Journal of the ACS Advances in Computer Science
Volume 14, Issue 1, 2023

An Artificial Immune System for Detecting Network Anomalies Using Hybrid Immune Theories

Tarek S. Sobh
The Higher Institute of Computer and Information Technology, El Shorouk Academy, Cairo, Egypt
E-mail: tarekbox2000@yahoo.com

Abstract: Detecting network anomaly attacks is important due to the need for security guarantees, reliability, and privacy. The human immune mechanisms intelligently detect, fight, and destroy foreign bodies. This work introduces an artificially intelligent immune approach associated with monitoring systems for detecting network anomalies.
Hybrid Artificial Immune Principles (HAIP) theories such as Self/Non-Self Theory, Natural Killer Cells, and Danger Theory were studied and proposed. HAIP combines several ideas to detect network anomalies in a real-time environment. Ideas were built and tested and presented the pros and cons of HAIS. This work explores the HAIP approach. It focuses on three immune capabilities: feedback, self-organizing, and adaptive learning.
Today, new attacks are complex and not easy to detect. Therefore, the need for network anomaly defense becomes more important to face new threats. The NLS-KDD dataset trains and evaluates our proposed HAIP for detecting network anomalies. The average (AVG) cost and the standard error (STDERR) of the proposed HAIP model were 0.2718 and 0.004, respectively.
It is quite important to present the vaccination process. A vaccination component was designed to formulate this function in HAIP. After the reevaluation using our complete model including the vaccination module, the AVG cost become 0.0420 while the STDERR become 0.001.
Index Terms: Cybersecurity, Intrusion Detection and Prevention, Artificial Immune Systems, Anomaly Detection, Natural Killer Cells, Danger Theory.

1. Introduction

Normally Intrusion Detection Systems (IDSs) are designed to recognize behaviors that may attack a network and/or system resources. There are different classifications of IDS such as misuse-based and anomaly-based [19]. In the case of using systems that are based on misuse approach contains one or more signatures of each attack, which are matched with monitored data. The source of monitored data is collected from the network, operating system, and/or logs [6]. Signature-based IDS has the characteristic of a low false positive rate, it detects only attacks of specific signatures. While anomaly-based follow approaches that are based on misuse detection techniques [28]. The anomaly approach depends on the behavior of profiles, user applications, and network traffic. Changes from normal behavior are seen as threatening acts. The advantage of anomaly detection systems is that they can spot brand-new forms of attack. To identify suspicious activities, regardless of whether they are included in the threat hypothesis, a baseline normal condition must be established first. As a result of this feature, anomaly-based systems should be highly sought after. The ability to identify previously unidentified threats has its benefits, but it often comes with the cost of a high rate of false positives. As a network manager receives an overwhelming number of false alarms, they may get immune to them and the system becomes unworkable.

Training and testing are common components of anomaly detection strategies. Several designs and approaches for identifying anomalies have been presented [6]. Methods based on machine learning (ML), statistics, and data mining are all examples. Here, we employ a novel hybrid immunology technique for identifying anomalies.

The HIS of the human immune can recognize and neutralize potentially dangerous cells [1, 4]. Therefore, based on the same concept other systems may be designed to utilize an Artificial Immune System (AIS) for building an intrusion detection system. Clustering, data analysis, and classification are only some of the difficulties that have inspired the development of novel AIS models. AIS is currently a hot topic in academia. The goal of AIS is to create systems that include various desired qualities of the natural HIS by metaphorically using observed immune system elements and activities. Then, such systems are used to address issues in several fields [2]. The immune system can serve as a model for data mining for many reasons, including its capacity for diversity, recognition, self-regulation, memory, learning, and dynamic protection [16].

The immune system mainly revolves around different ways such as Danger theory [21, 26], Clonal Selection [3], Immune Network [8], and Negative Selection [17]. Recently the combinations of different algorithms become normal to build effective IDS. This study aims to further explore how immunological concepts like self/non-self, natural killer, and risk theory might be applied to the world of network security

DOI: 10.21608/asc.2024.258634.1021

[23, 31]. The immune system provides important information about self-cells versus non-self cells differentiation, inherent resilience to many sorts of old and new infections, and quick response [15]. In this work, a specified self-set database is compared to the collected traffic by the non-self detector. Each collected packet is compared to the number of self-packets in the record set based on the affinity between them. The Danger Theory [8, 21] also emphasizes the importance of innate immunity in shaping adaptive immunological reactions. However, Danger Theory relies on identifying internal threats rather than external ones. When tissue cells encounter stress or harm, they release innate danger signals. Along with the non-self detector, a danger detector uses a mensuration to evaluate the degree of variation between the two profiles by comparing the present system profile with the normal one.

Similar to other forms of computational science like fuzzy systems and artificial neural networks, AIS was implemented to improve network security. Additionally, we attempted to suggest ways in which several theories may be used within a single system as an independent detection engine, with the resulting data being used to inform decisions. Additionally, the hybrid proposed model in this article can quickly detect the threats by using a vaccination process. Although frequently employed in natural life, this biological operation is not addressed in artificial immunity. We made an effort for presenting a basic model of the vaccination procedure and demonstrate how it may be combined with additional components. The tasks of the vaccination procedure are charge of updating the system's knowledge related to the resources profile and ensuring that it is capable of taking action for facing threats.

This work contains Section 2 which describes some previous works. Section 3 introduces elements of schematic IDS. Information on the immune system is explained in Section 4. The concepts of this system components are presented in Section 5. While the system results are discussed in Section 6. A comparative study is introduced in Section 7. While Section 8 defines work conclusions and future directions.

2. Related Work

The issue of utilizing the immunological method to detect network intruders has been addressed in several earlier research papers. In this work, some related works are mentioned and studied. The first Natural Killer (NK) Cells in AISs to detect network intruders [10, 31]. The second is a suggested Intrusion Prevention System (IPS) by Bejoy and Janakiraman (2021) [4] that uses NK Cells of AIS. The third introduces a hybrid AIS for detecting network anomalies [22]. The fourth introduced by Zhang et al., [32] was based only on the theory of self/non-self cells and is known as a multi-AIS paradigm. The fifth employed immunity theory in conjunction with AIS ideas to identify faults [17]. The proposed system, however, combines the self/non-self, danger, and NK Cell theories to create a hybrid IDS system that takes an immunology methodology. The final objective of utilizing the immunity method was to create an architecture that is quite similar to the immune system of humans, which is inherently filled with properties such as robustness, configurable, the ability to scale, the ability to adapt, global analytics, extendibility, and effectiveness.

In our bodies, white blood cells contain Natural killer (NK) cells that destroy both infected and cancer cells [5]. In our immune system, NK is an essential fighter to protect us from harmful invaders, such as pathogens and cancer. Using NK Cells in AIS was first proposed by Fu et al. [10]. It has been suggested that a HIDS that is relying on NK Cells can detect masked spyware. The notion made use of the ideas of initiating and activating signals. Signals that inhibit NK initiation stop them. If the software programs continue to operate normally, then Inhibitory indications are activated. NK engagement is advanced by initial signals. The concept of using natural killer (NK) Cells in AIS was developed by Fu et al. [10]. To find covert spyware, a host-based intrusion detection application that utilizes NK cells was created. The usage of inhibitory signals was here. If the software's regular characteristics were displayed, the inhibiting signal would be active, and if spying behavior was displayed, the activating signal would be engaged. Such NK cells produce cytokines (baits) causing undetectable activities from dormant spyware.

A proposed IPS based on NK cells of AIS was made by Bejoy and Janakiraman [4]. The NK cells were generated via negative selection, and the high fitness of NK cells was multiplied utilizing the clonal selection technique. High-fitness NK cells that can detect numerous attacks were moved to IPS, where the original drop of packets takes place, according to a threshold level.

An adaptable multi-layered framework that can adapt to variations in the implementation has been established by Sobh and Mostafa [22]. The self-non-self theory, danger theory, and NK cells were all combined in this study. The usage of a vaccine module allowed the system's knowledge to be updated. A sniffing module has been used for assistance with packet capture. The affinity relationships of the gathered packets were identified utilizing the Non-self-detector component. The risk module is used to determine any discrepancies from the norm. The module of decision-making made decisions, while a response was used to decide how to respond to an attack.

Sobh and Mostafa [22] used an AIS-based flexible, multi-layered architecture to demonstrate how it may respond to environmental changes. They apply a combination of theories such as self- and non-self and danger theory. The framework continuously scans the system for data that is readily available and checks data stored in two databases. The basic data contains self-identifiers that are constructed and reviewed under controlled settings to generate the necessary game planthe of bundle as well as information that the system may manage. Profiles of system resources (IP addresses, ports, etc.) are contained in the database that follows. A vaccine mechanism was used to refresh system knowledge. The combination of these methods contributed to developing a multiple levels resistant mechanism to gradual incorporation modifications. In general, the design utilized the self/non-self and danger theories, additionally, an immunization part also inspired by conventional immunology.

T lymphocytes and B lymphocytes, which are immunological elements in the HIS, were the main point of interest in a theoretical framework proposed by reference [32] that considers the immune defense system at multiple tiers (various levels). B cells recognize epitopes on the surface of antigens, whereas T cells recognize peptides isolated from foreign proteins. Consequently, in the computing approach, activated T-detectors are used to deliver a signal that activates B-detectors. Furthermore, somatic hypermutation, clonal selection, and negative selection were replicated in individual T and B cells by an on multiple levels AIS model.

With the aid of immunological theory, Rashid et al. [17] applied AIS ideas to find flaws. A negative selection algorithm was employed. A variable radius method was employed to determine the detector radius in this multi-operational approach for enhanced coverage. The method used a dynamic radius allocated to a detector for overlapped situations. The detection module keeps moving once there is less overlap. The mechanism was used to find anomalies in an operation.

3. Elements of a Schematic Intrusion Detection

To assess whether certain system events are a sign of attack activity or simply normal system usage. An Intrusion Detection System (IDS) continuously audits and evaluates the system's events to detect any suspicious activities or security breaches [14]. By obtaining information regarding the nearby surroundings, the system evaluates its activities and detects attempted breaches, current risks, and security breaches that could potentially result in breaches. The primary components of an IDS are the Monitor, which performs network data audits, the Detection component, which makes decisions according to available data and system knowledge, and the Resolver, which aggregates the results of the detector and warns the user via log entries in a database. Fig. 1 depicted Wu and Banzhaf's [27] general IDS architecture, where continuous lines represent the movement of data and control, which represent how the system reacts to intrusion attempts.

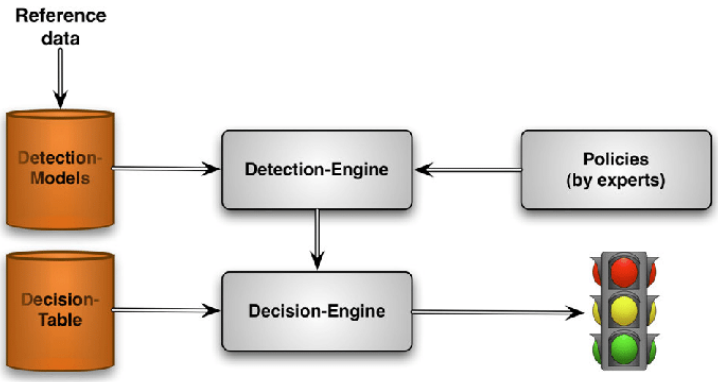

Fig. 1. Schematic of generalized IDS [13]

3.1 Classifications

IDS was divided into two basic categories: host-based systems and network-based systems. The host-based monitoring system keeps track of every action that takes place on a specific host, whereas a network-based monitoring system keeps track of networks traffic, including routers and switches, and focuses on detecting intrusions by monitoring and studying data gathered from this traffic [3].

IDS is categorized based on strategy, framework, and other factors. The design objectives of IDSs are impacted by a variety of conditions. The emphasis of this work is on classification using an approach. The detection techniques are the detection of misuse and detection of anomalies. We have two system kinds in this

categorization: 1) Attacks are represented by misuse-based IDS as signature, allowing even variations of the same attack to be recognized. They are effective at identifying the most well-known signatures of attacks but are of minimal utilization against unidentified attacks. Examples of approaches used in this form of IDS include analysis of state transition, expert systems, and pattern matching. 2) IDS based on anomaly detection, which presupposes that all disruptive behaviors must be unusual. Unusual behaviors that are not obtrusive are marked as such. False negatives are caused by intrusive behaviors that are not unusual (Even while certain events are intrusive, they are not) [5].

3.2 Anomaly Detection

Through anomaly detection of the underlying system's regular data streams, new attack patterns can be discovered [5]. Anomaly detection's main issue is how to distinguish between normal and unusual behaviors. Keeping track of how typical behavior evolves to provide dynamic anomaly detection represents another issue. Because of the overhead associated with monitoring system profile data updating dynamically, systems for anomalies are computationally costly [5]. Recently different works handled anomaly detection by using the AIS application [3, 9].

Table 1 lists the basic techniques for knowledge-based (KB), statistics, and machine learning (ML) that are used with anomaly detection. Also, it describes the main cons and pros of each technique.

Table 1. Anomaly detection basic techniques [11]

Technique	Pros	Cons
Based on statistics: random behavior	- Prior knowledge of regular tasks is not necessary. - Timely detection of harmful activity.	- Capable of being trained by intruders. - Difficulty setting measurements and parameters. - The unrealistic assumption of a semi-stationary procedure.
KB: availability of preceding knowledge/data	- Robustness, Scalability, and Flexibility	- It takes a lot of time and effort to obtain Knowledge or information of outstanding quality.
Pattern classification using ML	- Flexibility and adaptability. - Capture of interdependencies.	- Relying heavily on an assumption that system behavior is acceptable. - Excessive resource use.

3.3 NSL-KDD Dataset

IDS evaluation issues and how it's solved typically have an impact on the selection of an appropriate IDS for a certain environment based on some aspects. The first four instances are True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) that prompt us to inquire about different aspects. These inquiries aid in computing the false alarm rate, detection rate, and identifying the most significant factors in the process.

The IDS is evaluated using a dataset that includes both labeled and unlabeled data points. Various datasets exist, including DARPA, SNORT, and NLS-KDD.

Additionally, there are additional diverse datasets accessible to train IDS. Following are descriptions of the training datasets taken from UNM [25]:

1) The Sun SPARC workstations at UNM used Sendmail with unpatched versions of SunOS 4.1.1 and 4.1.4, and a total of 47 distinct system calls out of 19,526 total system calls were used.
2) On Sun SPARC platforms running unpatched SunOS 4.1.4, the synthetic dataset was gathered using the lpr application. Out of the 2398 total system calls, 37 are unique.
3) The dataset has been tracked using a customized Linux 2.0.35 kernel on a UNM computer, which enables users to gather system call logs. There are 35 unique system calls out of the 541 overall system calls in this dataset.

Here we are going to discuss into the NSL-KDD dataset which is derived from KDD '99 to tackle issues found in the KDD-CUP dataset established by Lincoln Labs at MIT [24]. The NSL-KDD dataset comprises five categories: normal, Probing (Surveillance, port scanning, etc.), Denial of Service (DoS), U2R (Unauthorized usage of local superuser permissions), and R2L (Unauthorized access from distant computer). This dataset is widely utilized as a standard for assessing Intrusion Detection Systems (IDS), which are examined, educated, and authenticated using it. The NSL-KDD dataset boasts connection classes that are

classified as either normal or one of the specified attack types.

One of the few complete datasets that may be shared in anomaly detection is NLS-KDD, which is widely used among numerous academics. In the NLS-KDD dataset, various aspect classes are present. First, the characteristics that may be gleaned from a connection made using TCP/IP. Second, the characteristics of connections with the same host as the connection at a present instance were formed within the last two seconds. Thirdly, characteristics from links that connected to the current instance within the past two seconds and associated service with that connection. Fourth, characteristics that depend on content, like the number of unsuccessfully attempted logins. Additionally, the probability distribution used to create the training and testing datasets is different. Additionally, the testing dataset includes methods of attack that are absent from the training dataset. IDS developers are intended to be challenged by this. The pattern of distribution of an older dataset could vary from that of a dataset acquired later because IDS data always changes in terms of attack vectors and feature distribution. Machine learning is particularly attractive for IDS research because it does not make assumptions regarding data distribution. Numerous researchers have evaluated their anomaly detection techniques using NLS-KDD datasets. They become ubiquitous in the interchange of the link between learning and IDS. Due to all of the previously mentioned factors, the NLS-KDD datasets were chosen for this study.

4. AIS Principals

Abdelhaq et al. [1] presented groundbreaking research on artificial immunity as a suggested approach for developing anomaly detection systems. AIS are algorithms that are utilized in complicated areas of concern and are motivated by fundamental immunology and observable immune activities [3, 18]. In the middle of the 1980s, AIS was created in the area of theoretical immunology. One notion is that computer science (CS) may study the AIS. Since then, those systems have seen a great deal of evolution, and many scholars have attempted to apply this concept to address an extensive variety of issues. AIS makes extensive use of ideas and methods with biological roots. Several algorithms include clonal selection, negative selection, and positive selection. Examples of the theories include the Self/Non-Self, the Danger Theory [8, 17], and Natural Killer cells (NK) [4].

A host's immune system serves as a swift, effective, and innate defense against pathogens. Both the natural immune system and adaptive immunity play a role in this dual defense mechanism. The inherent immune system is crucial for preventing and treating common illnesses, as noted by Zhou et al. [30]. It serves as the body's primary defense against various microorganisms and cancer cells. The adaptive immune system has the ability to recall previous threats and identify new ones, expediting the response to recurring dangers. The innate immune response remains active throughout an individual's life, independent of antigen exposure. While the adaptive immune response can prevent new infections or re-infections by the same pathogen, the innate immune system cells are vital for initiating and regulating the adaptive immune response [16].

People discovered several enticing qualities for a variety of application fields. These fields were found when they considered the innate immune system as an entirely novel source of ideas for computerized applications. The immune system's diversity considerably enhances reliability, both in terms of general and individual scales. For instance, different individuals are susceptible to various bacteria and viruses; it is distributed and made up of multiple elements that work together locally to provide global defense. It lacks centralized management and a single point of failure, making it error-tolerant. Few mistakes in categorization and response have minimal impact. The system is dynamic, with parts continuously produced, destroyed, and circulating, enhancing the immune system's temporal and spatial variety. This process helps eliminate harmful components and strengthen existing ones. It adapts to new bacteria and retains a microbial archive for future reactions. It is self-protecting, using techniques that defend the human body to safeguard the immune system. Key traits include detection, variety, and learning.

By considering the characteristics mentioned previously, the AIS framework is applied in numerous cybersecurity scenarios such as virus identification and IDS. Specifically, cybersecurity is the primary area where AIS is directly applied because of the functional parallels between artificial and natural systems. The contrast of security concerns between HIS and AIS can be found in Table 2.

Table 2. Security concerns analogy between HIS and AIS [26]

Immune System / Security Objective	Human	Artificial
Confidentiality	There is no such thing as confidential or secret information.	Only authorized users should be able to access data.
Integrity	This is a strategy to make sure that no disease will alter the genetic material that exists in the cells.	Data must be shielded from malicious or unintentional corruption.
Availability	This feature enables the body to function even while being attacked by a pathogen.	Computer Information should be available when and how it is wanted.
Accountability	The immune system's goal is to identify, find, and get rid of pathogens from the body.	Cybersecurity applications must be set up to retain enough data related to the penetration to allow for the ability to identify the attack's origin.
Correction	The process of preventing the immune system from attacking cells of the human body itself.	The process of preventing false alarms resulting from improper analytics of attack incident classification has to be kept to a minimum.

The process to let AIS design to adopts a set process for facing challenges such as application business area (domain), representation, calculating for affinities, and algorithms. In the process in order to enable us to map the problem from an innate domain to an artificial one, a group of stages is often taken to solve a particular problem related to the same domain. Step one is to identify the problem domain, which in this work is to design an IDS based on anomalies. Step two is picturing the problematic components that act as an immune system. For illustration, to demonstrate, every single biological cell within the innate immune system was depicted by a protocol (e.g., TCP, UDP, ICMP, ...etc.), source IP address and port number, destination IP address and port number, ... and so on. To arrange and improve the various cells that were generated in step two. The third step involves measuring the affinities or fitness. For this step, an equation must be created to compare the condition of the cells to the end goal of the desired solution. Step four entails selecting a particular algorithm amongst algorithms provided by the AIS framework that is suitable to the application area.

The Self/Non-Self Theory, Danger Theory (DT), and Natural Killer Cells (NK) are the three most significant theories that have been discussed and applied in this research. Within Table 3, you will find a comprehensive overview of the key terms and elements of the innate immune system that have been analyzed for potential implementation in the realm of cybersecurity.

Table 3. Identifying the elements found in the natural immune

Natural component	**Function in the IDS system**
Bone marrow	Self-detection grouped as a set
Antibodies	Each individual detector is symbolized by a specific antibody. The unique traits of the detector (such as packet attributes) are symbolized by a binary vector that is utilized to symbolize each antibody.
Antigen	Attacks on the system are a representation of this.
Matching function	Compare the present antigen with the predetermined antibodies to determine the affinity

4.1 Theory of Self/Non-Self

It is commonly acknowledged that the HIS eliminates viruses that have already infected the body and restores the body's health. Thus, it makes sense that the immune system's role is commonly perceived as one of bodily defense. It additionally makes sense to conclude that as it reacts to infections, which are referred to as non-self cells in immunology language, the immune system creates the distinction between self and non-

self in order to provide such defense. Since the majority of immunological models have been based on defense via self/non-self discrimination, scientists in immunology still mostly agree with this theory of immunity nowadays [20]. Previous immune theories predicated on the concept that the immune system ignores host components (referred to as "self") while reacting to other factors (referred to as "non-self"), like infections, invaders, or modified self [7].

4.2 Danger Theory

The immune system detects "risk" instead of non-self, according to the Danger Theory (DT). This theory suggests that the immune system reacts to danger signals like tissue damage or stress, rather than just recognizing foreign substances. In the post-production stage, a "danger" signal is used to trigger the screening phase. As a result, it is acceptable to produce antibodies known as auto reactive antibodies. With the lack of risk, an antibody that matches a stimulus is eliminated. As a result, innocuous antigens are accepted, and altering selves' cells are accommodated.

The DT offers a new perspective on how the immune system is activated [8]. According to the DT model, the immune system is able to recognize danger signals caused by the necrosis of cells in a host's tissue, as contrasted with the detection of on-self antigens or pathogenic molecules. Death is a result of cellular stress and destruction brought on by an infectious disease or prolonged exposure to harsh environments. The danger signals are considered to be created by the metabolism found in cells and discharged into outside tissue liquid. The cell border breaks down, allowing its contents—such as mitochondria and DNA—to leak out into the surrounding fluids of the tissue.

According to the DT theory, the immune system responds to changes in the tissue's concentration of the danger signal, On the other hand, when the tissue is functioning properly, cells endure an intentional critical process called apoptosis. The release of immune-suppressive enzymes (safe signals) is an indication that the tissue is working healthily. The DT essentially entails quick action in response to necrosis danger signals and active repression while the tissue is healthy. Here, network damage is not perceived as a warning signal. We notice the profile has changed.

4.3 Natural Killer Cells

The natural immune system's cytotoxic subgroup of white blood cells is known as natural killer cells (NK) [4, 31]. They offer rapid responses to cancerous or virus-contaminated contaminated cells. Fig. 2 represents the situation of a normal cell against a virally infected one. NK cells seek to restore lost self-recognition. Stimulating and inhibiting surface receptors are present in NK cells. The largest class I Histocompatibility molecules in cells (MHC-1), the NK cell operates based on Histocompatibility Complex class I molecules (MHC-1) in the cell. A cell's downregulation of MHC-1 is brought on by viral action. Activation of receptors is triggered when cells with less MHC-1 are contacted, making those cells more susceptible to Apoptosis. When inhibitory receptors are active, the cell is seen as normal and is allowed to pass through. Natural killer cells (NK) were originally thought to be the foundation of innate immunity; however, more recent research has shown that they also play a role in adaptive immunity.

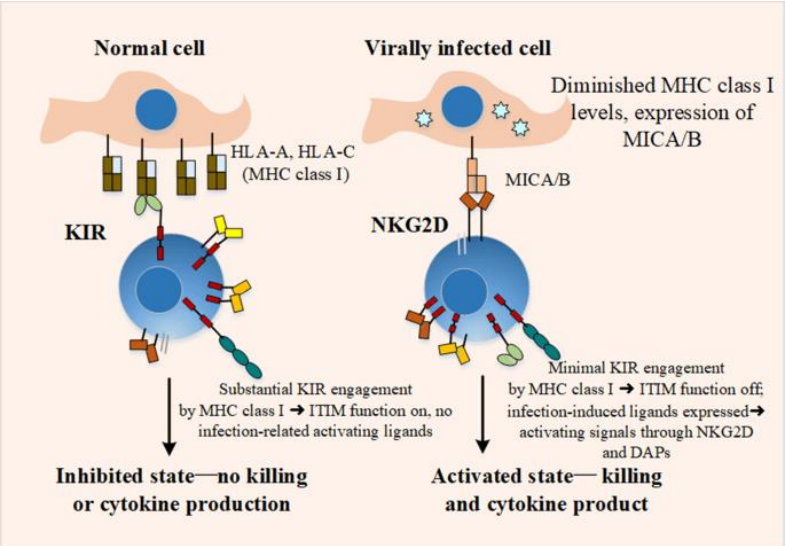

Fig. 2. Normal cell Vs Virally infected cell in NK [30]

Here, artificial NK cells are shown for IDS. Output: Artificial NK cells shown for IDS, memory of NK cells with antigen-specific immunological memory, components like natural NK Cells, immune system agents monitoring data security, activating and inhibitory receptors, response to activation, cytokines alarm or apoptosis, artificial NK cell as NK (Type, AR, Fitness, State).

Type here designates the category of attack that the NK cell is equipped to recognize.
Fitness: The number of attacks the NK cell has identified is used to calculate its fairness level. The ability of NK cells to proliferate or clone is better the greater their fitness value.
State: Until they are triggered, all NK cells are basically in a dormant condition.
Activating Range (Ar): The distance between an individual NK cell's central vector and its detection radius is known as the activating range or Ar.

When an NK cell receives an incoming MHC1, it becomes activated. The NK cell is in an activating response (AR) if the MHC1 is inside Ar; otherwise, it is in an inhibiting response (IR). The cell is regarded as mature if the fitness evaluation exceeds the fitness threshold. The cell has multiplied if the total number of cells is more than the entire population.

Zhou et al., [30] assumptions are:
NK cells are defined in Deterministic Finite Automata (DFA) as a 5-tuple $(Q, \Sigma, \delta, q_0, F)$.
NK = DFA $(Q, \sum, \delta, q_0, F)$ where:
A finite set $Q = \{q_0, q_1, q_2, q_3, q_4, q_5\}$ is the set of states
A finite set of symbols $\sum = \{a, b, c, d, e, f, g, h\}$ is the set of inputs
A transition function $\delta: Q \times \sum \rightarrow Q$ as defined where:
An initial state $q0 \in Q$ q_0 is the start state and
A set of accepting states $F = \{q_0\}$ is the set of final states.

According to Zhou et al., [30], the states are described as follows: q_0 Passive, q_1 Active, q_2 Activating Response, q_3 Inhibitory Response, q_4 Mature, and q_5 Cloning.

5. System Design

For the purpose of detecting network anomalies, the proposed HAIP aims to integrate various immunology concepts and methods into a unified system. These approaches collaborate to establish a multi-layered security system capable of responding to dynamic environmental shifts. In addition to the immunization procedure, our primary hypotheses included NK, self/non-self, and the danger theories.

Receiving network traffic, looking into intruders, and carrying out his duties are NK's first lines of defense against intrusion. While the self/non-self distinction and the threat theories underpin two opposing perspectives in the field of immunology and serve as the second line of defense against intrusions. But in the field of computer science, we think that both two lines of defense may be combined to create a system with cooperative parts which complement one another. The function of the vaccine unit is the same as it is in nature. It aims to change how the system behaves in response to fresh or more sophisticated threats. This combination ensures that there is more flexibility in responding to environmental changes and that there is no only one method to protect. Additionally, this combination offers a compassionate and real hybrid IDS system that is both compassionate and a real hybrid IDS.

Applying the aforementioned concept to the security realm—and using the Smurf attack as a prime example—we can see that an administrator of networks would be suspicious of traffic coming from an unknown source. However, if this is coupled with an important change from the norm of traffic, an alert signal should be expressed, and possible action needs to be taken.

5.1 Modules

It operates in real-time to detect attacks. It gives a summary of how runtime operations work. The suggested system logs data using a connection vector that is produced to represent each incoming connection and includes the port, IP, and the number of packets transferred to the source and destination in order to keep track of the connections that arrive while it is in use. The connection vector is then subjected to detectors created for anomaly detection, as we will see later. A categorization method is then projected onto any connection vectors that have been identified as unusual. Fig. 3 emphasizes the suggested system's operation that works in real-time.

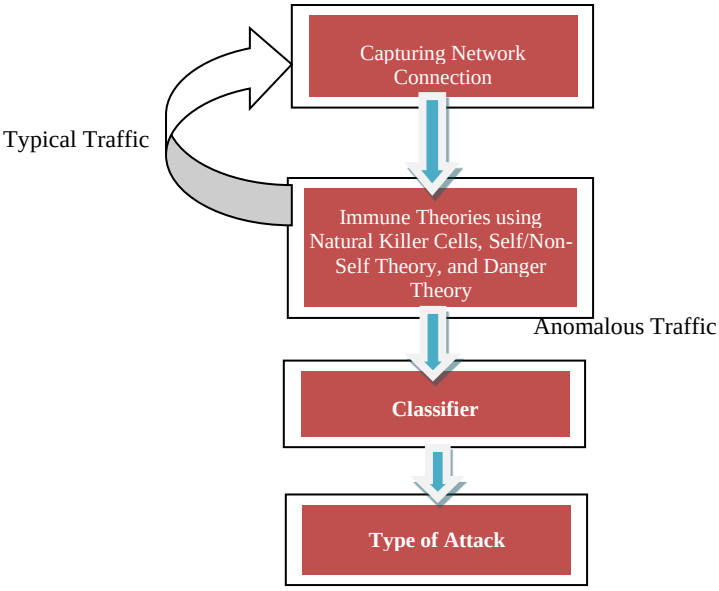

Fig. 3. Required steps of the underlying system

The suggested system continuously examines the network data and checks it against the databases that are currently in use. A collection of self-detectors that were gathered and inspected to produce the basic set of packets and data that the system as a whole needed to provide well formed the initial database. The next DB has profiles of typical system resource utilization, such as network connections and ports that have been contacted. This database was created to aid in separating typical consumption from unusual usage. A decision-maker module determines whether or not there is an attack (regular traffic) based on the results of each packet comparison with those two sources. Fig. 4 introduces the system modules and the data flow between them.

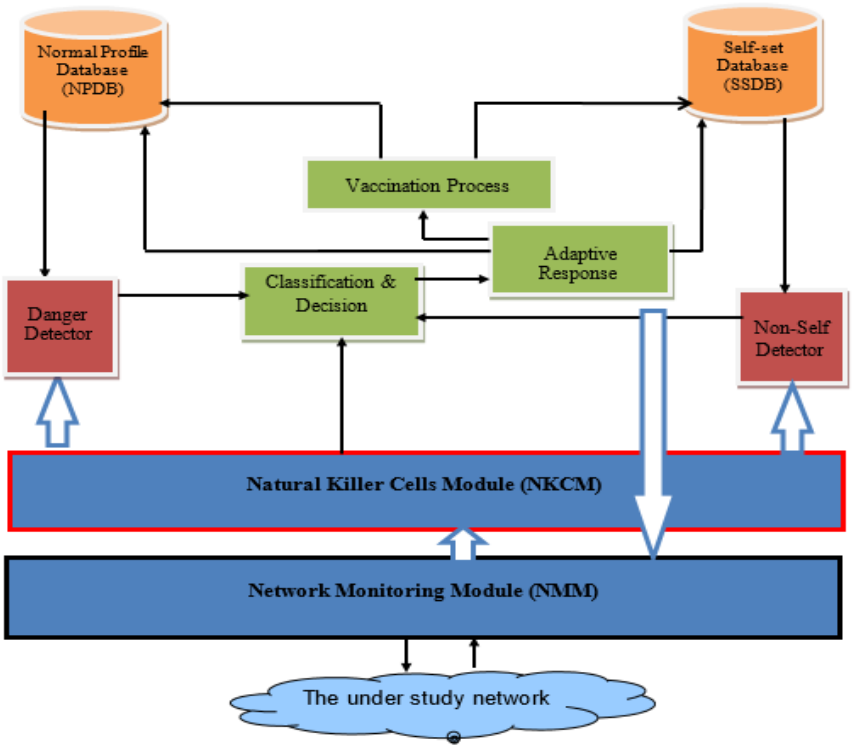

Fig. 4. System main components

This work contains Network Monitoring Module (NMM), Natural Killer Cells Module (NKCM), Non-Self Theory Module (NSTM), Danger Theory Module (DTM), Natural Killer Module (NKM), Vaccination Process Module (VPM), Classification and Decision Module (CDM), Adaptive Response Module (ARM), Self-Set DB (SSDB) and Normal Profile Database (NPDB).

NMM audits network traffic using network lines. It sniffs packets and analyzes each packet's parts that make up it. It gathers every data packet that passes through a certain network interface. Before being sent to the detection component, data is online reviewed to look for possible attacks. Here, we interface with Winpcap from our module.NET program using the SharpPcap.NET assembly (library). If there is a lot of traffic, NMM can still function offline and the results are preserved in a log file.

NKCM uses an information vector that is collected by the NMM module. From IP packets, an information vector (MHC1) that may include the IP address, port number, protocol types, etc., can be obtained. The NK cell agents employ it as an inhibitory signal or an activating signal. Whenever it is the initiating receptor, the process of (programmed cell death) occurs. That indicates that it is an intruder, and either notification indicating the detection of an attack is delivered to the admin. Future development will include a packet-dropping technique. While if it is the sensory communication typical then the packet is normal. Each NK cell has three main roles: perceiving, processing, and reacting. Depending on the type of attack the NK cell is taught to recognize, the sensing unit chooses specific properties from a packet. The NK cell's detection range is compared by the analyzing unit, which is then employed to activate the activating receptor or the inhibitory receptor. A unit of response was utilized to respond according to the analysis unit's output. In this work, we used Natural Killer (NK) cells for detecting network intruders. In Natural Killer Cells Module (NKCM) we implemented the same algorithms of Bejoy and Janakiraman [4]. As depicted in Fig. 5, they suggested Natural Killer (NK) cells with immunological memory. The negative selection technique is used to calculate each NK cell's detection radius, and then each NK cell is trained to recognize various threats. A clonal selection technique is used to spread out and distribute efficient cells with high fairness values throughout the network

Heavyweight NK cells (HWNK) and many Lightweight NK cells (LWNK) are the two types of NK cells used in this study. The Major Histocompatibility Complex Class I (MHC1) is created after vectoring the received data. An activating receptor or an inhibitory receptor is then activated in response to this MHC1. Activating Receptor is turned on if it is an attack's signature. Apoptosis or the release of cytokines is the outcome of activating receptor activation. Apoptosis in this context refers to the falling off of the packet, while cytokine release denotes the generation of an alert informing the administrator.

The collected packet is compared to the self-contained database by NSTM. It assesses the packet's affinity with each self-packet in the collection and shows the highest match value. To ascertain if the collected packet is known or unknown to the system, the maximum match value is compared to a threshold. This process is known as abuse or signature-based detection in the security sector. This comparison between traffic patterns and known attack patterns or signatures led to the analogy. Based on what was discovered in this comparison, all decisions of IDS are made. The collected packet is compared to the self-contained database by NSTM. It analyzes the packet's connection to every self-packet in the group in order to find the most suitable match. The system displays the highest matching value, which is then evaluated against a specific threshold to determine if the packet is acknowledged by the system. This component is commonly referred to as the misuse or signature-based detection module within the realm of security.

To detect deviations and evaluate their severity, DTM compares the present system's usage characteristic to the profile database's regular system usage. This is seen from the perspective of the security field as the anomaly-based detection component, which can identify recent and novel attacks by identifying variations in typical behavior. This module's other function is to tune the self-database, which is described further down, by identifying the sources that have generated alerts. If these sources were listed as participants in the self-database, it then reports them so they can be deleted. This role illustrates how the various ideas (Self/Non-Self and Danger) could work together and adjust to one another.

VPM works similarly to the vaccination of human immunization procedures. It is in charge of refining the system's knowledge (such as thresholds and profiled resources) by examining how an attack behaves in an audited environment and determining if the system is capable of responding to the attack. The training procedure follows the standard procedure for creating the anomalies profile. The immunization procedure is more similar to a method of warning the system ahead of time of impending attacks.

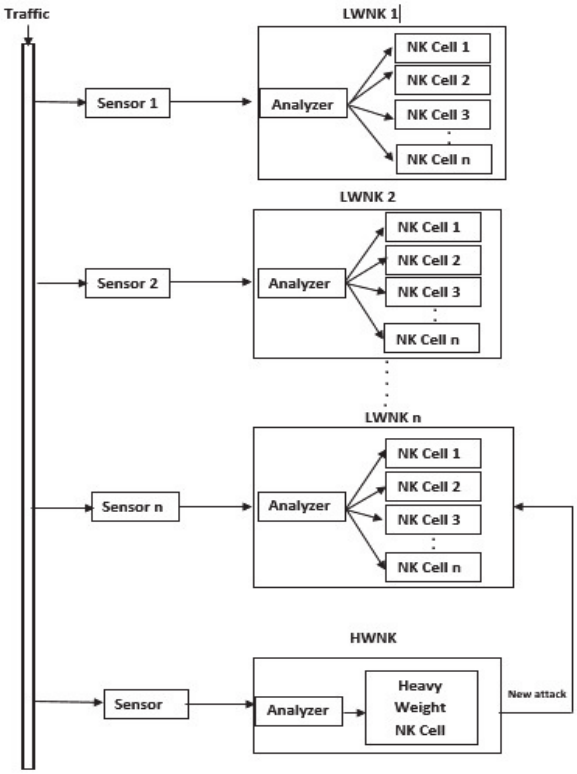

Fig. 5. An NK cell-based IDS architecture proposed by Bejoy and Janakiraman [4]

After the vaccine, once the system capable to continuo (i.e., survive) the subsequent attack, it suggests the new profile is acceptable. However, if the vaccination is not acceptable (i.e., harmless), it is required a new profile or at least some changes to the existing DB are mandatory.

To enhance the system's capabilities, specific measures must be made based on the reaction of the system, such as enabling defensive software (such as the new configuration of a firewall). This gives the system more dynamic behavior and makes it possible to detect new attacks early on. Briefly, the following vaccination process phases are implemented by the vaccination module: First, it obtains the necessary attack profile, and second, an outside computer attacks the system. Third, examine the attack's effects on the system and how the system reacted. Fourth, maintain the system databases to better prepare for future attacks.

The outputs of the two detectors stated above are combined by the CDM module, which also produces consolidated results with some analysis of the attack's source, potential causes, and name if the system is aware of the attack. The two detecting modules' collaboration in this component is essential. They coordinate in both coming to the final choice and keeping each other informed with updates.

It is up to the ARM module to take the necessary steps. Responses could include informing other hosts on the network or updating databases. For instance, if the attack signature was present to imitate the ability of the natural immune system to react more swiftly to repeated attacks, this module stamps the attack signature and removes it from the safe list. When an attack produces a risky behavior, we can identify its signature. If something is safe even if we remove it, we lower its level of safety and if the risky activity continues, we might outright forbid it. Therefore, if the same attack occurs again, the reaction will be fast. The response mechanism could be changed to serve as a preventative mechanism by immediately stopping the attack in real time (online). However, this will put more pressure on the system's performance.

SSDB records the collection of secure packets. There are columns for the protocol, destination (IP and port), and source IP. To determine whether any new packets mimic any other members of this safe set, each one is compared to the data in this DB. This database can be created offline using reliable historical information or online in a controlled environment. Based on the steps taken by the decision-making module, the database is updated as needed.

The NPDB component collects the system usage profile to create a starting point that may be compared to any typical behavior. The profiles change over time to suit actual usage. Database columns for numerous connections may include the number of connected ports, and error messages from inaccessible hosts. The profiles may be modified and updated either manually by an individual user or automatically by tracking

system usage and running statistical analyses.

These aforementioned data house the backend DB that the system uses to detect attacks. These databases can be created either online or offline using already-created files. The system gives the user the ability to change the database's structure. It allows users to add or remove system resources that will be profiled to enable more comprehensive detection.

5.2 Working Steps

This work has two detector repositories, as was mentioned in the primary idea section and is seen in Fig. 4 above. The first set of detectors stands in for the main communication triplets (Source IP and Port, Destination IP and Port, and Protocol). These stand in for the self-set and are constantly updated as new attacks or false positives are found. A collection of profiles that record system variables is contained in the second set. Here offer a few instances that illustrate starting profiles for variables that can be measured and their period: 1) the number of connections made within a given period, such as 20 seconds. 2) The number of ports contacted in a given period, such as 15 seconds. These parameters were selected after researching attack behavior. The number of contacted ports over range, for instance, is impacted by the Nmap port scanner. The network administrator adds to the initial profile. A deviation from these characteristics by a certain amount will signal a risk. Here, a quick check was used to identify deviations from the profile: When a profile variable's variation from a real variable exceeds the threshold value outlined in the profile definition within the same preset time frame, the system detects and produces a potentially risky activity. The stages taken by the suggested system are as follows:

1. *The Natural Killer Cells Module (NKCM) will test a new packet when it reaches the IDS host.*
2. *Once NKCM finished its algorithm the new packet that passed NKCM arrives at the next detection step, it will be evaluated to see if it triggers a danger alert or non-self alert. Here's how the test is conducted:*
    - *At the beginning monitoring the packets*
    - *Apply "non-self" matching detector*
        If not then
            Stamp a non-self signal at the conclusion
        End IF
    - *Apply "danger pattern" matching detector*
        If a danger pattern founded then
            Stamp a danger signal at the conclusion
        End IF
3. *If there is an alert with a degree of certainty, those alerts are raised to the classifier of the CDM module if they exist.*
4. *4. The CDM can then take the necessary step according to the information provided by both of these sources.*

Activities that can be performed include logging the suspected source and a brief description, warning the rest of the hosts on the underlying network about the threat. Therefore, the next step is updating the detectors' repositories, and analyzing the patterns of attack to create a method for identifying attacks that are identical to but slightly different from one another.

Self-set's database is built in a controlled setting environment. Users of such a suggested system can load their self-set from a file or collect it online. The system keeps track of user activity and system resource usage to build the profile database. The user may request the creation of the profile. The investigation of numerous attacks and associated events that have an impact on system resources is the basis of the initial resources to be monitored [6]. Additionally, the r-contiguous bits technique was used in this work to calculate the affinity. The largest continuous number of bits between two antibodies recorded in binary format was used in the proposed technique to define affinity. The system includes a mechanism for collaboration between those two detection modules in addition to two attack detection approaches in two detection modules.

When a new packet is collected, the NSTM pseudo-code is:

```
Maximum = -1
For I = 0 to Self Set Size
        Matching Array [I] = Match Strings (New Packet, Self Set [I])
        If (Matching Array [I] > max) then
                Maximum = Affinity Vector [I];
    End if
End For
```

If (max < matching threshold) then
Create a non-self as a warning message
End if

The pseudo-code of the DTM (regular checks):

If (Calculated Variance (Current Profile, System Profile) > Variance Threshold) then
Create a warning signal
Send the self-set removal of suspicious IP source addresses
End IF

5.3 Operations

We utilized the open-source "SharpPcap" to monitor network packets, and the system was developed using the .net framework. As shown in Fig. 6, the system provides users with various features, such as:

1) Restart/Stop the system whenever you like;
2) Select the network interface to activate (such as Ethernet, Wi-Fi, etc.);
3) Create fresh packets to represent attacks (for vaccination trials);
4) Save the current self-set (group of trusted packets) or load one from a file;
5) Create a profile for a user's utilization of recommended resources (like established connections or contacted ports), or the user can choose an alternative resource for the system to track for usage changes;
6) Evaluate the escalated attack analysis description generated by the decision-making module against the confidence level of each detection method (self/non-self and threat indicators);

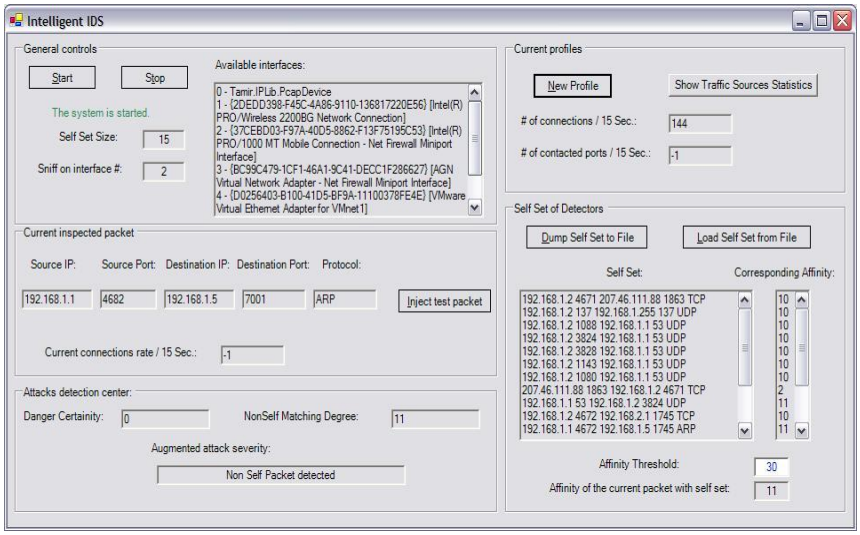

Fig. 6. Shows a user interface of the proposed system.

6. System Results

In this case, the suggested system was tested on an actual experimental configuration network. It uses and divides the NLS-KDD dataset into two sets. 86,001 normal connections, 9001 DoS, 4,000 Probes, 900 U2R, and 600 R2L are all included in the training set. 30356 normal connections, 3,313 DoS, 2,096 Probe, 453 U2R, and 105 R2L were included in the testing set.

As shown in Fig. 7, the test involved a large number of computers running Windows 10 that were all additionally protected by firewalls and linked to the Internet via network devices such as routers and switches.

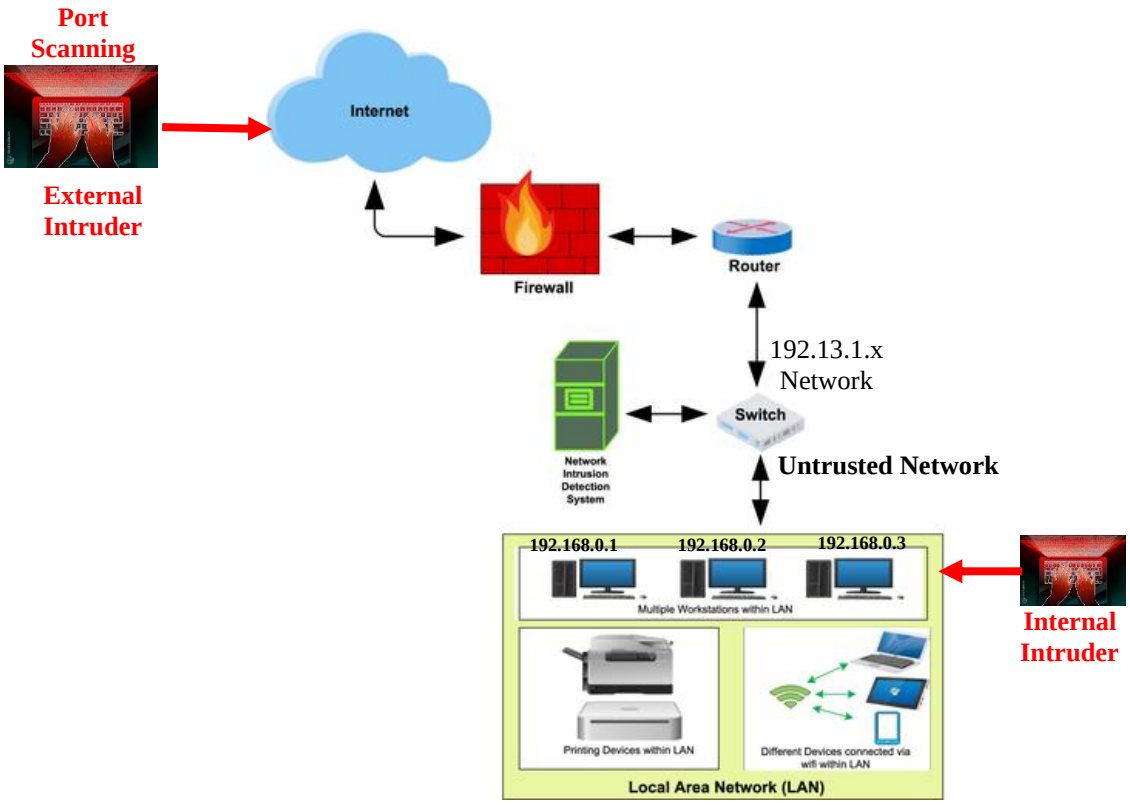

Fig. 7. Testbed Environment

Real network traffic is tested over the testbed environment using the suggested system. As shown in Table 4, compares the observed network traffic against the profile of a typical user to discover possible network attacks.

Table 4. Attacks and attached system resources

Characteristic of Attack	Attack	Watched Resources
During the password-checking process, there was a buffer overrun error.	DoS	Authorized users cannot access some network-based services.
The access ratio between common and uncommon ports	Nmap Port	Keep an eye on the total number of ports being reached at certain times and look for changes.
An attacker is capable of exploiting current system flaws since they are aware of them.	Probe	To learn more about what services are active on a host, a port scan establishes connections to numerous ports on that host.
The proportion of traffic volume flowing in and coming out every second	Smurf	At regular intervals, keep an eye on network traffic and detect changes.
The identical modification to specified performance elements on two or more networked systems	UDP Storm	Observe the inbound and outbound traffic at a certain interval.
Using system resources like the network, files, and RAM suddenly failed.	ARP Poison	Keep an eye on errors messages in reaching destinations

The implementation of anomaly IDS based on transactions including performance evaluation and computer specs should be a part of this valuation (Core i7 processor Generation 11 with 8 Mbytes caches, 2.4 GHz Intel, 4-Gbyte DIMMs, 500-Gbyte HD).

The system is informed of the signal's source(s) when a danger signal is sent so that it can be compared to the self-set. By only keeping the IP of source addresses that have a high level of trust, this helps to fix the

self-set members. Given that attacks rely on a high signal for a short time rather than a low signal for an extended period, as illustrated in Fig. 8. The main source address connecting to the system does not necessarily have to be the greatest attacking host expectation.

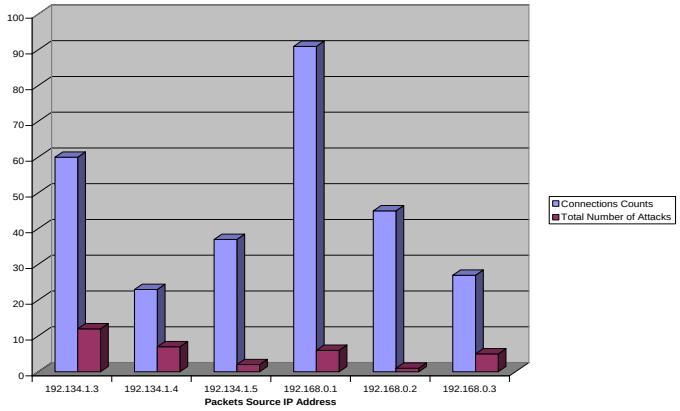

Fig. 8. Plots packet source IP address data against connection counts and overall attack counts.

Finally, Fig. 9 shows the preliminary testing results for the recommended HAIS anomaly detection system. It demonstrates that the NMM recorded 30,050 typical connections. It displays 5,010 suspicions of anomalies that were discovered by this recommended HAIS.

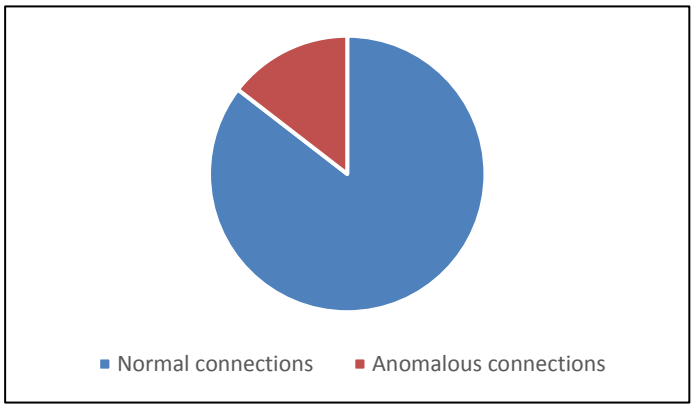

Fig. 9. Proposed HAIS classified about 30,050 typical connections Vs 5,010 abnormal (anomalous) connections

When examining such data, it's important to understand that although the attack categorizes the effectiveness of both non-self detectors and danger detectors, they are not the same. As a result, without taking into account the various classifications of anomalous connections, the AIS component classifies each connection as either normal or anomalous. Nevertheless, the results are displayed in terms of attack categories. Only known attacks against this module occur using attack classes using the "CDM" module. As shown in Fig. 10, were not classified by CDM, however, it did classify 1002 DoS, 179 Nmap Port, 301 Probe, 702 Smurf, 301 UDP Storm, and 96 ARP Poison while the remaining 5,010 abnormal connections. As a result, Fig. 10 enhances the classifiers for anomalous attacks.

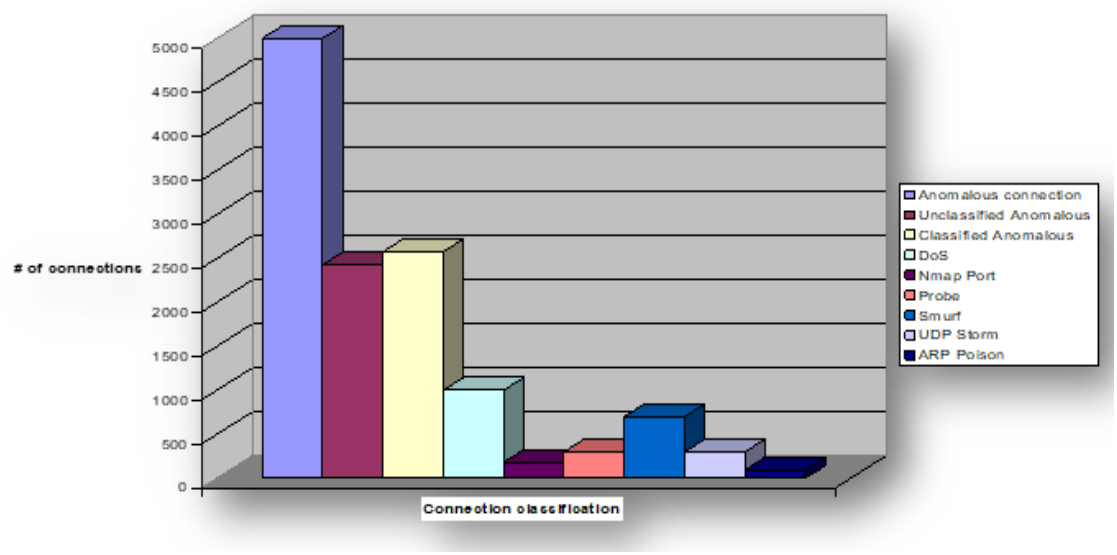

Fig. 10. Classifications for anomalous attacks

DTM measures the difference between the profile of the present system and the database of typical profiles. Fig. 11 displays how the detection time is varying with the size of the profile. The network state and the target host's reaction time are only a few of the many factors that determine the detection time, which varies significantly from run to run. Generally, we observe that as the combined size of the two profiles grows, so does the detection time. Even in the most severe scenario, classifying with a total size of 200K (100 Kbyte for the present system profile and 100 Kbyte for the default system profile) takes no more than 2.4 seconds. In reality, the NLS-KDD dataset only allows us to extract profiles up to 100 Kbyte in size. The experimental findings demonstrate that while DTM requires big profiles, the DTM module's processing time is still sufficient for it to operate in a real-time setting. Of course, in addition to profile size, additional elements affecting detection time include network traffic and target host response time.

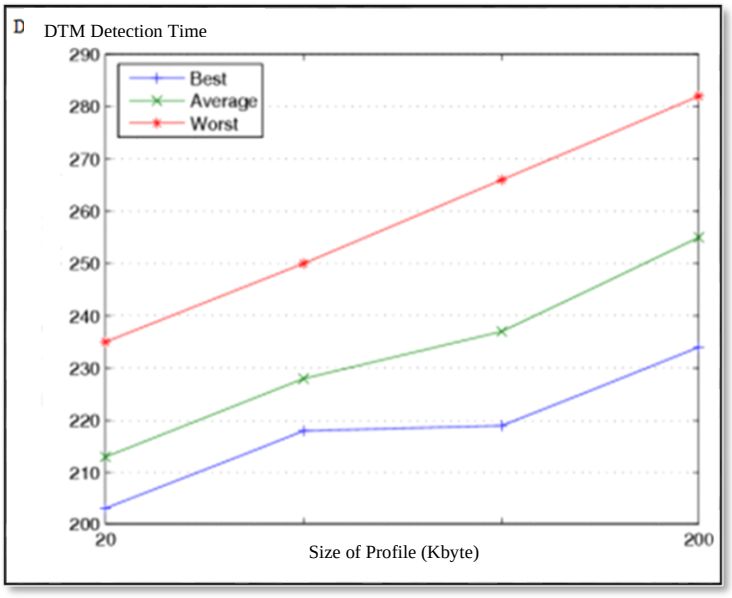

Fig. 11: The complete size of normal and current profiles relative to DTM module detection time.

The confusion matrix of the main categories is shown in Table 5. As shown in Table 5, four key attacks are classified as Probe, DoS, U2R, and R2L while network traffic may also be used for routine activities.

Table 5. Confusion matrix by main attack categories

	Probe	Normal	DoS	U2R	R2L	Total Count
Probe	3471	511	184	0	0	4166
Normal	243	60262	78	6	4	60593
DoS	1328	5299	223224	1	1	229853
U2R	294	14527	1	1360	8	16190
R2L	20	168	1	10	30	229
Total Count	5356	80767	223488	1377	43	**311031**

According to the displayed data in this table, the calculated date of TP (True Positive) = 228085, FP (False Positive) = 20505, FN (False Negative) = 331, and TN (True Negative) = 60262. The accuracy formula that gives is accuracy = (TP+TN) / (TP+FP+FN+TN). Therefore, the accuracy percentage of our correct classifications becomes 93.26%.

Using the average (AVG) cost based on the test example, we analyzed the suggested model without the vaccination part using the cost matrix from the NLS-KDD contest. According to the confusion matrix in Table (5), the AVG cost of the given model in this case was 0.2718. The standard deviation was 1.1067, and we additionally calculated the standard error (STDERR), which was 0.004. As seen in Table 6, certain attacks fall under one of the four main attack groups mentioned above.

Table 6. Different Attack Types in Four Main Classes

Category/Class	Attacks
Probes	Satan, ipsweep, Nmap, portsweep
DoS	Neptune, Smurf, teardrop
U2R	Buffer overflow, load module, rootkit
R2L	Guess password, IMAP, multihop

The confusion matrix is presented in Table 7. While in Table 5 each row represents a specific occurrence in a class of actual network traffic, and each column represents a similar instance in a class of predicted network traffic. Along with the typical traffic class, Table 7 also lists the following network attack categories: Satan from the Probes category, Teardrop from the DoS category, rootkit from the U2R category, and IMAP from the R2L category.

Table 7. Confusion matrix of traffic class

	Normal	Satan	Teardrop	rootkit	IMAP
Normal	12019	43	121	2	2
Satan	51	756	22	0	0
Teardrop	83	14	998	0	0
rootkit	8	2	0	180	0
IMAP	4	1	0	0	74

At this point we used the offered hybrid model, which includes the vaccination process, to evaluate the confusion matrix final results. It had a STDERR of 0.001 and an AVG of 0.0420.

Packets of self-set DB play an essential role in raising our confidence about the attack's level. It generates a high false positive alarm when the system first starts, but later on, the DTM supports refining the set of values as illustrated in Fig. 12 below.

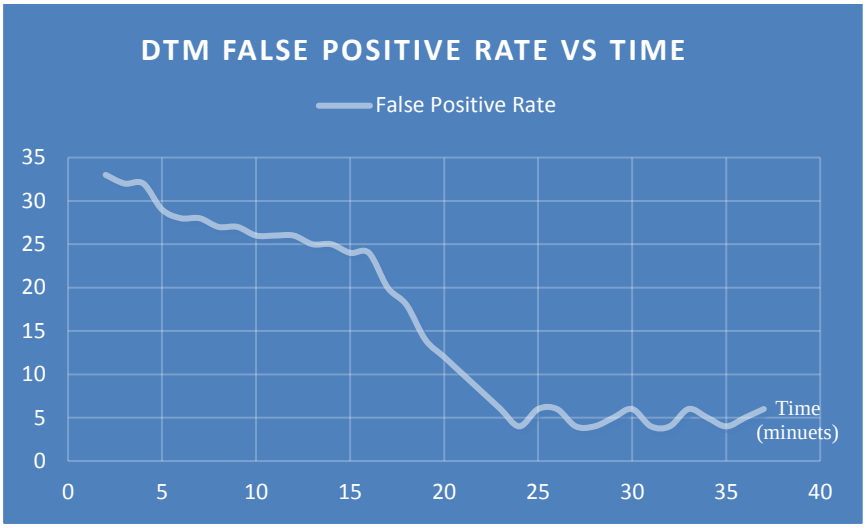

Fig. 12. The self-set is updated using the DTM component and thus indicates that there are fewer FP rates over time.

A perfect IDS should have a zero percent false alarm rate and a detection rate of 100%. The (ROC) curve created by our suggested anomaly detection system for the receiver is indicative of its operation by the area under the curve in Fig. 12. Our experimental setup involves vaccination as well as the proposed HIS algorithms. For evaluating classifier performance across a variety of TPR and FPR tradeoffs, ROC curves are employed. The x-axis of a ROC curve displays the false alarm rate while the y-axis is the detection rate such as ROC=TPR; FPR, for example. The ability of ROC diagrams to distinguish between error cost factors and anomaly detection performance is one of their advantages. The proposed anomaly detection in Fig. 13 is shown as a blue line using only a non-self cells module. The proposed anomaly detection utilizing simply the danger detector module is shown by the green line. The recommended model conclusion is shown by the red line.

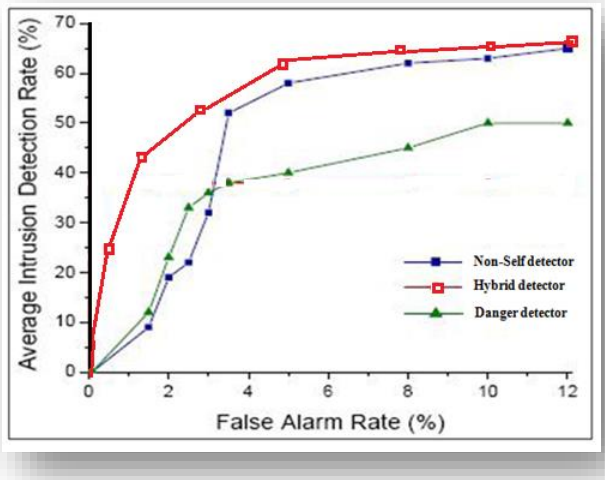

Fig. 13. ROC curve

The performance of the system is also impacted by two system variables. The first is the size in MB of the self-set of detectors (trusted packet signatures). The performance of the system will reduce exponentially as the self-set database size increases. Still, Mid-size sets are acceptable, particularly if the entire system has been distributed over many hosts that can alert one another to an expected attack. This will also reduce the frequency of false positive alarms. Second is the threshold for self-set packets and newly arriving packets matching. In this case, very low and extremely high values are undesirable.

The connection phase is referred to here as (Data Transmission). Connection establishment, packet transfer, and end of connection are the phases of a connection. The term "Total Connections" refers to these various connecting processes. The overall throughput for a TCP/IP-based network connection serves as an example of starting a connection session, packet transfer, and connection cancellation; the best-case throughput is just 24 Mb/s. The overall throughput achieved in the case of data transfer entirely is 118 Mb/s.

Analytical findings from the measurements clearly indicate that a significant amount of additional effort will be required in order to effectively enhance the performance evaluation of this particular work.

7. Comparative Study

Related immune system-inspired anomaly detection research has three main antecedents. The earliest techniques make use of traditional algorithms, including IBM's virus detector [14]. Second, Rashid et al. [17] and Zhang et al. [32] adopted the negative selection paradigm. While the Danger Theory is exploited in the third strategy [8].

Although they had various implementations and architectural designs, all of these approaches were based on immunological techniques. Building a system that is extremely similar to the HIS has always been the ultimate goal.

The thymus gland engages in a process known as negative selection that helps in preventing the entry of self-reactive cells into the lymphatic system. The algorithm of negative selection is introduced using this norm to find data modification that is carried on by computer viruses. This method's fundamental idea is to create certain detectors in the adjacent space, then use those detectors to categorize newly classified data to be a self or non-self as used in an immune system.

According to Hart and Timmis [12], they employ the negative selection strategy, which has a number of limitations including scale problems, high false-positive rates, and complicated concerns. But, as a result of its capacity to produce a collection of detectors from a single class of data (the typical network traffic), the negative selection method is frequently mentioned as having potential application in anomaly detection difficulties. Also, the negative selection approach can train the system using only one class of data, some investigations tend to indicate that the system needs a second class to be tuned.

To address the limitations of the negative selection strategy only, we present NK cells, the danger theory, and negative selection approaches in this study. Normal profiles can be dynamically updated in response to network changes. Additionally, based on the outcomes of our experiments, the self-set is updated by utilizing the danger detector over time, which reduces the frequency of false-positive alarms. The activation mechanism of T-detectors is regulated by T-suppression cells, in contrast to the utilization of T-suppression detectors as described by Zhang et al. [32]. Furthermore, prior research efforts failed to incorporate the vaccination process. While our study excels in detecting a wide range of attacks such as Nmap Port, Smurf, UDP Storm, and ARP Poison, alternative studies like LISYS [29] focus solely on the source IP address and port number. This is inadequate for detecting various attack types. In this research, we have developed a hybrid approach that includes the vaccination process into the detection mechanism of T-detectors.

Finally, the winning NLS-KDD dataset computation AVG cost is 0.233, compared to the hybrid immune model's AVG cost of 0.1195 without a vaccination module. The ultimate AVG cost was 0.0420 and the STDERR was 0.001 when employing the recommended hybrid immune system that includes a vaccination component. While some of the other comparable work finds anomalies offline, the suggested approach operates to detect anomalies in real-time.

8. Conclusion & Future Directions

This study demonstrates how various immune system theories can be merged to form the basis of intrusion detection systems that are more trustworthy. The decision-making unit was much aided in its efforts to take more appropriate action by relying on multiple data sources and analysis of those sources. In addition to discussing NK cells, this study discusses how an IDS system can make use of the self/non-self and danger theories. The suggested approach may successfully prevent incidents by distinguishing signatures and identifying the origins of attackers. Such action may happen if attackers launched additional attacks, their names and other available information would appear on blacklists. The system's ability to adapt, features that are inherited from the human immune system (natural immune), allowed manual or semi-automated dynamic control of system variables for the vaccination process. This made it possible to react quickly to threats. The performance of the system is satisfactory, particularly if it has multiple hosts and a distributed architecture. Each of these is equipped via a particular set of detectors and linked to the others over secure connections.

Future improvements may move the immunization process toward full automation so that it can generate a report of suspicious traffic in advance and respond to that report without operator intervention. By using the high fairness NK the proposed system may be upgraded to act as an intrusion prevention system (IPS). The development of more sophisticated security-related solutions that might imitate the inherent complexity of the human immune system will benefit from a deeper understanding of the other immune theory. Additionally, this effort may be focused on developing a software tool to evaluate the effect that happens by attacks on

certain networks, establish a scenario for defending against such assaults, or attempt to determine why the network that underwent the attack became exposed to those attacks.

References

[1] Abdelhaq, M., Hassan, R., Ismail, M., and Israf, D., "Detecting Resource Consumption Attack over MANET using an Artificial Immune Algorithm", Research Journal of Applied Sciences, Engineering, and Technology, Volume 3, Issue 9: 1026-1033, 2011

[2] Aldhaheri, S., Alghazzawi, D., Cheng, L., Barnawi, A. and Alzahrani, B. A., "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, Volume 157, 2020, 102537, 2020 https://doi.org/10.1016/j.jnca.2020.102537.

[3] Bejoy, B. J., Bijeesh T.V., Janakiraman, S., "ARTIFICIAL IMMUNE SYSTEM BASED FRAMEWORKS AND ITS APPLICATION IN CYBER IMMUNE SYSTEM: A COMPREHENSIVE REVIEW", Journal of Critical Reviews, Volume 7, Issue 2, Pages 552-560, 2020. https://doi.org/10.31838/jcr.07.02.103

[4] Bejoy, B. J. and Janakiraman, S., "Enhanced AIS Based Intrusion Detection System Using Natural Killer Cells", Journal of Cyber Security and Mobility, Vol. 9-4, Pages 515–534, 2021. https://doi.org/10.13052/jcsm2245-1439.942

[5] Bejoy, B.J., Raju, G., Swain, D., Acharya, B., and Hu, Y., "A generic cyber immune framework for anomaly detection using artificial immune systems", Applied Soft Computing, Volume 130, 2022. https://doi.org/10.1016/j.asoc.2022.109680

[6] Belhadj, N., Guerroumi, M. & Derhab, A., "NSNAD: negative selection-based network anomaly detection approach with relevant feature subset." Neural Comput & Applic 32, pp. 3475–3501, 2020. https://doi.org/10.1007/s00521-019-04396-2

[7] Chanal, P. M., Kakkasageri, M. S., and Manvi, S. K. S., Chapter 7 - Security and privacy in the internet of things: computational intelligent techniques-based approaches, Editor(s): Siddhartha Bhattacharyya, Paramartha Dutta, Debabrata Samanta, Anirban Mukherjee, Indrajit Pan, Recent Trends in Computational Intelligence Enabled Research, Academic Press, Pages 111-127, 2021, ISBN 9780128228449, https://doi.org/10.1016/B978-0-12-822844-9.00009-8.

[8] Dominik, W., Goeschka, K. M. and Kastner, W., "A Review on Immune-Inspired Node Fault Detection in Wireless Sensor Networks with a Focus on the Danger Theory" *Sensors* 23, no. 3: 1166, 2023. https://doi.org/10.3390/s23031166

[9] Duru, C., Ladeji–Osias, J., Wandji, K., Otily T., and Kone, R., "A Review of Human Immune Inspired Algorithms for Intrusion Detection Systems," IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 2022, pp. 364-371, 2022. doi: 10.1109/AIIoT54504.2022.9817213.

[10] Fu J., Yang H., Liang Y., Tan C., "Bait a Trap: Introducing Natural Killer Cells to Artificial Immune System for Spyware Detection." In: Coello C.A., Greensmith J., Krasnogor N., Liò P., Nicosia G., Pavone M. (eds) Artificial Immune Systems. ICARIS 2012. Lecture Notes in Computer Science, vol 7597. 2012, Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-33757-4_10

[11] Garcı´a-Teodoro, P., Dı´az-Verdejo, J., Macia´-Ferna´ndez, G., and Va´zquez, E., "Anomaly-based network intrusion detection: Techniques, systems and challenges, computers & security 28 (2009) pp. 18–28, 2009.

[12] Hart, E. and Timmis, J., "Application areas of AIS: The past, the present, and the future", Applied Soft Computing, 8 (2008): pp. 191–201, 2008.

[13] Hoppe, T., Kiltz, S., and Dittmann, J., "Applying intrusion detection to automotive IT-early insights and remaining challenges". Journal of Information Assurance and Security (JIAS). 4. 226-235, 2009.

[14] Iqbal, I., "A Systematic Literature Review Of Unknown Virus Detection And Artificial Immune System (AIS)", International Journal of Scientific and Technology Research, Volume 9, Issue 01, Pages 3875-3878, 2020.

[15] Nanda, S. J., "Artificial Immune Systems: Principle, Algorithms and Applications", A THESIS OF Master of Technology (Research) In Electronics and Communication Engineering, 2017.

[16] Ou, Chung-Ming, "Host-based intrusion detection systems adapted from agent-based artificial immune systems", Neurocomputing, Volume 88, 1 July 2012: 78–86, 2012.

[17] Rashid N, Iqbal J, Mahmood F, Abid A, Khan US and Tiwana MI, "Artificial Immune System–Negative Selection Classification Algorithm (NSCA) for Four Class Electroencephalogram (EEG) Signals". Front. Hum. Neurosci. 12:439, 2018. doi: 10.3389/fnhum.2018.00439

[18] Read, M., Andrews, P.S., Timmis, J., "An Introduction to Artificial Immune Systems.", In Rozenberg G., Bäck T., Kok J.N. (eds) Handbook of Natural Computing. Springer, Berlin, Heidelberg, 2012. https://doi.org/10.1007/978-3-540-92910-9_47

[19] Rimiru, R. M., Guanzheng, T. and Njuki, S. N., "Towards Automated Intrusion Response: A PAMP - Based Approach", International Journal of Artificial Intelligence and Expert Systems (IJAE), Volume 2, Issue 2: 23-35, 2011.

[20] Pradeu, Thomas, and Vitanza, E., 'Immunology, Self and Nonself', in Elizabeth Vitanza (ed.), *The Limits of the Self: Immunology and Biological Identity* (2012; online edn, Oxford Academic, 24 May 2012), https://doi.org/10.1093/acprof:oso/9780199775286.003.0002, accessed 19 Aug. 2023.

[21] Said, W. and Mostafa, A. M., "Towards a Hybrid Immune Algorithm Based on Danger Theory for Database Security", IEEE Access, Volume 8, August 19, 2020. https://doi.org/10.1109/ACCESS.2020.3015399

[22] Sobh, T.S., Mostafa, W.M., "A cooperative immunological approach for detecting network anomaly." Applied Soft Computing, Vol. 11, Issue 1, Pages 1275-1283, 2011. https://doi.org/10.1016/j.asoc.2010.03.004

[23] Sobh, T.S.,"Wi-Fi Networks Security and Accessing Control", International Journal of Computer Network and Information Security, Vol. 5, Issue 7, Pages 9-20, 2013. DOI: 10.5815/ijcnis.2013.07.02

[24] Tavallaee, M., Bagheri, E., Lu, W. and Ghorbani, A., "A Detailed Analysis of the KDD CUP 99 Data Set, Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), 2009.

[25] UNM - University of New Mexico's, Computer Systems Project, Oct. 24, (2008); http://www.cs.unm.edu/immsec/systemcalls.htm

[26] Vella, M., Roper, M., Terzis, S., "Danger Theory and Intrusion Detection: Possibilities and Limitations of the Analogy". In: Hart, E., McEwan, C., Timmis, J., Hone, A. (eds) Artificial Immune Systems. ICARIS 2010. Lecture Notes in Computer Science, Vol 6209, 2010. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-14547-6_22

[27] Wu, S. X., and Banzhaf, W., "The use of computational intelligence in intrusion detection systems: A review", Applied Soft Computing, 10 (2010), pp. 1–35, 2010.

[28] Xu, Xin, "Sequential anomaly detection based on temporal-difference learning: Principles, models and case studies", Applied Soft Computing, 10 (2010): pp. 859–867, 2010.

[29] Yang, H., Li, T., Hu, X., Wang, F., and Zou, Y., "A Survey of Artificial Immune System Based Intrusion Detection", The Scientific World Journal, Volume 2014, Article ID 156790, 2014. https://doi.org/10.1155/2014/156790

[30] Zhou, W., Zhang, K., Ming, Z., Chen, J., Liang, Y., "Immune optimization inspired artificial natural killer cell earthquake prediction method". J Supercomput 78, 19478–19500, 2022. https://doi.org/10.1007/s11227-022-04618-w

[31] Zou, M., Liu, W., Gao, F., Bai, X., Chen, H., Zeng, X., and Zhang X., "Artificial Natural Killer Cells for Specific Tumor Inhibition and Renegade Macrophage Re-Education", Adv. Mater. 2019, 31, 1904495, DOI:10.1002/adma.201904495
[32] Zhang, H., Ren, Z., Xin, S., Liu, S., Lan, C., and Sun, X., "A scale-adaptive positive selection algorithm based on B-cell immune mechanisms for anomaly detection", Engineering Applications of Artificial Intelligence, Volume 94, 2020, 103805, https://doi.org/10.1016/j.engappai.2020.103805.

Author Bibliography

Tarek Salah Sobh earned his B.Sc. in computer engineering from Military Technical College, Cairo, Egypt in 1987. He also obtained M.Sc. and Ph.D. degrees from the Computer and System Engineering Department, Faculty of Engineering, Al-Azhar University, Cairo, Egypt. Sobh has experience in managing, designing, and developing packages for business applications and security systems. He has authored/co-authored numerous refereed journal/conference papers and booklets, with some articles available in the ScienceDirect Top 25 hottest articles. His research interests include computer networks, security systems, distributed systems, knowledge discovery, data mining, and software engineering.