People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

University 8 Mai 1945-Guelma

Faculty of Mathematics, Computer Science and Science of Matter

Department of Computer Science

Master Thesis

Specialty : Computer Science

Option: Computer Systems

Theme

Intrusion Detection in Medical Networks Based on Hybrid Optimization algorithms

---

Presented by:
Hadil Merzougui

Jury Members:

Chairman : Dr Nabil BERRAHOUMA
Supervisor : Dr Karima BENHAMZA
Examiner : Dr Hiba ABDELMOUMENE
Representative POLE PRO: Dr Leila LERRARI

June 2025

Acknowledgments

*Above all, I humbly thank **God**, whose infinite grace and guidance have illuminated every step of my academic journey. Through moments of doubt and perseverance, He has been my source of strength, patience, and clarity.*

*I express my heartfelt gratitude to **Dr. Karima Benhamza**, my respected supervisor. Her trust in my potential, her unwavering support, and her insightful mentorship have deeply shaped both this work and my personal growth. It has been an honor to learn under her guidance.*

*To the **jury members**, I offer my sincere thanks for the time and thoughtfulness they have devoted to evaluating this thesis. Your expertise and feedback are of great value to me, and I am truly grateful for your contributions.*

Lastly, to all those who have walked with me in silence or in words friends, family, mentors, I extend my warmest thanks. Every gesture of encouragement, no matter how small, has left a lasting impact on this journey.

Hadil Merzougui

Dedication

To my beloved parents,

For your endless love, unwavering support, and silent sacrifices. Your strength and faith have shaped the person I am today.
This accomplishment is a reflection of everything you've given me especially you, ***Mom****, whose boundless devotion and gentle guidance have lit my path every step of the way.*

To my dear ***brothers,***
Thank you for always believing in me and cheering me on. To ***Borhan****e, especially your energy, your encouragement, and your confidence in me never went unnoticed. You've been my anchor more times than I can count.*

To ***Nahla****,*
For being the kind of friend everyone wishes to have present, sincere, and inspiring. Your words, patience, and kindness have meant the world to me.

And finally,
To my ***laptop*** *for enduring countless hours of code, heat, bugs, crashes, and stress without giving up.*

Abstract

The Internet of Medical Things (IoMT) has transformed modern healthcare by enabling continuous patient monitoring, remote diagnostics, and real-time data exchange. While these advancements improve service quality and clinical outcomes, they also expose medical networks to a wide range of cyber threats. IoMT environments are particularly vulnerable due to their reliance on heterogeneous, resource-constrained devices that often lack built-in security mechanisms. Conventional intrusion detection systems (IDS) are often inadequate for these settings, as they struggle to deliver high detection accuracy while remaining lightweight and adaptive.

This study proposes a hybrid IDS framework designed specifically for IoMT ecosystems. The approach integrates a Clonal Selection Algorithm (CSA) for dynamic feature selection with a Deep Neural Network (DNN) for accurate classification of network traffic. The CSA component effectively reduces data dimensionality while preserving critical threat-related features, thereby optimizing the model for environments with limited computational capacity. The DNN component captures complex patterns in traffic behavior, enhancing detection capability across diverse attack scenarios.

The model is evaluated using benchmark IoMT datasets, demonstrating its suitability for identifying both known and emerging threats. By combining bio-inspired optimization with deep learning, the proposed IDS offers a robust and scalable solution to enhance cybersecurity in sensitive and critical healthcare systems.

Keywords: Internet of Medical Things (IoMT); Intrusion Detection System (IDS; Clonal Selection Algorithm (CSA); Deep Neural Network (DNN); Cybersecurity in Healthcare environments.

Résumé

L'Internet des Objets Médicaux (IoMT) a profondément transformé le secteur de la santé moderne en permettant la surveillance continue des patients, le diagnostic à distance et l'échange de données en temps réel. Bien que ces avancées améliorent la qualité des soins et les résultats cliniques, elles exposent également les réseaux médicaux à un large éventail de menaces cybernétiques. Les environnements IoMT sont particulièrement vulnérables en raison de leur dépendance à des dispositifs hétérogènes et limités en ressources, souvent dépourvus de mécanismes de sécurité intégrés. Les systèmes classiques de détection d'intrusion (IDS) se révèlent souvent inadaptés à ces contextes, car ils peinent à conjuguer précision, légèreté et adaptabilité.

Cette étude propose un cadre hybride de détection d'intrusion spécifiquement conçu pour les écosystèmes IoMT. L'approche combine un Algorithme de Sélection Clonale (CSA) pour la sélection dynamique des caractéristiques avec un Réseau de Neurones Profond (DNN) assurant la classification précise du trafic réseau. Le module CSA permet une réduction efficace de la dimensionnalité tout en conservant les attributs critiques liés aux menaces, optimisant ainsi le modèle pour des environnements à faible capacité de calcul. Le DNN capte des schémas complexes dans le comportement du trafic, renforçant la capacité de détection face à divers scénarios d'attaque.

Le modèle est évalué à l'aide de jeux de données de référence pour l'IoMT, démontrant son efficacité à détecter aussi bien les menaces connues qu'émergentes. En combinant optimisation bio-inspirée et apprentissage profond, l'IDS proposé constitue une solution robuste et évolutive pour renforcer la cybersécurité dans les systèmes de santé sensibles et critiques.

Mots-clés : Internet des Objets Médicaux (IoMT) ; Système de Détection d'Intrusion (IDS) ; Algorithme de Sélection Clonale (CSA) ; Réseau de Neurones Profond (DNN) ; Cybersécurité dans les environnements de santé.

ملخص

ساهمت إنترنت الأشياء الطبية في إحداث نقلة نوعية في مجال الرعاية الصحية الحديثة، من خلال تمكين المراقبة المستمرة للمرضى، والتشخيص عن بُعد، وتبادل البيانات في الوقت الحقيقي. ورغم أن هذه التطورات تعزز جودة الخدمات وتحسّن النتائج السريرية، إلا أنها تجعل الشبكات الطبية عرضة لمجموعة متزايدة من التهديدات السيبرانية. وتُعد هده البيئات معرضة بشكل خاص لهذه المخاطر بسبب اعتمادها على أجهزة غير متجانسة ومحدودة الموارد، وغالبًا ما تفتقر إلى آليات الحماية المدمجة. كما أن أنظمة كشف التسلل التقليدية لا تلبي بشكل كافٍ متطلبات هذه البيئات، نظرًا لصعوبة تحقيق توازن بين الدقة العالية وخفة الأداء والقدرة على التكيّف.

في هذا البحث، نقترح إطارًا هجينا لنظام كشف التسلل مصممًا خصيصًا لبيئات 'إنترنت الأشياء الطبية' يدمج النموذج خوارزمية الاختيار التناسلي لاختيار الميزات الديناميكية، مع شبكة عصبية عميقة لتصنيف حركة مرور الشبكة بدقة عالية. تعمل هده الخوارزمية على تقليل أبعاد البيانات مع الحفاظ على الخصائص الأمنية الجوهرية، مما يجعل النموذج ملائمًا للأجهزة ذات القدرات الحوسبة المحدودة. أما مكوّن الشبكة العصبية العميقة، فيتمتع بقدرة عالية على تحليل الأنماط المعقدة مما يعزز من كفاءة الكشف عن التهديدات المختلفة.

تم تقييم النموذج باستخدام مجموعات بيانات معيارية خاصة بأنترنت الأشياء الطبية، وأثبت كفاءته في الكشف عن الهجمات المعروفة والناشئة. ومن خلال الجمع بين تقنيات التحسين الحيوي المستوحاة والتعلم العميق، يوفر النظام المقترح حلاً فعالًا وقابلاً للتوسّع لتعزيز الأمن السيبراني في البيئات الصحية الحساسة والحرجة.

الكلمات المفتاحية :إنترنت الأشياء الطبية؛ نظام كشف التسلل؛ خوارزمية الاختيار التناسلي؛ الشبكات العصبية العميقة؛ الأمن السيبراني في الرعاية الصحية.

List of Abbreviations

AI	Artificial Intelligence
API	Application Programming Interface
CSA	Clonal Selection Algorithm
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DNN	Deep Neural Network
DoS	Denial of Service
ECG	Electrocardiogram
FPR	False Positive Rate
HIDS	Host-based Intrusion Detection System
HTTP	HyperText Transfer Protocol
IDS	Intrusion Detection System
IoMT	Internet of Medical Things
IoT	Internet of Things
IP	Internet Protocol
KNN	K-Nearest Neighbors
MAC	Media Access Control
MitM	Man-in-the-Middle
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
NIDS	Network-based Intrusion Detection System
PCA	Principal Component Analysis
PSO	Particle Swarm Optimization
RAM	Random Access Memory
ReLU	Rectified Linear Unit
RNN	Recurrent Neural Network
SVM	Support Vector Machine
TCP	Transmission Control Protocol
TPR	True Positive Rate
URL	Uniform Resource Locator
UTM	Unified Threat Management
WSN	Wireless Sensor Network

List of Figures

Table of Contents

General Introduction

The Internet of Medical Things (IoMT) has emerged as a major technological advancement in modern healthcare. Through the intelligent interconnection of medical devices, IoMT enables real-time patient monitoring, automated medical data collection, and overall improvement in patient care, particularly for chronic diseases. Devices such as insulin pumps and pacemakers can not only monitor vital signs but also autonomously respond, thereby reducing the need for continuous hospitalization. Other applications include fall detection for the elderly, performance monitoring for athletes, and improved access to healthcare in remote areas.

Despite these numerous benefits, the large-scale deployment of IoMT raises critical security concerns. The distributed nature of devices, reliance on wireless communication, limited computational resources, and the sensitivity of medical data make IoMT environments a prime target for cyberattacks. A breach in data confidentiality, integrity, or availability can lead to incorrect diagnoses, inappropriate treatments, or even endanger patients' lives.

Traditional security mechanisms, often designed for conventional IT systems, are not well-suited to the constrained and heterogeneous nature of IoMT. Initial efforts in securing IoMT have relied on encryption, authentication, and trust-based models. However, these techniques struggle to address the growing sophistication of modern cyber threats.

In this context, Intrusion Detection Systems (IDS) represent an essential layer of defense for strengthening IoMT security. Artificial intelligence-based approaches, particularly those using bio-inspired algorithms, offer promising capabilities for detecting abnormal behaviors, including previously unknown attacks.

The aim of this study is to design, implement, and evaluate a high-performance IDS specifically adapted to the constraints of IoMT environments. To achieve this, we propose a hybrid approach that combines a bio-inspired feature selection algorithm, the Clonal Selection Algorithm (CSA), with a Deep Neural Network (DNN) for the classification phase. The model is evaluated using two benchmark IoMT datasets. The goal is to demonstrate the system's ability to detect intrusions effectively while maintaining the lightweight, fast, and reliable characteristics required by IoMT devices.

This document is structured into three chapters:

Chapter 1 provides an overview of the Internet of Medical Things (IoMT), its architecture, and its role in modern healthcare. It highlights the specific security challenges posed by IoMT environments and explains the importance of Intrusion Detection Systems (IDS) as a key line of defense against cyberattacks.

Chapter 2 reviews existing security approaches used in IoMT, including machine learning, deep learning, and hybrids methods. It also introduces the datasets used in this research and explains their relevance to intrusion detection in medical networks.

Chapter 3 presents the proposed model, combining feature selection through a bio-inspired algorithm with a deep learning-based classification system. It describes the implementation process, experimental setup, and analysis of results, demonstrating the model's potential for securing IoMT environments.

Finally, the **conclusion** summarizes the main contributions of this work and outlines directions for future research.

Chapter 1: Intrusion Detection Systems in the Internet of Medical Things (IoMT)

1.1 Introduction

Cybersecurity is a major concern due to the increasing number of cyber threats. Intrusion Detection Systems (IDS) play a crucial role in identifying attacks and protecting infrastructures. This chapter explores IDS, their categories, architecture, and their application in the Internet of Medical Things (IoMT). Finally, IoMT security challenges and potential attacks are discussed to better understand the risks and existing solutions.

1.2 Intrusion Detection System

An Intrusion Detection System (IDS) is a relatively recent technology designed to help computer systems prepare for and respond to network attacks. Its primary function is to monitor and analyze user and system activities, assess vulnerabilities, and track violations of user policies. By collecting information from various sources within systems and networks, IDS compares this data against pre-existing patterns to identify potential attacks or weaknesses. The goal of IDS is to detect anomalous behavior and misuse in network assets, providing a critical layer of security within the information security infrastructure [1].

1.3 Intrusion Detection System Categories

Intrusion detection system is classified into three categories based on its detection methodology: Signature-Based Detection Systems, Anomaly-Based Detection Systems and Specification-Based Detection Systems.

1.3.1 Signature-Based Detection System

This system identifies intrusion attempts by comparing detected signatures with a predefined database of known threats. Upon detecting a match, it promptly generates an alert.

1.3.2 Anomaly-Based Detection System

Anomaly detection system is characterized by its ability to identify unknown attacks by analyzing deviations from the network's usual behavior. Unlike signature-based approach, it relies on rules or heuristics, enabling them to detect novel threats, although they often result in a high rate of false positives. Its implementation requires an initial learning phase to establish a reference model of the system’s normal operation [1].

1.4 Types of Intrusion Detection Systems

Intrusion detection system is classified into three types Host based IDS , Network based IDS and Hybrid based IDS.

1.4.1 Host-Based Intrusion Detection Systems (HIDS)

HIDS monitor host computer activities and detect malicious behaviors. Installed directly on each machine, they analyze audit logs, identify activity patterns or signatures, and assess their behavior [2]. Their operation is based on three main steps: activity monitoring, attack detection, and threat response [3].

1.4.2 Network-Based Intrusion Detection Systems (NIDS)

NIDS (Network-Based Intrusion Detection Systems) monitor network traffic to identify potential attacks [2]. Deployed on network devices such as routers and switches [4], they perform three primary functions: traffic monitoring, attack detection, and the implementation of response mechanisms.

1.5 Architecture of intrusion detection systems

The architecture of an Intrusion Detection System (IDS) is based on several essential components that interact to identify and manage threats. First, the information source corresponds to the monitored system, which generates raw data such as logs and network packets. This data is collected by sensors and transmitted to the detection engine. The detection engine analyzes the information and compares it to rules and signatures stored in the knowledge base to identify potential anomalies. If a threat is detected, an alert is generated and sent to the response component, which can take various actions such as sending a notification or blocking suspicious activity. Finally, the configuration module allows the system's parameters to be adjusted, including updating detection rules and response strategies. Figure1.1 illustrates a typical IDS architecture, highlighting the interactions among its main components.

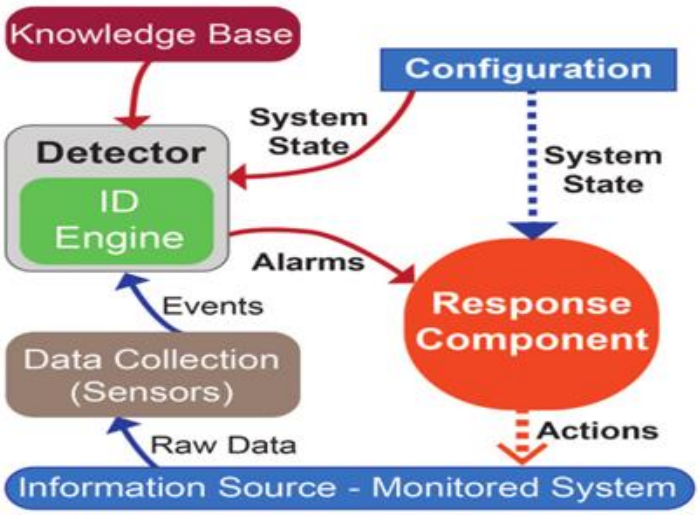

Figure 1. 1. Architecture of intrusion detection systems [5].

1.6 Internet of Things (IoT)

The Internet of Things facilitates communication between people and objects by leveraging computing capabilities and hardware accessibility for a wide range of applications. In general terms, IoT is defined as an interconnected network of objects capable of continuously generating information about the physical world. These objects can exchange data and be controlled by various agents (computer systems or users) to interact with their environment and manage numerous everyday services [6].

IoT applications span multiple domains, including [7]:

Smart Cities : IoT technologies facilitate advanced traffic control and urban mobility by utilizing interconnected sensor networks. These systems contribute to the optimization of transportation infrastructures and the enhancement of urban service efficiency ;

Smart Environments: IoT plays a crucial role in environmental monitoring, including earthquake prediction, fire detection, and other real-world data collection. A notable example is meteorological technology, which relies on IoT to track and forecast weather conditions.

Industrial Control: IoT enables continuous monitoring of industrial operations, supporting real-time data acquisition, predictive maintenance, and remote fault diagnosis. These capabilities reduce the need for on-site inspections and enhance the operational reliability of industrial systems.

Healthcare: The integration of IoT in healthcare systems supports remote monitoring of patient health by collecting biometric data through connected medical devices. This facilitates proactive health management and improves access to care, especially for patients with chronic conditions.

Smart Agriculture: IoT applications in agriculture contribute to increased productivity and sustainability by automating critical processes such as irrigation, fertilization, and environmental monitoring. The real-time analysis of soil and climatic conditions allows for more precise and efficient farming practices.

1.7 Internet of medical things (IoMT)

The Internet of Medical Things (IoMT) refers to the interconnected network of medical devices that communicate via the Internet to collect and transmit health-related data. This ecosystem is crucial in modern healthcare, enabling applications such as real-time patient monitoring, chronic disease management, and personalized treatments. By enhancing patient care and optimizing operational efficiency, IoMT supports a more data-driven, patient-centered healthcare approach [8].

1.7.1 Types of IoMT Devices

Different IoMT devices operate at various layers of smart healthcare systems, ensuring seamless service delivery, as illustrated in Figure 1.2 These devices can be broadly categorized into the following groups:

Wearable Devices: These smart healthcare devices continuously collect patient data, enabling real-time health monitoring while being cost-effective. Examples include smartwatches, blood pressure and

glucose monitors, heart rate trackers, and fitness bands [9].

Home-based IoMT Devices: These include diagnostic test kits, first-aid tools, treatment devices, infant care equipment, feeding devices, infusion pumps, ventilators, and other medical tools designed for home use. These devices can connect to hospital-based systems and healthcare providers via the Internet [10].

Hospital-based IoMT Devices and Equipment: Hospitals can be equipped with medical devices to handle routine treatments and emergency situations effectively. Smart hospital devices, such as surgical tables, anesthesia machines, electrosurgical systems, defibrillators, and other critical equipment, play a vital role in ensuring high-quality patient care [11].

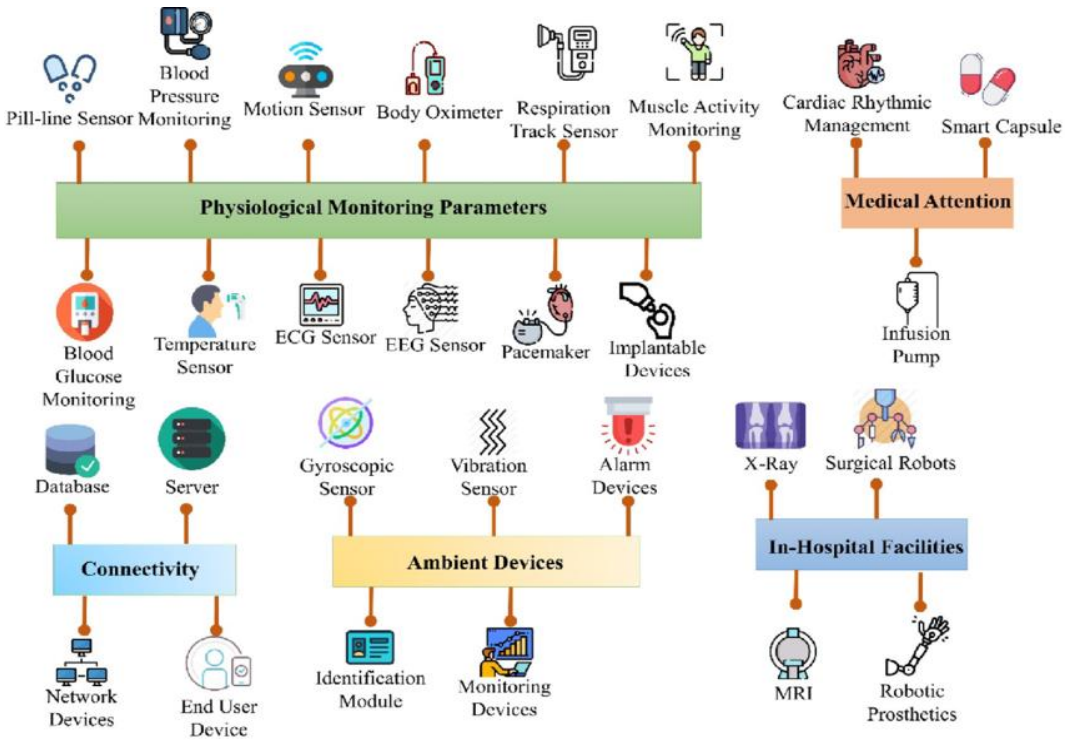

Figure 1. 2. IoMT devices [12].

1.7.2 Architecture of IoMT

The architecture of the IoMT, illustrated in Figure 1.3, is structured as a multi-layered framework, where each layer fulfills specific functions and responsibilities [13]:

This architecture consists of the following layers:

1. **Perception Layer**: This layer is responsible for collecting data from connected medical devices, such as ECG monitoring sensors, insulin pumps, smartwatches, and CPAP devices. It serves as the interface between patients and the IoMT system.

2. **Network Layer**: It ensures the secure transmission of collected data using various network protocols and infrastructures, including wireless routers, virtual routers, UTM routers, and dedicated communication servers.

3. **Data Layer**: This layer manages the storage, synchronization, and processing of medical data through cloud servers, hospital physical servers, and server clusters.

4. **Application Layer**: It allows end users, such as healthcare professionals and patients, to interact with the collected data through specific applications, such as assistive listening systems, remote monitoring, medical interpreters, and digital medical libraries.

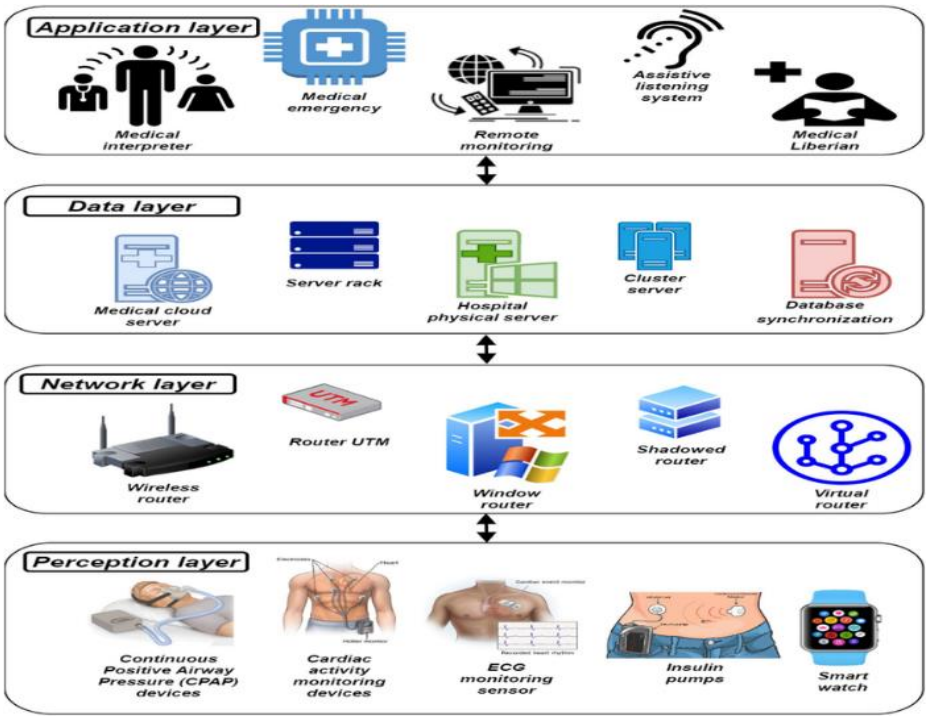

Figure 1. 3. IoMT architecture [13].

1.7.3 IoMT Security Requirements

To ensure the protection of sensitive medical data and the reliable functioning of IoMT systems, three core security requirements must be addressed: confidentiality, integrity, and availability [14].

Confidentiality safeguards the patient's health status and treatment details by preventing unauthorized access to personal information during data storage and transmission in IoMT systems.

Integrity ensures that medical data remains accurate and unaltered, preventing corruption or unauthorized modifications during storage and transmission.

Availability guarantees the continuous functionality of medical devices, services, and patient records, playing a crucial role in ensuring timely responses to health emergencies.

1.7.4 Attacks on IoMT

The Internet of Medical Things (IoMT) has revolutionized healthcare by enabling seamless connectivity between medical devices. However, this connectivity also exposes IoMT systems to

various cyber threats (Figure 1.4). The following are some of the most critical attacks targeting IoMT environments:

Denial of Service (DoS) Attacks: These attacks aim to disrupt or render a service unavailable by overwhelming a system's resources, posing a major threat to data and service availability in IoMT environments [15,16].

Distributed Denial of Service (DDoS) Attacks: A DDoS attack is a type of DoS attack in which multiple sources simultaneously target a single system, causing IoMT devices to disrupt their healthcare services [17,18].

Man-in-the-Middle (MitM) Attacks: This type of threat occurs when an attacker intercepts communication between two parties to eavesdrop on their exchange. In healthcare organizations, a MitM attack can lead to the exposure of confidential patient data or the alteration of sensitive medical information. These compromised details may then be sold, used for criminal activities, or leveraged to blackmail affected patients [17,19].

Ransomware Attacks: Ransomware attacks aim to block user access to files by encrypting them and demanding a ransom for decryption. This threat is increasingly concerning in hospitals due to its financial impact and the disruption it causes to healthcare services[20].

Malware Attacks: Once a system is compromised, attackers can target the user by deploying various types of malicious software. These harmful programs, known as malware, are designed to modify, damage, spy on, or delete data without the user's consent. In recent years, vulnerabilities in device protocols and systems have been widely exploited to implant malware[21].

Injection Attacks: Injection attacks enable attackers to insert malicious code into a program or deploy malware on a system, allowing them to access sensitive information, escalate privileges, alter data, and compromise devices. While reported cases of injection attacks on hospitals remain limited, cybersecurity experts remain concerned about the significant risks they pose[22].

Password Attacks: This attack seeks to gain control of a system by attempting to guess the user's password. Moreover, password attacks pose a significant threat due to their infrequent occurrence and localized nature, which makes them challenging to detect [15].

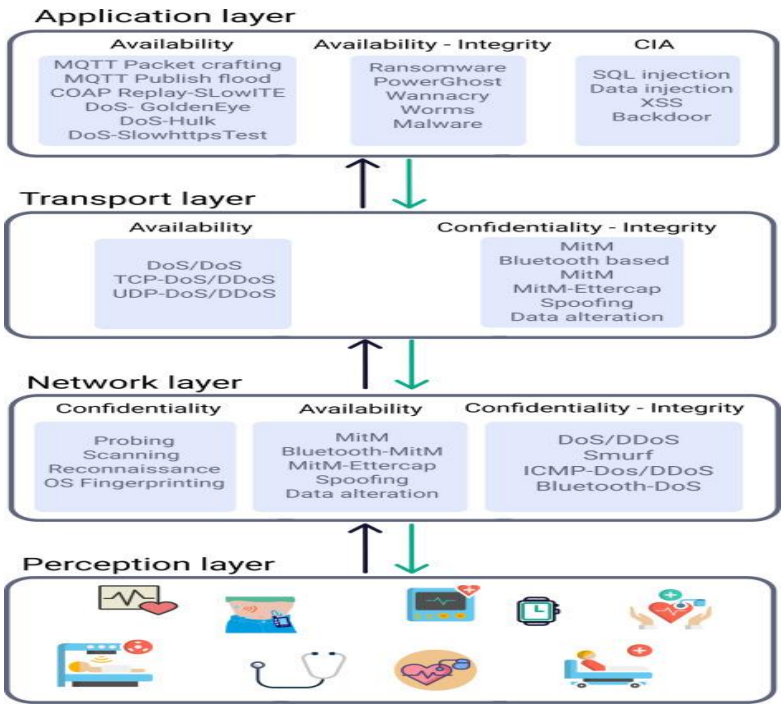

Figure 1. 4. Attacks on IoMT [23].

1.8 Conclusion

This chapter presented intrusion detection systems (IDS), covering their definitions, categories, types, and architecture. It also introduced the Internet of Things (IoT) and the Internet of Medical Things (IoMT), detailing their devices, architecture, security requirements, and the main attacks targeting IoMT. The next chapter will provide a comprehensive literature review of the various security techniques applied to IoMT.

Chapter 2: Review of Related Works

2.1 introduction

The rapid expansion of the Internet of Medical Things (IoMT) necessitates sophisticated security measures to protect against cyber threats. This chapter presents a comprehensive review of existing intrusion detection techniques applied in the Internet of Medical Things (IoMT), focusing on datasets, machine learning, deep learning, and hybrid bio-inspired approaches.

2.2 IoMT Security Datasets Overview

Several datasets have been developed to realistically simulate Internet of Medical Things (IoMT) environments and support the effective evaluation of Intrusion Detection Systems (IDS). These datasets differ in scale, attack diversity, number of classes, and the types of medical devices modeled.

The WUSTL-EHMS-2020 dataset, developed by Washington University in St. Louis [23], provides time-series data collected from smart medical devices. It includes both benign and malicious traffic, enriched with metadata such as timestamps, sensor readings, and communication logs, making it particularly suitable for behavior-based intrusion detection approaches.

The ECU-IoHT dataset, presented in [24], was generated using the Libelium MySignals Healthcare kit. It simulates a realistic Internet of Health Things (IoHT) environment through a wide range of biometric sensors, enabling researchers to develop and test intrusion detection strategies tailored to healthcare systems.

The BlueTack dataset, proposed by Zubair et al. [25], contains data related to Bluetooth Low Energy (BLE) and Basic Rate/Enhanced Data Rate (BR/EDR) technologies. It features multiple attack scenarios targeting these communication protocols, aimed at assessing the robustness of security mechanisms for Bluetooth-enabled medical devices.

Lastly, the CIC-IoMT 2024 dataset, published by the Canadian Institute for Cybersecurity [26], captures network traffic from a simulated yet realistic IoMT setting. It includes 18 types of cyberattacks, such as ICMP/TCP DoS, SYN flood, MQTT-based DDoS, and port scanning, collected using Raspberry Pi devices and an iPad controller to emulate real-world IoMT communication patterns.

In this study, we primarily selected the WUSTL EHMS (2020) and CIC-IoMT2024 (2024) datasets. The former provides on-body data from wearable medical devices, with attacks targeting data manipulation such as spoofing and alteration, which is relevant for individual patient monitoring. The CIC-IoMT2024 dataset simulates a broader IoMT network environment, featuring a wide variety of network attacks, allowing for the evaluation of detection systems' robustness against diverse and realistic attack scenarios. These two datasets complement each other by covering both threats related to the medical devices themselves and those affecting overall network communication within an IoMT environment.

2.3 Evaluation metrics of IDS

The performance evaluation of AI-based IDS commonly relies on standard measures based on True Positives (TP), False Positives (FP), True Negatives (TN), and False Negatives (FN), including accuracy, precision, recall, f1-score, detection rate (DR) or True Positive Rate (TPR), false positive rate (FPR), training time, and detection time, described as follows [27,28,29].

TP Intrusions that the IDS correctly detects as attacks.

FP refers to the benign or normal samples in the IoMT-based data that are incorrectly classified as malicious activity.

TN represents the number of benign samples in the IoMT-based data that is correctly identified as benign.

FN corresponds to malicious IoMT-based data that are incorrectly classified as benign samples.

Accuracy describes the proportion of correctly predicted samples out of all the instances.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

Precision identifies the ratio of the number of true samples to all observations predicted as positives.

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

Recall calculates the ratio of the total number of true positives to all true positives.

$$Recall = \frac{TP}{TP + Fn} \quad (3)$$

F1-Score is a harmonic average of recall and precision metrics by taking their weighted average. The harmonic mean is used instead of a simple arithmetic mean to give more weight to lower values, which

helps to penalize imbalances between precision and recall

$$F1 - Score = 2x\frac{PrecisionxRecall}{precision+recall} \quad (4)$$

TPR corresponds to the relation between the number of correctly true positive samples and the total number of actual positive samples.

$$TPR = \frac{TP}{TP + Fn} \quad (5)$$

FPR is the number of incorrectly predicted negative samples related to the total of negative instances.

$$FPR = \frac{FP}{FP + TN} \quad (6)$$

2.4 Literature Review on Security Techniques for IoMT

A structured and methodical literature review was conducted using reputable academic databases, including IEEE Xplore, Springer, ScienceDirect, Elsevier, and MDPI. The search strategy was based on a set of targeted keywords such as *"intrusion detection"*, *"IoMT security"*, *"machine learning"*, *"deep learning"*, *"smart healthcare"*, and *"Internet of Health Things (IoHT)"*, among others. To ensure relevance and recency, only peer-reviewed publications from 2019 to 2025 that met specific inclusion criteria were selected.

The reviewed literature was then categorized into three main classes of security approaches: machine learning-based methods, deep learning-based methods, and hybrid or bio-inspired techniques. This classification enables a comprehensive analysis of current methodologies, highlighting their strengths, limitations, and their practical relevance to securing IoMT environments against increasingly sophisticated cyber threats.

2.4.1 Advanced Approaches in Intrusion Detection Systems for IoMT

With the increasing complexity of cyberattacks targeting healthcare infrastructures, conventional intrusion detection systems (IDS) often fall short in providing real-time, adaptive, and intelligent protection. In response, modern approaches leveraging Machine Learning (ML), Deep Learning (DL), and hybrid models have emerged as innovative and effective solutions for enhancing IDS capabilities within the IoMT ecosystem.

This section reviews recent research employing these intelligent techniques to improve detection accuracy and adapt to the dynamic nature of medical data.

2.4.1.1 Machine Learning-Based IDS

Machine Learning (ML)-based IDS are widely used to identify abnormal or malicious behavior by analyzing historical patterns in network or system data. These systems are capable of learning automatically from data and adapting to evolving threats without the need for explicit programming. In

Internet of Medical Things (IoMT) environments, where real-time data and security requirements are critical, ML offers flexible and efficient solutions for detecting intrusions with high accuracy.
Several supervised classification algorithms are frequently applied in this context. The most commonly used models are described below :

Decision Tree (DT) is a non-parametric supervised learning algorithm used for classification and regression. It builds a hierarchical structure by recursively splitting the data based on feature tests, leading to final predictions at the leaf nodes. Due to its interpretability and simplicity, it is widely applied in machine learning, particularly in cybersecurity and intrusion detection systems [30].
Figure 2.1 illustrates the basic structure of a decision tree, showing how input data is split into branches until reaching leaf nodes that determine the final output.

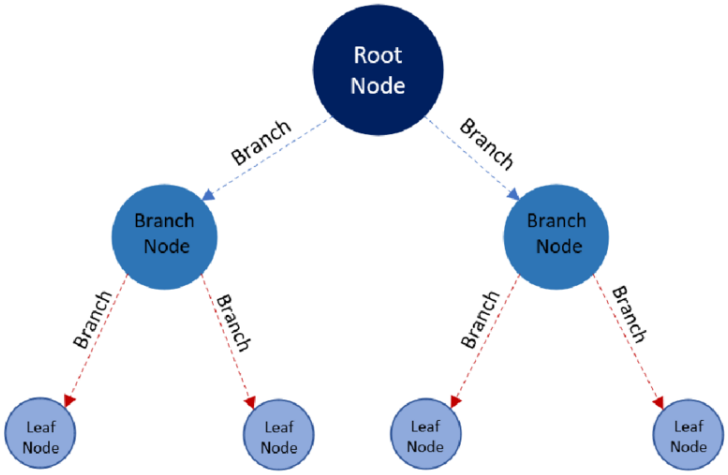

Figure 2. 1. Decision tree [31].

Random Forest (RF) is a popular ensemble learning method that combines the predictions of multiple decision trees to improve accuracy and robustness. During the training phase, it builds several decision trees on different subsets of the dataset, using a random selection of features. For classification tasks, the final output is determined by the majority vote of all trees, while for regression, the average of their predictions is used [32].

Logistic Regression (LogR) is a supervised learning algorithm mainly used for binary classification tasks. Although it is a linear model, it differs from classical linear regression through the use of the logistic function, which models the probability that a given sample belongs to a particular class. Logistic regression is appreciated for its simplicity, fast training speed, and good performance on linearly separable problems, making it a common choice for the initial stages of intrusion detection or exploratory data analysis [33].

Naive Bayes (NB) Naive Bayes is a supervised classification algorithm based on Bayes' theorem, which estimates the probability of a class given a set of features by assuming conditional independence among them. This method uses the prior probability of each class and the likelihood of the observed features to compute the posterior probability [34].

Support Vector Machine (SVM) is a supervised learning algorithm used mainly for classification and, in some cases, regression. It works by finding the optimal hyperplane that maximizes the margin between classes in a multidimensional space. SVM is effective in high-dimensional settings and can handle both continuous and categorical data, even when classes are not linearly separable [35].
Figure 2.2 illustrates the principle of binary classification using Support Vector Machines, where the optimal hyperplane separates two distinct classes with maximum margin.

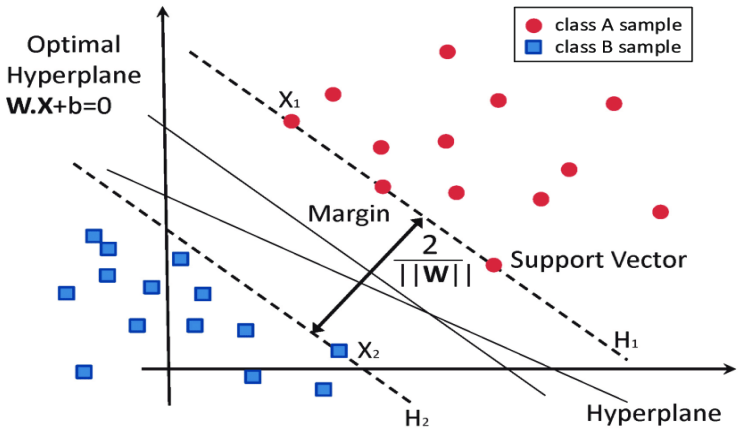

Figure 2. 2. SVM Classification with Optimal Hyperplane [36].

XGBoost (Extreme Gradient Boosting) is a powerful and scalable supervised learning algorithm based on the gradient boosting framework. It is designed to improve the performance of weak learners, particularly decision trees, in both classification and regression tasks. One of its key innovations is the use of a second-order Taylor expansion of the loss function, which allows for more precise optimization. XGBoost is also known for its efficiency, regularization capabilities, and high predictive accuracy, making it widely adopted in real-world machine learning applications [37].
Figure 2.3 presents the general structure of the XGBoost model, which consists of an ensemble of decision trees built sequentially to minimize prediction errors.

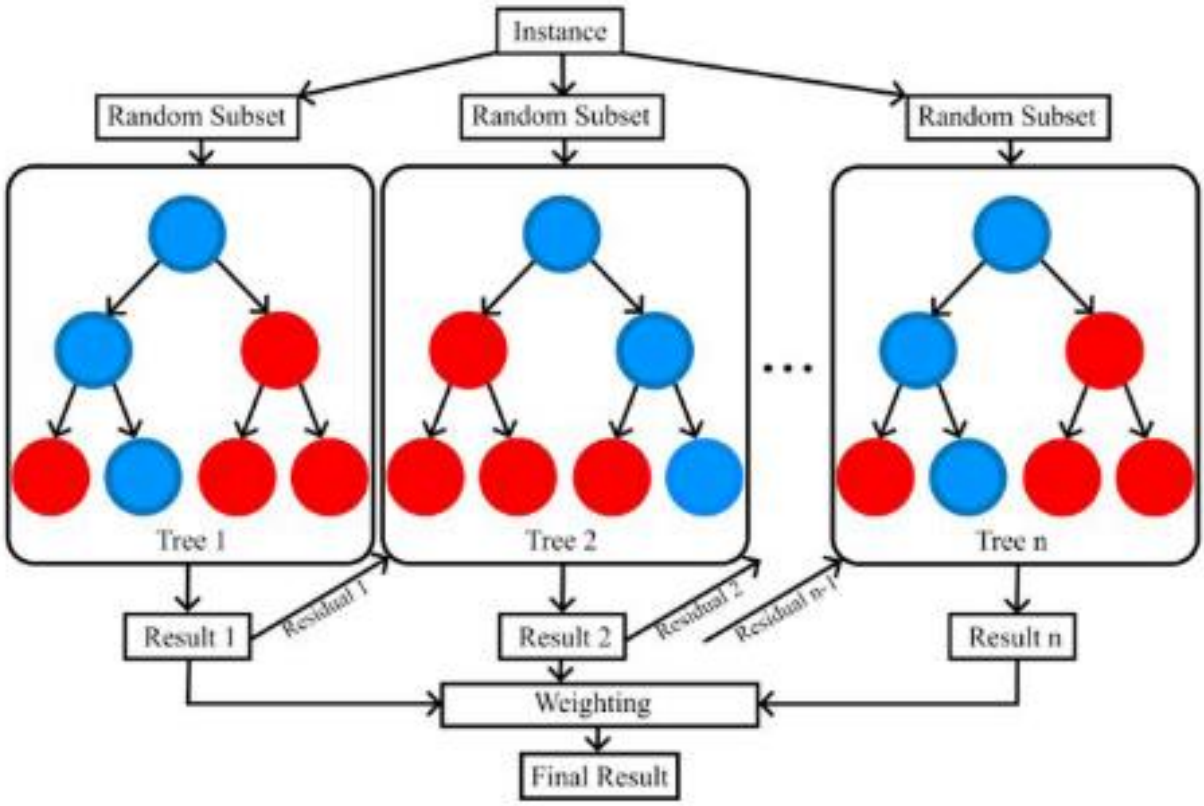

Figure 2. 3. XGBoost Model Structure [38].

2.4.1.2 Deep Learning-Based IDS

A Deep Learning-based Intrusion Detection System (IDS) leverages deep neural networks to detect anomalies or malicious behaviors within network traffic or system activity. By learning patterns from large volumes of data, these systems can identify subtle deviations from normal behavior, making them particularly effective for securing complex environments such as the Internet of Medical Things (IoMT). In this context, several Deep Learning models are commonly used for intrusion detection. The most widely adopted architectures are presented below [43].

Convolutional Neural Network (CNN): CNNs are primarily used for spatial feature extraction from structured input like network traffic matrices. They are particularly effective in identifying localized patterns, making them suitable for detecting intrusion signatures in IoMT data streams. Figure 2.4 presents the architecture of a Convolutional Neural Network (CNN), which utilizes convolutional and pooling layers to automatically learn spatial features from input data.

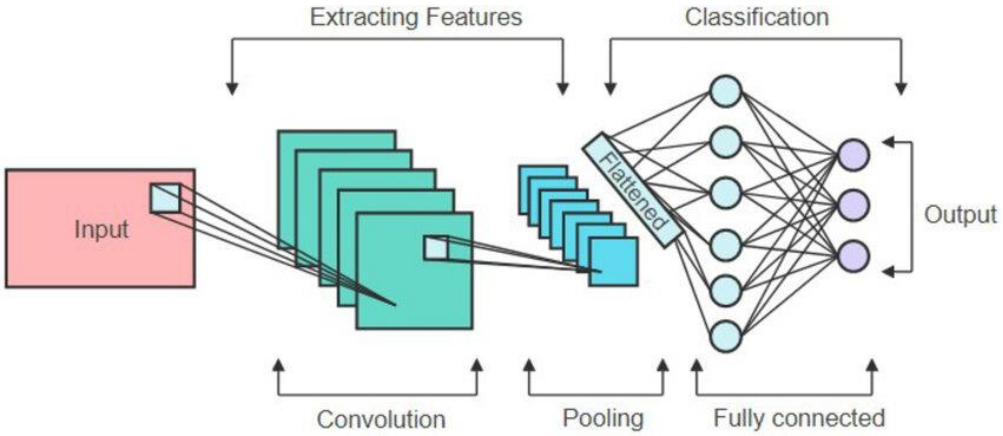

Figure 2. 4. Convolutional Neural Network (CNN) Architecture [44].

Long Short-Term Memory (LSTM): LSTMs are a type of recurrent neural network (RNN) capable of learning long-term dependencies, especially useful for sequential data. In IoMT environments, they can model the temporal evolution of network traffic, enhancing the detection of time-dependent attack patterns.

Deep Neural Network (DNN): DNNs are multi-layers perceptrons that capture complex nonlinear relationships in large datasets. They are effective for high-dimensional intrusion detection tasks, especially when used with feature engineering or attention mechanisms.

Figure 2.5 illustrates the architecture of a Deep Neural Network (DNN), composed of multiple hidden layers that extract and transform features to perform classification.

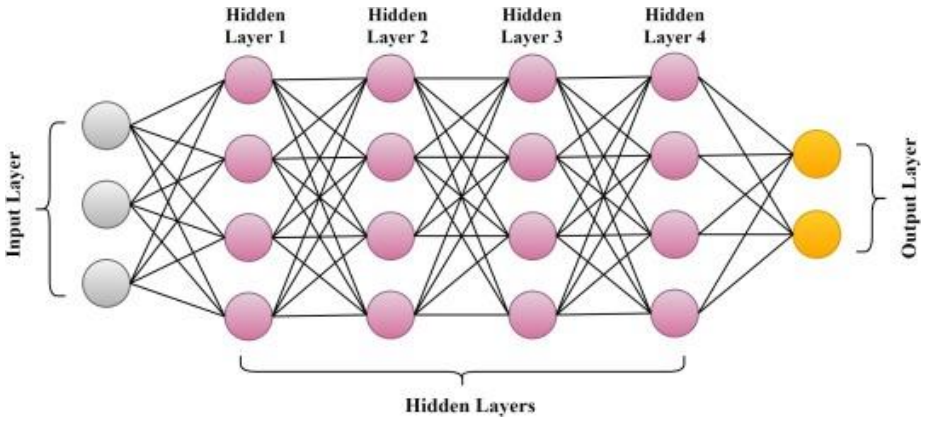

Figure 2. 5. Deep Neural Network (DNN) Architecture [45].

2.4.1.3 Hybrid and Bio-Inspired IDS Approaches

As cyber threats targeting IoMT systems become more complex, standalone machine learning (ML) or deep learning (DL) techniques often face limitations in terms of efficiency and adaptability. To overcome these challenges, hybrid approaches that combine bio-inspired algorithms with ML or DL have been introduced. These methods are inspired by natural processes such as evolution, the immune system, or collective swarm behavior. They help improve feature selection, optimize model parameters, and enhance the generalization ability of detection systems. Such approaches are especially suitable for intrusion detection in medical environments, where both precision and resource constraints are critical. Various studies have employed bio-inspired techniques to enhance security in the Internet of Medical Things (IoMT). Below are some notable findings:

A comprehensive review of existing research on intrusion detection in the Internet of Medical Things (IoMT) has been conducted, with particular emphasis on methodological trends and performance benchmarks. The findings of this review were presented at the IAM'24 conference, offering critical insights into current advancements and persisting gaps in the field [54].

2.5 Conclusion

This chapter reviewed existing research on IoMT security. The comparative analysis highlights that hybrid approaches, especially those integrating bio-inspired algorithms with machine or deep learning models, offer superior performance in feature optimization and anomaly detection. These insights support the development of our proposed hybrid model, which will be presented in the next chapter to enhance intrusion detection in healthcare environments.

Chapter 3: Conception and Implementation

3.1 Introduction

This chapter presents the conception and implementation of MedCentry, a hybrid intrusion detection system designed for Internet of Medical Things (IoMT) environments. The proposed architecture integrates a bio-inspired Clonal Selection Algorithm (CSA) for optimal feature selection and a Deep Neural Network (DNN) for robust classification of network traffic. This system aims to detect cyber threats accurately and efficiently while considering the resource constraints and complexity of smart healthcare environments.

3.2 Proposed Model

In this study, we proposed hybrid intrusion detection system tailored for IoMT environments. The architecture combines two complementary components:

- A Clonal Selection Algorithm (CSA) for optimal feature selection,
- A Deep Neural Network (DNN) for classification of network traffic as either benign or malicious.

Figure 3.1 illustrates the architecture of the hybrid CSA-DNN intrusion detection system

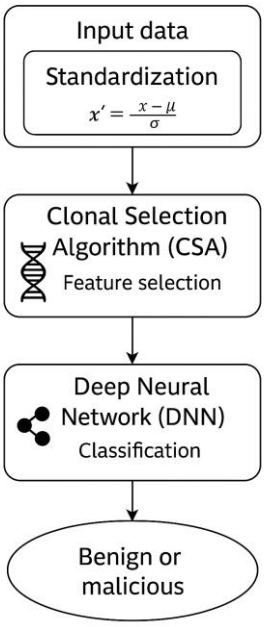

Figure 3. 1. Proposed CSA-DNN Model Architecture.

3.2.1 Biological Principle of Clonal Selection

The Clonal Selection Algorithm (CSA) draws inspiration from the adaptive immune system, particularly

the behavior of B lymphocytes. When an antigen is detected, B-cells that match the antigen undergo [55]:

- Cloning, to amplify the immune response,
- Mutation, to introduce diversity and improve recognition,
- Selection, based on their affinity to the antigen.

This biological process results in memory and strong protection against future threats. CSA translates this mechanism into a computational optimization technique for identifying the most relevant features in a dataset.

Figure 3.2 visualizes the biological clonal selection process that inspired the CSA.

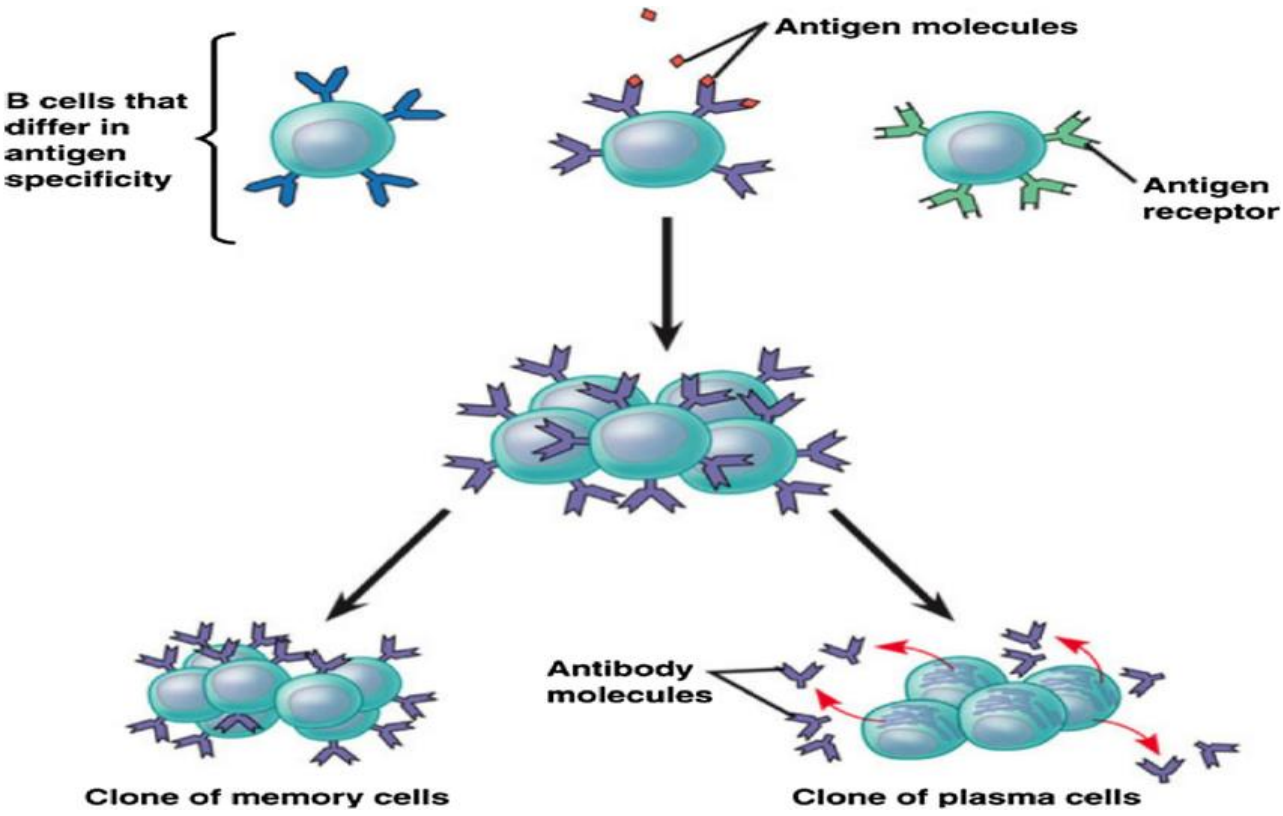

Figure 3. 2. Biological clonal selection process [55].

3.2.2 Functioning of CSA for Feature Selection

In proposed model, each candidate solution is encoded as a binary vector of length D, where D is the total number of available features.

A bit set to 1 means the corresponding feature is selected, while 0 means it is excluded.

3.3 Implementation

3.3.1 Runtime Environment

The experiments were conducted using Google Colaboratory (Colab), a cloud-based Python development environment offering free access to virtualized computational resources. The full implementation pipeline, including data preprocessing, feature selection, and classification, was developed and executed within this environment.

The system was accessed from a local machine with the following specifications:

- Operating System : Windows 10
- Processor : Intel Core i5-7440HQ CPU @ 2.80GHz
- Memory : 8GB RAM
- Google Colaboratory, more commonly known as Google Colab, is a free cloud-based platform developed by Google Research. It provides a serverless Jupyter notebook environment that supports interactive Python development with access to powerful hardware accelerators such as CPUs, GPUs, and TPUs. It is widely used for prototyping and training machine learning models, especially in research and academic contexts.[63]

3.3.2 Libraries and Tools

The development of the hybrid CSA-DNN intrusion detection system relied on a combination of open-source Python libraries and front-end web technologies. Each tool contributed to a specific stage of the system, from data preprocessing to model training and web deployment.

- NumPy: (Numerical Python) is a core library for scientific computing in Python. It enables efficient manipulation of large multi-dimensional numerical arrays and serves as a foundation for many other scientific libraries [64].
- Pandas: (short for Python and data analysis) is an open-source Python library that provides powerful tools for data manipulation and analysis. It offers robust data structures, such as Series and DataFrames, which enable efficient handling of tabular, heterogeneous, and labeled data [65].
- Scikit-learn: is a well-established open-source machine learning library developed in 2007. It offers a wide range of algorithms for tasks such as classification, regression, clustering, and dimensionality reduction. In addition, it provides modules for data preprocessing, feature extraction, hyperparameter tuning, and model evaluation [66].

- SMOTE: (Synthetic Minority Oversampling Technique) is an oversampling method used to address imbalanced datasets. It generates synthetic samples by interpolating between a minority class instance and its K nearest neighbors in the feature space. This technique helps reduce overfitting and improves the model's ability to correctly classify minority class instances [67].
- TensorFlow: is a powerful open-source machine learning framework developed by Google Brain. It provides a comprehensive ecosystem of tools and libraries for building and training deep learning models, including Keras, its high-level API, which simplifies the construction of neural networks such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) [68].
- Matplotlib: is a widely used data visualization library in the Python ecosystem. Originally developed by John Hunter, it enables the creation of static, interactive, and animated plots. It is fully compatible with libraries such as NumPy and Pandas, making it essential for data analysis and visual representation in scientific research [69].
- Seaborn: is a Python data visualization library built on top of Matplotlib. It provides a high-level interface for generating attractive and informative statistical graphics, such as heatmaps and distribution plots, which assisted in understanding the internal behavior of the model [70].
- Flask: is a Python micro-framework designed for rapid web application development. It provides only the essential core features, allowing developers to flexibly integrate additional functionalities as needed during implementation [71].

In addition to Python-based tools, this project also utilized front-end web technologies to develop the graphical interface of the system:

- HTML: (HyperText Markup Language) is the standard markup language used to define the structure and content of web pages. Created by Tim Berners-Lee in 1989, it organizes web content through a set of elements that describe how text, images, and other components are displayed in a browser [72].

- CSS: (Cascading Style Sheets), as defined by the W3C (World Wide Web Consortium), is the language used to describe the presentation of web pages, including colors, fonts, and layouts. It enables responsive and customized styling for HTML documents across devices of different screen sizes [72].

- JavaScript: is a dynamically typed, high-level programming language with asynchronous capabilities. It was developed by Brendan Eich in 1994 and originally named *Mocha*, then *LiveScript*, before becoming *JavaScript*. It is now a core web technology used to add interactivity and dynamic behavior to web applications [73].

3.3.3 Exploratory Data Analysis

This section explores the characteristics of the two datasets used in this study: WUSTL-EHMS-2020

[23] and CIC-IoMT2024[26]. The goal is to highlight class imbalances, variable types, and any necessary preprocessing requirements.

Figure 3.3 shows the distribution of normal and attack traffic in the WUSTL-EHMS-2020 dataset, where label 0 represents normal traffic and label 1 corresponds to attack traffic.

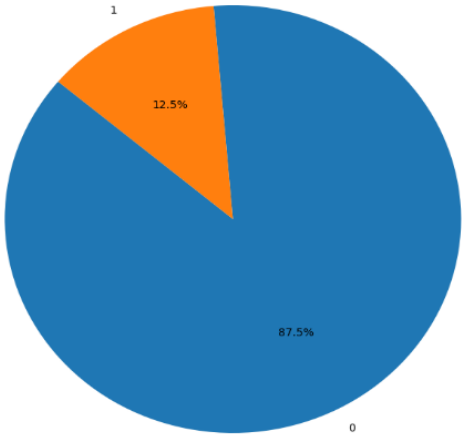

Figure 3. 3. Class Distribution in the WUSTL-EHMS-2020 Dataset

Figure 3.4 displays the distribution of the six traffic classes in the CIC-IoMT2024 dataset.

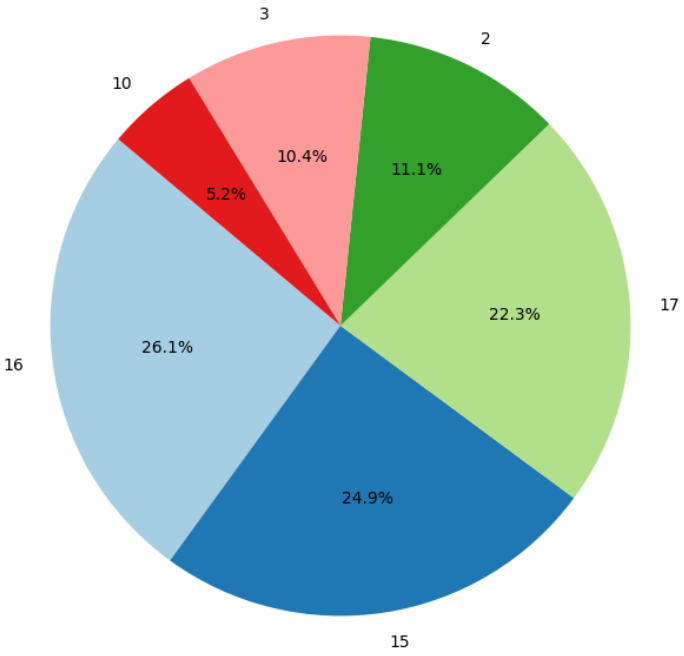

Figure 3. 4. Class Distribution in the CIC-IoMT-2024 Dataset

3.3.4 Preprocessing

To ensure reliable training and evaluation of the proposed hybrid IDS, a dedicated preprocessing pipeline was applied to both the CIC-IoMT-2024 and WUSTL-EHMS-2020 datasets. This step was essential to clean the data, the distinct nature and structure of each dataset necessitated specific adaptations, as detailed below.

a. CIC-IoMT-2024 Dataset [26]

1. Data Cleaning: Using Pandas, the dataset was inspected for missing values, infinite values, and constant columns. The columns that contained only zero values were removed due to their lack of relevance.
2. Data Splitting:The dataset was split using stratified sampling into: 80% training,20% testing.
3. Label Encoding:The class labels in y were encoded into integers to ensure compatibility with machine learning algorithms.

b. WUSTL-EHMS-2020 Dataset [23]

1. Data Cleaning
2. Categorical Encoding
3. Feature and Target Separation
4. Feature Scaling:
5. Data Splitting: The preprocessed data was divided into 80% training and 20% testing sets. The 80/20 split is commonly used to provide enough data for training the model (80%) while reserving a sufficient portion for reliable evaluation (20%).
6. SMOTE Oversampling: This method synthetically generated new instances of the minority class to achieve a balanced class distribution and improve classification performance.

3.3.5 Model Building

This section presents the design, implementation, and performance evaluation of the proposed hybrid Intrusion Detection System (IDS), which integrates a Clonal Selection Algorithm (CSA) for feature selection with a Deep Neural Network (DNN) for classification. The experiments were conducted independently on two datasets: CIC-IoMT-2024 and WUSTL-EHMS-2020.

a. Feature Selection using Clonal Selection Algorithm (CSA)

Selected Features: At the end of the optimization process, the following features were selected:

For CIC-IoMT-2024 (35 features) :

Header_Length, Protocol Type, Duration, Rate, Drate, fin_flag_number,syn_flag_number, rst_flag_number, psh_flag_number, ack_flag_number,cwr_flag_number, ack_count, syn_count, fin_count, rst_count, HTTP, HTTPS,Telnet, SMTP, IRC, TCP, DHCP, ARP, IGMP, IPv, LLC, Tot sum,Min, Max, AVG, Std, IAT, Number, Magnitude, Covariance.

For WUSTL-EHMS-2020 (33 features):

Dir, Flgs, SrcAddr, DstAddr, Dport, SrcLoad, DstLoad, SrcGap, DstGap,DIntPkt, SIntPktAct, DIntPktAct, SrcJitter, dMaxPktSz, dMinPktSz, Trans,TotPkts, TotBytes, Load, Loss, pLoss, pSrcLoss, pDstLoss, Rate, SrcMac, DstMac, Packet_num, Temp, SYS, DIA, Resp_Rate, ST.

b. Deep Neural Network

Each selected feature subset was passed into a DNN model. The architecture was consistent across datasets but adapted in the output layer.

3.4 Evaluation

The generalization capability and robustness of the proposed hybrid model were assessed on the test sets of both CIC-IoMT-2024 and WUSTL-EHMS-2020 datasets. For each dataset, a confusion matrix was generated to provide a comprehensive view of the classification performance, including correct predictions and misclassifications per class.

- Figure 3.5 presents the confusion matrix for the WUSTL-EHMS-2020 dataset, demonstrating the model's ability to accurately distinguish between benign and malicious instances in a binary classification context.
- Figure 3.6 illustrates the confusion matrix obtained on the CIC-IoMT-2024 dataset, highlighting the model's effectiveness in handling multiclass classification scenarios within heterogeneous IoMT traffic.

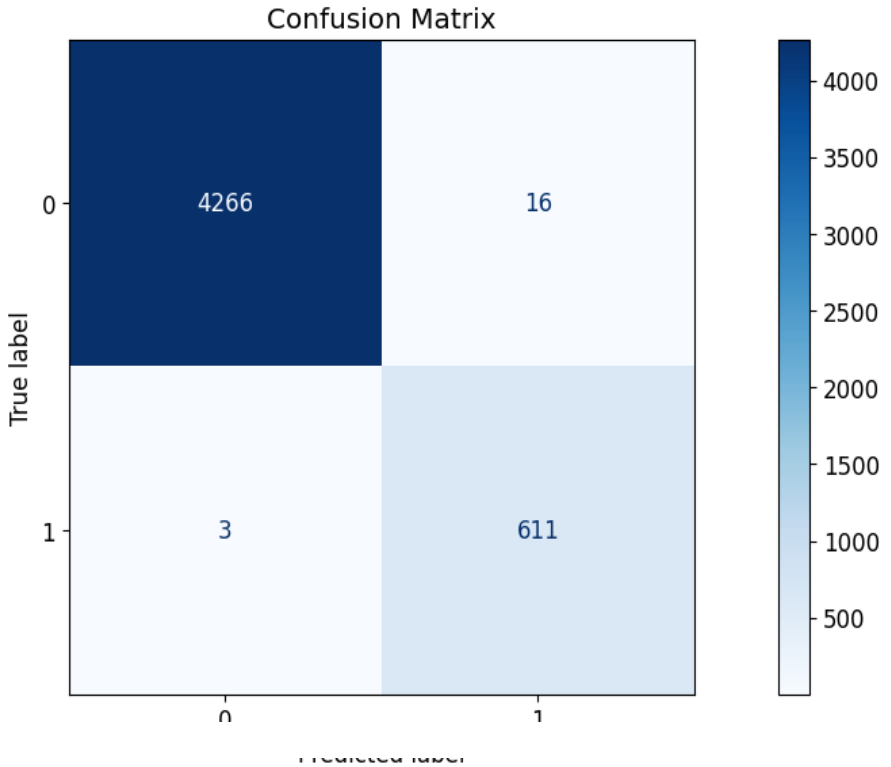

Figure 3. 5. Confusion Matrix of the CSA-DNN model on the WUSTL-EHMS-2020 dataset.

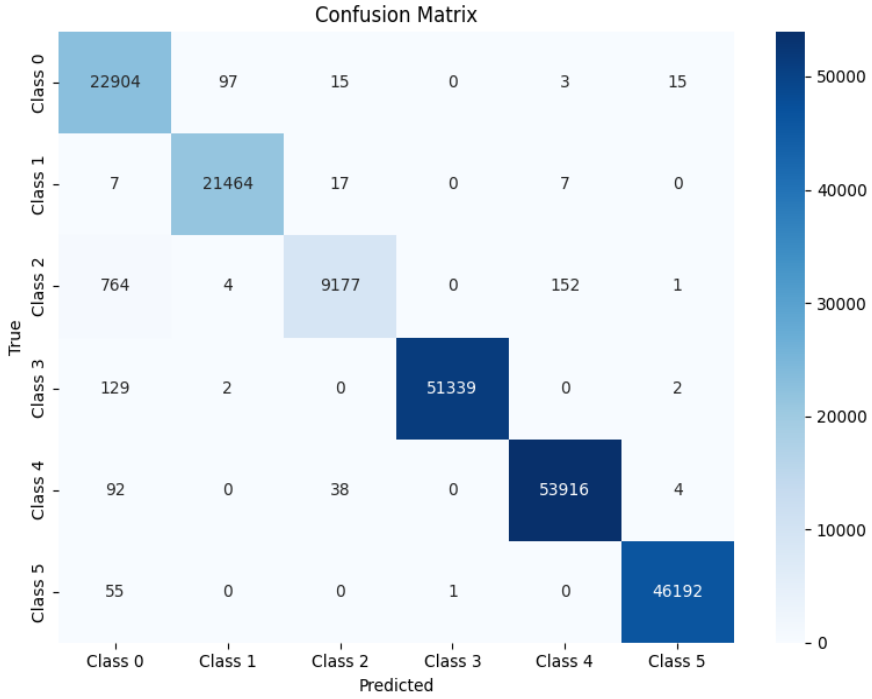

Figure 3. 6. Confusion Matrix of the CSA-DNN model on the CIC-IoMT-2024 dataset.

These results indicate a high detection capability with strong sensitivity and specificity, demonstrating the system's ability to effectively minimize both missed threats and false alarms.

The Precision-Recall curve [75], offers a comprehensive assessment of the model's performance across various decision thresholds for both datasets, highlighting its ability to maintain a balance between precision and recall under different classification conditions. Figures 3.7 and 3.8 illustrate the Precision–Recall curves of the model on the WUSTL-EHMS-2020 and CIC-IoMT-2024 datasets, respectively.

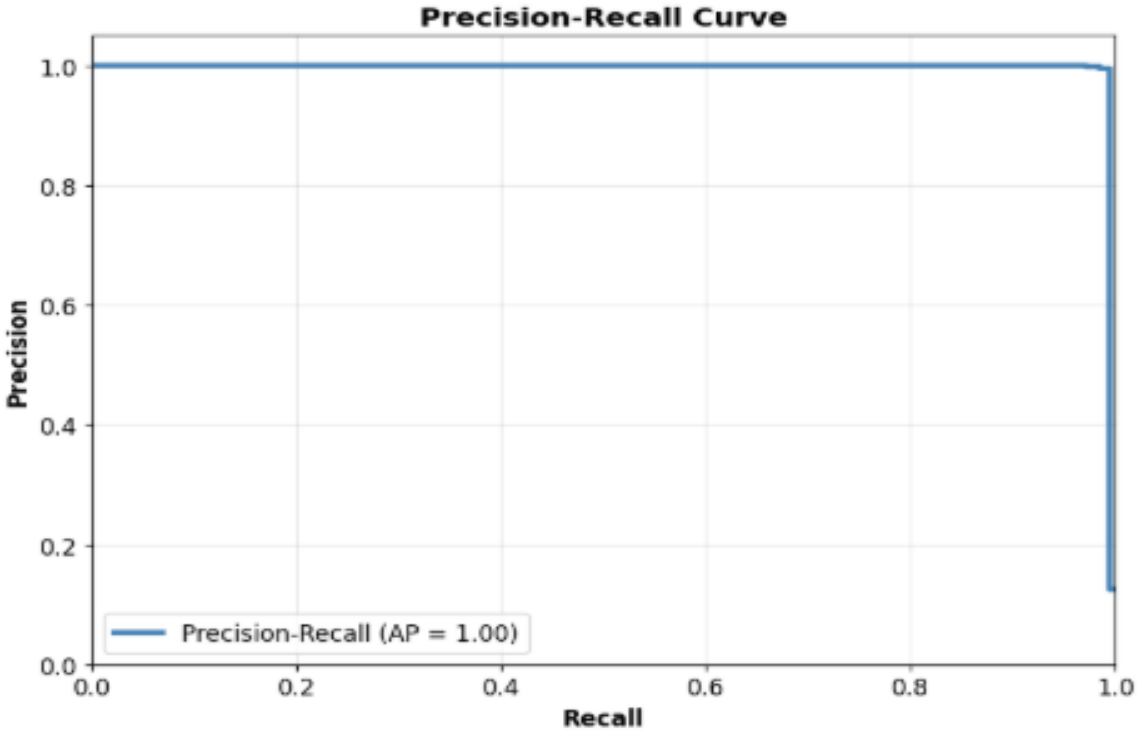

Figure 3. 7. Precision-Recall Curve on the WUSTL-EHMS-2020 Dataset.

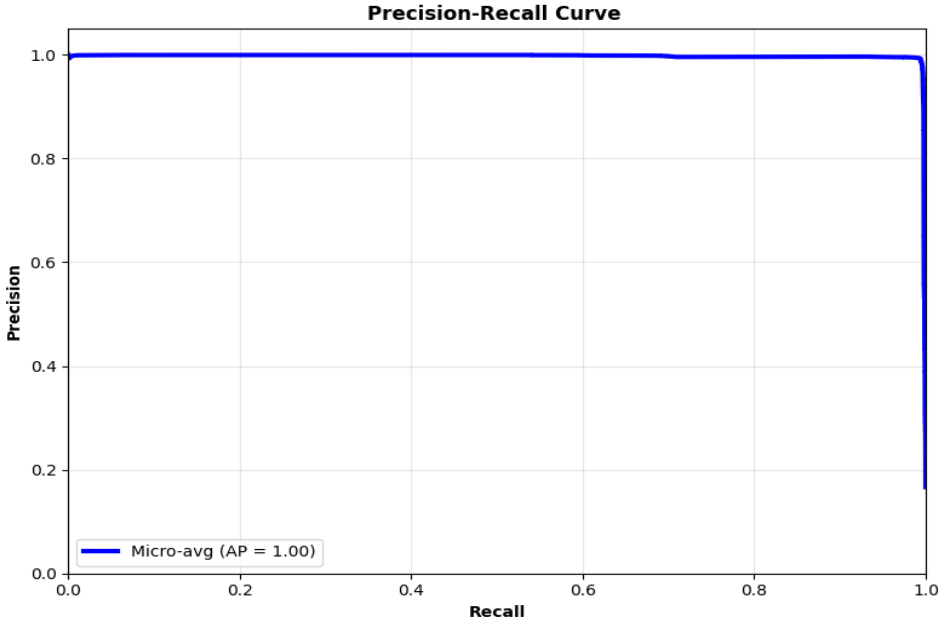

Figure 3. 8. Precision-Recall Curve on the CIC-IoMT-2024 Dataset.

The Precision-Recall curve remains consistently high across a wide range of recall values, indicating the model's strong ability to detect true positives while keeping false positives to a minimum.

3.6 Web User Interface

To facilitate the practical use of the CSA-DNN detection system, a web interface was developed using Flask. This interface allows users to easily interact with the model through a series of well-defined steps, simulating a real-world IoMT intrusion detection workflow.

The MEDCENTRY interface guides the user through a complete offline intrusion detection and cleaning workflow, simulating a realistic usage scenario. It enables users — such as medical IT staff or cybersecurity analysts to detect, analyze, and mitigate threats within sensitive healthcare infrastructures. Figure 3.9 shows the homepage of the MEDCENTRY web interface, followed by the main pages used for navigation and functionality.

Figure 3. 9.Home Page of the MEDCENTRY Web Interface.

The **homepage** of MEDCENTRY features a **"Get Started"** button to launch the detection process. On the same page, **"About Us"** briefly explains that MEDCENTRY helps secure IoMT networks by detecting and cleaning threats

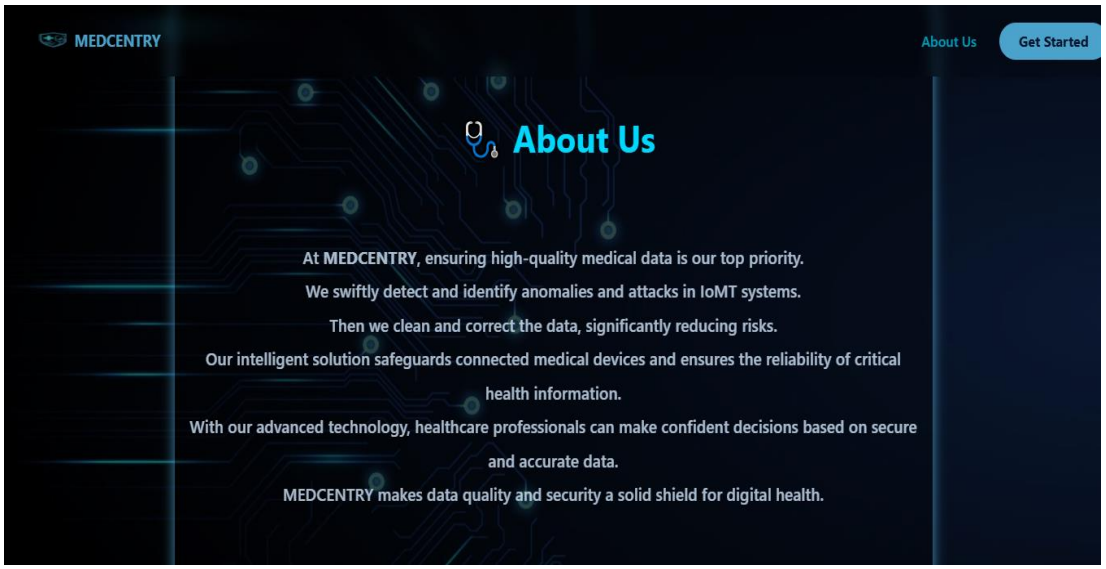

Figure 3. 10.About Page of MEDCENTRY Web Interface.

The following steps describe the typical usage process of the MEDCENTRY web interface for analyzing medical network traffic:

Step 1 : CSV File Upload

The user begins by uploading a CSV file containing network traffic data from medical devices. This file may include both normal traffic and potential intrusions. Figure 3.11 displays the upload form where users submit CSV files for analysis.

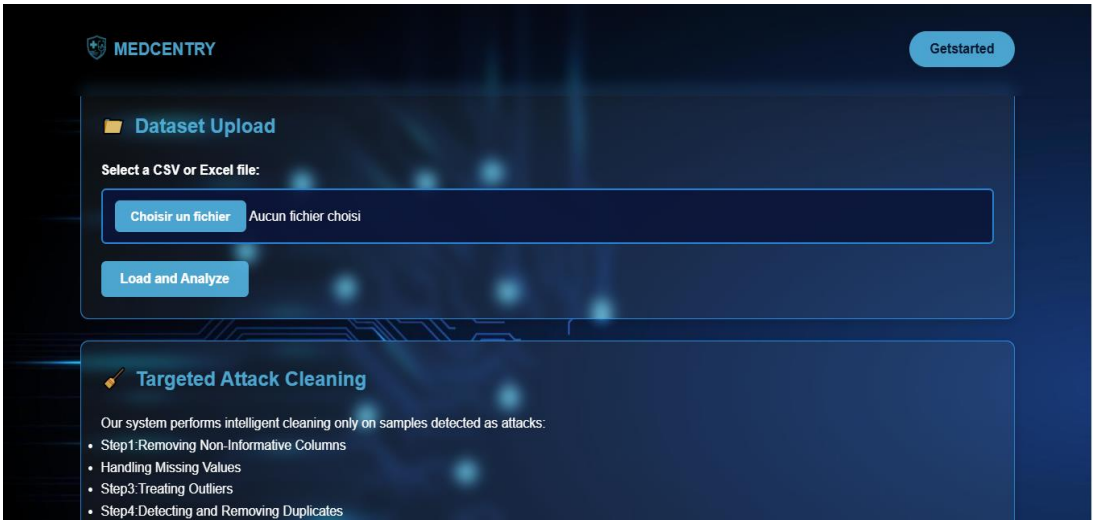

Figure 3. 11. CSV File Upload Page.

Step 2: Initial Intrusion Detection

Once uploaded, the system immediately runs the CSA-DNN model to detect any malicious instances. The number of detected intrusions is displayed, giving the user an overview of the dataset's current threat level. Figure 3.12 shows the immediate results after the uploaded file is processed.

Figure 3. 12.Intrusion Detection Result interface.

Step 3: Automated Data Cleaning

After the CSV file is uploaded and the initial detection is complete, the system executes an advanced data cleaning routine encapsulated in the function clean_data(df). This function ensures data quality and reliability before any re-evaluation. It performs the following operations:

- Removal of non-informative columns: All empty columns or those with constant values are eliminated to reduce noise and redundancy.
- Elimination of duplicates: Fully duplicated rows are detected and removed to prevent bias in the model.
- Handling of missing values:
    - Rows with more than 50% missing values are discarded.
    - Remaining missing values in numeric columns are imputed using the median to preserve data distribution.
- Outlier detection and correction: Outliers are detected using the Interquartile Range (IQR) method. For each numeric feature:

First, the first quartile (Q1, 25th percentile) and the third quartile (Q3, 75th percentile) are calculated. The interquartile range (IQR) is then defined as the difference between Q3 and Q1:

$$IQR = Q3 - Q1 \quad (9)$$

Next, the lower and upper bounds are determined using the formulas:

$$\text{Lower bound} = Q1 - 1.5 \times IQR \quad (10)$$

$$\text{Upper bound} = Q3 + 1.5 \times IQR. \quad (11)$$

Any value falling outside these bounds is considered an outlier and is corrected by clipping it to the nearest bound. This method reduces the impact of extreme values while preserving the integrity of the dataset by avoiding the removal of entire rows.

- Attack tracking: If the prediction column is present, the system tracks the number of attacks (prediction = 1) before and after cleaning.

A detailed cleaning report is automatically generated, including:

- Initial and final dataset shape,
- List of removed columns,
- Number of duplicate rows eliminated,
- Number of missing values imputed,
- Number of outliers corrected,
- Total number of detected attacks before and after cleaning.

Figure 3.13 presents the automated report generated during the data cleaning step.

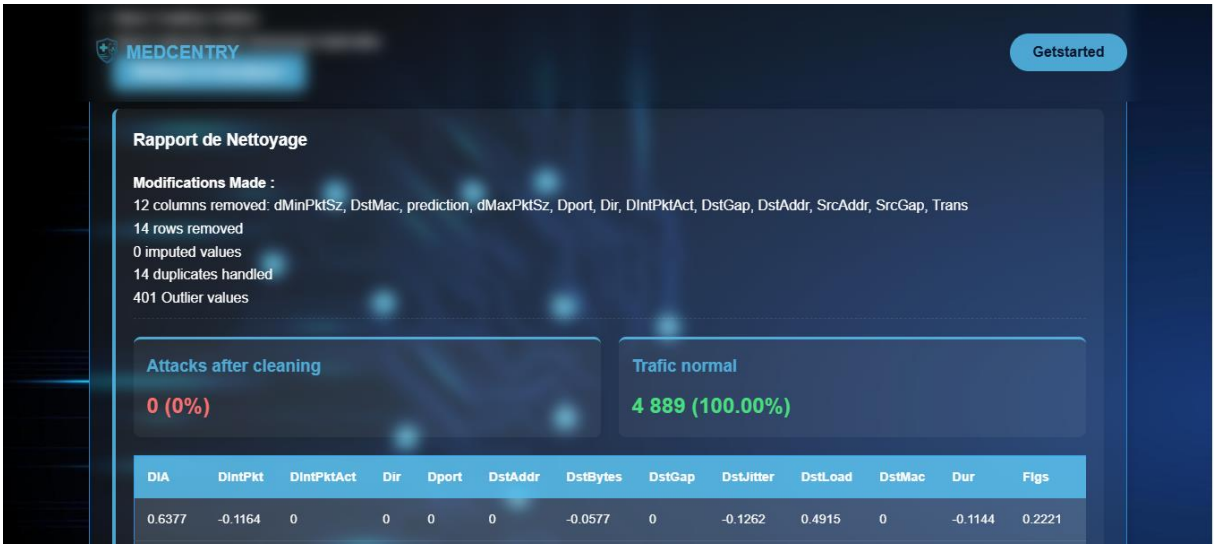

Figure 3. 13. Automated Data Cleaning Summary.

Step 4: Re-detection on Cleaned Data

The cleaned dataset is then re-analyzed by the proposed CSA-DNN model. This second detection step verifies the effectiveness of the cleaning process. In most cases, the output shows “0 attacks detected”, confirming that all threats have been successfully removed.

Step 5: Attack Comparison Report

The final step provides a comparative summary between the number of attacks before and after cleaning. This output helps users assess the real impact of the cleaning phase. If the system detects “0 attacks” post-cleaning, the file is declared clean and ready for reintegration into the medical network.

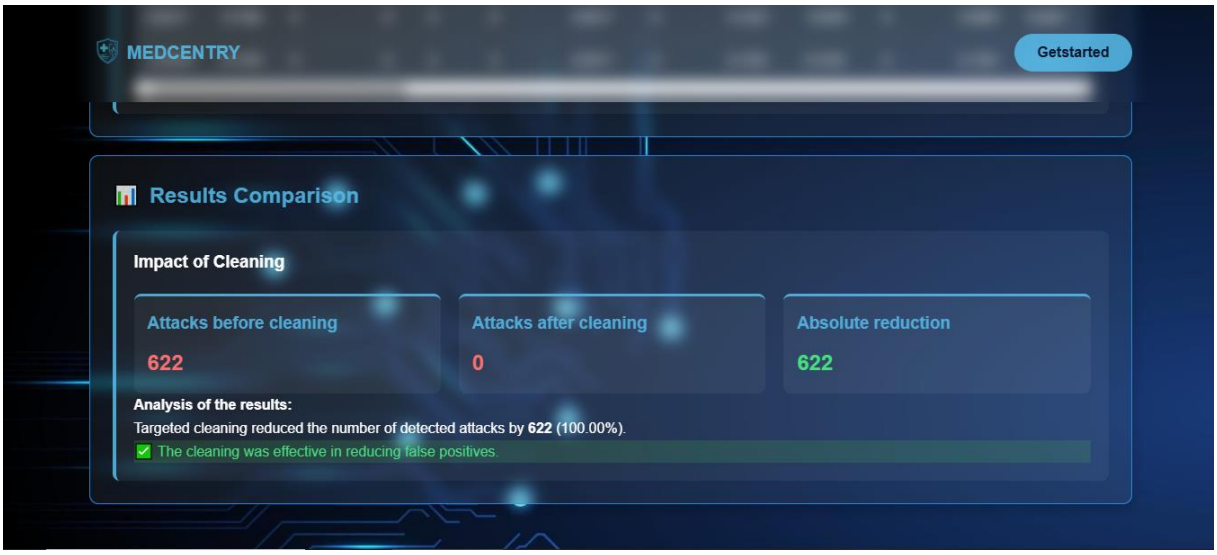

Figure 3. 14. Attack Comparison Report Interface.

3.7 Conclusion

This chapter has presented the conception, development, and empirical validation of MedCentry, a hybrid intrusion detection system (IDS) that integrates CSA-based feature selection with DNN-based classification to enhance threat detection in Internet of Medical Things (IoMT) networks. The proposed system was rigorously evaluated on two benchmark datasets simulating real-world IoMT environments, demonstrating superior performance in terms of detection accuracy, precision, recall, and computational efficiency compared to conventional approaches.

To ensure practical applicability, the system was implemented as a web-based platform using Flask, providing healthcare professionals with an intuitive, step-by-step interface for analyzing potential cyber threats. A comparative analysis against baseline models, including Random Forest (RF), DNN, Convolutional Neural Network (CNN), and Particle Swarm Optimization (PSO)-based IDS, confirmed that MedCentry consistently achieves higher detection rates while maintaining lower false positives and processing latency.

These results confirm that MedCentry is a promising and effective solution for protecting smart medical networks against cyber threats.

General Conclusion

In an era where medical technologies are increasingly interconnected through the Internet of Medical Things (IoMT), ensuring the security and integrity of sensitive health data has become a paramount concern. This thesis addressed the critical challenge of intrusion detection in IoMT environments, which are particularly vulnerable due to their heterogeneous composition, constrained resources, and the high sensitivity of the data they handle.

To meet this challenge, we proposed a hybrid Intrusion Detection System (IDS) named **MEDCENTRY**, which combines a Clonal Selection Algorithm (CSA) for optimal feature selection with a Deep Neural Network (DNN) for efficient and accurate classification. Our approach was rigorously evaluated using two benchmark medical datasets: CIC-IoMT2024 and WUSTL-EHMS-2020.

This master thesis is organized into three chapters. The first chapter introduces the IoMT paradigm, outlines its benefits, and highlights the specific security challenges it faces. The second chapter provides a synthesis of existing security solutions, particularly those based on machine learning and bio-inspired methods, and describes the datasets employed. The third chapter presents the proposed model, implementation details, and experimental validation.

Throughout this work, we demonstrated that the synergy between evolutionary optimization and deep learning offers a powerful and scalable solution for real-time intrusion detection, even within the constraints typical of medical networks. The experimental results confirmed the robustness, generalization capacity, and practical viability of the MEDCENTRY framework in real-world healthcare contexts.

This research contributes to the growing field of intelligent cybersecurity in medical systems by proposing a method that is not only accurate but also adaptable and lightweight. It opens several promising avenues for future research, such as deploying MEDCENTRY in live hospital networks, integrating federated learning for privacy preservation, and extending the model to detect zero-day attacks and insider threats.

By enhancing the resilience of IoMT infrastructures, MEDCENTRY plays a crucial role in safeguarding patient safety, preserving trust in digital healthcare systems, and supporting the broader vision of smart, secure, and connected medical care.

Bibliography

[1] Ashoor, A. S., & Gore, S. (2011). Importance of intrusion detection system (IDS). *International Journal of Scientific and Engineering Research*, *2*(1), 1-4.

[2] Thakkar, A., & Lohiya, R. (2022). A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artificial Intelligence Review*, *55*(1), 453-563.

[3] Jyothsna, V. V. R. P. V., Prasad, R., & Prasad, K. M. (2011). A review of anomaly based intrusion detection systems. *International Journal of Computer Applications*, *28*(7), 26-35.

[4] Kumar, Y., & Subba, B. (2023). Stacking ensemble-based HIDS framework for detecting anomalous system processes in windows based operating systems using multiple word embedding. *Computers & Security*, *125*, 102961.

[5] Geo Francis, E., & Sheeja, S. (2023, December). IDSSA: An Intrusion Detection System with Self-adaptive Capabilities for Strengthening the IoT Network Security. In *International Conference on Advances in Computational Intelligence and Informatics* (pp. 23-30). Singapore: Springer Nature Singapore.

[6] Pérez-Gaspar, M., Gomez, J., Bárcenas, E., & Garcia, F. (2024). A fuzzy description logic based IoT framework: Formal verification and end user programming. *Plos one*, *19*(3), e0296655.

[7] Chataut, R., Phoummalayvane, A., & Akl, R. (2023). Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0. *Sensors*, *23*(16), 7194.

[8] El-Saleh, A. A., Sheikh, A. M., Albreem, M. A., & Honnurvali, M. S. (2025). The internet of medical things (IoMT): opportunities and challenges. *Wireless networks*, *31*(1), 327-344.

[9] Yuen, S. G. J., Park, J., Ghoreyshi, A., & Wu, A. (2017). *U.S. Patent No. 9,693,711*. Washington, DC: U.S. Patent and Trademark Office.

[10]: Hung, K., Zhang, Y. T., & Tai, B. (2004, September). Wearable medical devices for tele-home healthcare. In *The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society* (Vol. 2, pp. 5384-5387). IEEE.

[11] Perry, L., & Malkin, R. (2011). Effectiveness of medical equipment donations to improve health systems: how much medical equipment is broken in the developing world?. *Medical & biological engineering & computing*, *49*, 719-722.

[12] Rani, S., Kataria, A., Kumar, S., & Tiwari, P. (2023). Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review. *Knowledge-based systems*, *274*, 110658.

[13] Praveen, R., & Pabitha, P. (2023). Improved Gentry–Halevi's fully homomorphic encryption-based lightweight privacy preserving scheme for securing medical Internet of Things. *Transactions on Emerging Telecommunications Technologies*, *34*(4), e4732.

[14] Alsubaei, F., Abuhussein, A., & Shiva, S. (2017, October). Security and privacy in the internet of medical things: taxonomy and risk assessment. In *2017 IEEE 42nd conference on local computer networks workshops (LCN workshops)* (pp. 112-120). IEEE.

[15] Saba, T. (2020, December). Intrusion detection in smart city hospitals using ensemble classifiers. In *2020 13th International Conference on Developments in eSystems Engineering (DeSE)* (pp. 418-422). IEEE.

[16] Li, S., Cao, Y., Liu, S., Lai, Y., Zhu, Y., & Ahmad, N. (2024). Hda-ids: A hybrid dos attacks intrusion detection system for iot by using semi-supervised cl-gan. *Expert Systems with Applications*, *238*, 122198.

[17] Saif, S., Das, P., Biswas, S., Khari, M., & Shanmuganathan, V. (2022). HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare. *Microprocessors and Microsystems*, 104622.

[18] Gide, A. I., & Mu'azu, A. A. (2024). A real-time intrusion detection system for dos/ddos attack classification in IoT networks using KNN-neural network hybrid technique. *Babylonian Journal of Internet of Things*, *2024*, 60-69.

[19] Gupta, L., Salman, T., Ghubaish, A., Unal, D., Al-Ali, A. K., & Jain, R. (2022). Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach. *Applied Soft Computing*, *118*, 108439.

[20] Fang, L., Li, Y., Liu, Z., Yin, C., Li, M., & Cao, Z. J. (2020). A practical model based on anomaly detection for protecting medical IoT control services against external attacks. *IEEE Transactions on Industrial Informatics*, *17*(6), 4260-4269.

[21] Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., ... & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems*, *44*, 1-9.

[22] Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Feregrino-Uribe, C. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures. *Internet of Things*, *23*, 100887.

[23] Hady, A. A., Ghubaish, A., Salman, T., Unal, D., & Jain, R. (2020). Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access*, *8*, 106576-106584.

[24] Ahmed, M., Byreddy, S., Nutakki, A., Sikos, L. F., & Haskell-Dowland, P. (2021). ECU-IoHT: A dataset for analyzing cyberattacks in Internet of Health Things. *Ad Hoc Networks*, *122*, 102621.

[25] Zubair, M., Ghubaish, A., Unal, D., Al-Ali, A., Reimann, T., Alinier, G., ... & Qadir, J. (2022). Secure Bluetooth communication in smart healthcare systems: A novel community dataset and intrusion detection system. *Sensors*, *22*(21), 8280.

[26] Dadkhah, S., Neto, E. C. P., Ferreira, R., Molokwu, R. C., Sadeghi, S., & Ghorbani, A. (2024). Ciciomt2024: Attack vectors in healthcare devices-a multi-protocol dataset for assessing iomt device

security. *Raphael and Chukwuka Molokwu, Reginald and Sadeghi, Somayeh and Ghorbani, Ali, CiCIoMT2024: Attack Vectors in Healthcare Devices-A Multi-Protocol Dataset for Assessing IoMT Device Security*.

[27] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms. *Sensors*, *24*(2), 713.

[28] Akhiat, Y., Touchanti, K., Zinedine, A., & Chahhou, M. (2024). IDS-EFS: Ensemble feature selection-based method for intrusion detection system. *Multimedia Tools and Applications*, *83*(5), 12917-12937.

[29] Ahmad, R., Salahuddin, H., Rehman, A. U., Rehman, A., Shafiq, M. U., Tahir, M. A., & Afzal, M. S. (2024). Enhancing database security through AI-based intrusion detection system. *Journal of Computing & Biomedical Informatics*, *7*(02).

[30] Wedagedara, H., Witharana, C., Fahey, R., Cerrai, D., Parent, J., & Perera, A. S. (2024). Non-parametric machine learning modeling of tree-caused power outage risk to overhead distribution powerlines. *Applied Sciences*, *14*(12), 4991.

[31] Chen, A. (2022). Occupancy detection and prediction with sensors and online machine learning: Case study of the Elmia exhibition building in Jönköping.

[32] Salman, H. A., Kalakech, A., & Steiti, A. (2024). Random forest algorithm overview. *Babylonian Journal of Machine Learning*, *2024*, 69-79.

[33] Surdeanu, M., & Valenzuela-Escárcega, M. A. (2024). *Deep learning for natural language processing: a gentle introduction*. Cambridge University Press.

[34] Vishwakarma, M., & Kesswani, N. (2023). A new two-phase intrusion detection system with Naïve Bayes machine learning for data classification and elliptic envelop method for anomaly detection. *Decision Analytics Journal*, *7*, 100233.

[35] Pisner, D. A., & Schnyer, D. M. (2020). Support vector machine. In *Machine learning* (pp. 101-121). Academic Press.

[36] García-Gonzalo, E., Fernández-Muñiz, Z., Garcia Nieto, P. J., Bernardo Sánchez, A., & Menéndez Fernández, M. (2016). Hard-rock stability analysis for span design in entry-type excavations with learning classifiers. *Materials*, *9*(7), 531.

[37] Guembe, B., Misra, S., & Azeta, A. (2024). Federated Bayesian optimization XGBoost model for cyberattack detection in internet of medical things. *Journal of Parallel and Distributed Computing*, *193*, 104964.

[38] Öztornacı, B. U. R. A. K., Ata, B., & Kartal, S. (2024). Analysing household food consumption in Turkey using machine learning techniques. *Agris on-line Papers in Economics and Informatics*, *16*(2).

[39] Hussain, F., Abbas, S. G., Shah, G. A., Pires, I. M., Fayyaz, U. U., Shahzad, F., ... & Zdravevski, E. (2021). A framework for malicious traffic detection in IoT healthcare environment. *Sensors*, *21*(9), 3025.

[40] Zachos, G., Essop, I., Mantas, G., Porfyrakis, K., Ribeiro, J. C., & Rodriguez, J. (2021). An

anomaly-based intrusion detection system for internet of medical things networks. *Electronics*, *10*(21), 2562.

[41] Areia, J., Bispo, I., Santos, L., & Costa, R. L. D. C. (2024). IoMT-TrafficData: Dataset and tools for benchmarking intrusion detection in internet of medical things. *IEEE Access*.

[42] Balhareth, G., & Ilyas, M. (2024). Optimized intrusion detection for IoMT networks with tree-based machine learning and filter-based feature selection. *Sensors*, *24*(17), 5712.

[43] Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). CNN-LSTM: hybrid deep neural network for network intrusion detection system. *IEEE Access*, *10*, 99837-99849.

[44] Ismail, W. N., Alsalamah, H. A., Hassan, M. M., & Mohamed, E. (2023). AUTO-HAR: An adaptive human activity recognition framework using an automated CNN architecture design. *Heliyon*, *9*(2).

[45] Oluleye, B. I., Chan, D. W., & Antwi-Afari, P. (2023). Adopting Artificial Intelligence for enhancing the implementation of systemic circularity in the construction industry: A critical review. *Sustainable Production and Consumption*, *35*, 509-524.

[46] Mohammadi, A., Ghahramani, H., Asghari, S. A., & Aminian, M. (2024, October). Securing Healthcare with Deep Learning: A CNN-Based Model for medical IoT Threat Detection. In *2024 19th Iranian Conference on Intelligent Systems (ICIS)* (pp. 168-173). IEEE.

[47] Faruqui, N., Yousuf, M. A., Whaiduzzaman, M., Azad, A. K. M., Alyami, S. A., Liò, P., ... & Moni, M. A. (2023). SafetyMed: A novel IoMT intrusion detection system using CNN-LSTM hybridization. *Electronics*, *12*(17), 3541.

[48] Ravi, Vinayakumar & Pham, Tuan & Alazab, Mamoun. (2023). Deep Learning-Based Network Intrusion Detection System for Internet of Medical Things. IEEE Internet of Things Magazine. 6. 10.1109/IOTM.001.2300021.

[49] Fadhil, H. M., Dawood, Z. O., & Al Mhdawi, A. (2024). Enhancing Intrusion Detection Systems Using Metaheuristic Algorithms. *Diyala Journal of Engineering Sciences*, 15-31.

[50] Goswami, N., Raj, S., Thakral, D., Arias-Gonzáles, J. L., Flores-Albornoz, J., Asnate-Salazar, E., ... & Kumar, S. (2023). Intrusion detection system for iot-based healthcare intrusions with lion-salp-swarm-optimization algorithm: metaheuristic-enabled hybrid intelligent approach. *Engineered Science*, *25*, 933.

[51] Alamro, H., Marzouk, R., Alruwais, N., Negm, N., Aljameel, S. S., Khalid, M., ... & Alsaid, M. I. (2023). Modelling of Blockchain Assisted Intrusion Detection on IoT Healthcare System using Ant Lion Optimizer with Hybrid Deep Learning. *IEEE Access*.

[52] Norouzi, M., Gürkaş-Aydın, Z., Turna, Ö. C., Yağci, M. Y., Aydin, M. A., & Souri, A. (2023). A hybrid genetic algorithm-based random forest model for intrusion detection approach in internet of medical things. *Applied Sciences*, *13*(20), 11145

[53] Chaganti, R., Mourade, A., Ravi, V., Vemprala, N., Dua, A., & Bhushan, B. (2022). A particle swarm optimization and deep learning approach for intrusion detection system in internet of medical

things. *Sustainability*, *14*(19), 12828.

[54] Merzougui H., Benhamza K., Seridi H. (2024). *A Review of Bio-Inspired Methods for Intrusion Detection in the Internet of Medical Things*. The 7th International Conference on Informatics and Applied Mathematics (IAM'24), December 4–5, 2024, Guelma, Algeria.

[55] Batur Şahin, C., & Abualigah, L. (2021). A novel deep learning-based feature selection model for improving the static analysis of vulnerability detection. *Neural Computing and Applications*, *33*(20), 14049-14067.

[56] Wang, D., Huang, Y., Ying, W., Bai, H., Gong, N., Wang, X., ... & Fu, Y. (2025). Towards Data-Centric AI: A Comprehensive Survey of Traditional, Reinforcement, and Generative Approaches for Tabular Data Transformation. *arXiv preprint arXiv:2501.10555*.

[57] De Castro, L. N., & Von Zuben, F. J. (2000, July). The clonal selection algorithm with engineering applications. In *Proceedings of GECCO* (Vol. 2000, pp. 36-39).

[58] Gal, M. S., & Rubinfeld, D. L. (2019). Data standardization. *NYUL Rev.*, *94*, 737.

[59] Alrayes, F. S., Zakariah, M., Amin, S. U., Khan, Z. I., & Alqurni, J. S. (2024). Network Security Enhanced with Deep Neural Network-Based Intrusion Detection System. *Computers, Materials & Continua*, *80*(1).

[60] Solovyeva, E., & Abdullah, A. (2021). Binary and multiclass text classification by means of separable convolutional neural network. *Inventions*, *6*(4), 70.

[61] Mao, A., Mohri, M., & Zhong, Y. (2023, July). Cross-entropy loss functions: Theoretical analysis and applications. In *International conference on Machine learning* (pp. 23803-23828). PMLR.

[62] Dereich, S., & Jentzen, A. (2024). Convergence rates for the Adam optimizer. *arXiv preprint arXiv:2407.21078*.

[63] Bisong, E. (2019). Google colaboratory. In *Building machine learning and deep learning models on google cloud platform: a comprehensive guide for beginners* (pp. 59-64). Berkeley, CA: Apress.

[64] Gupta, P., & Bagchi, A. (2024). Introduction to NumPy. In *Essentials of Python for Artificial Intelligence and Machine Learning* (pp. 127-159). Cham: Springer Nature Switzerland.

[65] Gupta, P., & Bagchi, A. (2024). Introduction to Pandas. In *Essentials of Python for Artificial Intelligence and Machine Learning* (pp. 161-196). Cham: Springer Nature Switzerland.

[66] Hackeling, G. (2014). Mastering machine learning with scikit-learn. Packt Publishing.

[67] Pradipta, G. A., Wardoyo, R., Musdholifah, A., Sanjaya, I. N. H., & Ismail, M. (2021, November). SMOTE for handling imbalanced data problem: A review. In *2021 sixth international conference on informatics and computing (ICIC)* (pp. 1-8). IEEE.

[68] https://www.tensorflow.org/?hl=fr Last access to the website 16/06/2025.

[69] Sial, A. H., Rashdi, S. Y. S., & Khan, A. H. (2021). Comparative analysis of data visualization libraries Matplotlib and Seaborn in Python. *International Journal*, *10*(1), 277-281.

[70] Odegua, R., & Ikpotokin, F. (2019). DataSist: A Python-based library for easy data analysis, visualization and modeling. *arXiv preprint arXiv:1911.03655*.

[71] https://learning.oreilly.com/library/view/flask-building-python/9781787288225/ch01.html Last access to the website 10/06/2025.
[72] Ghimire, D. (2020). Comparative study on Python web frameworks: Flask and Django.
[73]https://learning.oreilly.com/library/view/webprogrammingwith/9781284091809/xhtml/23_Chapter08_02.xhtml#ch8lev1_2 access to the website 10/06/2025.
[74] Merzougui H., Benhamza K. (2025). A Hybrid Intrusion Detection System Based on the Clonal Selection Algorithm and Deep Neural Networks for IoMT Environments. National Conference on Innovation in Data Engineering and AI Science (IDEAS 2025), June 11-12, 2025, Oran , Algeria
[75] Miao, J., & Zhu, W. (2022). Precision–recall curve (PRC) classification trees. *Evolutionary intelligence*, *15*(3), 1545-1569.