Dissertation/Report submitted to the

UNIVERSITY OF MOHAMED BOUDIAF - M'SILA, ALGERIA

FACULTY OF COMPUTER SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

in partial fulfillment of the requirements for the degree of

Master in Computer Science

Specialization: Computer Science

Option: Networks and Information and Communication Technologies

Presented by

BEN AZI Wafa
HASNAOUI Cheyma

Entitled

DDoS Attack Detection using Artificial Intelligence

Under the supervision of

Pr. Lamri Sayad

Jury Members

Prof. First Name Last Name	University of M'sila	President
Pr. Lamri Sayad	University of M'sila	Supervisor
Dr. First Name Last Name	University of M'sila	Examiner

June, 2026

الملخص

أصبحت الهجمات الإلكترونية، وخاصة هجمات حجب الخدمة الموزعة ،(DDoS) تشكل تهديداً متزايداً لاستقرار البنى التحتية للشبكات والخوادم والخدمات الرقمية. تهدف هذه الهجمات إلى استنزاف موارد النظام وإغراقه بحركة مرور كثيفة، مما يؤدي إلى تعطيل الخدمات ومنع المستخدمين الشرعيين من الوصول إليها. كما أن اعتماد أنظمة الكشف التقليدية على التوقيعات أو العتبات الثابتة يجعلها أقل قدرة على مواكبة الهجمات الحديثة والمتطورة.

يهدف هذا العمل إلى تصميم وتنفيذ نظام كشف آني يعتمد على تقنيات تعلم الآلة للكشف عن هجمات حجب الخدمة الموزعة. يتكون النظام المقترح من أربعة مكونات رئيسية: (1) وحدة لالتقاط الحزم وتحليل حركة الشبكة باستخدام مكتبة ،Scapy (2) محرك لاستخراج خصائص تدفقات الشبكة الإحصائية، (3) مصنف يعتمد على خوارزمية Random Forest لتمييز الحركة الطبيعية عن الهجومية، و(4) آلية هجينة تجمع بين المراقبة المرجعية **Baseline Monitoring**، وتحليل الإنتروبيا **Analysis Entropy**، ومنطق الطوارئ **Logic Emergency** لتحسين موثوقية الكشف. كما تم تطوير لوحة تحكم تفاعلية باستخدام Streamlit لعرض النتائج والتنبيهات في الزمن الحقيقي.

تم تقييم النظام باستخدام مجموعة بيانات CIC-DDoS2019 بالإضافة إلى سيناريوهات محاكاة في بيئة معزولة. أظهرت النتائج التجريبية أن النظام حقق دقة تصنيف بلغت 97.99% مع سرعة استجابة تقارب 5 ميلي ثانية لكل نافذة تحليل، مما يجعله مناسباً للكشف الآني وقابلاً للتكامل مع أنظمة كشف ومنع الاختراق .(IDS/IPS)
الكلمات المفتاحية: هجمات حجب الخدمة الموزعة ،(DDoS) تعلم الآلة، **Forest Random**، الكشف الآني، تحليل حركة الشبكة، الأمن السيبراني.

Abstract

Distributed Denial of Service (DDoS) attacks have become one of the most critical threats to the availability of modern network infrastructures and online services. These attacks aim to overwhelm system resources with massive volumes of malicious traffic, causing service disruption and preventing legitimate users from accessing network resources. Traditional detection approaches based on signature matching or static thresholds often struggle to detect modern and evolving DDoS attacks due to their limited adaptability.

This work presents the design and implementation of a real-time Machine Learning-based DDoS detection system. The proposed architecture consists of four main components: (1) a packet capture and traffic monitoring module using the Scapy library, (2) a statistical network flow feature extraction engine, (3) a Random Forest classifier for distinguishing between benign and malicious traffic, and (4) a hybrid detection mechanism combining Baseline Monitoring, Entropy Analysis, and Emergency Logic to improve detection reliability. An interactive Streamlit dashboard was also developed to provide real-time visualization, monitoring, and intelligent alert generation.

The proposed system was evaluated using the CIC-DDoS2019 dataset together with controlled attack simulations in an isolated environment. Experimental results achieved a classification accuracy of **97.99%** with an average inference latency of approximately 5 milliseconds per analysis window. These results demonstrate that DDoSentinel provides an efficient, lightweight, and scalable solution suitable for real-time DDoS detection and integration with modern Intrusion Detection and Prevention Systems (IDS/IPS).
Keywords: Distributed Denial of Service (DDoS), Machine Learning, Random Forest, Real-Time Detection, Network Traffic Analysis, Cybersecurity.

Dedication

To my mother,
the source of love, tenderness, and endless prayers.
Your tears and sacrifices will forever be my greatest motivation.

To my father,
my role model and backbone.
Your hard work, wisdom, and guidance have shaped who I am today.

To my brothers,
my protectors and supporters.
Thank you for always having my back.

To my sisters,
my first friends and lifelong companions.
Thank you for your patience, encouragement, and love.

To all my family,
this achievement belongs to you as much as it belongs to me.

Ben Azi Wafa

Dedication

To my mother…
The first home I ever knew, and the first love I ever felt.
Thank you for being my strength, my comfort, and my peace through every difficult moment.
Your patience, prayers, and endless love carried me farther than words can express.
You were always my safe place and my greatest support.
I dedicate my success and joy to you.

To my dear father…
Thank you for being my strength, my support, and the safe place I could always lean on.
Thank you for every sacrifice you made so I could reach this moment.

To my beloved sisters…
Thank you for being the beautiful part of my days and for making every difficult moment feel lighter.

And finally… to myself,
To the version of me that struggled silently, felt afraid, yet never gave up…
I am proud of you. You finally made it.

Hasnaoui Cheyma

Acknowledgements

First and foremost, we thank **Almighty Allah** for granting us the strength, patience, and knowledge to complete this work.

We are deeply indebted to our thesis supervisor **Pr. Lamri Sayad** whose steadfast support and inspiration made this project a success. In a very special way, we thank him for his continuous guidance, valuable feedback, and encouragement throughout this challenging study.

We also extend our sincere gratitude to the jury members for their time, valuable insights, and constructive evaluation of this work.

Special thanks go to our families and friends who endured the hectic moments and supported us during the course of this research. Their patience and encouragement have been our greatest motivation.

Contents

List of Tables

List of Figures

Part I: Thesis

General Introduction

The field of network security has significantly evolved in recent years, becoming a fundamental component for protecting modern digital infrastructures. With the continuous growth of internet traffic and the increasing sophistication of cyber threats, ensuring reliable and real-time protection has become a major challenge. Among these threats, Distributed Denial of Service (DDoS) attacks remain one of the most disruptive, as they aim to exhaust network resources and cause service unavailability, leading to serious financial and operational impacts. Recent industry reports indicate that DDoS attack volume has increased by **121% year-over-year in 2025**, with the largest recorded attack reaching **31.4 Tbps** [1].

Traditional Intrusion Detection Systems (IDS) typically rely on signature-based or static rule-based approaches. However, these methods present several limitations, including the inability to detect unknown (zero-day) attacks, high false positive rates, and limited adaptability to dynamic network environments. Moreover, many existing solutions lack real-time decision-making capabilities and struggle to effectively detect low-rate and application-layer distributed attacks.

To address these limitations, this work proposes a hybrid and intelligent detection approach that combines machine learning techniques with statistical and behavioral analysis methods. The objective is to design an adaptive, accurate, and real-time DDoS detection system capable of handling modern and evolving attack patterns.

Study Objectives:

1. Design and implement a hybrid DDoS detection system combining machine learning and statistical analysis
2. Develop a real-time packet capture and flow processing module using Scapy
3. Integrate entropy-based analysis and adaptive baseline monitoring for anomaly detection
4. Build an interactive Streamlit dashboard for real-time visualization and alerting
5. Evaluate the system using dataset replay and controlled attack simulations

Methodological Overview: The proposed system is built on a multi-layer detection framework. Network traffic is processed in 5-second sliding windows, where nine flow-based

features are extracted. A Random Forest classifier trained on the CIC-DDoS2019 dataset is used for primary classification. In parallel, statistical techniques such as Z-score-based adaptive baseline monitoring and Shannon entropy analysis are applied to detect abnormal traffic behavior. The final decision is produced by a hybrid fusion engine that combines machine learning predictions, statistical anomalies, and emergency threshold detection.

Research Contributions: This work proposes **DDoSentinel**, a hybrid real-time DDoS detection system designed to overcome the limitations of traditional IDS solutions. The main contributions of this research are:

- A real-time hybrid detection pipeline combining machine learning and statistical analysis
- Integration of Random Forest classification with entropy-based analysis and adaptive baseline monitoring
- A multi-signal decision engine providing explainable detection results
- A Streamlit-based dashboard for real-time monitoring and incident visualization

The system achieves **97.99% detection accuracy**, with a false positive rate below 2% and an average inference latency of approximately 5 ms per detection window on standard CPU hardware.

Overall, the proposed system integrates multiple complementary detection mechanisms into a unified framework. By combining predictive modeling, statistical anomaly detection, and real-time monitoring, DDoSentinel improves detection accuracy, reduces false positives, and ensures fast response to DDoS attacks in practical environments.

Document Organization:

- **Chapter 1:** Introduces network security fundamentals, CIA triad, and DDoS attack models.
- **Chapter 2:** Presents artificial intelligence techniques for DDoS detection and dataset description.
- **Chapter 3:** Covers IDS/IPS architectures, detection methods, and related work analysis.
- **Chapter 4:** Details the implementation of the DDoSentinel system, including architecture, detection modules, and experimental results.
- **General Conclusion:** Summarizes contributions, limitations, and future research directions.

Chapter 1: Network Security and DDoS Attack Background

1.1 Introduction

A computer network is a set of interconnected systems that enables data exchange and resource sharing. With the rapid growth of Internet-based services, networks have become fundamental to modern infrastructures, including healthcare, finance, and cloud computing [2].

However, this dependence has expanded the attack surface, making networks more vulnerable to cyber threats. Among these, Distributed Denial of Service (DDoS) attacks are among the most severe, aiming to exhaust resources by generating massive traffic from multiple sources, leading to service unavailability [3].

This chapter provides a structured overview of network security fundamentals, including network types, security objectives, vulnerabilities, attack types, and an in-depth presentation of DDoS attacks, their classification, techniques, and mitigation tools.

1.2 Types of Networks

Networks can be classified according to different criteria, including their geographic size, architecture, and transmission technology.

1.2.1 Classification by Geographic Size

The most common classification of networks is based on their geographic coverage area [2].

Personal Area Network (PAN)

A **Personal Area Network (PAN)** is a small-scale network designed for communication among devices within a person's immediate workspace, typically within a range of **10 meters**. Examples include Bluetooth headset connections, wireless keyboards, and smartphone-to-laptop tethering.

Local Area Network (LAN)

A **Local Area Network (LAN)** connects devices within a limited geographic area, such as a home, office, school, or university campus. LANs are characterized by high data transfer rates, low error rates, and private ownership.

Campus Area Network (CAN)

A **Campus Area Network (CAN)** connects multiple LANs within a limited geographic area, such as a university campus or corporate park.

Metropolitan Area Network (MAN)

A **Metropolitan Area Network (MAN)** spans a city or large campus and interconnects multiple LANs over medium distances.

Wide Area Network (WAN)

A **Wide Area Network (WAN)** covers a large geographic area such as countries or continents. The Internet is the largest example of a WAN.

Storage Area Network (SAN)

A **Storage Area Network (SAN)** is a specialized high-speed network that provides access to consolidated data storage systems. Unlike general-purpose communication networks, SAN is primarily designed for storage connectivity rather than general data exchange.

1.3 Network Security Challenges

As computer networks expanded in scale and became increasingly interconnected, they also became more exposed to cyber threats and malicious activities. The diversity of services provided by modern networks makes them attractive targets for attackers seeking to disrupt operations, steal information, or exploit system resources [2]. Consequently, protecting network infrastructures has become a critical requirement in order to ensure confidentiality, integrity, and availability of services in modern digital environments [4].

1.3.1 Why Networks Are Targeted

Networks are targeted for several reasons:

- They carry sensitive and valuable data
- They provide access to critical services
- They can be used as launching points for further attacks
- Disrupting a network can cause significant financial and operational damage

According to the VIVA framework (Value, Inertia, Visibility, Access), which identifies four factors that increase an organization's DDoS victimization risk the perceived value of its assets, inertia in adopting security measures, online visibility, and ease of access organizations with higher popularity and those operating in certain industry sectors face a significantly higher risk of DDoS victimization [5].

Among the most significant and evolving risks are **Distributed Denial of Service (DDoS) attacks**, which are capable of crippling network infrastructure and disrupting critical services. According to recent studies, the number and scale of DDoS attacks continue to increase dramatically, causing severe operational and financial consequences for organizations worldwide [3].

1.4 Network Security

1.4.1 Definition

Network security can be defined as the set of technical, organizational, legal, and human measures implemented to protect computer networks and their associated systems against unauthorized access, misuse, destruction, or service disruption [6].

Information security encompasses all activities related to the protection of information regardless of its storage or transmission medium. It aims to preserve data against unauthorized access, modification, disclosure, or destruction.

In the context of computer networks, security mechanisms aim not only to protect data confidentiality and integrity, but also to guarantee service availability against attacks that attempt to disrupt network operations, such as Distributed Denial of Service (DDoS) attacks.

1.5 Security Objectives

The main objectives of computer and network security are summarized as follows [7]:

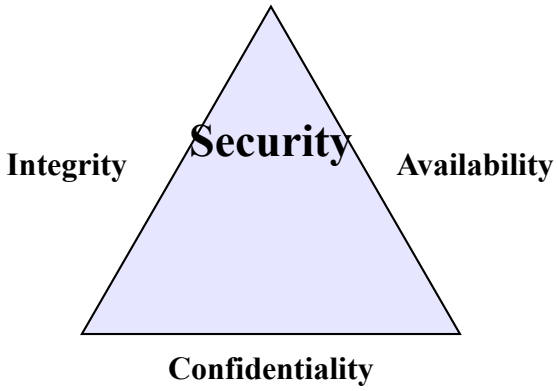


Figure 1.1. The CIA Triad: Core Objectives of Information Security

1.5.1 Confidentiality

Confidentiality ensures that information is accessible only to authorized entities.

1.5.2 Integrity

Integrity guarantees that information is not modified or altered in an unauthorized manner.

1.5.3 Availability

Availability ensures that systems, services, and data remain accessible and operational whenever needed. This objective is particularly important in the context of DDoS attacks, whose primary goal is to disrupt service availability.

1.5.4 The Reasons for Securing Networks

Economic Stakes

Organizations rely heavily on information systems to support their operations and competitiveness. Therefore, securing networks is essential to protect business activities and ensure service reliability [6].

Political Stakes

Organizations often follow government security standards and guidelines related to network protection, encryption, and cybersecurity practices. Failure to comply with these regulations may expose organizations to significant risks [6].

Legal Stakes

Network and information system management must comply with legal and regulatory requirements. Non compliance with these laws can lead to serious legal and organizational consequences [6].

1.6 Vulnerabilities and Threats

1.6.1 Vulnerabilities

A vulnerability is a weakness in a computer system that can be exploited to compromise security. Vulnerabilities can be classified into human, technological, organizational, and implementation-based categories [6].

1.6.2 Threats

A cyber threat is any malicious or accidental action capable of compromising system security [8]. Threats are classified as:

- **Accidental threats**: unintentional user errors or system failures
- **Intentional threats**: deliberate attacks targeting confidentiality, integrity, or availability.

1.7 Network Attacks

1.7.1 Definition of Attack

An attack is a malicious action that exploits vulnerabilities in a computer system or network for purposes unknown to those responsible for the system [6], and generally harmful to the information system. Attacks are carried out for various reasons:

- Disrupting the proper functioning of a system or service
- Theft of sensitive information (e.g., banking data)
- Using system resources for other purposes
- Espionage or sabotage
- Financial gain through ransomware

1.7.2 Types of Network Attacks

Common network attacks include [6]:

- **Intrusion Attack:** Infiltrating a system to retrieve unauthorized information.
- **Man-in-the-Middle Attack:** Intercepting communications between two parties without their knowledge.
- **Denial-of-Service (DoS) Attack:** Disrupting service functionality by exploiting protocol weaknesses.
- **Phishing Attack:** Impersonating legitimate entities to steal credentials or financial information.
- **Password Attacks:** Dictionary attacks (testing pre-existing wordlists) and brute-force attacks (testing all possible combinations).
- **Social Engineering Attack:** Manipulating users to disclose sensitive information through psychological deception.

Among these attacks, Distributed Denial of Service (DDoS) attacks are the most dangerous because they combine multiple sophisticated techniques: they leverage botnets to launch coordinated floods from distributed sources, exploit network asymmetries where minimal attacker resources cause massive damage, and use reflection and amplification to multiply traffic volume. Combined with IP spoofing, these methods hide the attacker's identity while overwhelming targets, with modern attacks exceeding 31.4 Tbps [9].

1.8 Network Security Techniques

Several techniques are used to protect computer networks against cyberattacks and unauthorized access [10].

1.8.1 Encryption

Encryption protects sensitive information by converting readable data into unreadable ciphertext [10].

1.8.2 Firewall

A firewall monitors and filters incoming and outgoing traffic according to predefined security policies [10].

1.8.3 Antivirus

Antivirus software detects and removes malicious software such as viruses and malware [10].

1.8.4 Virtual Private Network (VPN)

VPN technology enables secure communication over public networks using encrypted tunnels [10].

1.8.5 Authentication and Access Control

Authentication and access control mechanisms ensure that only authorized users can access network resources [10].

1.9 Distributed Denial of Service (DDoS) Attacks

1.9.1 Definition

Distributed Denial of Service (DDoS) attacks are defined as coordinated malicious attempts to disrupt or interrupt the availability of network services by overwhelming the target system with traffic from multiple sources [11].

1.9.2 Targets of DDoS Attacks

According to Bhattacharyya and Kalita (2015), a DDoS attacker may target several components within a network infrastructure. Understanding these targets is essential for designing effective defense mechanisms [9].

The main targets of DDoS attacks include:

- **Routers:** By overwhelming routing resources, attackers can disrupt network connectivity and packet forwarding.
- **Communication links:** Through bandwidth saturation, attackers consume available network capacity, preventing legitimate traffic from flowing.
- **Firewalls and defense systems:** Attackers target security devices to bypass access controls or exhaust their processing capabilities.
- **Victim infrastructure:** This includes servers and network resources that support critical services and applications.

- **Victim operating system:** By consuming system resources such as CPU, memory, or file handles, the attacker degrades overall system performance.
- **Current communications:** Ongoing connections between users and services can be disrupted, causing session terminations or degraded quality of service.
- **Applications and services:** Attackers make specific applications unavailable to legitimate users by exhausting application layer resources or exploiting software vulnerabilities.

1.9.3 Stages of a DDoS Attack Orchestration

Launching a successful DDoS attack requires the attacker to follow a structured process consisting of several distinct phases [12].

Agent Selection

The first stage involves identifying and selecting the machines that will serve as attack agents (bots or zombies), based on the presence of exploitable vulnerabilities. Attackers seek machines with sufficient computational and network resources to generate high volume attack traffic [12].

Compromise and Infection

Once potential agents are identified, the attacker exploits their security flaws to install malicious code, concealing it from detection mechanisms. System owners typically remain unaware that their machines have been compromised [12].

Communication and Coordination

Before initiating the attack, the attacker communicates with the command-and-control (C&C) servers to determine available agents and optimal timing. Common protocols include TCP, UDP, and ICMP [12].

Attack Execution

The attacker issues the command to commence the attack, customizing parameters such as target identity, attack duration, and packet properties (TTL values, port numbers) to evade detection [12].

1.9.4 DDoS Attack Architecture

A DDoS attack consists of four elements: the attacker, the control masters (handlers), the agents (zombies), and the victim.

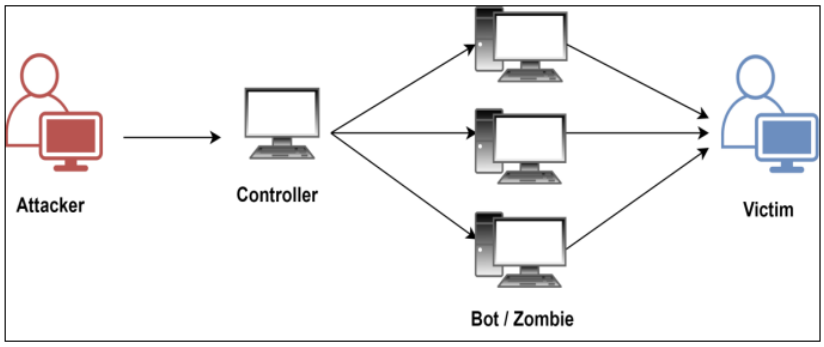


Figure 1.2. Architecture of a DDoS Attack [13]

A DDoS botnet is a network of hundreds or thousands of compromised machines controlled by an attacker through command-and-control (C&C) servers, often using IP spoofing to hide their identity [14]. When the attacker issues a command, all bots simultaneously send requests to the victim. The combined volume far exceeds the target's capacity, causing service disruption.

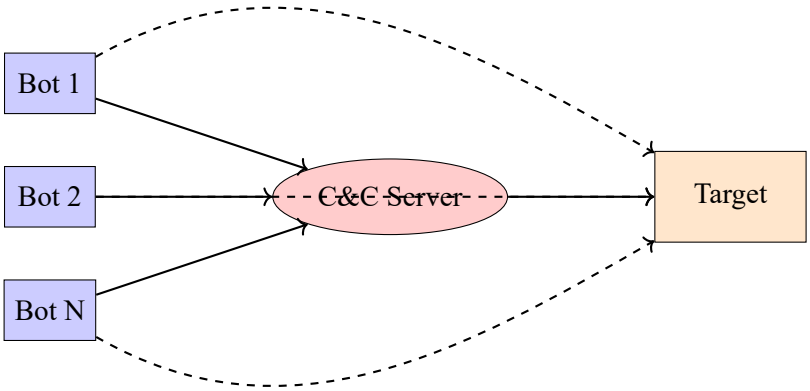


Figure 1.3. Botnet Architecture for DDoS Attacks

1.9.5 Classification of DDoS Attacks

DDoS attacks can be classified in multiple ways. Figure 1.4 shows the common classifications.

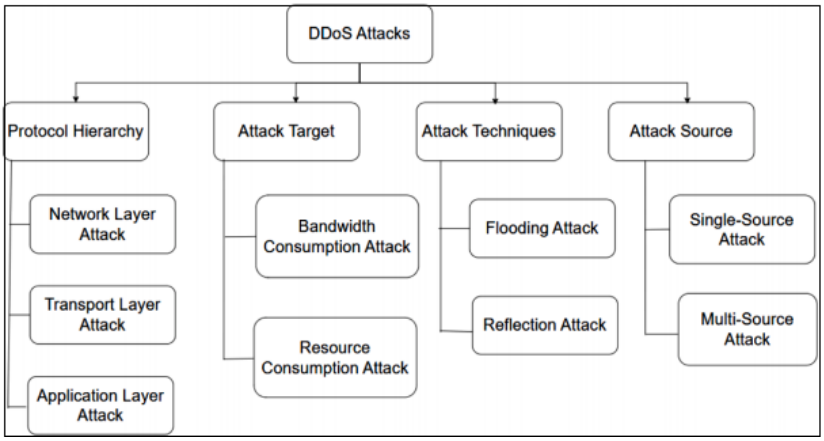


Figure 1.4. Classification of DDoS Attacks [15]

Classification Based on Protocol Hierarchy

Network Layer Attacks: Target network layer protocols to overload network devices by consuming bandwidth.

- **ICMP Flooding:** Massive ICMP echo request packets overwhelm the target [16].
- **IP Fragmentation Attack:** Forged fragmented packets force excessive reassembly resource consumption.

Transport Layer Attacks: Exhaust transport layer resources such as connection state and ports.

- **SYN Flooding:** Large numbers of SYN requests create numerous half-open connections [17].
- **ACK Flooding:** Flood of spoofed ACK packets consumes significant system resources.

Application Layer Attacks: Target application layer resources by simulating normal user behavior [15].

- **HTTP GET/POST Flooding:** Overloads web servers with massive HTTP requests.
- **Slowloris Attack:** Keeps connections open with partial requests, exhausting connection pools.

Classification Based on Attack Target

Bandwidth Consumption Attacks:

- **UDP Flood:** UDP packets consume network bandwidth [18].

- **NTP Amplification:** Forged NTP requests generate amplified responses toward the victim [19].

Resource Consumption Attacks:

- **XML Bomb:** Nested XML elements exhaust CPU and memory during parsing [20].
- **Complex SQL Query Attack:** Heavy database queries consume processing power [21].

Classification Based on Attack Techniques

- **Amplification Attacks:** A small request to a vulnerable service generates a much larger response, multiplying traffic toward the victim [15].
- **Reflection Attacks:** The attacker spoofs the victim's IP, causing public servers to send large responses directly to the victim [15].

Classification Based on Attack Source

- **Single-Source Attack:** Traffic from a single IP, typically using proxies [15].
- **Multi-Source Attack:** Traffic from distributed botnet nodes the typical DDoS form [15].

1.9.6 Techniques Used to Carry Out a DDoS Attack

TCP SYN Flood Attack

The attacker sends massive SYN packets with spoofed IPs, exhausting the server's connection table [17].

UDP Flood Attack

Random ports are flooded with UDP packets, consuming bandwidth and CPU [22].

ICMP Flood Attack

High volume ICMP echo requests consume network bandwidth [22].

DNS Amplification Attack

Small DNS queries with spoofed victim IP trigger large responses (50-100x amplification) [23].

NTP Amplification Attack

Small NTP requests generate responses up to 1000x larger [19].

HTTP Flood Attack

Large numbers of legitimate-looking HTTP requests are sent using real bot IPs, making detection difficult [22].

Slowloris Attack

Multiple partial HTTP connections exhaust the server's concurrent connection pool [24].

1.9.7 Recent DDoS Attack Statistics (2024--2025)

DDoS attacks have escalated dramatically in recent years. The largest attack recorded reached **31.4 Tbps** in 2025 (Cloudflare), while Microsoft Azure mitigated a 15.72 Tbps attack from the AISURU botnet. Overall, attack volume increased by **121% year-over-year** in 2025, with over 47.1 million attacks mitigated globally [1], [25], [26].

Table 1.1: Evolution of Largest Recorded DDoS Attacks (2022--2025)

Year	Peak Size	Attack Type	Source
2022	1.7 Tbps	UDP Flood	AWS
2023	2.0 Tbps	Reflection/Amplification	Google
2024	3.8 Tbps	HTTP/2 Rapid Reset	Cloudflare
2025	**31.4 Tbps**	**Hyper-volume HTTP**	**Cloudflare**

1.9.8 Limitations of Traditional DDoS Detection Approaches

Traditional DDoS detection methods (signature based and threshold based) face three main limitations: they cannot detect zero-day attacks, suffer from high false positive and false negative rates, and lack scalability for large scale traffic. Real time detection remains challenging due to computational overhead [4]. These limitations motivate the need for machine learning techniques, discussed in the next chapter.

1.10 Network Security Tools

Several tools are used to secure and monitor network infrastructure.

1.10.1 OpenVAS (Open Vulnerability Assessment System)

OpenVAS is a powerful open-source vulnerability scanning toolkit providing a comprehensive solution for identifying security weaknesses. Originally forked from NESSUS, it offers regular database updates and detects potential entry points that attackers might exploit [27].

1.10.2 NMAP

NMAP is a network scanning tool designed to identify active services and open ports on target systems. It is widely used for security auditing and is compatible with Unix/Linux, Windows, and Mac [28].

1.10.3 Wireshark

Wireshark is a network protocol analyzer that allows real-time visualization and inspection of network activity. It uses the `libpcap` library to capture packets and displays comprehensive information including source/destination IPs, protocols, and raw packet content. It is open-source software released under the GNU GPL [29].

1.10.4 Scapy

Scapy is a Python based interactive tool for packet manipulation forging, decoding, sending, capturing, and analyzing network packets. It is commonly used for network scanning, packet injection, and traffic analysis.

Key Features:

- Packet crafting and manipulation
- Packet sniffing and capture
- Network discovery and scanning
- Protocol analysis and decoding
- Real-time network sensor capability

In the context of this thesis, Scapy serves as the primary packet capture engine for DDoSentinel, extracting source IP, destination IP, ports, protocol, packet length, and timestamps from live traffic [30].

1.11 Conclusion

This chapter introduced the fundamental concepts of network security and DDoS attacks, covering network types, security objectives, vulnerabilities, threats, and attack techniques such as SYN flood, DNS amplification, and HTTP flood.

Recent statistics confirm the growing severity of DDoS attacks, with the largest recorded attack reaching **31.4 Tbps** in 2025 [1]. Traditional detection methods (signature-based, anomaly-based, statistical) remain insufficient due to their inability to detect zero-day attacks, high false positive rates, and lack of real-time scalability [4].

These limitations motivate the adoption of machine learning for DDoS detection. The next chapter introduces AI and ML concepts, presents the CIC-DDoS2019 dataset, and discusses machine learning algorithms for DDoS detection.

Chapter 2: Artificial Intelligence for DDoS Detection

2.1 Introduction

With the rapid evolution of DDoS attacks, traditional detection methods (signature-based, anomaly-based, statistical) face significant limitations against large-scale, adaptive, and unseen attack patterns.

To overcome these challenges, artificial intelligence particularly machine learning has emerged as a powerful paradigm capable of learning complex traffic patterns and adapting to evolving attacks without predefined rules.

This chapter presents AI, ML, and DL concepts in the context of DDoS detection. It introduces common datasets, feature selection considerations, main algorithms, evaluation metrics, and general challenges in ML-based DDoS detection.

2.2 Definitions and Concepts

2.2.1 Artificial Intelligence

Artificial intelligence (AI) refers to computer systems capable of performing tasks typically associated with human intelligence, such as reasoning, decision-making, and problem-solving.

According to NASA, AI can be defined from multiple perspectives [31], [32], [33]:

- Systems capable of operating in dynamic environments without human intervention
- Systems performing cognitive tasks such as perception, learning, and planning
- Systems designed to emulate human thinking or behavior
- Computational techniques approximating cognitive functions

In cybersecurity, AI enables:

- Real-time threat detection
- Learning from historical attacks
- Adaptation to new attack patterns
- Reduction of false positives

2.2.2 Machine Learning

Machine learning (ML) is a subset of AI that enables systems to learn from data without explicit programming [34]. ML algorithms identify patterns and make predictions based on statistical analysis of data.

Unlike rule-based systems, ML models are trained on data rather than programmed with fixed rules, making them suitable for dynamic environments such as DDoS detection.

2.2.3 Deep Learning

Deep learning (DL) is a subset of ML that uses multi-layer neural networks to automatically learn hierarchical feature representations from raw data [35].

While DL achieves high accuracy, it typically requires large datasets, GPU acceleration, and offers limited interpretability compared to classical ML methods.

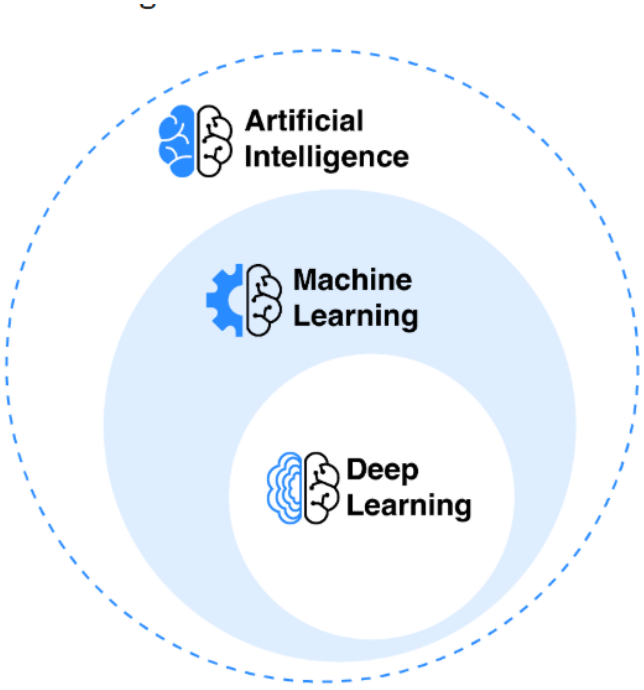


Figure 2.1. Hierarchy of Artificial Intelligence, Machine Learning, and Deep Learning [31]

2.3 Types of Machine Learning

Machine learning can be broadly classified into three main categories: supervised learning, unsupervised learning, and reinforcement learning [36].

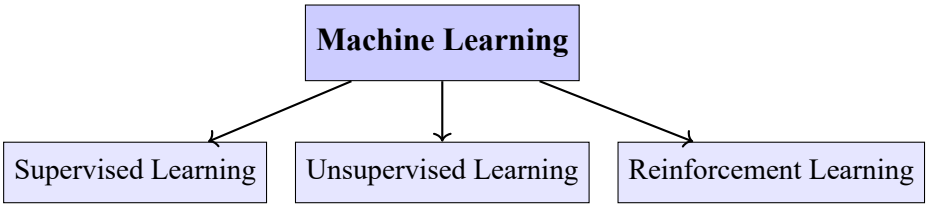


Figure 2.2. Three Main Types of Machine Learning

2.3.1 Supervised Learning

Supervised learning trains models using labeled data, where each training sample has a known output. The model learns the mapping from inputs to outputs, enabling predictions on unseen data [36].

Supervised learning can be divided into two subcategories:

- **Classification tasks:** Predict categorical labels such as attack versus normal traffic [36].
- **Regression tasks:** Predict continuous values such as traffic volume or attack intensity [36].

For DDoS detection, classification is the primary approach because the goal is to distinguish between attack and normal traffic.

2.3.2 Unsupervised Learning

In unsupervised learning, machines are trained on unlabeled datasets, where there is no ground truth assigned by a human. Common unsupervised methods include clustering, dimensionality reduction, and anomaly detection. These approaches enable the machine to identify patterns, relationships, and structures within the data without prior knowledge of expected outcomes [36].

2.3.3 Reinforcement Learning

Reinforcement learning (RL) is a form of ML in which an autonomous agent acquires the ability to make decisions through iterative interactions with its environment, receiving rewards or penalties as feedback for its actions. The agent learns optimal actions through trial and error to maximize cumulative rewards [36].

2.4 Machine Learning Pipeline

A typical ML pipeline for DDoS detection includes the following stages:

1. **Data Collection:** Network traffic capture from live interfaces or datasets
2. **Preprocessing:** Cleaning, normalization, and handling of missing values
3. **Feature Extraction:** Deriving statistical features from network flows
4. **Feature Selection:** Choosing relevant features to reduce dimensionality
5. **Data Split:** Dividing data into training and testing subsets
6. **Model Training:** Learning patterns from labeled training data
7. **Model Evaluation:** Assessing performance on unseen test data
8. **Inference:** Applying the trained model to new traffic

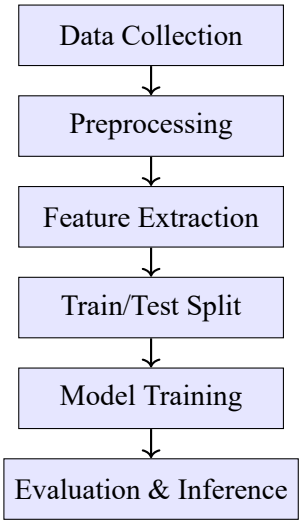


Figure 2.3. General Machine Learning Pipeline for DDoS Detection

2.5 Machine Learning for DDoS Detection

Traditional DDoS detection approaches rely on predefined signatures, thresholds, or manually crafted rules. Although effective against known attacks, these methods struggle to identify zero-day attacks and rapidly evolving attack patterns.

Machine learning overcomes these limitations by learning traffic behavior directly from data. Instead of relying on fixed rules, ML models can automatically identify hidden patterns and distinguish malicious traffic from legitimate traffic even when attack characteristics change over time.

For this reason, machine learning has become one of the most widely adopted approaches in modern DDoS detection systems [37].

2.6 Datasets for DDoS Detection

2.6.1 CIC-DDoS2019 Dataset

The CIC-DDoS2019 dataset is one of the most widely used benchmarks for DDoS detection research [38], [39].

- Contains 12 different DDoS attack types (SYN, UDP, DNS, NTP, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP-Lag, WebDDoS, TFTP)
- Includes over 80 network flow features extracted using CICFlowMeter-V3
- Features realistic background traffic simulating multiple users
- Available in both PCAP and CSV formats

2.6.2 Common Dataset Challenges

Public DDoS datasets often present several challenges:

- **Class imbalance:** Attack samples typically far outnumber benign samples
- **Feature redundancy:** Many features are correlated or irrelevant
- **Age of datasets:** Some datasets do not reflect recent attack techniques

2.7 Feature Engineering

2.7.1 Flow-Based Features

Network flow analysis is commonly used in DDoS detection. A flow is defined by the 5-tuple: source IP, destination IP, source port, destination port, and protocol.

Common flow-based features include:

- Flow duration
- Packet and byte counts (forward and backward)
- Packet and byte rates (per second)
- Inter-arrival time (IAT) statistics (mean, standard deviation)
- TCP flag counts (SYN, ACK, FIN, RST)
- Flow direction statistics

2.7.2 Feature Selection Considerations

Selecting appropriate features is important because:

- Irrelevant features increase computational cost without improving accuracy
- Redundant features may cause overfitting
- Lightweight features enable faster real-time processing

2.8 Machine Learning Algorithms for DDoS Detection

2.8.1 Logistic Regression

A linear supervised algorithm for binary classification. It models class probability using a sigmoid function. Simple and fast, but limited to linear decision boundaries [40].

2.8.2 K-Nearest Neighbors (KNN)

An instance-based algorithm that classifies samples by majority vote of their K nearest neighbors. No explicit training phase, but inference is computationally expensive for large datasets [40].

2.8.3 Support Vector Machine (SVM)

Finds the optimal hyperplane that maximizes the margin between classes. Strong generalization for high-dimensional data, but training time scales poorly with dataset size [40].

2.8.4 Decision Tree

A tree-structured classifier that partitions the feature space using binary splitting rules. Highly interpretable but prone to overfitting without regularization [40].

2.8.5 Random Forest

An ensemble method that builds multiple decision trees on bootstrap samples and aggregates predictions by majority voting. Advantages include resistance to overfitting, ability to handle high-dimensional data, and built-in feature importance [41].

2.8.6 XGBoost

A gradient boosting implementation with L1/L2 regularization. Achieves high accuracy but requires careful hyperparameter tuning [42].

2.8.7 CatBoost

A gradient boosting algorithm with ordered target encoding designed to handle categorical features [43].

2.9 Algorithm Comparison

Table 2.1: Comparison of Machine Learning Algorithms for DDoS Detection [37], [44]

Algorithm	**Accuracy**	**Training Speed**	**Inference Speed**
Logistic Regression	99.70%	Fast	Fast
K-Nearest Neighbors	98.50%	Very Fast	Slow
Support Vector Machine	99.10%	Slow	Fast
Decision Tree	99.78%	Fast	Fast
Random Forest	**97.99%**	Moderate	Fast
XGBoost (Real-world)	95.30%	Moderate	Fast
CatBoost	99.63%	Moderate	Fast

2.10 Random Forest Selection Rationale

Among the machine learning algorithms discussed in this chapter, **Random Forest** is often preferred for DDoS detection tasks due to several theoretical and practical advantages.

2.10.1 Superior Accuracy

Ensemble methods, particularly Random Forest, consistently achieve higher accuracy than individual classifiers on network traffic data. By aggregating predictions from multiple decision trees trained on bootstrap samples, Random Forest reduces both bias and variance, leading to better generalization on unseen data [41].

2.10.2 Robustness to Noise and Missing Values

Network traffic data often contains imperfections such as packet loss, incomplete flows, and measurement errors. Random Forest is inherently robust to noisy data because each tree is trained on a different bootstrap sample, and the final prediction is based on majority voting.

This ensemble structure makes it less sensitive to outliers and missing values compared to single classifiers [45].

2.10.3 Built-in Feature Importance

Random Forest provides intrinsic feature importance scores based on how much each feature reduces impurity across all trees. This enables systematic feature selection without requiring additional computational overhead, which is particularly valuable when dealing with high-dimensional network flow data (80+ features).

2.10.4 Handling Class Imbalance

DDoS datasets typically exhibit extreme class imbalance, with attack samples far outnumbering benign samples. Random Forest addresses this through bootstrap sampling, where each tree is trained on a random subset of the data. This sampling strategy helps maintain sensitivity to minority classes without requiring explicit resampling techniques [41].

2.10.5 Efficient Inference

For real-time DDoS detection, inference latency is critical. Random Forest achieves fast prediction times because classification involves traversing each decision tree (O(log n) depth) and aggregating votes. This makes it suitable for high-speed network monitoring environments.

These properties make Random Forest a widely adopted algorithm in network security applications, including DDoS detection systems, as reported in recent literature [44], [45].

2.11 Challenges in ML-Based DDoS Detection

2.11.1 Class Imbalance

DDoS datasets often contain far more attack samples than benign samples. Models trained on imbalanced data may become biased toward the majority class, failing to detect minority class samples (e.g., normal traffic) [41].

2.11.2 Data Quality

Real-world network traffic may contain:

- Missing values due to packet loss
- Noise from measurement errors

- Outliers from unusual network conditions

2.11.3 Concept Drift

Attack patterns evolve over time. Models trained on historical data may become less effective as new attack techniques emerge.

2.11.4 Real-Time Constraints

DDoS detection requires low-latency analysis to enable timely mitigation. Feature extraction and model inference must be fast enough to keep pace with high-speed network traffic.

2.11.5 Scalability

Network traffic volumes can reach millions of packets per second. Detection systems must scale to handle this volume without dropping packets.

2.11.6 Interpretability

Security operators need to understand why a detection system flagged certain traffic. Black-box models may be less trusted in operational environments.

2.12 Evaluation Metrics

2.12.1 Confusion Matrix

Table 2.2: Confusion Matrix Structure

	Predicted Attack	**Predicted Normal**
Actual Attack	TP (True Positive)	FN (False Negative)
Actual Normal	FP (False Positive)	TN (True Negative)

2.12.2 Accuracy

Accuracy measures the proportion of correctly classified instances [46].

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

2.12.3 Precision

Precision measures the fraction of predicted attacks that are genuine. High precision indicates few false alarms [46].

$$\text{Precision} = \frac{TP}{TP + FP}$$

2.12.4 Recall (Detection Rate)

Recall measures the fraction of actual attacks correctly detected. High recall indicates few missed attacks [46].

$$\text{Recall} = \frac{TP}{TP + FN}$$

2.12.5 F1-Score

The F1-Score is the harmonic mean of precision and recall, providing a single balanced metric [46].

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

2.13 Related Work

This section provides a comprehensive review of recent studies focused on DDoS attack detection.

2.13.1 Real-Time DDoS Detection Using 1D-CNN (Wang et al., 2025)

Wang et al. (2025) proposed a real-time DDoS attack detection system based on a one-dimensional Convolutional Neural Network (1D-CNN) designed to process continuous network traffic efficiently and detect volumetric attacks characterized by sudden traffic spikes and abnormal patterns. The model is built on a hierarchical CNN architecture optimized for feature extraction from time-series network data. It was evaluated on the CIC-DDoS2019 dataset and achieved high performance, with an accuracy of 99.17%, precision of 99.95%, recall of 98.98%, F1-score of 99.46%, and an AUC of 0.9992. The results demonstrate that the proposed 1D-CNN model outperforms traditional machine learning methods such as Random Forest, SVM, and LSTM, highlighting its effectiveness for real-time and high-speed network intrusion detection scenarios [47].

2.13.2 Hybrid Autoencoder-HDBSCAN Framework for Agriculture 4.0 Security(Kaliyaperumal et al., 2025)

Kaliyaperumal et al. (2025) proposed a hybrid Intrusion Detection System (IDS) for securing Agriculture 4.0 environments, where IoT, fog computing, and cloud infrastructures are widely used in modern smart farming systems. The authors highlighted the increasing vulnerability of these environments to Distributed Denial of Service (DDoS) attacks.

The proposed approach combines a deep Autoencoder (dAE) for anomaly detection with HDBSCAN clustering for multi-class attack classification. The Autoencoder is used to learn normal network behavior and detect anomalies based on reconstruction error, while HDBSCAN is used to group detected attack instances into different categories without requiring labeled data.

The framework was evaluated using the CIC-DDoS2019 dataset. The results showed that the hybrid model achieved strong performance in both binary detection and multi-class classification tasks. The study demonstrated that combining deep learning with clustering techniques can improve DDoS detection in Agriculture 4.0 and fog computing environments [48].

2.13.3 Feature-Optimized Machine Learning Framework (Ibrahim et al., 2025)

Ibrahim et al. (2025) proposed a machine learning-based framework for DDoS attack detection and mitigation focused on feature optimization to improve efficiency and reduce computational complexity. The study highlights the importance of using optimized feature sets instead of large redundant network features to enhance real-time applicability.

The proposed approach is evaluated using the CIC-DDoS2019 dataset and applies feature selection techniques to extract relevant network traffic characteristics such as packet length, flow-based statistics, and inter-arrival time. Several supervised machine learning algorithms are used for classification, including Logistic Regression, Decision Tree, Random Forest, Gradient Boosting, and CatBoost.

The experimental results show that tree-based models, particularly Decision Tree and Random Forest, achieve very high detection performance, reaching accuracy values up to 99.85%, with very low inference time suitable for real-time DDoS detection and mitigation systems. The study demonstrates the effectiveness of lightweight machine learning models for building scalable and efficient network security solutions [44].

2.13.4 Optimized Random Forest Using Backward Elimination (Sawah et al., 2025)

Sawah et al. (2025) proposed a machine learning-based approach for DDoS attack detection in Software-Defined Network (SDN) environments. The study focuses on improving classification performance through feature selection and hyperparameter optimization techniques.

The proposed framework is evaluated using the DDoS-SDN dataset and applies different supervised machine learning algorithms, including Random Forest, Naïve Bayes, K-Nearest Neighbors, Linear Discriminant Analysis, and Support Vector Machine. Feature selection techniques such as Backward Elimination (BE) and Recursive Feature Elimination (RFE) are used together with Grid Search and 5-fold cross-validation to optimize model performance.

The experimental results show that Random Forest achieves the best performance among all tested models, with an accuracy reaching 99.99%, along with high precision, recall, and F1-score. The study demonstrates that optimized ensemble learning models are highly effective for accurate and efficient DDoS detection in SDN environments [49].

2.13.5 A real-time machine-learning model for detecting and mitigating DDoS attacks

Recent research has focused on the development of machine learning-based approaches for detecting and mitigating Distributed Denial of Service (DDoS) attacks, which remain one of the most severe threats to the availability of online services. These attacks aim to exhaust network resources and make services unavailable to legitimate users, motivating the need for efficient detection systems.

In this context, a real-time DDoS detection system was proposed based on machine learning models trained using the CIC-DDoS2019 dataset. The study employs a comprehensive data preprocessing strategy followed by the application of several supervised learning algorithms, including Decision Tree, Random Forest, AdaBoost, and XGBoost, for traffic classification. Among these models, XGBoost and AdaBoost achieved the highest performance on offline data, with accuracy reaching 99.99%, while Decision Tree and Random Forest also provided competitive results.

The key contribution of this work is the deployment of the trained machine learning model into an online real-time detection system capable of operating outside the training environment. The system was evaluated using real DDoS attack traffic generated by Hping3, achieving an accuracy of 95.30% in real-world conditions. This demonstrates the effectiveness of integrating machine learning models into real-time environments for practical DDoS detection and mitigation [37].

2.13.6 A Machine Learning-Based Intrusion Detection System for Securing Internet of Things Networks (Zhang, 2025)

Zhang (2025) proposed a machine learning-based Intrusion Detection System (IDS) to enhance the security of Internet of Things (IoT) networks, which are increasingly vulnerable due to their large scale and heterogeneous nature. The study highlights that traditional rule-based security methods are not sufficient to handle the dynamic behavior of IoT environments.

The proposed approach applies supervised machine learning techniques to detect both known and unknown intrusion behaviors, including attacks such as DDoS, malware, and data theft. Several classification algorithms are evaluated, including Decision Tree, Random Forest, and K-Nearest Neighbors, using the BoTNeTIoT-L01 dataset.

The experimental results show that Decision Tree and Random Forest achieve the best performance in terms of detection accuracy, demonstrating the effectiveness of machine learning models in improving IoT network security and outperforming traditional security approaches [46].

Table 2.3: Comparative Analysis of Recent DDoS Detection Systems

Study	**Dataset**	**Method**	**Accuracy**	**Real-Time**	**Limitation**
Wang et al. (2025)	CIC-DDoS2019	1D-CNN	99.17%	No	High computational requirements and limited interpretability
Kaliyaperumal et al. (2025)	CIC-DDoS2019	Autoencoder + HDBSCAN	98%	No	Complex architecture and offline evaluation
Ibrahim et al. (2025)	CIC-DDoS2019	Random Forest, CatBoost	99.85%	Partial	Focused mainly on feature optimization
Sawah et al. (2025)	DDoS-SDN	Optimized Random Forest	99.99%	No	Limited to SDN environments
Fathian et al. (2026)	CIC-DDoS2019	XGBoost / AdaBoost	95.30%	Yes	Lower performance in real-world deployment
Zhang (2025)	BoTNeTIoT-L01	Decision Tree / RF	High	No	Focused on IoT environments only

2.14 Conclusion

This chapter presented the fundamental concepts of artificial intelligence, machine learning, and deep learning in the context of DDoS attack detection. Key topics covered include:

- Definitions of AI, ML, and DL

- Types of machine learning (supervised, unsupervised, reinforcement)
- The general ML pipeline for DDoS detection
- Overview of common datasets, particularly CIC-DDoS2019
- Feature engineering considerations
- Comparison of main ML algorithms (Logistic Regression, KNN, SVM, Decision Tree, Random Forest, XGBoost, CatBoost)
- Evaluation metrics (Accuracy, Precision, Recall, F1-Score, Confusion Matrix)
- General challenges in ML-based DDoS detection (class imbalance, data quality, concept drift, real-time constraints, scalability, interpretability)

The next chapter presents Intrusion Detection and Prevention Systems (IDS/IPS) and a critical review of related work in AI-based DDoS detection.

Chapter 3: Intrusion Detection and Prevention Systems (IDS/IPS)

3.1 Introduction

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are essential components of modern network security infrastructure, playing a crucial role in monitoring traffic and mitigating DDoS attacks.

Building upon the machine learning techniques introduced in Chapter 2, this chapter examines how IDS/IPS leverage these approaches for effective real-time DDoS detection. Integrating anomaly-based detection with machine learning classifiers overcomes the limitations of traditional signature-based systems, which fail to detect zero-day and low-rate attacks.

This chapter presents IDS/IPS definitions, architectures, types, detection methods, and DDoS related challenges, followed by a critical review of related work identifying research gaps that motivate the proposed detection system.

3.2 Definition of an Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a mechanism or piece of equipment (hardware or software) used to monitor the activity of a network or a given host in order to detect any intrusion attempt and potentially react to it (by implementing a risk prevention strategy) [50].

An IDS typically has either:

- A signature database that can be regularly updated as new threats are identified
- A behavioral approach that analyzes differences from the network's normal operating level as defined by the administrator

There are three concepts to classify intrusion-detection systems, which are summarized in Figure 3.1:

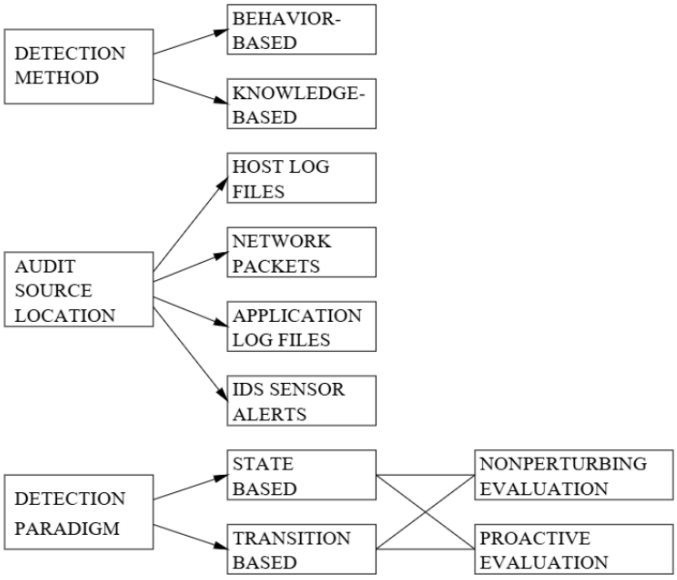


Figure 3.1. Classification of Intrusion Detection Systems [51]

3.3 Characteristics of an Intrusion Detection System

The following characteristics are desirable in an effective IDS [50]:

- **Continuous operation** with minimal manual supervision
- **Fault tolerance**, meaning it must recover after a failure or machine reset
- **Resistance to corruption attempts**, meaning it must be able to detect if it has itself undergone an unwanted modification
- **Minimal use** of the monitored system's resources
- **Easy configurability** to implement a network's specific security policy

3.4 The Main Tasks of an Intrusion Detection System

An IDS detects anomalies in network traffic and performs the following functions [50]:

- Detect network discovery attempts
- Detect, in some cases, whether an attack was successful
- Detect Denial of Service (DoS) attacks
- Detect the level of infection of the computer system and the affected network areas

- Identify infected machines
- Provide centralized alerts for all attacks
- Respond to attacks and correct any problems

3.5 Types of IDS

Several types of IDS have been developed since the 1980s, each with its own functions, characteristics, and applications. The placement of an IDS within a network depends heavily on the type of protection it offers.

3.5.1 Network Intrusion Detection Systems (NIDS)

NIDS are network IDS that analyze and interpret traffic across an entire network to identify signatures of known attacks at various points on the network or anomalies in IP packet headers [50].

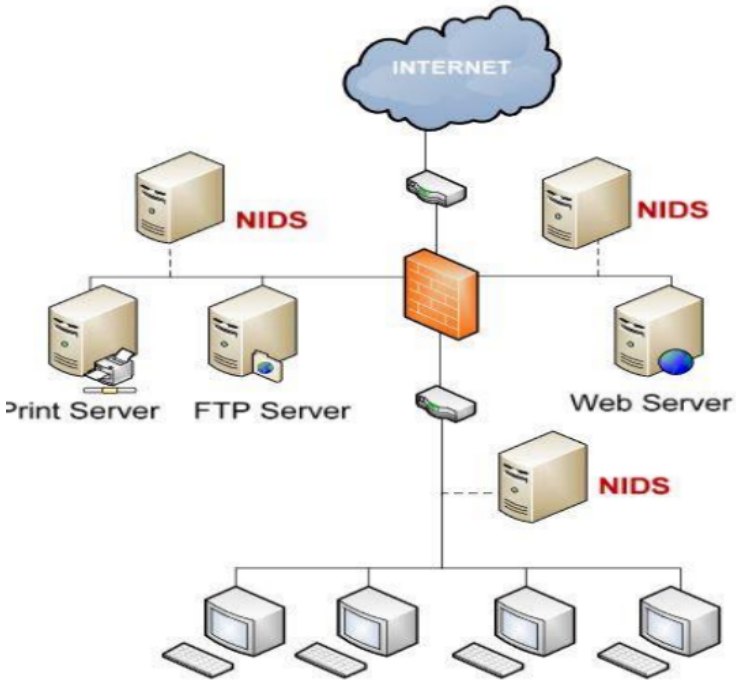


Figure 3.2. Network-Based IDS

Characteristics:

- Monitors entire network segments
- Analyzes network traffic in real-time

- Can detect attacks targeting multiple hosts
- Placed at strategic points within the network

3.5.2 Host-Based Intrusion Detection Systems (HIDS)

HIDS are IDS that allow the examination of the operation of a given machine and report any malicious behavior that could compromise its security. HIDS are generally placed on servers [50].

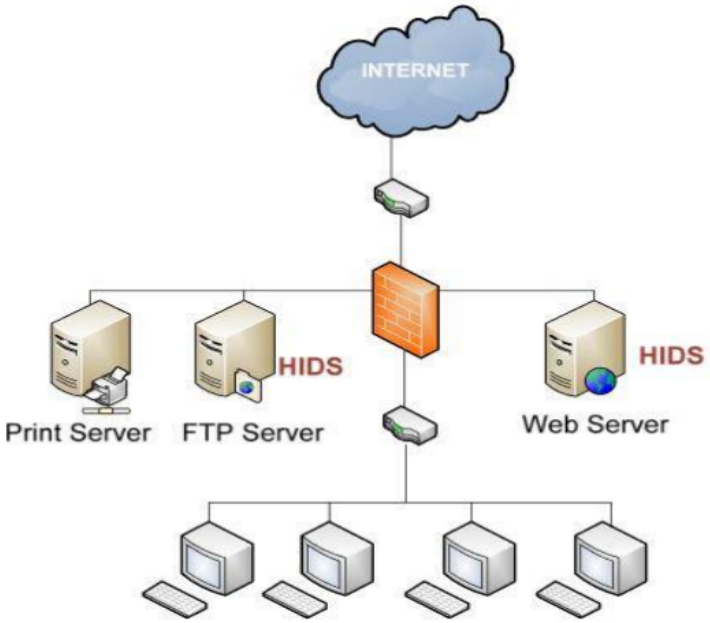


Figure 3.3. Host-Based IDS

3.5.3 Hybrid Intrusion Detection System

HIDS are extremely complementary to NIDS. Indeed, they allow for the easier detection of Trojan Horse type attacks, whereas this type of attack is difficult to detect by a NIDS. Hybrid IDS is a system capable of gathering information from both a HIDS and a NIDS. Generally used in a decentralized environment, it allows the collection of information from various probes placed on the network [50].

Characteristics:

- Combines monitoring of both network and individual hosts
- Analyzes system logs, file systems, network flows, and processes simultaneously
- Can detect attacks that either NIDS or HIDS alone would miss

- Considered more comprehensive and effective for complex multi-vector attacks such as DDoS

Table 3.1: Comparison of IDS Types

IDS Type	**Advantages**	**Limitations**
NIDS	Monitors entire network, Real-time detection	Cannot analyze encrypted traffic, May miss host-specific attacks
HIDS	Detailed host monitoring, Detects host-specific attacks	Resource intensive, Limited to single host
Hybrid	Comprehensive protection, Combines strengths of NIDS and HIDS	Complex to manage, Higher cost

3.6 Intrusion Detection Methods

3.6.1 Signature-Based Detection

Signature-based detection techniques analyze system activity, searching for events (or sets of events) that match a predefined pattern. This involves analyzing signatures that represent a known attack pattern. A signature can be the interpretation of packet sequences or data contained within those packets. It can also be found in audit logs, system logs, or modifications to files or memory within the compromised system [50].

Advantages:

- High accuracy for known attacks
- Low false positive rate
- Easy to implement and maintain

Limitations:

- Cannot detect zero-day attacks (new, unknown attacks)
- Must be regularly updated with new signatures
- Signature definition is critical: loosely defined signatures increase false alarms, tightly defined signatures risk missing attacks

3.6.2 Anomaly-Based Detection

Anomaly detection identifies any unacceptable deviation from expected behavior. It assumes that attacks are different from normal activity and can therefore be detected by identifying these differences. Expected behaviors of users, hosts, or network connections are built in advance. Profiles can be created manually or automatically based on data previously collected over a period of normal (assumed attack-free) operation [50].

Advantages:

- Can detect new and unknown attacks (zero-day attacks)
- Adapts to changes in network behavior
- No need for signature updates

Limitations:

- Requires a training phase
- Performance is highly sensitive to training data
- Often produces a large number of false alarms
- Normal user and system behaviors can vary considerably

3.6.3 Hybrid Detection

Hybrid detection is an attack detection method that combines both anomaly-based and signature-based detection to improve attack detection efficiency while reducing false positive rates [50].

Table 3.2: Comparison of Intrusion Detection Methods

Method	**Advantages**	**Limitations**
Signature-Based	High accuracy for known attacks, Low false positives	Cannot detect zero-day attacks, Needs regular updates
Anomaly-Based	Can detect new attacks, Adapts to changes	High false positives, Requires training
Hybrid	Combines strengths of both methods	More complex to implement

3.6.4 Machine Learning-Based Detection

Anomaly detection in network traffic is essential for protecting IT systems against DDoS attacks. Traditional rule-based methods often lack the precision needed to detect complex malicious behavior. This is why machine learning methods, as introduced in Chapter 2, have been increasingly adopted to improve anomaly detection in IDS/IPS systems.

By training on historical labeled traffic data, machine learning classifiers such as Random Forest can autonomously identify unusual traffic patterns that may indicate a DDoS attack. While this approach offers improved accuracy and reduces false positives compared to threshold-based methods, it typically requires large labeled datasets and significant computational resources for training. The integration of machine learning into IDS/IPS represents the current state of the art in DDoS detection, and forms the foundation of the system proposed in this thesis.

3.7 DDoS Detection

IDS and IPS play a crucial role in detecting and mitigating DDoS attacks. The following approaches are commonly used:

3.7.1 Traffic Volume Analysis

DDoS attacks are characterized by abnormally high traffic volume. IDS can detect such anomalies by:

- Monitoring bandwidth usage patterns and establishing baseline traffic profiles
- Triggering alerts when packets-per-second (PPS) or bytes-per-second (BPS) exceed defined thresholds
- Tracking sudden spikes in the number of active flows per second (FPS)

For example, a legitimate web server may handle 200--500 requests per second under normal load, whereas a volumetric DDoS attack may inject thousands of packets per second from distributed sources. The adaptive baseline mechanism introduced in Chapter 1 (Z-score monitoring) provides a dynamic and statistically sound alternative to fixed-threshold detection, and is integrated into the proposed system.

3.7.2 Protocol Analysis

Many DDoS attacks exploit protocol weaknesses. IDS can detect protocol-level anomalies including:

- SYN flood attacks (excessive half-open TCP connections with high SYN/ACK ratio)
- UDP flood attacks (high rate of UDP packets to random destination ports)
- ICMP flood attacks (ping floods consuming bandwidth)
- HTTP flood attacks (excessive web requests mimicking legitimate user behavior)

3.7.3 Statistical Anomaly Detection

Using statistical methods to identify deviations from normal behavior:

- Packet rate analysis using Z-score: $Z = (X - \mu)/\sigma$
- Flow entropy calculation using Shannon entropy: $H = -\sum p(x_i) \log_2 p(x_i)$
- Source IP distribution monitoring to detect botnet concentration

A sudden drop in source IP entropy below a critical threshold (e.g., $H < 2.0$) is a strong indicator of a botnet-based DDoS attack, as traffic becomes concentrated from a limited set of controlled sources rather than diverse legitimate users.

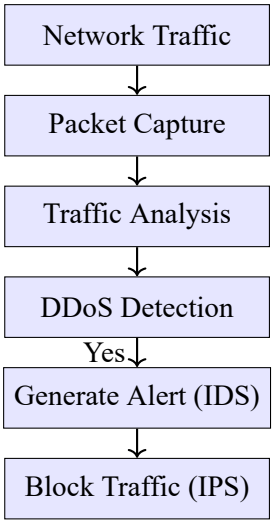


Figure 3.4. DDoS Detection Workflow in IDS/IPS

3.8 SNORT: Popular Open Source IDS

Snort is an open source Network Intrusion Detection System (NIDS) available free of cost. It is used for scanning data flowing on the network and is ranked among the top quality open-source security systems available today [52].

3.8.1 Snort Operation Modes

- **Sniffer Mode:** Reads and displays packets from the network interface
- **Packet Logger Mode:** Logs packets to disk for later analysis
- **Network Intrusion Detection Mode:** Analyzes traffic against configurable rule sets
- **Inline Mode (IPS):** Can drop malicious packets in real time

3.8.2 Snort Rules for DDoS Detection

The following example illustrates a Snort rule for detecting SYN flood attacks:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 80
(msg:"Possible SYN Flood"; flags:S; threshold:type both,
track by_src, count 100, seconds 10; sid:1000001;)
```

This rule triggers an alert when a single source IP sends more than 100 SYN packets to port 80 within 10 seconds, which is a strong indicator of a SYN flood attack.

3.9 IDS Architecture

An IDS is typically composed of three main components: a sensor, an analyzer, and a manager [50].

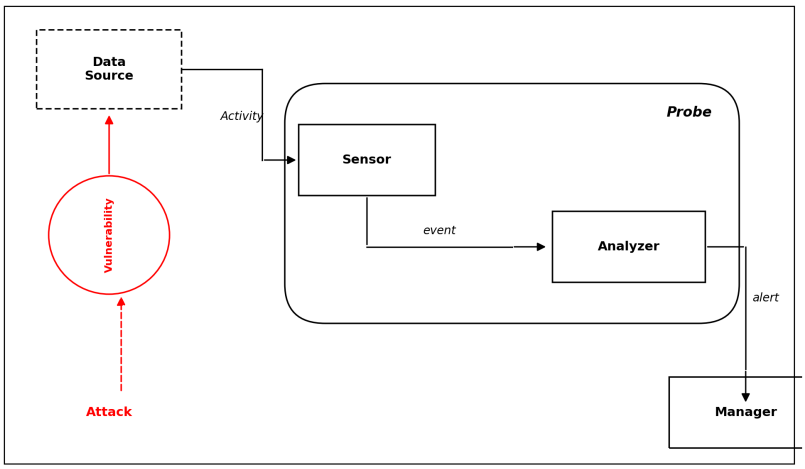


Figure 3.5. IDS Architecture [50]

3.9.1 Sensor

The sensor observes system activity via a data source and provides the analyzer with a sequence of events indicating the evolution of the system's state. Three types of sensors are distinguished based on their data sources:

- **System sensors:** Monitor operating system activities and system calls
- **Network sensors:** Monitor network traffic and packet flows
- **Application sensors:** Monitor specific application logs and behaviors

In the proposed system of this thesis, the Scapy-based packet capture module acts as a network sensor, feeding bidirectional flow statistics to the detection engine.

3.9.2 Analyzer

The analyzer's objective is to determine if the event stream provided by the sensor contains elements characteristic of malicious activity. This is where detection algorithms (signature-based, anomaly-based, or hybrid) are applied. In our system, this role is fulfilled by the Random Forest classifier combined with the statistical anomaly detection module.

3.9.3 Manager

The manager collects the alerts generated by the analyzer, formats them, and presents them to the operator. The manager is also responsible for determining the appropriate response:

- **Containment:** Limits the effects of the attack (e.g., rate limiting)
- **Eradication:** Attempts to stop the attack (e.g., source IP blocking)
- **Recovery:** Restores the system to a healthy state
- **Diagnosis:** Identifies the root cause of the detected incident

3.10 IDS Location

There are several strategic locations where an IDS should be placed within a network architecture:

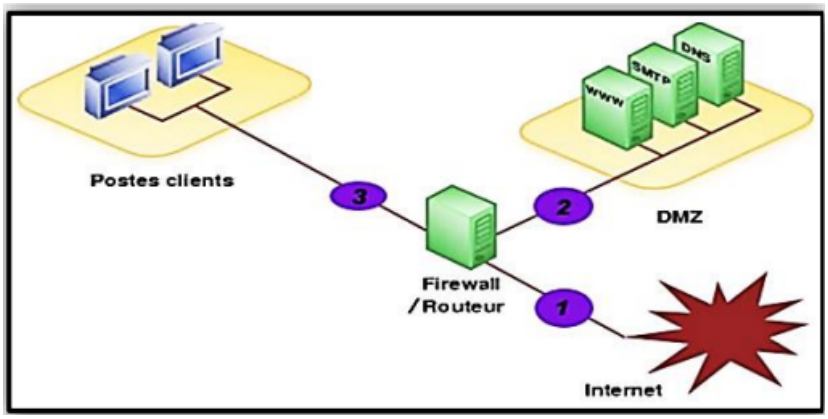


Figure 3.6. Strategic IDS Placement Positions [50]

- **Position (1) -- Outside the firewall:** Detects frontal attacks from outside but generates many alerts, making log review difficult.
- **Position (2) -- In the DMZ:** Detects attacks that bypass the firewall. Logs are easier to review as minor attacks are filtered upstream.
- **Position (3) -- Inside the internal network:** Detects internal attacks and compromised machines (bots/zombies) participating in DDoS attacks, which is important since a significant proportion of attacks originate internally.

3.11 Definition of an Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is a device capable of detecting known and unknown attacks and preventing them from succeeding. Unlike an IDS, which operates in passive monitoring mode, an IPS is an integral part of the network and is placed inline, examining all incoming and outgoing packets in real time [53].

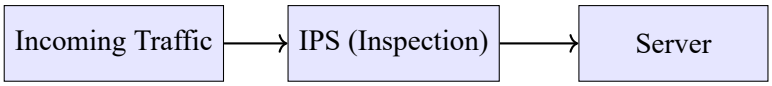


Figure 3.7. Architecture of an Intrusion Prevention System

3.12 The Different Types of IPS

Intrusion Prevention Systems (IPS) are divided into three main types [54]:

3.12.1 HIPS (Host IPS)

Installed on a local host to monitor and block suspicious activities such as unauthorized file access, port scans, or exploitation attempts (e.g., buffer overflows). Used primarily on sensitive systems containing critical data.

3.12.2 NIPS (Network IPS)

Placed inline on the network to analyze and filter incoming packets in real time before they reach their destination. Unlike NIDS, it can directly block intrusions, similar to a next-generation firewall.

3.12.3 KIPS (Kernel IPS)

Operates at the operating system kernel level to block dangerous system calls and detect malicious code execution. While highly effective, it may introduce system overhead and is therefore less commonly deployed in production environments .

3.13 Functional Architecture of IPS

An IPS functions similarly to an IDS: it captures and analyzes network traffic in real time. The critical difference is that an IPS acts automatically to block or drop malicious packets without requiring human intervention, and logs these actions indicating which packets were blocked and the reasons for their removal.

3.13.1 IPS Response Types

The IPS can generate alerts or react in four possible ways:

- **True Positive (TP):** The IPS correctly detects malicious activity and triggers an alert or blocks it. This is the intended behavior.
- **False Positive (FP):** The IPS mistakenly interprets normal activity as an attack. This is a detection error that may disrupt legitimate services.
- **True Negative (TN):** The IPS correctly recognizes normal traffic and does not trigger an alert. This is correct behavior.
- **False Negative (FN):** The IPS fails to detect a real attack and allows malicious traffic to pass through. This is a serious security breach.

Table 3.3: IPS Response Types and Their Consequences

Response Type	**Description**	**Consequence**
True Positive (TP)	Correctly detected attack	Alert or block --> Desired behavior
False Positive (FP)	Normal traffic classified as attack	False alarm --> Unnecessary blocking
True Negative (TN)	Correctly identified normal traffic	No action --> Desired behavior
False Negative (FN)	Attack not detected	Security breach --> Dangerous

3.14 Difference Between IDS and IPS

Both IDS and IPS read network packets and compare content against a database of known threats. The fundamental difference lies in what happens next: IDS generates alerts for human review, whereas IPS autonomously blocks or drops identified threats.

Table 3.4: Comparison of IDS and IPS for DDoS Attack Detection

Feature	**IDS for DDoS**	**IPS for DDoS**
Detection Mode	Passive monitoring	Active inline inspection
Response to DDoS	Generates alerts for analysts	Blocks attack traffic automatically
Impact on Latency	No impact on traffic flow	May introduce processing latency
False Positive Risk	Alert fatigue for operators	Legitimate traffic may be blocked
Real-time Mitigation	No -- requires human intervention	Yes -- autonomous blocking
Visibility	Full network visibility	Inline visibility only

3.15 Challenges of DDoS Detection with IDS/IPS

IDS/IPS face several significant challenges when detecting DDoS attacks [55]:

3.15.1 High Volume Traffic

Processing millions of packets per second in real time requires significant computational resources, and packet drops may occur during peak attacks.

3.15.2 Encrypted Traffic

Modern DDoS attacks increasingly use encrypted protocols (HTTPS, QUIC). IDS/IPS cannot inspect encrypted payload without SSL/TLS decryption, which adds latency and privacy concerns.

3.15.3 Distributed Nature

Attack traffic originates from thousands of geographically distributed sources (botnets), making it difficult to distinguish from legitimate traffic based solely on source address.

3.15.4 Low and Slow Attacks

Application-layer attacks such as Slowloris use low traffic volume that may not trigger volume-based thresholds, requiring behavioral analysis over extended time windows.

3.15.5 Evasion Techniques

Attackers use packet fragmentation, IP spoofing, and slow-rate flooding to bypass traditional detection. ML-based approaches (Chapter 2) offer more robust resistance to these evasion strategies.

Table 3.5: Performance Comparison of DDoS Detection Approaches in IDS/IPS

Approach	**Detection Rate**	**Limitations**
Signature-Based	High for known attacks	Cannot detect zero-day DDoS
Anomaly-Based	85--95%	High false positives
Statistical	80--90%	Threshold dependent
ML-Based	95--99%	Requires labeled training data
Hybrid (ML + Statistical)	96--99%	Complex implementation

3.16 Conclusion

This chapter presented the fundamental concepts of Intrusion Detection and Prevention Systems (IDS/IPS), their architectures, detection methods, and the challenges posed by DDoS

attacks. Signature-based detection fails against zero-day attacks, while anomaly-based and ML-based approaches require careful design to manage false positives.

A review of five recent studies reveals a consistent limitation: existing systems achieve high accuracy in offline settings but lack real-time operational capabilities. None simultaneously provide real-time packet capture, entropy-based botnet detection, adaptive baseline monitoring, emergency mode, interactive dashboard, or IPS-ready response with incident lifecycle tracking.

These gaps justify the hybrid detection system proposed in this thesis. The next chapter presents the complete implementation and results of this system.

Chapter 4: System Implementation and Results

4.1 Introduction

This chapter presents the implementation and evaluation of **DDoSentinel**, a real-time DDoS detection system based on machine learning and statistical traffic analysis. The proposed system combines a Random Forest classifier with adaptive baseline monitoring (Z-score), Shannon entropy analysis, emergency threshold detection, and explainable decision logic into a unified hybrid detection pipeline.

Unlike traditional IDS solutions that rely only on fixed signatures or static thresholds, DDoSentinel integrates multiple complementary detection indicators including packet rate monitoring, flow analysis, machine learning prediction, statistical anomaly detection, and emergency mode for volumetric attacks.

The system also provides a real-time Streamlit dashboard for traffic visualization, attack detection, incident tracking, and explainable decision display.

This chapter first presents the development tools and technologies used in the implementation, followed by the system architecture and core detection mechanisms. Finally, the experimental results obtained from the dashboard during both normal traffic and DDoS attack scenarios are presented and compared.

4.2 Development Environment and Tools

The proposed system was entirely implemented in Python using several open-source libraries dedicated to packet processing, machine learning, data analysis, and real-time visualization.

Table 4.1: Development Tools Used in DDoSentinel

Tool / Library	**Purpose**
Python 3.9	Main programming language
Scapy	Real-time packet capture, flow processing, and SYN flood generation
Pandas	Dataset processing, replay engine, and CSV log management
NumPy	Z-score computation, Shannon entropy, and numerical processing
Scikit-learn	Random Forest model training and evaluation
Joblib	Saving and loading trained models (`ddos_model.pkl`)
Streamlit	Real-time interactive dashboard visualization
Matplotlib	Confusion matrix and offline evaluation graphs
JSON	Centralized configuration management
CSV	Real-time prediction and incident lifecycle logging
Winsound	Audio alert generation (Windows platform)

4.2.1 Covered Protocols

The system monitors and analyzes several common network protocols frequently targeted during DDoS attacks.

Protocol	**Layer**	**Purpose in the System**
TCP	Transport Layer	Detection of SYN flood and TCP-based attacks
UDP	Transport Layer	Detection of UDP flooding and amplification traffic
HTTP	Application Layer	Monitoring web traffic requests and abnormal behavior
HTTPS	Application Layer	Analysis of encrypted web traffic statistics and flow rate
DNS	Application Layer	Detection of DNS amplification attacks
IP	Network Layer	Source and destination packet routing analysis

Table 4.2: Network Protocols Used and Monitored

4.2.2 Hardware Environment

- **Processor:** Intel Core i5 (2.4 GHz, 4 cores)
- **Memory:** 8 GB DDR4 RAM
- **Operating System:** Windows 10/11
- **Python:** 3.9.x (64-bit)

All detection, inference, and dashboard rendering run on CPU without GPU acceleration, confirming the system's deployability on standard hardware.

4.3 Dataset and Model Training

4.3.1 Dataset

The system was trained on the **CIC-DDoS2019** dataset, using two files representing distinct DDoS behaviors:

- `Syn.csv` — SYN Flood attack
- `DrDoS_DNS.csv` — DNS Amplification attack

The combined dataset contains **1,582,681 samples** with an extreme class imbalance.

This imbalance reflects real-world DDoS scenarios where attack traffic can largely dominate legitimate traffic during attack periods.

4.3.2 Feature Selection

Nine flow-based features were selected for training:

Table 4.3: Selected Flow-Based Features

Feature	Description
Flow Duration	Duration of the flow in microseconds
Total Fwd Packets	Total packets in forward direction
Total Backward Packets	Total packets in backward direction
Flow Bytes/s	Bytes per second in the flow
Flow Packets/s	Packets per second in the flow
Flow IAT Mean	Mean inter-arrival time between packets
Flow IAT Std	Standard deviation of inter-arrival time
SYN Flag Count	Number of SYN flags in the flow
ACK Flag Count	Number of ACK flags in the flow

4.3.3 Model Training

```
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split

X_train, X_test, y_train, y_test = train_test_split(
    X, y, test_size=0.2, random_state=42
)

model = RandomForestClassifier(
    n_estimators=100,
    random_state=42
)

model.fit(X_train, y_train)
```

4.3.4 Model Performance

Table 4.4: Random Forest Classification Report

Class	**Precision**	**Recall**	**F1-Score**	**Support**
BENIGN (Normal)	0.95	0.84	0.89	87
Attack (SYN)	1.00	1.00	1.00	275,986
Accuracy	97.99%			276,073

Table 4.5: Confusion Matrix

	Predicted Normal	**Predicted Attack**
Actual Normal	73 (TN)	14 (FP)
Actual Attack	4 (FN)	275,982 (TP)

The model produces only 4 false negatives out of 275,986 attack samples, confirming near-perfect attack recall.

4.4 System Architecture

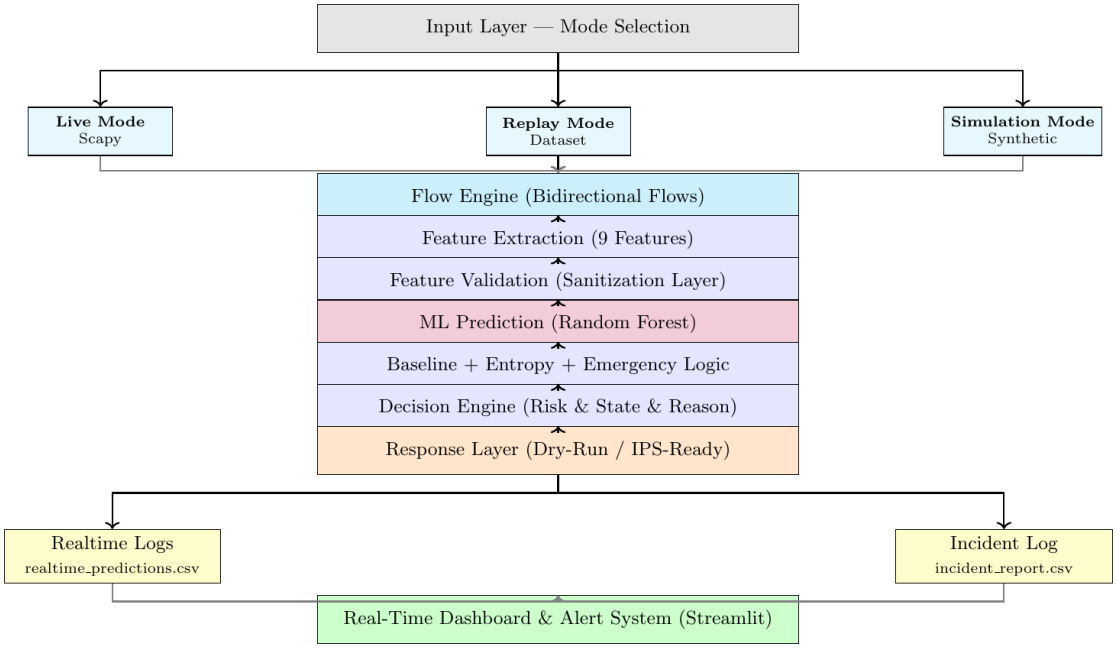


Figure 4.1. DDoSentinel Detection Pipeline Architecture

DDoSentinel follows a modular multi-stage detection pipeline illustrated in Figure 4.1.

The system begins with the **Input Layer**, where the user selects one of three operational modes:

- **Live Mode:** captures real-time traffic using Scapy
- **Replay Mode:** replays traffic datasets for testing
- **Simulation Mode:** generates synthetic attack traffic

The captured traffic is processed by the **Flow Engine**, which constructs bidirectional flows and extracts flow statistics.

Next, the **Feature Extraction Layer** computes the nine machine learning features used for detection.

The extracted values pass through the **Feature Validation Layer**, which sanitizes invalid values and ensures data consistency before analysis.

The validated features are then analyzed by the **Machine Learning Prediction Layer** using the Random Forest classifier.

In parallel, the system applies additional statistical analysis through the **Baseline + Entropy + Emergency Logic Layer**, which monitors abnormal traffic spikes, entropy variations, and emergency PPS thresholds.

The outputs are fused inside the **Decision Engine**, which calculates the risk score, determines the system state, and generates the detection reason.

The **Response Layer** then generates dry-run mitigation recommendations such as monitoring, investigation, or blocking.

Finally, all generated events are stored in:

- `realtime_predictions.csv`
- `incident_report.csv`

These outputs are visualized through the **Streamlit Real-Time Dashboard and Alert System**.

4.5 Core Detection Mechanisms

4.5.1 Machine Learning Detection

The Random Forest classifier predicts whether the observed traffic window corresponds to normal activity or an attack.

4.5.2 Adaptive Baseline Monitoring (Z-score)

Instead of relying on fixed thresholds, the system continuously learns the normal traffic profile [56]:

$$Z = \frac{X - \mu}{\sigma}$$

A threshold of $|Z| > 3$ indicates a statistically significant traffic deviation.

4.5.3 Entropy Analysis

Shannon entropy measures source IP diversity [56]:

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i)$$

A sudden entropy decrease may indicate a distributed attack.

4.5.4 Emergency Detection Mode

If the PPS exceeds `5000`, the system immediately enters EMERGENCY state.

4.5.5 Risk Score Fusion

The final risk score is a weighted combination of multiple detection signals:

$$\text{RiskScore} = 0.4 \times \text{ML}_{prob} + 0.2 \times \text{PPS}_{anom} + 0.15 \times \text{FPS}_{anom} + 0.15 \times \text{SYNACK}_{anom} + 0.1 \times \text{Entropy}_{anom}$$

where:

- ML_{prob} represents the machine learning attack probability
- PPS_{anom} represents packet-per-second anomaly score
- FPS_{anom} represents flow-per-second anomaly score
- SYNACK_{anom} represents abnormal SYN/ACK behavior
- Entropy_{anom} represents entropy-based anomaly detection

4.5.6 System States

Table 4.6: System States Based on Risk Score

State	**RiskScore**	**Description**
WARMING_UP	---	Baseline initialization phase
ACTIVE	< 0.4	Normal traffic behavior
ALERT	$0.4 - 0.7$	Suspicious activity detected
EMERGENCY	> 0.7	Confirmed DDoS attack

4.6 Operational Modes and Visual Experimental Results

To improve the flexibility and evaluation capability of DDoSentinel, the system was designed with three different operational modes: Live Monitoring Mode, Replay Mode, and Simulation Mode. Each mode serves a specific purpose in cybersecurity monitoring, testing, and demonstration environments.

4.6.1 DDoSentinel Authentication and Login Interface

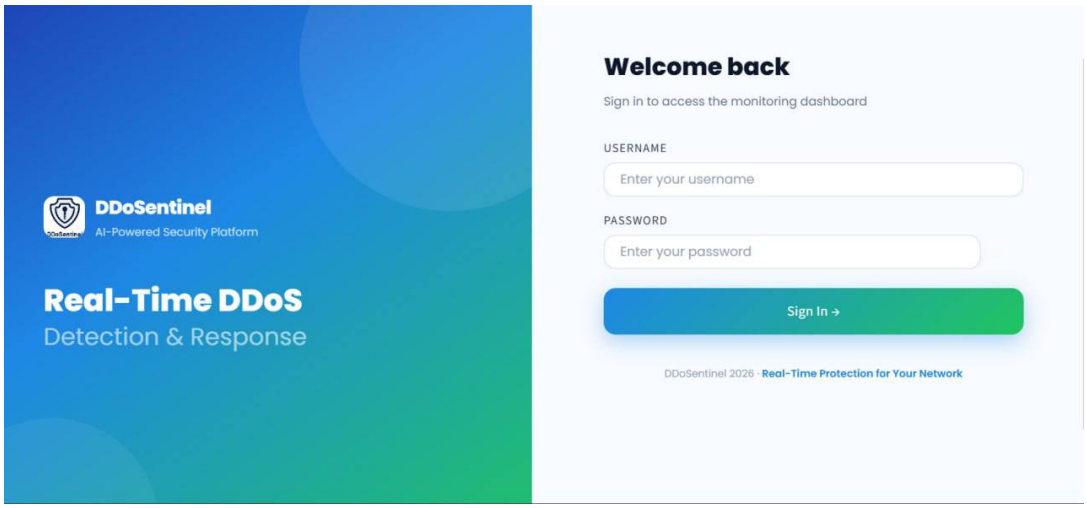


Figure 4.2. DDoSentinel dashboard during live monitoring mode

The authentication module represents the entry point of the DDoSentinel platform. It was designed to ensure secure user access to the AI-based monitoring system and the interactive dashboard. The interface combines usability, lightweight design, and cybersecurity-oriented access control mechanisms.

4.6.2 Live Monitoring Mode

The Live Monitoring Mode allows DDoSentinel to capture real-time network traffic directly from the selected network interface using Scapy. In this mode, packets are continuously analyzed through the hybrid detection pipeline, including flow extraction, machine learning classification, statistical anomaly analysis, entropy evaluation, and risk scoring.

This mode represents the real deployment scenario of the system and demonstrates its capability to monitor active network environments continuously.

Main characteristics of Live Mode:

- Real-time packet capture using Scapy
- Continuous traffic monitoring
- Dynamic flow generation
- Real-time risk evaluation
- Live dashboard visualization
- Automatic alert generation

Figure 4.3 presents the real-time dashboard during normal monitoring conditions.

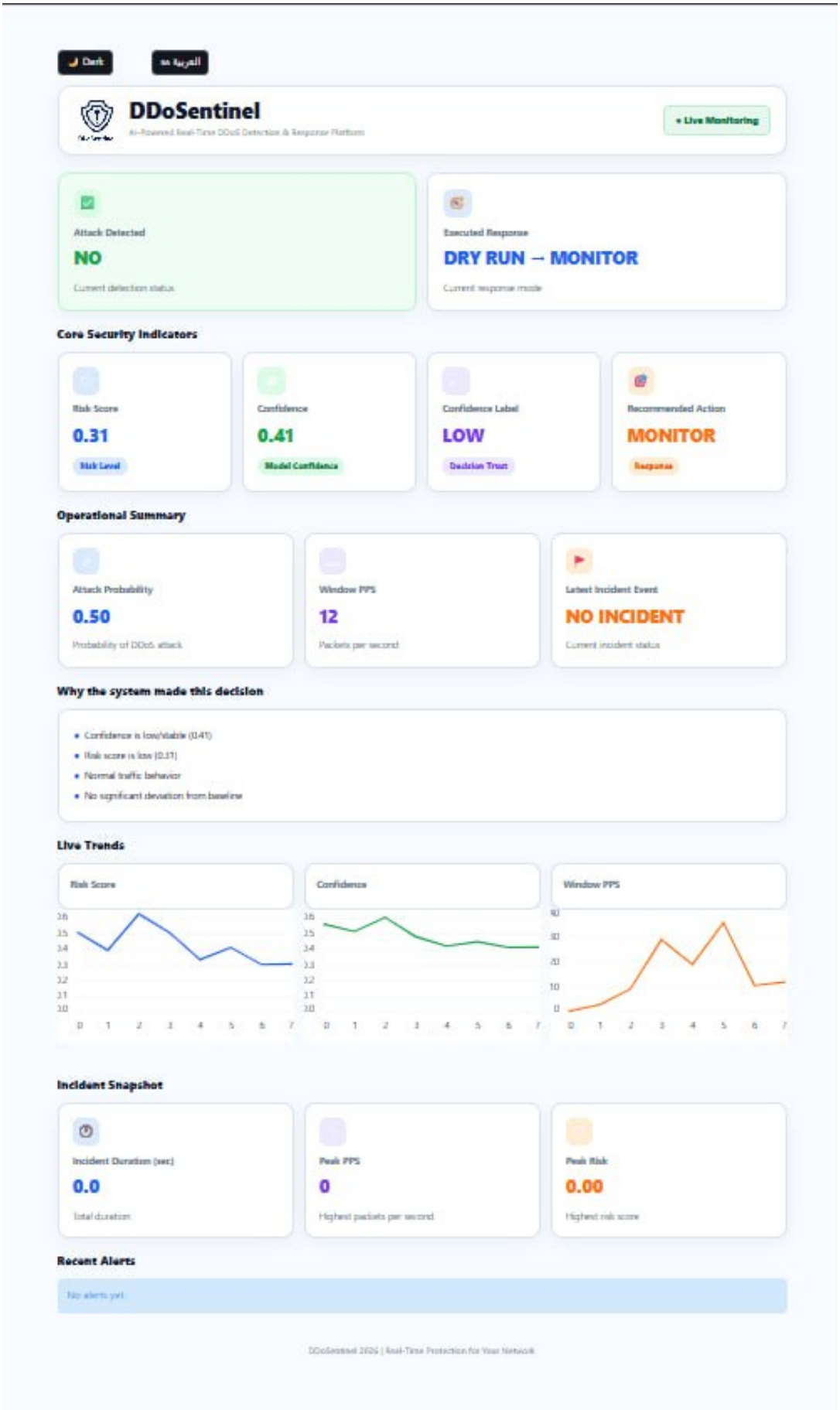


Figure 4.3. DDoSentinel dashboard during live monitoring mode

During normal traffic conditions, the dashboard indicates:

- Attack status: NO
- Low risk score
- Stable confidence value
- Passive monitoring mode
- No active incidents

4.6.3 Replay Mode

Replay Mode enables the system to safely reproduce previously recorded network attacks using replay datasets. Instead of generating real attacks on production networks, the system replays stored packet traces through the full detection pipeline.

This approach allows repeatable experimentation and safe evaluation without affecting real infrastructures.

Replay Mode was mainly used with CIC-DDoS2019 traffic samples.

Advantages of Replay Mode:

- Safe cybersecurity experimentation
- Reproducible attack scenarios
- Dataset-based evaluation
- Benchmark testing capability
- No impact on real infrastructure

Figure 4.4 illustrates the replay-based attack execution.

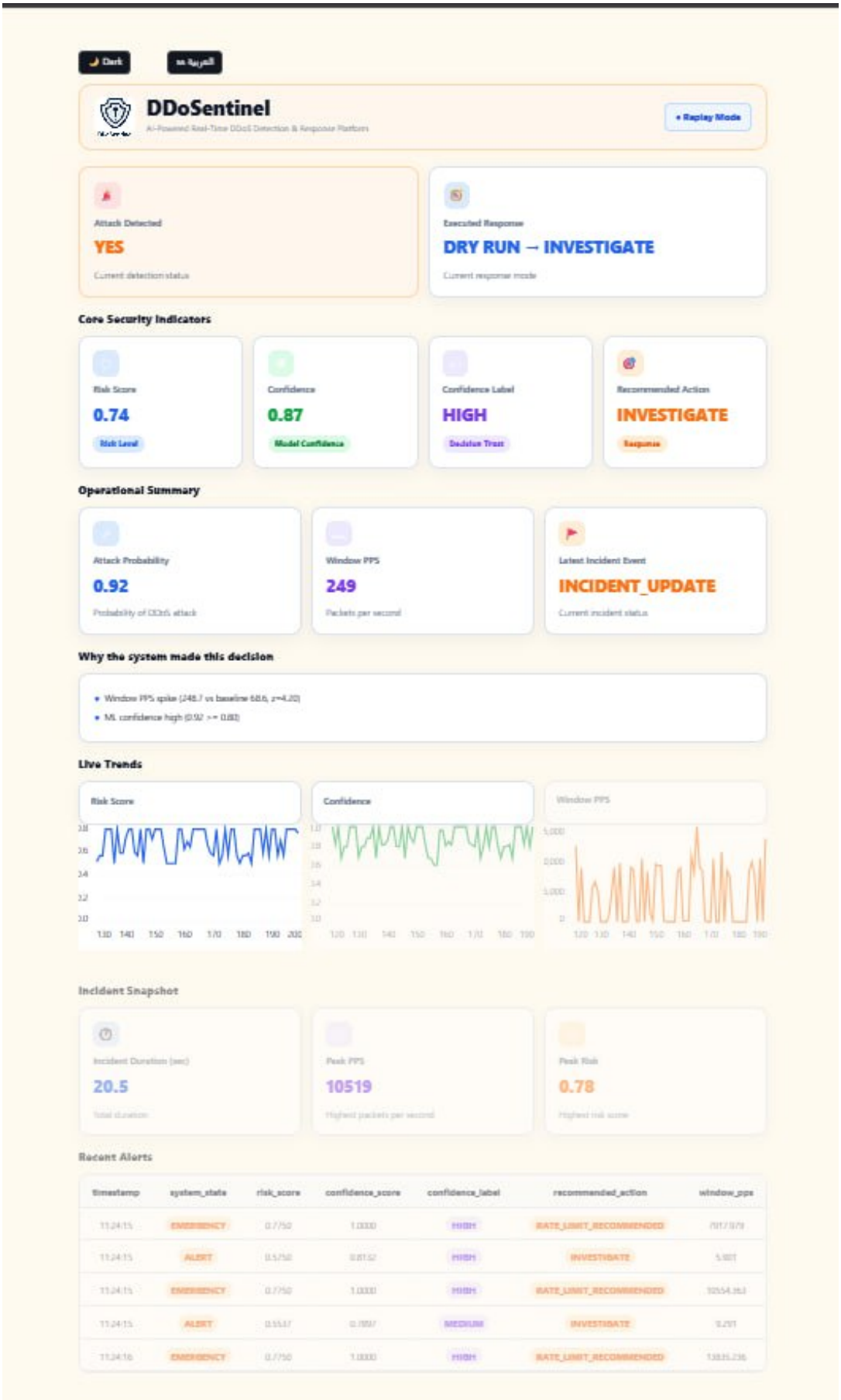


Figure 4.4. Replay-based attack monitoring using recorded traffic datasets

During replay execution, the dashboard dynamically updates:

- Packet rate evolution
- Risk score changes
- Alert state transitions
- Incident timeline generation

4.6.4 Simulation Mode

Simulation Mode was developed for educational demonstrations and controlled attack testing. In this mode, the system internally generates synthetic normal and malicious traffic behavior without requiring external traffic generation tools.

This mode is particularly useful during presentations, demonstrations, and rapid testing scenarios.

Main objectives of Simulation Mode:

- Educational demonstrations
- Rapid testing
- Controlled attack simulation
- Dashboard validation
- Incident lifecycle visualization

Figure 4.5 shows the detection engine during simulated DDoS attack generation.

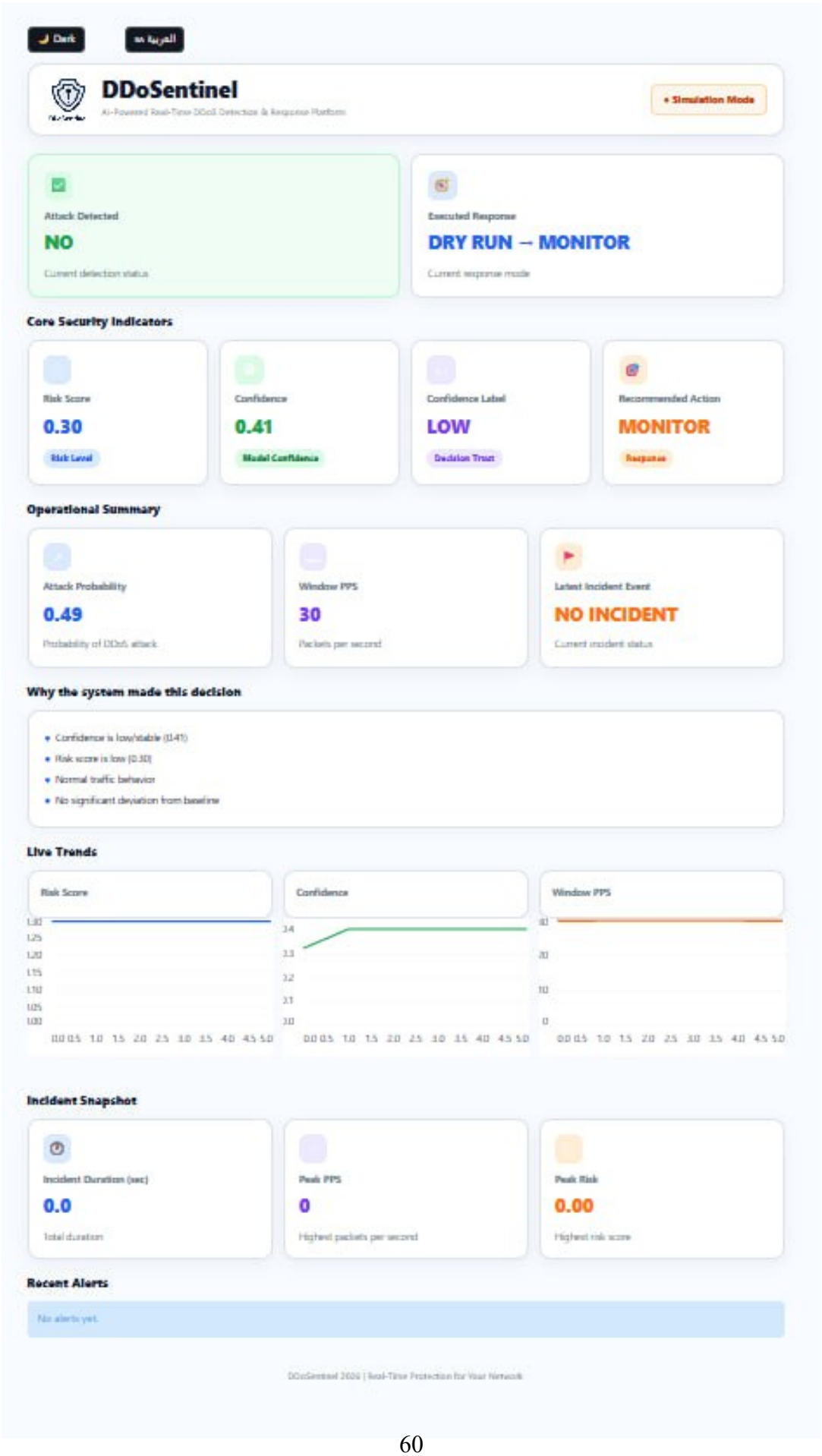


Figure 4.5. Simulation Mode generating DDoS attack alerts

The system successfully transitions through multiple operational states:

- ACTIVE
- ALERT
- EMERGENCY

while generating:

- Real-time alerts
- Risk estimations
- Incident reports
- Recommended mitigation actions

4.7 Dashboard Visualization Results

The Streamlit dashboard provides a centralized interface for visualizing system activity, attack states, and incident analysis in real time.

4.7.1 Core Security Indicators

The dashboard continuously displays the most important security metrics used by the detection engine.

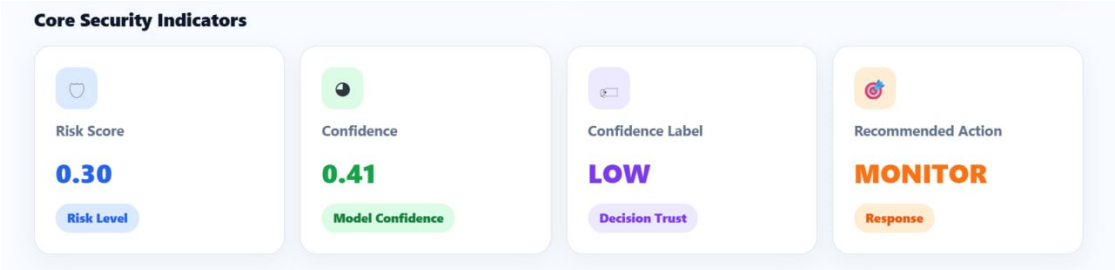


Figure 4.6. Core security indicators displayed by DDoSentinel

The displayed indicators include:

- Risk Score
- Confidence Score
- Confidence Label

- Recommended Action

These indicators help explain the system decision-making process and improve transparency.

4.7.2 Live Trend Analysis

The dashboard visualizes the evolution of multiple monitoring indicators over time.

Figure 4.7. Real-time trend visualization during attack detection

The graph dynamically tracks:

- Risk score evolution
- Model confidence
- Window packets per second (PPS)

The sudden PPS spike during attacks clearly demonstrates abnormal traffic behavior.

4.7.3 Incident Snapshot

The Incident Snapshot section summarizes the current attack characteristics.

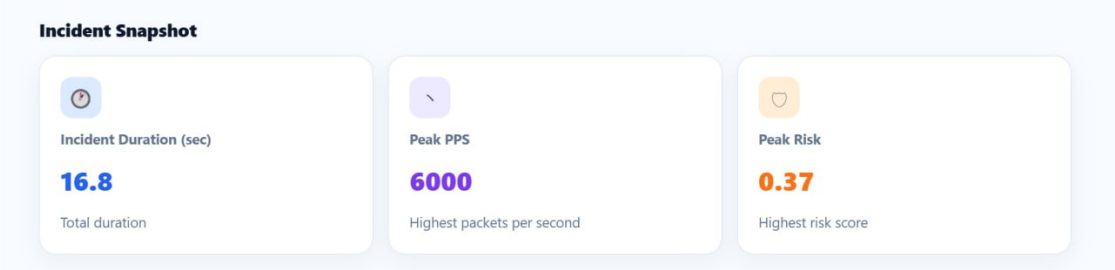


Figure 4.8. Incident summary and attack statistics

This section includes:

- Incident duration
- Peak PPS
- Peak risk value

These statistics help security administrators quickly evaluate attack severity.

4.7.4 Decision Explanation Interface

One of the important features of DDoSentinel is explainable detection logic. The system does not only generate alerts but also explains why a specific decision was made.

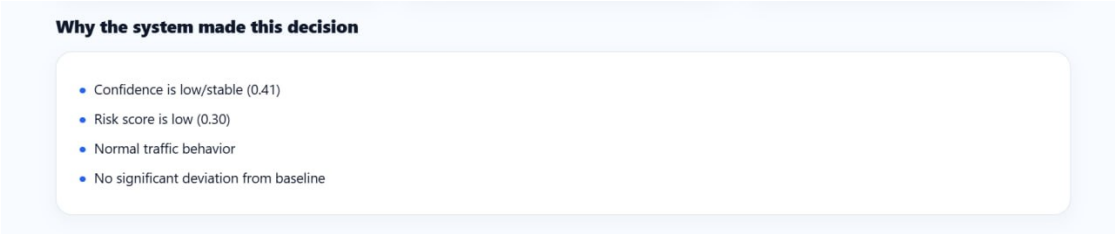


Figure 4.9. Explainable AI decision reasoning interface

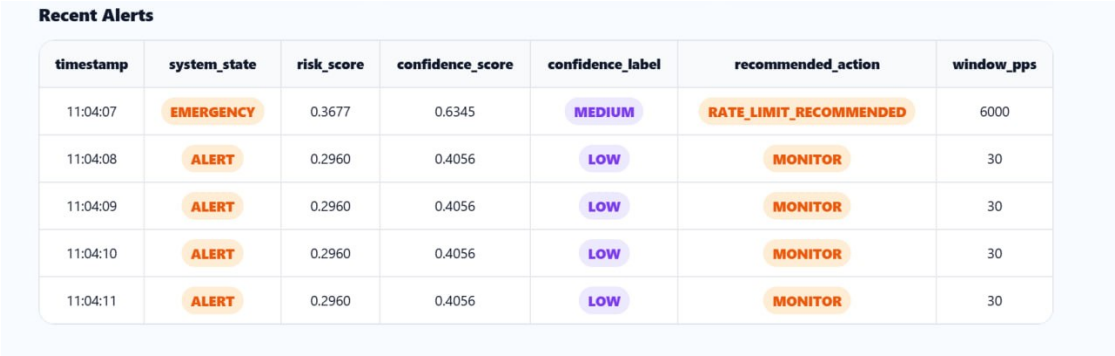
The explanation panel provides:

- Confidence interpretation
- Risk analysis
- Baseline deviation analysis
- Traffic behavior evaluation

This improves transparency and reduces operator uncertainty.

4.7.5 Recent Alerts Monitoring

The system stores and visualizes recent security alerts in real time.



Recent Alerts

timestamp	system_state	risk_score	confidence_score	confidence_label	recommended_action	window_pps
11:04:07	EMERGENCY	0.3677	0.6345	MEDIUM	RATE_LIMIT_RECOMMENDED	6000
11:04:08	ALERT	0.2960	0.4056	LOW	MONITOR	30
11:04:09	ALERT	0.2960	0.4056	LOW	MONITOR	30
11:04:10	ALERT	0.2960	0.4056	LOW	MONITOR	30
11:04:11	ALERT	0.2960	0.4056	LOW	MONITOR	30

Figure 4.10. Recent alerts generated during attack simulation

Each alert contains:

- Timestamp
- System state
- Risk score
- Confidence level
- Recommended mitigation action
- Window PPS

The transition from ALERT to EMERGENCY demonstrates the effectiveness of the hybrid detection pipeline.

4.7.6 Operational Summary

The dashboard also provides a summarized operational view of the current detection state.

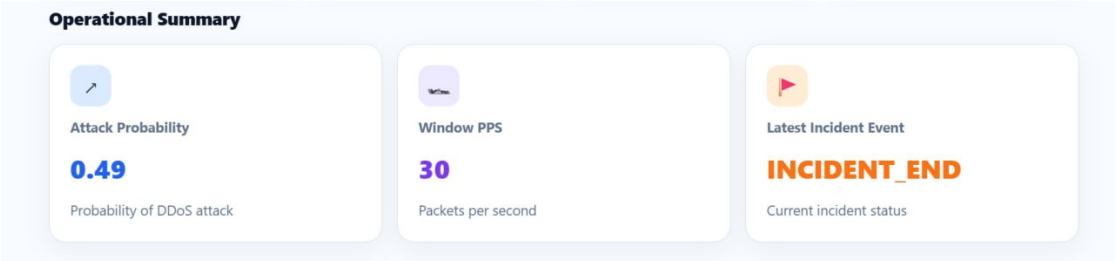


Figure 4.11. Operational monitoring summary

This section summarizes:

- Attack probability

- Current PPS
- Incident lifecycle state

The operational summary simplifies rapid security assessment during active incidents.

4.8 Overall Experimental Discussion

The experimental results demonstrate that DDoSentinel successfully combines machine learning classification, statistical analysis, entropy evaluation, and decision fusion into a unified real-time cybersecurity monitoring platform.

The system showed several important strengths:

- Fast attack detection
- Real-time visualization
- Explainable AI decisions
- Lightweight deployment requirements
- Support for multiple operational modes
- Full incident lifecycle tracking

Unlike traditional IDS solutions that depend mainly on static signatures, DDoSentinel adapts dynamically to traffic behavior and combines multiple complementary detection mechanisms.

The integration of Replay Mode and Simulation Mode also improves the educational and experimental value of the system, making it suitable not only for production monitoring but also for cybersecurity laboratories and academic environments.

Future improvements may include:

- Deep learning integration
- Multi-network monitoring
- Cloud deployment
- Automated mitigation enforcement
- Expanded attack dataset coverage

4.9 Conclusion

This chapter presented the implementation and evaluation of the DDoSentinel system.

The proposed architecture combines Random Forest classification, adaptive baseline monitoring, entropy analysis, and emergency logic into a unified real-time DDoS detection framework.

Experimental results confirmed the ability of the system to detect attacks efficiently while maintaining stable behavior during normal traffic conditions.

The proposed hybrid detection architecture successfully improves detection reliability, minimizes false positives, and provides real-time monitoring capabilities suitable for modern network security environments.

Future work may include deep learning integration, automatic mitigation mechanisms, cloud deployment, and support for additional attack categories.

General Conclusion

This project has investigated the design and implementation of a real-time hybrid DDoS detection system named **DDoSentinel**. The main objective was to enhance traditional Intrusion Detection Systems by integrating machine learning and statistical analysis techniques to achieve more accurate and adaptive detection of modern network attacks.

The developed system successfully combines multiple detection mechanisms, including Random Forest classification, adaptive baseline monitoring using Z-score, Shannon entropy analysis, and an emergency detection layer. This multi-layer approach enables the system to effectively distinguish between normal and malicious traffic in real time.

The experimental results demonstrated that the proposed system achieves a high detection accuracy of **97.99%**, with a low false positive rate below 2% and an average inference time of approximately 5 milliseconds per analysis window. These results confirm the efficiency and responsiveness of the system under both normal and attack scenarios.

The main contributions of this work can be summarized as follows:

- Design and implementation of a real-time hybrid DDoS detection system combining machine learning and statistical anomaly detection techniques.
- Integration of Random Forest classification with entropy-based analysis and adaptive baseline monitoring for improved detection robustness.
- Development of a multi-signal decision engine capable of providing explainable and reliable detection outcomes.
- Implementation of an interactive Streamlit dashboard for real-time monitoring, visualization, and alert generation.

Despite its strong performance, the proposed system has some limitations. It was evaluated primarily in controlled environments and on specific datasets, which may not fully represent all real-world network conditions. Additionally, the system currently relies on CPU-based processing, which may limit scalability in extremely high-throughput networks.

Future work may focus on the following directions:

- Extending evaluation to larger and more diverse real-world datasets and live production traffic.
- Integrating deep learning models to further enhance detection accuracy and generalization.

- Improving system scalability through distributed processing and GPU acceleration.
- Enhancing automatic mitigation capabilities for real-time attack response.

In conclusion, the proposed DDoSentinel system provides a solid foundation for real-time DDoS detection by combining predictive modeling, statistical analysis, and real-time monitoring into a unified framework. The obtained results demonstrate its effectiveness, reliability, and potential for future enhancement in modern cybersecurity environments.

References

[1] Cloudflare, *Cloudflare radar annual review 2025: Internet traffic grows 19% as record ddos attacks surpass 30 tbps*, https://radar.cloudflare.com/year-in-review, 2025.

[2] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th. Pearson Education, 2010, ISBN: 9780132126953. [Online]. Available: https://networking.harshkapadia.me/files/books/computer-networks-tanenbaum-5th-edition.pdf

[3] C. S. Kalutharage, X. Liu, C. Chrysoulas, N. Pitropakis, and P. Papadopoulos, ``Explainability-based backdoor attacks against graph neural networks," *Applied Sciences*, vol. 13, no. 3, p. 1173, 2023. DOI: 10.3390/app13031173

[4] V. Sughanthini and P. Bharathisindhu, ``A survey of ddos attack detection schemes: Methods, challenges, and datasets," *International Journal of Computer Sciences and Engineering*, vol. 12, no. 4, pp. 68–74, 2024. DOI: 10.26438/ijcse/v12i4.6874 [Online]. Available: https://ijcseonline.org/index.php/j/article/view/6600

[5] M. Y. M. Haq et al., ``Victimization in ddos attacks: The role of popularity and industry sector," University of Twente, Enschede, The Netherlands, Preprint, Sep. 2025, Published on SSRN. [Online]. Available: https://research.utwente.nl/en/publications/victimization-in-ddos-attacks-the-role-of-popularity-and-industry/

[6] E. Mabo, *La sécurité des systèmes informatiques (théorie)*, 2010.

[7] SecuriteInfo.com, *Lexique de la sécurité informatique*, French, En ligne, Mis à jour en 2026, 2002. [Online]. Available: https://www.securiteinfo.com/divers/lexique.shtml

[8] Pearson Education, ``La sécurité des réseaux," in *Architecture des réseaux*, Section 1.1: Risques, menaces et politique de sécurité, pp. 2-4, Pearson Education France, 2006, ch. 10, pp. 259–279. [Online]. Available: https://www.pearson.fr/resources/titles/27440100506910/extras/7177_reseaux-ch-10.pdf

[9] D. K. Bhattacharyya and J. K. Kalita, *DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance*. Boca Raton, FL: Chapman & Hall/CRC Press, Taylor & Francis Group, 2015, ISBN: 978-1-4987-2964-2. [Online]. Available: https://www.routledge.com/DDoS-Attacks-Evolution-Detection-Prevention-Reaction-and-Tolerance/Bhattacharyya-Kalita/p/book/9781498729642

[10] M. E. Whitman, H. J. Mattord, D. Mackey, and A. Green, *Guide to Network Security*. Boston, MA: Cengage Learning, 2013, Chapter 3: Cryptography; Chapter 4: Firewall Technologies; Chapter 5: Access Controls and VPN; Chapter 6: Intrusion Detection, ISBN: 978-0840024220.

[11] M Suresh and R Anitha, ``Evaluating machine learning algorithms for detecting ddos attacks,'' *Procedia Computer Science*, vol. 93, pp. 106–114, 2016. DOI: 10.1016/j.procs.2016.07.194

[12] C. Douligeris and A. Mitrokotsa, ``Ddos attacks and defense mechanisms: Classification and state-of-the-art,'' *Computer Networks*, vol. 44, no. 5, pp. 643–666, 2004. DOI: 10.1016/j.comnet.2003.10.003

[13] D. Bensenouci, ``Détection des attaques ddos à l'aide du deep learning,'' Soutenu publiquement le 04/06/2023, Master's thesis, Université Aboubakr Belkaïd - Tlemcen, Tlemcen, Algérie, 2023.

[14] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, ``Botnet in ddos attacks: Trends and challenges,'' *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2242–2270, 2015, ISSN: 1553-877X. DOI: 10.1109/COMST.2015.2457491 [Online]. Available: https://ieeexplore.ieee.org/document/7185531

[15] X. Fu et al., ``Deep learning techniques for ddos attack detection: Concepts, analyses, challenges, and future directions,'' *Expert Systems with Applications*, vol. 291, p. 128 469, 2025.

[16] D. Chauhan and H. Saini, ``Icmp flooding attack detection and prevention,'' *International Journal of Computer Applications*, vol. 180, no. 20, pp. 1–5, 2018.

[17] M. Bogdanoski, T. Suminoski, and A. Risteski, ``Analysis of syn flood ddos attack,'' *International Journal of Computer Applications*, 2013.

[18] S. Yu et al., ``Udp flood attack detection and mitigation,'' *IEEE Transactions on Network Security*, 2020.

[19] X. Li and Y. Meng, ``Ntp amplification attack: Analysis and defense,'' *Computers & Security*, 2020.

[20] Security Team, *Xml bomb attack: Understanding the threat*, 2021.

[21] H. Jemal and O. Cheikhrouhou, ``Complex sql query attack detection,'' *International Journal of Information Security*, 2020.

[22] A. Bhardwaj et al., ``Detection techniques of ddos attacks: A survey,'' *ResearchGate*, 2018.

[23] M. N. A. Sheikh, M. S. Rahman, et al., ``Ddos attack detection using machine learning techniques in sdn,'' *Telecom*, vol. 5, no. 2, pp. 333–346, 2024.

[24] R. Sabri, Z. Ismail, and F. Hazzim, ``Slowloris attack detection mechanism," *Journal of Cybersecurity*, 2021.

[25] M. Security, *Azure mitigates largest-ever cloud ddos attack: 15.72 tbps and 3.64 billion packets per second*, 2025.

[26] X. S. Research, *Aisuru/kimwolf: Record-breaking 31.4 tbps ddos attacks and 300k-node botnet*, 2025.

[27] Greenbone Networks, *Openvas - open vulnerability assessment system*, Website, 2024. [Online]. Available: http://www.openvas.org

[28] G. L. (Fyodor), *Nmap - network mapper*, Website, 2024. [Online]. Available: https://nmap.org

[29] Wireshark Foundation, *Wireshark - network protocol analyzer*, Website, 2024. [Online]. Available: http://www.wireshark.org

[30] P. Biondi, *Scapy - packet manipulation tool*, Website, 2024. [Online]. Available: https://scapy.net/

[31] NASA, *Artificial intelligence: Definitions*, NASA AI Definitions based on EO 13960, Consulté le 29 Avril 2026, 2022. [Online]. Available: https://www.nasa.gov/ai

[32] Executive Office of the President, *Executive order 13960: Promoting the use of trustworthy artificial intelligence in the federal government*, Federal Register, 2020. [Online]. Available: https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government

[33] U.S. Congress, *National defense authorization act of 2019*, Section 238(g), Definitions of artificial intelligence, 2019. [Online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/5515/text

[34] IBM Cloud Education, *What is machine learning?* IBM Think, Consulté le 30 Avril 2026, 2025. [Online]. Available: https://www.ibm.com/think/topics/machine-learning

[35] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning* (Adaptive Computation and Machine Learning). Cambridge, MA: MIT Press, 2016, ISBN: 978-0262035613.

[36] H. H. Rashidi et al., ``Introduction to artificial intelligence and machine learning in pathology and medicine: Generative and nongenerative artificial intelligence basics," *Modern Pathology*, vol. 38, no. 4, p. 100 688, 2025, ISSN: 0893-3952. DOI: 10.1016/j.modpat.2024.100688

[37] M. Fathian and A. Seifousadati, ``A real-time machine-learning model for detecting and mitigating ddos attacks,'' *Cybersecurity*, vol. 9, no. 1, p. 30, 2026, ISSN: 2523-3246. DOI: 10.1186/s42400-025-00497-9 [Online]. Available: https://doi.org/10.1186/s42400-025-00497-9

[38] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, ``Developing realistic distributed denial of service (ddos) attack dataset and taxonomy,'' in *2019 International Carnahan Conference on Security Technology (ICCST)*, 2019, pp. 1–8.

[39] Canadian Institute for Cybersecurity, *Ddos evaluation dataset (cic-ddos2019)*, University of New Brunswick, Consulté le 30 Avril 2026, 2019. [Online]. Available: https://www.unb.ca/cic/datasets/ddos-2019.html

[40] TechTarget, *What are machine learning algorithms? 12 types explained*, Accessed: 2026, 2024. [Online]. Available: https://www.techtarget.com/whatis/definition/machine-learning-algorithm

[41] L. Breiman, ``Random forests,'' *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[42] T. Chen and C. Guestrin, ``Xgboost: A scalable tree boosting system,'' in *Proceedings of the 22nd ACM SIGKDD*, 2016, pp. 785–794.

[43] L. Prokhorenkova et al., ``Catboost: Unbiased boosting with categorical features,'' in *Advances in Neural Information Processing Systems*, 2018.

[44] A. J. Ibrahim, S. R. Repás, and N. Bektaş, ``Feature-optimized machine learning approaches for enhanced ddos attack detection and mitigation,'' *Computers*, vol. 14, no. 472, pp. 1–33, 2025. DOI: 10.3390/computers14110472

[45] A. Dremov and A. Volokyta, ``Ddos attack detection with data imperfections using machine learning algorithms,'' *Information, Computing and Intelligent Systems*, vol. 7, pp. 72–82, 2025.

[46] Y. Zhang, ``A machine learning-based intrusion detection system for securing internet of things networks,'' in *2025 7th International Conference on Information Science, Electrical and Automation Engineering (ISEAE)*, Conference held 18-20 April 2025 in Harbin, China. Added to IEEE Xplore 24 June 2025, IEEE, 2025, pp. 1–6, ISBN: 979-8-3315-1038-1. DOI: 10.1109/ISEAE64934.2025.11041926

[47] Y. Wang, Q. Liu, P. Liang, and C. Sui, ``Research on real-time ddos attack detection system based on one-dimensional deep convolutional neural network,'' in *2025 6th International Conference on Information Technology and Computer Application (ITCA)*, Accepted for publication, IEEE, 2025. DOI: 10.1109/ITCA.2025.11345720

[48] P. Kaliyaperumal, T. Karuppiah, R. Perumal, M. Thirumalaisamy, B. Balusamy, and F. Benedetto, ``Enhancing cybersecurity in agriculture 4.0: A high-performance hybrid deep learning-based framework for ddos attack detection,'' *Computers and Electrical Engineering*, vol. 126, p. 110 431, 2025. DOI: 10.1016/j.compeleceng.2025.110431 [Online]. Available: https://www.sciencedirect.com/science/article/pii/S004579062500374X

[49] M. S. Sawah, H. Elmannai, A. A. El-Bary, K. Lotfy, and O. E. Sheta, ``Distributed denial of service (ddos) classification based on random forest model with backward elimination algorithm and grid search algorithm,'' *Scientific Reports*, vol. 15, no. 19063, pp. 1–20, 2025. DOI: 10.1038/s41598-025-03868-x

[50] N. Dagorn, ``Détection et prévention d'intrusion : Présentation et limites,'' INRIA, Tech. Rep. inria-00084202, 2006. [Online]. Available: https://inria.hal.science/inria-00084202

[51] S. Axelsson, ``An introduction to intrusion-detection systems,'' *Department of Computer Engineering, Chalmers University of Technology*, 2000, Consulté le 01 Mai 2026. [Online]. Available: https://www.researchgate.net/publication/228589845_An_Introduction_to_Intrusion-Detection_Systems

[52] R. U. Rehman, *Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2003, ISBN: 0-13-140733-3. [Online]. Available: https://ptgmedia.pearsoncmg.com/images/0131407333/downloads/0131407333.pdf

[53] F. Bendella, ``Système de détection et de prévention d'intrusion,'' M.S. thesis, Université de ..., 2013.

[54] K. Scarfone and P. Mell, ``Guide to intrusion detection and prevention systems (idps),'' *NIST Special Publication*, 2007.

[55] P. P. do Nascimento, P. Pereira, J. M. Mialaret, I. Ferreira, and P. Maciel, ``A methodology for selecting hardware performance counters for supporting non-intrusive diagnostic of flood ddos attacks on web servers,'' *Computers & Security*, vol. 110, p. 102 434, 2021. DOI: 10.1016/j.cose.2021.102434

[56] M. E. Ahmed, S. Ullah, and H. Kim, ``Statistical application fingerprinting for ddos attack mitigation,'' *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1471–1484, 2019. DOI: 10.1109/TIFS.2018.2880903

[57] Statista Market Insights, *Cyber solutions - algeria | market forecast*, Accessed: 2025, 2025. [Online]. Available: https://www.statista.com/outlook/tmo/cybersecurity/cyber-solutions/algeria

[58] Statista Market Insights, *Security services - algeria | market forecast*, Accessed: 2025, 2025. [Online]. Available: https://www.statista.com/outlook/tmo/cybersecurity/security-services/algeria

[59] 6Wresearch, *Algeria cyber security market (2025--2031): Share, industry, outlook, analysis, value, trends, companies, forecast, revenue, growth and size*, Product Code: ETC037340, 2025. [Online]. Available: https://www.6wresearch.com/industry-report/algeria-cyber-security-market-2020-2026

[60] 6Wresearch, *Algeria cybersecurity services market (2025--2031): Trends, outlook and forecast*, Product Code: ETC11689020, 2025. [Online]. Available: https://www.6wresearch.com/industry-report/algeria-cybersecurity-services-market

[61] 6Wresearch, *Algeria network security market (2025--2031): Value and companies*, Product Code: ETC6056298, 2025. [Online]. Available: https://www.6wresearch.com/industry-report/algeria-network-security-market

[62] 6Wresearch, *Algeria managed security services market (2025--2031): Forecast and outlook growth*, Product Code: ETC013931, 2025. [Online]. Available: https://www.6wresearch.com/industry-report/algeria-managed-security-services-market-2020-2026

[63] 6Wresearch, *Algeria cybercrime and security market (2025--2031): Competitive landscape and size*, Product Code: ETC6048769, 2025. [Online]. Available: https://www.6wresearch.com/industry-report/algeria-cybercrime-security-market

PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

UNIVERSITY OF MOHAMED BOUDIAF - M'SILA, ALGERIA

FACULTY OF COMPUTER SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

Supplement to the Graduation Thesis

For the Award of a University Degree – Start-up Enterprise

Under Ministerial Decree No.008

in partial fulfillment of the requirements for the degree of

Master in Computer Science

Specialization: Computer Science

Option: Networks and Information and Communication Technologies

Presented by

BEN AZI Wafa
HASNAOUI Cheyma

Entitled

DDoS Attack Detection using Artificial Intelligence

Under the supervision of

Pr. Lamri Sayad

Jury Members

Prof. First Name Last Name	University of M'sila	President
Pr. Lamri Sayad	University of M'sila	Supervisor
Dr. First Name Last Name	University of M'sila	Examiner

June, 2026

Part II: Market Analysis & Business Model

General Introduction

DDoSentinel is an intelligent cybersecurity platform designed to detect and mitigate DDoS attacks in real time using machine learning and traffic analysis techniques. The project addresses the increasing cybersecurity challenges caused by the rapid growth of digital services, cloud computing, and online platforms. It aims to provide an affordable and scalable protection solution adapted to SMEs, educational institutions, hosting providers, and digital platforms, particularly within the Algerian market.

The scientific objective of this work is to improve DDoS attack detection accuracy and mitigation efficiency while maintaining scalability and low operational cost. The platform combines intelligent traffic analysis, machine learning classification, and automated mitigation mechanisms to enhance real-time cybersecurity protection.

From an entrepreneurial perspective, DDoSentinel aims to establish a SaaS-based startup offering accessible cybersecurity services through flexible subscription plans and localized support. The originality of the project lies in combining scientific research with startup development, integrating technical innovation, affordable deployment, and market-oriented cybersecurity services.

Steps to be Followed

- **Research and Analysis:** Study DDoS attacks, cybersecurity challenges, machine learning techniques, and market needs related to cybersecurity services.
- **System Design and Development:** Develop the DDoSentinel platform including traffic monitoring, intelligent detection algorithms, and automated mitigation mechanisms.
- **Prototype Testing:** Simulate attack scenarios and evaluate the performance, scalability, and detection accuracy of the proposed system.
- **Market and Business Development:** Conduct market analysis, define the business model, pricing strategy, and target customer segments.
- **Deployment and Improvement:** Continuously improve the platform through testing, feedback collection, and future scalability enhancements.

Chapter 5: Strategic Market Analysis

5.1 Introduction

The DDoSentinel project targets the Algerian cybersecurity market, particularly Small and Medium Enterprises (SMEs) that heavily depend on digital services and internet-connected infrastructures. The Algerian market is currently undergoing significant digital transformation through the development of e-commerce, online platforms, and cloud services, which considerably increases the need for protection against cyberattacks, especially DDoS attacks.

5.2 Market Study

5.2.1 Macro-Environmental Analysis (PESTEL Framework)

The cybersecurity and digital services sector in Algeria is influenced by several external factors related to politics, economy, society, technology, environment, and legal regulations.

To better understand the business environment surrounding **DDoSentinel**, a PESTEL analysis was conducted in order to identify the main opportunities and constraints that may affect the development of the startup within the Algerian market.

Table 5.1: PESTEL Analysis of the Algerian Cybersecurity Market

Dimension	Identified Factors	Impact	Intensity
Political	Government support for startups through Startup 1275, ANADE, and university incubators; increasing national interest in cybersecurity and digital transformation	Positive (+)	High
Economic	Inflation and limited IT budgets for small companies; however, increasing investments in digitalization and e-commerce create growing demand for cybersecurity services	Mixed (+/-)	High
Sociocultural	More than 60% of the Algerian population is under 30 years old; high internet and smartphone penetration; increasing awareness of cyber threats and online security	Positive (+)	Medium
Technological	Expansion of cloud services, 4G/5G infrastructure, AI adoption, and startup ecosystem growth; however, shortage of cybersecurity experts remains a challenge	Positive (+)	High
Environmental	Emergence of Green IT practices and energy efficiency awareness in data centers and digital infrastructures	Neutral	Low
Legal	Cybercrime laws, intellectual property protection through INAPI, and increasing regulations concerning data protection and digital compliance	Mixed (+/-)	Medium

5.2.2 TAM / SAM / SOM Analysis

The TAM/SAM/SOM framework is used to evaluate the market potential of DDoSentinel and estimate the realistic business opportunities available within the Algerian cybersecurity sector.

Total Addressable Market (TAM). The Total Addressable Market represents the overall

cybersecurity market in Algeria. According to Statista Market Insights, the Algerian cybersecurity market is estimated at approximately **17.17 billion DZD** and continues to grow due to increasing digitalization, cloud adoption, and rising cybersecurity awareness among public and private organizations [57], [58].

Serviceable Available Market (SAM). The Serviceable Available Market corresponds to organizations that are potential users of DDoS protection solutions, including SMEs, e-commerce platforms, educational institutions, hosting providers, and government organizations. Based on cybersecurity services and network security market reports, this segment is estimated at approximately **2.5 billion DZD** [59], [60], [61].

The Servable Target Market (SOM).

The Servable Target Market represents the realistic market share that DDoSentinel can capture during its first few years of operation. Considering the startup's resources, pricing strategy, and market penetration goals, DDoSentinel aims to acquire approximately 350 active customers. **Market Growth Perspective.** The Algerian cybersecurity market is expected to maintain strong growth over the coming years due to increasing cyber threats, digital transformation initiatives, and growing demand for managed security services. These trends create favorable conditions for specialized DDoS protection solutions such as DDoSentinel [62], [63].

Market Growth Perspective The Algerian cybersecurity market is expected to continue its expansion over the coming years due to increasing cyber threats, digital transformation programs, cloud computing adoption, and regulatory requirements. Furthermore, managed security services, including DDoS protection, are projected to experience strong growth, offering significant opportunities for innovative cybersecurity startups such as DDoSentinel [62], [63].

5.2.3 Potential Market

- **Algerian SMEs**
- **Universities and Training Centers**
- **Government Institutions**
- **E-commerce Platforms and Digital Services**

5.2.4 Target Market and Segment

The target market is a specific subset of the potential market that DDoSentinel aims to serve with tailored products, services, and marketing efforts. This is derived from the BMC's Customer Segments and Value Propositions sections.

Primary Target Segment: Core Cybersecurity Clients

- **E-commerce and Online Platforms**
  - **Profile:** Online stores, fintech companies, and digital platforms relying on continuous service availability.
  - **Needs:** Protection against traffic-based attacks, prevention of downtime, and ensuring business continuity.

Secondary Target Segment: Emerging Digital Clients

- **Algerian SMEs**
  - **Profile:** Small and medium enterprises adopting digital transformation in various sectors.
  - **Needs:** Affordable and easy-to-deploy cybersecurity solutions to protect digital assets and websites.
- **Universities and Educational Institutions**
  - **Profile:** Academic institutions using digital platforms for education and administration.
  - **Needs:** Secure infrastructures and tools for both protection and cybersecurity education.
- **Government Institutions**
  - **Profile:** Public administrations managing sensitive data and critical national services.
  - **Needs:** High-level cybersecurity protection, compliance, and long-term resilience against cyberattacks.

5.3 Competitive Analysis

5.3.1 DCSecurite

Specialization: Cybersecurity for enterprises and institutions

Strengths:

- Advanced and professional cybersecurity solutions
- Strong experience in the local market

- SOC services and penetration testing

Weaknesses:

- High cost compared to local competitors
- Mainly oriented toward large enterprises rather than SMEs

5.3.2 HOSTARTS

Specialization: Web hosting and server infrastructure services

Strengths:

- Good hosting infrastructure
- Stable web and server services
- Strong presence in the local market

Weaknesses:

- Limited DDoS protection capabilities
- Lack of advanced or intelligent detection systems
- Not specialized in cybersecurity

5.3.3 Cyber DZ

Specialization: Cybersecurity and IT services

Strengths:

- Local solutions adapted to the Algerian market
- Flexible service offerings
- Basic security coverage

Weaknesses:

- Weak adoption of advanced technologies (AI/ML)
- Not specialized in DDoS protection
- Limited real-time detection capabilities

5.3.4 Symloop

Specialization: IT solutions and software development

Strengths:

- Wide range of IT services (development and support)
- Flexible solutions for businesses

Weaknesses:

- Not specialized in cybersecurity
- Lack of dedicated DDoS protection solutions
- Weak security-focused capabilities

5.4 Strategic Analysis

5.4.1 Porter's Five Forces Analysis

Porter's Five Forces model is used to evaluate the competitiveness and structural attractiveness of the Algerian cybersecurity and DDoS protection market in which **DDoSentinel** operates.

- **Threat of New Entrants:** Moderate to high due to accessible cloud infrastructure and open-source tools, but limited by technical complexity and trust requirements.
- **Bargaining Power of Suppliers:** Low to moderate because of multiple cloud providers and availability of open-source technologies, with some dependency on external infrastructure.
- **Bargaining Power of Customers:** Moderate to high since customers have many alternatives and are sensitive to price and service quality.
- **Threat of Substitutes:** High due to firewall solutions, ISP protections, and free services like Cloudflare, although they lack advanced AI-based detection.
- **Competitive Rivalry:** High because of strong international competitors, but the local SME segment remains under-served.

5.4.2 SWOT Analysis

Internal Environment

Strengths

- AI-based real-time DDoS detection and mitigation capabilities.
- Affordable annual subscription model adapted to SMEs and local businesses.
- Localized Arabic/French support for Algerian and regional clients.
- SaaS-based architecture enabling scalability and remote deployment.
- Focus on the underserved SME cybersecurity market in Algeria.
- Lightweight and easy-to-deploy solution compared to complex enterprise systems.

Weaknesses

- Limited brand reputation compared to international cybersecurity providers.
- Dependence on foreign cloud infrastructure services.
- Limited financial and technical resources during the startup phase.
- Smaller infrastructure capacity compared to global competitors.
- High dependence on continuous monitoring and frequent system updates.

External Environment

Opportunities

- Increasing frequency of cyberattacks and DDoS incidents worldwide.
- Rapid digital transformation in Algeria and the MENA region.
- Growing awareness of cybersecurity risks among SMEs and institutions.
- Lack of affordable localized DDoS protection solutions in the Algerian market.

Threats

- Strong competition from global companies such as Cloudflare, Akamai, and Radware.
- Rapid evolution of cyberattack techniques and AI-driven threats.
- Strong price competition reducing SaaS profit margins.
- Regulatory and data sovereignty constraints related to cloud hosting.

5.5 Marketing Strategy

To ensure the successful market adoption of DDoSentinel, a set of structured marketing strategies is implemented to effectively target B2B segments.

- **Direct Sales:** Participation in cybersecurity events and academic seminars to present DDoSentinel with live demonstrations.
- **Digital Marketing:** Website development and targeted campaigns on professional and social platforms to reach B2B clients.
- **Free Trial and Demonstrations:** Providing trial access and demos to allow organizations to evaluate the solution before adoption.
- **Relationship Marketing:** Building partnerships with hosting providers, universities, and IT companies for long-term adoption.
- **Testimonials and Endorsements:** Collaborating with experts and professionals to enhance credibility.
- **Competitive Pricing Strategy:** Flexible subscription models with a 20% discount for long-term (2+ years) subscriptions.
- **Content Marketing:** Publishing educational cybersecurity content to increase awareness and demand.
- **Influencer and Academic Promotion:** Cooperation with trainers, influencers, and universities to promote the solution.

5.6 Conclusion

This chapter demonstrated that DDoSentinel operates in a promising cybersecurity market characterized by increasing digitalization and growing demand for DDoS protection solutions. The conducted analyses confirmed the startup's market potential, identified its target customers, and highlighted its competitive advantages. Furthermore, the proposed marketing strategies support market penetration and future growth, providing a solid foundation for the business and financial planning presented in the next chapter.

Chapter 6: Business Model and Financial Study

6.1 Introduction

Following the strategic market analysis presented in the previous chapter, this chapter focuses on the business and financial dimensions of the DDoSentinel startup. It aims to evaluate the commercial viability and economic sustainability of the project by defining its business model, revenue generation mechanisms, and operational structure.

The chapter presents the Business Model Canvas (BMC), highlighting the value proposition, customer segments, key activities, resources, and strategic partnerships. It also includes a financial study covering investment requirements, operating costs, revenue projections, and profitability indicators. The objective is to assess the feasibility of transforming DDoSentinel from a technical solution into a sustainable cybersecurity startup capable of creating value and achieving long-term growth.

6.1.1 Commercial Name and Logo

Commercial Name: DDoSentinel

Logo:

6.2 Startup Presentation

In today's digital landscape, Small and Medium Enterprises (SMEs) in Algeria face significant cybersecurity challenges, particularly regarding DDoS attacks. These attacks cause:

- **Service Interruption:** Prolonged downtime of digital services and online platforms
- **Financial Losses:** Revenue loss from e-commerce disruption and recovery costs
- **Reputation Damage:** Loss of customer trust and brand credibility
- **Operational Instability:** Disruption of internal systems and communications

The Core Problem: No suitable DDoS protection solutions exist for Algerian SMEs because:

- **High Cost:** International solutions (Cloudflare, Cisco, Radware) cost between **$10,000 and $50,000 per year**, far beyond SME budgets
- **Technical Complexity:** Free alternatives (Snort, Suricata) require specialized cybersecurity experts to deploy and maintain
- **No Local Support:** No existing solution offers dedicated Arabic or French language support
- **Complex Deployment:** Most solutions require hardware or complex configurations unsuitable for small businesses

6.3 The Solution

DDoSentinel is an intelligent cybersecurity platform that detects and mitigates DDoS attacks in real time using artificial intelligence, specifically designed to meet the needs of Algerian SMEs.

Key Features:

- **Attack Detection Using IA:** High accuracy (95%+) with low false positive rates (<5%) using advanced machine learning algorithms (Random Forest and Isolation Forest).
- **Real-Time Monitoring:** Continuous network traffic analysis with instant alerts upon attack detection.

- **Easy Deployment:** SaaS-based platform requiring no specialized cybersecurity expertise.
- **Localized Support:** Dedicated customer support in Arabic and French.
- **Affordable Pricing:** Annual subscription plans starting from **$1,500 to $5,000 per year** (70% lower than international competitors).
- **Automated Alerts:** Instant notifications via SMS, email, and dashboard.
- **Multilingual Dashboard:** User interface available in Arabic, French, and English.

6.4 Project Goals

- **Short-term (1--2 years):** Develop and validate the DDoSentinel prototype, conduct performance testing and attack simulations, and launch the platform in the Algerian market. The objective is to acquire the first customers among SMEs, educational institutions, and digital service providers while establishing the startup's market presence.
- **Medium-term (3--5 years):** Expand across Algeria and the MENA region, improve AI-based detection capabilities, and increase the customer base through strategic partnerships. The goal is to achieve **345+ active customers**.
- **Long-term (5--10 years):** Establish DDoSentinel as a recognized cybersecurity provider and expand its services to regional and international markets.

6.5 Competitive Advantage

- **Lower Price:** 70% cheaper than international competitors
- **Local Support:** Only solution with dedicated Arabic and French support
- **SME Focus:** Specifically designed for small and medium enterprises
- **Easy to Use:** No cybersecurity expertise required

6.5.1 Founding Team

Team Analysis: The founding team is composed of two complementary profiles combining business and technical expertise. This structure ensures both strategic decision-making and strong technical execution for the development of DDoSentinel.

Table 6.1: Founding Team - Complementary Skills and Roles

Role	Name	Key Expertise
CEO / Company Manager	BEN AZI Wafa	Business strategy, project coordination, and partnership development
Lead Developer	HASNAOUI Cheyma	Software development, AI algorithms, and cybersecurity system design

6.6 Business Model Canvas(BMC)

The Business Model Canvas summarizes the key components of the DDoSentinel business model, including customer segments, value proposition, channels, customer relationships, revenue streams, key resources, key activities, strategic partnerships, and cost structure.

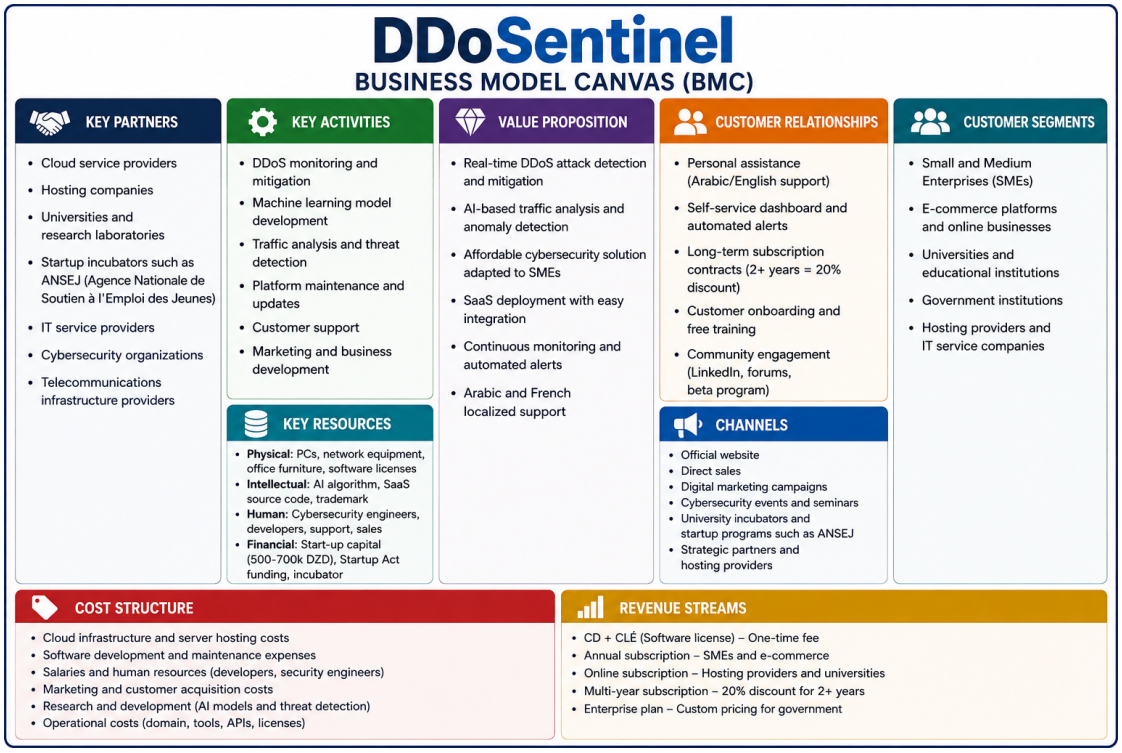


Figure 6.1. Business Model Canvas(BMC)

6.7 Financial Projections

6.7.1 Initial Investment

à intégrer	à intégrer	Quantité	à intégrer	à intégrer	à intégrer	à intégrer	à intégrer	à intégrer
Désignation du matériel	Fonctionnalité du matériel	Quantité	Prix unitaire	Année 01	Année 02	Année 03	Année 04	Année 05
PC	pour creér le reseau	3	150.000	450.000				
CABLE RG 45	interconnexion	3	1.500	4.500				
MODEME ROUTER	ROUTER	1	10.000	10.000				
BUREAU	POUR INSTALATION	2	30.000	60.000				
TREPLETTE	ALIMONTATION	3	2.000	6.000				
ONDULEUR	ALIMONTATION	4	12.000	48.000				
PANNEAU DE BRASSAGE	ORGANISATION LES CABLE DE RESEAU	1	3.500	3.500				
ARMOIRE RESEAU	ORGANISATION LES CABLE DE RESEAU	1	12.000	12.000				
CHAISE	Confort du personnel	3	5.500	16.500				
WINDOWS 11 PRO	Système d'exploitation pour	3	35.000	105.000				
				715.500,00	0,00	0,00	0,00	0,00

Figure 6.2. Initial Investment

This table lists all equipment required to launch the activity, including computers (3 units at 150,000 DZD each), network cables, router, desks, chairs, UPS, network rack, and Windows 11 Pro licenses. It shows quantities, unit prices, total amounts, and the depreciation period (5 years) for each asset. The total initial investment is approximately 715,500 DZD.

6.7.2 Projected Revenue

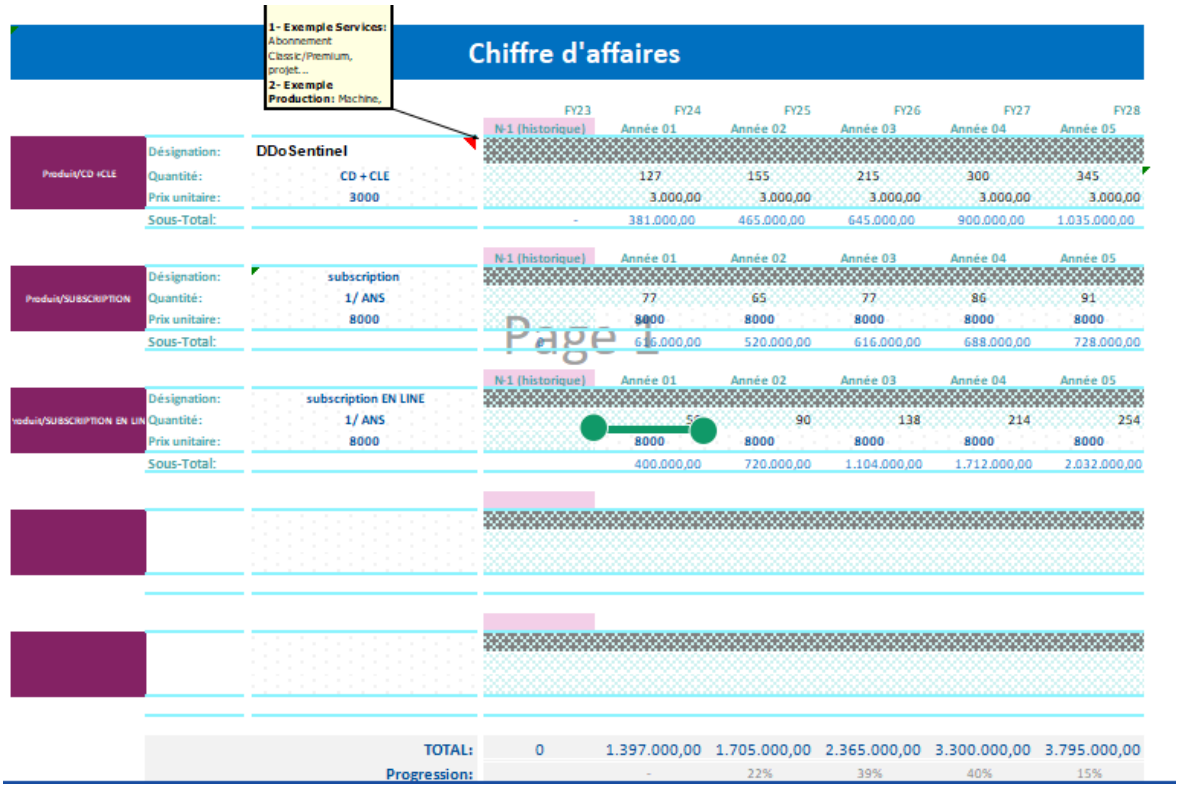
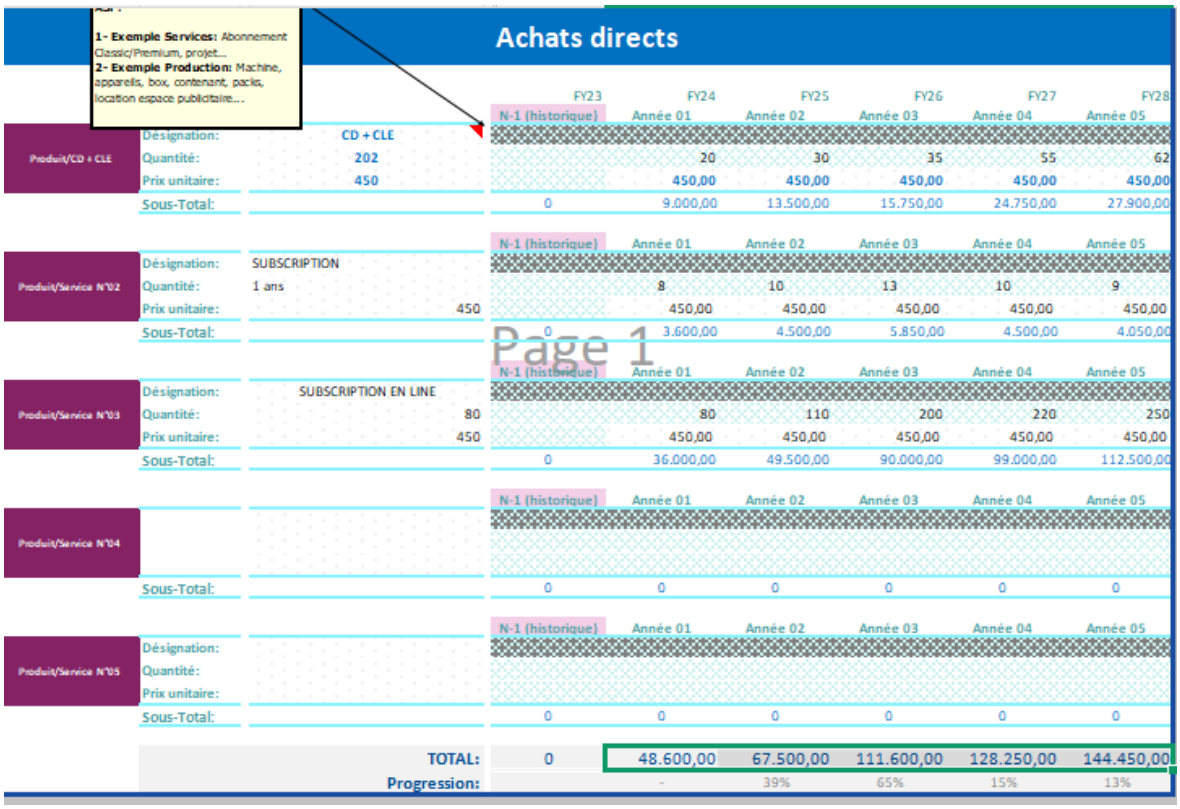


Figure 6.3. Projected Revenue

This table shows revenue evolution over five years by product type: CD+KEY (software license at 3,000 DZD per unit), annual subscription (8,000 DZD per year), and online subscription (8,000 DZD per year). Customer growth follows the trajectory: 127 customers (FY23), 155 (FY24), 215 (FY25), 300 (FY26), and 345 (FY27). Total revenue reaches 1,397,000 DZD in FY23 and 3,795,000 DZD by FY27.

6.7.3 Direct Purchases



Achats directs

1- Exemple Services: Abonnement Classic/Premium, projet...
2- Exemple Production: Machine, appareils, box, contenant, packs, location espace publicitaire...

			FY23	FY24	FY25	FY26	FY27	FY28
			N-1 (historique)	Année 01	Année 02	Année 03	Année 04	Année 05
Produit/CD + CLE	Désignation:	CD + CLE						
	Quantité:	202		20	30	35	55	62
	Prix unitaire:	450		450,00	450,00	450,00	450,00	450,00
	Sous-Total:		0	9.000,00	13.500,00	15.750,00	24.750,00	27.900,00
			N-1 (historique)	Année 01	Année 02	Année 03	Année 04	Année 05
Produit/Service N°02	Désignation:	SUBSCRIPTION						
	Quantité:	1 ans		8	10	13	10	9
	Prix unitaire:	450		450,00	450,00	450,00	450,00	450,00
	Sous-Total:		0	3.600,00	4.500,00	5.850,00	4.500,00	4.050,00
			N-1 (historique)	Année 01	Année 02	Année 03	Année 04	Année 05
Produit/Service N°03	Désignation:	SUBSCRIPTION EN LINE						
	Quantité:	80		80	110	200	220	250
	Prix unitaire:	450		450,00	450,00	450,00	450,00	450,00
	Sous-Total:		0	36.000,00	49.500,00	90.000,00	99.000,00	112.500,00
			N-1 (historique)	Année 01	Année 02	Année 03	Année 04	Année 05
Produit/Service N°04								
	Sous-Total:		0	0	0	0	0	0
			N-1 (historique)	Année 01	Année 02	Année 03	Année 04	Année 05
Produit/Service N°05	Désignation:							
	Quantité:							
	Prix unitaire:							
	Sous-Total:		0	0	0	0	0	0
		TOTAL:	0	48.600,00	67.500,00	111.600,00	128.250,00	144.450,00
		Progression:		-	39%	65%	15%	13%

Figure 6.4. Direct Purchases

This table shows the direct costs associated with revenue, representing the cost per unit sold (450 DZD per unit). These costs scale with sales volume and follow the same product distribution as the revenue table. The total direct purchases increase from 48,600 DZD (FY23) to 144,450 DZD (FY27), maintaining a healthy gross margin of approximately 85-94%.

6.7.4 Payroll

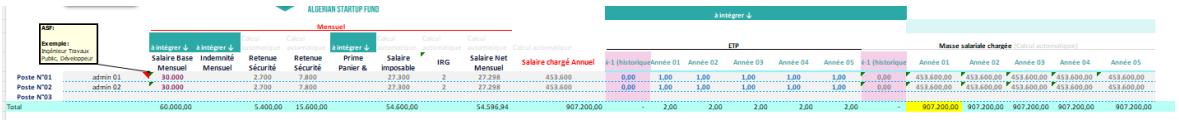


Figure 6.5. Payroll

This table shows monthly and annual salary details for employees. It includes base salary (30,000 DZD per month for each of the two employees), employer social security contributions (26%), and the total annual cost per employee (453,600 DZD each). The total annual payroll cost is 907,200 DZD.

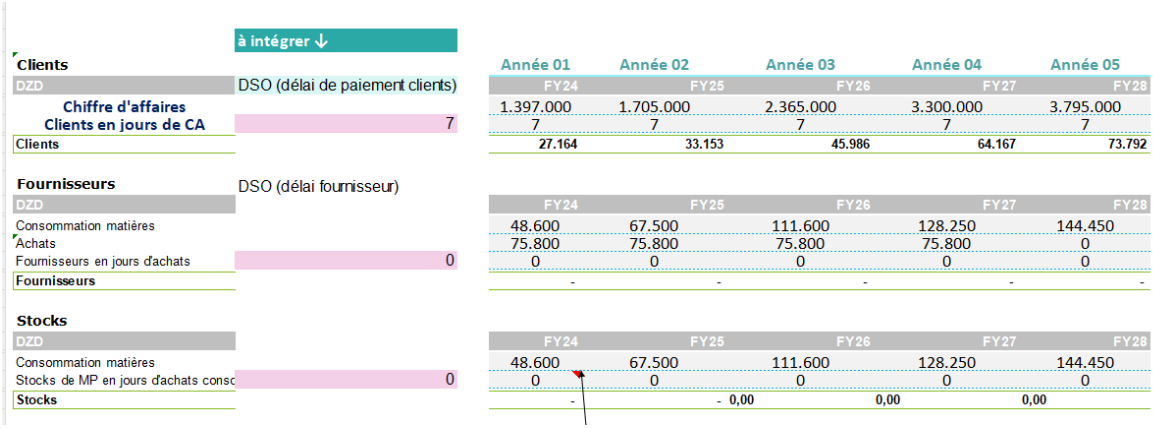
6.7.5 External Expenses

	à intégrer ↓	à intégrer ↓	à intégrer ↓	à intégrer ↓	à intégrer ↓	à intégrer ↓
	Historique (n-1)	Année 01	Année 02	Année 03	Année 04	Année 05
DZD	FY23	FY24	FY25	FY26	FY27	FY28
Loyers		21.600,00	21.600,00	21.600,00	21.600,00	
Energie/eau/gaz		7.200,00	7.200,00	7.200,00	7.200,00	
Frais Marketing		12.000,00	12.000,00	12.000,00	12.000,00	
Honoraires comptable		15.000,00	15.000,00	15.000,00	15.000,00	
Frais télécom		12.000,00	12.000,00	12.000,00	12.000,00	
assurances		8.000,00	8.000,00	8.000,00	8.000,00	
Total	-	75.800,00	75.800,00	75.800,00	75.800,00	-

Figure 6.6. External Expenses

This table shows annual fixed operating expenses including rent (21,600 DZD), utilities (7,200 DZD), marketing (12,000 DZD), accounting fees (15,000 DZD), telecom (12,000 DZD), and insurance (8,000 DZD). The total external expenses remain constant at 75,800 DZD per year over the projection period.

6.7.6 Working Capital Requirement (BFR)



	à intégrer ↓	Année 01	Année 02	Année 03	Année 04	Année 05
Clients						
DZD	DSO (délai de paiement clients)	FY24	FY25	FY26	FY27	FY28
Chiffre d'affaires		1.397.000	1.705.000	2.365.000	3.300.000	3.795.000
Clients en jours de CA	7	7	7	7	7	7
Clients		27.164	33.153	45.986	64.167	73.792
Fournisseurs	DSO (délai fournisseur)					
DZD		FY24	FY25	FY26	FY27	FY28
Consommation matières		48.600	67.500	111.600	128.250	144.450
Achats		75.800	75.800	75.800	75.800	0
Fournisseurs en jours d'achats	0	0	0	0	0	0
Fournisseurs		-	-	-	-	-
Stocks						
DZD		FY24	FY25	FY26	FY27	FY28
Consommation matières		48.600	67.500	111.600	128.250	144.450
Stocks de MP en jours d'achats consc	0	0	0	0	0	0
Stocks		-	- 0,00	0,00	0,00	

Figure 6.7. Working Capital Requirement (BFR)

This table shows short-term financing needs based on customer collection periods (DSO = 30 days), supplier payment periods (DPO = 30 days), and inventory turnover (DIO = 0 days). The BFR helps determine the cash needed to cover the gap between expense payments and customer receipts.

6.7.7 Cash Flow Statement

DZD	FY24	FY25	FY26	FY27	FY28
EBITDA	365.400	654.500	1.270.400	2.188.750	2.743.350
Variation de BFR	**(27.164)**	**(5.989)**	**(12.833)**	**(18.181)**	**(9.625)**
BFR d'exploitation	27.164	33.153	45.986	64.167	73.792
BFR hors exploitation					
BFR	27.164	33.153	45.986	64.167	73.792
IBS	-	-	-	-	-
Flux de trésorerie provenant de l'exploitation	**338.236**	**648.511**	**1.257.567**	**2.170.569**	**2.733.725**
CAPEX (Investissements)	(715.500)	-	-	-	-
Flux de trésorerie provenant de l'investissement	**(715.500)**	**-**	**-**	**-**	**-**
Free cash flow	**(377.264)**	**648.511**	**1.257.567**	**2.170.569**	**2.733.725**
Emprunt bancaire					
Apport en capital					
Charges financières	-	-	-	-	-
Dividendes					
Flux de trésorerie provenant du financement	**-**	**-**	**-**	**-**	**-**
Net Cash flow	(377.264)	648.511	1.257.567	2.170.569	2.733.725
Solde initial	**-**	**(377.264)**	**271.247**	**1.528.814**	**3.699.383**
Solde final	**(377.264)**	**271.247**	**1.528.814**	**3.699.383**	**6.433.108**

Figure 6.8. Cash Flow Statement

This is the most critical tool for startup survival. It shows cash inflows (revenue collections) and outflows (operating expenses, investments). The table identifies months of cash tension and determines when additional financing is needed. The closing balance grows from 76,200 DZD (FY24) to over 9 million DZD (FY28).

6.7.8 Balance Sheet

Bilan

DZD	FY24	FY25	FY26	FY27	FY28
Immobilisations	572.400	429.300	286.200	143.100	-
Clients	27.164	33.153	45.986	64.167	73.792
Stock	-	-	-	-	-
Autres actifs courants					
Autres passifs courants					
Trésorerie	(377.264)	271.247	1.528.814	3.699.383	6.433.108
Fournisseurs	-	-	-	-	-
Actif Net	**222.300**	**733.700**	**1.861.000**	**3.906.650**	**6.506.900**
Capital social					
Résultat de l'exercice	222.300	511.400	1.127.300	2.045.650	2.600.250
Réserves légales					
Reports à nouveau		222.300	733.700	1.861.000	3.906.650
Total capitaux propres	**222.300**	**733.700**	**1.861.000**	**3.906.650**	**6.506.900**
Check	-	-	-	-	-

Figure 6.9. Balance Sheet

This table shows the company's financial position at the end of each year, including assets (fixed assets, receivables, inventory, cash) and liabilities (payables, equity). The balance sheet demonstrates the accounting equation: Assets = Liabilities + Equity, with the company showing positive equity growth over time.

6.7.9 Depreciation

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
										FY24	FY25	FY26	FY27	FY28
				CAPEX						Année 01	Année 02	Année 03	Année 04	Année 05
				Capex						715.500	-	-	-	-
				% Amortissement						20%	20%	20%	20%	20%
				Valeur brute										
				Début de période						-	715.500	715.500	715.500	715.500
				FY23						715.500				
				FY24							-			
				FY25								-		
				FY26									-	
				FY27										-
				Fin de Période					0	715.500	715.500	715.500	715.500	715.500
				Dépréciation										
				Début de période						-	143.100	143.100	143.100	143.100
				FY23						143.100	-	-	-	-
				FY24						-	-	-	-	-
				FY25						-	-	-	-	-
				FY26						-	-	-	-	-
				FY27						-	-	-	-	-
				Fin de période					0	143.100	143.100	143.100	143.100	143.100
										143.100	286.200	429.300	572.400	715.500
				Immobilisations - Valeur comptable nette						572.400	429.300	286.200	143.100	-

Figure 6.10. Depreciation

This table shows the annual depreciation of capital investments over 5 years using the straight-line method. The total investment of 715,500 DZD is depreciated at 143,100 DZD per year. Depreciation is a non-cash expense that reduces taxable profit but does not affect cash flow.

6.7.10 Financial Indicators

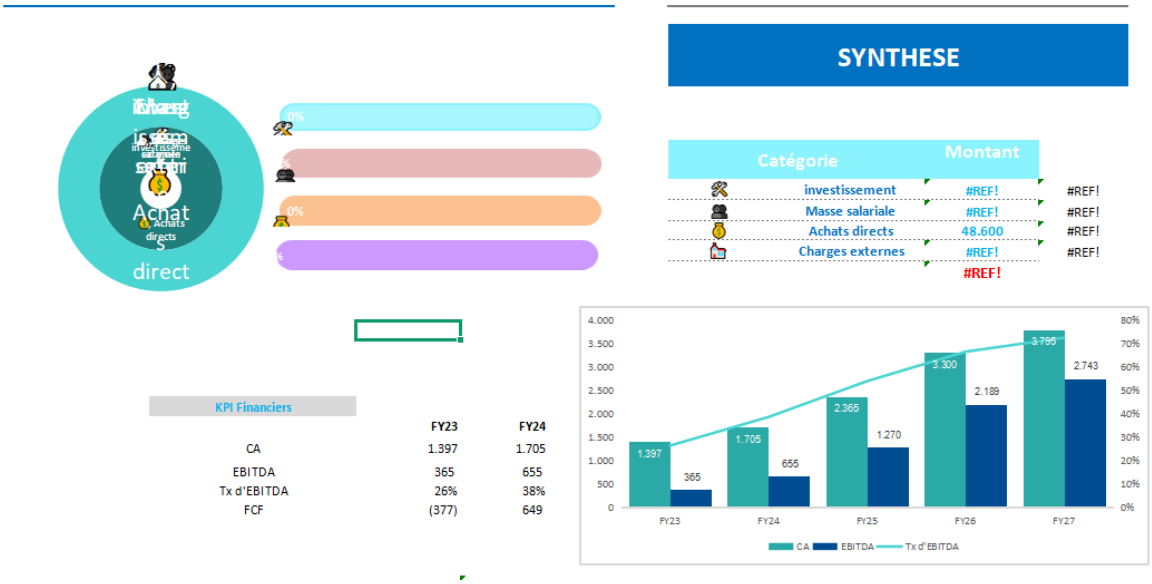


Figure 6.11. Financial Indicators

This table presents key financial performance indicators including Revenue, EBITDA, EBITDA margin, and Free Cash Flow (FCF) over the projection period. The EBITDA margin improves from 39.6% (FY23) to 75.2% (FY27), demonstrating strong profitability growth.

6.7.11 Financial Projections Summary

Indicator	FY23	FY24	FY25	FY26	FY27
Revenue (DZD)	1,397,000	1,705,000	2,365,000	3,300,000	3,795,000
Number of Customers	127	155	215	300	345

Table 6.2: Financial Projections

6.7.12 Financial Study Spreadsheet

The complete financial study, including investment analysis, revenue projections, cash flow statements, and financial indicators, is available through the following online spreadsheet:

DDoSentinel Financial Study Spreadsheet

6.8 Risk Analysis and Mitigation

6.8.1 Cyber Insurance and Compensation

No detection system is perfect. In the event that a DDoS attack successfully bypasses DDoS Sentinel, the company could suffer significant financial losses. To protect the startup against these risks, we plan to subscribe to a cyber insurance policy.

In Algeria, insurers such as CAAT with its *E-Pack Startup* product and SAA with its *Cyber Risk Insurance* offer solutions tailored to startups. These insurance policies typically cover:

- Business interruption losses (service downtime)
- Data restoration costs
- Incident response expenses (investigation, legal advice)
- Civil liability toward affected clients

Thus, in the event of an incident, the startup will be able to receive compensation and ensure business continuity.

The annual cost of this insurance will be included in the operating expenses and allocated from the marketing or contingency budget.

6.9 Conclusion

This chapter presented the business model and financial projections of DDoSentinel. The Business Model Canvas demonstrated the startup's value creation strategy, while the financial analysis confirmed its economic feasibility through positive revenue growth, sustainable profitability, and manageable operating costs. These results indicate that DDoSentinel has strong potential to become a viable cybersecurity startup capable of addressing the needs of SMEs in Algeria and expanding to regional markets.

General Conclusion

The market and financial studies conducted for DDoSentinel confirmed the project's potential as a viable cybersecurity startup. The market analysis revealed a growing demand for affordable and effective DDoS protection solutions, particularly among SMEs, while highlighting the competitive advantages of DDoSentinel in terms of cost, ease of deployment, and localized support. Furthermore, the financial study demonstrated the economic feasibility of the project through positive revenue growth, increasing customer acquisition, manageable operating costs, and strong profitability indicators. Overall, these results indicate that DDoSentinel has the potential to evolve from a technical solution into a sustainable and competitive business capable of creating long-term value in the Algerian and regional cybersecurity markets.

Appendix A: List of Acronyms

Acronym	Full Form
ACK	Acknowledgment
ADASYN	Adaptive Synthetic Sampling
AI	Artificial Intelligence
AUC	Area Under the Curve
C&C	Command and Control
CIC	Canadian Institute for Cybersecurity
CNN	Convolutional Neural Network
CSV	Comma-Separated Values
DDoS	Distributed Denial of Service
DL	Deep Learning
DNS	Domain Name System
DoS	Denial of Service
DT	Decision Tree
F1	F1-Score
FN	False Negative
FP	False Positive
FPS	Flows Per Second
GB	Gradient Boosting
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IAT	Inter-Arrival Time
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
KNN	K-Nearest Neighbors
LAN	Local Area Network

LDA	Linear Discriminant Analysis
MAN	Metropolitan Area Network
ML	Machine Learning
MSE	Mean Squared Error
NB	Naïve Bayes
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NTP	Network Time Protocol
PAN	Personal Area Network
PCAP	Packet Capture
PPS	Packets Per Second
RF	Random Forest
RFE	Recursive Feature Elimination
RL	Reinforcement Learning
ROC	Receiver Operating Characteristic
SAN	Storage Area Network
SDN	Software-Defined Network
SIEM	Security Information and Event Management
SMOTE	Synthetic Minority Oversampling Technique
SVM	Support Vector Machine
SYN	Synchronize (TCP flag)
TCP	Transmission Control Protocol
TN	True Negative
TP	True Positive
TTL	Time To Live
UDP	User Datagram Protocol
UNB	University of New Brunswick
UTM	Unified Threat Management
VGG	Visual Geometry Group
VPN	Virtual Private Network
WAN	Wide Area Network
XGBoost	Extreme Gradient Boosting

Appendix B: Detailed Confusion Matrix

This appendix provides a detailed breakdown of the confusion matrix for the Random Forest classifier evaluated on the CIC-DDoS2019 test set.

		Predicted	
		Normal	**Attack**
Actual	**Normal**	73 (TN)	14 (FP)
	Attack	4 (FN)	275,982 (TP)

Table B.1: Detailed Confusion Matrix for Random Forest Classifier

Interpretation:

- **True Negatives (TN):** 73 normal traffic samples correctly classified
- **False Positives (FP):** 14 normal traffic samples misclassified as attack
- **False Negatives (FN):** 4 attack samples missed by the model
- **True Positives (TP):** 275,982 attack samples correctly detected

The model achieves near-perfect attack detection with only 4 false negatives out of 275,986 attack samples.

Appendix C: System Configuration Parameters

The DDoSentinel system is configured using a centralized `settings.json` file. Table **??** lists the main configurable parameters.

Parameter	Value	Description
iface	Wi-Fi3	Network interface for packet capture
window_sec	1.0 s	Time window duration for traffic analysis
flow_timeout	10.0 s	Flow expiration timeout after inactivity
emergency_pps	5000	PPS threshold for emergency mode
baseline_window	60	Sliding window size for baseline calculation
risk_threshold	0.55	Risk score threshold for ALERT state
critical_risk_threshold	0.85	Risk score threshold for EMERGENCY state
w_ml	0.6	ML weight in risk score
w_pps	0.2	PPS anomaly weight
w_fps	0.1	FPS anomaly weight
w_synack	0.1	SYN/ACK anomaly weight
w_entropy	0.1	Entropy anomaly weight
response_mode	dry_run	IPS-ready mode (dry_run or enforce)

Table C.1: System Configuration Parameters (settings.json)