IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 23, 2020, accepted August 5, 2020, date of publication August 10, 2020, date of current version August 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3015399

Towards a Hybrid Immune Algorithm Based on Danger Theory for Database Security

WAEL SAID[1,2], (Member, IEEE), AND AYMAN MOHAMED MOSTAFA[1,3], (Member, IEEE)
[1]Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Egypt
[2]College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia
[3]College of Computer and Information Sciences, Jouf University, Sakaka 72314, Saudi Arabia

Corresponding author: Ayman Mohamed Mostafa (amhassane@ju.edu.sa)

ABSTRACT In Databases, the most prevalent cause of data breaches comes from insiders who misuse their account privileges. Due to the difficulty of discovering such breaches, an adaptive, accurate, and proactive database security strategy is required. Intrusion detection systems are utilized to detect, as fast as possible, user's account privilege misuse when a prevention mechanism has failed to address such breaches. In order to address the foremost deficiencies of intrusion detection systems, artificial immune systems are used to tackle these defects. The dynamic and more complex nature of cybersecurity, as well as the high false positive rate and high false negative percentage in current intrusion detection systems, are examples of such deficiency. In this paper, we propose an adaptable efficient database intrusion detection algorithm based on a combination of the Danger Theory model and the Negative Selection algorithm from artificial immune system mechanisms. Experimental results for the implementation of the proposed algorithm provide a self-learning mechanism for achieving high detection coverage with a low false positive rate by using the signature of previously detected intrusions as detectors for the future detection process. The proposed algorithm can enhance detecting insider threats and eliminate data breaches by protecting confidentiality, ensuring integrity, and maintaining availability. To give an integrated picture, a comprehensive and informative survey for the different research directions that are related to the proposed algorithm is performed.

INDEX TERMS Danger theory model, artificial immune system, negative selection algorithm, database intrusion detection system.

I. INTRODUCTION

Artificial Immune System (AIS) is a subfield of computational intelligence derived from the Biological Immune System (BIS) to solve some certain problems. AIS is also considered as a rule-based machine learning approach [1], a bio-inspired computing technique [2], a natural computation paradigm [3], and a theoretical immunology model [4]. In the literature, AIS could be known in different contexts as immune-inspired system [5], Immuno-inspired system [6], immunological computation [7], [8], immune computation [9], Immuno-computing [10], or digital immune system [11]. In commercial and industrial communities AIS could be named as cyber-immunity or digital immunity [12], [13]. AIS has represented some of the features, principles, and mechanisms of BIS in forms of models and algorithms to be applied in different application domains [14], [15]. These models and algorithms [16] include the Negative Selection Algorithm (NSA), Positive Selection Algorithm (PSA), Clonal Selection Algorithm (CSA), Danger Theory (DT) model, Dendritic Cell Algorithm (DCA), Toll-like Receptor (TLR) Algorithm, Artificial Immune Network Algorithm (aiNet), Immune Concentration Algorithm [17], [18], Tunable Activation Threshold (TAT) Theory [19], and Artificial Immune Recognition System (ARIS). In BIS, there are more theories that have not been represented and utilized in AIS such as disease tolerance mechanisms [20], the discontinuity theory of immunity [21], [22], Sensory immune system theory [23], and multi-pronged theory [24]. Regardless of the considerable interpretations and theories that are trying to understand BIS and its distinctive characteristics, AIS has been used in enormous applications in various fields [25]–[27]. In the field of computer security, AIS provides a significant role in creating dynamic, automated, memorization, and adaptive defense tools to obtain effective outcomes [28]. One of such tools is

The associate editor coordinating the review of this manuscript and approving it for publication was Sudhakar Babu Thanikanti.

the Intrusion Detection System (IDS), whose key challenge is the capability to recognize what is normal and what is malicious [29]–[31]. According to the analogy between IDS major challenge and BIS objective, AIS models and algorithms are used to provide unconventional solutions in various detection systems such as anomaly detection, fraud detection, malicious process detection, scan and flood detection, and intrusion detection as well.

IDSs are classified into different categories based on several criteria [32]–[35]. According to the placement where detection takes place, IDSs could be used for securing networks, hosts, and applications. The Network-based IDS (NIDS) is applied to different types of networks and is utilized to monitor and investigate network traffic. The Host-based IDS (HIDS) is used to keep track of the activities on a certain machine. The Application-based IDS (AppIDS) [36] is used to keep an eye on the user-application interaction by analyzing the application log file to detect malicious user behavior such as those who bypass the security authorization rules. The database IDS (DIDS) [37], [37]–[39] and Web application IDS (WAIDS) [40] are two examples of AppIDS.

The AIS-IDS is categorized as a subclass of the anomaly detection technique [41]. According to [2], AIS-IDSs could be applied by using two main mechanisms. The first mechanism is the usage of NSA, which is inspired by the acquired, adaptive, and immune system to distinguish between self and non-self. The DT is applied as the second mechanism to activate the innate immune system along with the adaptive immune system when cell damage has occurred. The TLR algorithm and DCA are used under the second mechanism as they are inspired by the DT [42]. By using one of these mechanisms or combining some of them, integrity, privacy, availability, and/or authenticity could be maintained [43].

The DT explores the BIS response to the presence of molecules known as danger signals that are released as a result of the attacks. The immune system will be activated only when damage or an attack occurred and will be suppressed otherwise. The DT is based on the assumption that antigen-presenting cells (APCs) contain danger signal receptors for recognizing signals sent out by damaged cells. These signals stimulate the immune systems to initiate responses. Based on the DT, any cell that is under attack sends out a danger signal to generate a danger zone around itself.

The epidemic Coronavirus (COVID-19) is considered as an example of the most dangerous intrusions on the Human Immune System (HIS), as a special case of BIS. During the writing of this research paper, more than five hundred and ninety thousand persons had died with more than fourteen million were infected with the virus. The mechanism of the virus is based on attacking the normal cells. Once the human cells are attacked, an alarm is raised to apply a danger zone. The memory cells guarantee that if the body encounters the same virus again, it will be able to interact immediately, according to pre-existing defensive strategies.

Unfortunately, the signature of COVID-19 is unknown to HIS and there are no pre-defined antivirals for it, which means that the number of infected people is increasing very quickly. The best method for dealing with this problem is to scan the virus by using a new learning mechanism to build a protective memory.

In this paper, a DT-based Database Intrusion System (DT-DIDS) is proposed for identifying abnormal insider user behaviors to prevent and mitigate data breach. It consists of a multilayered preprocessing mechanism and a DT-based Intrusion Detection (DT-ID) algorithm that is based on the combination of R-contiguous bit matching parameter and the danger value parameters. The DT-DIDS can address some challenges and obstacles for traditional database intrusion detections. These challenges include the ability to determine a strong discriminatory measurement for identifying intruders with a low false alarm rate, the ability to manage various alarms and determine the appropriate alarm threshold level, the ability to self- learning from the False Positive (FP) and False Negative (FN) alarms for improving the efficiency by searching the antigen log which is considered to be the memory of previously detected intrusions, and the ability to detect and prevent insider intrusions in real-time. It also tackles another important challenge for IDSs with immunity features. This challenge is the ability to use a minimum number of detectors to reduce space complexity. The proposed intrusion detection algorithm deals with this issue by applying a danger signal alarm around each user privilege that is assigned by the Trusted Third Party (TTP). Each signal creates a danger zone around itself that will be activated if the user violates her/his predefined privileges. The contribution of this paper is as follows:

- Proposing a DT-DIDS for protecting the secrecy and integrity of data.
- Presenting a set of security parameters applied by a TTP for determining the systems' immunity degree and user privileges.
- Designing and implementing an intrusion detection algorithm for detecting a database of abnormal user behavior.
- Improving Detection Rate (DR) with low FP and low FN alarms based on the proposed intrusion detection algorithm.
- Providing a comprehensive survey of the different cross-cutting research trends that help in understanding the proposed algorithm in an integrated way.

The remainder of this paper can be navigated in the following way: Section II explains the recent related work in the field of data breach in databases, database intrusion detection, immune inspired intrusion detection, immune inspired database intrusion detection, NSA-based intrusion detection, and DT-based intrusion detection. Section III presents the proposed immune-based DIDS and the overall process of granting privileges using the NSA. Section IV shows different enhancements in the NSA. Section V explores the

TABLE 1. Summary of major acronyms.

Acronym	Definition	Acronym	Definition
ABC	Artificial Bee Colony	IAS	Immune Analysis System
aiNet	Artificial Immune Network Algorithm	IDS(s)	Intrusion Detection System(s)
AIS	Artificial Immune System	IoT	Internet of Things
AIS-IDS	Artificial Immune System -based Intrusion Detection System	KNN	K-Nearest Neighbor
APCs	antigen-presenting cells	MANETs	Mobile Ad-hoc Networks
App IDS	Application based IDS	MINID	Multi-layered Immune Network Intrusion Detection
ARIS	Artificial Immune Recognition System	NIDS	Network-based Intrusion Detection System
ART	Adaptive Resonance Theory	NK	Natural Killer
BIS	Biological Immune System	NRI	Negative Representation of Information
CSA	Clonal Selection Algorithm	NSA	Negative Selection Algorithm
CR	Correctness Rate	OPTICS	Ordering Points To Identify The Clustering Structure
DBIDS	Database Intrusion Detection System	PAMP	Pathogen-Associated Molecular Pattern
DCA	Dendritic Cell Algorithm	P_S	System Privilege
DCSA	Dynamic Clonal Selection Algorithm	P_d	Database Privilege
DDoS	Distributed Denial-of-Service	PRR	Pattern Recognition Receptors
DIDS	Database Intrusion Detection System	PSA	Positive Selection Algorithm
DoS	Denial-of-Service	RBFN	Radial Basis Functional Neural Network
DR	Detection Rate	RCB	R-Contiguous Bit
DT	Danger Theory	RTOPS	Real-time Online Processing System
D_{TC}	Detector	SDS	Synthetic Dataset
DT-DIDS	Danger Theory-based Database Intrusion Detection System	SOM	Self-Organizing Map
DT-ID	Danger Theory-based Intrusion Detection	SVD	Singular Value Decomposition
DV	Danger Value	SVM	Support Vector Machines
DZV	Danger Zone Value	TAT	Tunable Activation Threshold
FDD	Fault Detection and Diagnoses	TLR	Toll-like Receptor
FIN	Formal Immune Network	TTP	Trusted Third Party
FP	False Positive	UF	User Factor
FN	False Negative	VANETs	Vehicular Ad-hoc Networks
GA	Genetic Algorithm	VMs	Virtual Machines
HIDS	Host-based Intrusion Detection System	WAIDS	Web application Intrusion Detection System
HIS	Human Immune System	WSNs	Wireless Sensor Networks

experimental results of the proposed algorithm. Finally, the paper concludes with future work spotlights in Section VI. The definitions of the major used acronyms in this paper are presented in Table 1.

II. RELATED WORKS

In this section, a comprehensive, informative survey for the different research directions that are related to the proposed DT-DIDS is performed. The main objective of a DIDS in an organization is to prevent or mitigate the data breach effects. In Section A, we shed light on the problem of data breach in databases and its impact on the reputation of organizations. Besides, we provide some known data breach in the last five years. In Section B, we survey the field of database intrusion detection. The immune inspired IDSs are discussed in Section C. We study the database intrusion detection with immunity features in Section D. In Section E, we review and discuss the applicability, possibility, and capability of using the NSA in IDSs. The DT-based IDSs in different environments are discussed in Section F.

A. BREACHES IN DATABASES

Confidential and sensitive data is the cornerstone and the pole of the tent for organizations and individuals. Data breach is the ability to gain unauthorized access to such data in an information system with the aim of compromising the information security measures; confidentiality, integrity, and availability [44]. According to the cause of the occurrence, the data breach is classified as intentional and unintentional. Whereas by location, it is divided into physical and logical. The impact of data breach is categorized as confidentiality data breach, integrity data breach, and availability data breach [45]. At a corporate level, significant financial losses and bad reputation are the most important implications of a data breach [46], [47]. Table 2 represents the biggest data breaches in some companies and website database from 2016 to 2020 [48]–[50]. One of the most important reasons for the biggest data breach is the insiders' privilege of account misuse. The other insiders' causes of data breach incidents might include authorization abuse, weak authentication, and information misuse [51]. The privilege account

TABLE 2. Data breach samples from 2016 to 2020 [48]–[50].

Company Name	Month and Year	Data Impact
Sina Weibo	March 2020	538 million accounts
Zynga	September 2019	218 million user accounts
Canva	May 2019	137 million user accounts
First American Financial Corp.	May 2019	885 million users records
Verifications.io	February 2019	763 million users accounts
Dubsmash	December 2018	162 million user accounts
Black Media Games	December 2018	7.6 million user accounts
Quora	November 2018	100 million user accounts
Apollo	July 2018	126 million users records
Exactis	June 2018	340 million user records
MyHeritage	June 2018	92 million user records
Twitter	May 2018	330 million users accounts
Ticket Fly	May 2018	27 million user records
FaceBook	April 2018	97 million user accounts
Panera	April 2018	37 million user records
Heartland Payment Systems	March 2008	134 million credit cards exposed
Aadhar (Indian government)	March 2018	1.5 billion Indian citizens
Cathay Pacific	March 2018	9.4 million user accounts
My Fitness Pal (Under Armour)	February 2018	150 million user accounts
Yahoo	October 2017	3 billion user accounts
Equifax	July 2017	147.9 million consumers
Uber	November 2016	57 million user accounts
Youku	December 2016	92 million users accounts
Dailymotion	October 2016	85 million users accounts
Adult Friend Finder	October 2016	412.2 million accounts
MySpace	May 2016	360 million user accounts

misuse is composed of excessive and inappropriate privilege abuse, legitimate privilege abuse, and unauthorized privilege promotion [52].

The inevitable consequence of data breach incidents is to secure confidential and sensitive data. Proactive and reactive data security is the two main approaches for securing data. In the proactive approach, threats are prevented before they occur. In the reactive approach, a security breach could be detected after it has occurred. In Database Systems, the proactive and reactive approaches are used at different security layers to prevent and detect data breach.

As shown in [53], various mechanisms are presented to explore the state of the art techniques for securing database with proposing new trends. The presented mechanisms

include cryptography, access control, database watermarking, and database auditing. These countermeasures are applied to prevent insider and outsider attackers from compromising system resources. As presented in [54], [55], interactive policies are applied to secure databases based on multi-layer mechanisms. The proposed layers are implemented based on the concept of separation of duty. Each layer has a function to secure part of system resources and finally, all layers are embedded into a central mechanism for securing the overall system. As presented in [56], different security mechanisms are designed and implemented using service-oriented algorithms to secure and monitor all database transmissions between the server-side and client-side. Any request sent from the user or administrator must be monitored under a two-way communication pattern for securing both sides using a secret sharing algorithm. The TTP applies the secret-sharing mechanism by providing the minimum number allowed to grant or reject the transmission request. If the database administrator sends a request to the server-side, a counter mechanism will be created to count the number of grants and finally accept or reject the request.

In Database systems, there is often a tendency to rely on detective controls rather than preventive measures. The DIDS is used to detect malicious activities by reducing data breaches caused by privileged account users. In this paper, we present a DIDS that protect the database from insider threats and eliminate data breaches by protecting confidentiality, ensuring integrity, and maintaining availability. Moreover, the proposed system helps to overcome the problem of a bad reputation.

B. DATABASE INTRUSION DETECTION

The problem of identifying malicious database transactions and the problem of securing databases from insider threats are non-trivial problems that cannot be ignored. The DIDSs, or DBIDS as in [57], are used to identify any intruder; either insider or outsider; in a database system by monitoring the activities across database transactions. Whenever any abnormal activity is identified, the DIDS sends signals to the database administrators warning of a potential intruder. A recent comprehensive, systematic survey up to the year 2017 on database intrusion detection is presented in [58].

Instead of reinventing the wheel in surveying various researches related to DIDS, we rely on this updated survey. We suffice here only to complete the survey from 2018 to June 2020, as well as to indicate the areas that this research paper has not been exposed to.

By following the same approach that is described in [58], we use the five keywords for the suggested general and specific search techniques. With a focus on the titles that contain the keywords ''Database, Intrusion, Detection'' among journals, conferences, and book chapters. We obtain 26 different research papers that are published in the period from the year 2018 till June 2020. Table 3 represents the author(s), year of publication, and title for these 26 research papers.

The DIDSs confront many challenges [58], [37]. There are mainly three most important challenges. The first one is the ability to manage various alarms and determine the appropriate alarm threshold level. On the one hand, many intrusions might not be detected according to the high threshold level determination; known as FP alarms. On the other hand, a low threshold level might produce a very large number of alarms, most of which are likely to be false which is known as FN alarms. Incorrect determination of the threshold level causes the DIDS to lose its relevance, reliability, credibility, and uselessness. The second main challenge is the ability to self-learning from the FP and FN results for improving efficiency. The third challenge is the ability to detect, react, and prevent intrusions in real-time.

In this paper, we present a DT-DIDS that has high DR of insider threats with low FP and low FN alarms. This is due to the use of danger value, danger zone, immune memory, and affinity maturation inspired by DT and NSA from the BIS. The presented DT-DIDS has the ability to detect and prevent insider users who abuse their account privileges.

C. IMMUNE INSPIRED INTRUSION DETECTION

The BIS is a complex and pervasive set of defensive responses that maintain a balanced state and help repel invaders with sufficient tolerance to avoid allergies and autoimmune diseases. The method to stimulate the immune response is the most challenging question for immunologists. Therefore, some theories are proposed to describe, explain, and predict the immune response and immune tolerance. In the digital world, the AIS is the equivalent terminology of BIS for solving non-biological problems. The AISs contain algorithms and models inspired by the theories of BIS.

The AISs have been utilized in enormous applications in various fields, including Data Analysis, Fault Diagnosis, Optimization, Control, Image Processing, Robotics, and Computer Security [2], [26], [27]. AIS-based applications in the computer security field include computer virus detection, malware detection, spyware detection, anomaly detection, fraud detection, malicious process detection, scan and flood detection, and intrusion detection as well [28].

Numerous algorithms, principles, functions, and models of AIS have been positively used as an IDS in various environments. In [83], a dynamic real-time network anomaly detection algorithm based on the PAS is proposed. In [18], an intrusion detection method is proposed based on the Immune Concentration Algorithm which depends on the changes of antibody concentration in an immune response. A virus detection approach is introduced based on Immune Concentration Algorithm in [84]. The authors of [85] formulate a multi-layered immune network intrusion detection defense model (MINID) as a pattern recognition task based on the theory of Pattern Recognition Receptors (PRR).

The CSA is applied to the process of modeling normal behavior of network traffic data in NIDS [86]. Inspired by the CSA and avidity model, the authors of [87] present a NIDS

TABLE 3. Database intrusion detection systems publications from 2018 to June 2020.

Author(s)	Year	Title
Khan et al. [59]	2018	A Semantic Approach to Frequency Based Anomaly Detection of Insider Access in Database Management Systems
Solanki and Phutane [60]	2018	An Innovative Recipe for Intrusion Detection In Relational Databases using Mean-Shift Clustering and C 4.5 Algorithm
Ramachandran et al. [61]	2018	Anomaly Detection in Role Administered Relational Databases — A Novel Method
Seo and Cho [62]	2018	Applying Accuracy-Based LCS to Detecting Anomalous Database Access
Jayaprakash and Kandasamy [63]	2018	Database Intrusion Detection System using Octraplet and Machine Learning
Hagen et al. [64]	2018	Efficient and Effective Ransomware Detection in Databases
Mostafa et al. [65]	2018	False Alarm Reduction Scheme for Database Intrusion Detection System
Wankar [66]	2018	Implementation of Log Mining and Forensic Analysis for Database Intrusion Detection and Protection System
Khan et al. [67]	2018	Towards Modeling Insiders Behavior as Rare Behavior to Detect Malicious RDBMS Access
Brahma et al. [68]	2019	A Hybrid Database Intrusion Detection Algorithm using Swarm Intelligence and Radial Basis Function Network
Subudhi and Panigrahi [69]	2019	Application of OPTICS and Ensemble Learning for Database Intrusion Detection
Subudhi [70]	2019	Application Specific Database Intrusion Detection using Data Mining Techniques
Sani Bala [57]	2019	Cloud Computing and Database Security
Kim and Cho [71]	2019	CNN-LSTM Neural Networks for Anomalous Database Intrusion Detection in RBAC-Administered Model
C.Bakir et al. [72]	2019	Comparisons on Intrusion Detection and Prevention Systems in Distributed Databases
Le et al. [73]	2019	Customized Intrusion Detection based on A Database Audit Log
Hasan et al. [74]	2019	Detection of SQL Injection Attacks: A Machine Learning Approach
Bu and Cho [75]	2019	Genetic Algorithm-Based Deep Learning Ensemble for Detecting Database Intrusion via Insider Attack
Bu and Cho [76]	2019	A Convolutional Neural-based Learning Classifier System for Detecting Database Intrusion via Insider Attack
Iffländer et al. [77]	2019	Hands off My Database: Ransomware Detection in Databases Through Dynamic Analysis of Query Sequences
Yanyan Zhou [78]	2019	Intrusion Detection Method of Marine Ecological Database under Weak Association Rules
Sallam and Bertino [79]	2019	Techniques and Systems for Anomaly Detection in Database Systems
Srivastava et al. [80]	2019	Verity: Block chains to Detect Insider Attacks in DBMS
Brahma and Panigrahi [51]	2020	Database Intrusion Detection using Adaptive Resonance Network Theory Model
Sahu and Panigrahi [81]	2020	Application of Deep Learning for Database Intrusion Detection
Brahma and Panigrahi [82]	2020	Role of Soft Outlier Analysis in Database Intrusion Detection

for overcoming scalability and coverage. In [88], an improved CSA is used to detect intrusion behavior by identifying and cloning the best individual overall. Three improvements to the dynamic CSA (DCSA) are conducted in [89] that are used in distributed NIDS. The three improvements belong to the detection rules of any known intrusions, the memory detectors' lifetime, and the synergistic signal mechanism. The CSA and the NSA, are surveyed and evaluated based on the

NSL-KDD dataset with various sets of features and variant numbers of detectors [90].

In BIS, the DCA is inspired by the dendritic cell differentiation theory of the congenital immune mechanism. In AIS, the DCA is used widely in the intrusion detection field. This is due to the nature of the dendritic cells which are considered as the intrusion detection agents of the human body [91]. The reasons why DCA is being the appropriate candidate for intrusion detection problems are explained in [92]. In the literature, extensive research articles are presented. Some of these articles include [93]–[102].

In the literature, the IDS could be treated as a learning system that is able to classify system activities and user behaviors either as normal or intrusive. On the other hand, feature reduction could be applied to increase the efficiency and effectiveness of real-world detection systems. In this context, the authors of [103], [104] use Rough Set theory to reduce the dimension of the features of network traffic as well as applying the (aiNet) to cluster the reduced features. The authors argue that the unsupervised anomaly detection approach using immune network clustering is robust in identifying novel attacks in the absence of labels. In [105], the aiNet is used to compress and cluster RFID operation antigen log data and generated collaborative detectors in the proposed RFID intrusion detection method. In [105], the use of an artificial immune network to generate detection rules is proposed in the DWIDS intrusion detection system. The authors of [106] utilize the aiNet to cluster the common features of normal data in the proposed IAIIDS intrusion detection system.

Antunes *et al.* published a series of research papers that describe and utilize the TAT immunological hypothesis on the development of a temporal anomaly detection algorithm. In [107], a temporal anomaly detection architecture and algorithm based on the TAT is presented. Antunes and Correia develop a NIDS architecture based on TAT hypothesis, for temporal anomaly detection, in [108]. In [109], [110], an improved generic anomaly detection system based on the TAT theory along with two immunological concepts are presented. These two concepts are cell clonal size regulation mechanisms and a dynamic equilibrium based on the sharing of finite resources mechanism. In [111], they demonstrate the ability to use the TAT theory in developing and deploying adaptive behavior-based NIDS using the temporal adaptation of the immune T-cells activation thresholds. In [112], a hybrid approach for text classification based on TAT theory inspiration and the support vector machines (SVM) approach is analyzed. In [19], Antunes and Correia present a description for a generic TAT-AIS based anomaly detection framework. This framework is based on a simplified version of the TAT model to detect new patterns and also to distinguish them from unseen ''normal'' and ''abnormal'' behaviors.

In [113], Bejoy and Janakiraman design a Natural Killer (NK) cell-based network intrusion detection and prevention system inspired by the NK immune cells in the human body. The idea of inspiration of NK cell is firstly introduced in [114] to develop a NK cell-based HIDS for spyware detection.

A NIDS approach using Immuno-Computing model is represented and discussed in [10], [115], and [116]. The main model of the proposed approach is to apply a mathematical model of the Formal Immune Network (FIN) with apoptosis and immunization controlled by cytokines where the FIN inspired by network theory of the immune system.

In this paper, we present AIS-based IDS for database security inspired by combining the DT and the NSA. The presented AIS-based IDS proposed a self-learning mechanism by constructing the antigen log which is considered as the memory of previously identified intrusions. The novelty of the proposed mechanism is based on detecting a large number of intrusions with a low number of detectors.

D. IMMUNE INSPIRED DATABASE INTRUSION DETECTION

As presented in Section C, most researchers apply IDSs and algorithms based on the inspiration of BIS mechanisms for hosts and networks in various environments. Very limited research papers utilize the AIS algorithms and models to detect malicious activities for database systems. In this section, we survey the immune-based DIDS.

In [117], an immunity-based intrusion detection and recovery system for a relational database system is suggested to identify malicious transactions. The proposed system simulates the concepts antibody, immunocytes, matures immunocytes, immature immunocytes, memory immunocytes, symptoms, and adaptively from the BIS. It consists of two main layers and each layer contains some functional components. The two layers are: RTOPS layer and IAS layer. The RTOPS is responsible for detecting malicious transactions and recovering the effects of the intrusion in case it is not detected. The treatment system component of the RTOPS is responsible for the evaluation of the severity and the extent of damage caused by malicious transactions as well as the execution of transactions cleaning procedures to take care of the damaged parts of the database. The IAS layer has the ability to produce and manage immunocytes, antibodies, and symptoms. The matching process between the mature immunocytes and the suspicious transaction is done by using the CSA. Accordingly, the suspicious transaction is stored as a symptom in the Symptom DB component of the IAS layer.

In [118], an immune-based database intrusion detection model is proposed. The immune cells in BIS are inspired as immune detectors which encode the self-set. The binary encoded approach is used with a length of 8 bits. These 8 bits encode the different user, the four database operations (select, insert, delete, and update), and the number of operations for each user as intervals categories. The enumeration of all candidate detectors is generated rather than random generation. Mature detectors are selected based on the negative selection mechanism in the BIS.

The authors of [119] introduce an intruder recognition algorithm based on the inspiration of the DT. The basic idea of

the introduced algorithm is to use two danger signals to secure a relational database system. Three danger-based parameters are proposed to detect and prevent authorized users such as database administrators and privileged users to breach the database system. The first parameter provides the amount of sensitivity to the whole security system. The second one provides the top margin for each user to execute system different database operations such as select, insert, update, and delete. The third parameter provides database privilege that may be granted to users. Moreover, an R-Contiguous Bit (RCB) matching parameter is used as an inspiration from the negative selection mechanism in BIS to distinguish between legitimate and malicious users based on the R-value. In the context of the introduced algorithm, the properties achieved by inspiring the immune system are explained.

In [120] a danger signal inflammation algorithm is developed for securing a database system. The results are based on using only the R-value inspired of the NSA to detect unknown database intrusions. The main objective of the research paper is to apply a set of predefined roles based on a secret sharing mechanism with different immune features. Then the DR is determined using the R-value with limited dataset size.

Indeed, we complement the work presented in [119]. However, three danger signals are used instead of two. These three signals are alarmed in case of the failure of intruder recognition process, intruder detection process, and certificate confirmation mechanism. Therefore, how relevant are these values in securing databases for different settings, is the question that arises.

The authors of [121] introduce an integrated solution for securing databases based on three sequential processes of security. The first process is presented in [120] to detect and prevent malicious intruders using the inspiration of the negative selection mechanism and DT model. The second process is an immunity-based error containment algorithm for post-security. This algorithm is based on the inspiration of Apoptotic and Necrotic immune mechanisms to discover malicious users from executing transactions if they already compromise detection and prevention algorithms. The authors introduce and define Apoptotic signal and Necrotic signal. The Apoptotic signal is low-level alarms that could be alarmed when a legitimate user tries to exceed his/her allowed number of transactions. The Necrotic signal identifies the high-level alarms that are issued when an actual successful attack is achieved. The third process is the system hibernation framework used to audit user transactions to determine whether to grant or deny it.

In this paper, we propose a DIDS inspired by combining two immune mechanisms; namely, the DT and the NSA. As far as we know, this the first use of the combination of these two mechanisms in the context of database intrusion detection. In the literature, the combination of DT and NSA for Mobile Ad-hoc Networks (MANETs) security is presented in [122]. The authors of [123] study the applicability, restrictions, and limitations of using NSA and DT to detect anomalies in heterogeneous networks. The authors of [124], discuss the creation of the Internet of Things (IoT) intrusion detection based on DT and NSA.

E. NSA-BASED INTRUSION DETECTION

The NSA is inspired by the ability of an immune system to get rid of self-reactive cells. In contrast, the PSA is based on the capability of an immune system to recognize self-cells. Therefore, the non-self-cells are considered as intruders. The NSA is essentially designed to be used in anomaly detection, intrusion detection, change detection, similar pattern recognition, and two-class classification problems. Because of its simplicity and ease of implementation, over time NSA has been successfully used in a wide range of application domains.

Table 4, represents our survey of various application domains that utilize the NSA either alone or in conjunction with other AIS algorithms.

In the literature, various improved versions of NSA are developed to tackle the drawbacks of the classical NSA that is presented by Forrest *et al.* [125]. The variations of these improvements depend on one or more of some factors. These factors include self-definition, data representation scheme, detector representation, detector generation mechanism, detector elimination mechanism, matching rule, as well as the combination of NSA with other different strategies [126]–[128]. In [129], Ramdane and Chikhi introduce a recent survey for NSA-based intrusion detection systems up to the year 2016.

The authors also present a classification of NSA, which includes Binary NSA and Real NSA. The Real NSA is classified into Constant-sized detectors and Variable-sized detectors. The most 20 improvements of the NSA until 2106 are presented with the demonstration of the drawbacks of the classical NSA. For completeness, we follow the same approach in [129] to survey and summarize other NSA improvements in different domain areas up to 2020.

We present Table 5 that include three columns, Author(s) and year, acronym, and testing datasets. The acronyms are used as in Table 1.

The suitability of NSA for network-based intrusion detection applications is a controversial issue. In [156], Kim and Bentley evaluate the NSA for network intrusion detection. They conclude that it is futile to use NSA for network intrusion detection. This is due to the impractical time computation for generating a sufficient number of detectors. Kim and Bentley suggest that the most suitable use of NSA is to be a filter for invalid detectors, rather than to be a generator detector. The author of [157] concludes that NSA is inappropriate and cannot be applied to real-world anomaly detection, network intrusion detection problems, and classification problems.

On the contrary, the authors of [158] present a survey for the applicability of a negative selection approach in NIDSs. They conclude that the NSA is the most compatible with the anomaly detection approach. The authors also come up with some notes which include the importance of

TABLE 4. The NSA-based various application domains.

Author and year	AIS algorithm	Application Domain
Farzadnia et al. (2020) [130]	NSA + DCA	Anomaly Detection
KARATAS¸ (2019) [131]	NSA	Anomaly Detection
Igawa and Ohashi (2009) [132]	NSA	Classification and Reduction of Noise Effect
Barontini et al. (2019) [133]	NSA	Damage Detection in Civil Engineering Systems
Igbe et al. (2017) [134]	NSA + DCA	Detecting Denial of Service Attacks
Rashid1 et al. (2018) [135]	NSA	Detection and Classification in Electroencephalography (EEG) Brain Signals
Seresht and Azmi (2014) [136]	NSA + CSA	Distributed IDS-based on Virtual Machine
Igbe et al. (2016) [137]	NSA + GA	Distributed Network Intrusion Detection System
Cao et al. (2007) [138]	NSA	Evolutional Optimization
Silva et al. (2019) [139]	NSA	Identity Recognition based on Facial Biometry
Mohamed and Abdullah (2010) [140]	NSA + CSA + DT	Intrusion Detection in MANETs
Barani and Abadi (2012) [141]	NSA + ABC	Intrusion Detection for AODV Routing Protocol in MANETs
Pamukov (2017) [124]	NSA + DT	Intrusion Detection in IoT
Song et al. (2018) [142]	NSA	Intrusion Detection in Smart Grid AMI Network
Zeeshan et al. (2015) [143]	NSA	Intrusion Detection in WSNs
Liu and Yu (2008) [144]	NSA	Intrusion Detection in WSNs
Zhang and Ma (2016) [145]	NSA + PSA	Malware Detection
Wawryn and Widulinski (2019) [146]	NSA	Malware-Originated Code Detection
Gao et al. (2008) [147]	NSA	Motor Fault Detection
Dasgupta and Saha (2009) [148]	NSA	Negative Password Authentication
Saleh et al. (2019) [149]	NSA	Spam e-mails Detection
Idris and Selamat (2011) [150]	NSA	Spam e-mails Detection
Ma et al. (2009) [151]	NSA	Spam e-mails Detection
Chikh and Chikhi (2017) [152]	NSA	Spam e-mails Detection
Hang and Dai (2005) [153]	NSA + PSA	Supervised Learning for Anomaly Detection
Ma et al. (2010) [154]	NSA	Temporal Pattern Discovery
Nguyen et al. (2014) [155]	NSA + aiNet	Virus Detection

combining NSA with other classification methods, generating detectors in a reasonable time without random generation, using a matching rule to avoid high false alarms, continuous learning by detectors to be compatible with the dynamic behavior of the self-elements, and updating communication rules between detectors as an environmental change has occurred. The authors of the survey [159] argue that the NSA and Genetic Algorithms (GA) can be used as a good approach for solving the intrusions in the real-time world.

The authors of [127] describe the most powerful features of NSA as a Negative Representation of Information (NRI), a detection mechanism, and a one-class classification. The NRI feature has become a standalone topic that is inspired by the discrimination of the self and non-self-mechanism in the BIS and stores the complement information rather than the information itself. This emerging topic contains three main elementary branches which are the NSA, Negative Databases, and Negative Surveys [160]. Basically, NRI is used as a technique for security and privacy.

Traditional NSA is based on randomly generating a large number of self-cells and detectors in addition to a matching process between both of them. The matched detectors are eliminated where only non-matched detectors will remain. The non-matched detectors are used as a countermeasure for detecting unknown intrusions. This mechanism can waste more time in both the generation of self-cells and detectors and the matching process.

TABLE 5. Various NSA improvements in different domain areas up to 2020.

Author and year	Abbreviation	Testing Dataset
YANG et al. (2020) [161]	ADC-RNSA	BCW and KDD Cup 1999
Aissa et al. (2020) [162]	NSNAD	NSL-KDD, Kyoto2006+, UNSW-NB15
Sharma and Bhadauria (2019) [163]	NS-ANN	KDD Cup 1999
Wang et al. (2019) [164]	RS-NSA	Satellite, Arrhythmia
Zhang and Xiao (2019) [165]	SD-RNSA	Iris
Pamukov et al. (2018) [166]	NSNN	NSL-KDD
Chikh and Chikhi (2017) [152]	CNSA–FFO	Spambase Dataset
Guo et al. (2017) [167]	DE-CMOP based NSA	Iris
Zheng et al. (2017) [168]	DNSA	UCI, BCW, Chess, KDD Cup 1999
Pamukov (2017) [169]	MNSA	Synthesis Dataset (SDS)
Sharma and Gupta (2017) [170]	NSA + J48	KDD Cup 1999
Yang et al. (2017) [171]	RNSAP	KDD CUP 1999
Liu et al. (2017) [172]	SDS-RNSA	Survival, BCW, KDD Cup 1999
Zhu et al. (2017) [173]	VorNSA	Skin Segmentation, SDS
Fouladvand et al. (2016) [174]	Densa	2D SDS
Fouladvand et al. (2015) [175]	DENSA	2D SDS, NSL-KDD
Li et al. (2015) [176]	FFB-NSA	2D SDS, Iris, Ball Bearing Fault Data
Tao et al. (2015) [177]	NNSA	KDD CUP 1999, Iris, BCW
Idris and Selamat (2015) [178]	SNSA	Spambase Dataset
Barani and Abadi (2012) [141]	BeeID	Data collected from a series of simulations
Majd et al. (2012) [179]	CH-NSA	Six SDS
Wang and Luo (2009) [180]	PTS-RNSA	2D SDS
Hang and Dai (2004) [181]		Iris, KDD Cup 1999
González (2003) [182]	NSDR	MIT-Darpa 99
González (2003) [182]	NSFDR	Mackey-Glass, MIT-Darpa 99, MIT-Darpa 98
González et al. (2003) [183]	RRNS	Mackey-Glass
Zhang e t al. (2002) [184]	NNSGA	Random Binary Strings
Ayara et al. (2002) [185]	NSMutation	Randomly generated 8-bits data

In this paper, a set of enhancements to NSA have been presented by avoiding the creation of a large number of self-cells and detectors that are used during the detection process. The checking mechanism between self-cells and detectors are also eliminated as there are no created self-cells and detectors. As a result, the time and space complexities will be reduced.

F. DT-BASED INTRUSION DETECTION

The essential idea of the DT is that the immune response arises from danger and not from the non-self. This danger results from any abnormal changes to the system, body or computer system, resources that are expressed as danger signals. Accordingly, danger signals are the main stimulator of the immune responses. Defining, representing,

TABLE 6. Various DT-based IDSs in (WSNs).

Author and year	Danger signals	Misbehavior/detection
Zamani et al. (2009) [197]	• One hop delay • Interest throughput • Long buffer probability	Distributed Denial-of-Service (DDoS)
Shamshirband et al. (2014) [198]	• Sensor node's energy consumption • Variance of time difference between two connections during a specific time window • Length of the packet • Number of connections to the same host • CPU usage • Memory load on the host • Bandwidth saturation	Denial-of-Service (DoS)
Zhang (2009) [199]	Normalized weight function based on CPU usage and memory usage	
Alaparthy and Morgera (2019) [200]	Aggregator output calculated based on: • PAMPs • danger signals • cytokine signal	• Energy Depleting • Blackhole • Wormhole • DDoS • Selective Forwarding
Xiao and Zhang (2019) [201]	A weight function based on: • Energy decline rate • Packet avoidance frequency • Average packet avoidance duration • Receiving frequency of frames • Transmission frequency of frames	• Resource Depletion • Sybil • Selective Forwarding • Wormhole • Sinkhole
Li et al. (2018) [202]	Calculated Value Optimized by GA	Network Traffic

and classifying danger signals are the most important challenge in DT. In the literature, danger signals are defined roughly according to the problem context, environmental conditions, human experience, or a weighted value based on all danger signals. In [186], the cloud model is used to define danger signal as a triple of system parameters to be monitored, weight of danger signals, and threshold of danger. In [187], danger signals are defined based on changes using the principle of differential calculus. In [188], the theory of differential coefficient is used to identify the danger signals as the whole changes of system variables related to system imbalance.

In biology, the DT could be viewed as an extension of immune signals which are categorized either as a one-signal model, two-signal model, three-signal model, or four-signal model [189]. The one-signal model considers only one danger signal from an infected cell that is needed to stimulate the immune response. This signal is known as an antigen recognition signal. In the two-signal model, the immune response according to two types of signals, antigen recognition signal and co-stimulation signal. The third-signal model includes initiation signal, antigen recognition signal, and the co-stimulation signal. An internal signal between immune cells is added to the three-signal model to construct the four-signal model. In the context of the DT in tissue, Greensmith *et al.* [190] the four-signal model includes four groups of signals known as PAMPs signals, Safe Signals or apoptotic signals, Danger Signals, and Inflammatory Cytokine signals.

Even though danger signals have a difficulty to be defined and classified, the AIS-based DT model has great interests and is applied in various application domains. Some of these applications include Fault Detection and Diagnoses (FDD) [191], e-mail Classification [192], Malware Detection [193], Social Network Water Army Detection [194], Rockbolts detection [195], Mobile Spam Detection [196], and IDSs which are our central concern in this research paper. Table 6 shows a list of various DT-based IDSs in the Wireless Sensor Networks (WSNs) with the used danger signals and misbehavior or attack detection for each detection system. Whereas Table 7 shows a list of various DT-based IDSs in other different environments by mentioning the used danger signals and misbehavior/detection.

In this paper, we present a DT-DIDS that consists of a multilayer preprocessing mechanism and the DT-ID algorithm. Different parameters in both the preprocessing mechanism and the DT-ID algorithm are identified. The relations between these parameters are empirically determined in order to obtain a high DR with low FP and low FN alarms.

TABLE 7. Various DT-based IDSs in different environments.

Author and year	Environment	Danger signals	Misbehavior/detection
Sarafijanović and Boudec (2004) [203]	MANETs	Information about the time and nodes correlated with a packet loss	Dynamic Source Routing
Fu et al. (2007) [204]	Network	• Apoptotic alarms • Necrotic alarms	Viruses
Fu et al. (2007) [205]		Normalized weighted function of three factors: attack severity, certainty and the length of attack time.	
Chun and Xing-shu (2007) [206]		Calculated value from antibody concentration and the category of antigen at the t time	DoS
Xiuying et al. (2008) [207]		Number of packets	Abnormal Traffic
Rawat and Saxena (2009) [208]	Autonomous Communication Network (CASCADAS)	CPU utilization over a time window	TCP SYN Flooding
HASHIM et al. (2012) [123]	Heterogeneous Networks	• Initiation Signal • Recognition Signal • Co-stimulation Signal	TCP SYN Flooding
Sun and Wu (2011) [209]	Host Computer	IP packet	TCP SYN Flooding
Krizhanovsky and Marasanov (2007) [210]		Three-signals model	Process

III. PROPOSED IMMUNE-BASED DATABASE INTRUSION DETECTION SYSTEM

The building block of this paper is the applicability and implementation of a DIDS inspired by the BIS. The inspiration process is based on the merging of the NSA and the DT model. By using this merging, some advantages of both mechanisms are applied to protect the secrecy and integrity of data with high efficiency in obtaining low FP and low FN alarms. Therefore, a database is protected from data breaches by using our proposed DT-DIDS.

In this section, the operational structure and the detection algorithm of the proposed DT-DIDS are discussed. In Section A, a multilayer preprocessing mechanism is presented. The needed definitions and terms are also introduced. In Section B, the proposed algorithm for detecting insider user misuse behavior is presented.

A. PROPOSED MULTILAYER PREPROCESSING MECHANISM

The proposed preprocessing mechanism depends on the TTP that is represented by a super administrator for fully controlling the roles, privileges, and the sensitivity of the proposed immune-based detection system. The TTP is considered as the central authority for passing security parameters during the proposed immune-based detection algorithm. There exist four parameters that are categorized based on the preprocessing mechanism and the type of granted privileges to authorized users and database administrators.

The first parameter is to determine the danger zone value (DZV) from which the DT-ID algorithm will start raising danger alarm signals. The second parameter is based on identifying system and database privileges that are used in the overall security system. The third parameter is the user factor that is generated by concatenating system and database privileges. The last parameter is based on identifying the R-contiguous bit matching between the authorized factors. These parameters are discussed based on the following definitions:

Definition 1 (Danger Value Identification): let $S_1, S_2, \ldots, S_n \subset S$ where, S is the overall security system with $S_i \subset S$ be a standalone system with a specific DZV. Each standalone system S_i will have a danger value (DV) specified by the TTP based on the following formula:

$$\forall DV_j \in S_i \; such \; that \; DV_j \propto \frac{1}{D_I} \; \& \; DV_j \geq DZV \qquad (1)$$

where, D_I is the degree of immunity. This degree is subject to adaptation and change based on the sensitivity of user privileges. The danger values DV_j for each granted bit signal must be greater than or equal to the DZV. There exists an inverse relationship between the danger value and the degree of immunity. If the danger value of the system S_i is reduced, the immunity degree of the system S_i will be increased due to the high ability of the system to detect intrusions at lower levels of dangers.

Definition 2 (System and Database Privileges): in database applications, all transactions are classified into P_s and P_d. In system privileges (P_s), the user will have the authorization to perform a particular action on the database schema. Based on ORACLE statistics, there are more than 60 distinct system privileges that can be granted to or revoked from users. Database privileges (P_d) are a set of authorizations that affect the database schema based on different parameters such

TABLE 8. User privileges samples.

	SYSTEM PRIVILEGES							DB PRIVILEGES		
	SELECT	INSERT	UPDATE	DELETE	CREATE TABLE	CREATE VIEW	…	UPDATE_SYSCAT	CONNECT TIME_LIMIT	…
$USER_1$	1	0	1	1	0	0	…	1	0	…
$USER_2$	1	1	1	0	1	0	…	0	1	…
……..	……..	……..	……..	……..	……..	……..	…	……..	……..	…
$USER_N$	1	0	0	1	1	1	…	1	1	…

as roles, updating system catalog, selecting system catalog, session priority, and so on. The system and database privileges are applied based on the following formula:

$$\forall\, P_s \,\&\, P_d \in S_i \; such\; that \; P_s \,\&\, P_d \in \{0,\, 1\} \tag{2}$$

where, P_s is the system privilege and P_d is the database privilege. Each user privilege can take a binary value (0 or 1). If the privilege is granted to the user, a value of 1 is taken; otherwise, a value of 0 is taken.

Definition 3 (User Factor Generation): after identifying the user privileges, a User Factor (UF) is generated and will be used as a Detector (D_{TC}) for detecting intrusive users who try to penetrate the system. Each detected factor is considered as an intrusion and will be stored in an antigen log that is created to store all the detected intrusion factors. By selecting the most sensitive 20 system and database privileges, the user factor will be generated by concatenating both privileges types based on the following formula:

$$\forall\, P_s \,\&\, P_d \in S_i \; such\; that \; UF_{ui} = P_s \parallel P_d \tag{3}$$

Finally, the user factor is created based on users granted and not granted privileges. Besides, the system and database privileges have multiple types of operations such as inserting, updating, creating tables, etc. Each user should know his/her privileges based on a predefined order. Each privilege, whether it is 0 or 1 has a danger value identified by the TTP. Based on the DT, this danger value will raise an alarm if the user violates her/his privileges. As shown in Table 8, each user is granted a set of predefined privileges and each privilege will be associated with a danger value according to its sensitivity and effect on the database. Each granted privilege will have a value of 1 and each privilege that is not allowed to a specific user will have a value of 0.

Definition 4 (R-Value Identification): the R-value is considered to be one of the main features inspired by the NSA. The value of R is identified based on the degree of immunity D_I to detect intrusions.

The R-value is based on matching each bit in the user factor with the stored privilege factor such that if contiguous bits are matched between both factors, the immune-based DT-ID algorithm will raise an alarm. The value of R is identified by the TTP with a Boolean value set to false. A counter parameter is created for counting each matched bit factor until the R-value is verified. In this case, the Boolean value is converted to True and an alarm is raised.

TABLE 9. Inverse relationship between R and DR.

		DR	FP	FN
R Value	High	Low	Low	High
	Low	High	High	Low

In recent intrusion detection researches [211], [212], FP alarms are considered a major drawback in security applications due to the classification of legitimate users as intrusive ones. Most security systems that try to reduce false alarms will have a deficiency in the detection process of unauthorized users. There is an inverse relationship between the value of R and the detection coverage. As presented in Table 9, if the value of R is increased, then to activate the alarm system, a large number of matched bit factors should be satisfied. Based on this concern, two distinct cases should be considered:

Case I: if the value of R is increased, the DR and FP alarms will be low whereas the FN alarms will be high due to the low detection coverage.

Case II: if the value of R is decreased, the detection coverage and FP alarms will be high whereas the FN alarms will be low due to the high detection coverage.

The preprocessing mechanism explores two main layers for achieving high DR of users' intrusions. The first layer is the R-value while the second layer is the DV. The proposed mechanism is effectively integrating both the R-value and the DV.

If the first layer fails in detecting the intrusions and an alarm is not raised, the preprocessing mechanism will be automatically switched to the second layer of the preprocessing mechanism which is the danger value. The overall mechanism gives the priority not to raise an intrusion alarm until the second layer is verified. This can delay raising FP alarms.

Therefore, the FP alarms are reduced with the ability of the mechanism to detect intrusions with high detection coverage and low FN alarms. In the proposed preprocessing mechanism, the DV signal is embedded with the R-value. If the R bit matching algorithm fails in detecting the malicious user, the second and final security layer using DV is activated.

To explore the overall multi-layer preprocessing mechanism, Figure 1 presents the intrusion detection mechanism

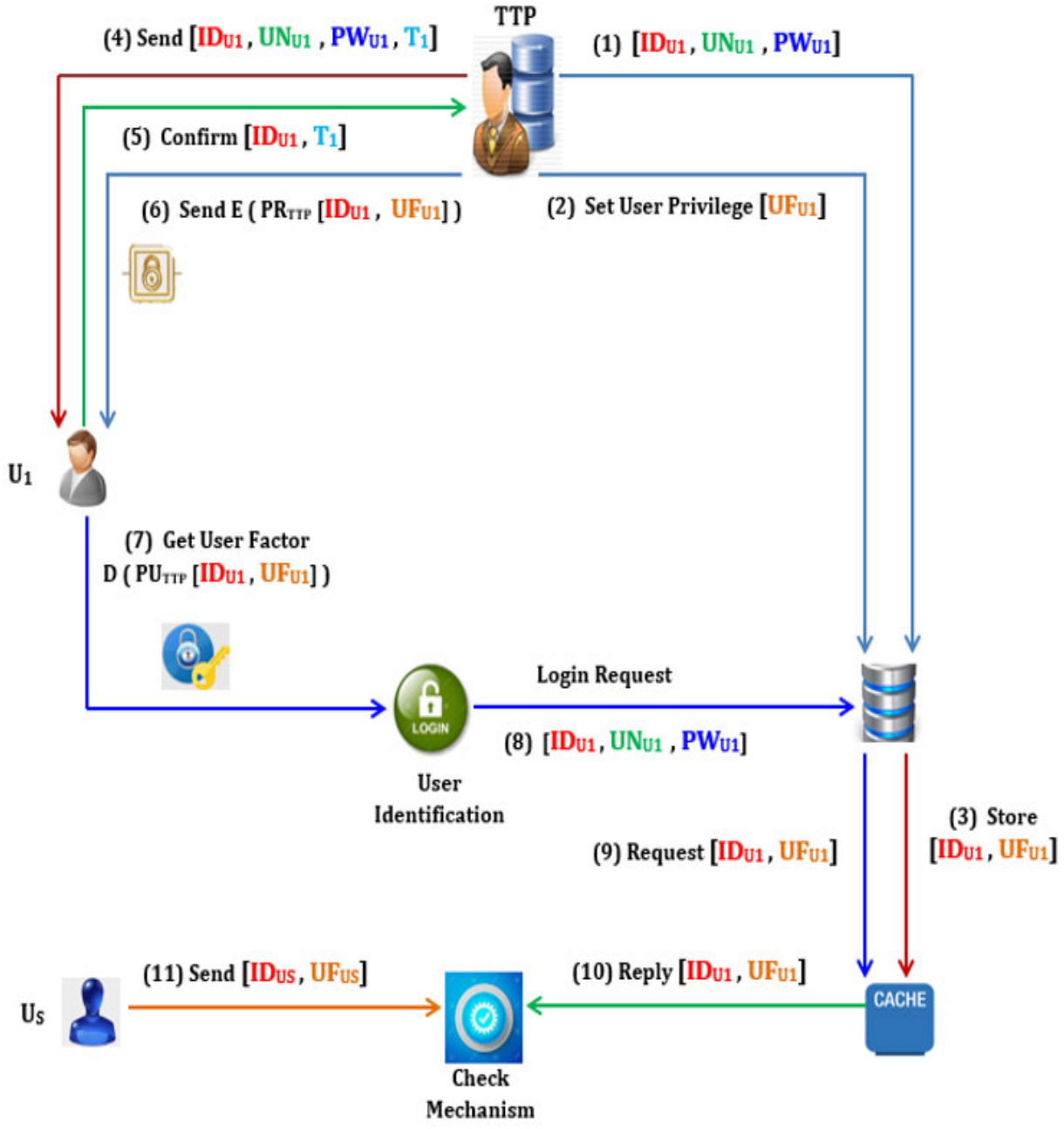


FIGURE 1. Intrusion detection mechanism.

based on the TTP that identifies the degree of system immunity and controls all user privileges and factors. The main mechanism steps are presented as follows:

(1) $[ID_{u1}, UN_{u1}, PW_{u1}]$: The TTP generates an identity for the authorized user ID_{u1}, username UN_{u1}, and password PW_{u1}. These parameters are stored in the database server.

(2) Set User Privilege $[UF_{u1}]$: A user factor UF_{u1} is generated based on specified user privileges. The user factor is stored in the database server.

(3) Store $[ID_{u1}, UF_{u1}]$: The user identity ID_{u1} and user factor UF_{u1} are stored in the system cache for the later detection process.

(4) Send $[ID_{u1}, UN_{u1}, PW_{u1}, T_1]$: The TTP sends the user parameters with a specific timestamp T_1 to the authorized user. The timestamp T_1 is used as a verification between the TTP and user.

(5) Confirm $[ID_{u1}, T_1]$: Once the user receives the parameters, he sends a confirmation to the TTP for receiving the parameters by replying his identity ID_{u1} and the timestamp T_1 to the TTP.

(6) Send E $(PR_{TTP}\ [ID_{u1}, UF_{u1}])$: Once the TTP verifies the user, the user identity ID_{u1} and user factor UF_{u1} are encrypted using the private key of the TTP (PR_{TTP}) while the public key of the PU_{TTP}, is public to all connected users.

(7) Get User Factor D ($PU_{TTP}[ID_{u1}, UF_{u1}]$): The encrypted message is sent to the user U_1 then the user decrypts the message using the public key of the trusted third party PU_{TTP}. After the decryption process, the user will obtain his authentic user factor UF_{u1} that will be used later in the DT-ID algorithm.

(8) Login Request $[ID_{u1}, UN_{u1}, PW_{u1}]$: In this stage the authorized user uses the triple authentic parameters to perform a login process.

(9) Request $[ID_{u1}, UF_{u1}]$: When the user performs a login process using the authorized parameters ID_{u1}, UN_{u1} and PW_{u1}, the database server retrieves the authentic user factor UF_{u1} from the system cache.

(10) Reply $[ID_{u1}, UF_{u1}]$: The authentic parameters are brought from the system cache to be checked with a suspicious user U_s parameters.

(11) Send $[ID_{us}, UF_{us}]$: If a suspicious user U_s succeeds in obtaining the username and password using a brute force attack, then s/he must provide her/his legitimate user factor. A checking mechanism is used in this step using the DT-DIDS to verify the suspicious user U_s based on the immune-based detection system.

B. PROPOSED IMMUNE-BASED DATABASE INTRUSION DETECTION ALGORITHM

The main objective of the proposed DT-ID algorithm is to enhance the performance of the DT-DIDS in detecting intrusions with the high ability for achieving low FN and low FP alarms. The proposed DT-ID algorithm is used to detect intrusive users using the R-value and the enhanced features of NSA with the danger value based on the DT model. As a result, the proposed DT-ID algorithm is more convenient in detecting unknown intrusions that have not been previously discovered. The overall structure of the DT-ID algorithm is shown in Algorithm 1.

As presented in Figure 2, the data flow of the overall steps of the proposed hybrid immune-based algorithm is introduced. The algorithm starts by identifying the DZV that determines the level of security upon which the DR will be obtained based on different levels of DZV. The DZV is considered as an early danger sensor for each bit of privilege.

Each predefined bit privilege takes a danger values DV_j according to its sensitivity and confidentiality of the system S_i. The P_s and P_d are defined to identify the overall roles and privileges that are embedded in the immune-based mechanism. The user parameters: ID, UN, and PW are identified with authentic factor of the user (UF_{u1}).

Each bit in the authentic user factor has a DV inspired by the HIS. The user factor is used as a D_{TC} that is matched with the unknown user factor (UF_{US}). An antigen log is created as a memory of the DT-ID algorithm to scan the log for previously detected intrusions UF_j. The antigen log is also updated to store new detected intrusions from the detection process of the DT-ID algorithm.

Algorithm 1 DT-ID Algorithm

Initialization Step
Initialize S_i
Initialize Danger Zone Value DZV
Initialize Immunity Degree D_I
Initialize danger value DV_j for each bit privilege
Initialize R value
Initialize Boolean value $R_{matched} = false$
Initialize Boolean value $DV_{matched} = false$
For $S_{i=1} \rightarrow S_k$ **do**
  For $U_{q=1} \rightarrow U_n$ **do**
  For $DV_{m=1} \rightarrow DV_j$ **do**
  Inputs: $ID_{u1}, UN_{u1}, PW_{u1}$ // Normal User
  Generate: UF_{u1}
  SET: $ID_{us}, UN_{us}, PW_{us}$ // Suspicious User
  SET: UF_{us}
  IF $UN_{u1} \neq UN_{us}$ OR $PW_{u1} \neq PW_{us}$ **THEN**
    Raise Danger Signal Alarm
  ELSE
    GET UF_{u1} from Cache
    Generate $\mathbf{D_{TC}}$ // Detector
    $\forall UF_{ui} \in S_i$ *such that* $UF_{u1} =, \mathbf{D_{TC}}$ *where* $S_i \subset S$
    IF $\boldsymbol{D_{TC}}$. Length $\neq UF_{us}$. Length **THEN**
      Raise Danger Signal Alarm
      UPDATE Antigen Log
    ELSE
      Search Antigen Log
      IF $UF_{us} \neq$ Antigen Log. UF_j **THEN**
        IF $DV_j \neq Null$ **THEN**
          Check ($UF_{us}, \mathbf{D_{TC}}, R$)
          IF $R_{matched} = true$ **THEN**
            Raise Danger Signal Alarm
            UPDATE Antigen Log
            SET $UF_j = UF_j \cup UF_{us}$ // Attack
          ELSE
            Check ($DV_j, UF_{us}, \mathbf{D_{TC}}, R$)
            IF $DV_{matched} = true$ **THEN**
              Raise Danger Signal Alarm
              UPDATE Antigen Log
              SET $UF_j = UF_j \cup UF_{us}$ // Attack
            END IF
          END IF
        END IF
      ELSE
        Raise Danger Signal Alarm
        UPDATE Antigen Log
        SET $UF_j = UF_j \cup UF_{us}$// Attack
      END IF
    END IF
  END IF
END FOR

For improving the intrusion detection process, three pre-security parameters must be checked during the DT-ID algorithm:

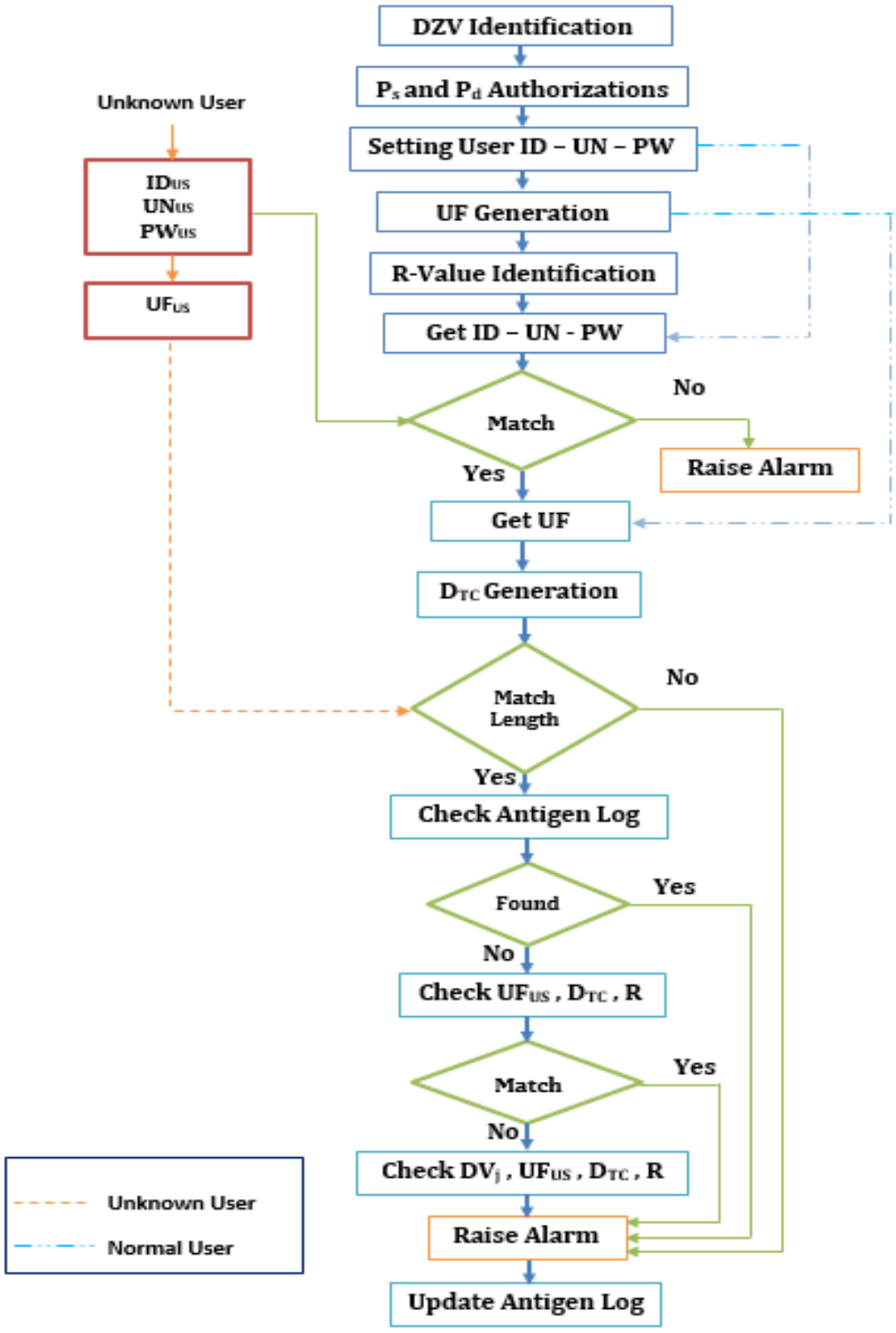


FIGURE 2. Data flow of the proposed DT-ID algorithm.

- The UF_{u1} length is checked as each authorized user knows his legal privileges.
- The antigen log is checked to determine whether the unknown user factor UF_{us} is matched with a pre-detected intrusion in the log.
- The R-value and the DV are checked with the DZV that is identified during the preprocessing mechanism.

Based on these parameters, the DT-ID algorithm will not classify a normal user as intrusive due to the different layers of validity checking. As a result, FP alarm rate can be reduced.

TABLE 10. DVS mechanism.

R = 4 with DZV = 50%																			
Detector D_{TC}																			
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	1	0	1	1	1	0	1	0	0	0	1	0	1	1	0	0	1	0
Suspicious Users UF_{US}																			Status
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
1	0	1	0	1	0	1	0	0	1	1	1	0	1	1	1	0	1	0	1	Intrusion Detection
30%	-	80%	90%	80%	-	40%	40%	-	-	-	-	-	-	50%	50%	10%	-	-	-	DV_i Value
off	-	on	on	on	-	off	off	-	-	-	-	-	-	on	on	off	-	-	-	Signal Alarm
0	0	1	0	1	0	1	0	1	1	1	0	0	1	1	0	1	1	0	1	Intrusion Detection
-	-	80%	90%	80%	-	40%	40%	70%	-	-	10%	-	-	50%	-	-	-	-	-	DV_i Value
-	-	on	on	on	-	off	off	on	-	-	off	-	-	on	-	-	-	-	-	Signal Alarm
1	0	1	1	1	0	0	0	1	1	1	0	0	1	1	0	0	1	0	1	Intrusion Detection
30%	-	80%	-	80%	-	-	40%	70%	-	-	10%	-	-	50%	-	10%	-	-	-	DV_i Value
off	-	on	-	on	-	-	off	on	-	-	off	-	-	on	-	off	-	-	-	Signal Alarm

As presented in Algorithm 1: DT-ID algorithm, the subsystem $S_i \subset S$ is initialized with the DZV and the immunity degree D_I. The R-value is initialized as a first layer of the immune-based detection process. The second layer DV_j is initialized for each bit privilege such that the DV_j must be greater than or equal to the DZV to apply the detection process. Both R and DV_j are set to a Boolean value = False. The Boolean values will be converted to 'True' when unknown user is detected.

The normal or authorized user parameters ID, UN, and PW are defined and the authentic user factor UF_{u1} is generated. The user identification process is activated by invoking the normal user parameters UN_{u1}, PW_{u1} to match them with the suspicious user parameters UN_{us}, PW_{us}.

If there is no match, a danger signal alarm will be raised. Otherwise, the unknown user proceeds to the next level into which the authentic UF_{u1} is brought from system cache. The user factor UF_{u1} is used as a D_{TC} and is matched with the suspicious user factor UF_{us}.

If the D_{TC} length is not matched with the suspicious user factor UF_{us} length, an alarm will be raised and the antigen log will be updated by adding the suspicious user factor UF_{us} in the memory of the DT-ID algorithm in order to be checked in future immune-based detection processes.

If the length of both D_{TC} and UF_{us} is matched, the antigen log will be scanned for UF_{us} to check whether the UF_{us}, is previously detected or not. If the UF_{us} exists in the previously detected intrusions UF_j of the antigen log, an alarm will be raised.

This means that the immune-based detection process has already detected the UF_{us} before. If the UF_{us} does not exist in the antigen log, the DT-ID algorithm will be initialized based on two main layers.

The first layer uses the R-value and our enhanced features of NSA; see section IV, along with the D_{TC} to check the UF_{us}. If a match is found, then the Boolean value of R will be set to True. An alarm will be raised and the antigen log will be updated to the store the UF_{us} as a malicious user; such that previously detected intrusions $UF_j = UF_j \cup UF_{us}$. Otherwise, the second layer will be activated by embedding the danger value DV_j with the R-value and the D_{TC} to satisfy the value of the DZV.

In order to demonstrate the importance of merging the R-value and the DV parameters in the detection process, we present a case study of using the R-value alone and the use of both two parameters together in Table 10. As presented in Table 10, the D_{TC} will not be able to detect suspicious users if the detection process is based on R = 4 only. In order to detect suspicious users, there must be at least 4 contiguous matches between the fake user and the main D_{TC}. The two suspicious users have 5 matches with the D_{TC}, but these matches are not contiguous.

This means that if the detection process is based on the R-value alone, then the two suspicious users will succeed in penetrating the database security system. Although the value of R is small (R = 4) when compared to the UF length, the R-value did not succeed in detecting the malicious user. So, FN alarms will increase in the same manner.

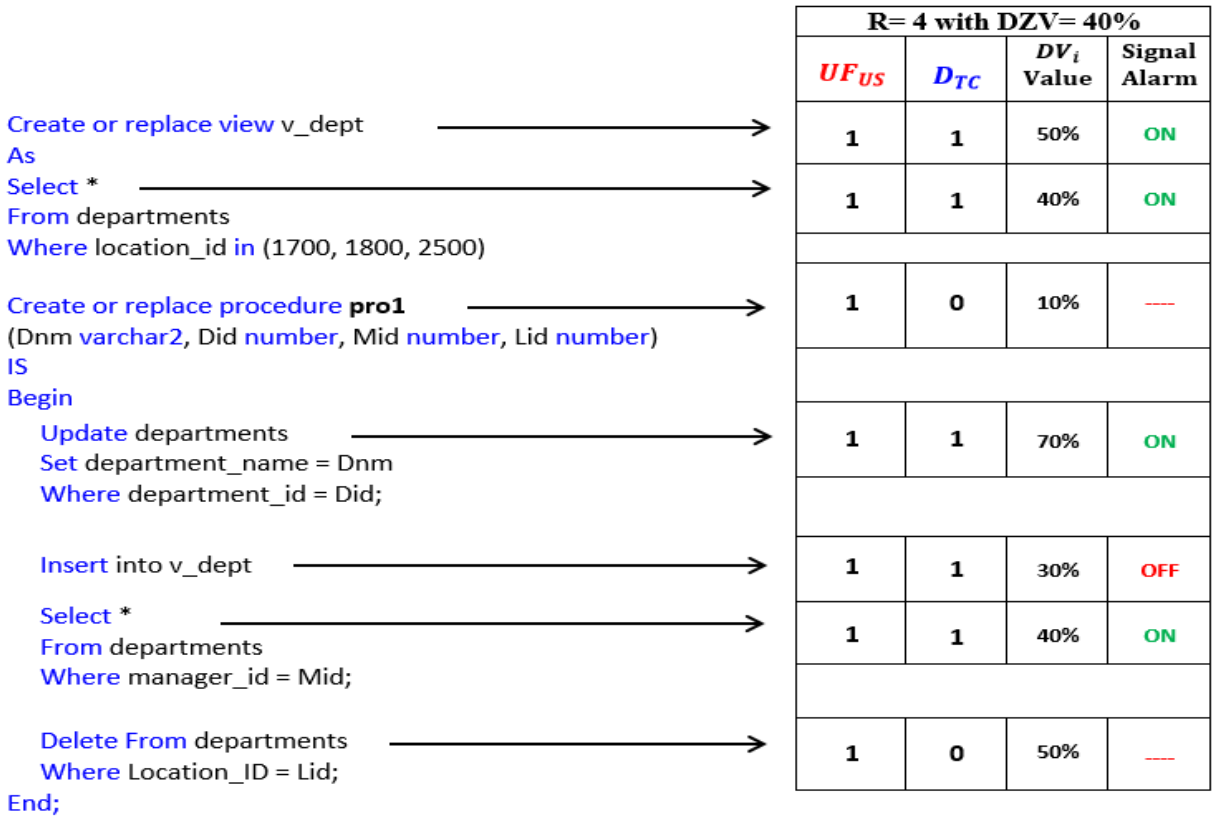


FIGURE 3. DZV with user transactions.

The DV presented in the DT-ID algorithm will have the ability to detect both suspicious users. Each signal creates a danger zone around itself that will be activated if the user violates his predefined privileges.

For example, the first suspicious user has 9 matches with the main detector, but only 5 matches will alarm a danger zone because their inflammation is larger than or equivalent to the main DZV which is 50%. The 5 matches have 3 contiguous matches in the 3rd, 4th, and 5th position and 2 contiguous matches in the 15th and 16th positions. The second fake user has 8 matches with the main detector, but only 5 matches will alarm a danger zone because their inflammation is larger than or equivalent to the DZV which is 50%.

The presented DT-ID algorithm is based on proactive and reactive methodologies. Proactive methodology is based on eliminating breaches and enforcing the least privileges with the ability to detect intruders before penetrating system resources. The DT-ID algorithm is not only convenient in verifying the authenticity of users' factors, but also has a reactive methodology to check the validity of each user transaction during transmission using the DV.

As presented in Figure 3, different user transactions are executed. The pending transactions are converted to user factor and then the user factor is compared with the detector. With main DZV = 40%, all matched factors that DV exceeds the DZV will raise a signal alarm that reflects the sensitivity of the system.

The process of creating database roles and granting the roles to authorized users is considered a time-consuming mechanism with high FP alarms as the user may need to perform a critical transaction that will be denied based on his privilege. Instead, the proposed DT-ID algorithm can permit users to perform their transactions using a proactive methodology that verifies the danger level of each distinct transaction.

IV. NEGATIVE SELECTION ENHANCEMENTS

In the traditional NSA, a large number of self-sets and detectors are generated randomly. Self-sets represent normal user behaviors while the detectors are used to detect abnormal behaviors. A matching process is executed between self-sets and detectors in order to find the similarities between both of them. If there is a match, the detector is deleted until only non-matched detectors are maintained. The non-self or non-matched detectors are considered the defender of the system from breaches. This strategy causes a waste of time and space to generate detectors that can detect abnormal behavior.

In our proposed DT-DIDS, the preprocessing mechanism is applied to generate logical self-users based on harmonious security architectures. The developed DT-ID algorithm can generate different roles with different degree of immunity and sensitivity signals. Each role can be granted to different users and vice versa. The generated role is still distinct, so the

developed DT-DIDS does not require any redundancy checking. The developed security system is more dynamic because the number of privileges can be increased and decreased at any time according to users' authorizations and privileges. This can make the length of the detector more dynamic and makes the DT-DIDS more flexible.

The capability and strength of NSA are based on different parameters that can enhance the detection process. These parameters are:

- The detectors are not generated randomly. The privileges of each authorized user are considered a detector.
- The non-self-detectors are not required to be stored in the antigen log. This means that the NSA can detect unknown intruders that may have not any previous signatures.
- There is no relationship between detectors that are stored in the antigen log for the future detection process. This means that each D_{TC} will be an independent defense unit.
- Checking the activity of each user is considered a standalone process while DT-ID algorithm is used over multiple users' mechanism.
- The user signature that has been detected using the DT-ID algorithm is stored in the antigen log as a D_{TC} to detect unknown intrusions.
- Symmetric protection is applied so that the malicious manipulation of detector set can be detected by normal behavior of the DT-DIDS.
- The detection process will be high with a low number of detectors. As a result, the time and space complexities for searching the detectors will be optimal.

In addition to the previous enhancements, one of the major limitations of NSA is that a vast number of randomly generated self-cells and detectors need to be discarded before the required number of detectors is obtained. As a result, space and time complexity will be high. As shown in Table 11, the enhanced features do not generate self-cells and the detectors are generated from the authorized normal users of the system $S_i \subset S$. So, the checking mechanism between self-cells and detectors is not required because self-cells are not generated. As a result, space and time complexity will be reduced.

TABLE 11. NSA enhanced features.

Parameters	Traditional Features	Enhanced Features
Self-cells	Large Number of Self-cells	No self-Cells
Detectors	Large Number of Detectors	Single Detector $\mathbf{D_{TC}}$ for each User
Checking Mechanism	Required	Not Required
Time	High	Low
Space	High	Low

V. EXPERIMENTAL RESULTS AND DISCUSSION

Lack of benchmark datasets is one of the challenges for Database intrusion detection. Therefore, in this section, we use synthetic data to evaluate the efficiency of the proposed DT-ID algorithm by measuring the overall DR according to different DZV inflammations, FN alarm rate, FP alarm rates, and Correctness Rate (CR). The effect of DZV and the R-value is also addressed. The proposed DT-ID algorithm is designed using Microsoft SQL Server 2017 to perform the following processes:

- Building database roles with different privileges.
- Granting the created roles to different administrators and users.
- Applying a TTP for tracing all user processes.
- Building different multiple distinct DT-DIDS where $S_i \subset S$ with different immunity degrees.
- Applying a dynamic danger value DV_j for each granted bit signal.
- Specifying the value of R with different levels of immunity.
- Specifying the DV with the combination of R to measure and verify different detection coverage.

The proposed DT-DIDS was implemented using Microsoft Visual Studio C# 2019 for deploying the security system components on a client-server application. The experiments are conducted on an Intel(R) Core (TM) i5 CPU @ 1.8 GHz machine with 8 GB of RAM. Microsoft Windows 10 is the used operating system.

Each test in the DT-DIDS contains 1000 malicious processes that are scanned for a single value of R-value with distinct DZV signal. For example, the parameters for a single test are R = 3 with DZV inflammation signals: 50%, 40%, 30%, 20%, and 10%. The lower the value of inflammation signal, the higher the sensitivity of the DT-DIDS for any intrusions as presented in formula (1). The values of R-value and DZV signals are examined 6 times for R = 3, 4, 5, 6, 7, and 8 with different DZV signals. This creates a total of 6000 malicious processes for every single DZV signal.

In order to realize high system reliability, the experimental results are conducted 5 times for different DZV signals: 50%, 40%, 30%, 20%, and 10% to deliver accurate and efficient results. This generates a total of 30,000 malicious processes that will be examined into the proposed artificial immune security system to measure the overall DR of the developed algorithms.

The overall malicious processes are tested into the DT-DIDS to measure the average response time from the antigen log response. The antigen log response is considered the primary memory of the DT-DIDS. Each detected user is stored in the antigen log response as a fake user. If another user uses the same signature that has been previously detected, the DT-DIDS will scan the antigen log response first to reduce the time complexity resulted from testing the user signature using DT-ID Algorithm.

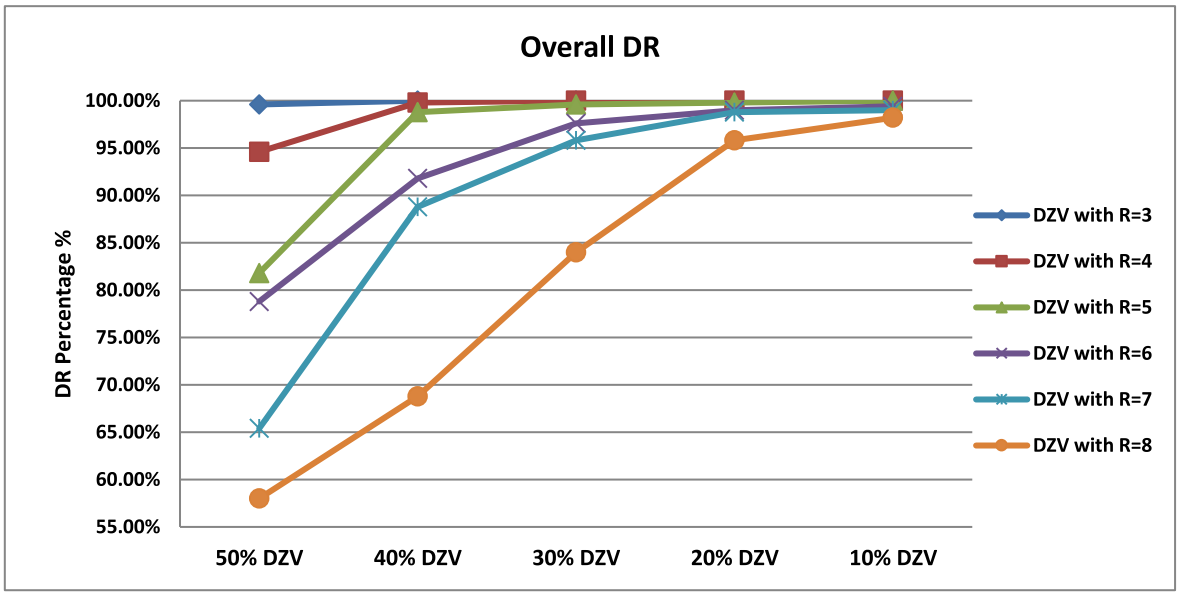


FIGURE 4. Overall DR for DZV inflammation signals.

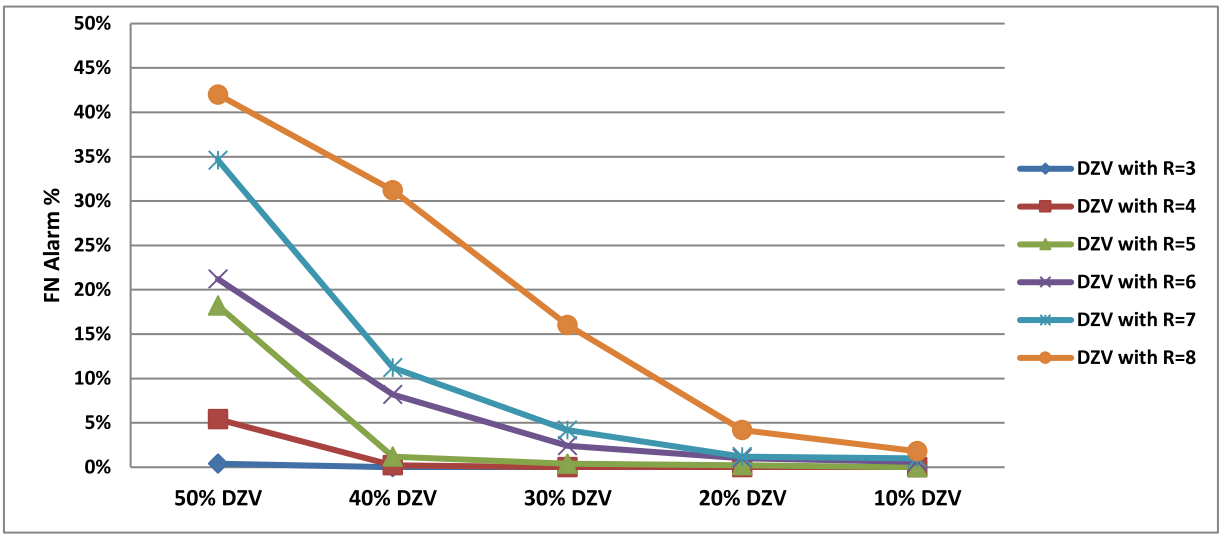


FIGURE 5. FN alarms.

The DR indicates the percentage of detected intrusion action. It is calculated by dividing the total number of detected users (N_d) by the total number of users (N). This is presented in formula (4).

$$DR = \frac{N_d}{N} \times 100\% \tag{4}$$

As shown in Figure 4, the DT-DIDS produces a high DR with different R-values and different DZV signals. With R = 3, the DR recorded 99.6% with DZV signal = 50%. By increasing the DZV value sensitivity to 10%, the DR recorded 100% detection. The overall DR is increased linearly with the increase of DZV sensitivity.

When R = 8, the DR records 58% with DZV signal equal to 50%. The value of DR increases linearly until it reaches 98.2% whenever the DZV signal becomes more sensitive with DZV = 10%.

While the system S_i uses DZV signal with 10%, the DR achieved 99.6% with R = 3 until it reaches 100% with R = 8.

The FN alarms indicate the number of malicious users who succeeded in passing the DT-DIDS. The percentage of FN alarms is calculated by dividing the number of passing malicious users (N_p) by the total number of examined users (N). This is presented in formula (5).

$$FN = \frac{N_p}{N} \times 100\% \tag{5}$$

As presented in Figure 5, FN records low values due to the high DR presented in Figure 4. With R = 3, FN records 0.4% with DZV inflammation signal = 50%. By increasing

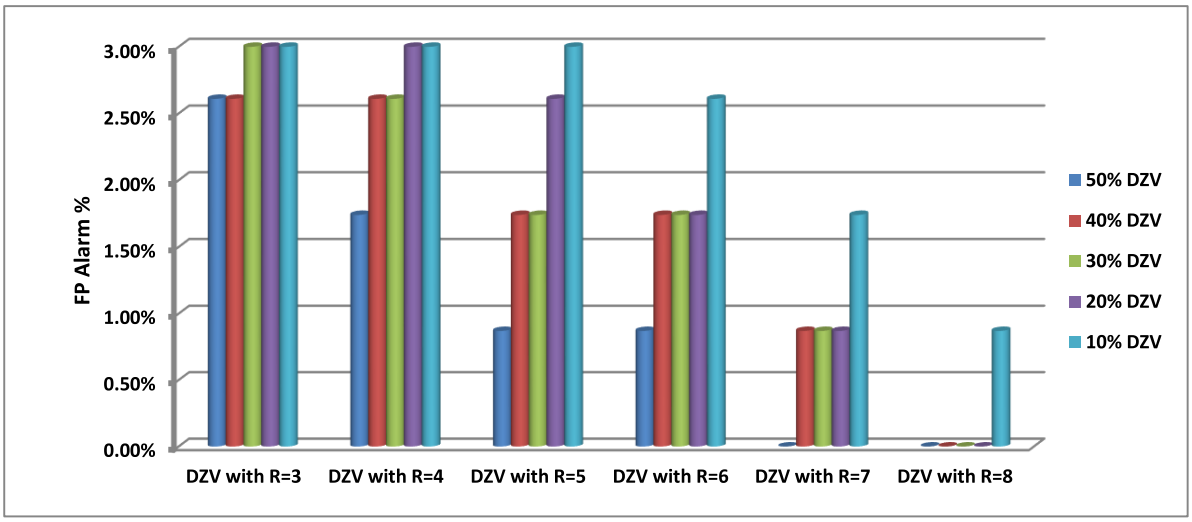


FIGURE 6. FP alarms.

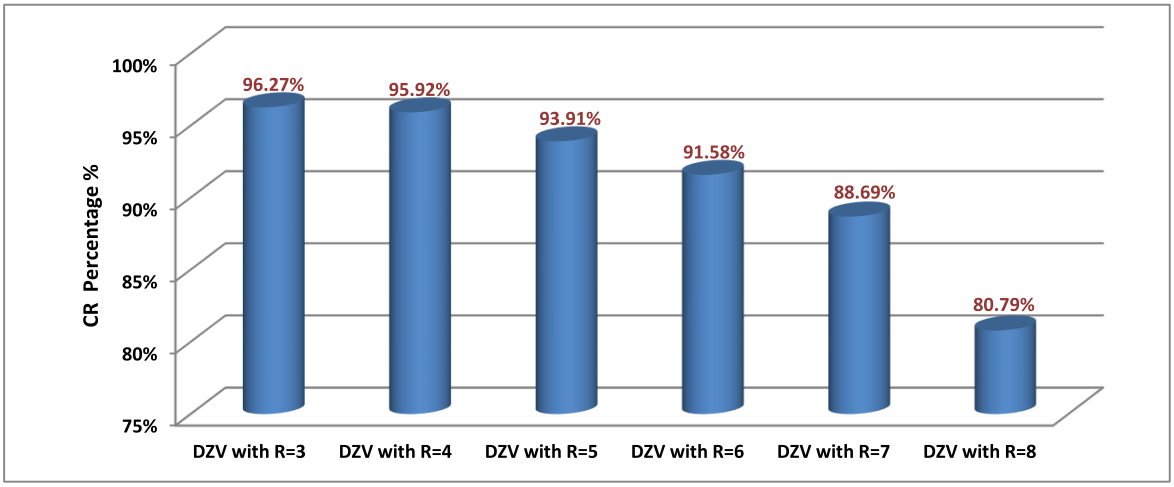


FIGURE 7. Average CR.

the DZV value sensitivity to 10%, FN alarms are minimized until it reaches 0%. Regardless of the value of R or the DZV signals, all the recorded FN alarms are below to 0.5% when R = 3 with all DZV signals from 50% to 10% respectively. This can achieve a high DR with low FN alarms.

The FP alarms refer to the probability that legitimate users are detected in the wrong way as malicious users. This is presented in formula (6).

$$FP = \frac{N_f}{N} \times 100\% \tag{6}$$

where (N_f) is the number of legitimate users who are detected as malicious users. As presented in Figure 6, the FP alarms records low values, especially when the value of R is increasing. By testing 115 normal users in the system S_i for verifying the FP alarms, when the R = 3, the FP alarms recorded 2.61%, 2.61%, 3.48%, 4.35%, and 5.2% with DZV signal = 50%, 40%, 30%, 20%, and 10% respectively.

This means that when the DZV signal sensitivity increase, the FP alarms increase as well. The testing operation is continued by increasing the value of R to decrease the FP alarms. With R = 8, the FP alarms have vanished in all DZV inflammation signals except for the DZV signal = 10% that records 0.87% FP alarms.

Depending on multiple levels for verifying the user before raising the danger signal alarm, the FP rate will be minimized. Moreover, increasing the value of R reduces the FP alarms that may be recorded in the system due to the difficulty in obtaining errors in the user factor UF_{u1} in the case of increasing the value R.

The CR of the proposed experimental study is presented. The CR indicates the probability of correct detection and could be obtained by subtracting FP and FN alarms from equations 5 and 6 as expressed in the formula (7).

$$CR = (1 - FP - FN) \times 100\% \tag{7}$$

As presented in Figure 7, the CR achieves average correct detection with 96.27% to the value of R = 3 with DZV inflammation signals. With DZV inflammation signals and

value of R = 8, the CR records 80.79% due to the lower value of DR.

TABLE 12. Performance metrics.

DZV Value	R Value	DR	FN Rate	FP Rate	CR
DZV = 50%	R=3	99.6%	0.4%	2.61%	96.99%
	R=4	94.6%	5.4%	1.74%	92.86%
	R=5	81.8%	18.2%	0.87%	80.93%
	R=6	78.8%	21.2%	0.87%	77.93%
	R=7	65.4%	34.6%	0.0%	65.40%
	R=8	58.0%	42.0%	0.0%	58.00%
DZV = 40%	R=3	100%	0.0%	2.61%	97.39%
	R=4	99.8%	0.2%	2.61%	97.19%
	R=5	98.8%	1.2%	1.74%	97.06%
	R=6	91.8%	8.2%	1.74%	90.06%
	R=7	88.8%	11.2%	0.87%	87.93%
	R=8	68.8%	31.2%	0.0%	68.80%
DZV = 30%	R=3	100%	0.0%	3.48%	96.52%
	R=4	100%	0.0%	2.61%	97.39%
	R=5	99.6%	0.4%	1.74%	97.86%
	R=6	97.6%	2.4%	1.74%	95.86%
	R=7	95.8%	4.2%	0.87%	94.93%
	R=8	84.0%	16.0%	0.0%	84.00%
DZV = 20%	R=3	100%	0.0%	4.35%	95.65%
	R=4	100%	0.0%	3.48%	96.52%
	R=5	99.8%	0.2%	2.61%	97.19%
	R=6	99.0%	1.0%	1.74%	97.26%
	R=7	98.8%	1.2%	0.87%	97.93%
	R=8	95.8%	4.2%	0.0%	95.80%
DZV = 10%	R=3	100%	0.0%	5.2%	94.80%
	R=4	100%	0.0%	4.35%	95.65%
	R=5	100%	0.0%	3.48%	96.52%
	R=6	99.4%	0.6%	2.61%	96.79%
	R=7	99.0%	1.0%	1.74%	97.26%
	R=8	98.2%	1.8%	0.87%	97.33%

The overall performance metrics of the proposed DT-ID algorithm with DZV signals and R-values are demonstrated in Table 12 for recording approximate values for DR, FN rates, FP rates, and CR. Whenever the DZV = 50%, the system is considered in a permissive or tolerant mode.

When applying different values of R = 3 to R = 8, the DR is decreased from 99.6% for R = 3 to 58% for R = 8. This is due to the difficulty in obtaining more bit signal alarms for detecting intrusions. At the same time, the FP rate is also decreased due to the difficulty of predicting normal users as intrusive; because of the increasing R-values. By decreasing the DZV values from 50% to 10%, the system becomes less tolerant. As a result, the sensitivity of the system to detect intrusions will increase.

For DZV = 50% and R = 3, the DR achieved 99.6%. Whenever R is increased to R = 8, the DR achieved 58% with a reduction rate −41.6%. For DZV = 40% and R = 3, the DR achieved 100%. With an increase of R to 8, the DR achieved 68.8% with reduction rate −31.2%. For DZV = 30% and R = 3, the DR achieved 100%. Whenever R = 8, the DR achieved 84% with a reduction rate −16%. For DZV = 20% and R = 3, the DR achieved 100%. Whenever R = 8, the DR achieved 95.8% with a reduction rate of −4.2%.

By having DZV = 10% and R = 3, the DR achieved 100% while R = 8, the DR achieved 98.2% with a reduction rate of only −1.8%. As seen from the results, the DR difference between R = 3 and R = 8 is highly decreased whenever the DZV value is decreased to be more sensitive.

From the conducted experiments, as the DZV value is decreased, the ability of the system becomes more sensitive to detect intrusions with the ability to obtain low FP rates in all DZV values. By using DZV = 50%, the FP rate achieved 0% with R = 7 and 8. Whenever DZV = 40%, 30%, and 20%, the FP rates achieved 0% with R = 8. While DZV = 10%, the FP rate with R = 8 achieved 0.87% which is below 1%. The best achieved CR is 97.93% for DZV = 20% and R = 7.

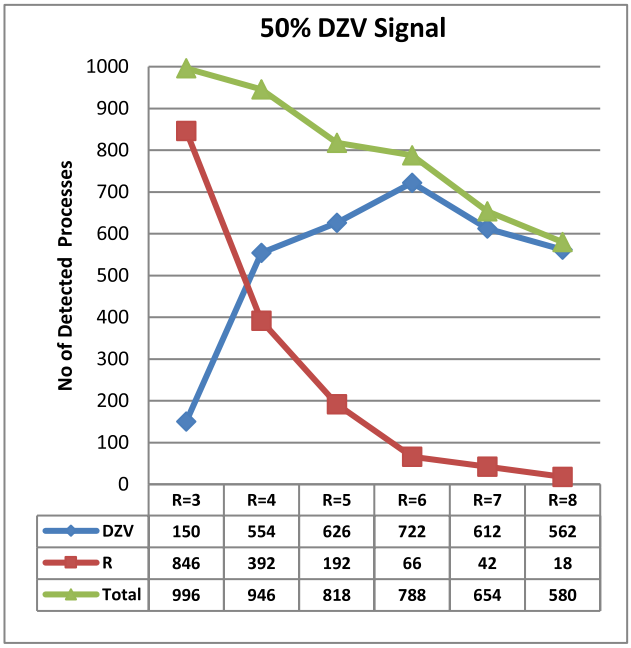
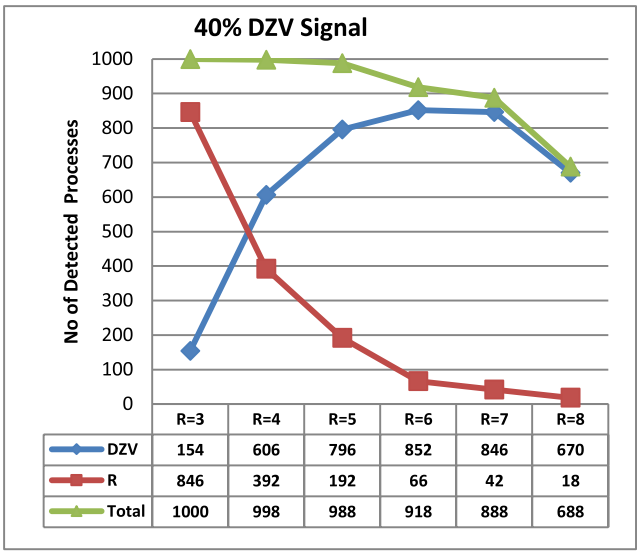


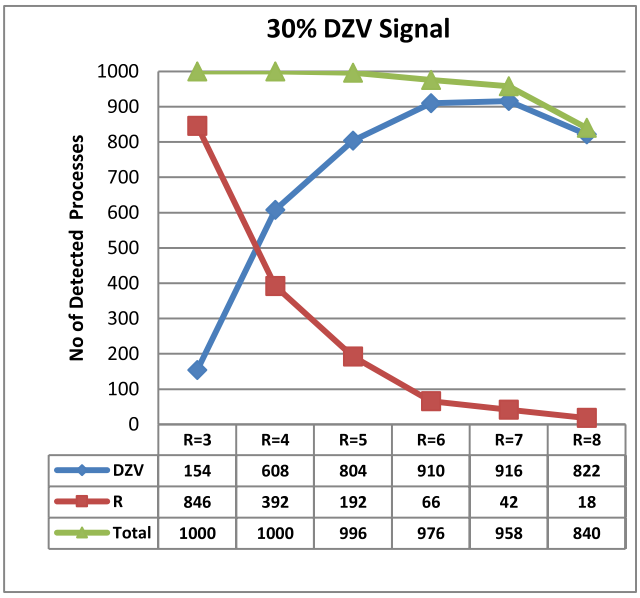
FIGURE 8. 50% DZV signal.

Each test in the DT-DIDS contains 1000 malicious processes that are scanned for a single value of R with each DZV signal. Figures 8 to 12 present the comparison between R-value and DZV inflammation value according to the number of malicious processes detected. The number of detected intrusions are decreased whenever the value of R is increased.



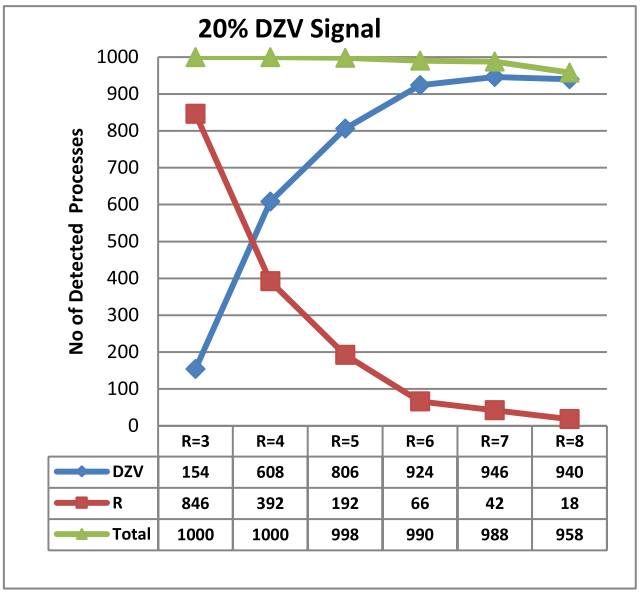
	R=3	R=4	R=5	R=6	R=7	R=8
DZV	154	606	796	852	846	670
R	846	392	192	66	42	18
Total	1000	998	988	918	888	688

FIGURE 9. 40% DZV signal.



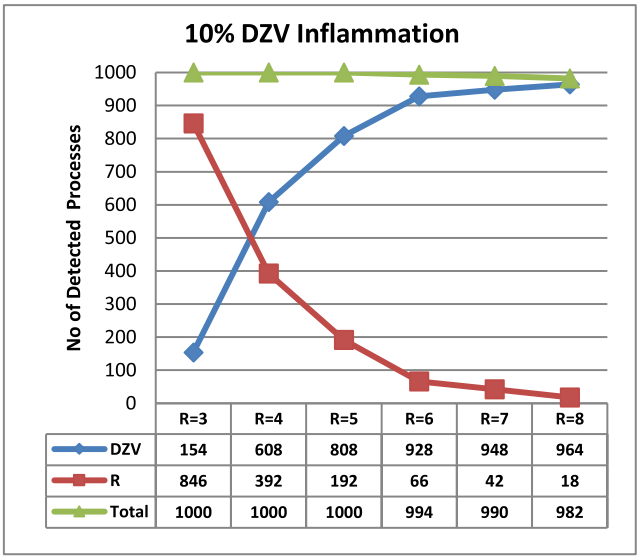
	R=3	R=4	R=5	R=6	R=7	R=8
DZV	154	608	804	910	916	822
R	846	392	192	66	42	18
Total	1000	1000	996	976	958	840

FIGURE 10. 30% DZV signal.



	R=3	R=4	R=5	R=6	R=7	R=8
DZV	154	608	806	924	946	940
R	846	392	192	66	42	18
Total	1000	1000	998	990	988	958

FIGURE 11. 20% DZV signal.



	R=3	R=4	R=5	R=6	R=7	R=8
DZV	154	608	808	928	948	964
R	846	392	192	66	42	18
Total	1000	1000	1000	994	990	982

FIGURE 12. 10% DZV signal.

In order to study the relationship between the DZV with its DV and R-value, the DZV is minimized with 10% in each test to increase the sensitivity of the system to detect more intrusions. In Figure 8, the detected intrusions using the DZV signal are increased linearly until the value of R = 6. At this point, the detected intrusions start decreasing but in a small limit.

In Figure 9, the DZV signal is increased linearly until the value of R is 7 with 846 detected intrusions. While the detected intrusions using R-value = 42. At this point whenever R = 8, the detected intrusions decreased due to the difficulty in detecting 8 dangerous signals in the same factor with DZV = 40% that means low sensitivity.

In Figure 10, the DZV signal is increased linearly until the value or R is 7 with 916 detected intrusions. Whereas the number of detected intrusions using R-value recorded 42 processes with 4.2%. Whenever R = 7, the total number of detected malicious processes is 958 processes with 95.8% accuracy. When the sensitivity of the DT-DIDS increases, its ability to detect malicious intrusions increases as well. This makes the detected intrusions of Figure 10 where the DZV signal is 30%, generates a high result, although the value of R-value increases, and the difficulty in detection increases as well. As shown in Figure 11, whenever R = 3, the overall detected intrusions are 1000 where R achieved an accuracy of 84.6% and DZV accuracy achieved 15.4%. By increasing

the R-value, the DZV is increasing linearly until it achieved 94% with 940 detected processes while the R-value achieved 1.8% accuracy from the overall detected processes.

In Figure 12, the DZV signal became in a highly sensitive state. As a result, the DZV recorded high detection results until it reaches 964 malicious intrusions from a total of 982 detected processes with an overall DR of 98.2 %. Figure 13 presents the overall detected intrusions with different values of R and DZV. As shown, all detected intrusions are increasing with different values of R but at a specific value, the results are decreased except with the DZV = 10%. In this level, the detected intrusions are increasing linearly due to the high sensitivity of the DT-DIDS to detect malicious intrusions.

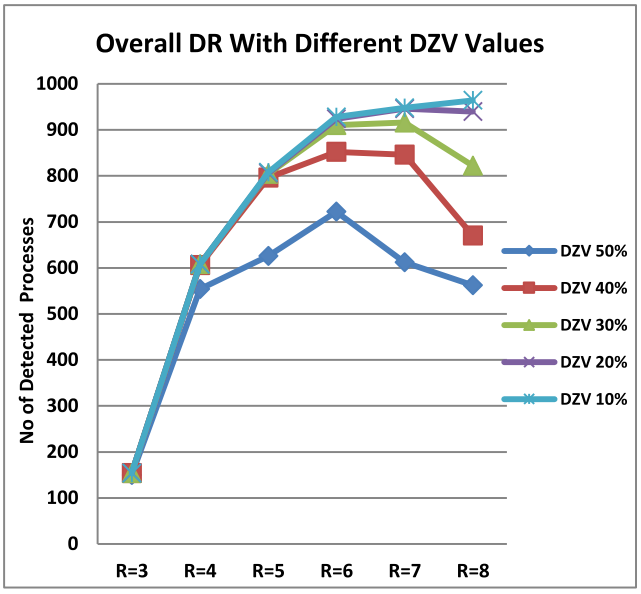


FIGURE 13. Overall DR with different DZV values.

It is worth mentioning that one of the major contributions of this paper is the minimization of time complexity. The time overhead is reduced due to the antigen log response which can be used as an early warning system to detect malicious processes that have been previously detected.

As shown in Figure 14, the average detection time and average antigen log response time is calculated for all DZV inflammation signals. The average detection time increases linearly with the increase in the complexity of detecting malicious signals in the same user factor. The average detection time when R = 5 with different DZV inflammation signals is 7.35 milliseconds while the average detection time when R = 8 recorded 8.17 milliseconds due to the time spent in scanning the malicious transaction for 3 more dangerous signals. The average antigen log response to different R-values and DZV signals recorded relatively fixed results. For R = 8, the average antigen log response reduced to be 1.97 milliseconds due to the decrease of the search space.

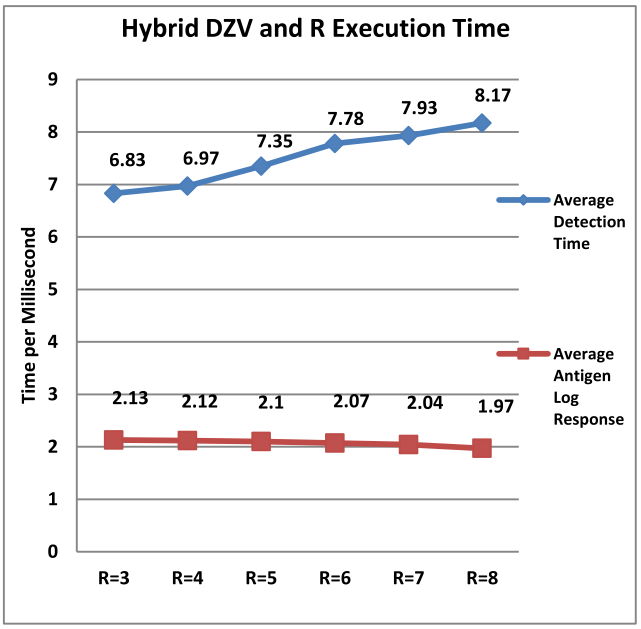


FIGURE 14. Execution time of hybrid DZV and R.

Table 13 explores a comparison between the proposed DT-ID Algorithm with other techniques to analyze the DT-ID Algorithm with others.

In Table 13, a comparison model is presented to compare the performance of the proposed DT-ID algorithm with recent research models that do not use a DT model. The proposed DT-ID algorithm achieves a high DR with low FP and low FN alarms. As illustrated in [51], the ART1 based DIDS model has achieved relatively good results at DR = 98.06%. With FP = 4.53 and FN = 1.94. Whereas by using the SOM based DIDS, the FP and FN alarms are high with values of 10.22% and 8.77% respectively. The RBFN based DIDS model has achieved a DR = 94.42% with a moderated FP and FN values compared to ATR1 and SOM based models. The authors of [60] use a mean-shift clustering with the C4.5 algorithm to detect unknown intrusions with different dataset sizes. The highest DR is achieved at 96% but the FP and FN are still high with 9.56% and 5.46% respectively. As shown in [68], by using swarm intelligence to detect database intrusions with the use of KNN and SVD algorithms to optimize the results. The best results are achieved by obtaining DR = 97.2% with FP and FN of 2.5% and 2.8% respectively. The authors of [69] use OPTICS and ensemble learning to detect intrusive processes in the database using different machine learning algorithms. The RBFN reach the highest DR = 92.17% with 3.5% FP rate. By using only, the NSA to detect unknown database intrusions in [120], which is a contribution for the second author of this paper, the DR = 98.3% with significant FP and FN values.

The DT-ID algorithm has achieved the best DR, FP, and FN of different DZV and R-values are selected based on the highest correctness rate of Table 12. With DZV = 50% and R = 3, the best DR, FP, and FN achieved 99.6%, 2.61%,

TABLE 13. Performance comparison of the proposed model.

Reference	Dataset Size	Technique / Algorithm	DR	FP	FN
[51]	80000	ART1 based DIDS	98.06%	4.53%	1.94%
		SOM based DIDS	91.23%	10.22%	8.77%
		RBFN based DIDS	94.42%	6.76%	5.58%
[60]	60	Mean-Shift Clustering and C4.5 Algorithm	88%	22%	11%
	110		92%	14.3%	9.11%
	160		94.89%	9.68%	8.17%
	210		96%	9.56%	5.46%
[68]	80000	K-NN and SVD	97.2%	2.5%	2.8%
[69]	484	RBFN	92.17%	3.5%	7.83%
		Naïve Bayes	91.23%	3.51%	8.77%
		Decision Tree	91.83%	4.23%	8.17%
		Rule Induction	91.81%	4.21%	8.19%
		K-NN	90.24%	11.84%	9.76 %
[120]	1388	NSA	98.3%	1%	1.67%
Proposed DT-ID Algorithm	30000	DZV = 50% R = 3	99.6%	2.61%	0.4%
		DZV = 40% R = 3	100%	2.61%	0%
		DZV = 30% R = 5	99.6%	1.74%	0.4%
		DZV = 20% R = 7	98.8%	0.87%	1.2%
		DZV = 10% R = 8	98.2%	0.87%	1.8%

and 0.4% respectively while the DZV = 40% and R = 3, the DR achieved 100% and FP rate still 2.61%. With DZV = 30% and R = 5, the DR achieved 99.6% with low FP and FN rates of 1.74% and 0.4% respectively. With DZV = 20% and R = 7, the DR achieved 98.8% with FP and FN rates of 0.87% and 1.2% respectively. By using DZV = 10% which is considered as the highest degree of sensitivity of the proposed DT-ID algorithm, all values of R achieved high results. The best-balanced results are obtained with R = 8 into which the DR achieved 98.2% while FP and FN rates achieved 0.87% and 1.8% respectively.

VI. CONCLUSION AND FUTURE SPOTLIGHTS

Database is considered as the last line of defense in securing the confidentiality and integrity of data. Insider attacks or intrusions are considered the most dangerous factors that affect the efficiency of databases. A hybrid immune algorithm based on DT is presented to apply different countermeasures that can preserve the secrecy of data from disclosure. A DT-DIDS is developed and implemented based on a multilayer preprocessing immunity-based mechanism and the DT-ID algorithm.

Empirically, the proposed DT-ID algorithm is tested with different DZV and R-values to achieve a high DR with low FP alarm, low FN alarms and high CR. The proposed DT-DIDS is considered in a permissive or tolerant mode whenever the DZV = 50%. The overall DR is linearly increased with the increase of DZV signals and the decrease of the R-value. By increasing the DZV value sensitivity, the FN alarms are decreased and the FP alarms are increased as well. There is also an inverse relationship between the CR and the R-values. The higher the value of the R, the lower the value of the CR. The best achieved CR is 97.93% for DZV = 20% and R = 7. The FP alarms have vanished in all DZV inflammation signals except for the DZV signal = 10% that records 0.87% FP alarms. By increasing the DZV value sensitivity to 10%, FN alarms are minimized until it reaches 0%.

The DT-DIDS can be adapted to address different Database security systems with various R-values and DZV to achieve the required DR, FP, FN, and CR. By using DZV = 10% which is considered as the highest degree of sensitivity, the best-balanced results are obtained with R = 8 into which the DR achieved 98.2% while FP and FN rates achieved 0.87% and 1.8% respectively. By comparing the performance of the DT-DIDS among other different models with various techniques other than the DT, we obtain a high DR with low FP and low FN as well. Indeed, the combination of the NSA and the DT is considered as a promising mechanism to detect insider intrusions and deviations for preventing and mitigating data breaches in database systems.

According to the conducted survey in this paper, we believe that database intrusion detection systems with immunity features should have the ability to achieve the following three concepts: aggregation, integration, and individualization. For aggregation, the immunity-based database intrusion detection systems should be aggregated from different artificial immune system mechanisms such as the Negative Selection Algorithm, the Clonal Selection Algorithm, the DT model, the Dendritic Cell Algorithm, the Natural Killer cells, Toll-like Receptor Algorithm, and Artificial Immune

Network Algorithm. The more used mechanisms for the aggregation process as in the BIS, the better the results of the intrusion detection process. As the immune system integrates with other systems in the biological body, the immune inspired database intrusion detection should integrate with other intrusion detection systems such as network-based intrusion detection and host-based intrusion detection. Therefore, the integration concept is achieved. For individualization, each immune-based database intrusion detection system should have his individual parameters and configurations. This concept is to simulate the uniqueness of each biological body to detect and prevent intrusions.

The Danger Theory-based intrusion detection systems are used in different environments such as Networks, WSNs, Autonomous Communication Network, Heterogeneous Networks, Virtual Machines (VMs) of Cloud Environment, and Mobile Ad-hoc Networks (MANETs). Vehicular ad-hoc networks (VANETs) are a subclass of MANETs where it is established by moving or stationary vehicles coupled with a wireless network. Accordingly, developing a Danger Theory-based intrusion detection system for securing VANETs could achieve satisfactory results in this area.

REFERENCES

[1] C.-M. Ou, "Host-based intrusion detection systems inspired by machine learning of agent-based artificial immune systems," in *Proc. IEEE Int. Symp. Innov. Intell. Syst. Appl. (INISTA)*, Jul. 2019, pp. 1–5, doi: 10.1109/INISTA.2019.8778269.

[2] F. Hosseinpour, K. A. Bakar, A. H. Hardoroudi, and N. Kazazi, "Survey on artificial immune system as a bio-inspired technique for anomaly based intrusion detection systems," in *Proc. Int. Conf. Intell. Netw. Collaborative Syst.*, Nov. 2010, pp. 323–324.

[3] L. N. de Castro, "Fundamentals of natural computing: An overview," *Phys. Life Rev.*, vol. 4, no. 1, pp. 1–36, Mar. 2007, doi: 10.1016/j.plrev.2006.10.002.

[4] C. Zhang and Z. Yi, "A danger theory inspired artificial immune algorithm for on-line supervised two-class classification problem," *Neurocomputing*, vol. 73, nos. 7–9, pp. 1244–1255, Mar. 2010, doi: 10.1016/j.neucom.2010.01.005.

[5] S. Mohapatra and P. M. Khilar, "Immune inspired fault diagnosis in wireless sensor network," in *Nature Inspired Computing for Wireless Sensor Networks* (Springer Tracts in Nature-Inspired Computing), D. De, A. Mukherjee, S. K. Das, and N. Dey, Eds. Singapore: Springer, 2020, pp. 103–116.

[6] T. Semwal and S. B. Nair, "An immuno-inspired distributed artificial classification system," in *Soft Computing for Problem Solving*, vol. 1138. Singapore: Springer, 2020, pp. 31–49.

[7] S. Schaust and H. Szczerbicka, "Artificial immune systems in the context of misbehavior detection," *Cybern. Syst.*, vol. 39, no. 2, pp. 136–154, Feb. 2008, doi: 10.1080/01969720701853434.

[8] W. F. A. El-Wahed, E. M. Zaki, and A. M. El-Refaey, "Artificial immune system based neural networks for solving multi-objective programming problems," *Egyptian Inform. J.*, vol. 11, no. 2, pp. 59–65, Dec. 2010, doi: 10.1016/j.eij.2010.10.002.

[9] W. Luo and X. Lin, "Recent advances in clonal selection algorithms and applications," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Nov./Dec. 2017, pp. 1–8.

[10] A. Tarakanov, "Immunocomputing for intelligent intrusion detection," *IEEE Comput. Intell. Mag.*, vol. 3, no. 2, pp. 22–30, May 2008.

[11] T. Oda and T. White, "Developing an immunity to spam," in *Proc. Genet. Evol. Comput. Conf. (GECCO)*, vol. 2723. Berlin, Germany: Springer, 2003, pp. 231–242.

[12] P. Wlodarczak, "Cyber immunity a bio-inspired cyber defense system," in *Proc. Int. Conf. Bioinf. Biomed. Eng. (IWBBIO)*. Cham, Switzerland: Springer, 2017, pp. 199–208.

[13] O. Igbe, T. Saadawi, and I. Darwish, "Digital immune system for intrusion detection on data processing systems and networks," U.S. Patent 10 609 057 B2, Mar. 31, 2020.

[14] V. F. Popentiu and A. Grigore, "Recent advances in artificial immune systems: Models, algorithms, and applications," in *Recent Developments in Intelligent Nature-Inspired Computing*, P. Srikanta, Ed. Hershey, PA, USA: IGI Global, 2017, pp. 92–114.

[15] J. R. Al-Enezi, M. F. Abbod, and S. Alsharhan, "Artificial immune systems-models, algorithms and applications," *Int. J. Res. Rev. Appl. Sci.*, vol. 3, no. 2, pp. 118–131, 2010.

[16] D. Dasgupta, S. Yu, and F. Nino, "Recent advances in artificial immune systems: Models and applications," *Appl. Soft Comput.*, vol. 11, no. 2, pp. 1574–1587, Mar. 2011, doi: 10.1016/j.asoc.2010.08.024.

[17] J. Zeng, T. Li, G. Li, and H. Li, "A new intrusion detection method based on antibody concentration," presented at the Intell. Comput. 5th Int. Conf. Emerg. Intell. Comput. Technol. Appl., Ulsan, South Korea, 2009.

[18] R. Zhang and X. Xiao, "An intrusion detection method based on changes of antibody concentration in immune response," *J. Inf. Process. Syst.*, vol. 15, no. 1, pp. 137–150, 2019.

[19] M. J. Antunes and M. E. Correia, "Self tolerance by tuning T-cell activation: An artificial immune system for anomaly detection," presented at the 5th Int. ICST Conf. Bio-Inspired Models Netw., Inf., Comput. Syst. (BIONETICS), Boston, MA, USA, 2012.

[20] R. Medzhitov, D. S. Schneider, and M. P. Soares, "Disease tolerance as a defense strategy," *Science*, vol. 335, no. 6071, pp. 936–941, Feb. 2012.

[21] G. Eberl and T. Pradeu, "Towards a general theory of immunity?" *Trends Immunol.*, vol. 39, no. 4, pp. 261–263, Apr. 2018.

[22] T. Pradeu and E. Vivier, "The discontinuity theory of immunity," *Sci. Immunol.*, vol. 1, no. 1, p. aag0479, Jul. 2016.

[23] H. Veiga-Fernandes and A. A. Freitas, "The S(c)ensory immune system theory," *Trends Immunol.*, vol. 38, no. 10, pp. 777–788, Oct. 2017.

[24] Z. Grossman, "Immunological paradigms, mechanisms, and models: Conceptual understanding is a prerequisite to effective modeling," *Frontiers Immunol.*, vol. 10, p. 2522, Nov. 2019.

[25] D. Dasgupta and D. Dasgupta, Ed., *Artificial Immune Systems and Their Applications*. Berlin, Germany: Springer, 1999.

[26] E. Hart and J. Timmis, "Application areas of AIS: The past, the present and the future," *Appl. Soft Comput.*, vol. 8, no. 1, pp. 191–201, Jan. 2008, doi: 10.1016/j.asoc.2006.12.004.

[27] S. Arannya, "Applications of artificial immune system: A review," *Int. J. Found. Comput. Sci. Technol.*, vol. 5, no. 1, pp. 35–46, Jan. 2015, doi: 10.5121/ijfcst.2015.5104.

[28] D. A. B. Fernandes, M. M. Freire, P. A. P. Fazendeiro, and P. R. M. Inácio, "Applications of artificial immune systems to computer security: A survey," *J. Inf. Secur. Appl.*, vol. 35, pp. 138–159, Aug. 2017.

[29] S. Singh, J. P. Singh, and G. Shrivastva, "A review: AIS based intrusion detection system," *Int. J. Inf. Technol.*, vol. 20, no. 1, 2014.

[30] B. Bejoy and S. Janakiraman, "Artificial immune system based intrusion detection systems—A comprehensive review," *Int. J. Comput. Eng. Technol.*, vol. 8, no. 1, pp. 85–95, 2017.

[31] I. Dutt, S. Borah, and I. Maitra, "Survey of bio-inspired techniques based on system resource usage in intrusion detection," *TEST Eng. Manage.*, vol. 82, pp. 5734–5738, Jan./Feb. 2020.

[32] H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, "A taxonomy and survey of intrusion detection system design techniques, network threats and datasets," 2018, *arXiv:1806.03517*. [Online]. Available: http://arxiv.org/abs/1806.03517

[33] S. M. Othman, N. T. Alsohybe, F. M. Ba-Alwi, and A. T. Zahary, "Survey on intrusion detection system types," *Int. J. Cyber-Secur. Digit. Forensics*, vol. 7, no. 4, pp. 444–463, 2018.

[34] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, p. 20, Dec. 2019.

[35] P. Wanda, "A survey of intrusion detection system," *Int. J. Inform. Comput.*, vol. 1, no. 1, pp. 1–10, 2020.

[36] D. Mangla and H. Gupta, "Application based intrusion detection system," *Int. J. Control Theory Appl.*, vol. 9, no. 20, pp. 391–397, 2016.

[37] R. J. Santos, J. Bernardino, and M. Vieira, "Approaches and challenges in database intrusion detection," *ACM SIGMOD Rec.*, vol. 43, no. 3, pp. 36–47, Dec. 2014, doi: 10.1145/2694428.2694435.

[38] A. Thusoo and G. Jethava, "A survey: Intrusion detection system for database using data mining techniques," *Int. J. Eng. Res. Gen. Sci.*, vol. 3, no. 2, pp. 362–369, 2015.

[39] D. Nandasana and V. Barot, "A framework for database intrusion detection system," in *Proc. Int. Conf. Global Trends Signal Process., Inf. Comput. Commun. (ICGTSPICC)*, Dec. 2016, pp. 74–78.

[40] Y. Park and J. Park, "Web application intrusion detection system for input validation attack," in *Proc. 3rd Int. Conf. Converg. Hybrid Inf. Technol.*, vol. 2, Nov. 2008, pp. 498–504.

[41] V. Jyothsna and K. M. Prasad, "Anomaly-based intrusion detection system," in *Computer and Network Security*. London, U.K.: IntechOpen, 2019.

[42] U. Aickelin and J. Greensmith, "Sensing danger: Innate immunology for intrusion detection," *Inf. Secur. Tech. Rep.*, vol. 12, no. 4, pp. 218–227, 2007.

[43] 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," *J. Netw. Comput. Appl.*, vol. 157, May 2020, Art. no. 102537, doi: 10.1016/j.jnca.2020.102537.

[44] C. Chatterjee and D. D. Sokol, "Data security, data breaches, and compliance," in *Cambridge Handbook on Compliance*, D. D. Sokol and B. van Rooij, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2019.

[45] F. S. Khan, J. H. Kim, R. L. Moore, and L. Mathiassen, "Data breach risks and resolutions: A literature synthesis," in *Proc. 25th Amer. Conf. Inf. Syst. (AMCIS)*, Cancún, Mexico, 2019, pp. 1–10.

[46] A. M. Algarni and Y. K. Malaiya, "A consolidated approach for estimation of data security breach costs," in *Proc. 2nd Int. Conf. Inf. Manage. (ICIM)*, May 2016, pp. 26–39.

[47] R. Syed, "Enterprise reputation threats on social media: A case of data breach framing," *J. Strategic Inf. Syst.*, vol. 28, no. 3, pp. 257–274, Sep. 2019.

[48] D. McDaniel. (2019). *Data Breaches: Who is Behind them, Why they do it, and How to Protect Your Data*. [Online]. Available: http://www.infosecwriters.com/Papers/dmcdaniel_databreaches.pdf

[49] M. Rai and H. Mandoria, "A study on cyber crimes, cyber criminals and major security breaches," *Int. Res. J. Eng. Technol.*, vol. 6, no. 7, pp. 1–8, 2019.

[50] R. Adlakha, S. Sharma, A. Rawat, and K. Sharma, "Cyber security goal's, issue's, categorization & data breaches," in *Proc. Int. Conf. Mach. Learn., Big Data, Cloud Parallel Comput. (COMITCon)*, 2019, pp. 397–402.

[51] A. Brahma and S. Panigrahi, "Database intrusion detection using adaptive resonance network theory model," in *Computational Intelligence in Data Mining*. Singapore: Springer, 2020, pp. 243–250.

[52] S. Jain and D. Chawla, "A relative study on different database security threats and their security techniques," *Int. J. Innov. Sci. Res. Technol.*, vol. 5, no. 5, pp. 794–799, 2020.

[53] M. A. Hashem, I. M. El-Henawy, and A. M. Mostafa, "Database security—Mechanisms, techniques, breaches, and new directions," presented at the Int. Arab Conf. e-Technol. (IACe-T), 2012.

[54] M. A. Hashem, I. M. El-Henawy, and A. M. Mostafa, "Interactive multilayer policies for securing relational databases," in *Proc. Int. Conf. Inf. Soc. (i-Soc.)*, Jun. 2012, pp. 65–70.

[55] A. M. Mostafa, M. H. Abdel-Aziz, and I. M. El-Henawy, "Design and implementation of multi-layer policies for database security," *Inf. Sci. Lett.*, vol. 2, no. 3, pp. 147–153, Sep. 2013.

[56] A. M. Mostafa, M. H. Abdel-Aziz, and I. M. El-Henawy, "Design and implementation of extensible service-oriented algorithms for securing relational databases," *Int. J. Digit. Content Technol. Appl.*, vol. 7, no. 5, pp. 753–763, Mar. 2013.

[57] S. Bala, "Cloud computing and database security," *Int. J. Adv. Stud. Ecol., Develop. Sustainability*, vol. 6, no. 1, pp. 47–55, 2019.

[58] R. Jindal and I. Singh, "A survey on database intrusion detection: Approaches, challenges and application," *Int. J. Intell. Eng. Inform.*, vol. 7, no. 6, pp. 559–592, 2019.

[59] M. I. Khan, B. O'Sullivan, and S. N. Foley, "A semantic approach to frequency based anomaly detection of insider access in database management systems," in *Proc. Int. Conf. Risks Secur. Internet Syst.* Cham, Switzerland: Springer, 2018, pp. 18–28.

[60] M. Solanki and T. Phutane, "An innovative recipe for intrusion detection in relational databases using mean-shift clustering and C 4.5 algorithm," *Int. J. Res. Eng., Sci. Manage.*, vol. 1, no. 11, pp. 579–582, 2018.

[61] R. Ramachandran, R. Nidhin, and P. P. Shogil, "Anomaly detection in role administered relational databases—A novel method," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2018, pp. 1017–1021.

[62] S. Seo and S.-B. Cho, "Applying accuracy-based LCS to detecting anomalous database access," in *Proc. Genet. Evol. Comput. Conf. Companion*, Jul. 2018, pp. 1442–1448.

[63] S. Jayaprakash and K. Kandasamy, "Database intrusion detection system using octraplet and machine learning," in *Proc. 2nd Int. Conf. Inventive Commun. Comput. Technol. (ICICCT)*, Apr. 2018, pp. 1413–1416.

[64] C. Hagen, A. Dmitrienko, L. Iffländer, M. Jobst, and S. Kounev, "Efficient and effective ransomware detection in databases," presented at the Annu. Comput. Secur. Appl. Conf. (ACSAC), 2018.

[65] A. M. Mostafa, F. A. Almutairi, and M. Hassan, "False alarm reduction scheme for database intrusion detection system," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 10, pp. 1–10, 2018.

[66] S. B. Wankar, "Implementation of log mining and forensic analysis for database intrusion detection and protection system," Tech. Rep., 2018.

[67] M. I. Khan, B. O'Sullivan, and S. N. Foley, "Towards modelling insiders behaviour as rare behaviour to detect malicious RDBMS access," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2018, pp. 3094–3099.

[68] A. Brahma, S. Panigrahi, and J. Mahapatra, "A hybrid database intrusion detection algorithm using swarm intelligence and radial basis function network," *Helix Sci. Explorer*, vol. 9, no. 3, pp. 5031–5035, Jun. 2019.

[69] S. Subudhi and S. Panigrahi, "Application of OPTICS and ensemble learning for database intrusion detection," *J. King Saud Univ.-Comput. Inf. Sci.*, May 2019.

[70] S. Subudhi, "Application specific database intrusion detection using data mining techniques," Ph.D. dissertation, Dept. Comput. Sci. Eng., Veer Surendra Sai Univ. Technol., Burla, India, 2019.

[71] T.-Y. Kim and S.-B. Cho, "CNN-LSTM neural networks for anomalous database intrusion detection in RBAC-administered model," in *Proc. Int. Conf. Neural Inf. Process.* Cham, Switzerland: Springer, 2019, pp. 131–139.

[72] C. Bakir, V. Hakkoymaz, B. Diri, and M. Güçlü, "Comparisons on intrusion detection and prevention systems in distributed databases," *Balkan J. Electr. Comput. Eng.*, vol. 7, no. 4, pp. 446–455, Oct. 2019, doi: 10.17694/bajece.605134.

[73] T. Le, W. Mitchell, and B. Arad, "Customized intrusion detection based on a database audit log," in *Proc. 34th Int. Conf. Comput. Appl.*, vol. 58, 2019, pp. 117–126.

[74] M. Hasan, Z. Balbahaith, and M. Tarique, "Detection of SQL injection attacks: A machine learning approach," in *Proc. Int. Conf. Electr. Comput. Technol. Appl. (ICECTA)*, Nov. 2019, pp. 1–6.

[75] S.-J. Bu and S.-B. Cho, "Genetic algorithm-based deep learning ensemble for detecting database intrusion via insider attack," in *Proc. Int. Conf. Hybrid Artif. Intell. Syst.* Cham, Switzerland: Springer, 2019, pp. 145–156.

[76] S.-J. Bu and S.-B. Cho, "A convolutional neural-based learning classifier system for detecting database intrusion via insider attack," *Inf. Sci.*, vol. 512, pp. 123–136, Feb. 2020.

[77] L. Iffländer, A. Dmitrienko, C. Hagen, M. Jobst, and S. Kounev, "Hands off my database: Ransomware detection in databases through dynamic analysis of query sequences," 2019, *arXiv:1907.06775*. [Online]. Available: http://arxiv.org/abs/1907.06775

[78] Y. Zhou, "Intrusion detection method of marine ecological database under weak association rules," *Ekoloji*, vol. 28, no. 107, pp. 1789–1795, 2019.

[79] A. Sallam and E. Bertino, "Techniques and systems for anomaly detection in database systems," in *Policy-Based Autonomic Data Governance*. Cham, Switzerland: Springer, 2019, pp. 113–133.

[80] S. S. Srivastava, M. Atre, S. Sharma, R. Gupta, and S. K. Shukla, "Verity: Blockchains to detect insider attacks in DBMS," 2019, *arXiv:1901.00228*. [Online]. Available: http://arxiv.org/abs/1901.00228

[81] R. K. Sahu and S. Panigrahi, "Application of deep learning for database intrusion detection," in *Advanced Computing and Intelligent Engineering*. Singapore: Springer, 2020, pp. 501–511.

[82] A. Brahma and S. Panigrahi, "Role of soft outlier analysis in database intrusion detection," in *Advanced Computing and Intelligent Engineering*. Singapore: Springer, 2020, pp. 479–489.

[83] L.-X. Peng and T.-W. Chen, "Automated intrusion response system algorithm with danger theory," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery*, Oct. 2014, pp. 31–34.

[84] W. Wang, P. Zhang, and Y. Tan, "An immune concentration based virus detection approach using particle swarm optimization," presented at the 1st Int. Conf. Adv. Swarm Intell., Beijing, China, 2010, doi: 10.1007/978-3-642-13495-1_43.

[85] X. Zheng, Y. Fang, Y. Zhou, and J. Zhang, "A novel multi-layered immune network intrusion detection defense model: MINID," *J. Netw.*, vol. 8, no. 3, pp. 636–644, Mar. 2013.

[86] L. Fang, Q. Bo, and C. Rongsheng, "Intrusion detection based on immune clonal selection algorithms," presented at the 17th Austral. Joint Conf. Adv. Artif. Intell., Cairns, QLD, Australia, 2004, doi: 10.1007/978-3-540-30549-1_127.

[87] W. Tang, X.-M. Yang, X. Xie, L.-M. Peng, C.-H. Youn, and Y. Cao, "Avidity-model based clonal selection algorithm for network intrusion detection," in *Proc. IEEE 18th Int. Workshop Qual. Service (IWQoS)*, Jun. 2010, pp. 1–5.

[88] C. Yin, L. Ma, and L. Feng, "Towards accurate intrusion detection based on improved clonal selection algorithm," *Multimedia Tools Appl.*, vol. 76, no. 19, pp. 19397–19410, Oct. 2017, doi: 10.1007/s11042-015-3117-0.

[89] L. Ma, J. Qu, Y. Chen, and S. Wei, "An improved dynamic clonal selection algorithm using network intrusion detection," in *Proc. 14th Int. Conf. Comput. Intell. Secur. (CIS)*, Nov. 2018, pp. 250–253.

[90] D. Hooks, X. Yuan, K. Roy, A. Esterline, and J. Hernandez, "Applying artificial immune system for intrusion detection," in *Proc. IEEE 4th Int. Conf. Big Data Comput. Service Appl. (BigDataService)*, Mar. 2018, pp. 287–292.

[91] J. Greensmith, U. Aickelin, and S. Cayzer, "Detecting danger: The dendritic cell algorithm," in *Robust Intelligent Systems*, A. Schuster, Ed. London, U.K.: Springer, 2008, pp. 89–112.

[92] F. Gu, J. Greensmith, and U. Aicklein, "The dendritic cell algorithm for intrusion detection," in *Biologically Inspired Networking and Sensing: Algorithms and Architectures*, P. Lio and D. Verma, Eds. Hershey, PA, USA: IGI Global, 2012.

[93] X. Zheng and Y. Fang, "Principle and application of dendritic cell algorithm for intrusion detection," in *Proc. 3rd Int. Comput. Sci. Inf. Technol. (ICSPS)*, vol. 48. Singapore: International Association of Computer Science and Information Technology Press, 2012, pp. 85–91, doi: 10.7763/IPCSIT.2012.V48.15.

[94] M. Abdelhaq, R. Hassan, and R. Alsaqour, "Using dendritic cell algorithm to detect the resource consumption attack over MANET," in *Proc. Int. Conf. Softw. Eng. Comput. Syst. (ICSECS)*. Berlin, Germany: Springer, 2011, pp. 429–442.

[95] K. Kumari, "Intrusion detection technique based on dendritic cell algorithm and dempster belief theory," *IOSR J. Comput. Eng.*, vol. 1, no. 5, pp. 38–43, 2012.

[96] W. Guo and Y. Chen, "An improved dendritic cell algorithm based intrusion detection system for wireless sensor networks," *Int. J. Secur. Appl.*, vol. 11, no. 4, pp. 11–26, Apr. 2017, doi: 10.14257/ijsia.2017.11.4.02.

[97] A. Ahmad, N. B. Idris, and M. N. Kama, "Cloud intrusion detection model inspired by dendritic cell mechanism," *Int. J. Commun. Netw. Inf. Secur.*, vol. 9, no. 1, pp. 1–5, 2017.

[98] X. Xiao and R. Zhang, "Study of immune-based intrusion detection technology in wireless sensor networks," *Arabian J. Sci. Eng.*, vol. 42, no. 8, pp. 3159–3174, Aug. 2017, doi: 10.1007/s13369-017-2426-1.

[99] M. F. M. Mohsin, A. A. Bakar, A. R. Hamdan, and M. H. A. Wahab, "An improved artificial dendrite cell algorithm for abnormal signal detection," *J. Inf. Commun. Technol.*, vol. 17, no. 1, pp. 33–54, Jan. 2018.

[100] V. P. Sharma and R. Tiwari, "Immunity based intrusion detection system using probabilistic dendritic cell algorithm," *Int. J. Recent Res. Aspects*, vol. 5, no. 1, pp. 90–99, 2018.

[101] N. Elisa, L. Yang, X. Fu, and N. Naik, "Dendritic cell algorithm enhancement using fuzzy inference system for network intrusion detection," in *Proc. IEEE Int. Conf. Fuzzy Syst. (FUZZ-IEEE)*, Jun. 2019, pp. 1–6.

[102] E. Farzadnia, H. Shirazi, and A. Nowroozi, "A new intrusion detection system using the improved dendritic cell algorithm," 2020, *arXiv:2004.09274*. [Online]. Available: http://arxiv.org/abs/2004.09274

[103] M. A. Rassam, M. A. Maarof, and A. Zainal, "Intrusion detection system using unsupervised immune network clustering with reduced features," *Int. J. Advance Soft Comput. Appl.*, vol. 2, no. 3, pp. 244–263, 2010.

[104] M. A. Rassam and M. A. Maarof, "Artificial immune network clustering approach for anomaly intrusion detection," *J. Adv. Inf. Technol.*, vol. 3, no. 3, pp. 147–154, Aug. 2012.

[105] H. Yang, J. Guo, and F. Deng, "Collaborative RFID intrusion detection with an artificial immune system," *J. Intell. Inf. Syst.*, vol. 36, no. 1, pp. 1–26, Feb. 2011, doi: 10.1007/s10844-010-0118-3.

[106] X. Xiao and R. R. Zhang, "A network intrusion detection model based on artificial immune," *Adv. Mater. Res.*, vols. 361–363, pp. 687–690, Oct. 2011, doi: 10.4028/www.scientific.net/AMR.361-363.687.

[107] M. J. G. Antunes, M. E. Correia, and J. Carneiro, "Towards an immune-inspired temporal anomaly detection algorithm based on tunable activation thresholds," in *Proc. BIOSIGNALS*, 2009, pp. 357–362.

[108] M. Antunes and M. Correia, "TAT-NIDS: An immune-based anomaly detection architecture for network intrusion detection," in *Proc. 2nd Int. Workshop Practical Appl. Comput. Biol. Bioinf. (IWPACBB)*. Berlin, Germany: Springer, 2009, pp. 60–67.

[109] M. J. Antunes and M. E. Correia, "An artificial immune system for temporal anomaly detection using cell activation thresholds and clonal size regulation with homeostasis," in *Proc. Int. Joint Conf. Bioinf., Syst. Biol. Intell. Comput.*, 2009, pp. 323–326.

[110] M. J. Antunes and M. E. Correia, "Temporal anomaly detection: An artificial immune approach based on T cell activation, clonal size regulation and homeostasis," in *Advances in Computational Biology*, H. R. Arabnia, Ed. New York, NY, USA: Springer, 2010, pp. 291–298.

[111] M. Antunes and M. E. Correia, "Tunable immune detectors for behaviour-based network intrusion detection," in *Artificial Immune Systems*, P. Liò, G. Nicosia, and T. Stibor, Eds. Berlin, Germany: Springer, 2011, pp. 334–347.

[112] M. Antunes, C. Silva, B. Ribeiro, and M. Correia, "A hybrid AIS-SVM ensemble approach for text classification," in *Proc. Int. Conf. Adapt. Natural Comput. Algorithms (ICANNGA)*. Berlin, Germany: Springer, 2011, pp. 342–352.

[113] B. J. Bejoy and S. Janakiraman, "An intrusion detection and prevention system using AIS—An NK cell-based approach," in *Proc. Int. Conf. ISMAC Comput. Vis. Bio-Eng. (ISMAC)*. Cham, Switzerland: Springer, 2019, pp. 883–893.

[114] J. Fu, H. Yang, Y. Liang, and C. Tan, "Bait a trap: Introducing natural killer cells to artificial immune system for spyware detection," in *Artificial Immune System*. Berlin, Germany: Springer, 2012, pp. 125–138.

[115] Y. Melnikov and A. Tarakanov, "Immunocomputing model of intrusion detection," in *Computer Network Security*, V. Gorodetsky, L. Popyack, and V. Skormin, Eds. Berlin, Germany: Springer, 2003, pp. 453–456.

[116] V. D. Kotov and V. Vasilyev, "Immune model based approach for network intrusion detection," presented at the 3rd Int. Conf. Secur. Inf. Netw., Taganrog, Russian, 2010, doi: 10.1145/1854099.1854146.

[117] K. Chen, G. Chen, and J. Dong, "An immunity-based intrusion detection solution for database systems," in *Advances in Web-Age Information Management*. Berlin, Germany: Springer, 2005, pp. 773–778.

[118] X. Dong and X. Li, "An immune based relational database intrusion detection algorithm," in *Proc. 9th Int. Conf. Hybrid Intell. Syst.*, 2009, pp. 295–300.

[119] A. M. Mostafa, M. H. Abdel-Aziz, and I. M. El-Henawy, "Securing relational databases with an artificial immunity features," *Int. J. Comput. Appl.*, vol. 68, pp. 11–16, Apr. 2013.

[120] A. M. Mostafa, N. Yanes, and S. A. Alanazi, "A cognitive adaptive artificial immune algorithm for database intrusion detection systems," *J. Theor. Appl. Inf. Technol.*, vol. 97, no. 16, pp. 4387–4400, 2019.

[121] N. Yanes, A. M. Mostafa, N. O. Alshammari, and S. A. Alanazi, "An immunity-based error containment algorithm for database intrusion response systems," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 10, pp. 1–12, 2019.

[122] A. Khannous, A. Rghioui, F. Elouaai, and M. Bouhorma, "MANET security: An intrusion detection system based on the combination of negative selection and danger theory concepts," in *Proc. Int. Conf. Next Gener. Netw. Services (NGNS)*, May 2014, pp. 88–91.

[123] F. Hashim, K. S. Munasinghe, and A. Jamalipour, "On the negative selection and the danger theory inspired security for heterogeneous networks," *IEEE Wireless Commun.*, vol. 19, no. 3, pp. 74–84, Jun. 2012.

[124] M. E. Pamukov, "Application of artificial immune systems for the creation of IoT intrusion detection systems," in *Proc. 9th IEEE Int. Conf. Intell. Data Acquisition Adv. Comput. Syst., Technol. Appl. (IDAACS)*, vol. 1, Sep. 2017, pp. 564–568.

[125] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, "Self-nonself discrimination in a computer," in *Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy*, May 1994, pp. 202–212.

[126] F. González, D. Dasgupta, and J. Gómez, "The effect of binary matching rules in negative selection," in *Proc. Genet. Evol. Comput. Conf. (GECCO)*. Berlin, Germany: Springer, 2003, pp. 195–206.

[127] Z. Ji and D. Dasgupta, "Revisiting negative selection algorithms," *Evol. Comput.*, vol. 15, no. 2, pp. 223–251, Jun. 2007, doi: 10.1162/evco.2007.15.2.223.

[128] A. Lasisi, R. Ghazali, and T. Herawan, "Negative selection algorithm: A survey on the epistemology of generating detectors," in *Proc. 1st Int. Conf. Adv. Data Inf. Eng. (DaEng)*. Singapore: Springer, 2013, pp. 167–176.
[129] C. Ramdane and S. Chikhi, "Negative selection algorithm: Recent improvements and its application in intrusion detection system," *Int. J. Comput. Acad. Res.*, vol. 6, no. 2, pp. 20–30, 2017.
[130] E. Farzadnia, H. Shirazi, and A. Nowroozi, "A novel sophisticated hybrid method for intrusion detection using the artificial immune system," Tech. Rep., Apr. 2020.
[131] M. M. Karataş, "Malicious user input detection on Web-based attacks with the negative selection algorithm," M.S. thesis, Cyber Secur., Middle East Tech. Univ., Ankara, Turkey, 2019.
[132] K. Igawa and H. Ohashi, "A negative selection algorithm for classification and reduction of the noise effect," *Appl. Soft Comput.*, vol. 9, no. 1, pp. 431–438, Jan. 2009, doi: 10.1016/j.asoc.2008.05.003.
[133] A. Barontini, R. Perera, M. G. Masciotta, P. Amado-Mendes, L. Ramos, and P. Lourenço, "Deterministically generated negative selection algorithm for damage detection in civil engineering systems," *Eng. Struct.*, vol. 197, Oct. 2019, Art. no. 109444, doi: 10.1016/j.engstruct.2019.109444.
[134] O. Igbe, O. Ajayi, and T. Saadawi, "Detecting denial of service attacks using a combination of dendritic cell algorithm and the negative selection algorithm," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, Nov. 2017, pp. 72–77.
[135] N. Rashid, J. Iqbal, F. Mahmood, A. Abid, U. S. Khan, and M. I. Tiwana, "Artificial immune system–negative selection classification algorithm (NSCA) for four class electroencephalogram (EEG) signals," *Frontiers Hum. Neurosci.*, vol. 12, p. 439, Nov. 2018, doi: 10.3389/fnhum.2018.00439.
[136] N. A. Seresht and R. Azmi, "MAIS-IDS: A distributed intrusion detection system using multi-agent AIS approach," *Eng. Appl. Artif. Intell.*, vol. 35, pp. 286–298, Oct. 2014, doi: 10.1016/j.engappai.2014.06.022.
[137] O. Igbe, I. Darwish, and T. Saadawi, "Distributed network intrusion detection systems: An artificial immune system approach," in *Proc. IEEE 1st Int. Conf. Connected Health, Appl., Syst. Eng. Technol. (CHASE)*, Jun. 2016, pp. 101–106.
[138] X. Cao, H. Qiao, and Y. Xu, "Negative selection based immune optimization," *Adv. Eng. Softw.*, vol. 38, no. 10, pp. 649–656, Oct. 2007, doi: 10.1016/j.advengsoft.2006.11.006.
[139] J. C. Silva, F. P. A. Lima, A. D. P. Lotufo, and J. M. M. C. P. Batista, "Artificial immune system with negative selection applied to facial biometry based on binary pattern characteristics," *Int. J. Artif. Intell. Tools*, vol. 28, no. 1, Feb. 2019, Art. no. 1950005, doi: 10.1142/s0218213019500052.
[140] Y. A. Mohamed and A. B. Abdullah, "Implementation of IDS with response for securing MANETs," in *Proc. Int. Symp. Inf. Technol.*, Jun. 2010, pp. 660–665.
[141] F. Barani and M. Abadi, "BeeID: Intrusion detection in AODV-based MANETs using artificial bee colony and negative selection algorithms," *ISC Int. J. Inf. Secur.*, vol. 4, no. 1, pp. 25–39, 2012, doi: 10.22042/isecure.2015.4.1.4.
[142] K. Song, P. Kim, S. Rajasekaran, and V. Tyagi, "Artificial immune system (AIS) based intrusion detection system (IDS) for smart grid advanced metering infrastructure (AMI) networks," Virginia Polytech. Inst. State Univ., Blacksburg, VA, USA, Tech. Rep., 2018, vol. 24061. [Online]. Available: https://vtechworks.lib.vt.edu/handle/10919/83203
[143] M. Zeeshan, H. Javed, A. Haider, and A. Khan, "An immunology inspired flow control attack detection using negative selection with R-contiguous bit matching for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 11, Nov. 2015, Art. no. 169654, doi: 10.1155/2015/169654.
[144] Y. Liu and F. Yu, "Immunity-based intrusion detection for wireless sensor networks," in *Proc. IEEE Int. Joint Conf. Neural Netw., IEEE World Congr. Comput. Intell.*, Jun. 2008, pp. 439–444.
[145] F. Zhang and Y. Ma, "Integrated negative selection algorithm and positive selection algorithm for malware detection," in *Proc. Int. Conf. Prog. Informat. Comput. (PIC)*, Dec. 2016, pp. 605–609.
[146] K. Wawryn and P. Widulinski, "A human immunity inspired algorithm to detect infections in a computer program," in *Proc. 26th Int. Conf. Mixed Design Integr. Circuits Syst. (MIXDES)*, Jun. 2019, pp. 381–385.
[147] X. Z. Gao, S. J. Ovaska, and X. Wang, "Negative selection algorithm with applications in motor fault detection," in *Soft Computing Applications in Industry*, B. Prasad, Ed. Berlin, Germany: Springer, 2008, pp. 93–115.
[148] D. Dasgupta and S. Saha, "A biologically inspired password authentication system," presented at the 5th Annu. Workshop Cyber Secur. Inf. Intell. Res. Cyber Secur. Inf. Intell. Challenges Strategies (CSIIRW), Oak Ridge, TN, USA, 2009, doi: 10.1145/1558607.1558654.
[149] A. J. Saleh, A. Karim, B. Shanmugam, S. Azam, K. Kannoorpatti, M. Jonkman, and F. D. Boer, "An intelligent spam detection model based on artificial immune system," *Information*, vol. 10, no. 6, p. 209, Jun. 2019, doi: 10.3390/info10060209.
[150] I. Idris and A. Selamat, "Negative selection algorithm in artificial immune system for spam detection," in *Proc. Malaysian Conf. Softw. Eng.*, Dec. 2011, pp. 379–382.
[151] W. Ma, D. Tran, and D. Sharma, "A novel spam email detection system based on negative selection," in *Proc. 4th Int. Conf. Comput. Sci. Converg. Inf. Technol.*, 2009, pp. 987–992.
[152] R. Chikh and S. Chikhi, "Clustered negative selection algorithm and fruit fly optimization for email spam detection," *J. Ambient Intell. Hum. Comput.*, vol. 10, no. 1, pp. 143–152, Jan. 2019, doi: 10.1007/s12652-017-0621-2.
[153] X. Hang and H. Dai, "Applying both positive and negative selection to supervised learning for anomaly detection," presented at the 7th Annu. Conf. Genet. Evol. Comput., Washington, DC, USA, 2005, doi: 10.1145/1068009.1068064.
[154] W. Ma, D. Tran, and D. Sharma, "Negative selection as a means of discovering unknown temporal patterns," *Int. J. Biomed. Biol. Eng.*, vol. 41, no. 5, pp. 226–232, 2010. [Online]. Available: https://publications.waset.org/pdf/2600.
[155] V. T. Nguyen, T. T. Nguyen, K. T. Mai, and T. D. Le, "A combination of negative selection algorithm and artificial immune network for virus detection," in *Future Data and Security Engineering*. Cham, Switzerland: Springer, 2014, pp. 97–106.
[156] J. Kim and P. J. Bentley, "An evaluation of negative selection in an artificial immune system for network intrusion detection," presented at the 3rd Annu. Conf. Genet. Evol. Comput., San Francisco, CA, USA, 2001.
[157] T. Stibor, "On the appropriateness of negative selection for anomaly detection and network intrusion detection," Ph.D. dissertation, Fachbereich Informatik, Technischen Univ. Darmstadt, Darmstadt, Germany, 2006.
[158] A. Sayed A. Aziz, A. T. Azar, A. E. Hassanien, and S. E.-O. Hanafy, "Negative selection approach application in network intrusion detection systems," 2014, *arXiv:1403.2716*. [Online]. Available: http://arxiv.org/abs/1403.2716
[159] A. Rajachandran and J. S. Anju, "A survey—Appropriateness of negative selection and genetic algorithm for network based intrusion detection," *Int. J. Adv. Res. Trends Eng. Technol.*, vol. 4, no. 6, pp. 1–7, 2017.
[160] W. Luo, R. Liu, H. Jiang, D. Zhao, and L. Wu, "Three branches of negative representation of information: A survey," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 2, no. 6, pp. 411–425, Dec. 2018.
[161] C. Yang, L. Jia, B.-Q. Chen, and H.-Y. Wen, "Negative selection algorithm based on antigen density clustering," *IEEE Access*, vol. 8, pp. 44967–44975, 2020.
[162] N. B. Aissa, M. Guerroumi, and A. Derhab, "NSNAD: Negative selection-based network anomaly detection approach with relevant feature subset," *Neural Comput. Appl.*, vol. 32, no. 8, pp. 3475–3501, Apr. 2020, doi: 10.1007/s00521-019-04396-2.
[163] D. Sharma and S. S. Bhadauria, "Intrusion detection using negative selection based neural network algorithm," *Int. J. Sci. Technol. Res.*, vol. 8, no. 11, pp. 9–12, 2019.
[164] Y. Wang, T. Li, and F. Zhu, "Augmented negative selection algorithm with complete random subspace technique for anomaly detection," in *Proc. IEEE 2nd Int. Conf. Inf. Comput. Technol. (ICICT)*, Mar. 2019, pp. 1–4.
[165] R. Zhang and X. Xiao, "Intrusion detection in wireless sensor networks with an improved NSA based on space division," *J. Sensors*, vol. 2019, Apr. 2019, Art. no. 5451263, doi: 10.1155/2019/5451263.
[166] M. E. Pamukov, V. K. Poulkov, and V. A. Shterev, "Negative selection and neural network based algorithm for intrusion detection in IoT," in *Proc. 41st Int. Conf. Telecommun. Signal Process. (TSP)*, Jul. 2018, pp. 1–5.
[167] W. Guo, Y. Chen, Y. Cai, T. Wang, and H. Tian, "DIntrusion detection in WSN with an improved NSA based on the DE-CMOP," *KSII Trans. Internet Inf. Syst.*, vol. 11, no. 11, pp. 5574–5591, 2017, doi: 10.3837/tiis.2017.11.022.

[168] X. Zheng, Y. Zhou, and Y. Fang, "The dual negative selection algorithm and its application for network anomaly detection," *Int. J. Inf. Commun. Techol.*, vol. 11, no. 1, pp. 94–118, 2017, doi: 10.1504/ijict.2017.085464.

[169] M. E. Pamukov and V. K. Poulkov, "Multiple negative selection algorithm: Improving detection error rates in IoT intrusion detection systems," in *Proc. 9th IEEE Int. Conf. Intell. Data Acquisition Adv. Comput. Syst., Technol. Appl. (IDAACS)*, Sep. 2017, pp. 543–547.

[170] S. Sharma and R. K. Gupta, "A model for intrusion detection based on negative selection algorithm and J48 decision tree," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 5, no. 12, Dec. 2017 [Online]. Available: https://www.ijraset.com

[171] T. Yang, W. Chen, and T. Li, "A real negative selection algorithm with evolutionary preference for anomaly detection," *Open Phys.*, vol. 15, p. 13, Apr. 2017. [Online]. Available: https://ui.adsabs.harvard.edu/abs/2017OPhy..15..13Y

[172] Z. Liu, T. Li, J. Yang, and T. Yang, "An improved negative selection algorithm based on subspace density seeking," *IEEE Access*, vol. 5, pp. 12189–12198, 2017.

[173] F. Zhu, W. Chen, H. Yang, T. Li, T. Yang, and F. Zhang, "A quick negative selection algorithm for one-class classification in big data era," *Math. Problems Eng.*, vol. 2017, Jun. 2017, Art. no. 3956415, doi: 10.1155/2017/3956415.

[174] S. Fouladvand, A. Osareh, B. Shadgar, M. Pavone, and S. Sharafi, "DENSA: An effective negative selection algorithm with flexible boundaries for self-space and dynamic number of detectors," *Eng. Appl. Artif. Intell.*, vol. 62, pp. 359–372, Jun. 2017, doi: 10.1016/j.engappai.2016.08.014.

[175] S. Fouladvand, A. Osareh, and B. Shadgar, "Distribution estimation based negative selection algorithm (DENSA)," in *Proc. Int. Workshop Artif. Immune Syst. (AIS)*, Jul. 2015, pp. 1–7.

[176] D. Li, S. Liu, and H. Zhang, "Negative selection algorithm with constant detectors for anomaly detection," *Appl. Soft Comput.*, vol. 36, pp. 618–632, Nov. 2015, doi: 10.1016/j.asoc.2015.08.011.

[177] Y. Tao, M. Hu, and Y. Yu, "A novel negative selection algorithm for recognition problems," *Int. J. Hybrid Inf. Technol.*, vol. 8, no. 11, pp. 101–112, Nov. 2015.

[178] I. Idris and A. Selamat, "A swarm negative selection algorithm for email spam detection," *J. Comput. Eng. Inf. Technol.*, vol. 4, no. 1, pp. 1–4, 2015, doi: 10.4172/2324-9307.1000122.

[179] M. Majd, A. Hamzeh, and S. Hashemi, "A polymorphic convex hull scheme for negative selection algorithms," *Int. J. Innov. Comput., Inf. Control*, vol. 8, no. 5, pp. 2953–2964, 2012.

[180] Y. Wang and W. Luo, "PTS-RNSA: A novel detector generation algorithm for real-valued negative selection algorithm," in *Proc. Int. Joint Conf. Bioinf., Syst. Biol. Intell. Comput.*, Aug. 2009, pp. 577–583.

[181] X. Hang and H. Dai, "An extended negative selection algorithm for anomaly detection," in *Advances in Knowledge Discovery and Data Mining*. Berlin, Germany: Springer, 2004, pp. 245–254.

[182] F. González, "A study of articial immune systems applied to anomaly detection," Ph.D. dissertation, Univ. Memphis, Memphis, TN, USA, 2003.

[183] F. González, D. Dasgupta, and L. F. Niño, "A randomized real-valued negative selection algorithm," in *Artificial Immune Systems*. Berlin, Germany: Springer, 2003, pp. 261–272.

[184] Y.-J. Zhang, C.-Z. Hou, F. Wang, and L.-M. Su, "A niching negative selective genetic algorithm for self-nonself discrimination in a computer," in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 1, Nov. 2002, pp. 276–280.

[185] M. Ayara, J. Timmis, R. D. Lemos, L. N. D. Castro, and R. Duncan, "Negative selection: How to generate detectors," in *Proc. 1st Int. Conf. Artif. Immune Syst. (ICARIS)*, Canterbury, U.K., 2002, pp. 89–98.

[186] H. Yang, Y.-W. Liang, and J. Chen, "Definition of danger signal in artificial immune system with cloud method," in *Proc. 4th Int. Conf. Natural Comput.*, vol. 1, Oct. 2008, pp. 644–647.

[187] Y. He, L. Yiwen, L. Tao, and M. Bo, "A method inspired from differential coefficient for calculating danger signals in artificial immune system," in *Proc. Asia–Pacific Conf. Comput. Intell. Ind. Appl. (PACIIA)*, vol. 1, Nov. 2009, pp. 429–432.

[188] Y. He and X. Si, "Method for presenting danger signals based on system balance," in *Proc. Int. Conf. Adv. Mech. Eng. Ind. Inform.*, Apr. 2015, pp. 251–256, doi: 10.2991/ameii-15.2015.46.

[189] U. Aickelin and S. Cayzer, "The DT and its application to artificial immune systems," in *Proc. 1st Int. Conf. Artif. Immune Syst. (ICARIS)*, Canterbury, U.K., 2002.

[190] J. Greensmith, U. Aickelin, and S. Cayzer, "Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection," in *Artificial Immune Systems*. Berlin, Germany: Springer, 2005, pp. 153–167.

[191] D. Widhalm, "DT in sensor networks: Immune-inspired fault detection in wireless sensor networks," Univ. Appl. Sci. Technikum Wien, Vienna, Austria, Tech. Rep., 2020.

[192] X. Li and Y. Zhuang, "Anomaly detection algorithm based on DT," *J. Tsinghua Univ.*, vol. 52, no. 10, pp. 1370–1375, 2012.

[193] S. Amer and J. Leonard, "Danger theory concepts improving malware detection of intrusion detection systems that uses exact graphs," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2015, pp. 232–237.

[194] H. Zhang, T. Li, and Y. Wang, "A social network water army detection model based on artificial immunity," *J. Phys., Conf. Ser.*, vol. 1187, no. 5, Apr. 2019, Art. no. 052097, doi: 10.1088/1742-6596/1187/5/052097.

[195] X. Sun, Y. Zhao, and J. Cheng, "Study of rockbolts nondestructive detecting based on improved immune DT," in *Progress in Mine Safety Science and Engineering II*, H. M. X. He, B. Nie, Y. Wang, T. X. Ren, W. Chen, and X. Li, Eds. London, U.K.: CRC Press, pp. 269–273, vol. 20144.

[196] N. F. Sulaiman, Z. Jali, Z. H. Abdullah, and S. Ismail, "A study on the performances of DT and negative selection algorithms for mobile spam detection," *Adv. Sci. Lett.*, vol. 23, no. 5, pp. 4586–4590, 2017, doi: 10.1166/asl.2017.8887.

[197] M. Zamani, M. Movahedi, M. Ebadzadeh, and H. Pedram, "An artificial immune system for detecting DDoS attacks in wireless sensor networks," presented at the 14th Int. Comput. Soc. Iran Conf. (CSICC), Tehran, Iran, 2009. [Online]. Available: http://csicc2009.aut.ac.ir/

[198] S. Shamshirband, N. B. Anuar, M. L. M. Kiah, V. A. Rohani, D. Petković, S. Misra, and A. N. Khan, "Co-FAIS: Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 42, pp. 102–117, Jun. 2014, doi: 10.1016/j.jnca.2014.03.012.

[199] K. Zhang, "A danger model based anomaly detection method for wireless sensor networks," presented at the 2nd Int. Symp. Knowl. Acquisition Modeling, vol. 1, 2009, doi: 10.1109/KAM.2009.7.

[200] V. T. Alaparthy and S. D. Morgera, "A multi-level intrusion detection system for wireless sensor networks based on immune theory," *IEEE Access*, vol. 6, pp. 47364–47373, 2018.

[201] X. Xiao and R. Zhang, "A DT inspired protection approach for hierarchical wireless sensor networks," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 5, pp. 2732–2753, 2019, doi: 10.3837/tiis.2019.05.027.

[202] L. Li, L. Sun, and G. Wang, "An intrusion detection model based on DT for wireless sensor networks," *Int. J. Online Biomed. Eng.*, vol. 14, no. 9, pp. 53–65, 2018, doi: 10.3991/ijoe.v14i09.8625.

[203] S. Sarafijanović and J.-Y. Le Boudec, "An artificial immune system for misbehavior detection in mobile ad-hoc networks with virtual thymus, clustering, danger signal, and memory detectors," in *Proc. Int. Conf. Artif. Immune Syst. (ICARIS)*. Berlin, Germany: Springer, 2004, pp. 342–356.

[204] H. Fu, X. Yuan, and L. Hu, "Design of a four-layer model based on danger theory and AIS for IDS," in *Proc. Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Sep. 2007, pp. 6337–6340.

[205] H. Fu, X. Yuan, and N. Wang, "Multi-agents artificial immune system (MAAIS) inspired by danger theory for anomaly detection," in *Proc. Int. Conf. Comput. Intell. Secur. Workshops (CISW)*, Dec. 2007, pp. 570–573.

[206] C. Xu, X. Chen, H. Zhao, Y. Jiang, N. Liu, and T. Wang, "Research of DoS intrusion real-time detection based on DT," in *Proc. 1st Int. Symp. Data, Privacy, E-Commerce (ISDPE)*, Nov. 2007, pp. 209–211.

[207] W. Xiuying, X. Lizhong, and S. Zhiqing, "A danger-theory-based abnormal traffic detection model in local network," in *Proc. Int. Conf. Comput. Sci. Softw. Eng.*, vol. 3, Dec. 2008, pp. 943–946.

[208] S. Rawat and A. Saxena, "DT based SYN flood attack detection in autonomic network," presented at the 2nd Int. Conf. Secur. Inf. Netw., Famagusta, North Cyprus, 2009, doi: 10.1145/1626195.1626248.

[209] F. X. Sun and Z. G. Wu, "Immune danger theory based model for SYN flooding attack situation awareness," *Adv. Mater. Res.*, vols. 181–182, pp. 66–71, Jan. 2011, doi: 10.4028/www.scientific.net/AMR.181-182.66.

[210] A. Krizhanovsky and A. Marasanov, "An approach for adaptive intrusion prevention based on the danger," in *Proc. 2nd Int. Conf. Availability, Rel. Secur. (ARES)*, Apr. 2007, pp. 1135–1142.

[211] S. Gowda, D. Prajapati, R. Singh, and S. S. Gadre, "False positive analysis of software vulnerabilities using machine learning," in *Proc. IEEE Int. Conf. Cloud Comput. Emerg. Markets (CCEM)*, Nov. 2018, pp. 3–6.
[212] N. Chergui and N. Boustia, "Contextual-based approach to reduce false positives," *IET Inf. Secur.*, vol. 14, no. 1, pp. 89–98, Jan. 2020.

WAEL SAID (Member, IEEE) received the M.Sc. degree in computer science from Helwan University, in 2004, and the Ph.D. degree in computer science from Technical University Darmstadt, in 2011. He is currently an Assistant Professor with the Department of Computer Science, Faculty of Computers and Informatics, Zagazig University, and the Department of Computer Science, College of Computer Science and Engineering, Taibah University, Saudi Arabia. He has served as a Reviewer for many journals and conferences. His research interests include text and data mining, cloud and mobile computing, information and database security, cryptography, and cryptanalysis. He is also a member of the Syndicate of Scientific Professions in Egypt, and the Egyptian Software Engineers Association (ESEA).

AYMAN MOHAMED MOSTAFA (Member, IEEE) received the M.Sc. and Ph.D. degrees in information systems from the Faculty of Computers and Informatics, Zagazig University, Egypt. He is currently an Assistant Professor with the Faculty of Computers and Informatics, Zagazig University, and the College of Computer and Information Sciences, Jouf University, Saudi Arabia. He has published more than 20 scientific articles in various national and international journals and conferences. He is also an Oracle Certified Associate, an Oracle Certified Professional, and an EMC Academic Associate in Cloud Infrastructure and Services. His areas of interest include information security, cloud computing, E-business, E-commerce, big data, and data science.