5G Security Threat Assessment in Real Networks" peer-reviewed scientific journal Sensors 2021, vol. 21, Issue 16, article number 5524. ISSN NO. no. 1424-8220. August 17, 2021, pp 5524.DOI: https://doi.org/10.3390/s21165524

[17] Dolente, F., Garroppo, R. G., and Pagano, M. et al. "A vulnerability assessment of open-source implementations of fifth-generation core network functions" Journal Future Internet (MDPI), vol. 16, Issue 1, article 1, ISSN NO. no. 1999-5903. February 2, 2023, DOI: 10.3390/fi16010001.

[18] Pascale, Francesco, Ennio Andrea Adinolfi, Simone Coppola, et al. "Cybersecurity in Automotive: An Intrusion Detection System in Connected Vehicles" (2021). journal Electronics (MDPI), vol. 10, Issue 15, as article number 1765. The ISSN NO. is 2079-9292, July 23, 2021. DOI: https://doi.org/10.3390/electronics1015176.

[19] M. A. Ahmad, S. Paiva, and G. Tripathi et al. "A comprehensive review on 5G-based smart healthcare network security: Taxonomy, Issues, solutions and future research directions", Journal Array (Elsevier), vol. 18, article number 100290, in 2023. The journal's ISSN NO. is 2590-0056, July 1, 2023, DOI: 10.1016/j.array.2023.100290.

[20] Francesco Pascale, Ennio Andrea Adinolfi, Simone Coppola, and Emanuele Santonicola (2021) "Cybersecurity in Automotive: An Intrusion Detection System in Connected Vehicles," peer-reviewed journal Electronics (MDPI), vol. 10, Issue 15, article 1765 (ISSN NO. 2079-9292) July 23, 2021, DOI: 10.3390/electronics1015176,

[21] Rajasekhar Chaganti, Bharat Bhushan, and Vinayakumar Ravi. "A survey on Blockchain solutions in DDoS attacks mitigation: Techniques, open challenges and future directions" peer-reviewed journal Computer Communications (Elsevier), vol. 198, pp 68–88. Issued January 2023. ISSN NO. is 0140-3664. DOI: https://doi.org/10.1016/j.comcom.2022.10.026

[22] Aslam, M., Ye, D., Tariq, A., Asad, M., Hanif, M., Ndzi, D., Chelloug, S.A., Elaziz, M.A., Al-Qaness, M.A.A., and Jilani, S.F. et al. "Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT," journal in 2022. Sensors is an open access, peer-reviewed journal published by MDPI, ISSN NO. 1424-8220. vol. 22, Issue 7, on pp 2697. April 2022, DOI: https://doi.org/10.1016/j.comcom.2022.10.026

[23] George Amponis, Panagiotis Radoglou Grammatikis, et al. "DoS attacks: the case of blocking UAV communications" 2022 EURASIP Journal on Wireless Communications and Networking. vol. 2022, article number 124, pp 1–27. ISSN NO. 1687-1499.date: July 13, 2022, DOI: https://DOI.org/10.1186/s13638-022-02204-5.

[24] Dongfeng Fang, Yi Qian, and Rose Qingyang Huet al. "Security for 5G Mobile Wireless Networks" IEEE Access (ISSN NO.: 2169-3536), vol. 6, pp 4850–4874. The article was received on October 25, 2017, accepted on November 20, 2017, and published on December 4, 2017. DOI: https://doi.org/10.1109/ACCESS.2017.2779146

[25] Claudiu V. Kifor and Adrian Popescu. "Automotive Cybersecurity: A Survey on Frameworks, Standards, and Testing and Monitoring Technologies" peer-reviewed journal Sensors (MDPI), vol. 24, Issue 18, article number 6139, spanning pp 1–20. The article was

published on September 23, 2024. ISSN NO. is 1424-8220. DOI: https://doi.org/10.3390/s24186139

[26] Pablo Benlloch-Caballero, Qi Wang, and Jose M. Alcaraz Calero. Et al. "Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks" journal Computer Networks (ISSN NO.: 1389-1286), vol. 222, article number 109526, pp 1–19. 21 December 2022 DOI: https://doi.org/10.1016/j.comnet.2022.109526

[27] Md. Mobin Akhtar, Sultan Ali Alasmari, Sk Wasim Haidar, and Ali Abdulaziz Alzubaidi. et al. "Distributed denial of service attack detection and mitigation strategy in 5G-enabled internet of things networks with adaptive cascaded gated recurrent unit" Peer-to-Peer Networking and Applications 2025 (vol. 18, article 81, pp 1–31; ISSN NO.: 1936-6442). June 5, 2024, accepted on December 20, 2024, January 28, 2025. DOI: https://doi.org/10.1007/s12083-024-01894-6

[28] Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa et al. "An Overview on Denial-of-Service Attacks in Control Systems: Attack Models and Security Analyses" journal Entropy in 2019 (vol. 21, Issue 2, article 210, ISSN NO.: 1099-4300, pp 1–29). January 29, 2019, accepted on February 19, 2019, and published on February 22, 2019. DOI: https://doi.org/10.3390/e21020210

[29] Rathore and Park et al. "Distributed denial of service attacks and its defenses in IoT: a survey," 2020 journal The Journal of Supercomputing by Springer. ISSN NO. no.: 0920-8542) vol. 76, Issue 3, on pp 2083–2136. November 7, 2019, DOI: https://doi.org/10.1007/s11227-019-02945

[30] Kimmi Kumari and M. Mrunalini et al. "Application of machine learning algorithms for detection of distributed denial-of-service attacks" Journal of Big Data in 2022 (vol. 9, article number 56, pp 1–17; ISSN NO.: 2196-1115). March 24, 2022, DOI: https://doi.org/10.1186/s40537-022-00616-0

[31] Naeem Firdous Syed, Zubair Baig, Ahmed Ibrahim, and Craig Valli, "Denial of service attack detection through machine learning for the IoT" Journal of Information and Telecommunication in 2020 (vol. 4, Issue 4, pp 482–503; ISSN NO.: 2475-1839). June 12, 2020, DOI: https://doi.org/10.1080/24751839.2020.1767484

[32] Noman Haider, Zeeshan Baig, and Muhammad Imran, "Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, advantages, and future research trends" a magazine-type article on arXiv July 9, 2020 DOI: https://arxiv.org/abs/2007.04490

[33] Ala Mughaid et al. (2024) "Improved dropping attacks detecting system in 5G networks using machine learning and deep learning approaches", journal Multimedia Tools and Applications, ISSN NO. 1380-7501, spanning pp 1–23, on April 18, 2024. The DOI: https://doi.org/10.1007/s11042-024-18413-94.

[34] Jordan Lam and Robert Abbas et al. "Machine Learning based Anomaly Detection for 5G Networks" preprint on arXiv (arXiv:2003.03474v1) (Cryptography and Security) on March 7, 2020. DOI: https://arxiv.org/abs/2003.03474v1

[35] Alashhab, Zeyad, Mohammad Anbar, Khaled Alhmouz, and Ahmad Alhammadi. 2022. "Distributed Denial of Service Attacks against Cloud Computing Environments: A Survey." Applied Sciences, 12(23): 12441. ISSN NO. 2076-3417. December 1, 2022. DOI: https://doi.org/10.3390/app122312441

[36] Mikail Mohammed Salim, Shailendra Rathore, and Jong Hyuk Park, "Distributed denial of service attacks and its defenses in IoT: a survey" The Journal of Supercomputing in 2020 (vol. 76, pp 5320–5363;

Turnitin Originality Report

Processed on: 19-May-2025 10:07 IST
ID: 2679436419
Word Count: 6645
Submitted: 1

review.docx By Kajal Morwal

Similarity Index	Similarity by Source	
8%	Internet Sources:	5%
	Publications:	9%
	Student Papers:	2%

1% match (Amir Afaq, Noman Haider, Muhammad Zeeshan Baig, Komal S. Khan, Muhammad Imran, Imran Razzak. "Machine learning for 5G security: Architecture, recent advances, and challenges", Ad Hoc Networks, 2021)
Amir Afaq, Noman Haider, Muhammad Zeeshan Baig, Komal S. Khan, Muhammad Imran, Imran Razzak. "Machine learning for 5G security: Architecture, recent advances, and challenges", Ad Hoc Networks, 2021

1% match (Internet from 06-May-2025)
https://www.mdpi.com/2079-9292/14/3/471

1% match (Dongfeng Fang, Yi Qian, Rose Qingyang Hu. "Security for 5G Mobile Wireless Networks", IEEE Access, 2018)
Dongfeng Fang, Yi Qian, Rose Qingyang Hu. "Security for 5G Mobile Wireless Networks", IEEE Access, 2018

< 1% match (Internet from 16-Feb-2025)
https://WWW.MDPI.COM/1424-8220/24/18/6139

< 1% match ("Securing the Connected World", Springer Science and Business Media LLC, 2025)
"Securing the Connected World", Springer Science and Business Media LLC, 2025

< 1% match (student papers from 14-Apr-2024)
Submitted to King Faisal University on 2024-04-14

< 1% match (Doaa Mohsin Abd Ali Afraji, Jaime Lloret, Lourdes Peñalver. "Deep Learning-Driven Defense Strategies for Mitigating DDoS Attacks in Cloud Computing Environments", Cyber Security and Applications, 2025)
Doaa Mohsin Abd Ali Afraji, Jaime Lloret, Lourdes Peñalver. "Deep Learning-Driven Defense Strategies for Mitigating DDoS Attacks in Cloud Computing Environments", Cyber Security and Applications, 2025

< 1% match (Ruhma Sardar, Tayyaba Anees, Ahmad Sami Al-Shamayleh, Erum Mehmood, Wajeeha Khalil, Adnan Akhunzada, Fatema Sabeen Shaikh. "Challenges in detecting security threats in WoT: a systematic literature review", Artificial Intelligence Review, 2025)
Ruhma Sardar, Tayyaba Anees, Ahmad Sami Al-Shamayleh, Erum Mehmood, Wajeeha Khalil, Adnan Akhunzada, Fatema Sabeen Shaikh. "Challenges in detecting security threats in WoT: a systematic literature review", Artificial Intelligence Review, 2025

< 1% match (Internet from 12-Jul-2024)
https://dl.univ-blida.dz/jspui/bitstream/123456789/28993/1/Thesis_of_Walid__After_Annex_6.pdf

< 1% match (Internet from 12-May-2023)
https://www.arxiv-vanity.com/papers/2007.04490/

< 1% match (Internet from 13-Jan-2025)
http://www.epstem.net/en/download/article-file/4394796

< 1% match (Internet from 06-Oct-2022)
https://s23.q4cdn.com/171843108/files/doc_financials/2016/FY-2016-Annual-Report.pdf

< 1% match (Tariq Ahamed Ahanger, Imdad Ullah, Shabbab Ali Algamdi, Usman Tariq. "Machine learning-inspired intrusion detection system for IoT: Security issues and future challenges", Computers and Electrical Engineering, 2025)
Tariq Ahamed Ahanger, Imdad Ullah, Shabbab Ali Algamdi, Usman Tariq. "Machine learning-inspired intrusion detection system for IoT: Security issues and future challenges", Computers and Electrical Engineering, 2025

< 1% match (Kwitee D. Gaylah, Ravirajsinh S. Vaghela, Wend-Benedo Simeon Zongo. "A Cost Optimized Solution for Defending Against DDoS Attacks: An Analysis of a Multi-layered Architecture", SN Computer Science, 2023)
Kwitee D. Gaylah, Ravirajsinh S. Vaghela, Wend-Benedo Simeon Zongo. "A Cost Optimized Solution for Defending Against DDoS Attacks: An Analysis of a Multi-layered Architecture", SN Computer Science, 2023

< 1% match (Internet from 03-Dec-2020)
https://www.tandfonline.com/doi/full/10.1080/24751839.2020.1767484

< 1% match (Abdullah M. Alnajim, Faisal Mohammed Alotaibi, Sheroz Khan. "Detecting and Mitigating Distributed Denial of Service Attacks in Software-Defined Networking", Computers, Materials & Continua, 2025)
Abdullah M. Alnajim, Faisal Mohammed Alotaibi, Sheroz Khan. "Detecting and Mitigating Distributed Denial of Service Attacks in Software-Defined Networking", Computers, Materials & Continua, 2025

< 1% match (Internet from 29-Mar-2025)
https://journal.esrgroups.org/jes/article/download/4360/3204/7894