

A COGNITIVE ADAPTIVE ARTIFICIAL IMMUNITY ALGORITHM FOR DATABASE INTRUSION DETECTION SYSTEMS

^{1,2} AYMAN MOHAMED MOSTAFA, ^{1,3} NACIM YANES, ¹ SAAD AWADH ALANAZI

¹ College of Computer and Information Sciences – Jouf University – KSA

² College of Computers and Informatics – Zagazig University - Egypt

³ RIADI Laboratory – La Manouba University - Tunisia

E-mail: ¹amhassane@ju.edu.sa, ²am_mostafa@zu.edu.eg, ¹nanacim@ju.edu.sa, ¹sanazi@ju.edu.sa

ABSTRACT

Applying artificial immune system in database security is a challenging trend to increase detection rate for internal intrusive users or administrators. Negative selection algorithm and danger theory are artificial immunity algorithms that provide promoting solutions for obtaining privacy-preserving data. This paper develops a mixed innate and adaptive immunity algorithm based on negative selection algorithm and danger theory to detect unknown intrusive users based on multi-layer pattern matching. A secret sharing mechanism is applied to monitor database administrators' transactions in a lowest possible time. The proposed immunity algorithm is based on a continuous cognitive adaptive methodology for using detected users as antigens for future faster response to unknown patterns. The key features of the presented immunity algorithm are its uniqueness for each detector, multi-layer detection and pattern matching, diversification in detecting unknown users at all levels of security, self-protection by using detected users as antigens for future detection process, and finally learning and memorization for storing previously detected users in antigen table to be used in pattern detection process. The conducted experimental results of the developed artificial immunity algorithm are compared to five algorithms and have achieved a high detection rate, low false positive and low false negative alarms.

Keywords: Database Security, Artificial Immune System, Negative Selection Algorithm, Danger Theory, and Secret Sharing

1. INTRODUCTION

Protecting the privacy and integrity of data with maintaining high detection rate with low false positive and false negative alarms, are major success factors for security systems. Different algorithms and techniques are used for obtaining data privacy such as access control mechanisms, cryptography, watermarking, and intrusion detection systems. These techniques are applied as stand-alone or integrated solutions for preventing unauthorized access from breaching system resources. Multiple access control mechanisms can be also applied based social relations model and the socio-technical design paradigm [1]. Based on the presented access control mechanism, the security policies of an application can be improved by applying different security layers that can maintain and fulfill data privacy with high detection coverage.

Artificial immune system (AIS) is one of the promoting solutions for maintaining data privacy. It is a comprehensive term that covers

the development of computational models inspired by biological immune systems. It can connect the disciplines of immunology, computer science and engineering [2]. The AIS can be defined as interconnected components that emulate the natural immune system (NIS) to achieve certain tasks [3]. The AIS can be applied in different domains such as anomaly detection, neural networks, signal processing, data analysis, and intrusion detection systems. The artificial immune system (AIS) consists of a set of detectors that are generated randomly and are used as immature detectors to be used in negative selection algorithms [4]. Negative selection algorithm (NSA) is considered one of the promoting algorithms in AIS that is used for anomaly detection, and network security. In the generation stage of negative selection algorithm, the detectors are generated by some random process and censored by trying to match self-samples. The matched candidates are eliminated, and the rest are kept as mature detectors [5]. The mature detectors will be used to detect malicious

intruders that attack the system. This means that self-samples should be correct regardless of whether they are complete or not. Even if self-samples are complete as well as correct, negative selection algorithm (NSA) still a probabilistic in most methods because it depends on data properties [5]. Danger theory (DT) is one of the recent algorithms of artificial immune system (AIS) which builds a danger signal around a defended area. Any attack within the defended area will raise a danger signal alarm.

One of the proposed mechanisms for building security applications is MANET [6]. This mechanism is used for intrusion detection system based on a combination of negative selection algorithm and danger theory. It collects signals from hosts or networks and correlates these signals to determine whether they are good or bad. This mechanism is completely different from the proposed immunity algorithm in this paper for different reasons. First: the MANET mechanism is used for intrusion detection systems in networks. Second: it did not provide a declarative infrastructure for the proposed mechanism. Third: this mechanism is just used for detector generation process. Fourth: the generation process is based on fixed length elements. Fifth: it did not provide experimental results to measure the accuracy of the mechanism.

As presented in [7], intrusion detection system monitors intrusive behaviors by collecting and analyzing users' records and data. Obtaining data privacy is based both identifier fields such as username, IP addresses and non-identifier fields such as URLs and time stamping. By applying artificial immune algorithms in intrusion detection system for protecting data from disclosure, high detection rate with low false positive and low false negative rates are obtained.

The main goal of this paper is to develop an artificial immune algorithm based on negative selection algorithm and danger theory to obtain an efficient, flexible, and solid security system for database applications by detecting intrusive users who try to get confidential information from the system.

Based on our previous papers presented in [8, 9, 10, 11, and 12], this paper presents a database security system which merges the merits, features, and capabilities of artificial immune system in order to provide an interactive security system that can be used in different real world applications. The developed artificial immune

algorithm is compared with the original negative selection algorithm, association rule mining, and sequential pattern mining and achieved high detection rate with low false positive and low false negative alarms. The contribution of this paper is as follows:

- Building an immunity-based system based on artificial immune system for securing relational databases.
- Eliminating the random generation of data by building an efficient learning mechanism.
- The developed immunity learning mechanism provides complete, efficient, and correct data with a variable length pattern that can be changed according to granted privileges.
- Developing hybrid detection algorithms based on negative selection algorithm and danger theory that can achieve high performance and high detection coverage.
- Reducing the false positive and false negative alarms of the developed security system.
- Better experimental results compared with five immunity algorithms for achieving high detection rate.

2. RELATED WORKS

Different cognitive techniques and algorithms have been developed for protecting data confidentiality such as database cryptography, access control mechanisms, watermarking techniques, intrusion detection and response systems, authentication, secret sharing, and secure data management [13]. Some of the proposed techniques can obtain confidentiality of information but with high false positive alarms while other techniques can obtain low false positive alarms but with a lower degree of data protection.

Most real time solved problems are inspired from nature. Artificial immune system (AIS) is considered the artificial simulation of natural immune system (NIS). The immune system has the responsibility to defend the human body from foreign and dangerous microorganisms called pathogens. To overcome these pathogens, the immune system depends on innate and adaptive immune subsystems [14]. The innate immune subsystem is considered the immutable first line of defense for alarming danger signals around suspicious item. The adaptive immune subsystem relies on a faster response to unknown detected patterns.

One of the most promoting features of human immune system is the ability to discriminate vast number of unknown patterns using limited number of antibodies. Retaining a memory for detected unknown patterns is considered another major concern for future faster response for unknown pathogens. Based on the innate and adaptive immune subsystems, the detection rate is considered the major concern in developing security applications.

Artificial immune systems (AISs) have been modeled on several research papers. As presented in [15], the authors stated that artificial immune systems (AISs) are considered complementary in regard to complex security problems. One of the main obstacles in applying AISs is the definition of balanced set of parameters for obtaining efficient detection rate. Different research methodologies complement intrusion detection system (IDS) with artificial immune system (AIS) for improving the detection rate of unknown patterns. As presented in [3], the authors monitor the increase of detector selection percentage with the size of training data set. To implement a novel solution using immunity-based systems, several steps must be executed starting from application domain, immune entities, representation, affinity measures, and finally immune algorithms such as negative selection algorithms.

In negative selection algorithm, a large set of detectors are generated randomly and matched with a set of self-samples. A matching process is performed between self-samples (S) and detectors (D) such that the matched detectors (D) will be deleted from the system and the non-matched detectors are kept as mature detectors. These mature detectors have the ability to detect malicious users or intruders in the system.

One of the advances in negative selection algorithm (NSA) was presented in [16]. In this research, the negative selection algorithm is used for detecting faults in the area of engineering processes. A novel negative selection algorithm was presented in [17]. In many actual anomaly detection systems, the training data are just partially composed of the normal elements, and the self/non-self space often varies over time. An optimized negative selection approach was presented in [18]. This research optimizes the negative selection algorithm to run faster using a filtering process for feature-by-feature process rather than comparing a new detector with self-samples. Another novel negative selection algorithm called r[-]NSA was presented in [19].

In this research, a detector has an array of partial matching lengths, while not just one partial matching length as previous NSAs. Negative selection algorithm can be used also in fault detection in mobile robot sensors [20]. The developed system consists of an environment that includes differential wheel robot equipped with four distance sensor of same type and three obstacles. The NSA can also be used in target identification by suggesting takeover targets for novice firms that are at the beginning of their merger and acquisition process [21].

One of the recent researches for applying negative selection algorithm (NSA) in intrusion detection systems (IDSs) was presented in [22]. The research focuses on applying two-tiered negative selection mechanism for implementing a co-stimulation approach to decrease the detection error rate.

Danger theory is based on danger signal approach in immune system. It is considered an innate immunity subsystem for creating danger signals around suspicious patterns. Danger theory (DT) postulates that the human immune systems respond to the presence of molecules known as danger signals, which are released as results of unnatural cell deaths. The danger signals inform the immune systems to initiate immune responses [2]. One of the recent researches in danger theory is presented in [23]. In this research, the danger theory is used in node replication attacks detection in wireless network. By using danger theory, good performance and results are achieved with minimum false positive rate. One of the recent researches for applying danger theory (DT) in artificial immune system was presented in [24]. The authors of that research apply a multi-layer intrusion detection system for wireless sensor networks to predict different types of attacks in a timely manner.

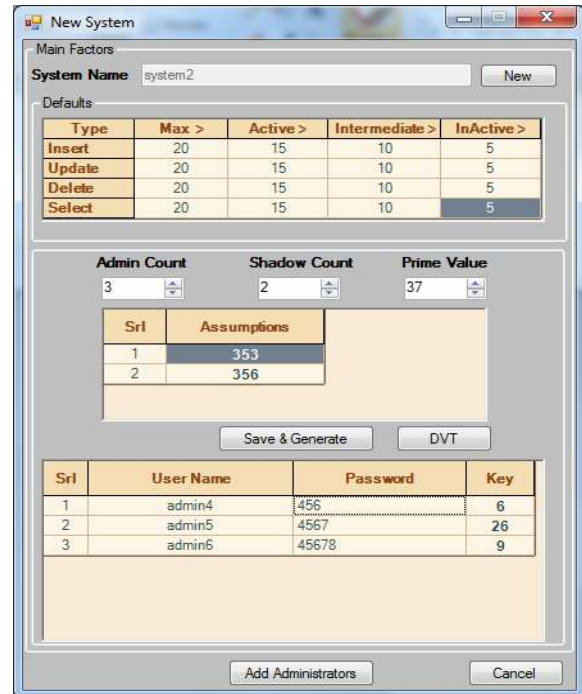
Although a number of advantages are claimed by the danger theory (DT), it has several limitations. First: the exact nature of the danger signal is unclear. Second: how to distinguish danger from non-danger [25]. One of our major contributions in this paper is to develop a database security system based on the danger theory (DT) of the artificial immune system (AIS). In the developed immune system, danger signals can be clarified and distinguished from non-danger signals in order to reduce false positive and false negative alarms.

3. DB IMMUNITY LEARNING PHASE

Based on our papers [8, 9, 10, 11, and 12] that present a package of interactive database security policies and architectures, the main goal of this paper is to provide an artificial immune security algorithm for preventing database administrators and users from performing any hostile. The learning mechanism in collects data based on a harmonious interaction between super administrator (SA), database administrators (DBAs), and authorized users instead of collect them randomly as in the original negative selection algorithm.

3.1 Super Admin Secret Sharing Mechanism

As presented in Figure 1, the super administrator (SA) manages all authorizations and capabilities to control and monitor database administrators, users, and transmissions through the database server. He can perform different operations inside the system. First: providing the maximum number of operations (insert-update-delete-select) allowed to each user to distinguish between active, intermediate and inactive user profiles. Second: determining the total number of database administrators (N DBAs) who can connect to the database system and the number of shadows (K DBAs) that must be available to provide a secret sharing process for every request from a single administrator. Third: providing each database administrator with a *username*, *password*, and a *secret key certificate*. The super administrator (SA) determines immunity parameters that will be embedded inside the developed immunity algorithms as follows:



Type	Max >	Active >	Intermediate >	InActive >
Insert	20	15	10	5
Update	20	15	10	5
Delete	20	15	10	5
Select	20	15	10	5

Srl	Assumptions
1	353
2	356

Srl	User Name	Password	Key
1	admin4	456	6
2	admin5	4567	26
3	admin6	45678	9

Figure 1: Immunity Learning Phase

3.1.1 Main danger value threshold (MDVT)

The main danger value threshold (MDVT) provides the amount of sensitivity to the security system. There is an inverse relationship between the MDVT value and the system sensitivity. If the super administrator (SA) wants to increase the sensitivity of the system to any hostile act, the MDVS must be decreased.

3.1.2 System privileges danger signals

The super administrator (SA) specifies a danger percentage value for DML system privileges. Each DML system privilege can take different danger value according to its dangerous and importance in the security system.

3.1.3 Database privileges Danger signals

As presented in Table 1, the super administrator (SA) specifies a danger value signal (DVS) for each database privilege that may be granted to users. These danger signals can be changed according to the values given by the super administrator. The authors of [26] presented a security model for access control based on a set of DDL and DML permissions. Each user is granted a set of authorities but it did not cover the sensitivity of each privilege to unauthorized patterns.

Table 1: Database Privileges

Database Privileges DVS			
Privilege	DVS	Privilege	DVS
Create Table	80%	Create Index	40%
Create View	70%	Create Synonym	10%
Create Function	50%	Create Procedure	50%
Create Sequence	10%	Alter Table	80%
Alter Index	40%	Alter View	70%
Alter Synonym	10%	Alter Function	50%
Alter Procedure	50%	Alter Sequence	10%

3.1.4 R-Contiguous bit matching (RCB) algorithm

The (RCB) matching algorithm will be used later in the proposed detection phase to detect unauthorized. Matching requirement is defined as R contiguous matching symbols in corresponding positions.

3.2 Database Administrator Level

Once the super administrator (SA) stores all database administrators' accounts, each database administrator can now access the database security system separately using his authentication parameters. The database administrator (DBA) performs different operations inside the system such as: building database users, building database roles based on system privileges and database privileges, granting roles to different users.

Finally, a user certificate authorization (UCA) is built to specify a secret key certificate for each created user to be used as a final countermeasure if unauthorized users succeed in breaching the security system defenses. The user certificate authorization (UCA) is a secret certificate encrypted using 128 bit AES encryption algorithm and is stored in the database server.

4. DATABASE IMMUNITY DETECTION ALGORITHM

Based on the database immunity learning phase, a novel adaptation of the danger theory (DT) is applied to the field of database security by developing a database immunity detection algorithm based on artificial immune negative selection algorithm (NSA) and danger theory (DT). The main algorithm is based on three signals: intruder recognition (Signal I), intruder detection (Signal II). The last signal which is considered the last line of defense contains the certificate confirmation (Signal III).

4.1 Signal I: Intruder Recognition

The first layer of security in the detection algorithm is to recognize malicious users or intruders by using two methods of recognition. As presented in Algorithm 1, the first mechanism is to check for a human being interaction using Captcha system to eliminate any computer-machine generators.

If the Captcha entry is valid, the security system brings all usernames and passwords that have been created by database administrators (DBAs) from the database server and puts them into "system cache".

If the user enters authentic username and password, the security system will move from danger signal I alarm to danger signal II alarm. If the user entry is invalid, the security system will initiate the danger signal I alarm.

Algorithm 1: Intruder Recognition

1. **If** Captcha is valid **Then**
2. {
3. Get all usernames and passwords from **Security. Users**
4. Put usernames and passwords into **system cache**
5. **If** entered username and password is authentic **Then**
6. {
7. Go to Danger Signal II // Second Algorithm
8. }
9. **Else**
10. {
11. Raise Danger Signal I Alarm
12. }
13. }

4.2 Signal II: Intruder Detection

The second layer of security depends on detecting malicious users who succeed in penetrating the first layer. Malicious users can perform a brute-force attack until a successful username and password are obtained.

The second layer of security depends on 18 bits factor matching mechanism includes 4 bits for DML system privileges (Select – Insert – Update – Delete) and 14 bits for database privileges as presented in Table 1. The predefined access control privileges are explained in Figure 2.

As shown, each privilege is checked will have a value of 1 while unchecked privileges will have a value of 0. This mechanism will be illustrated in formula (1).

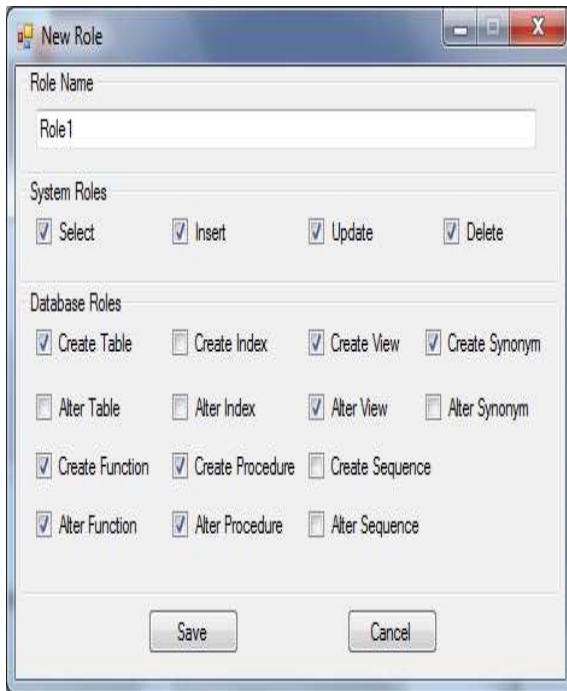


Figure 2: Database and System Privileges

When the database administrator (DBA) grants a privilege to a user, each granted privilege takes a value of 1, non-granted privilege takes a value of 0. This is presented in formula (1).

$$f(x) = \begin{cases} 1, & \text{if } x \text{ granted} \\ 0, & \text{if } x \text{ not granted} \end{cases} \quad (1)$$

Where x is the privilege created by the database administrator (DBA).

$$\text{System privilege (SP)} = \{ (X_s + X_i + X_u + X_d) \forall x \in f(x) \} \quad (2)$$

Where X_s is the select privilege, X_i is the insert privilege, X_u is the update privilege, and X_d is the delete privilege.

$$\text{Database privilege (DP)} = \{ (X_1 + X_2 + \dots + X_n) \forall x \in f(x) \} \quad (3)$$

Where X_1 to X_n are the database privileges as presented in Table 1.

The factor set combines both the system privileges and database privileges in the factor set as explained in formula (4).

$$\text{Factor set (FS)} = \text{System privilege (SP)} || \text{Database Privilege (DP)} \quad (4)$$

Each bit in the factor set (FS) has a dangerous value limit that has been identified by the super administrator (SA) to detect anomalous users based on the danger theory (DT).

As presented in Figure 3, the intruder detection algorithm is based on five nested stages. These stages are presented as follows:

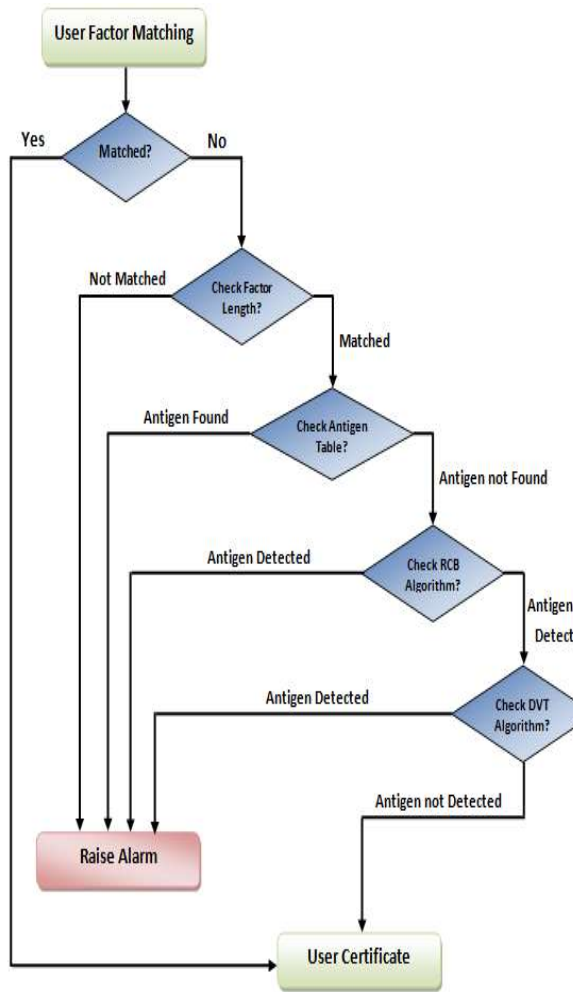


Figure 3: Intruder Detection Checking Mechanisms

4.2.1 Stage 1: verified factor authentication (VFA)

If the user passes danger signal I alarm, his authentication factor that has been created by the database administrator (DBA) is brought from the database server to the “system cache” and waits for the user to enter an authentic factor. The user must pass his 18 bits in a correct manner so as not to be detected as a malicious user. If the user passes his authentic factor, he can move to the last layer of security which is user certificate authorization (UCA); otherwise the security system will perform a set of serial checking mechanisms which are factor length matching, antigen table matching, RCB matching, and DVS matching.

4.2.2 Stage 2: factor length matching (FLM)

If the user fails in verifying his authentication factor, the first checking mechanism of the intruder detection algorithm is to match the privilege factor length with the user entry. Malicious users who try to penetrate the security system may not be aware about the number of privileges granted for each user.

If the factor length is not correct, the security system will raise the danger signal II alarm. Otherwise, the system will proceed to the next checking mechanism which is antigen table matching.

4.2.3 Stage 3: antigen table matching (ATM)

The developed antigen table is the learning and memorization stage that stores all previously detected users for performing fast detection response to unknown patterns. The security system searches the user factor in the antigen table to get a quick response instead of applying the detection algorithm. As a result, the time complexity for the detection process is reduced.

4.2.4 R-Contiguous bit matching

The value of R threshold is determined by the super administrator (SA) as presented in (Section 3.1.4). The security system traces each bit of the user factor and matches it with the authentic user factor stored in the “system cache”. As presented in Algorithm 2, the security system will raise

Algorithm 2: RCB Algorithm

1. Boolean isAntigen = False
2. Integer Counter = 0
3. For (i = 0; i < input factor. Length ; i ++)
4. {
5. If input factor [i] = valid factor [i] Then
6. {
7. Counter = Counter + 1 ;
8. If Counter = R Then
9. {
10. isAntigen = True
11. Raise Danger Signal II Alarm
12. }
13. }
14. Else
15. {
16. Counter = 0
17. }
18. }

danger signal **II** alarm if at least R-contiguous bits are matched in both authentic and fake factors. Otherwise, the security system will activate the second detection algorithm which is the danger value algorithm (DVS). Increasing the value of R will decrease both detection rate and false positive operations but will increase false negative operations as a result of the low detection rate. Decreasing the value of R will increase both detection rate and false positive operations but will decrease false negative operations as a result of high detection rate.

In order to achieve a high detection rate, low false positive and low false negative operations, the security system will activate the final detection algorithm which is based on the danger value threshold.

4.2.5 Stage 5: danger value signal (DVS) algorithm

The last detection algorithm in the developed security system is to initialize the danger value signal (DVS) algorithm. The main idea of this algorithm is to detect unauthorized users who succeed in passing the four previous detection mechanisms. In negative selection algorithm (NSA), the self-users (Normal users) and non-self-users (Malicious users) creates a universe such that:

$$S \cup N = U, \quad S \cap N = \emptyset \quad (5)$$

Where **S** is the self-users, **N** is the non-self-users, and **U** is the sample space (universe).

As presented in Algorithm 3, the main danger value threshold (MDVT) that has been identified by the super administrator (SA) is brought into the “system cache” and the counter of matched factors is initialized with 0.

The first operation is to build a **data dictionary table** that stores matched danger signals of the user factor that has been created by the database administrator (DBA) while the value of the danger signals is identified by the super administrator (SA).

The data dictionary table contains an **index** for the value of each matched danger signal. Each matching between the input factor of the user and the valid factor stored in the system cache; will store the danger value in the system index whether the matching was contiguous or not.

Each value from the danger signals stored in the system index is compared to main danger value threshold (MDVT) such that the value of each matched danger signal must be greater than or equal to the main danger value threshold (MDVT). This will increment the counter with 1 until the value of R is satisfied. If R is satisfied the algorithm will raise danger signal **II** alarm.

Algorithm 3: DVS Algorithm

1. **Boolean** isAntigen = **False**
2. **Integer** MainDVT = **System**. MainDVT
3. **Integer** DVsvalue
4. **Integer** Counter = 0
5. Build Data Dictionary table to store matched Danger Signals
6. **For** (i = 0; i < input factor. Length ; i ++)
7. {
8. **If** input factor [i] = valid factor [i] **Then**
9. {
10. **Get** the index for matched factor
11. indexMatch. **add** (i)
12. }
13. }
14. Loop at the indices form list
15. Get the item from the list
16. DVsvalue = itemDVS.Value
17. *Compare the value of the selected index to the MainDVT*
18. **If** DVsvalue >= MainDVS **Then**
19. {
20. Counter = Counter + 1
21. }
22. *Ensure whether the counter will be greater than or equal to R*
23. **If** Counter >= R **Then**
24. {
25. isAntigen = True
26. Raise Danger Signal II Alarm
27. }

4.3 Signal III: User Certificate Authorization (UCA)

If the user succeeds in passing the intruder recognition (Signal I) and intruder detection

(Signal II), the security system will activate the user certificate authorization that is considered the last line of defense. As presented in (Section 3.2), the user certificate authorization is a secret key that has been developed by the database administrator (DBA) as a final operation if the user succeeds in breaching the security system.

5. EXPERIMENTAL RESULTS

The adaptive artificial immunity system is developed using Microsoft Visual Studio.net community 2017 with Microsoft SQL Server 2012 database. The experimental results were conducted on an Intel(R) Core (TM) i5 CPU @ 1.28 GHz machine with 8 GB of RAM. The operating system was Microsoft Windows 10.

The immunity-based algorithms are compared with five different algorithms that have been presented in [27, 28, and 29]. Authors of [27], presents three algorithms for detecting unknown user behavior. The three algorithms are: association rule mining, sequential pattern mining, and immune based negative selection. The authors of [28] presented a novel method for database intrusion detection system based on profile creation, training phase, and detection phase.

The detection process is performed using class identified support vector machine (SVM). The results were recorded based on IDS DVD rental database. The authors of [29] presented an intrusion detection system framework for mining host log based on association rules, time series, and intrusion detection. The authors combined the three methodologies (ATI) and recorded the results. The results of the ATI mechanism were recorded based on the highest three values. The same testing data has been applied to the DVS inflammation algorithm to ensure the accuracy, efficiency and provable security.

The parameters of the DVS inflammation algorithm have been specified as $R=7$ and the Main DVS =10% high inflammation.

The value of R is set to 7 in order to reduce the false positive alarms and the DVS inflammation signal is set to 10% inflammation to make the artificial immune security system more sensitive

to any malicious users. By increasing the sensitivity of the system, the detection rate can be increased. The distribution of testing data is presented in Table 2.

Table 2: Testing Data Distribution

Data Groups	Normal Events	Abnormal Events
Group 1	387	165
Group 2	351	150
Group 3	227	108

As presented in Figure 4, the detection rate is calculated by dividing the total number of detected users (N_d) to the total number of examined users (N). This is presented in formula (6).

$$D_R = \frac{N_d}{N} \times 100\% \quad (6)$$

The DVS inflammation algorithm presented in the artificial immune security system proves a high detection rate when compared with the other five algorithms: immune based negative selection, association rule mining, sequential pattern mining, IDS rental database, and ATI. When applying the three data groups: group 1, group 2, and group 3; the detection rate of the DVS inflammation algorithm recorded 98.2%, 98.7%, and 98.1% respectively. The detection rate of negative selection algorithm recorded 92%, 92%, and 88% respectively. The detection rate of sequential pattern mining algorithm recorded 82%, 84%, and 81% respectively.

The detection rate of association rule mining algorithm recorded 84%, 85%, and 83% respectively. The detection rate of IDS rental database recorded 91.67%, 93.75%, and 95.45% respectively while the detection rate of ATI algorithm recorded low values of 75.6%, 79.1%, and 83.5% respectively.

Although the detection rate of the DVS inflammation algorithm is high when comparing to other security algorithms but the detection rate needs to be enforced by adding additional security layer in the intruder recognition phase.

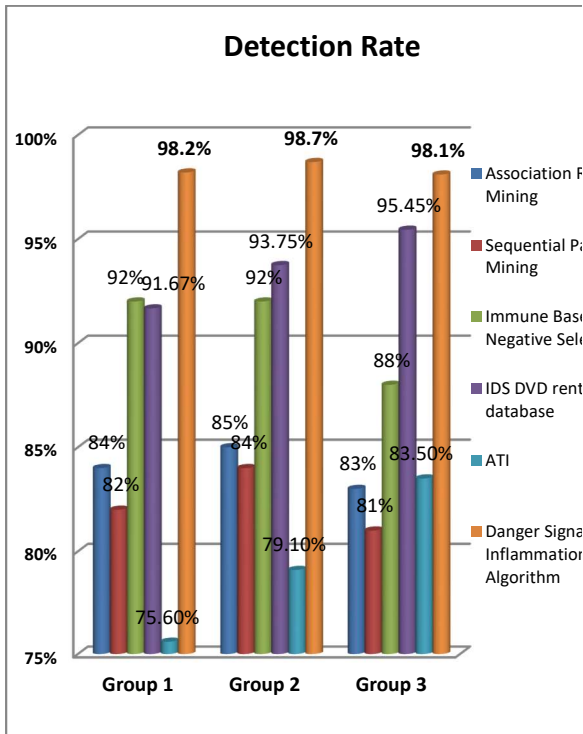


Figure 4: Detection rate Comparison

The false negative alarms (FN) are calculated by dividing the number of passed malicious users (N_p) to the total number of examined users (N). This is presented in formula (7).

$$F_N = \frac{N_p}{N} \times 100\% \quad (7)$$

As presented in Figure 5, the false negative alarms (FN) recorded low values due to the high detection rate. The percentage of false negative alarms refers to the number of malicious users who succeeded in passing the artificial immune security system. In Figure 5, the DVS inflammation algorithm presented in the artificial immune security system proves low false negative alarms when compared with the other four algorithms: negative selection algorithm, association rule mining, sequential pattern mining, and IDS rental DB. When applying the three data groups: group 1, group 2, and group 3; the false negative alarms of the DVS inflammation algorithm recorded 1.8%, 1.3%, and 1.9% respectively. The false negative alarms for negative selection algorithm recorded 8%, 8%, and 12% respectively.

The false negative alarms for sequential pattern mining algorithm recorded 18%, 16%, and 19% respectively. The false negative alarms for IDS rental DB recorded 8.33%, 6.25%, and 4.55% respectively while the false negative alarms of association rule mining algorithm recorded 16%, 15%, and 17% respectively.

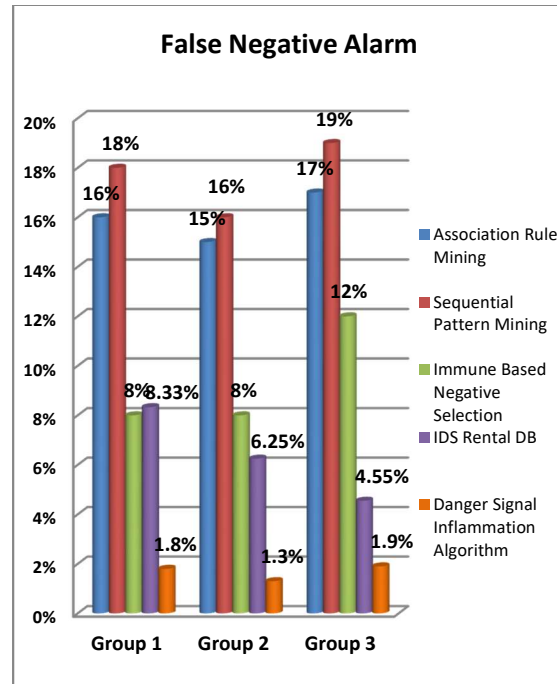


Figure 5: False Negative Alarms Comparison

False positive alarms (FP) refer to the probability that normal actions being alarmed as abnormal actions. This is presented in formula (8).

$$F_p = \frac{N_f}{N} \times 100\% \quad (8)$$

As presented in Figure 6, when applying the three data groups: group 1, group 2, and group 3; the false positive alarms (FP) of the proposed danger signal inflammation algorithm recorded 1%, 1%, and 0% respectively. The false positive alarms of negative selection algorithm recorded 1%, 1%, and 1% respectively. The false positive alarms of sequential pattern mining recorded 5%, 5%, and 7% respectively. Association rule mining algorithm recorded the highest false positive alarms by recording 13%, 13%, and 11% respectively. Finally, the IDS rental DB recorded false positive rate with 12.5%, 8.57%, and 7.78% respectively.

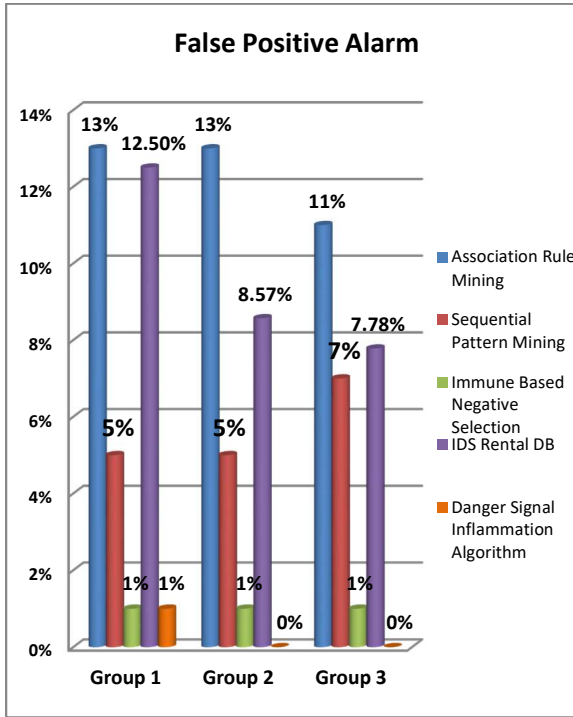


Figure 6: False Positive Alarms Comparison

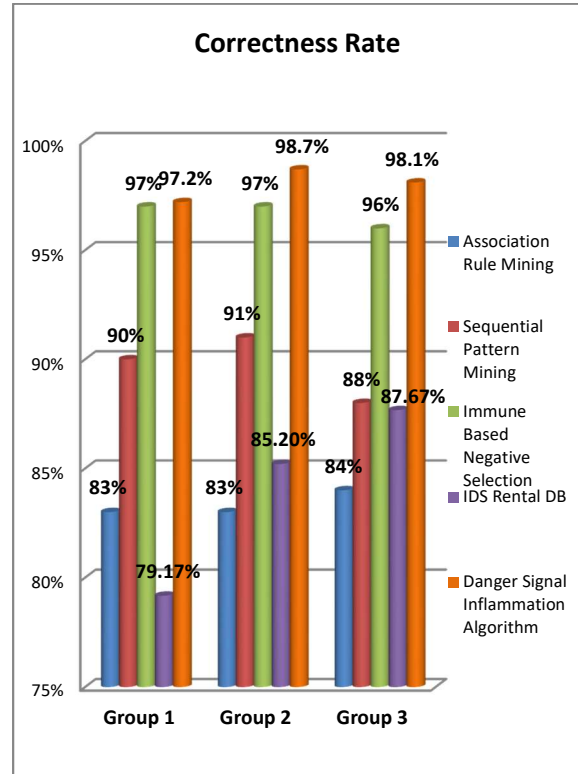


Figure 7: Correctness Rates Comparison

The correctness rate (CR) of the proposed experimental study is presented in Figure 7. The correctness rate refers to the probability of correct detection and is calculated by subtracting the false positive and false negative alarms from 1 as explained in formula (9).

$$C_R = (1 - F_P - F_N) \times 100\% \quad (9)$$

As presented in Figure 7, the danger value signal (DVS) algorithm achieves high correctness rate (CR) when compared with the other four algorithms: negative selection algorithm, association rule mining, sequential pattern mining, and IDS rental DB with values 97.2%, 98.7% and 98.1% respectively. The negative selection algorithm recorded 97%, 97%, 96% respectively. Association rule mining recorded low correctness rate with 83%, 83%, and 84% in the three data groups respectively. Sequential pattern mining recorded 90%, 91%, and 88% respectively. Finally the IDS rental DB recorded low correctness rate with 79.17%, 85.2%, and 87.67% respectively.

One of the major features of the proposed artificial immune algorithm is the adaptability for detecting unknown patterns faster due to the learning and memorization mechanism that provides faster response. When the pattern of an intrusive user is detected for the first time, the system initializes the immunity algorithm for storing the detected pattern in order to be used as an antigen in future detection process. The memorization methodology stores the detected pattern in the antigen table. As a result, if the same pattern is used in another login attempt, the artificial immunity algorithm will search in the antigen table first to provide faster response time.

As presented in Figure 8, the three data groups are tested to provide the execution time for the immunity algorithm and the antigen table response. As shown, the average execution time for detection process of unknown pattern for the first time is 28.44 ms, 27.68 ms, and 27.2 ms. After applying the antigen table response from the memorization methodology, the system recorded 6.58 ms, 6.48 ms, and 6.42 ms.

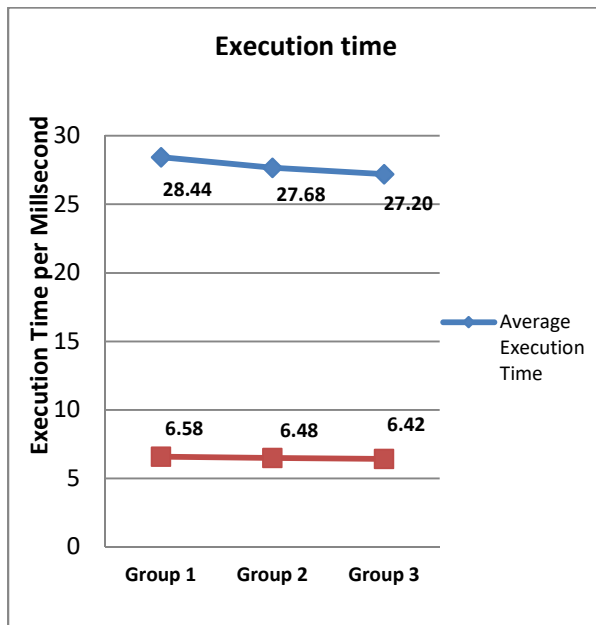


Figure 8: Average Execution Time and Antigen Table Response

The developed artificial immune-based security system achieves better space complexity when the danger value signal (DVS) algorithm is executed. The space complexity is calculated by storing only the authentic factor set (AFS) which is considered as the authentication of the user and the detector of malicious users. The space complexity is presented in formula (10).

$$O(1) \quad (10)$$

Where l is the length of the authentic factor set (AFS). The developed immunity-based security system is considered an enhancement to due to its ability to detect infinite number of intruders with the same authentic factor set (AFS). So, the security system eliminates generating any additional detectors to achieve high detection coverage. The space complexity for the antigen table response is determined by storing the number of detected antigens with their length. The space complexity for the antigen table response is presented in formula (11).

$$O(l \times N_d) \quad (11)$$

Where, l is the length of the detected user (antigen) and N_d is the number of detected antigens.

The detected unknown intruders (antigens) are stored in the antigen table response to provide a quick response if the same intruder attacks the security system more than once. All detected intruders are stored in the database server and only the super administrator (SA) has the authorizations to retrieve the detected intruders or to modify the inflammation signal of the security system as presented in the following script.

```
SELECT *
FROM Security.AntiGen
WHERE Systemid = 'F49FD2DE-46B0-4EE7-
AB6B-FC80D1DBA114'
```

The super administrator (SA) can retrieve all intruders who have been detected by the immunity algorithms in a specified system by providing the encrypted name of the system ID.

6. CONCLUSION

Securing database with traditional methods can preserve confidentiality, integrity and availability of data but can raise some subtle issues such as detection rate and false positive alarms that affect system performance. Negative selection algorithm (NSA) is one of the recent artificial immune algorithms that achieve good performance in reducing false negative alarms with high detection rate. Negative selection algorithm (NSA) is one of the most popular algorithms for detecting unknowing patterns in database. This paper presents a cognitive adaptive mechanisms and algorithms for enhancing system performance and increasing detection rate with low false positive alarms based on negative selection algorithm and danger theory. The developed algorithm is compared with the original NSA, association rule mining, sequential pattern mining, IDS rental database, and ATI algorithm. By applying the developed algorithm; high detection coverage with low false positive and low false negative alarms are achieved. Future directions of this research will

focus on applying proposed algorithms on cloud computing infrastructure to measure the security performance on cloud.

REFERENCES

- [1] A. Adnan, W. Brian, Z. Furkh, J. Lech, A. Munwar, M. Hasanain, F. Robert, "A relation-aware multiparty access control," *Journal of Intelligent and Fuzzy Systems*, vol.37, 2019, pp.1-17
- [2] C.M. Ou, "Host-Based Intrusion Detection Systems Adapted from Agent-Based Artificial Immune Systems," *International Journal of Neurocomputing*, ELSEVIER, vol.88, 2012, pp.78-86
- [3] P. Haripriya, and J. Anju, "An AIS Based Anomaly Detection System," *IEEE International Conference on Computing Methodologies and Communication*, 2017, pp.708-711
- [4] J. Brown, M. Anwar, G. Dozier, "Intrusion Detection using a Multiple-Detector Set Artificial Immune System," *IEEE International Conference on Information Reuse and Integration*, 2016, pp. 283-286
- [5] Z. Ji, and D. Dasgupta, "Revisiting Negative Selection Algorithms," *International Journal of Evolutionary Computation*, Massachusetts Institute of Technology, vol.15, 2007, pp.223-251
- [6] 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," *IEEE International Conference on Next Generation Networks and Services (NGNS)*, 2014, pp.88-91
- [7] S. Niksefat, P. Kaghazgaran, B. Sadeghiyan, "Privacy issues in intrusion detection systems: A taxonomy, survey and future directions," *ELSEVIER Journal of Computer Science Review*, vol. 25, 2017, pp.69-78
- [8] M. Hashem, I. El-Henawy, A. Mostafa, "Database Security – Mechanisms, Techniques, Breaches, and New Directions," *International Arab Conference of e-Technology (IACe-T)*, 2012, pp.74-82
- [9] M. Hashem, I. El-Henawy, A. Mostafa, "Interactive Multi-Layer Policies for Securing Relational Databases," *IEEE International Conference on Information Society*, 2012, pp.65-74
- [10] A. Mostafa, M. Hashem, I. El-Henawy, "Design and Implementation of Multi-Layer Policies for Database Security," *International Journal of Information Sciences*, Natural Science Publishing, vol. 2, no.3, 2013, pp.147-153
- [11] A. Mostafa, M. Hashem, I. El-Henawy, "Design and Implementation of Extensible Service Oriented Algorithms for Securing Relational Databases," *International Journal of Digital Content Technology and its Applications (JDCTA)*, ELSEVIER, vol.7, 2013, pp.753-763
- [12] A. Mostafa, M. Hashem, and I. El-Henawy, "Securing Relational Databases with Artificial Immunity Features," *International Journal of Computer Applications (IJCA)*, vol.68, 2013, pp.11-16
- [13] M. Ogiela, "Cognitive Solutions for Security and Cryptography," *ELSEVIER Journal of Cognitive Systems Research*, vol. 55, 2019, pp. 258-261
- [14] D. Fernandes, M. Freire, P. Fazendeiro, P. Ináci, "Applications of artificial immune systems to computer security: A survey," *ELSEVIER Journal of Information Security and Applications*, vol. 35, 2017, pp. 138-159
- [15] J. Timmis, P. Andrews, E. Hart, "On artificial immune systems and swarm intelligence," *Journal of Swarm Intelligence*, SPRINGER, vol. 4, 2010, pp. 247-273
- [16] C. Laurentys, G. Ronacher, R. Palhares, and W. Caminhas, "Design of an Artificial Immune System for Fault Detection: A Negative Selection Approach," *International Journal of Expert Systems and Applications*, ELSEVIER, vol.37, 2010, pp.5507-5513
- [17] J. Zeng, X. Liu, T. Li, C. Liu, L. Peng, and F. Sun, "A Self Adaptive Negative Selection Algorithm used for Anomaly Detection," *International Journal of Progress in Natural Science*, ELSEVIER, vol.19, 2009, pp.261-266
- [18] B. Schmidt, and A. Al-Fuqaha, "A New Approach to Optimized Negative Selection," *IEEE Congress on Evolutionary Computation*, 2016, pp. 1793-1799
- [19] W. Luo, X. Wang, Y. Tan, and X. Wang, "A Novel Negative Selection Algorithm with an Array of Partial Matching Lengths for each Detector," *International Conference on Parallel Problem Solving from Nature*, SPRINGER, vol.4193, 2006, pp.112-121

- [20] M. Khan, S. Hussain, S. Bakhtair, A. Khan, and J. Iqbal, "Fault Detection in Robot Sensors Using Negative Selection Algorithm," IEEE International Conference on Computer Science and Education, 2014, pp.38-43
- [21] S. Paul, and A. Janecek, "Applying the Negative Selection Algorithm for Merger and Acquisition Target Identification," IEEE International Conference on Computational Intelligence, 2013, pp.609-616
- [22] M. Pamukov, and V. Poulkov, "Multiple Negative Selection Algorithm: Improving Detection Error Rates in IoT Intrusion Detection Systems," IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2017, pp. 543-547
- [23] H. Shaukat, F. Hashim and A. Sali, "Danger Theory based Node Replication Attacks Detection in Mobile Wireless Sensor Network," IEEE International Symposium on Computer Applications & Industrial Electronics, 2014, pp.18-23
- [24] V. Alaparthi, and S. Morgera, "A Multi-Level Intrusion Detection System for Wireless Sensor Networks based on Immune Theory," Journal of IEEE Access, vol. 6, 2018, pp. 47364 – 47373
- [25] D. Dasgupta, S. Yu, and F. Nino, "Recent Advances in Artificial Immune Systems: Models and Applications," International Journal of Applied Soft Computing, ELSEVIER, vol.11, 2011, pp.1574-1587
- [26] C. Morgado, G. Baioco, T. Basso, R. Moraes, "A Security Model for Access Control in Graph-Oriented Databases," IEEE International Conference on Software Quality, Reliability, and Security, 2018, pp. 135-142
- [27] X. Dong, and X. Li, "An Immune Based Relational Database Intrusion Detection Algorithm," IEEE International Conference on Hybrid Intelligent Systems, 2009, pp.295-300
- [28] R. Ramachandran, and A. Jayanthi, "A Novel Method for Intrusion Detection in Relational Databases," IEEE International Conference on Advances in Computing, Communications and Informatics, 2017, pp. 230-234
- [29] M. Zhu, and Z. Huang, "Intrusion Detection System Based on Data Mining for Host Log," IEEE International Conference on Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2017, pp. 1742-1746