People's Democratic Republic of Algeria
الجمهورية الجزائرية الديمقراطية الشعبية
Ministry of Higher Education and scientific researche
وزارة التعليم العالي و البحث العلمي
National Higher School of Advanced Technologies
المدرسة الوطنية العليا للتكنولوجيات المتقدمة

**Electrical Engineering and Industrial Computing Department**

Final Year Project to Obtain the Diploma of

**Master**

- Field -

**Telecommunication**

- Specialty -

**Telecommunication Systems and Networking**

- Subject -

# A State of the Art Review on the Integration of Blockchain and Machine Learning for DDoS Detection and Mitigation in 5G Networks

Realized by

**AISSA Manel Fatima Zohra & HAOUA Rania**

Members of the Jury

| | |
|---|---|
| CHIALI Imane | Chair |
| BOUTOUTA Dalila | Examiner |
| BEGHAMI Sami | Examiner |
| BENDOUDA Djamila | Supervisor |

Algiers, **June 24th 2025**

Academic year 2024-2025

# A State of the Art Review on the Integration of Blockchain and Machine Learning for DDoS Detection and Mitigation in 5G Networks

Manel Fatima Zohra AISSA [1], Rania HAOUA [2], Djamila Bendouda[3]
[1,2] Electrical Engineering and Industrial Computing Department
[1,2,3]Nationnal Higher School of Advanced Technologies (ENSTA), Algeiers, Algeria
E-mails: (m_aissa, r_haoua, djamila.bendouda)@ensta.edu.dz

***Abstract*—With the rise of 5G networks, the surface for cyber attacks has expanded significantly, particularly in the form of Distributed Denial of Service (DDoS) attacks that threaten the availability of network services. While Machine Learning (ML) has proven effective in detecting such attacks, these models often face challenges related to trust, transparency, and centralized control. This paper proposes a hybrid approach that combines ML-based detection with Blockchain technology to enhance the security, traceability, and robustness of DDoS defense mechanisms in 5G environments. By utilizing Blockchain's decentralized and tamper proof ledger, the system ensures that the outcomes of ML-based detections are securely recorded, verifiable, and resistant to manipulation. Smart contracts further enable automated and coordinated responses to threats across distributed network nodes. Crucially, the integration of ML and Blockchain enhances traceability, allowing detected malicious sources to be rapidly shared and acted upon across the network. This not only strengthens the reliability of detection but also significantly reduces the volume of DDoS traffic circulating in the network, by enabling earlier and more accurate blocking near the source. The proposed approach highlights how this synergy can improve both detection performance and overall network resilience.**

***Index Terms*—5G Networks, Cybersecurity, DDoS Attacks, Machine Learning, Blockchain,Smart Contracts.**

## I. Introduction

In the era of hyper connectivity, fifth generation (5G) networks have emerged as the cornerstone of next generation mobile communications and digital infrastructure, delivering unprecedented ultra-fast speeds, low latency, and massive device connectivity capabilities [1]. These features enable a wide range of transformative applications, including autonomous transportation, remote healthcare, industrial automation, and real time emergency response systems. However, the increased complexity and scale of 5G architecture have significantly expanded the attack surface, rendering these networks more vulnerable to sophisticated cyber threats.

Among the most pressing threats are Distributed Denial of Service (DDoS) attacks, which exploit the high bandwidth and decentralized architecture of 5G networks to overwhelm critical network components such as network slices and core infrastructure [1] [2]. Traditional rule-based security mechanisms, commonly used in earlier generations, have become inadequate due to their limited adaptability and inability to respond effectively to dynamic and large scale attacks in real time [1].

To overcome these limitations, the integration of Machine Learning (ML) and blockchain technologies has garnered increasing attention as a promising and robust approach to 5G cybersecurity [3], [4]. ML techniques are well-suited for detecting DDoS attacks by processing vast volumes of network traffic, learning typical behavior patterns, and identifying anomalies indicative of malicious activity. Unlike static approaches, ML models can adapt to evolving threat landscapes, offering enhanced generalization and real-time responsiveness [5].

In parallel, blockchain introduces a decentralized and tamper proof ledger that strengthens trust, transparency, traceability, and accountability across distributed 5G environments. When applied to DDoS mitigation, blockchain enables secure logging of malicious events and facilitates collaborative threat intelligence sharing among network entities [2]. Its decentralized nature supports real time propagation of blacklists without dependence on a central authority. By distributing knowledge of attack sources, blockchain ensures that all network nodes can access a synchronized list of blacklist, thereby improving the system's ability to prevent ongoing and future DDoS attacks [6].

The convergence of ML and blockchain technologies creates a synergistic framework capable of autonomously detecting and mitigating DDoS attacks while preserving the integrity and trustworthiness of shared data. This integration not only enhances detection accuracy and reaction time but also ensures traceability and decentralized propagation of threat intelligence throughout the network.

This paper presents a comprehensive survey of recent advancements in the integration of machine learning and blockchain for DDoS detection and mitigation in 5G networks. It reviews a state of the art methodologies, highlights key research challenges, and discusses emerging trends. By exploring this multidisciplinary intersection, the study aims to support the development of intelligent, decentralized, and resilient cybersecurity solutions for next generation wireless systems.

The remainder of this paper is organized as follows: Section II reviews Background on 5G networks,Machine Learning and Blockchain highlighting the limitations of existing ML-based approaches. Section III presents works related to DDoS attack detection and mitigation in 5G architectures and finally Section IV describes how the combination of both machine learning and blockchain can enhance the detection and mitigation of DDoS attacks in 5G Networks. Finally, Section VI concludes the paper and outlines directions for future work.

## II. Background

### A. 5G Networks

The architecture of 5G networks introduces a cloud-native, service-oriented design aimed at delivering ultra-reliable, high-speed communication with minimal latency and support for massive device connectivity. Standardized by the 3GPP and globally adopted since 2019 [7], 5G employs technologies such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Service-Based Architecture (SBA) [8].While this architecture improves scalability and flexibility, it also expands the potential attack surface particularly for DDoS attacks which threaten the reliability and availability of network services.

It is broadly divided into three main sections: the User Equipment (UE), the Radio Access Network (RAN), and the Core Network(CN).

*1) User Equipment (UE):* User Equipment includes all devices that connect to the 5G network ranging from smartphones and tablets to IoT devices and autonomous vehicles. These devices access the network through the RAN using advanced wireless technologies like massive MIMO and beamforming [1].

*2) Radio Access Network (RAN):* The 5G Radio Access Network (RAN) connects user devices to the 5G Core via the gNodeB (gNB), the primary base station. its Key responsibilities include radio resource management, user admission control, QoS enforcement, mobility management, and network slicing support [9].

*3) 5G Core Network:* The 5G Core (5GC) is designed around a Service-Based Architecture, enabling modular network functions (NFs) to communicate via APIs. This decoupled architecture improves scalability, service agility, and automation [8].

it is illustrated in Figure 1. As shown, the 5G core serves as the central brain of the network, coordinating and managing key services and connectivity.

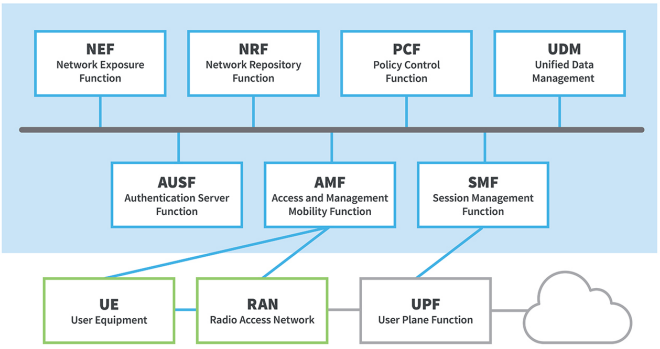


Figure 1: 5G network architecture [10].

Table I summarizes the major core functions and their respective roles.

Table I: Key 5G Core Network Functions

| **Network Function** | **Description** |
|---|---|
| Access and Mobility Management Function (AMF) | Handles device registration, mobility, and access management. Works with AUSF for user authentication [2]. |
| Session Management Function (SMF) | Manages session setup, IP address allocation, and mobility. Coordinates with PCF for QoS enforcement [2], [11]. |
| User Plane Function (UPF) | Routes and forwards user data between the 5G Core and external networks such as the internet [2]. |
| Policy Control Function (PCF) | Enforces network policies and ensures QoS across the core [2]. |
| Network Slice Selection Function (NSSF) | Chooses appropriate network slices based on user service needs [2]. |
| Authentication Server Function (AUSF) | Authenticates users in coordination with UDM [2]. |
| Unified Data Management (UDM) | Handles user subscription and authentication data [2]. |
| Network Repository Function (NRF) | Registers and enables discovery of all network functions [2]. |
| Network Exposure Function (NEF) | Exposes internal services to application functions securely [2]. |

*a) 5G Network Slicing:* 5G network slicing is one of the most transformative features introduced in the 5G networks. It enables a single physical infrastructure to be logically partitioned into multiple virtual networks, called *slices*, where each slice is tailored to serve a specific type of service, each with its own architecture, quality of service (QoS), and security mechanisms [11].

According to the 3GPP standard, 5G network slicing is typically categorized into three main types, each corresponding to a major family of use cases:

- *Enhanced Mobile Broadband (eMBB)*: For high speed data services such as video streaming and VR [11].
- *Ultra Reliable Low Latency Communications (URLLC)*: For mission critical applications like autonomous driving and remote surgery [11].
- *Massive Machine Type Communications (mMTC)*: For large scale IoT connectivity involving low power, low data rate devices [11].

### *B. DDoS Attacks in 5G Networks*

While the 5G architecture design introduces scalability and service agility, it also creates new avenues for cyber threats especially Distributed Denial of Service (DDoS) attacks. a DDoS attack is a common and disruptive cyber threat that aims to make a network or service unavailable by overwhelming it with massive amounts of traffic. this type of attacks use a large network of compromised devices often IoT-based botnets to flood the target with malicious traffic in order to exhaust its resources so it locks out legitimate users [12], [13].

*Types of DDoS Attacks:* DDoS attacks generally fall into three main categories based on the layers of the network they target:

Volumetric Attacks: These attacks aim to saturate the target's bandwidth with high volumes of traffic. Often amplified using techniques like DNS amplification, they are among the most common types of DDoS attacks. Many are powered by botnets made up of insecure IoT devices. Their scale is typically measured in bits per second (bps or Gbps) [12].

Protocol Attacks: this type of attacks target weaknesses in network protocols at the transport and network layers. Examples include SYN floods and Ping of Death attacks, which send malformed or excessive requests to exhaust system resources and cause service interruptions [12].

Application Layer Attacks: These attacks mimic legitimate user behavior to overwhelm applications (like web servers) at the top layer of the OSI model. They are harder to detect because they operate with smaller traffic volumes but focus on exploiting application logic and resource limits [12].

### *C. Machine Learning for DDoS Detection*

The increasing frequency and complexity of Distributed Denial of Service (DDoS) attacks demand the implementation of more intelligent, adaptive, and dynamic security solutions. In this context, Machine Learning (ML) has emerged as one of the most promising approaches for attack detection. Unlike traditional systems based on predefined rules or static signatures, ML algorithms can analyze large volumes of data in real-time and automatically learn both normal and abnormal system behaviors. This allows them to detect not only known attacks but also novel and evolving threats that conventional systems might miss [14].

Machine Learning (ML), a subfield of Artificial Intelligence (AI), involves the use of algorithms that learn from data—either labeled or unlabeled—to make predictions or classifications [15], [16]. These algorithms range from simple methods like linear regression to complex ensemble techniques. They are capable of identifying patterns, making decisions, and improving their performance over time and in real-world scenarios, all without the need for explicit programming [16]. Detecting Distributed Denial of Service (DDoS) attacks using machine learning involves two primary approaches: supervised and unsupervised learning. Each has distinct methodologies:

*Supervised learning :* Supervised learning is a commonly used machine learning approach for detecting Distributed Denial of Service (DDoS) attacks, where models are trained on labeled datasets that classify network traffic as either normal or malicious. These models learn to identify patterns associated with attacks based on extracted features such as packet rate, flow duration, and the number of unique IP addresses. Algorithms like Support Vector Machines (SVM) and Random Forest are frequently employed due to their high classification accuracy. While supervised learning can effectively detect known attack types and some variants, it requires large, high-quality labeled datasets which can be difficult to obtain in practiceand may suffer from overfitting or reduced performance when exposed to novel or evolving attack patterns. [14] , [16]

Random Forest is an ensemble learning method used for classification and regression that builds multiple decision trees during training, combining their predictions through majority voting (classification) or averaging (regression) as illustrate in Figure 2. Each tree is trained on a random subset of the data (bootstrap aggregating) and considers only a random subset of features at each split, enhancing diversity and reducing overfitting. This approach improves generalization, with the model's error converging to a limit as the number of trees increases, ensuring strong performance even with high-dimensional data, though this comes with reduced interpretability compared to single decision trees or linear models [17]. Random Forest mitigates the overfitting by combining diverse trees trained on randomized subsets of data and features [18]. In the field of cybersecurity, Random Forest has proven to be particularly effective for detecting attacks such as Distributed Denial of Service (DDoS) [18].

Support Vector Machine (SVM) is a prominent supervised machine learning algorithm employed for the detection of Distributed Denial of Service (DDoS) attacks in network environments. It constructs an optimal hyperplane to separate data points into distinct classes, effectively distinguishing between legitimate and malicious traffic. In the context of DDoS detection, SVM models are trained on labeled datasets to learn and recognize traffic patterns, enabling accurate identification of anomalous

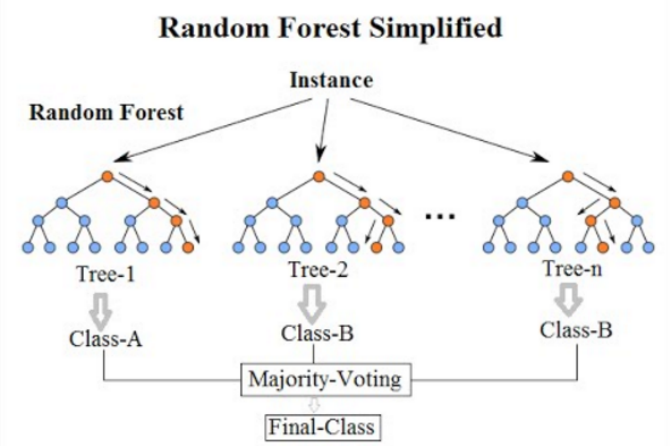


Figure 2: Random Forest Model Architecture [19].

behavior indicative of an attack. Owing to its strong capability in managing high-dimensional data and its proven effectiveness in binary classification, SVM is regarded as a dependable and efficient method for mitigating DDoS threats, particularly within the complex infrastructure of 5G networks [20]. The algorithm's ability to maximize the margin between classes ensures robust generalization to unseen data, while kernel functions extend its power to handle non-linear separations—making it suitable for the dynamic and diverse nature of 5G traffic [21] .

*Unsupervised learning:* Unsupervised learning works a bit differently from supervised methods—it doesn't need any labeled data to function. Instead, it looks for patterns or unusual behavior in the traffic on its own. This makes it especially useful for spotting brand-new or unexpected DDoS attacks that haven't been seen before. Since it doesn't rely on past examples, it's great in situations where we don't have labeled datasets. These methods can sometimes raise too many false alarms, and figuring out what the algorithm has actually found isn't always straightforward—it often needs a human expert to make sense of the results [14], [16].

### *D. Deep Learning for DDoS Detection*

Deep Learning (DL), a branch of ML, is based on multilayer artificial neural networks (ANNs), inspired by biological neurons [22]. A neural network consists of an input layer, one or more hidden layers, and an output layer, with each layer made up of interconnected neurons. The input layer processes raw data where each neuron corresponds to a feature. Hidden layers perform complex transformations, and the output layer generates predictions, such as classification labels or continuous values. Each neuron combines its inputs using weights, applies an activation function, and produces an output. If this output exceeds a threshold, the neuron activates and passes information to the next layer; otherwise, no signals transmitted [23]. Various neural network architectures have been designed to suit different data types and application requirements.

*1) The Convolutional Neural Network (CNN):* The Convolutional Neural Network (CNN) is one of the most prominent architectures in the field of deep learning [24]. CNNs have shown remarkable effectiveness in a variety of domains, including image reconstruction [25] and natural language processing [26]. In recent years, CNNs have also gained increasing attention in the field of cybersecurity [27], particularly for critical applications such as Distributed Denial of Service (DDoS) attack detection [14], [28], By leveraging components such as convolutional, pooling, and fully connected layers As depicted in Figure 3 , CNNs can automatically learn spatial feature hierarchies. These powerful pattern recognition capabilities make CNNs especially suitable for analyzing complex datasets, including traffic in 5G networks [29].

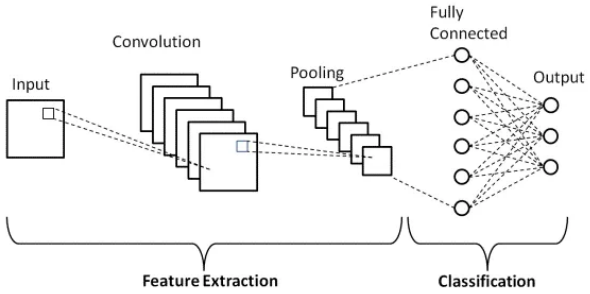


Figure 3: CNN Model Architecture [30]

Convolutional layers in a CNN use trainable filters to extract local patterns like edges and textures from the input data, producing feature maps that are then passed through non-linear activation functions, typically ReLU, to capture complex representations [31]. These layers benefit from sparse connectivity and shared weights, reducing computational cost and memory usage [32]. Pooling layers follow to downsample feature maps, preserving key information while minimizing parameters commonly using max or average pooling [32]. Finally, fully connected layers aggregate these features and generate predictions, ending with a SoftMax layer for classification tasks [31].

*2) Bidirectional Long Short-Term Memory (BiLSTM):* Bidirectional Long Short-Term Memory (BiLSTM) networks are an advanced extension of traditional LSTM models, designed to capture both past and future context in sequential data. While standard LSTM networks process information in a single direction from past to future BiLSTMs incorporate an additional LSTM layer that reads the input sequence in reverse. This dual-processing mechanism enables the network to have a more comprehensive understanding of the entire sequence, which is especially valuable in tasks where context on both sides of a token is essential, such as in speech recognition, sentiment analysis, or named entity recognition [33], [34]. BiLSTM has been successfully applied in the detection of cyberattacks, including DDoS attacks, intrusions, and anomalous traffic behavior in networks [35]. BiLSTM

network comprises two parallel LSTM layers—one As depicted in Figure 4, processing the input sequence forward and the other in reverse. At each time step, their outputs are combined, creating a richer representation that captures both past and future context. Each LSTM unit includes input, forget, and output gates that control the flow of information, helping retain important data over time and addressing issues like vanishing gradients [36]. This bidirectional structure makes BiLSTMs particularly effective for sequence-based tasks, and performance can be further enhanced by adding a CRF layer for structured prediction [37].

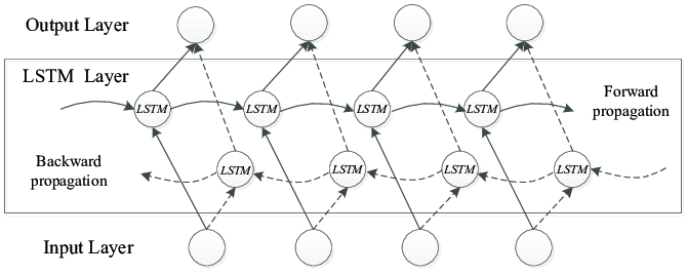


Figure 4: BiLSTM Model Architecture [38]

### *E. Blockchain Technology*

Blockchain is a decentralized and distributed ledger technology that securely records transactions across multiple network nodes as shown in figure5. Originally introduced for cryptocurrencies, its core principles, immutability, transparency, and decentralized trust make it highly suitable for a wide range of applications, including security in next generation networks. Data stored on a blockchain is grouped into blocks, cryptographically linked, and validated by consensus among participating nodes, ensuring resistance to tampering and unauthorized modifications [39].

The main features of blockchain are:

- Decentralization: Blockchain operates across a network of distributed nodes, each maintaining a synchronized copy of the ledger. This peer to peer structure removes the need for a central authority by distributing trust and control among all participants. If someone attempts to alter data on one node, the rest of the network can detect and reject the change, ensuring data integrity. This redundancy makes the system more resilient and tamper resistant [39].
- Immutability: Once a transaction is verified and added to the blockchain, it becomes permanent and cannot be altered or deleted. This is made possible by cryptographic hash functions that link each block to the previous one, creating a secure chain of records. Any attempt to change data in a past block would break the chain and be immediately rejected by the network. This property ensures that all recorded actions are irreversible and non repudiable, making blockchain a reliable source of truth [40].
- Transparency: In blockchain systems, every participant (node) has access to a shared copy of the ledger, which is continuously updated and verified. This means transactions can be viewed and traced in real time using blockchain explorers, ensuring full visibility across the network. Although data on the blockchain is encrypted and users can remain pseudonymous, the transaction history itself is completely transparent making it possible to trace the movement of assets while preserving user privacy [39].
- Security: Blockchain ensures data security through strong cryptographic algorithms and a structure that links each block to the previous one using hashes. Once a block is added to the chain, altering any data within it would change its hash breaking the connection with subsequent blocks. Since every node on the network maintains a copy of the chain, any tampered version would be rejected by the others due to mismatched hashes. This makes it nearly impossible to alter past records on large, well-distributed networks, providing a high level of integrity and protection against tampering [39].

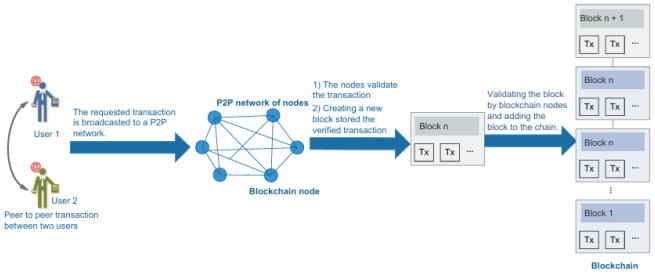


Figure 5: Illustration of the blockchain transaction process [40].

*1) Blockchain Architecture:* The architecture of a blockchain system is typically composed of several interconnected layers, each playing a crucial role in ensuring the functionality, security, and scalability of the network:

- Data Layer: This foundational layer stores all transaction-related data within blocks. It includes block headers, timestamps, cryptographic hashes, and Merkle trees to guarantee data integrity and verifiability [41].
- Network Layer: Responsible for peer-to-peer (P2P) communication among nodes. It manages transaction propagation, block dissemination, and node discovery across the decentralized network [41].
- Consensus Layer: Ensures all network participants agree on the current state of the blockchain. It employs various consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), or Byzantine

Fault Tolerance (BFT) to maintain consistency and prevent malicious activity [41].

- Incentive Layer: This layer introduces economic mechanisms to reward honest behavior and penalize malicious actions. Participants, such as miners or validators, are compensated with tokens or cryptocurrency for contributing computing power or validating transactions.
- Contract Layer: Also known as the smart contract layer, it enables the deployment and execution of programmable logic. This supports automation of transactions and rules-based operations within decentralized applications [41].
- Application Layer: The topmost layer that interacts with end users and external systems. It provides interfaces for real-world applications including supply chain management, identity verification, and e-voting [41].

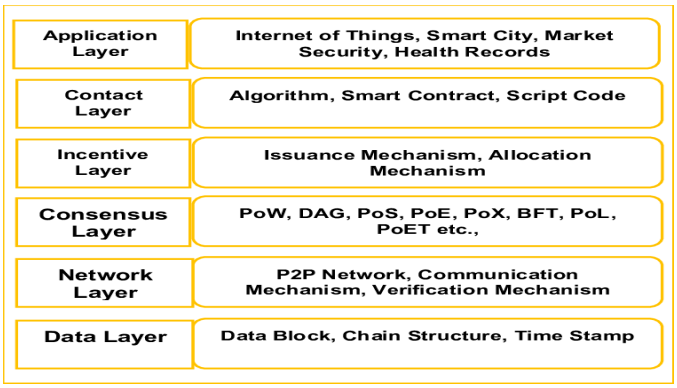


Figure 6: Layeres of blockchain systems [41].

*2) Blockchain Taxonomy:* Blockchain can be classified into three main types:

- Public Blockchain: Also known as permissionless blockchain where anyone can join, participate, and interact without needing approval [42]. every participant in this kind of blockchains has the ability to send and receive transactions, take part in the consensus process, and maintain a full copy of the distributed ledger [43].
  To add new blocks to the chain, participants usually have to either solve complex computational puzzles (as in Proof of Work) or stake their own cryptocurrency (as in Proof of Stake). These mechanisms help secure the network by making it extremely difficult and costly to alter any data. As a result, public blockchains are generally considered secure and tamper-resistant [44].
  Well-known examples of public blockchains include Bitcoin, Ethereum, and Litecoin [40].
- Private Blockchain: A private or a permissioned blockchain, operates under the control of a specific organization or group. Only authorized participants can join the network, and access is typically granted through invitations or approvals from existing members [42].
- Consortium Blockchain: A consortium blockchain, also called a federated blockchain, is a permissioned system managed by a group of trusted entities rather than a single organization. In this type of blockchain, only selected nodes are granted the authority to participate in the consensus process and verify transactions. Access to data can also be restricted to specific participants, offering a higher level of privacy compared to public blockchains [40].

## III. Related work

This section reviews recent works on using machine learning to detect and stop DDoS attacks, and how blockchain can improve the security and reliability of those systems. It highlights how combining both technologies can lead to smarter and more trusted solutions for protecting 5G networks.

Manikumar and Maheswari [3] proposed a hybrid system that combines machine learning and blockchain to detect and mitigate DDoS attacks. They used models like KNN, Decision Tree, and Random Forest to classify malicious traffic, with Random Forest achieving the best accuracy. Detected malicious IPs are stored on the Ethereum blockchain using smart contracts, ensuring they can't be altered. This decentralized and automated approach adds transparency and improves the trustworthiness of DDoS defense systems.

Agrawal et al [45] explore the integration of blockchain and artificial intelligence to enhance the performance and reliability of 5G-enabled IoT systems, which are often challenged by data congestion, privacy concerns, and limited processing efficiency. To address these issues, the authors propose a lightweight consensus mechanism (Raft), a high-speed blockchain distribution network (bloXroute) to improve data propagation, and the use of Hyperledger Fabric as a permissioned blockchain.

In another notable work, the authors in [46] proposed a collaborative system that combines machine learning with blockchain smart contracts to detect and mitigate DDoS attacks. Their architecture allows different autonomous systems and clients to share blacklisted IP addresses on a public blockchain, using Ethereum-based smart contracts to automate response actions. The system enables real-time detection through ML analysis of traffic patterns and ensures that mitigation decisions are stored in a tamper-proof and decentralized manner. Compared to traditional centralized methods, this approach enhances scalability, transparency, and cross-domain cooperation while preserving the privacy of contributors.

Liu et al. [40]provide a thorough survey on the integration of blockchain and machine learning to enhance the security, intelligence, and efficiency of modern communication networks. The paper highlights how blockchain

supports machine learning by enabling secure, decentralized data sharing and transparent decision-making, while ML strengthens blockchain through anomaly detection, resource optimization, and smarter contract execution. It also explores real-world use cases across 5G, IoT, and edge computing, and outlines key challenges such as scalability, privacy, and interoperability. This work offers a strong foundation for understanding the complementary roles of blockchain and ML in building more secure and autonomous network systems.

Fang et al. [47] proposed a blockchain-AI hybrid defense against DDoS attacks in 5G networks. Their framework hides protected servers within the blockchain, forcing all traffic through verified nodes. An AI module in smart contracts analyzes traffic in real time, assigning a confidence score—higher scores (indicating suspicious activity) trigger increased transaction fees (Gas), raising attack costs. To ensure trust, the AI is trained on-chain using secure methods like YODA and MIRACLE, preventing tampering.

Manikumar et al. [48] proposed a federated learning-based DDoS detection framework integrated with blockchain to enhance network resilience. Their approach enables distributed model training across nodes while preserving data privacy. To address potential poisoning by malicious nodes, they introduce a dynamic reputation-based miner selection mechanism and store the trained model on-chain for integrity. Experiments using Random Forest, Multilayer Perceptron, and Logistic Regression achieved up to 99.1 % accuracy, demonstrating superior performance over traditional centralized detection methods.

Ahmad Al'aziz et al. [6] proposed a blockchain-based blacklisted IP distribution system to enhance DDoS mitigation in Snort IPS. Their framework leverages Ethereum smart contracts to share malicious IP addresses across distributed IPS nodes, enabling collaborative attack blocking closer to the source. By deploying a private blockchain with a Proof-of-Authority (PoA) consensus, the system ensures tamper-proof IP blacklisting while minimizing latency. Experimental results demonstrated a 76% reduction in attack traffic (from 115,578 to 27,165 packets) by allowing edge IPS nodes to proactively block threats using shared intelligence. The study highlights blockchain's potential to decentralize threat intelligence, though it notes a 3–7 second delay for IP propagation. Future work includes testing public blockchains and diverse DDoS attack vectors.

Tayyab et al. [49] propose a decentralized approach in which each IDS functions as a node within a blockchain network. These IDS nodes collaborate by exchanging correlated alarm data to enhance the detection of ICMPv6-based DDoS attacks. While this distributed sharing of threat intelligence can improve detection performance, the practical deployment faces challenges. For instance, integrating blockchain compatibility across heterogeneous IDS vendors in enterprise environments may be difficult. Additionally, identifying DDoS attacks at the IDS level may occur too late in the attack lifecycle, by which point edge or content delivery network (CDN) resources could already be saturated.

## IV. Blockchain for Distributed Blacklist

In 5G networks, DDoS attacks pose a critical threat due to the increased connectivity and low-latency requirements of the infrastructure. Various detection mechanisms, including machine learning-based approaches, have been developed to identify such attacks. Once malicious activity is detected, the initial step involves identifying the source associated with the abnormal traffic pattern [3]. However, due to the dynamic IP allocation and the user-centric nature of 5G networks [50], IP-level identification alone is insufficient. The subsequent step consists of identifying the malicious source using unique user identifiers, such as the International Mobile Subscriber Identity (IMSI). These identifiers enable the network to accurately associate suspicious behavior with specific users or devices [51].

Traditionally, each Intrusion Detection System (IDS) maintains its own local mapping and blacklist, which can lead to fragmented threat intelligence and inconsistent responses across network functions. This highlights the need for a unified, distributed mechanism to ensure coherent and effective identification of malicious actors throughout the 5G architecture. To address this limitation, a distributed solution is required to ensure synchronization and consistency of blacklist across all IDS instances. Figure 7 illustrates the proposed architecture that combines machine learning-based DDoS detection with a blockchain-enabled distributed blacklist system.

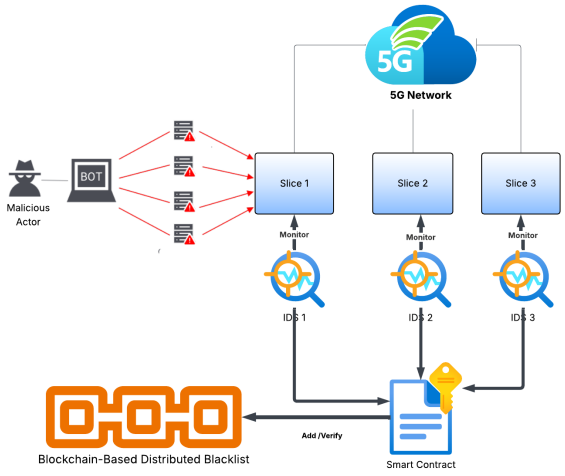


Figure 7: Architecture of a Blockchain-Enabled and ML-Based DDoS Detection System in 5G Networks.

### A. Benefits of Blockchain Integration

Integrating blockchain technology into DDoS defense systems offers two principal advantages that enhance the

effectiveness and responsiveness of network protection mechanisms:

- **Traceability:** Every interaction within the network, including malicious activities, is recorded immutably on the blockchain. This ensures a transparent and verifiable audit trail, enabling the accurate identification and accountability of attack sources.
- **Preemptive Attack Mitigation:** Blockchain enables real time propagation of verified threat intelligence across all IDS nodes. Once a malicious source is detected and blacklisted at any point in the network, the information is immediately synchronized, allowing other nodes to proactively block the threat before the attack traffic reaches them. This collective defense significantly reduces the impact, spread, and recurrence of DDoS attacks [52], [53].
- **Tamper Resistance**: Once a malicious source is blacklisted, the corresponding entry is recorded immutably on the distributed ledger, ensuring integrity and verifiability by all nodes [54].

This decentralized sharing of verified threat intelligence enables each detection node to contribute to and benefit from a collective and proactive defense strategy, ensuring traceability of malicious activity across the network. In addition to reducing response time but also limits attack propagation by enabling early identification and blocking of threats.

### *B. Smart Contracts for Autonomous Blacklist Management*

Smart contracts are self-executing programs deployed on blockchain platforms such as Ethereum. They autonomously enforce predefined rules and access control policies without relying on centralized authority. In the context of 5G network security, smart contracts significantly enhance the efficiency and integrity of distributed blacklist management by enabling secure, automated responses to DDoS threats.

Upon detection of a potential DDoS source, IDS generates a validated alert, which is forwarded to a smart contract. The contract then autonomously updates the blacklist on the blockchain in a tamper-proof and transparent manner. The smart contract is responsible for the following core functions:

- **Addition of malicious sources:** Upon receiving alerts from machine learning-based Intrusion Detection Systems (IDS), the identified malicious source is added to the blacklist along with metadata such as the timestamp and the unique identifier of the reporting IDS. This allows for traceability and trust in the source of the alert.
- **Verification and enforcement:** During access control decisions, the contract verifies the presence of the source in the blacklist and checks the time elapsed since the alert was issued. If the elapsed time is below a predefined threshold, and the IDS identifier is recognized as trustworthy, the source is temporarily denied access to the network. This ensures timely mitigation while avoiding permanent exclusion in cases of false positives or spoofed behavior.

By automating these tasks, smart contracts ensure that only authorized and trusted entities can modify the blacklist, preserving its integrity, transparency, and operational reliability [3].

Given the stringent performance requirements of 5G networks, permissioned blockchains are more suitable than public alternatives. While public platforms such as Ethereum offer open participation and full transparency, they typically involve higher latency, greater energy consumption, and reduced control over participant behavior. In contrast, permissioned blockchains limit participation to verified nodes and offer several advantages:

- Reduced latency through efficient consensus mechanisms .
- Improved scalability to support real-time and high-volume traffic.
- Enhanced regulatory compliance via identity management and traceability.

These characteristics make permissioned blockchain platforms highly suitable for deploying smart contract-based blacklist management systems within 5G infrastructures [4].

## V. Conclusion

The evolution of 5G networks has introduced unprecedented performance capabilities, including low latency, high throughput, and flexible network slicing to support diverse use cases. However, this complexity also increases the attack surface, making 5G infrastructures particularly vulnerable to sophisticated cyber threats such as Distributed Denial of Service (DDoS) attacks. Traditional defense mechanisms often fall short due to limitations in scalability, centralized control, and delayed response.

To address these challenges, this article explored a hybrid approach that combines Machine Learning (ML) and Blockchain technologies for enhanced DDoS mitigation. ML enables intelligent detection of anomalies in network traffic, while Blockchain introduces a decentralized, tamper proof ledger to ensure trusted information sharing across network nodes. The integration of Smart Contracts further automates and synchronizes the response process, allowing detected threats to be quickly shared and blocked across multiple Intrusion Detection Systems (IDS).

Notably, the traceability enabled by Blockchain plays a crucial role in mitigating DDoS traffic across the network. By distributing blacklist entries in real time, malicious entities can be identified and filtered closer to their origin, thereby preventing disruptive traffic from reaching and overwhelming critical infrastructure layers. This synergy between machine learning and Blockchain technologies provides a robust, scalable, and trustworthy solution for

protecting 5G network slices and maintaining service availability

Future research could explore adapting this architecture to public blockchain environments, incorporating additional attack types, and enhancing smart contract logic for more dynamic policy enforcement.

## References


[1] C. Wireless. (2023) Architectural advancements in 5g technology. Accessed: 2025-04-24. [Online]. Available: https://www.cavliwireless.com/blog/not-mini/architectural-advancements-in-5g-technology

[2] S. Park, B. Cho, D. Kim, and I. You, "Machine learning based signaling ddos detection system for 5g stand alone core network," *Applied Sciences*, vol. 12, no. 23, p. 12456, 2022, accessed: 2025-04-24.

[3] D. V. V. S. Manikumar and B. U. Maheswari, "Blockchain based ddos mitigation using machine learning techniques," in *Proceedings of the 2nd International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2020, pp. 906–911, accessed: 2025-04-24.

[4] M. J. C. S. Reis, "Blockchain-enhanced security for 5g edge computing in iot," *Computation*, vol. 13, no. 4, p. 98, 2025, accessed: 2025-06-6.

[5] R. A. Bakar *et al.*, "5gdad: A deep learning approach for ddos attack detection in 5g p4-based upf," in *Proceedings of the 2024 IEEE 25th International Conference on High Performance Switching and Routing (HPSR)*, Pisa, Italy, 2024, pp. 1–6.

[6] B. A. A. Al'aziz, P. Sukarno, and A. A. Wardana, "Blacklisted ip distribution system to handle ddos attacks on ips snort based on blockchain," in *2020 6th Information Technology International Seminar (ITIS)*, Surabaya, Indonesia, 2020.

[7] 3GPP, "System architecture for the 5g system (release 15)," 3GPP, Technical Specification TS 23.501, 2018.

[8] C. Inc. (2023) 5g service-based architecture (sba) explained. [Online]. Available: https://www.calsoftinc.com/blogs/5g-service-based-architecture-sba.html

[9] A. I. Grohmann, M. Seidel, S. A. W. Itting, R.-G. Cheng, M. Reisslein, and F. H. P. Fitzek, "Multi-ue 5g ran measurements: A gamut of architectural options," *IEEE Access*, vol. 13, 2025, accessed: 2025-04-24.

[10] D. International. (2023) What is 5g network architecture? [Online]. Available: https://www.digi.com/blog/post/5g-network-architecture

[11] M. S. Khan, "Detection of dos and ddos attacks on 5g network slices using deep learning approach," Master's thesis, University of Regina, Regina, Saskatchewan, 2023, accessed: 2025-04-24.

[12] Cloudflare. (2023) What is a ddos attack? [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[13] Y. Huang, Y. Bai, J. Zhang, Y. Li, and Y. Feng, "Trend analysis and countermeasure research of ddos attack under 5g network," *IEEE Access*, vol. 9, pp. 137 587–137 600, 2021, accessed: 2025-04-16.

[14] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. M. del Rincón, and D. Siracusa, "Lucid: A practical, lightweight deep learning solution for ddos attack detection," in *Proceedings of the 6th IEEE Conference on Network Softwarization (NetSoft)*, 2020, pp. 876–889.

[15] IBM. Machine learning. [Online]. Available: https://www.ibm.com/think/topics/machine-learning

[16] T. M. Mitchell, *Machine Learning*. New York: McGraw-Hill, 1997, online: https://www.cs.cmu.edu/~tom/files/MachineLearningTomMitchell.pdf.

[17] L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001, accessed: 2025-04-16.

[18] B. S. Reddy, "Advancing ddos detection in 5g networks through machine learning and deep learning techniques," Master's thesis, Blekinge Institute of Technology, Karlskrona, Sweden, 2024.

[19] W. Koehrsen. Random forest: Simple explanation. [Online]. Available: https://williamkoehrsen.medium.com/random-forest-simple-explanation-377895a60d2d

[20] S. Y. Alshunaifi, S. Mishra, and M. Alshehri, "Cyber-attack detection and mitigation using svm for 5g network," *Intelligent Automation & Soft Computing*, vol. 31, no. 1, pp. 275–288, 2022, accessed: 2025-04-24.

[21] IBM. What is a support vector machine (svm)? [Online]. Available: https://www.ibm.com/think/topics/support-vector-machine

[22] M. M. Noel, S. Bharadwaj, V. Muthiah-Nakarajan, P. Dutta, and G. B. D. Amali, "Biologically inspired oscillating activation functions can bridge the performance gap between biological and artificial neurons," *Expert Systems with Applications*, vol. 266, p. 126036, 2025.

[23] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016, online: http://www.deeplearningbook.org.

[24] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," *Communications of the ACM*, vol. 60, no. 6, pp. 84–90, 2017, accessed: 2025-04-16.

[25] C. Zeng, Z. Wang, and Z. Wang, "Image reconstruction of iot based on parallel cnn," in *Proceedings of the 2020 International Conference on Internet of Things (iThings)*, 2020, accessed: 2025-04-16.

[26] K. S. Varshitha, C. G. Kumari, M. Hasvitha, S. Fiza, A. K., and V. Rachapudi, "Natural language processing using convolutional neural network," in *Proceedings of the 2023 7th International Conference on Computing Methodologies and Communication (ICCMC)*, 2023, accessed: 2025-04-16.

[27] R. Alguliyev and R. Shikhaliyev, "Computer networks cybersecurity monitoring based on cnn-lstm model," in *Proceedings of the 2024 IEEE 18th International Conference on Application of Information and Communication Technologies (AICT)*, 2024, accessed: 2025-04-16.

[28] R. A. Bakar, F. Alhamed, P. Castoldi, A. Sgambelluri, J. J. V. Olmos, F. Cugini, and F. Paolucci, "5gdad: A deep learning approach for ddos attack detection in 5g p4-based upf," in *2024 IEEE 25th International Conference on High Performance Switching and Routing (HPSR)*, 2024.

[29] Z. Gao, "5g traffic prediction based on deep learning," *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–5, 2022, [Online]. Available: https://www.hindawi.com/journals/cin/2022/3174530/.

[30] U. Blog. Basic cnn architecture. [Online]. Available: https://www.upgrad.com/blog/basic-cnn-architecture/

[31] M. M. Taye, "Understanding of machine learning with deep learning: Architectures, workflow, applications and future directions," *Computers*, vol. 12, no. 6, p. 91, 2023.

[32] L. Alzubaidi *et al.*, "Review of deep learning: Concepts, cnn architectures, challenges, applications, future directions," *Journal of Big Data*, vol. 8, no. 1, pp. 1–74, 2021.

[33] M. Schuster and K. K. Paliwal, "Bidirectional recurrent neural networks," *IEEE Transactions on Signal Processing*, vol. 45, no. 11, pp. 2673–2681, 1997.

[34] A. Graves, *Supervised Sequence Labelling with Recurrent Neural Networks*. Springer, 2012.

[35] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in *2016 International Conference on Platform Technology and Service (PlatCon)*, 2016, pp. 1–5, accessed: 2025-04-16.

[36] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997, accessed: 2025-04-16.

[37] Z. Huang, W. Xu, and K. Yu, "Bidirectional lstm-crf models for sequence tagging," *arXiv preprint arXiv:1508.01991*, 2015, accessed: 2025-04-16.

[38] ResearchGate. Bat: Deep learning methods on network intrusion detection using nsl-kdd dataset - scientific figure. BLSTM-model_fig2_339174926, [Online]. [Accessed: Apr. 18, 2025].

[39] J. Kagan. (2023) Blockchain. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp

[40] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Blockchain and machine learning for communications and networking systems," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1392–1431, 2020, accessed: 2025-04-24.

[41] M. N. M. Bhutta *et al.*, "A survey on blockchain technology: Evolution, architecture and security," *IEEE Access*, vol. 9, pp. 61 044–61 080, 2021, accessed: 2025-04-25.
[42] W. Cai *et al.*, "Decentralized applications: The blockchain-empowered software system," *IEEE Access*, vol. 6, pp. 53 019–53 033, 2018.
[43] J. Xie *et al.*, "A survey on blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019, 3rd Quart.
[44] M. S. Ali *et al.*, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019, 2nd Quart.
[45] S. Agrawal *et al.*, "Blockchain and ai for 5g-enabled iot: Challenges, opportunities and solutions," *New Journal of Chemistry*, vol. 47, no. 9, pp. 3367–3381, 2023, accessed: 2025-04-24.
[46] N. Abdelaziz *et al.*, "Detect and mitigate blockchain-based ddos attacks using machine learning and smart contracts," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 13, no. 6, pp. 404–413, 2022, accessed: 2025-04-24.
[47] L. Fang *et al.*, "Countermeasure based on smart contracts and ai against dos/ddos attack in 5g circumstances," *IEEE Network*, vol. 34, no. 6, pp. 54–61, 2020, nov./Dec. 2020, Accessed: 2025-04-24.
[48] D. Saveetha *et al.*, "An integrated federated machine learning and blockchain framework with optimal miner selection for reliable ddos attack detection," *IEEE Access*, 2024, published: Jun. 12, 2024, current version: Sep. 19, 2024, Accessed: 2025-04-24.
[49] M. Tayyab, B. Belaton, and M. Anbar, "Icmpv6-based dos and ddos attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review," *IEEE Access*, vol. 8, pp. 170 529–170 547, 2020, accessed: 2025-04-24.
[50] N. A. Tuan *et al.*, "Caching and containerization of ip address allocation process in 5g core networks for performance improvements," in *Proceedings of the 17th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, 2023, pp. 1–8.
[51] H. Wen *et al.*, "5g-spector: An o-ran compliant layer-3 cellular attack detection service," in *Proceedings of the 30th ACM Conference on Computer and Communications Security (CCS)*, Copenhagen, Denmark, 2023, pp. 3217–3229.
[52] J. Burger, S. Rafati, and T. Bocek, "Collaborative ddos mitigation based on blockchains," Master's thesis, University of Zurich, Zurich, Switzerland, 2017.
[53] Z. Shah *et al.*, "Blockchain based solutions to mitigate distributed denial of service (ddos) attacks in the internet of things (iot): A survey," *Sensors*, vol. 22, no. 3, p. 1094, 2022, accessed: 2025-06-10.
[54] R. Gupta, *Hands-On Cybersecurity with Blockchain*. Birmingham: Packt Publishing, 2018.