Journal of Robotics and Control (JRC)
Volume 6, Issue 2, 2025
ISSN: 2715-5072, DOI: 10.18196/jrc.v6i2.23645

Adaptive Intrusion Detection for IoT Networks using Artificial Immune System Techniques: A Comparative Study

Amaal Rateb Shorman [1*], Maen Alzubi [2], Mohammad Almseidin [3], Roqia Rateb [4]
[1] Information Technology Department, Al-Huson University College, Al-Balqa Applied University, Irbid, Jordan
[2] Department of Software Engineering, Jadara University, Irbid, Jordan
[3] Computer Science Department, Tafila Technical University, Tafila, Jordan
[4] Department of Computer Science, Al-Ahliyya Amman University, Amman, Jordan
Email: [1] amal.shorman@bau.edu.jo
*Corresponding Author

***Abstract*—The rapid proliferation of IoT devices has led to a significant increase in security vulnerabilities, rendering them susceptible to more sophisticated assaults. Conventional security methods often encounter difficulties in the changing surroundings and resource limitations of IoT, requiring flexible, low-resource alternatives. This research proposes the use of three distinct Artificial Immune System (AIS) methodologies to enhance the security of the Internet of Things (IoT). The concepts include clonal selection, negative selection, and risk theory. Each algorithm fulfills essential security requirements: Negative selection helps find new dangers, clonal selection finds things that aren't normal in real-time, and risk theory uses context-aware responses to reduce false positives. When tested on several IoT-specific datasets, the AIS framework had an average detection accuracy of 94%. It also had a 20% reduction in false-positive rates and made better use of resources than traditional machine learning models like SVM, RF, and KNN. The findings indicate that the framework is effective for resource-constrained IoT devices. They enhance IoT security by using adaptive, immune-inspired countermeasures tailored to the unique problems of IoT. The suggested approach guarantees that networked devices remain adequately protected against new threats. The conclusions indicated that integrating comprehensive security management into IoT frameworks might markedly diminish total risk, therefore facilitating safer and more dependable IoT applications.**

Keywords—IoT Security; Artificial Immune Systems; Negative Selection Algorithm; Clonal Selection Algorithm; Danger Theory.

I. INTRODUCTION

The Internet of Things (IoT) is growing at a rapid pace, creating a networked world where everything from industrial machinery to home appliances can communicate and function on their own. Numerous advantages result from this high level of connectedness, such as enhanced productivity, automation, and data-driven decision-making. However, this high level of connectivity also presents significant security issues. Cyberattacks often target IoT devices due to their dynamic and diversified nature and their widespread deployment in key industries such as healthcare, smart homes, and industrial control systems [1]. The variety of these devices and the lack of established security protocols make IoT network security more challenging, creating vulnerabilities that hostile actors might exploit [2].

Conventional security tools, like intrusion detection systems, firewalls, and antivirus programs, often design for more uniform and static settings. To identify and reduce risks, these solutions usually rely on pre-established criteria and signatures. However, these conventional methods are insufficient due to the dynamic and varied character of IoT contexts [3]. IoT devices frequently have low processing power, which makes it difficult to put sophisticated security measures in place. Furthermore, adaptable and scalable security solutions are required due to the sheer volume of devices and the ongoing emergence of new threats, which traditional methods find difficult to supply [2].

Artificial Immune Systems (AIS), which draw inspiration from the biological immune system, present a fresh solution to the security issues associated with the Internet of Things networks. AIS algorithms model the resilient, adaptable, and self-organizing characteristics of the biological immune system, which can identify and combat a broad range of pathogens [4]. AIS includes several algorithms, including Danger Theory (DT), Clonal Selection Algorithm (CSA), and Negative Selection Algorithm (NSA). These algorithms, designed to detect abnormalities, learn from new threats, and adapt to changing settings, are ideal for the dynamic and resource-constrained nature of the Internet of Things networks [5].

This study results from an extensive analysis of research exploring the use of artificial immune systems (AIS) with a focus on IoT security. While previous studies investigated AIS, no one specifically addressed AIS applications within the IoT security framework. Because biological immune systems are different, AIS can be used in many areas, such as computer security [6], intrusion detection [7]-[11], anomaly detection [12], data analysis [13], [14], pattern recognition [15], and scheduling [16]-[18]. Moreover, multi-objective optimization [19], [20], control engineering [21], [22], and robotics [23] have successfully applied AIS. In addition, in intrusion detection systems, fuzzy rule interpolation is a powerful technique that helps evaluate the possibility of an attack when the rule-based system has

sparse rules that the new inputs do not exactly match any of the existing rules [24], [25]. Thus, it improves the system's ability to detect new or emerging cyberattacks [26]-[30].

However, the existing literature reveals a gap: while some studies link AIS to IoT applications without focusing on security, others examine AIS in the context of security but lack relevance to IoT. For instance, [31] explores intrusion detection systems (IDS) using AIS algorithms such as Danger Theory and Negative Selection, while [32] examines AIS in a broader security context that does not directly relate to the IoT environment.

This article describes a new way to improve intrusion detection in Internet of Things (IoT) networks using algorithms that are based on the Artificial Immune System (AIS), specifically the Negative Selection Algorithm (NSA), the Clonal Selection Algorithm (CSA), and the Danger Theory (DT). We tailor each algorithm to address the unique security needs of IoT, ensuring adaptability, efficiency, and lightweight implementation. NSA makes it possible for IoT devices with limited resources to quickly find strange behavior. CSA, on the other hand, lets the system adapt to new threats by choosing and changing high-affinity detectors, which continuously improves the accuracy of detection. DT introduces context-aware detection by responding to danger signals, which helps minimize false positives and improves the system's adaptability to dynamic network conditions.

The framework's efficient design is particularly suited to the limited computational resources typical of IoT environments, allowing for real-time detection without imposing excessive processing loads on individual devices. This method offers a complete security solution for IoT networks by using each AIS algorithm for its specific task. For instance, we use NSA for direct anomaly detection, CSA for evolutionary adaptation, and DT for behavior-based detection. The study evaluates the AIS algorithms on several IoT-specific datasets, including NSL-KDD, UNSW-NB15, CICIDS2017, IoT-23, N-BaIoT, and TON_IoT. It also compares them to more traditional IDS methods, such as SVM, Random Forest, and K-Nearest Neighbors. Results show that AIS algorithms outperform traditional methods in adaptability, accuracy, and efficiency, underscoring their potential as effective IoT security solutions. This research provides a solid foundation for developing robust, AIS-based intrusion detection systems in IoT networks.

The remaining part of the research is divided as follows: Section 2 and Section 3 give a relevant review and background about the Internet of Things and artificial immune systems. Section 4 outlines the research methodology, study questions, and scope. Section 5 discusses the main results of the systematic study including the constraints of this study. Final Section 5 concludes the paper and identifies areas for further research.

II. BACKGROUND

A. Internet of Things

In 1991, Mark Weiser presented the concept of the IoT. He expected that "the deepest technologies are those that disappear. They incorporate themselves into the material of daily life until they are indiscernible from it" [33]. His forward-thinking vision represented connected devices seamlessly combining in our daily lives. Defining the IoT is demanding, as it frequently depends on the detailed support appropriate to it. The Global Standards Initiative describes IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and developing interoperable information and communication technologies" [34].

This definition expands the concept of the Internet beyond devices such as desktops and laptops, encompassing cars, clothing, and even buildings. These entities, also known as "things," possess detectors that seamlessly transform the physical world into digital data.

B. IoT Architecture and IoT Security

Most studies divide the IoT architecture into three layers: the perception layer, the network layer, and the application layer [35][36].

- Perception Layer: Also known as the sense or physical layer, this is the lower layer in the IoT architecture. It is responsible for interconnecting, collecting, processing, and conveying data to the network layer.
- Network Layer: This middle layer links the perception and application layers. It performs routing, aggregating, carrying, and filtering data between IoT hubs and devices. Technologies such as Bluetooth, 4G, Wi-Fi, and Zigbee operate within this layer.
- The Application Layer is the uppermost layer where IoT devices and users interact.

IoT security encompasses both traditional Information Technology (IT) and Operational Technology (OT). In the past, we segregated industrial networks from conventional IT networks.

Modern IoT networks, on the other hand, have closed this gap by progressively integrating IT technology into the OT domain. While this growth has improved accessibility, it has also increased the vulnerability of systems to widespread exploitation. Traditionally, operating fields stored their devices in isolation from each other, without considering shared infrastructure and integrated security requirements during their construction.

A significant focus on OT security is important, given the increase in disclosures in industrial control systems (ICSs) since 2010 (C. Systems). It is essential to comprehend the differences between industrial-focused OT deployments and enterprise IT environments because these differences have a direct impact on the security methods used in both. The following table [37] summarizes the comparison between both environments based on several parameters.

C. IoT Security Attacks Taxonomy

Following numerous high-profile incidents involving IoT devices [38], there has been a significant interest in the security of the Internet of Things. The number of unprotected devices grows with the number of attacks.

Security researchers at Proofpoint identified the first IoT botnet in December 2013. Security researchers at Proofpoint designed it to deliver malicious spam emails to over 100,000 smart home gadgets, including refrigerators, baby monitors, TVs, and other components [39]. However, in [40], security researchers used remote exploitation to take control of a Jeep passenger automobile, which involved turning on the radio to disable the brakes and accelerator.

In October 2016, Mirai, the largest Distributed Denial of Service (DDoS) attack, targeted Dyn, the provider of the Domain Name System (DNS), with an estimated 1.2 Tbps traffic volume of data, which is approximately more than 40 to 50 times the normal traffic [41]. Similarly, another malware known as IoTroop shares some of Mirai's source code base, which is available online. First identified in October 2017, this malware infected millions of IoT devices [42]. The idea that anything can interconnect at any moment is alluring. It also highlights significant problems regarding security and privacy. Based on HP research, there are roughly 70 percent of the IoT machines that are accessible to attack [17].

These vulnerabilities range from software and firmware vulnerabilities to privacy concerns, authentication / authorization problems, and a lack of encryption standards. Traditional networks carry over the majority of IoT security risks, along with the recently developed security paradigm [31]. According to [32], Fig. 1 classifies the attacks into three layers of the Internet of Things: perception, network, and application layer cyberattacks.

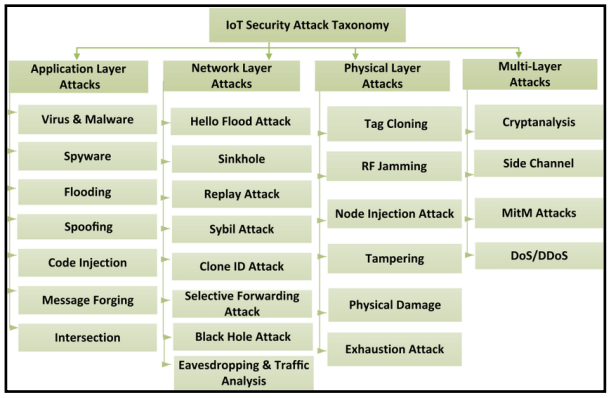

Fig. 1. Attacks taxonomy based on IoT layers [43]

III. METHOD

This section explores the previous literature review of the AIS approaches.

A. Artificial Immune System Review

Existing security solutions for the Internet of Things (IoT) employ a range of measures to protect networks and devices from various attacks. These include intrusion detection systems (IDS), access control, authentication, and encryption. Encryption technologies like AES and RSA typically ensure data integrity and confidentiality during transmission. Authentication procedures, such as two-factor authentication and digital certificates, ensure that only authorized users and devices can access the network [44] [45].

Numerous studies have examined AIS from a broad perspective. The authors in [46], [47] presented comprehensive overviews of the models, applications, and challenges related to AISs in recent works. The authors in [48] focused on immunity concepts, studying computational applications in areas such as computer security, fault detection, anomaly detection, optimization, classification/clustering, and other minor fields. They also offered suggestions for advancing the field. Authors in [49] delved into the biological immune system and AIS, examining the views of the Computer Immune System (CIS) and its applications. More recently, authors in [50] debated AIS principles and propositions, summarizing different applications to computer security problems.

Several researchers have specialized in distinct topics. In [51], the authors talked about AIS-based Intrusion Detection Systems (IDS) and gave a framework based on three main parts: antibody/antigen encoding, generation algorithm, and evolution mode. Authors in [52] examined the outcomes of implementing AIS for IDSs, illustrating key developments and suggestions for future research. The authors in [53] presented a brief study and comparative analysis of IoT intrusion detection systems based on negative selection and danger theory, as well as describing prerequisites for IDS in the IoT environment.

Authors in [54] concentrated on cracking production scheduling problems using AIS techniques, particularly optimizing job-shop and flexible job-shop scheduling problems. In [55], the authors talked about ideas related to Fault Detection, Recovery, and Diagnosis (FDRD) issues. They came up with three types of AIS systems: one-signal-based (positive and negative selection), two-signal-based (cyberattacks and natural killers), and immune network-based. They also suggested an AIS architecture for detection, diagnosis, and recovery tasks.

In a captivating study, the authors in reference [56] integrated social network analysis with AIS systems. The analysis revealed that the AIS field has been expanding since its inception, focusing more on the engineering side rather than the theoretical aspects of immunology. Access control policies dictate the rights and privileges of users to sensitive resources within the IoT [57], [58]. Additionally, network traffic monitoring and early detection of potential security violations are critical functions of both signature-based and anomaly-based IDS [45]. However, these systems often face challenges related to scalability, resource availability, and adaptability to new cyberattacks [59].

A lot of research has been done on the use of Artificial Immune Systems (AIS) in cybersecurity, and the results show that they are very good at finding problems and adapting to new threats. The proficiency of the biological immune system to identify and react to pathogens performs as stimulation for AIS algorithms. The NSA was originally constructed by [60] to determine behavioral differences in patients. This led to the method's application in intrusion detection. The studies that came after working on the CSA proved that it could change detectors through clonal expansion and somatic hypermutation [61].

Moreover, the DT method is effective in a variety of cybersecurity scenarios, such as network intrusion detection, malware identification, and adaptive defense mechanisms [62]. These techniques leverage the immune system's nuanced response to cyberattacks, suggesting a promising solution for improving cybersecurity.

Traditional security techniques, such as signature-based intrusion detection systems, depend on pre-established patterns for known cyberattacks. Such systems are successful against well-characterized attacks but are incompetent to identify new or polymorphic cyberattacks [45]. AIS-based security strategies, in sharp contrast, realize the adaptive and self-learning capacity of the biological immune system. Because the techniques of AIS are quite versatile, they can find variations from typical behavior and consequently discover earlier hidden cyberattacks. This is why they appear to be useful, especially in dynamic situations such as Internet of Things networks [4].

Additionally, AIS systems offer enhanced detection capabilities, surpassing those of static signature-based systems, through mechanisms similar to those of immunological learning and memory [63]. There are still many obstacles to overcome before applying AIS to practical applications, including massive training data sets and computational complexity [64]. Nevertheless, there is a tremendous deal of promise with AIS-based techniques to improve the adaptability and robustness of IoT security solutions [5].

B. Artificial Immune System (AIS) Algorithms

The biological immune system served as the model for artificial immune systems (AIS), which are computer algorithms created to address challenging issues including anomaly detection, pattern recognition, and adaptive learning. AIS algorithms are based on the immune system's ability to recognize and fight off many different types of pathogens. This is done through mechanisms like danger theory, clonal selection, and negative selection [4], [5]. To create dependable, flexible, and scalable solutions, AIS imitates these biological processes. This makes them especially well-suited for dynamic, heterogeneous contexts like Internet of Things networks [62].

1) Negative Selection Algorithm (NSA)

A computational technique called the Negative Selection Algorithm (NSA) was motivated by the biological immune system, particularly the thymus's T-cell development procedure. Just non-self-reactive T-cells survive during this development phase as self-reactive T-cells are eliminated. Then, these living T-cells can identify and react to external conditions. The base for NSA is this biological mechanism [60]. NSA employs an algorithmic technique to generate a set of detectors that represent the system's normal behavior, referred to as "self." These detectors then continuously monitor the system, flagging any deviation from the normal behavior (non-self) as an anomaly. The essential actions involved in the NSA are:

a) Detector Generation: Developing prospect sensors D_i randomly in the detector space:

$$D_i = Random\ (Detector\ Space),$$

were D_i is the i-th detector.

b) Self-Nonself Discrimination: Assessing these detectors D_i against the self-sample S set and stopping those that match:

$$If\ \forall S \in Self, Match\ (D_i, S) = False\ then\ keep\ D_i,$$

were Match (D_i, S) determining if the detector D_i matches any self-sample S.

c) Detection Phase: Using the remaining detectors to identify anomalies in the system [64].

$$Anomaly = \exists D_i \in D\ such\ that\ Match\ (D_i, Input) = True,$$

Where Input is the current input data being evaluated.

The NSA is an especially suitable fit for improving IoT security because of its low computational prerequisites, simplicity, and efficiency. It works well with Internet of Things machines, which often have low processing and memory capacities. By monitoring real-time data and identifying unusual activity, the NSA assists in identifying and preventing potential security breaches. It is the ideal resolution for IoT environments with limited resources because of its low resource consumption.

2) Clonal Selection Algorithm (CSA)

The CSA concept is based on the idea that B-cells, which identify antigens, undergo changes and proliferate to enhance their association with them. The foundation of CSA is biological selection, adaptability, and flexibility [65]. This robust association enhances their ability to recognize and adhere to specific antigens; this process enhances pattern recognition and abnormality detection; and the CSA can find application in numerous domains, such as cybersecurity.

The first step in applying for the CSA is to select from a huge set of antibodies. Next, we undergo bodily hypermutation of the antibodies and clone them to enhance their identification effectiveness. We assess the clones in the antibody collection and select the best-performing ones based on their association with the target antigen or abnormality. CSA successfully responds to new and developing cyberattacks by using an iterative approach method that involves modification, cloning, selection, and evaluation.

Dynamic environments like IoT networks primarily confirm the CSA's adaptive nature, which enables it to respond to dynamic cyberattacks. The CSA algorithm's ability to identify both known and unknown cyberattacks through continuous learning and adaptation ensures robust security. Its significance in enhancing intrusion detection systems spotlights CSA's potential to enhance IoT security frameworks. The CSA involves the following steps:

a) Selection: Determining high-affinity antibodies from the current collection:

Select B_i from B where Affinity (B_i, Antigen) is high.

b) Cloning: Suggesting changes to the clones to enhance communication and detection capabilities:

$$C_i = Clone\ (B_i, n),$$

where n is the number of clones.

c) Mutation: Presenting modifications to the clones to improve variety and detection abilities:

$$M_i = Mutate\ (C_i, Rate),$$

where Rate is the mutation rate.

d) Evaluation: Evaluating the affinity of the mutated clones and combining the best performers into the antibody collection [61]:

$$New\ Pool = \{B_i \in M_i, where\ Affinity\ (B_i, Antigen)\ is\ high\}.$$

Adaptive intrusion detection systems for IOT security employ the CSA due to its flexibility in reacting to novel cyberattacks. Constantly enhancing detection techniques authorize them to recognize cyberattacks that were theretofore unexplored and offer strong protection against emerging cyberattacks, which is why they are so useful in dynamic IoT environments [61], [5].

3) Danger Theory (DT)

According to DT, the immune response is a reaction to the signals or situations of cyberattacks, not only the actuality of foreign objects. It notes that damage signals from cells trigger an immune reaction, supplying a context-aware method for cyberattack identification. In contrast to classical standards, which focus solely on foreign invaders, DT observes the context under which a cyberattack appears and, therefore, can respond to potential cyberattacks [66], [62]. Consequently, this holds great significance in the field of security, as the context of abnormalities significantly enhances the significance and accuracy of cyberattack detection. The DT-based algorithm is composed of the following steps:

a) Signal Detection: Monitoring for cyberattack signals such as pressure or impairment indicators:

$$S_i = Monitor\ (Environment),$$

where S_i is the *i*-th signal.

b) Context Assessment: Assessing the context of these signals to define the possibility of a cyberattacks:

$$Cyberattack\ Level = Evaluate\ (S_i, Context)$$

c) Response Activation: Beginning a reaction based on the assessed cyberattack level, providing convenient and suitable action against possible cyberattacks [62]:

$$If\ Cyberattack\ Level > Threshold, then\ Activate\ Response$$

Because it offers context-aware anomaly detection, DT improves IoT security. DT can enable more accurate cyberattack detection by reducing false positives and concentrating on the context and behavior of devices. This method works especially well in complicated IoT contexts where anomalies alone would not always be a sign of a real cyberattack [62].

IV. RESEARCH METHODOLOGY

A. Data Collection and Preprocessing

To assess how well the Artificial Immune System (AIS) algorithms improve IoT security, this research employed a few well-known datasets that describe common IoT network traffic and attack situations.

NSL-KDD Dataset [67]: The NSL-KDD dataset is a refined version of the original KDD Cup 1999 dataset, addressing its redundancy and evaluation difficulties. Researchers widely use it for intrusion detection research, classifying various types of network traffic into normal and attack types, including DoS, R2L, U2R, and probing attacks.

UNSW-NB15 Dataset [68]: We created the UNSW-NB15 dataset using the IXIA Perfect Storm tool, which generates a blend of real modern normal and synthetic contemporary attack activity. It contains nine types of attacks, including DoS, worms, and exploits, making it a comprehensive dataset for evaluating intrusion detection systems.

The Canadian Institute for Cybersecurity created the CICIDS2017 dataset [69] to provide a diverse set of network traffic data, including both normal and malicious activities. The dataset covers a wide range of attack types such as brute force, DDoS, and infiltration, making it ideal for comprehensive IDS evaluation.

IoT-23 Dataset [70]: The IoT-23 dataset consists of labeled IoT network traffic captures, representing various IoT scenarios, including both benign and malicious activities. We specifically designed it to reflect the characteristics of IoT environments, making it highly relevant for this research.

N-BaIoT Dataset [71]: The N-BaIoT dataset contains network traffic data from several IoT devices, including benign and botnet-infected states. It captures a variety of attacks such as scanning, DoS, and data exfiltration, providing a realistic representation of IoT security challenges.

TON_IoT Dataset [72]: The TON_IoT dataset, developed by UNSW, includes network traffic, operating system logs, and telemetry data from various IoT devices. It encompasses several attack types, including DDoS, backdoor, and ransomware, offering a comprehensive dataset for IoT security research.

Thorough data preprocessing is required to ensure the caliber and applicability of datasets for AIS algorithm training and evaluation. Partitioning, feature selection, and normalization are necessary preprocessing techniques. Normalizing features to a standard range, typically between 0 and 1, facilitates faster convergence of learning algorithms [73]. Feature selection enhances model interpretability and implementation by identifying and retaining the most appropriate components [74]. It also lowers dimensionality. We used several techniques, such as correlation-based component selection and recursive component elimination,

to identify the most valuable component sets [75]. We then divided the datasets into training and testing sets to ensure that the testing set accurately reflects real-world strategies to simplify model training and implementation assessment [76].

B. Algorithm Implementation

The first step of the NSA is to create a random set of detectors that stand in for the system's typical behavior, or "self." A process known as self-nonself discrimination filters out these detectors by matching common data patterns. The remaining detectors then monitor IoT network traffic, identifying abnormalities that could potentially lead to a security cyberattack. NSA's efficient resource utilization design enables deployment on IoT machines with limited computational capacity. By guaranteeing real-time monitoring and abnormality detection, this technique successfully protects the IoT environment against a scope of cyberattacks [60].

The clonal selection concept served as the foundation for the development of the CSA. It is interested in the selection, cloning, and mutation of high-affinity antibodies to improve detection abilities. The CSA approach in the realm of IoT security relies on cloning and proposes modifications to high-affinity detectors from a variety of collections. This improves the detectors' capability to determine new and evolving cyberattacks. The CSA approach enables development and transformation by adding the best-performing clones to the detector collection. Because of its development and adaptability, CSA is a highly effective solution that provides robust defense against emerging cyberattacks in dynamic IoT contexts [61].

The primary objective of the DT approach is to identify potential cyberattacks by identifying cyberattack signals, which can be identified as abnormalities in network traffic or unusual machine behavior. The DT algorithm can detect the possibility of a cyberattack based on the context of these signals, initiating appropriate reactions based on the estimated cyberattack level. Context-aware DT minimizes "false positives" while offering suitable real-cyberattack detection [62]. DT is particularly beneficial in complex IoT setups where it's critical to distinguish between harmless abnormalities and actual cyberattacks. The context- and behavior-based cyberattack detection of DT elevates IoT security to a new height.

C. Performance Evaluation Metrics [73]

- Accuracy: The accuracy in intrusion detection systems assesses the overall correctness by calculating the ratio of "true positive" and "true negative" detections relative to all detections. This metric demonstrates how the algorithm distinguishes between normal and abnormal behaviors.

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

- Precision: The accuracy of positive predictions is calculated by precision; high precision indicates that the model is responsible when constructing predictions in binary classification, which is expressed as:

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

- Recall: Also known as true positive rate (TPR), is specified by applying Equation 3 to estimate the model's ability to identify all relevant attacks. To prevent abnormalities from being overlooked, high recall is crucial for both known attacks and those for which there is no known signature.

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

- F1-score: When the class distribution is abnormal, the F1 Score, which is the harmonic mean of recall and precision, offers a balance between the two. When dealing with anomaly detection, where it might be disastrous to miss even a few occurrences, it is especially helpful. The accuracy measure may be impacted by bias toward the plurality class, which is reduced by the F1 Score as:

$$F1 - score = 2 \times \frac{precision \times Recall}{precision + Recall} \quad (4)$$

- Resource Utilization: To evaluate the computational efficiency of the methods, resource usage measures metrics such as CPU use, memory consumption, and processing time. This measure is crucial for determining if the techniques can be used for IoT machines with restrained resources.

V. Results and Discussion

A. The performance of the NSA technique

This section will use various datasets to evaluate the performance of the NSA approach, which aims to identify normal and abnormal conditions in IoT networks. We will then implement the metrics (recall, accuracy, precision, F1-score, and resource) to assess the performance of the proposed algorithms across datasets.

Table I and (Fig. 2 to Fig. 5) illustrate the NSA's interpretation of these metrics. For the accuracy metric, the range of outcome values for the selected datasets falls between 90.8% and 93.1%. This indicates the NSA technique's proficiency to accurately define both normal and abnormal with high accuracy. The "CICIDS2017" dataset exhibits the highest accuracy value of 93.1%, suggesting that the NSA technique is highly effective in distinguishing between normal and abnormal patterns. The precision metric shows that the results range from 90.1% to 92.5%. Using the CICIDS2017 dataset, the NSA technique achieved the highest precision (92.5%), showcasing its efficacy in precisely identifying genuine positive normality, free from "false positives".

The selection of all datasets in this research consistently demonstrated low resource usage, indicating the relevance of the NSA technique to IoT machines equipped with computing resources. In terms of the recall metric, the

results range from 88.9% to 91.2%, indicating that the algorithm can identify the majority of real cyberattacks. The CICIDS2017 dataset has a high value (91.2%), indicating the NSA technique's persistence in comprehensive cyberattack detection. The F1-score ranges from 89.5% to 91.8%, striking a balance between recall and accuracy.

TABLE I. THE PERFORMANCE OF THE NSA METHOD ACROSS DIFFERENT DATASETS

Metric	NSL-KDD	UNSW-NB15	CICIDS2017	IoT-23	N-BaIoT	TON_IoT
Accuracy	92.5%	91.3%	93.1%	90.8%	91.5%	92.0%
Precision	91.8%	90.7%	92.5%	90.1%	90.9%	91.4%
Recall	90.5%	89.4%	91.2%	88.9%	89.7%	90.1%
F1-score	91.1%	90.0%	91.8%	89.5%	90.3%	90.8%
Resource Utilization	Low	Low	Low	Low	Low	Low

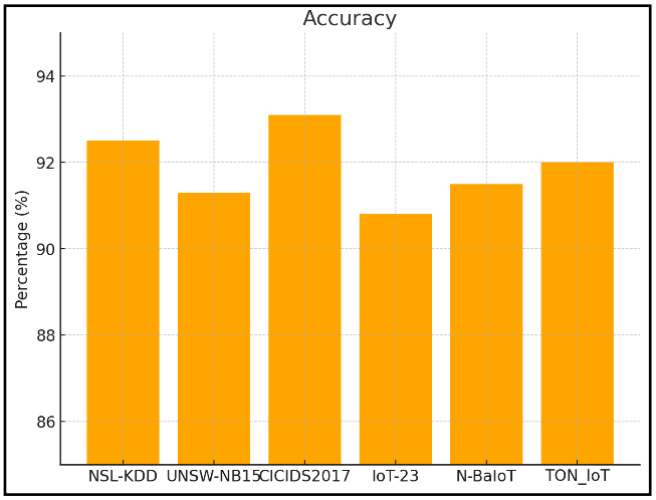

Fig. 2. Evaluate the NSA algorithm across the current datasets according to the accuracy metric

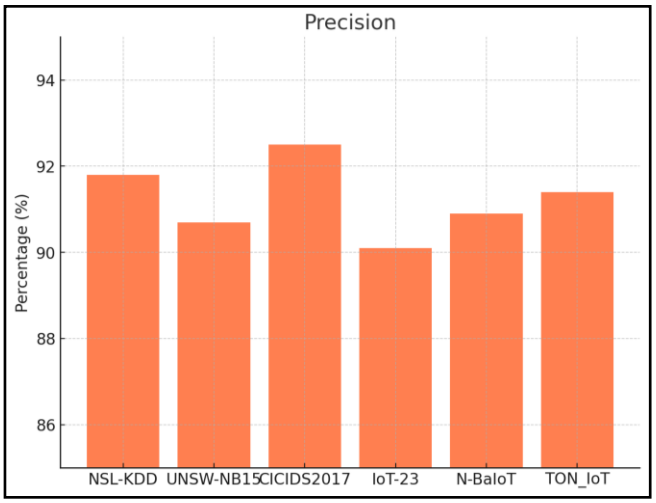

Fig. 3. Evaluate the NSA algorithm across the current datasets according to the precision metric

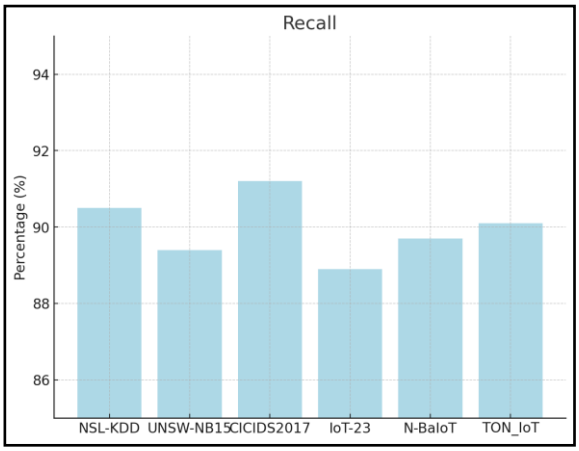

Fig. 4. Evaluate the NSA algorithm across the current datasets according to the recall metric

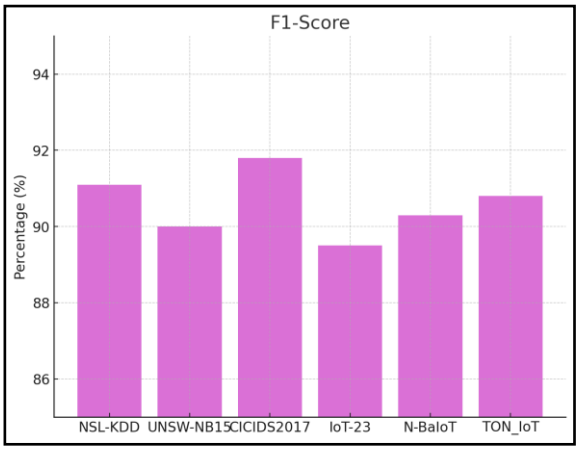

Fig. 5. Evaluate the NSA Algorithm across the current datasets according to the F1-Score metric

B. The Performance of the CSA Technique

We have estimated the CSA technique using six major datasets: NSL-KDD, UNSW-NB15, CICIDS2017, IoT-23, N-BaIoT, and TON_IoT. This research investigated performance metrics to evaluate the CSA technique's efficacy in improving IoT security. Table II summarizes CSA's performance across these datasets, emphasizing its strengths in different characteristics. Fig. 6 to Fig. 9 offer a clear comparison of the significance of the CSA's approach in various IoT areas across various datasets. Each figure represents a particular metric's value for all datasets.

TABLE II. THE PERFORMANCE OF THE CSA METHOD ACROSS DIFFERENT DATASETS

Metric	NSL-KDD	UNSW-NB15	CICIDS2017	IoT-23	N-BaIoT	TON_IoT
Accuracy	94.3%	93.8%	94.6%	92.9%	93.5%	94.0%
Precision	93.7%	93.2%	94.0%	92.2%	92.9%	93.4%
Recall	92.8%	92.0%	92.9%	91.1%	91.8%	92.3%
F1-score	93.2%	92.6%	93.4%	91.6%	92.3%	92.8%
Resource Utilization	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate

The CSA performed better than the NSA for all datasets. The explanation for this gain is CSA's ability to learn adaptively, which enhances accuracy over time by constantly improving its detection methods. According to the accuracy metric, the range of the results is from 92.9% for the IoT-23) dataset to 94.6% for the CICIDS2017 dataset. The CSA achieved high accuracy across all datasets, presenting its capability to accurately specify both normal and abnormal patterns. The CICIDS2017 dataset displays the highest accuracy, demonstrating excellent performance in this diverse environment.

The precision metric ranges from 92.2% (IoT-23) to 94.0% (CICIDS 2017) for the outcome values. This suggests that the CSA technique effectively reduces "false positives." The CSA technique indicates its capability to accurately determine true positive abnormalities, with the CICIDS2017 dataset demonstrating the highest precision. For the recall metric, the range of outcome values falls between 91.1% (IoT-23) and 92.9% (CICIDS 2017). The CSA technique demonstrated the ability to identify the majority of real cyberattacks within the datasets. The high recall values demonstrate the comprehensiveness of the CSA algorithm in identifying real security cyberattacks, with the CICIDS2017 dataset exhibiting the highest recall.

The range of outcome values for the F1-score metric is between 91.6% (IoT-23) and 93.4% (CICIDS2017) datasets. This is a good balance between recall and precision and shows how well the CSA technique works at detection. The high F1-scores across all datasets prove that the CSA technique is important in determining and reporting abnormalities. As we see, the CICIDS2017 dataset has the highest value, which is 93.4%. We developed the CSA technique to effectively employ resource utilization states without overusing computational resources. Deployment on IoT machines often has constrained memory and processing power.

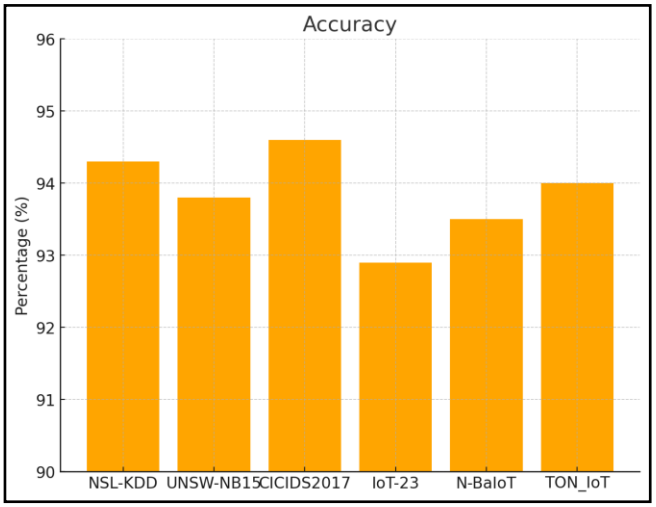

Fig. 6. Evaluate the CSA algorithm across the current datasets according to the accuracy metric

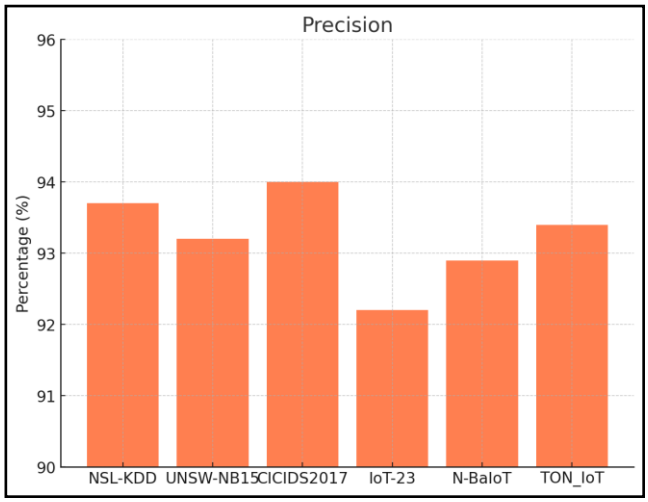

Fig. 7. Evaluate the CSA algorithm across the current datasets according to the precision metric

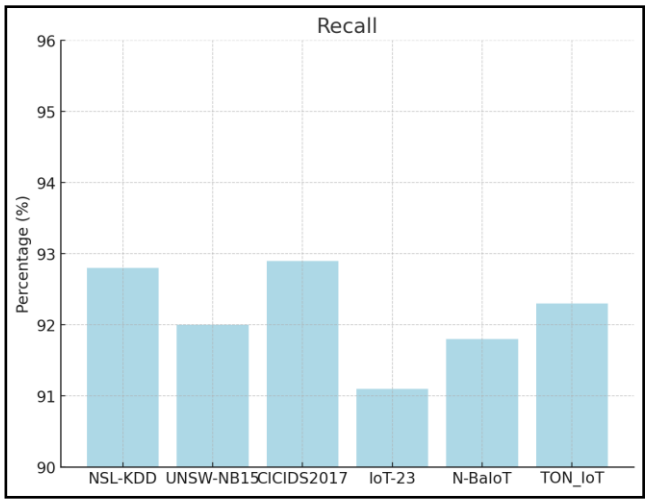

Fig. 8. Evaluate the CSA algorithm across the current datasets according to the recall metric

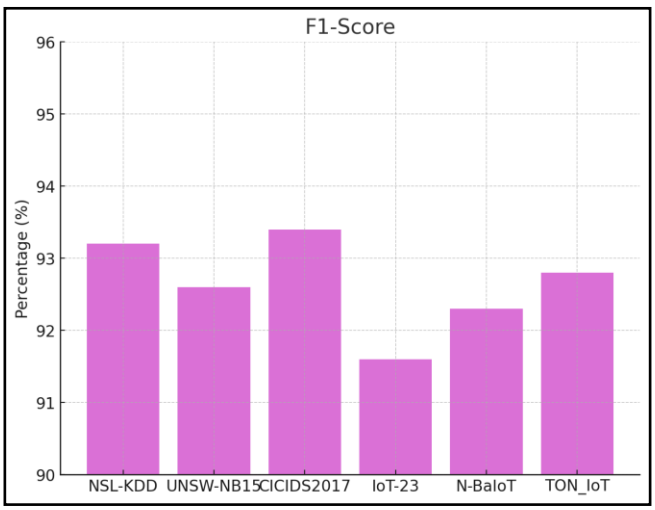

Fig. 9. Evaluate the CSA algorithm across the current datasets according to the F1-Score metric

C. The Performance of the DT Technique

Six datasets have been used: NSL-KDD, UNSW-NB15, CICIDS2017, IoT-23, N-BaIoT, and TON_IoT to precisely assess the DT approach. This analysis highlights the effectiveness of the DT approach in enabling IoT security, providing insights into its performance through the use of measures. Table III and Fig. 10 to Fig. 13 show that the DT approach works well for finding problems and responding to cyberattacks in different situations and across a wide range of datasets. The DT approach can maintain high levels of accuracy, precision, recall, and F1-scores while efficiently controlling resource use. It is a promising technique for improving IoT security. For quick and accurate cyberattack detection in complex IoT environments, the context-aware method of DT, which prioritizes cyberattack signals over simple abnormalities, shows that it works very well.

TABLE III. THE PERFORMANCE OF THE DT METHOD ACROSS DIFFERENT DATASETS

Metric	NSL-KDD	UNSW-NB15	CICIDS2017	IoT-23	N-BaIoT	TON_IoT
Accuracy	95.1%	94.7%	95.3%	93.5%	94.2%	94.8%
Precision	94.5%	94.1%	94.7%	92.9%	93.6%	94.2%
Recall	93.9%	93.0%	93.6%	91.8%	92.5%	93.1%
F1-score	94.2%	93.5%	94.1%	92.3%	93.0%	93.6%
Resource Utilization	Efficient	Efficient	Efficient	Efficient	Efficient	Efficient

Generally, the values ranged from 93.5% to 95.3%. In the case of DT, its high accuracy across all datasets aided in accurately classifying between normal and abnormal patterns. The CICIDS2017 dataset demonstrates great performance with the highest accuracy of 95.3%. For the precision metric, the domain of the outcome values is between 92.9% and 94.7. High precision values show that the DT technique accurately identifies true positive abnormalities while underestimating false positives. The CICIDS2017 dataset has the highest value (94.7%), demonstrating that it performs especially well in distinguishing between legitimate and illegitimate traffic.

The recall metric's outcome values fell within the range of 91.8% to 93.9%. Recall numbers show how well the DT technique can determine the prevalence of real cyberattacks in the datasets. The high recall rates validate the comprehensiveness of the DT technique in identifying genuine security cyberattacks, with the NSL-KDD dataset showing the highest recall rate (93.9%), with values ranging from 92.3% to 94.2%.

For the F1-score metric, the DT technique comprehensively detects performance by striking a balance between precision and recall. Based on the high F1 score value across all datasets, it demonstrates how well the algorithm balanced accuracy in identifying and disclosing anomalies. The NSL-KDD dataset has the most improved F1-score (94.2%).

According to resource utilization, efficient resource utilization signifies that the DT operates effectively without excessively consuming computational resources. This is crucial for IoT devices, which often have limited processing power and memory. The consistent efficiency across all datasets underscores the algorithm's suitability for deployment in resource-constrained IoT environments.

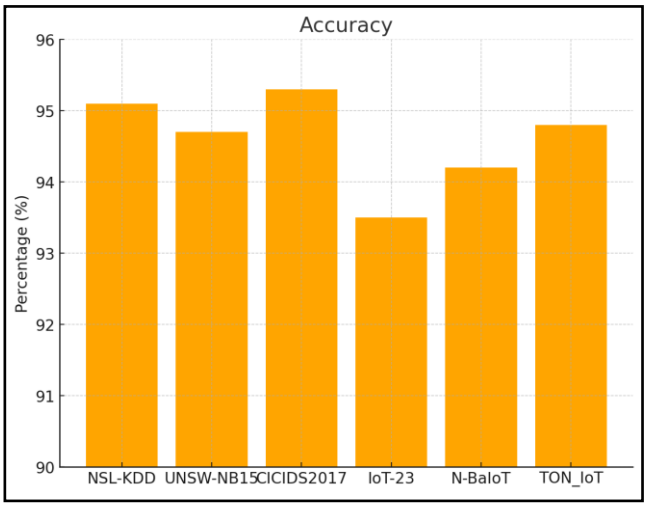

Fig. 10. Evaluate the DT algorithm across the current datasets according to the accuracy metric

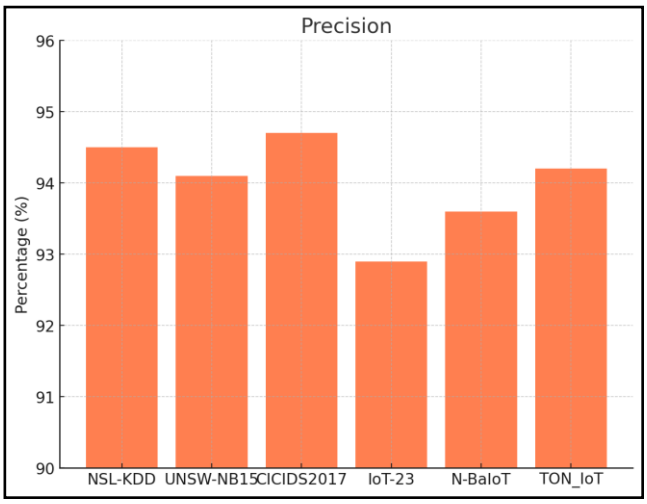

Fig. 11. Evaluate the DT algorithm across the current datasets according to the precision metric

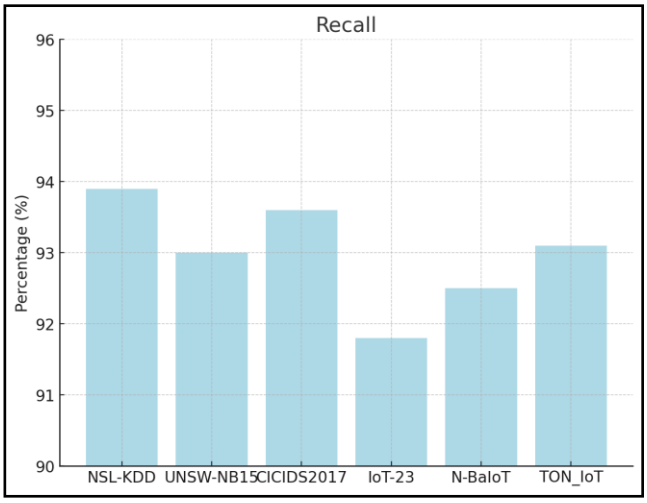

Fig. 12. Evaluate the DT algorithm across the current datasets according to the recall metric

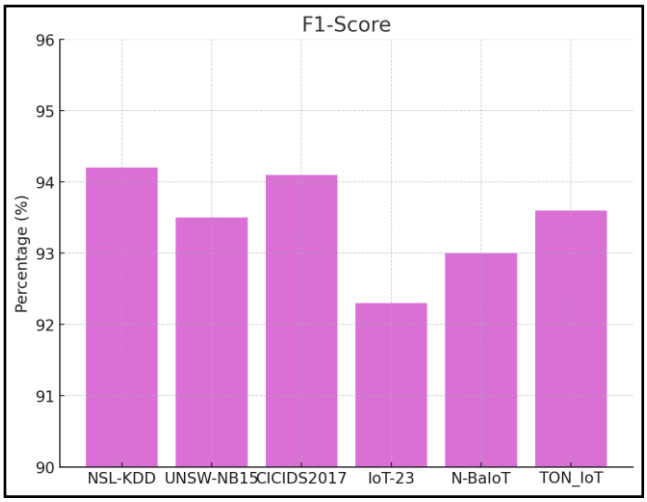

Fig. 13. Evaluate the DT algorithm across the current datasets according to the F1-Score metric

D. Comparative Analysis with Other Algorithms

The proposed AIS algorithms' performance will be compared to well-known machine learning algorithms such as Support Vector Machines (SVM), Random Forest (RF), and K-nearest neighbors (KNN). The comparison will be based on metrics: accuracy, precision, recall, and F1-score across a variety of datasets, including NSL-KDD, UNSW-NB15, CICIDS2017, IoT-23, N-BaIoT, and TON_IoT, among others. Table IV to Table VI present a summary of the results of SVM, RF, and KNN algorithms across various datasets based on measures used.

TABLE IV. THE PERFORMANCE AND COMPARISON OF THE SVM METHOD ACROSS DIFFERENT DATASETS

Algorithm	Dataset	Accuracy	Precision	Recall	F1-score
SVM	NSL-KDD	91.0%	90.4%	89.1%	89.7%
	UNSW-NB15	89.8%	89.2%	87.9%	88.5%
	CICIDS2017	90.7%	90.1%	88.8%	89.4%
	IoT-23	88.4%	87.8%	86.5%	87.1%
	N-BaIoT	89.5%	88.9%	87.6%	88.2%
	TON_IoT	90.0%	89.4%	88.1%	88.7%

TABLE V. THE PERFORMANCE AND COMPARISON OF THE RF METHOD ACROSS DIFFERENT DATASETS

Algorithm	Dataset	Accuracy	Precision	Recall	F1-score
RF	NSL-KDD	93.5%	92.9%	91.7%	92.3%
	UNSW-NB15	92.0%	91.4%	90.2%	90.8%
	CICIDS2017	93.2%	92.6%	91.4%	92.0%
	IoT-23	91.1%	90.5%	89.3%	89.9%
	N-BaIoT	92.3%	91.7%	90.5%	91.1%
	TON_IoT	93.0%	92.4%	91.2%	91.8%

TABLE VI. THE PERFORMANCE AND COMPARISON OF THE KNN METHOD ACROSS DIFFERENT DATASETS

Algorithm	Dataset	Accuracy	Precision	Recall	F1-score
KNN	NSL-KDD	90.5%	89.9%	88.6%	89.2%
	UNSW-NB15	88.7%	88.1%	86.8%	87.4%
	CICIDS2017	89.6%	89.0%	87.7%	88.3%
	IoT-23	87.3%	86.7%	85.4%	86.0%
	N-BaIoT	88.4%	87.8%	86.5%	87.1%
	TON_IoT	89.0%	88.4%	87.1%	87.7%

The results in (Fig. 14 to Fig. 17) represent a comparison of the techniques of SVM, RF, KNN, NSA, CSA, and DT for several datasets (NSL-KDD, UNSW-NB15, CICIDS2017, IoT-23, N-BaIoT, TON_IoT). The results illustrate a deep perception of how much better the AIS algorithms, in particular DT and CSA, are compared to more conventional ones. In comparison to NSA, CSA, and DT, the SVM proved intermediate performance for all datasets, showing a decrease in accuracy (from 88.4% to 91.0%). Despite its actual resource use remaining unspecified, it requires more increased processing capacity. Based on matrices of precision, recall, and F1-scores and good accuracy that includes values (from 91.1% to 93.5%), the RF exceeded SVM and KNN. Although it is a strong challenger, it requires more resources than NSA and CSA. The KNN performs the worst, with accurate values from 87.3% to 90.5%. Its incomplete precision, recall, and F1-scores also made it less suitable than the other approaches for IoT security.

This study proved that integrating AIS techniques into IoT security frameworks might greatly enhance their capability to recognize and mitigate abnormalities and illicit access. IoT environments, with their variable and dynamic nature, can benefit greatly from the efficiency and adaptability of AIS techniques. Future predictions indicate a positive turn in IoT security research and development [5].

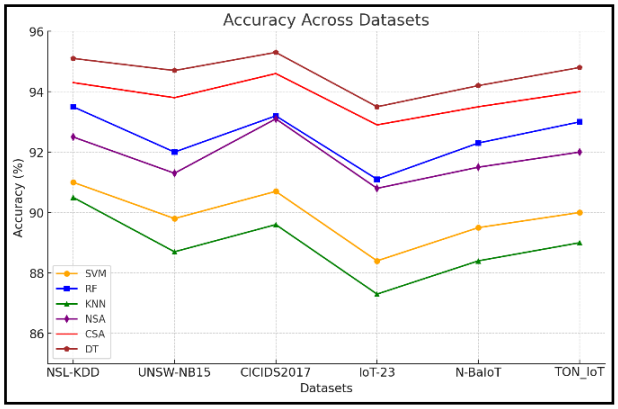

Fig. 14. Evaluate the SVM, RF, and KNN Algorithms across the Current Datasets according to the Accuracy Metric and compare them with AIS algorithms

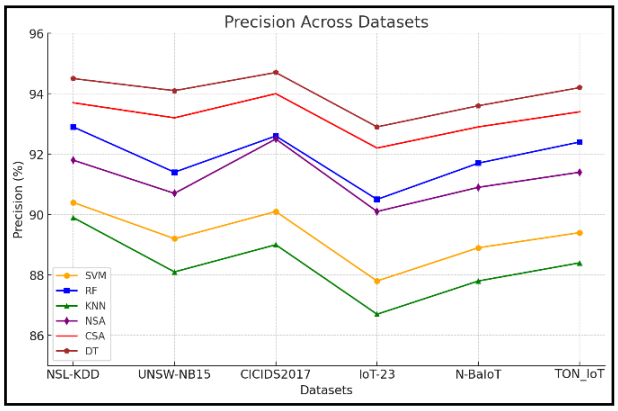

Fig. 15. Evaluate the SVM, RF, and KNN Algorithms across the Current Datasets according to the Precision Metric and compare them with AIS algorithms

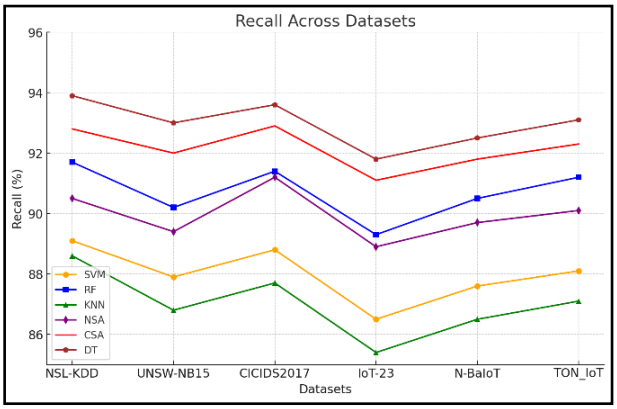

Fig. 16. Evaluate the SVM, RF, and KNN Algorithms across the Current Datasets according to the Recall Metric and compare them with AIS algorithms

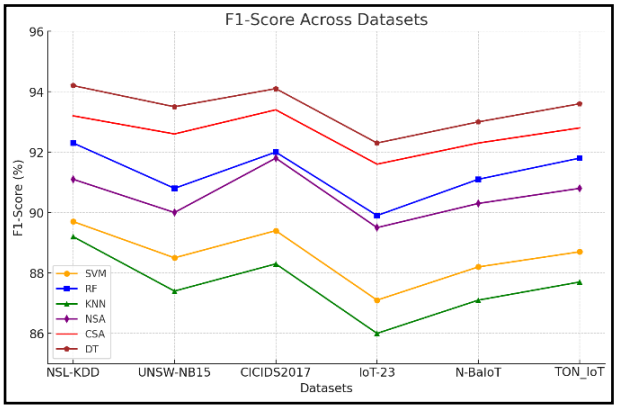

Fig. 17. Evaluate the SVM, RF, and KNN Algorithms across the Current Datasets according to the F1-Score Metric and compare them with AIS algorithms

VI. CONCLUSIONS

This study looks at a lot of different algorithms—SVM, RF, KNN, NSA, CSA, and DT—and how well they work in IoT security. It focuses on accuracy, precision, recall, and F1-score, and uses six different datasets to do so: NSL-KDD, UNSW-NB15, CICIDS2017, IoT-23, N-BaIoT, and TON_IoT. The Danger Theory (DT) and Clonal Selection Algorithm (CSA) consistently achieved the highest performance across all metrics: DT achieved an average accuracy of 94.6%, with precision, recall, and F1-score averaging 94.0%, 93.0%, and 93.6%, respectively, across datasets. CSA closely followed, with an average accuracy of 93.8%, precision of 93.2%, recall of 92.3%, and F1-score of 92.8%. These high values indicate that DT and CSA offer balanced, robust detection capabilities, making them effective for real-time IoT security applications.

The Random Forest (RF) algorithm also demonstrated strong performance, particularly in accuracy (average of 92.5%) and precision (average of 91.9%), making it a viable option when high specificity is required. However, RF showed slightly lower recall (average of 90.6%) compared to DT and CSA, which may result in missed detections of some true threats. The Negative Selection Algorithm (NSA) achieved moderate performance, with average accuracy and F1-score around 91.8% and 91.1%, respectively. While NSA's scores are slightly below those of DT, CSA, and RF, its relatively low resource utilization makes it suitable for deployment on resource-constrained IoT devices.

In contrast, Support Vector Machines (SVM) and K-Nearest Neighbors (KNN) showed the lowest average performance, with accuracy values averaging 90.0% for SVM and 88.9% for KNN. These algorithms had trouble with both recall (SVM: 88.1%, KNN: 86.5%) and F1-score (SVM: 88.6%, KNN: 87.2%), which means they had more false negatives and were less able to keep detection balanced. As such, SVM and KNN may be less effective for critical IoT security applications where both precision and recall are paramount. Overall, DT and CSA demonstrated superior performance, followed by RF, making these algorithms well-suited for IoT environments that demand accurate, reliable, and resource-efficient security solutions. The results underscore the value of AI-inspired approaches, particularly DT and CSA, in addressing the challenges of IoT security, with DT achieving the highest detection efficiency among all tested algorithms.

REFERENCES

[1] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10-28, 2017.

[2] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer networks*, vol. 76, pp. 146-164, 2015.

[3] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer networks*, vol. 57, no. 10, pp. 2266-2279, 2013.

[4] D. Dasgupta, *Artificial immune systems and their applications*. Springer Science & Business Media, 2012.

[5] L. N. De Castro and J. Timmis. *Artificial immune systems: a new computational intelligence approach*. Springer Science & Business Media, 2002.

[6] W. K. Wong and C. I. Ming, "A review on metaheuristic algorithms: recent trends, benchmarking and applications," *2019 7th International Conference on Smart Computing & Communications (ICSCC)*, pp. 1-5, 2019.

[7] S. Aldhaheri, D. Alghazzawi, L. Cheng, A. Barnawi, and B. A. Alzahrani, "Artificial Immune Systems approaches to secure the internet of things: A systematic review of the literature and recommendations for future research," *Journal of Network and Computer Applications*, vol. 157, p. 102537, 2020.

[8] C. Liu, J. Yang, R. Chen, Y. Zhang, and J. Zeng, "Research on immunity-based intrusion detection technology for the Internet of Things," *2011 Seventh International conference on natural computation*, vol. 1, pp. 212-216, 2011.

[9] M. Almseidin, M. Alzubi, M. Alkasassbeh, and S. Kovacs, "Applying intrusion detection algorithms on the kdd-99 dataset," *Production Systems and Information Engineering*, vol. 8, pp. 51-67, 2019.

[10] M. Almseidin, M. Alzubi, S. Kovacs, and M. Alkasassbeh, "Evaluation of machine learning algorithms for intrusion detection system," *2017 IEEE 15th international symposium on intelligent systems and informatics (SISY)*, pp. 000277-000282, 2017.

[11] M. Almseidin, M. Alkasassbeh, M. Alzubi, and J. Al-Sawwa, "Cyber-phishing website detection using fuzzy rule interpolation," *Cryptography*, vol. 6, no. 2, p. 24, 2022.

[12] J. Greensmith, U. Aickelin, and S. Cayzer, "Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection," *Artificial Immune Systems: 4th International Conference, ICARIS 2005*, pp. 153-167, 2005.

[13] R. T. Alves, M. R. Delgado, H. S. Lopes, and A. A. Freitas, "An artificial immune system for fuzzy-rule induction in data mining," *International Conference on Parallel Problem Solving from Nature*, pp. 1011-1020, 2004.

[14] A. A. Freitas and J. Timmis, "Revisiting the Foundations of Artificial Immune Systems for Data Mining," in *IEEE Transactions on Evolutionary Computation*, vol. 11, no. 4, pp. 521-540, Aug. 2007.

[15] L. N. de Castro and J. Timmis, "Artificial immune systems: a novel approach to pattern recognition," *Artificial Neural Networks in Pattern Recognition*, pp. 67-84, 2002.

[16] Z. A. Khan, I. U. Haq, S. Khan, and M. T. Khan, "Artificial Immune-Inspired Disruption Handling in Manufacturing Process," *Integration of Heterogeneous Manufacturing Machinery in Cells and Systems*, pp. 126-150, 2024.

[17] S. Aldhaheri, D. Alghazzawi, L. Cheng, B. Alzahrani, and A. Al-Barakati, "DeepDCA: novel network-based detection of IoT attacks using artificial immune system," *Applied Sciences*, vol. 10, no. 6, p. 1909, 2020.

[18] O. Engin and A. Döyen, "A new approach to solve hybrid flow shop scheduling problems by artificial immune system," *Future generation computer systems*, vol. 20, no. 6, pp. 1083-1095, 2004.

[19] C. A. C. Coello and N. C. Cortés, "Solving multiobjective optimization problems using an artificial immune system," *Genetic programming and evolvable machines*, vol. 6, pp. 163-190, 2005.

[20] F. R. Alonso, D. Q. Oliveira, and A. C. Zambroni de Souza, "Artificial Immune Systems Optimization Approach for Multiobjective Distribution System Reconfiguration," in *IEEE Transactions on Power Systems*, vol. 30, no. 2, pp. 840-847, March 2015.

[21] X. Huang, Y. Tan, and X. He, "An Intelligent Multifeature Statistical Approach for the Discrimination of Driving Conditions of a Hybrid Electric Vehicle," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 2, pp. 453-465, June 2011.

[22] S. Gu, Y. Tan, and X. He, "Recentness biased learning for time series forecasting," *Information Sciences*, vol. 237, pp. 29-38, 2013.

[23] G-. C. Luh and W. W. Liu, "An immunological approach to mobile robot reactive navigation," *Applied Soft Computing*, vol. 8, no. 1, pp. 30-45, 2008.

[24] M. Alzubi, M. Almseidin, M. A. Lone, and S. Kovacs, "Fuzzy Rule Interpolation Toolbox for the GNU Open-Source OCTAVE," *2019 17th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, pp. 16-22, 2019.

[25] M. Alzubi, Z. C. Johanyák, and S. Kovács, "Fuzzy rule interpolation methods and FRI toolbox," *arXiv preprint arXiv:1904.12178*, 2019.

[26] M. Alzubiand S. Kovacs, "Interpolative fuzzy reasoning method based on the incircle of a generalized triangular fuzzy number," *Journal of Intelligent & Fuzzy Systems*, vol. 39, no. 1, pp. 709-729, 2020.

[27] M. Alzubi and S. Kovács, "Investigating the piece-wise linearity and benchmark related to koczy-hirota fuzzy linear interpolation," *arXiv preprint arXiv:1907.01047*, 2019.

[28] M. Alzubi, M. Almseidin, S. Kovacs, J. Al-Sawwa, and M. Alkasassbeh, "EI-FRI: Extended incircle fuzzy rule interpolation for multidimensional antecedents, multiple fuzzy rules, and extrapolation using total weight measurement and shift ratio," *Journal of Robotics and Control (JRC)*, vol. 5, no. 1, pp. 217-227, 2024.

[29] M. Alzubi, M. Almseidin, M. Alkasassbeh, J. Al-Sawwa, and A. Aldweesh, "Comparative Analysis of Fuzzy Rule Interpolation Techniques Across Various Scenarios Using a Set of Benchmarks," in *IEEE Access*, vol. 12, pp. 33140-33153, 2024.

[30] M. Alzubi and S. Kovacs, "Some considerations and a benchmark related to the CNF property of the koczy-hirota fuzzy rule interpolation," *arXiv preprint arXiv:1911.05041*, 2019.

[31] M. E. Pamukov, "Application of artificial immune systems for the creation of IoT intrusion detection systems," *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, pp. 564-568, 2017.

[32] D. A. Fernandes, M. M. Freire, P. A. Fazendeiro, and P. R. Inácio, "Applications of artificial immune systems to computer security: A survey," *Journal of Information Security and Applications*, vol. 35, pp. 138-159, 2017.

[33] M. Weiser, "The computer for the 21st century," *IEEE pervasive computing*, vol. 1, no. 1, pp. 19-25, 2002.

[34] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview. *The internet society (ISOC)*, vol. 80, no. 15, pp. 1-53, 2015.

[35] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," *2015 IEEE symposium on computers and communication (ISCC)*, pp. 180-187, 2015.

[36] D. Chasaki and C. Mansour, "Security challenges in the internet of things," *International Journal of Space-Based and Situated Computing*, vol. 5, no. 3, pp. 141-149, 2015.

[37] D. Hanes, G. Salgueiro, P. Grossetete, R. Barton, and J. Henry. *IoT fundamentals: Networking technologies, protocols, and use cases for the internet of things*. Cisco Press, 2017.

[38] M. Almseidin, J. Al-Sawwa, M. Alkasassbeh, M. Alzubi, K. Alrfou, "DT-ARO: Decision tree-based artificial rabbit's optimization to mitigate IoT Botnet exploitation," *Journal of Network and Systems Management*, vol. 32, no. 1, p. 14, 2024.

[39] I. Proofpoint. *Proofpoint uncovers internet of things (iot) cyberattack*. Proofpoint Release, 2014.

[40] C. Miller. *Remote exploitation of an unaltered passenger vehicle*. Black Hat USA, 2015.

[41] J. Scott Sr and W. Summit. *Rise of the machines: The dyn attack was just a practice run december 2016*. Institute for Critical Infrastructure Technology, Washington, DC, USA, 2016.

[42] M. Banerjee, J. Lee, Q. Chen, and K.-K. R. Choo, "Blockchain-based security layer for identification and isolation of malicious things in IoT: A conceptual design," *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1-6, 2018.

[43] S. Khanam, I. B. Ahmedy, M. Y. I. Idris, M. H. Jaward, and A. Q. B. M. Sabri, "A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things," *IEEE access*, vol. 8, pp. 219709-219743, 2020.

[44] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," *2014 international conference on privacy and security in mobile systems (PRISMS)*, pp. 1-8, 2014.

[45] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *Journal of network and computer applications*, vol. 36, no. 1, pp. 42-57, 2013.

[46] G. C. Silva and D. Dasgupta, "A survey of recent works in artificial immune systems," *Handbook on Computational Intelligence: Volume 2: Evolutionary Computation, Hybrid Systems, and Applications*, pp. 547-586, 2016.

[47] U. Aickelin, D. Dasgupta, and F. Gu, "Artificial immune systems," In *Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques*, pp. 187-211, 2013.

[48] J. Zheng, Y. Chen, and W. Zhang, "A survey of artificial immune applications," *Artificial Intelligence Review*, vol. 34, no. 1, pp. 19-34, 2010.

[49] Y. Tan. *Artificial immune system: applications in computer security*. John Wiley & Sons, 2016.

[50] H. Alrubayyi, G. Goteng, M. Jaber, and J. Kelly, "Challenges of malware detection in the IoT and a review of artificial immune system approaches," *Journal of Sensor and Actuator Networks*, 10, no. 4, p. 61, 2021.

[51] H. Yang, T. Li, X. Hu, F. Wang, and Y. Zou, "A survey of artificial immune system-based intrusion detection," *The Scientific World Journal 2014*, no. 1, p. 156790, 2014.

[52] J. Kim, P. J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, and J. Twycross, "Immune system approaches to intrusion detection–a review," *Natural computing*, vol. 6, pp. 413-466, 2007.

[53] B. Naik, A. Mehta, H. Yagnik, and M. Shah, "The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review," *Complex & Intelligent Systems*, vol. 8, no. 2, pp. 1763-1780, 2022.

[54] A. S. Muhamad and S. Deris, "An artificial immune system for solving production scheduling problems: a review," *Artificial Intelligence Review*, vol. 39, pp. 97-108, 2013.

[55] N. Bayar, S. Darmoul, S. Hajri-Gabouj, and H. Pierreval, "Fault detection, diagnosis and recovery using Artificial Immune Systems: A review," *Engineering Applications of Artificial Intelligence*, vol. 46, pp. 43-57, 2015.

[56] A. A. Haidar, A. Six, J.-G. Ganascia, and V. Thomas-Vaslin, "The artificial immune systems domain: Identifying progress and main contributors using publication and co-authorship analyses," *Artificial Life Conference Proceedings*, pp. 1206-1217, 2013.

[57] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," *2016 IEEE symposium on security and privacy (SP)*, pp. 636-654, 2016.

[58] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure internet of things," *2016 IEEE 4th international conference on future internet of things and cloud (FiCloud)*, pp. 84-90, 2016.

[59] S. Latif, F. D. Faria, M. M. Afsar, I. J. Esha, and D. Nandi, "Investigation of machine learning algorithms for network intrusion detection," *International Journal of Information Engineering and Electronic Business*, vol. 15, no. 2, 2022.

[60] M. A. F. Pimentel, D. A. Clifton, L. Clifton, and L. Tarassenko, "A review of novelty detection," *Signal processing*, vol. 99, pp. 215-249, 2014.

[61] L. N. Castro and F. J. V. Zuben, "Learning and optimization using the clonal selection principle," *IEEE transactions on evolutionary computation*, vol. 6, no. 3, pp. 239-251, 2002.

[62] U. Aickelin, P. Bentley, S. Cayzer, J. Kim, and J. McLeod, "Danger theory: The link between AIS and IDS?," *Artificial Immune Systems: Second International Conference, ICARIS 2003, Edinburgh, UK, September 1-3, 2003. Proceedings 2*, pp. 147-155, 2003.

[63] J. Twycross and U. Aickelin, "Information fusion in the immune system," *Information Fusion*, vol. 11, no. 1, pp. 35-44, 2010.

[64] P. Saurabh and B. Verma, "Negative selection in anomaly detection—A survey," *Computer Science Review*, vol. 48, p. 100557, 2023.

[65] B. H. Ulutas and S. Kulturel-Konak, "A review of clonal selection algorithm and its applications," *Artificial Intelligence Review*, vol. 36, pp. 117-138, 2011.

[66] P. Matzinger, "The danger model: a renewed sense of self," *science*, vol. 296, no. 5566, pp. 301-305, 2002.

[67] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," *2009 IEEE symposium on computational intelligence for security and defense applications*, pp. 1-6, 2009.

[68] R. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," In *2015 military communications and information systems conference (MilCIS)*, pp. 1-6, 2015.

[69] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," *ICISSp*, vol. 1, pp. 108-116, 2018.

[70] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-baiot—network-based detection of iot botnet attacks using deep autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12-22, 2018.

[71] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1285-1297, 2019.

[72] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, p. 102419, 2020.

[73] W. I. D. Mining, "Data mining: Concepts and techniques," *Morgan Kaufinann*, vol. 10, no. 4, pp. 559-569, 2006.

[74] I. Guyon and A. Elisseeff, "An introduction to variable and feature selection," *Journal of machine learning research*, vol. 3, pp. 1157-1182, 2003.

[75] I. Guyon, J. Weston, S. Barnhill, and V. Vapnik, "Gene selection for cancer classification using support vector machines," *Machine learning*, vol. 46, pp. 389-422, 2002.

[76] J. M. Zhang, M. Harman, L. Ma, and Y. Liu, "Machine learning testing: Survey, landscapes and horizons," *IEEE Transactions on Software Engineering*, vol. 48, no. 1, pp. 1-36, 2020.