APPLICATIONS OF ARTIFICIAL IMMUNE SYSTEM: A REVIEW

Arannya.S

Faculty of Information Technology
University of Moratuwa

ABSTRACT

The Biological Immune System is a remarkable information processing and self-learning system that offers stimulation to build Artificial Immune System (AIS).During the last two decades, the field of AIS is progressing slowly and steadily as a branch of Computational Intelligence (CI). At present the AIS algorithms such as Negative Selection Theory, Clonal Selection Theory, Immune Networks Theory, Danger theory and Dendritic Cell Algorithm are widely used to solve many real world problems in a vast range of domain areas such as Network Intrusion Detection (NID), Anomaly Detection, Clustering and classification and Pattern recognition. This review paper critically discusses the theoretical foundation, research methodologies and applications of the AIS.

KEYWORDS

Artificial Immune System, Negative Selection, Clonal Selection, Immune Network.

1. INTRODUCTION

Almost all the human inventions have taken nature functions as the inspiration, especially human body and its functions lead to emergence of Artificial Intelligence Techniques. The Artificial Neural Networks are inspired by human neural network and its functions, Genetic Algorithms are inspired by biological genetic functions, and likewise the Artificial Immune System (AIS) is also inspired by Biological Immune System (BIS) and its functions. But not like artificial neural networks and genetic algorithms, the AIS has extracted almost all the functions of BIS, as BIS is a robust, error tolerance, decentralized and adaptive system[1].

The concept of AIS was proposed by Farmer, Packard and Perelson in late 1980s, but it has emerged in 1990s as a class of computational intelligence [2]. In BIS, white blood cells protecting our body from unwanted attacks from fungus, bacteria and viruses, by having well established network system [3]. By mimicking the cells and organism of BIS such as B-cells, T-cells, born marrow and antigens as in instance of a class, the immunologists have implemented five algorithms, namely Clonal Selection Theory (CST), Immune Network Theory (INT), Negative Selection Theory (NSA), Danger theory and Dendritic Cells Algorithm (DCA). Among these CST, INT and NST have well established by immunologists as first generation of AIS, but Danger theory and DCA are not yet well proven but they have many potentially interesting background as the second generation of AIS [4]. However, as an emerging artificial intelligence technique, AIS has already reached to a significant level with number of approaches to address many real world complex problems in a vast range of domain areas such as anomaly detection, pattern recognition, optimization, intrusion detection. Further these approaches can also be applied into robotics too.

Prior to that, Section II gives a brief introduction to BIS where AIS is inspired from. Section III give the Classes of AIS, IV the section will discuss the applications of AIS and finally the Conclusion for conclude the review work.

2. OVERVIEW OF BIS

The BIS is naturally well sophisticated, and decentralized, error tolerance, robust and adaptive system which plays two major roles; protecting the body against invading micro-organism such as fungi, bacteria and virus and keeping them out by failing them or destroying them and regulating bodily functions. The immunologists have found that, the BIS have two functional parts, namely innate immune system and adaptive immune system. The function of innate immune system is responding to known threats while the adaptive immune system is tackling the encountered threats. However within these two parts they have little cross over when they are functioning against pathogens [5]

The key ability of BIS is, it can distinguish the body's own cells- called self-cells and foreign cells-called non-self-cells. Normally the immune system works with self-cells which are carrying molecules, but when noticed a cell or organism carrying foreign invaders (non-self), it will quickly launch the attack; this is so called immune response. Another major capability of BIS is, it can remember millions of distinguishing enemies. Therefore they can produce secretions and can match up those cells and wipe nearly all of them out, by having a dynamic communication network [6].

The organs of BIS that are spread throughout the body are called lymphoid organs, as they are generated by lymphocytes (white blood cells), and are the key players of BIS. Lymphocytes are produced by bone marrow (it's the source of all blood cells), which is in the hollow center of bones and by using blood vessels, lymphocytes are travelling throughout the body. The lymphocytes have three subclasses; namely B-cells, T-cells and NKT cells and AIS are mimicking the functions of these cells [7].

The B-cells works primarily by concealing solvable know as antibodies and they mill around a lymph node and wait for an antigen. Once the antigen arrives it will match up with a specific antibody and proceed the immune response. At that time the antigen binds the antibody, the B-cell overwhelm it and the B-cell becomes large plasma, which can produce number of antibody copies (up to 100 million copies an hour), after a special helper T-cell joins the action. Then these antibodies will travel throughout the body by bloodstream to search more antigens. The antibodies of B-cells cannot kill an invading organism by themselves, but they make those antigens by their antibodies and let other immune cells to kill them [8].

The T-cells contribute to immune action in two ways; some help to regulate the overall immune response while the others which are called cytotoxic directly contact the non-self –cells (the cell marked by the antibodies of B-cells) and abolish them. The helper T-cells play a major role here. They are responsible to activate many immune cells including B-cells and other T-cells. The Killer cells (NKT) can be divided into at least two parts; cytotoxic T-cells and natural killer cells and both contain granules filled with intoxicating chemicals to destroy on contact [9].

3. THE CLASSES OF AIS

This section will discuss about the classes of AIS and the existing approaches of those classes.

3.1. The Clonal Selection Theory (CST)

Burnet has proposed CST in 1959. As we have seen in the Section II, when B-cells encountered a non-self-cell it will automatically take the immune action against the cell. By that it will create

plasma from the particular antigen to destroy the antibody [10]. This concept is extracted by CST. The CST has three main features;

- The new cells copy their parents (clone) exposed to a transformation mechanism with high rates.
- Eliminate the newly distinguished lymphocytes carrying self-reactive receptors.
- Proliferation and separation on contact of mature cells with non-self-cells.

Table 1. The approaches of CST [11], [10]

Author and Year	Algorithm	Purpose of the algorithm
Castro and Zuben (2002)	CLONALG	Learning and Optimization.
Rouchen (2003)	Immunity Clonal Strategy Algorithm (ICS)	Optimization.
Garret (2004)	Adaptive Clonal Selection (ACS) (is an alternation of CLONALG)	Increase the efficiency of clones when doing Optimization.
Yu and Hou (2004)	Enhanced CLONALG	Enhance the efficiency of Detection and learning.
Camples (2005)	Rea-Coded Clonal Selection Algorithm (RCSA).	Electromagnetic design Optimization.
Gong (2207)	Extended CLONALG	Increase the efficiency of learning by using logic adaptive method to learn the Antibody population.

3.2. Negative Selection Theory (NST)

The needs of negative selection are to provide tolerance for self-cells. It deals with the immune system's ability to detect non-self-cells without reacting to self-cells. During the production of T-cells, a pseudo-random genetic rearrangement process will be preceded by receptors. Then they undertake an editing process in the thymus which is called the negative selection [12].

Table 2. The approaches of NST [11]

Author	Algorithms	Purpose of those algorithms
Forrest (1994)	Founder of NSA	Anomaly Detection
Ayara (2002)	NSMutation	Removes Data redundancy
Gonzalez and Cannady (2004)	Self-adaptive NSA	Anomaly detection
Igawa and Ohashi (2008)	Artificial Negative Selection Classifier (ANSC)	Classification and Clustering

3.3. Immune Network Theory

The Immune Network Theory was proposed in the mid-seventies (Jerne 1974). The theory was that the immune system maintains an idiotic network of interconnected B cells for non-self-cell identification. These cells both increase and overwhelm each other in certain ways that lead to the steadiness of the network. Two B cells are connected if the affinities they share exceed a certain inception, and the strength of the connection is directly proportional to the affinity they share [13].

Table 3. The approaches of INT [11], [13]

Author	Algorithms	Purpose of those algorithms
Timmis (2000)	Artificial Immune Network (AINE)	Data Analysis
Castro and Zuben (2000)	aiNet (with some features of AINE)	Increase the efficiency of Data Analysis
Castro and Timmis (2002)	Hierarchy of aiNet	Data Analysis and Clustering
Nasraoui (2003)	TECNO-STREAMS	Clustering by detecting unwanted entries.
Bentley and Timmis (2204)	Fractal Immune Network	Classification and Clustering regardless of the data.
Lug and Liu (2004)	Reactive Immune Network (RIN)	Mobile Robot Learning Navigation Strategies

3.4. Danger Theory

The advocator Matzinger has proposed this theory in 2002, and it has become popular among immunologists during last decade. The idea behind her proposal is foreignness of a cell is not the important factor to trigger the immune response and selfness is not guarantee of acceptance [14]. The BIS do not react for the nutrient cells which have got into the body via consuming foods and drinks even though they are not self-cells. Therefore she has concluded that BIS reacting danger instead of foreignness. Danger is a signal which is emitted by an unnaturally injured cell.

Table 4. The approaches of danger theory [14]

Author	Algorithms	Purpose of those algorithms
Aickelin and Cayzer (2002)	Applications of Danger Theory (First paper on DT)	To distinguish between the positive danger signal and negative danger signal
Prieto	DTAL (Danger Theory Algorithm)	Goalkeeper strategy in robot soccer
Iqbal and Maarof	DASTON	Intelligent Data Processing

3.5. Dendritic Cell Algorithm (DCA)

The DCA is mimicking the function of naturally occurred dendritic cells (DCs), which are responsible for foreign invaders detection. They can get the signal from unhealthy cells and by combine those various signals, the DCs produce their own signals. These output signals are the one which are instructing the BIS cells for the immune response against the non-self-cell [15].

Table 5. The approaches of DCA [15]

Author	Algorithms	Purpose of those algorithms
Oates (2004)	Robotic DCA (with image processing)	Robotic classification problems
J.Kim and P.Bentley (2006)	BeeAIS-DC (inspired by MANET routing protocol)	Misbehavior detection system

4. APPLICATIONS OF AIS

This section will discuss about the application areas of AIS by using the approaches which are discussed in SECTION III.

4.1. Pattern recognition

Here binary string representation is used to recognize the pattern of a sample population. Therefore B-cells are taken as objects and antibodies and antigens are represented as a string form of 1's and 0's, where antibody's representation is the complementary of antigens. For the testing purpose the antigens are represented in three different ways, each with 20 elements and each will be 33% of the population (Figure 1).

The Farmers approach has used to find how well B-cells' antibody matches with the presented antigens. The following figures depict how the matching can be done.

The Figure 2 depicts the original form of the antibody and antigens and how the antibodies have changed according to the antigens.

Figure 1. Antigens representation

11111111110000000000	33%
00000000001111111111	33%
00000111111111100000	33%

Figure 2. Antibody matching

Antibody	0 0 1 0 1	0 1 1 1 0
Antigen	1 0 0 0 1	1 1 0 1 0
Bit shifted Antibody	0 1 1 1 0	0 0 1 0 1

Figure 3. Pseudo code of Antibody shifting

```
Repeat
        c=Ag XOR Ab
        M0=
        For each section consisting of 2 04 more 1s record their length
        M1=M0+  2
        If M1>Mmax the
        Mmax=M1 Shift Ab right
        1 bit
        Until Ab shift complete.
```

The antibody and antigen matching algorithms are illustrated in Figure 3. (Ag-Antigen and Ab-Antibody).

Matching value calculation is represented in the Figure 4. The 12 indicate the number of matching elements, and it has been added to the number of sections, for example 6 elements-26. Therefore the final matching value is 88%.

As for the conclusion, seven set of different antigens pattern have been taken and they have been tested by the same algorithm.

Test 1, 4 and 7 have shown almost a similar representation and the other set has represented in different ways. The Figure 6 depicts how the result can be changed according to the antigen pattern representation.

Figure 4 Matching value Calculation

Antigen:	0 1 1 0 0 0	0 1 1	1 1 0	1 1 0	
Antibody:	1 0 0 1 1 1	1 0 0	1 0 1	1 0 1	
XOR:	1 1 1 1 1 1	1 0 1	0 1 1	0 1 1	$\longrightarrow$ 12
Length:	6	2	2	2	
Match value:	$12+2^{6}+$	$2^{2}+$	$2^{2}+$	2^{2}	$\longrightarrow$ 88

Figure 5. The set of antigens which has taken for testing

1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0	Test 1
1 1 0 0 1 1 1 1 1 1 1 1 0 0 0 1 1 0 0 0	Test 2
1 1 1 1 0 0 0 0 1 1 0 0 0 0 0 0 0 0 1 0	Test 3
0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1	Test 4
1 0 0 0 0 1 0 1 0 1 0 0 1 1 1 1 0 1 1 0	Test 5
0 0 0 0 1 1 1 0 0 0 0 0 1 1 1 1 1 0 0 1	Test 6
0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0	Test 7

Figure 6. Results of testing

Test	**No of B cells**	**Worst**	**Average**	**Best**
Test 1	20	50	2678	16397
Test 2	20	47	2736	16393
Test 3	20	67	314	2055
Test 4	20	50	2678	16397
Test 5	20	38	110	263
Test 6	20	72	586	4109
Test 7	20	50	2678	16397

The original antigens representations such as test 1, 4 and 7 have given higher best and average matching value, and test 2's best and average matching values are also merely closer to the corresponding original representation's (Test 1, 4 &7) value. As from the observation it has been concluded as AIS also have the same pattern recognition ability as BIS [16]. Therefore, the AIS algorithms can used to identify any complex populations' patterns in efficient way.

4.2. Anomaly Detection

Computer viruses, hardware false and fraudulent connections can be considered as anomalies. To detect those anomalies the immunologists have extracted the concept of BIS. The main function of anomaly detection is protecting the systems from intruders [17]. For this non-self-cells are considered as unwanted or unauthorized connections and self-cells are considered as system itself. It is not the case that non-self-cells are always triggers the immune response, by time some non-self-cells can change as self-cells and wise versa. According to danger theory concept, danger alarm is the key player that triggers the immune response. In AIS, the concept applied system should transmit danger signal when it gets an unwanted or unauthorized access. The following situation can be considered as unwanted access;

- Too high or low memory usage.
- Insertion of inappropriate disk or its activities.
- Files changing unexpectedly and frequently (file size)
- Unwanted or unauthorized connection access.

Once the danger alarm is emitted by the connected devise or a system, the detector system (immune system) has to respond quickly. But for this action it not necessary to have the detector system nearby (physically) the effected device or system. When the detector gets the danger signals consequently, from the first signal the detector will identify the effected system and from the following signals the detector will further get into the effected system and it will specifically identify the dangerous component. After the confirmation of the antigen (effected part) the detector will send the information to the corrective action part which have already inbuilt. Therefore the anomaly detection system is avoiding human interactions and solving the issues by its self [18].

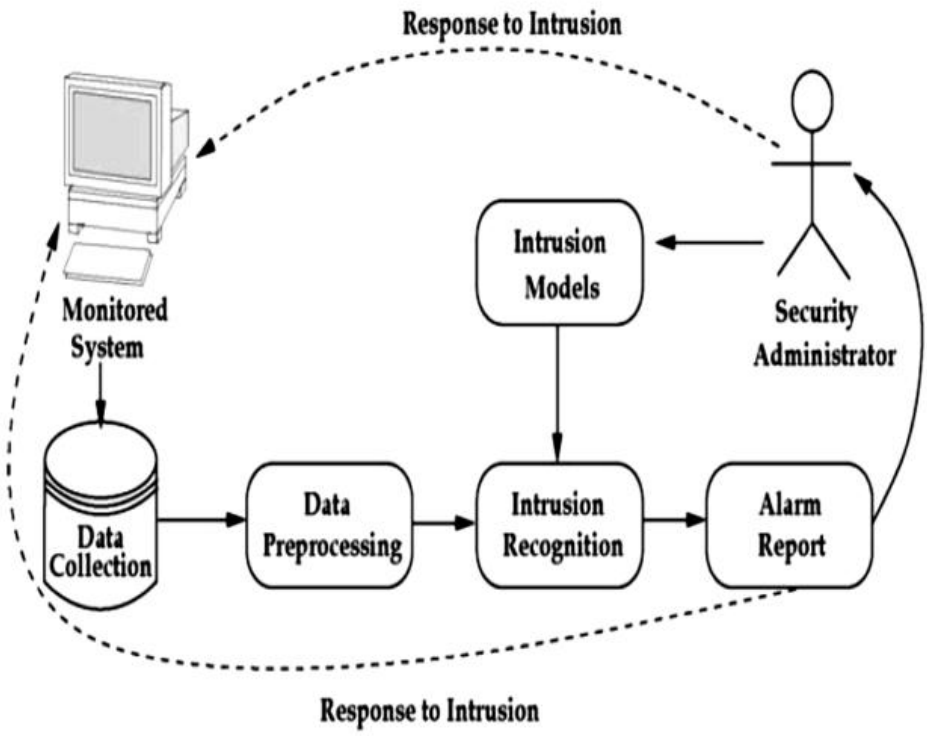
4.3. Intrusion Detection Systems (IDS)

When come to the network security traditional IDS such as data encryption mechanism, fire wall have already failed due to the malicious attacks and their highly technical attacking mechanisms [7]. This unsecured situation tools the concept of IDS, but to build a proper IDS, the following functions are needed,

- Data collection
- Data processing
- Intrusion recognition- key activity.
- Reporting about the intrusion
- Response to the detected intrusion.

To identify the unwanted accesses the IDS should monitor the connected system continuously, to check whether the access has the symptoms to an attack or it is a valid use of the operator. Figure 7 depicts the generalized organization of IDS, where straight line indicates the flow of data and control and dashed line response to intrusive activities [19].

Figure 7. Organizations of IDS



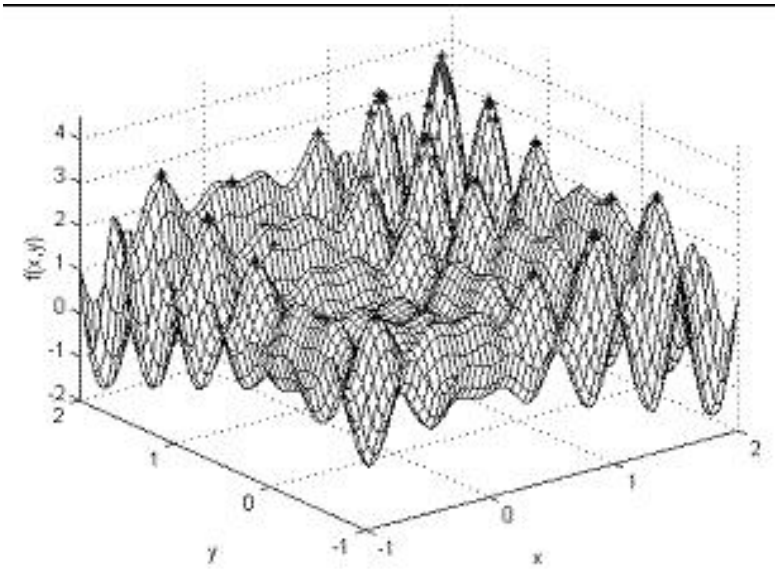
The major function intrusion detection will happen in the manner of observing the intrusions and matching with the already existing details about the intrusions (in knowledge base) and its' behavior, and the corrective action will be taken place according to the detected intrusion and its destructiveness. Therefore well-knows will be detected by the system easily and efficiently and the actions will also be taken place at the moment it got detected. Because of this features only the IDS became famous in the industry. But intrusions are evolving continuously and polymorph. Therefore pre-defined mechanism of IDS will fail in this case. To avoid this risk the system has to update daily and it can be achieved automatically or manually. When updating the system manually it will consume time and labor hours. But automatically updatable systems are possible with the help of learning and adaptive algorithms. Unfortunately this type of knowledge bases is most expensive, but this type of IDS will be more precise when compared to the traditional IDSs [20].

4.4. Optimization and Clustering

Optimization and clustering is one of the most popular application areas in AIS [21]. More advance AIS approaches used to address multimodal optimization problems. The CLONALG algorithm has proposed to recognize the pattern and to optimize the population according to the patterns. To address data compression and clustering issues including non-linear separable and high-dimensional issues opt-aiNet algorithm which is a combination of CLONALG and ai-Net has been used [22].

When functioning, firstly the system will do clustering as an optimization process, where the whole population will be divided into individual subgroups and the fitness peak will be indicated in each cluster. Then the aiNet perform destruction collaboration of the network cells each other. It is possible to maintain an active control of number of network population by evaluating the degree of resemblance among the population. When compared to CLONALG, opt-aiNet has performed better and found many peaks of the population as it has used greedy search algorithms to find the peaks of each and every cluster (Figure 8) [23].

Figure 8 Optimization results



Equation (1) represents the function used for the greedy search.

( ) ( ) ( ) ( ) (1)

It is a combination of many local optimums and a global optimum. Binary string are used for the values of x and y with the length of 22. As figure 4.8 indicates the solution covers most of the peaks including the global optimum. Therefore the conclusion can be made in an effective manner as its results will be coming in a sorted order. Therefore by using AIS approaches, the optimization can be done more efficiently.

5. DISCUSION

AIS are a comparatively new field of study that has gained well-known recognition and attention and it is a research area that ties the discipline of immunology, computer science and engineering. AIS can be applied across various areas including learning, information retrieval, communications, design, and health. This is extremely vital in the medical and electronic field. During the past two decades, they have been attracted a lot of interest from researchers aiming to develop immune-based models and techniques to solve complex computational problems. The immunologists try to expand the approaches of artificial immune systems by studying the BIS and its functionalities. By identifying more approaches the immunologists intend to address major unresolved problems like cancers, space optimization and network security issues. AIS would benefit more if there was more prominence in the use network security as it has been as a major issue now days. However, as research is still in early phases, it is apparent that there are much more research work to be done and has much promise in altering the world.

ACKNOWLEDGEMENT

I would like to use this paper to thank my dada, my better half and my family for the grate support they gave throughout my life time. I would like to express my thankfulness to Mrs. K.A Dilini T Kulawansa and Miss. Priyanga Talagala in the Department of Computational Mathematics of the Faculty of Information Technology of the University of Moratuwa for proposing this area of research to me and for their instructions on approaching the problem and valuable guidance throughout.

REFERENCES

[1] Immune Programming. Petr Musilek, Andriel Lau, Marek Reformat, Loren Wyard Scott. Department of Electrical and Computer Engineering.
[2] Artificial Immune Systems. U.Aickelin and D.Dasgupta. University of Nottingham.
[3] Artificial Immune Systems. Mark Read, Paul Andrews and Jon Timmis. Department of Computer Science, University of York.
[4] Application Area of AIS: The past, the present and the future. Emma Hart, Jon Timmis Department of Electronics and Computer Science. University of York.
[5] Theoretical advance in Artificial Immune Systems. J. Timmis, A.Hone, T.Stibon, E.Clark. Department of Electronics, University of York, UK.
[6] Understanding the Immune System. U.S. Department of Health and Human Service. National Institute of Health.
[7] The use of computational intelligence in intrusion detection system. Shely Xiaonan Wu, Wolfgang Banzhaf. Computer Science Department. Memorial University of Newfoundl
[8] Model application of information gain-based artificial immune recognition system. Sadik Kara, Bekir Hakan Aksebzeci, Halife Kodaz, Salih Gunes, Esma Kaya, Hatice Ozbilge.
[9] Elements of the Immune System and their Roles in Defense. Chapter I.
[10] The Clonal Selections with Engineering Applications. Leandro Nunes de Castro and Fernando J. Von Zuben. Scholl of Electrical and Computer Engineering.
[11] Learning using an artificial immune system. John E. Hunt and Denise E. Cooke. Centre of Intelligent Systems, Department of Computer Science. University of Wales.
[12] Artificial Immune systems. Models, Algorithms and Applications. J.R. Al-Enezi, M.F. Abbod and S. Alsharhan. Electronic and Computer Engineering Department. University of Brunel.
[13] Artificial Immune Networks: Models and Applications. Xian Shen, X.Z. Gao and Rongfang Bie. College of Information Science and Technology.
[14] Design of an artificial immune system based on Danger Model for fault detetion. C.A Laurentys, R.M. Palhares, M.W. Caminhas. Department of Electrical Engineering, Federal University of Minas Gerais.
[15] Detecting Danger: The Dendritic Cell Algorithm. Jilie Greensmith and Steve Crazer. School of Computer Science. University of Nottingham.
[16] Immune Programming. Petr Musilek, Andriel Lau, Marek Reformat, Loren Wyard Scott. Department of Electrical and Computer Engineering.
[17] Design of an artificial immune system for fault detection: A negative selection approach. C.A Laurentys, R.M. Palhares, M.W. Caminhas. Department of Electrical Engineering, Federal University of Minas Gerais.
[18] The Danger Theory and Its Application to Artificial Immune Systems. Uwe Aickelin, Steve Cayzer. School of Computer Science, University of Nottingham.
[19] A Novel Artificial Immune System for Fault behavior detection. C.A Laurentys, R.M. Palhares, M.W. Caminhas. Department of Electrical Engineering, Federal University of Minas Gerais.
[20] Immune inspired fault detection and diagnosis. Guilhereme Costa Silva, Reinaldo Martinez Palhares, Walmir Matos Caminhas. Graduate program in Electrical Engineering. Federal University of Minas Geris.
[21] Artificial Immune System. Basic Theory and Applications. Leandro Nunes de Castro and Fernando J. Von Zuben. Scholl of Electrical and Computer Engineering.
[22] Fault diagnosis based on support vector machine with parameter optimization by artificial

immunization algorithm. Shenfa Yuan. Fulie Chu.
[23] A Review of Clonal Selection Theory of Acquired Immunity. Jason Brownlee. Complex Intelligent System Laboratory, Swinburne University of Technology, Australia.

AUTHOR

I am Arannya Sivasubramaiam, undergraduate of Faculty of Information Technology, University of Moratuwa. I'm the first child who got into a university from my family, therefore from that day onward my father has some hope on me and he wants me to end up with as a high qualified personality in our society. Till the day started to read about Artificial Immune System (AIS), I have put all my effort on basketball, but now I have more interested on AIS, than basketball. As an aim of my life I would like to follow my higher studies on AIS, for that I set this paper as the first objectives and believe I have attained it as well.