Journal of Theoretical and Applied Information Technology
28th February 2023. Vol.101. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ARTIFICIAL IMMUNE SYSTEM: A SYSTEMATIC LITERATURE REVIEW

NIDA HASIB*[1], SYED WAJAHAT ABBAS RIZVI[2], VINODANI KATIYAR[3]
[1]Amity Institute of Information Technology, Amity University Uttar Pradesh, Lucknow, India
[2]Amity School of Engineering and Technology, Amity University Uttar Pradesh, Lucknow, India
[3]Dr. Shakuntala Misra National Rehabilitation University, Lucknow, India
E-mail: [1]nida.haseeb@s.amity.edu*, [2]swarizvi@lko.amity.edu, [3]vkatiyar@dsmnru.ac.in

ABSTRACT

Purpose – This work seeks to make clear that Artificial Immune Systems are computational paradigms that have drawn researchers to develop immune based models and methodologies using theories, processes, and algorithms in many domain areas to tackle various social or technical difficulties. Additionally included are the AIS methods and algorithms that have been applied during the past 20 years to deal with clustering, classification, and optimization problems.
Design/ Methodology/Approach – An analysis of the existing literature on artificial immune systems was compiled by the authors as part of their systematic literature review, which also served to highlight any gaps in the body of knowledge and set the stage for future study.
Findings - The evaluation process indicates the pervasive influence of Artificial Immune System approaches employed in issue domains other than software development projects but elevated the necessity of AIS has been examined to classify modules of software development projects. Algorithms are built on Immune system theories and computational features used in different domains to achieve the best classification accuracy. The authors found out that, compared to the number of proposed approaches, implementation of software project development approaches is lacking. The study further reveals that such approaches lack completeness from one or more perspectives.
Originality/Value – Since there are numerous experience reports and case studies on Artificial Immune Systems in the research literature, as far as the authors are aware, there is no systematic overview and synthesis of this expanding field of study. The authors organize the review process on the Artificial Immune system and their studies in various domains between 2000-2021. We used a systematic process to select one hundred four articles, twenty-eight conference proceedings, seven book sections, four workshop proceedings, eight symposiums, two technical reports, and five theses. This study focuses on various domains and their proposed approaches built on Artificial Immune Systems in the last two decades.
Keywords: *Artificial Immune System, AIS, Systematic Literature Review, SLR, Biological Immune System, BIS*

1. INTRODUCTION

Immunology provides a thorough overview of the antigens and antibodies that make up the immune system as well as the mechanisms that enable them to identify and get rid of an infinite number of foreign invaders. Pathogens are the name for these cells. The immune system recognizes an antigen, which is a component of these cells. To recognize these antigens, the immune system produces a wide range of antibodies. Any antigen containing cell receptors is recognized by these antibodies, which are made by B-cells. The immune system has a wide range of engineering applications. For repeat infections involving a similar antigenic receptor, the immune system can recall the antigenic receptor's structure and associated antibody combination in memory cells [1][2][3].

Oda and White commended that "If the immune system were inaccurate, the lifespan of the average human would be much shorter as the system would be much shorter as the system would mistakenly attack vital cells or fail to attack viruses and other dangerous pathogens". Immunity is capable of recognizing and eliminating specific foreign microbes and molecules[4][5][6].

The Biological Immune System can recognize self and non-self is detected, damaging, and killing the antigen from inside or outside the body in real time. Researchers used the principles and theories of the Biological Immune System (BIS) to create the theory, mechanisms, and algorithms of the Artificial Immunity based system. AIS provides a

solution to many complex problems [7][8]. The problems found in a computer security system are quite similar to those encountered in BIS. The countermeasures taken against the pathogens are mostly aimed at reducing the probability of infection due to pathogen attacks. A human body can also have physical barriers that reduce the probability of entry into its body and reduces its survival and replications. The pathogens can rapidly evolve ways to neutralize the countermeasures adopted by the host to keep pathogens outside of its body. This collection of countermeasures comprises an immune system. Its function is to detect the pathogens once they have entered the body and to eliminate them with minimal cost in terms of resources employed and damage done to the host. The immune system represents also protection against the possibility of malfunctioning and failure of the individual host cell[9][10][11][12][13]. The immune system is an efficient defense mechanism that serves a variety of infections. The biological Immune system constitutes two tiers of defense.

1. Innate immunity
   Innate immunity is the first line of defence mechanism also called nonspecific immunity against foreign invaders that individuals are born with. Innate immunity is mainly composed of physiologic barriers, phagocytic barriers, and inflammatory responses. Adaptive immunity allows the immune system to attack any foreign pathogens that the innate system cannot destroy [3][4].
2. Adaptive immunity
   Adaptive immunity is the second line of defence also called acquired or specific immunity. When this system is triggered, the antibodies are produced only in response to specific infections. If the same antigen repeats, these antibodies cope with the infections thus preventing the establishment of disease within the body. Adaptive immunity encloses several characteristics:
   a. Antigenic specificity: It allows the immune system to distinguish subtle differences among antigens.
   b. Diversity. The adaptive immune system is capable of generating an infinite number of receptors that can uniquely recognize different structures of foreign antigens.
   c. Immunologic memory: The adaptive immune system can remember a previous encounter with an antigen. This process helps in an efficient recognition system for recognizing an antigen again.
   d. Self/nonself recognition: The immune system has receptors that discriminate cells that belong to the body as self and foreign as nonself.
   e. B-cells and T-cells: These cells represent lymphocytes. In contrast to T-cells that require MHC molecules for detection, the B-cells are capable of recognizing antigenic material. T-cells migrate to the thymus for maturation and B-cell maturate in the bone marrow. These detectors circulate in the body, constituting an effective, distributed anomaly detection and response system. T-cells are generated in the thymus, and only a few mature to become naïve T-cells. The microenvironment within the thymus governs positive and negative selection. As soon as T-cells get in touch with antigens associated with an MHC molecule on a cell, it proliferates and differentiates into memory T-cells.

Through improved understanding and investigation, immune systems theories are developed under a new branch of Artificial intelligence, the Artificial Immune System (AIS). The biological immune systems offer several attractive features such as the ability to remember, classify and neutralize the effect of foreign particles [14][1]. AIS is closely modelled on the basic theory of the Biological Immune System. Many features of the Immune System are employed in the development of the Artificial Immune System [15]. The detector combines the properties of B-cells, T-cells, and antibodies. Lymphocytes have hundreds of thousands of detector symbols on their surface. These detectors bind to regions (epitopes) on pathogens. Binding depends on chemical structure and charge, so receptors are likely to bind to a few similar kinds of epitopes. The greater the chances of a bond occurring, the higher the affinity between the receptor and epitope [15][16].

2. BACKGROUND

Intelligent techniques known as AIS are used to solve problems in a variety of applications. They are inspired by the biological immune system's mechanisms, principles, and models. [17][18]. Theories of AIS serve as the foundation for a variety of approaches and algorithms, which in turn help to enhance the effectiveness of many engineering applications' processes and methods. [19][20][21][22].

1. Learning and Memory via Clonal Selection

Antigen identification is insufficient for the immune system to provide sustained protection. The immune system's ability to recognize antigens is insufficient to provide long-term protection. Antigens that are later met through cells and molecules are successfully combated by the immune system. Raising the population size and affinity of cells that have proven useful during the antigen learning process includes the clonal selection. Thus, the immune repertoire is biased from a random base to a repertoire that more clearly reflects the actual antigenic environment [23][24].

2. Self/Non-Self Discrimination

Antibodies and T-cell receptors produced by the lymphocytes can recognize any foreign (or self) molecule. Therefore, all molecules (shapes) can be recognized including our own, which are also seen as antigens, or self-antigens. The molecules must be distinguished between our cells(self) and foreign cells(non-self). The molecules of our cells (self) and foreign molecules (non-self) must be distinguished for the immune system to function properly.

3. Negative Selection

The concept of a negative signal following certain lymphocyte-antigen interactions allows for the control of those lymphocytes being anti-self. Negative selection of a lymphocyte describes the process whereby a lymphocyte-antigen interaction results in the death of that lymphocyte. The negative selection of T-cells has been broadly used by the AIS community as a model to perform anomaly detection [9][15][25] [26][27][28].

4. Immune Network

Niels. Jerne proposed the immune network theory as an alternative to explain how the immune system works. He suggested that the biological immune system is an efficient and adaptive system whose antigens and antibody receptors are capable of recognizing each other, thus forming an internal network of communication within the organism. The immune network acts as a self-supporting and self-organizing network and provides the basis for immunological memory [10][11][12][13][29].

Inspiration from the remarkable properties expressed by the natural immune system led to the conception and design of Artificial Immune Systems exhibiting similar functionalities (Dasgupta, 1998; de Castro & Timmis, 2002) [10][13][25].

1. Recognition

The immune system can recognize, identify and respond to a vast number of different patterns. Additionally, the immune system can differentiate between malfunctioning self-cells and harmful non-self cells, therefore maintaining some sense of self.

2. Feature Extraction

In the immune system, antigen presenting Cells (APC) can extract features of the antigen by filtering molecular noise from disease-causing agents called an antigen, before being presented to other immune cells, including the lymphocytes.

3. Diversity

The immune system generation and maintenance of diversity involve two major processes. The first is the generation of receptor molecules through the recombination of gene segments from gene libraries. The second process, which assists with diversity in the immune system, is known as somatic hypermutation. Immune cells reproduce themselves in response to invading antigens.

4. Self-regulation

Immune systems dynamics are such that their population is controlled by local interactions and not by a central point of control. After a disease has been successfully combated by the immune system, it returns to its normal steady state, until it is needed in response to another antigen. The immune network theory explicitly accounts for this type of self-regulatory mechanism [15][16].

The application of an algorithm for optimization and other problem-solving in many engineering applications consumes AIS theory and background. These algorithms are built on the methods and AIS guiding concepts [4][30][31]. The dataset is used to evaluate and test algorithms for classification accuracy. To achieve the best classification accuracy, algorithms like AIRS1, AIRS2, AIRS2 parallel, Immunos1, Immunos2, Immunos99, CSCA, and CLONALG have been used and researched. Other algorithms of AIS computational theories include the immune network algorithm, the negative selection algorithm, and the clonal selection algorithm [29][32]. Databases are used in many different fields, including danger theory [19][9][33][34].

The remaining portions of this review are structured as follows. The research technique is described in Section 3, the results of the research questions are shown in Section 4, a discussion based on important findings is included in Section 5, and the study's conclusions are presented in Section 6.

3. RESEARCH METHOD

The research procedures and approaches used in this SLR are based on a number of norms and recommendations that writers have detailed in

Journal of Theoretical and Applied Information Technology
28th February 2023. Vol.101. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

references [35][36][37][38]. The SLR has a step-by-step methodology that enables the researcher to specify their search strategy. This approach was chosen because it makes it easier to record, summarise, synthesize, and critically comment on each specific topic studied. According to the literature, this SLR has the following steps:
Step1: Identification of research questions
Step2: Strategy
Step3: Study selection Criteria,
Step4: Quality Assessment on the selection of potential papers,
Step5: Data Extraction and synthesis,
Step6: Results of SLR and answering the predefined questions
And lastly
Step7: Critical findings for future research

The research method framework is shown in fig 1. Through the SLR procedure, we tried approximately hundred papers related to the usage of Artificial Immune systems in various engineering problem domains. These articles are chosen from credible, highly cited, leading, peer-reviewed journals that are more likely to publish quality research papers.

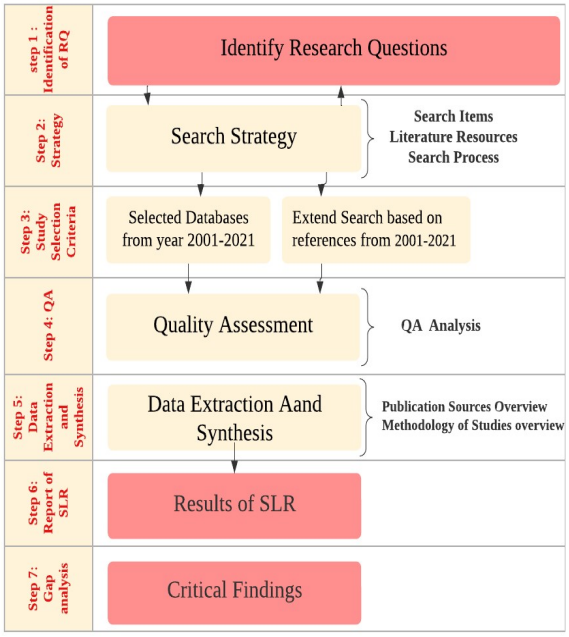

Figure 1: Research Method framework

3.1 Research Questions

The major goals of this study were to learn about, comprehend, and synthesize research on the biological immune system and its inherited notion in artificial intelligence (AIS), as well as to identify the domains in which this system is employed to address current issues. identified a research gap in the AIS field. Therefore, the study chose four research questions based on its aims (RQ). Based on the aim of the study, RQ is framed in figure2.

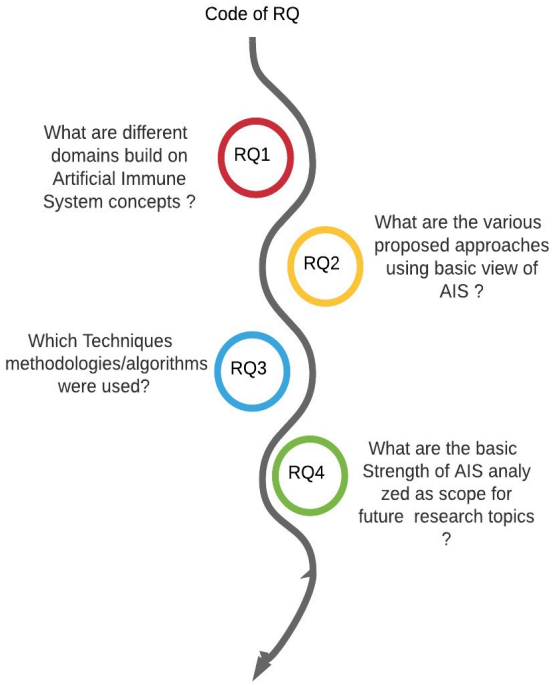

Figure 2: Research Questions

3.2 Search Strategy

The search strategy in the review process includes Search terms, literature resources, and a search process to achieve the aim of the study. In this study, data sources include IEEE, Springer, Google Scholar, Elsevier SCI, ResearchGate, Hinda Wi, Applied Sciences, Emerald, Springer, Taylor & Francis, and data sources from courses by Coursera and NPTEL and some reference books of publishers McGraw hill, PHI, WH freeman. The keywords in this review include: Fault prone classification, AIS, AIRS, Immunology, Immune System, clonal selection, negative selection, Biological Immune System, Biological Computation, optimization, positive selection, Danger Theory, and some special words that are randomly used in a various research paper are optimization, assessment, hybrid, artificial, fitness, affinity. Therefore, for a more accurate and precise search exercise, all terms were used. The search was limited to all articles published in English from 2000 to 2021. It was considered that this period allows the retrieval of a sufficient number of studies on the topic and the detection of the research trend for this topic.

3.3 Study Selection Criteria

Based on the above-mentioned sources, the authors identified 864 studies. Inclusion and exclusion criteria were established to make certain that the system included papers, books, articles, etc that were relevant to the current study. Table 1 summarizes all the inclusion and exclusion criteria.

Table 1: Study Selection Criteria

Inclusion criteria	Exclusion criteria
The complete text was published in the Years (2000-2021) It directly or indirectly responds to the research questions (RQ)	Excluded all duplicated and reproduced studies and Articles that don't relate to research questions

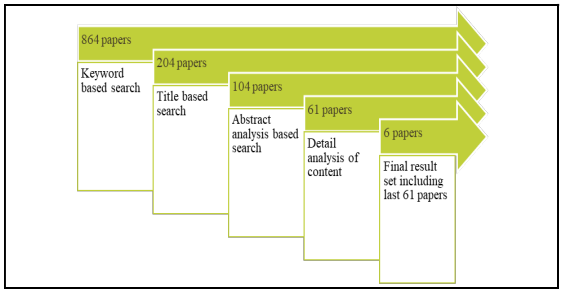

Figure 3: Number of publications gone through inclusion and exclusion criteria filters

Excluded all exclusion criteria and satisfies all inclusion criteria. The unauthorized journals, workshops, and conference proceedings are eliminated. Based on selection criteria 12 links,18 pdfs, and 70 studies were discarded. Based on the abstract, titles, keywords, detailed analysis, and final result set of 6 papers along with 61 papers of detailed content that purely satisfies our study in Fig 3.

3.4 Quality Assessment

QA helps in finding out the scale and quality of research. It helps define the population of research in different strategies [19] For evaluation and analysis of the result of the research process authors uses QA criteria

QA1: Data resources in this study used related to the review?

QA2: Does gap analysis done successfully through the research paper?

QA3: Extend to which research methodology is explained in the paper.

QA4: Result analysis achieved qualitatively?

QA5: Result analysis achieved quantitatively?

Five Quality Assessment criteria are used for assessing 104 studies to analyze the quality of the study. Quantitative analysis is performed on references for assessing their quality by scoring each QA criterion as 3(substantial), 2(intermediary), and 1(marginal). Thus, the SLR consisted of 104 papers in which there are a number of research that achieved substantial-quality value (Figure 4).

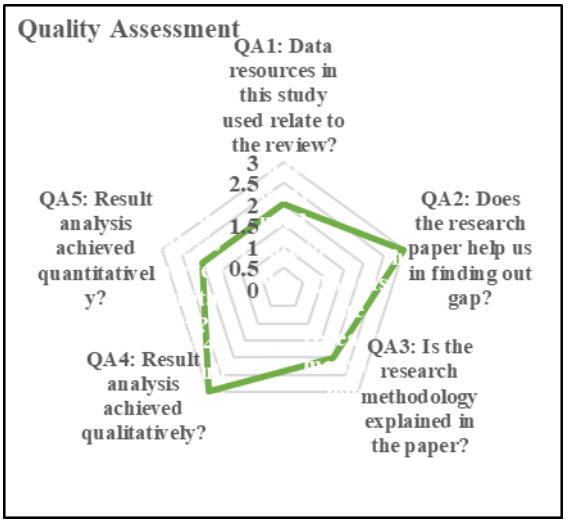

Figure 4: Quality Assessment

3.5 Data Synthesis

The study of 104 references leads to data extraction and data synthesis processes for extracting useful information. Statistical analysis is done to perform data extraction and synthesis. The author's description included primary studies including their sources, publications, and research methodologies.

3.5.1 Publication Sources Overview

As data sources for the current study, these are distributed in different types, these types are statistically presented through the figure. The majority of the studies were published and cited in journals and conferences. Figure 5 presents the distribution of these studies derived from their publication sources including 50 Articles from different journals (48%), 28 conference reports (27%), 7 Book sections/reference books (7%), 4 Workshop proceedings (4%), 8 Symposium (8%), 5 Theses (5%), 2 technical reports (2%).

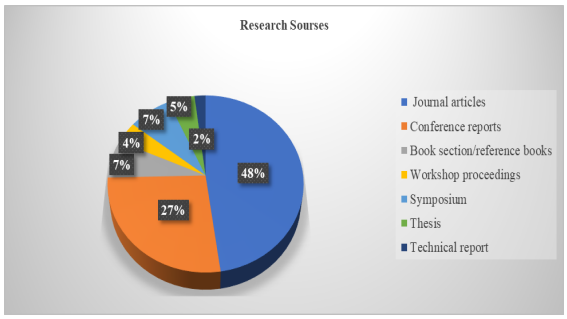

Figure 5: Research Sources

3.5.2 Methodology of Studies overview

The methodology is distributed differently according to the aim of the area of study. These are distributed and shown statistically in figure 6. It represents the distribution of all studies through research methodologies including 21 articles that used quantitative methods (20%), 17 qualitative techniques (16%), 13 mixed methods (12%), 28 reviews (27%), and 25 study/survey (25%).

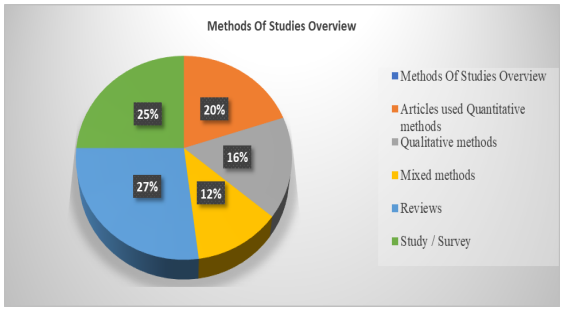

Figure 6: Methodologies used

4. RESULTS FOR RESEARCH QUESTIONS

The author then moves on to respond to research questions after assessing, extracting, and distributing all 104 searches according to their categories, methodology, and criteria. The mapping and grouping of related studies for all RQ-based investigations. This section summarises our pertinent research discussion, review, and conclusions. Results for each RQ are provided in the subsections that follow.

RQ1: What are different domains that use Artificial Immune System concepts?

Researchers recognized 42 issues related to analysis for RQ1. AIS concepts are used in various domains to upgrade their work or propose new work. This table is divided by domain and year of publications. The titles and abstracts of the retrieved articles were used to determine content relevancy. (Table 2)\

RQ2: What are the various proposed approaches achieved in this study?

Authors have identified 22 studies that achieve their aim of proposing a system, model, or algorithm. Table 3 is analysed and grouped by the aim of papers in achieving the proposed results from the papers that are discussed in RQ1.

RQ3: Which methodologies/algorithms are used?

After analyzing different modules of papers, it has been achieved that various computational aspects, algorithms, and methodologies are used to achieve the result, i.e., whether proposing a model or proposing an algorithm quantitatively or qualitatively. So, the authors have identified the following references which have used different methodologies and algorithms. (See Table 4)

RQ4: What is the basic strength of AIS analyzed as a scope for future research topics?

Various experimental results qualitatively or quantitatively achieved their aim of the study to develop or propose a model, algorithms, or some theoretical background. 21 papers have used qualitative study and 17 papers used qualitative and 13 papers used mixed methodology,28 reviews, 25 studies/surveys. Depending on the future scope the papers are analyzed and discussed for the strength of AIS. The following are some observations (see Tables 5&6).

Our analysis allows a better overview of current technical and methodical developments in this field and foresight of future research directions

A study of the current advancements in the literature as well as a theoretical framework on the key concepts and ideas of artificial immune systems (AIS) has been done. This has given people incentive to research AIS-related topics further and help advance the creation of new AIS models and methods. To show how the AIS techniques can be used to solve various data analysis tasks and cope with real-world challenges, a case study was conducted.

The key components of the AIS mechanisms have been investigated by researchers, who have used them in a variety of applications. Some AIS methods have been discovered to be more effective than others for particular application areas based on their characteristics.

This study discovered that self/non-self recognition-based fault detection and computer security applications frequently employed negative selection models and methods. As an alternative,

applications for clustering, classification, data analysis, and data mining used artificial immune network techniques. Most optimization issues were solved using clonal selection models. Although AIS models have had considerable success in a variety of application domains, key theoretical challenges, such as the creation of unified frameworks, convergence, and scalability, still need to be further investigated.

In addition to drawing inspiration from biological immunity principles and mechanisms, hybridizing artificial immune systems with other soft computing paradigms like neural networks, fuzzy logic, and genetic algorithms might be advantageous. They could also be researched more thoroughly and used to tackle more difficult application domains and difficult real-world issues. Above mentioned tables include a brief summary of each model or technique, the biological immune system aspect modeled, the type of representation utilized, and the application area to which AIS has been applied.

5. CRITICAL FINDINGS

The major gap in this research is that Artificial Immune System has not been used to assess and classify different types of risks involved in the project development of organizations or enterprises. Therefore, we can apply various computational techniques in the Artificial Immune system to assess and mitigate different types of risks that are hurdles in the way of a development project in an organization. This will surely help managers of that organization to run the system of project development smoothly by reducing, eliminating, or transferring risks. There are many methodologies created for risk management, but some failures are specified in those methodologies or they are not complete. Hence the research wants to find a relationship between the Immune System and other engineering domains to solve their problems. This will deliver a new approach with a new description of the Risk mitigation process and project development process in organizations and enterprises [39][40][41]. As AIS is used in other domains, similarly we develop a shield of protection in problems during project development using AIS, based on the human immune system philosophy. Input to this type of system will be a nature-inspired algorithm that helps in developing an efficient framework for an organization or enterprise [42][43][44]. AIS can increase the accuracy and speed of detection models developed for any type of problem statement. We create more memory cells for those records which contain critical fields. The immune system is a notable learning system. AIS has the features of being self-adaptive and distributed. Thus, it is justified that on the basis of the efficient functionalities of AIS, it can be used in the development of an efficient and accurate risk mitigation framework for managers of an organization to deal with various hurdles during project development. On the basis of the literature survey, we have found results and findings of different frameworks/models based on AIS which have been developed successfully as mentioned in table 3.

Detailed and careful reviews of the experts and researchers also promote a greater understanding of the chosen topic, procedures, methods, and algorithms and enable the frame of useful hypotheses. In the current state scenario, models exist according to research that considers risks associated with different stages of project development. The study further reveals that such models, in use, lack completeness from one or more perspectives.

AIS can be very helpful in research on micro and small-scale organizations to overcome risk strategies. Maintaining a library of hurdles and updating that library according to change can be one point that came in the way of the implementation of the framework. Many times, of the questionnaire, may prolong the research conduction time. Unique characteristics of the survey place a high value on personal initiative and on the spot problem solving.

6. CONCLUSIONS

We did a study on a Systematic Literature Review on Artificial Immune Systems seeking based on these developments and successes in Artificial Immune Systems research. Our analysis included 104 studies between 2000 and 2021 in a comprehensive review. It concentrated on responding to the four questions in Section 3. The use of the Artificial Immune System in several domain areas was the topic of the first query. The second question focuses on several proposed strategies that were attained in this study. The final question focuses on the Artificial Immune System's methods and algorithms as they are applied in various technical disciplines. Finally, we concentrated on the Artificial Immune System's power, which was examined as a potential area for further study.

A significant obstacle to the innovation and competitive advantage of one study is the

absence of an Artificial Immune System to manage various hazards in the project development of organizations. Therefore, it is necessary to produce data that demonstrates how previous studies are advantageous to researchers. Future researchers and practitioners in Artificial Immune Systems will find this review to be useful in applying the idea of AIS to other fields. The research is ongoing in the direction of enhancing the system development process using techniques and algorithms of Artificial Immune System, and it is clear from the aforementioned results that there is still much room for advancement in this field. The study further reveals that such domain areas where research must proceed further lack completeness from one or more perspectives. As future work, we can build more models to combine qualitative and intelligent risk models.

7. CONFLICT OF INTEREST:

The authors certify that they have NO affiliations with or involvement in any organization or entity with any financial interest (such as honoraria; educational grants; participation in speakers' bureaus; membership, employment, consultancies, stock ownership, or other equity interest), or non-financial interest (such as personal or professional relationships, affiliations, knowledge or beliefs) in the subject matter or materials discussed in this manuscript.

REFERENCES:

[1] U. Aickelin, D. Dasgupta, F. Gu, "Artificial Immune Systems", Search methodologies Introductory Tutorials in Optimization and Decision Support Techniques, 2013, DOI:10.1007/978-1-4614-6940-7_7, 187-211

[2] Immunology Department of Biotechnology Indian Institute of Technology, Kharagpur, NPTEL, Module No. 01 Lecture No. 01 Basic Concepts in Immunology

[3] Alma Moon Novotny, Biochemistry and Cell Biology Lecturer Department of Biosciences, Ph.D. Rice University, "Fundamentals of Immunology: Innate Immunity And B-Cell Function", Coursera.Org/Verif Y/8PVNX66M8R8J, A Course Authorized by Rice University and offered through Coursera, 2021.

[4] Abul K. Abbas, Andrew H. Lichtman, "Cellular and Molecular Immunology", Saunders,2005

[5] The Biology Project, The University of Arizona, Http://Www.Biology.Arizona.Edu, 2004

[6] James A Sullivan, Www.Cellsalive.Com

[7] Mario Poggiolini, "The Feature Detection Rule and its Application Within the Negative Selection Algorithm" A Theses, University of Pretoria, 2009.

[8] Caiming Liu, Minhua Guo, Lingxi Peng, Jing Guo, "Artificial Immunity Based Model for Information System Security Risk Evaluation", 2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT), 2010, ISBN:978-1-4244-5517-1, DOI: 10.1109/EDT.2010.5496552, 39-42.

[9] J.R. Al-Enzi, M.F. Abbod, S. Alsharhan, "Artificial Immune Systems-Models, Algorithms and Applications," International Journal of Research and Reviews in Applied Sciences (IRAS), 2010, 118-131.

[10] Elaine Rich, Kevin Knight, Shivashankar B Nair, "Artificial Intelligence",2016, 3rd edition, Mc Graw Hill Education.

[11] Dario Floreano, Claudio Mattiussi, "Bio-Inspired Artificial Intelligence Theories, Methods, And Technologies", 2008, Massachusetts Institute of Technology Press.

[12] Joseph Feher, "Quantitative Human Physiology", Academic Press Series in Biomedical Engineering

[13] Janis Kuby, "Immunology", W.H. Freeman

[14] Sarunas Raudys, Justas Arasimavicius, Gene Biziulevciene; "Learning the Affinity Measure in Real and Artificial Immune Systems"; IEEE 3rd International Conference on Biomedical Engineering and Informatics, 2010, 2904-2908.

[15] J. Timmis, T. Knight, L.N. De Castro and E. Hart "An Overview of Artificial Immune Systems", Computation in Cells and Tissues, Chapter of Natural Computing Series, 2004, 51-91

[16] Steven A. Hofmeyr, Stephanie Forrest, "Architecture for an Artificial Immune System", Journal of Evolutionary Computation, 2000, DOI: 10.1162/106365600568257, 443-473.

[17] Vitoantonio Bevilacqua, Filippo Menolascina, Roberto T. Alves, Stefania Tommasi, Giuseppe Mastronardi, Myriam Delgado, Angelo Paradiso, Giuseppe Nicosia,Alex A. Freitas, "Artificial Immune System In Bioinformatics", Computational Intelligence

in Biomedicine and Bioinformatics book series , 2008, 271–295, 2008

[18] Neda Soltani Halvaiee, Mohammad Kazem Akbari, "A Novel Model for Credit Card Fraud Detection Using Artificial Immune Systems ", Journal of the World Federation on Soft Computing,2014,
DOI: 10.1016/J.Asoc.2014.06.042, 40-49

[19] Cagatay Catal, Banu Diri, "Application and Benchmarking of Artificial Immune System to Classify Fault-Prone Modules for Software Development Projects", International Conference Applied Computing, Salamanca, 2007, 1-5

[20] Vijeta, Mr. Vivek Sharma, "A Review on Network Intrusion Detection Using Artificial Immune System (AIS)", International Journal of Engineering Research & Technology, 2014, ISSN: 2278-0181, 388-393

[21] Moeen Ali, Naqvi Merve, Astekin Sehrish, Malik Leon, Moonen Simula, "Adaptive Immunity for Software: Towards Autonomous Self-Healing Systems", 2021, IEEE International Conference on Software Analysis, Evolution, and Reengineering, ISBN:978-1-7281-9630-5, DOI:10.1109/SANER50967.2021.00058, 521-525.

[22] Ali Louati, Sabeur Elkosantini, Saber Darmoul, Lamjed Ben Said, "An Immune Memory Inspired Case-Based Reasoning System to Control Interrupted Flow at A Signalized Intersection", Artificial Intelligence Review, 2017, ISSN: 2099–2129, DOI: 10.1007/s10462-017-9604-0

[23] Berna Haktanirlar Ulutas · Sadan Kulturel-Konak, "A Review of Clonal Selection Algorithm and Its Applications", 2011, An International Science and Engineering Journal, DOI: 10.1007/s10462-011-9206-1, 117–138

[24] Zhuhong Zhang, Shuqu Qian, Xin Tu, "Dynamic Clonal Selection Algorithm Solving Constrained Multi-Objective Problems In Dynamic Environments", 6th International Conference On Natural Computation, 2010, ISBN:978-1-4244-5961-2, DOI: 10.1109/ICNC.2010.5584014, 2861-2865.

[25] Zaineb Chelly Dagdia, Pavel Avdeyev, Md. Shamsuzzoha Bayzid, "Biological Computation and Computational Biology: Survey, Challenges, and Discussion" An International Science and Engineering Journal, 2021, DOI:10.1007/S10462-020-09951-1,4169-4235.

[26] Farhoud Hosseinpour, Kamalrulnizam Abu Bakar, Amir Hatami Hardoroudi, Nazaninsadat Kazazi, "Survey on Artificial Immune System as A Bio-Inspired Technique for Anomaly Based Intrusion Detection Systems", IEEE International Conference on Intelligent Networking and Collaborative Systems, ISBN: 978-0-7695-4278-2/10, DOI 10.1109/INCOS.2010.40

[27] Vladimir Vasilyev, Rinat Shamsutdinov, "Distributed Intelligent System of Network Traffic Anomaly Detection Based on Artificial Immune System", 7th Scientific Conference on Information Technologies for Intelligent Decision-Making Support, 2019, DOI 10.2991/itids-19.2019.7, ISBN 978-94-6252-728-7, 40-45.

[28] Fabio González, "A Study of Artificial Immune Systems Applied to Anomaly Detection", A Dissertation, University of Memphis, 2003

[29] Cai Shuqin, Wang Ge, Cai Hong, "Research on the Applications of Immune Network Theory in Risk Assessment", IEEE ISECS International Colloquium on Computing, Communication, Control, and Management; ISBN:978-0-7695-3290-5, DOI: 10.1109/CCCM.2008.324, 1-5

[30] Andrew Watkins∗ And Jon Timmis, Lois Boggess, "Artificial Immune Recognition System (AIRS): An Immune Inspired Supervised Learning Algorithm", Genetic Programming and Evolvable Machines,2004, DOI:10.1023/B:ENP.0000030197.83685.94,291-317.

[31] Jason Brownlee, "Artificial Immune Recognition System (AIRS) A Review and Analysis", Technical Report No. 1-02, January 2005,1-44.

[32] Zhou Ji, Dipankar Dasgupta, "Revisiting Negative Selection Algorithms", The Massachusetts Institute of Technology Evolutionary Computation, 2007, 223-251

[33] Satyasai Jagannath Nanda, "Artificial Immune Systems: Principle, Algorithms and Applications", A Theses for the Degree of Master of Technology (Research) in Electronics and Communication Engineering, National Institute of Technology, Rourkela

[34] G. Costa Silva and D. Dasgupta. "A Survey of Recent Works in Artificial Immune Systems." Handbook on Computational Intelligence.

World Scientific, 2015, DOI: 10.1142/9789814675017_0015 547–586.

[35] Noor Hayani Abd Rahim, Steven Furnell, "A Systematic Review of Approaches to Assessing Cybersecurity Awareness", The international journal of cybernetics, systems, and management sciences, 2015, Emerald Group Publishing Limited, ISSN:0368-492X, DOI 10.1108/K-12-2014-0283, 606-622

[36] Karto Iskandar, Muhammad Ikhwan Jambak, Raymondus Kosala, Harjanto Prabowo, "Current Issue on Knowledge Management System for Future Research: A Systematic Literature Review", International Conference on Computer Science and Computational Intelligence, 2017, DOI 10.1016/j.procs.2017.10.011, 68-80.

[37] Omayma Husain, Naomie Salim, Rose Alinda Alias, Samah Abdelsalam and Alzubair Hassan, "Expert Finding Systems:A Systematic Review",Appl.Sci. 2019, Doi:10.3390/App9204250, 1-32

[38] Anass Rabii, Ounsa Roudies, "Information and Cyber Security Maturity Models: A Systematic Literature Review", Information & Computer Security, 2020, ISSN 2056-4961, DOI 10.1108/ICS-03-2019-0039,627-644.

[39] Junjiang He, Tao Li, Beibei Li∗, Xiaolong Lan, Zhiyong Li, Yunpeng Wang, "An Immune-Based Risk Assessment Method for Digital Virtual Assets", Journal of Computer and Security,2021, DOI: 10.1016/J.Cose.2020.102134, 0167-404

[40] Tao Liu; Yan Zhou; Chu-Hui Xie, "E-Commerce Risk Assessment Model Bases Immune Principal", Chinese Conference on Pattern Recognition2009, ISBN: 978-1-4244-4199-0, DOI: 10.1109/CCPR.2009.5344005, 1 – 5

[41] R.S. Srinivasan, "Supply Chain Immunity: A Methodology for Risk Management", International Journal of Services Sciences, 2010, DOI: 10.1504/IJSSCI.2010.029861, 1 – 20

[42] Bibhash Roy, Ranjan Dasgupta, "A Study on Risk Management Strategies and Mapping with SDLC", 2nd International Doctoral Symposium on Applied Computation and Security Systems, 2015, DOI:10.1007/978-81-322-2653-6_9.

[43] Bo Yang and Yuqi, "Research on the Characteristics of the Growth Risk Sources of New Ventures Based on Immune Theory", Journal of Physics: Conference Series, Yao 2020 J. Phys.: Conf. Ser. 1651 012045

[44] Gupta, Shikha, Saini, A. K and Belwal, Rajendra "An Artificial Intelligence-Based Framework for Risk Management of IT Systems", University: Teerthanker Mahaveer University, - A Theses,2018,Http://Hdl.Handle.Net/10603/226798

[45] Satyasai Jagannath Nanda, "Artificial Immune System: Principles, Algorithms, and Applications", A Theses, The National Institute of Technology, Rourkela, 2009.

[46] Fabio González, "A Study of AIS applied to Anamoly Detection", A Dissertation, The University of Memphis 2003

[47] Pearl Brereton, Barbara A. Kitchenham, David Budgen, Mark Turnera, Mohamed Khalil, "Lessons from Applying the Systematic Literature Review Process Within the Software Engineering Domain" Journal of Systems and Software, 2007, 571–583.

[48] Tranfield D, Denyer D, Smart P. "Towards A Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review". British Journal of Management, 2003, Doi:10.1111/1467-8551.00375, 207-222.

[49] Kitchenham B, Charters S. "Performing Systematic Literature Reviews in Software Engineering. Engineering", Proceedings - International Conference on Software Engineering, 2006, Doi:10.1145/1134285.11345001051-1052.

[50] Okoli C, Schabram K. "A Guide to Conducting a Systematic Literature Review of Information Systems Research", Communications of the Association for Information Systems, 2015, Doi:10.2139/Ssrn.1954824, 879-910

[51] Computation,2000,DOI:10.1162/106365600568257, 443-473.

[52] Azadeh Sarkheyli, Norafida Binti Ithnin, Arezoo Sarkheyli, "Study of Immune System of Human Body and Its Relationship with Risk Management in Organizations", 5'th International Symposium of Advances on Science and Technology (IEEE), 2011, Khavaran Higher-education Institute, Mashhad, Iran.

[53] Jason Brownlee, "Immunos-81 the misunderstood Artificial Immune System", Technical Report, 2005, 1-37.

[54] Simon M. Garrett, "How Do We Evaluate Artificial Immune Systems?", Evolutionary Computation,2005,
DOI: 10.1162/1063656054088512, 145-177.

[55] Brent Summers, Learnquest, "Artificial Intelligence Algorithms Models and Limitations", Coursera.Org/Verif Y/78MNFZTVGUBE, A Course Authorized by Learnquest and offered through Coursera, 2021-

[56] Liang Zhiwei, Zheng Chonghu, Shen Jie, Liu Juan, Zhu Songhao, "A Multi-Agent Task Allocation Strategy Based on Artificial Immune System", IEEE 25th Chinese Control and Decision Conference, DOI 10.1109/CCDC.2013.6561551, 2013, ISSN: 1948-9439

[57] Hexia Meng, Bing Wang, "A Modified Artificial Immune Algorithm for Fuzzy Resource-Constrained Project Scheduling Problem", 13th IFAC Symposium on Large Scale Complex Systems: Theory and Applications, 2013. DOI:10.3182/20130708-3-CN-2036.00116, Corpus ID: 62156154, 450-455.

[58] S. M. A. Mavee, E. M. Ehlers, "A Multi-Agent Immunologically-Inspired Model for Critical Information Infrastructure Protection", IEEE 11th International Conference on Trust, Security, and Privacy in Computing and Communications, 2012, ISBN:978-0-7695-4745-9,
DOI 0.1109/Trustcom.2012.40, 1089-1096.

[59] Ze-Jun Wu, Yong Han, Yi-Wen Liang, "A Real Estate Evaluation Risk Early Warning Model Based on Immune Algorithm", IEEE International Conference on Machine Learning and Cybernetics, 2007, ISBN:978-1-4244-0972-3

[60] Hua Yang,1,2 Tao Li,1 Xinlei Hu,1 Feng Wang,1 And Yang Zou1, "A Survey of Artificial Immune System Based Intrusion Detection System ", Scientific World Journal Volume 2014, Article ID 156790, DOI:10.1155/2014/156790

[61] Guilherme Costa Silvaa, Eduardo E.O. Carvalhoa, Walmir Matos Caminhas, "An Artificial Immune Systems Approach to Case-Based Reasoning Applied to Fault Detection and Diagnosis", Expert systems with applications, 2019,0957-4174,Doi: 10.1016/J.Eswa.2019.112906

[62] Ehsan Kamalloo And Mohammad Saniee Abadeh, "An Artificial Immune System for Extracting Fuzzy Rules in Credit Scoring", IEEE Congress on Evolutionary Computation, 2010, ISBN: ISBN:978-1-4244-6909-3,

[63] J. Timmis, A.R. Ismail, J.D. Bjerknes, A.F.T. Winfield "An Immune-Inspired Swarm Aggregation Algorithm for Self-Healing Swarm Robotic Systems", Journal of biosystems, 2016, DOI: 10.1016/J.Biosystems.2016.04.001, 1-17

[64] PeterSchmiedgen, Sebastian Wiesenhütter, Jörg Rainer Noennig, "Transferring Functions of Biological Immune Systems to Communication Processes in Disasters Using Cellular Automata", 18th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, Procedia Computer Science, 2014, Doi: 10.1016/J.Procs.2014.08.173, 1333-1341

[65] Wael Said, Ayman Mohamed, Mostafa, "Towards a Hybrid Immune Algorithm based on Danger Theory for Database Security",IEEE, ISSN:2169-3536,DOI:10.1109/ACCESS.2020.3015399, 145332 – 145362

[66] Ahmad Reda And Zsolt Csaba Johanyák, "Survey on Five Nature-Inspired Optimization Algorithms", 2021, ISSN 2064-8014, 173-183, DOI: 10.47833/2021.1.CSC.001

[67] Olfa Nasraoui, Fabio González Cesar Cardona, Dipankar Dasgupta, "Artificial Immune Systems and Data Mining: Bridging the And Data Mining: Bridging the Gap with Scalability and Gap with Scalability and Improved Learning", A Demo/Poster at The National Science Foundation Workshop on Next Generation Data Mining, Nov. 2002

[68] Mohamed Ahmed Mohamed Ali and Mohd Aizaini Maarof, "Malware Detection Techniques Using Artificial Immune System", Proceedings of the International Conference on IT Convergence and Security 2011, Lecture Notes in Electrical Engineering 120, DOI: 10.1007/978-94-007-2911-7_55, 2012

[69] Inadyuti Dutt, Samarjeet Borah, Indrakanta Maitra "Intrusion Detection System Using Artificial Immune System", International Journal of Computer Applications (0975 – 8887) Volume 144 – No.12, 2016, 19-22

[70] Bernardo J. B. Caldas, Flávio R. S. Oliveira, Fernando B. De Lima Neto, "Improving Support Of Appropriate Executive Decisions By Combining Artificial Immune Systems And Fuzzy Logic", 2008,IEEE,1522-4899/08,
DOI 10.1109/SBRN.2008.13

[71] Nawel Bayar, Saber Darmoul, Sonia Hajri-Gabouj, Henri Pierreval "Fault Detection, Diagnosis and Recovery Using Artificial Immune Systems: A Review", Engineering Applications of Artificial Intelligence the

International Journal of Intelligent Real-Time Automation, 2015, Doi: 10.1016/J.Engappai.2015.08.006, 43-57.

[72] He Yang; Yi-Wen Liang; Jia Chen; "Definition of Danger Signal in Artificial Immune System with Cloud Method", Fourth International Conference on Natural Computation,2008, ISBN: 978-0-7695-3304-9, DOI: 10.1109/ICNC.2008.711, 644 – 647

[73] Bo Yang, Meifang Yang, "Data-Driven Network Layer Security Detection Model and Simulation for The Internet of Things Based on An Artificial Immune System", S.I.: DPTA Conference, 2020, DOI: 10.1007/s00521-020-05049-5

[74] Sahar Aldhaheri A, Daniyal Alghazzawi, Li Cheng, Ahmed Barnawi, Bandar A. Alzahrani "Artificial Immune Systems Approaches to Secure the Internet of Things: A Systematic Review of the Literature and Recommendations for Future Research", Journal of Network and Computer Applications 2020, 1084-8045, DOI: 10.1016/j.jnca.2020.102537

[75] Bejoy B J, Dr. Janakiraman S, "Artificial Immune System Based Intrusion Detection Systems-A Comprehensive Review", International Journal of Computer Engineering & Technology, ISSN: 0976-6367, 85–95

[76] Sahar Aldhaheri A, Daniyal Alghazzawi, Li Cheng, Ahmed Barnawi, Bandar A. Alzahrani "Artificial Immune Systems Approaches To Secure The Internet Of Things: A Systematic Review Of The Literature And Recommendations For Future Research", Journal Of Network And Computer Applications,volume- 157 Issue C January 2020, ISSN: 1084-8045

[77] Priyadharshini Kaliyamoorthy, "Enhancing Data Security Using Global Mutation Based Novel Artificial Immune Network Optimization in Public Cloud Storage System", Transactions on Emerging Telecommunications Technologies, 2021, Doi: 10.1002/Ett.4390

[78] G. A. Samigulina, Z. I. Samigulina, "Design of Technology for Prediction and Control System Based on Artificial Immune Systems and The Multi-Agent Platform JADE, Agents and Multi-Agent Systems: Technologies and Applications 2020, DOI: 10.1007/978-981-15-5764-4_13, 143-153

[79] Pallav Negi, "Artificial Immune System Based Urban Traffic Control", A Theses, Texas A&M University, 2006

[80] S, Joseph Dominic Vijayakumar, Saravanan, M, "Artificial Immune System Algorithm for Optimization of Permutation Flow Shop Scheduling Problem", A Theses, AnnaUniversity,2016,Http://Hdl.Handle.Net/10603/181398

[81] Kumar, Amit, "Design and Implementation of Artificial Immune System for Security of Computers", Theses, Jaypee University of Engineering and Technology, Http://Hdl.Handle.Net/10603/42726, 2015

[82] Verma, Karunendra, "Devising Efficient Technique for Web Structure Mining Through Artificial Immune System", Theses, Sir Padampat Singhania University, Http://Hdl.Handle.Net/10603/293452, 2019

[83] Kamahazira Zainala, Mohd Zalisham Jalia, "A Perception Model of Spam Risk Assessment Inspired by Danger Theory of Artificial Immune Systems", International Conference on Computer Science and Computational Intelligence, 1877-0509, 2015, DOI: 10.1016/J.Procs.2015.07.530, 152-161

[84] Caiming Liu, Minhua Guo, Lingxi Peng, Jing Guo, Shu Yang, Jinquan Zeng, "Artificial Immunity Based Model for Information System Security Risk Evaluation", IEEE International Conference on E-Health Networking, Digital Ecosystems, and Technologies, 2010, ISBN:978-1-4244-5517-1,DOI: 10.1109/EDT.2010.5496552, 39-42

[85] Fei-Xian Sun, Shen-Wu Zhang, "Immunity Inspired Risk Assessment Approach for Network Security", IEEE International Conference on Web Information Systems and Mining, 2009, ISBN: 978-0-7695-3817-4/09, DOI 10.1109/WISM.2009.110, 515-318

[86] Delip Rao, David Yarosky, Chris Laplacian; "Affinity Measures Based on The Graph Laplacian"; 3rd Telegraphs Workshop on Graph-Based Algorithms in Natural Language Processing, 2008, 41-48

[87] Dr. Gene Mayer, "Immunoglobulins-Antigen-Antibody reactions and selected tests"2010 Richardhunt http://www.microbiologybook.org/mayer/ab-ag-rx.htm

[88] Yanheng Ren, Xianghua Wang, Chunming Zhang, "A Novel Fault Diagnosis Method Based on Improved Negative Selection Algorithm", IEEE Transactions on Instrumentation and Measurement, Vol. 70,

2021, 1557-9662, ISSN: 0018-9456, DOI: 10.1109/TIM.2020.3031166, 1-8

[89] Kaushik Ghosh, Srinivasan, "Negative Selection Algorithm: An Artificial Immune System for Fault Diagnosis in Continuous and Batch Processes", Proceedings of AIChE Annual Meeting, 2010

[90] Dan W Taylor and David W Corne, "An Investigation of The Negative Selection Algorithm for Fault Detection in Refrigeration Systems", International Conference on Artificial Immune Systems,2003, DOI: 10.1007/978-3-540-45192-1_4, 34-35

[91] Nasir Rashid, Javaid Iqbal, Fahad Mahmood, Anam Abid, Umar S. Khan, and Mohsin I. Tiwana, "Artificial Immune System–Negative Selection Classification Algorithm (NSCA) For Four Class Electroencephalogram (EEG) Signals", Frontiers in Human Neuroscience, Article,2018, DOI: 10.3389/Fnhum.2018.00439

[92] X. Z. Gao, S. J. Ovaska, X. Wang, "Multi-Level Optimization of Negative Selection Algorithm Detectors with Application in Motor Fault Detection ", Intelligent Automation and Soft Computing, Vol. 16, No. 3, Pp. 353-375, 2010

[93] Mohammad Tahir Khan, Mohammad Abdul, Anam Abid, Fazale Nasir, "Robot Fault Detection Using an Artificial Immune System (AIS).", Conference on Evolvable Hardware Proceedings, 2003, ISBN:0-7695-1977-6, DOI:10.2316/Journal.201.2015.2.201-2704

[94] Kevin Leung, France Cheong, Christopher Cheong, "Consumer Credit Scoring Using an Artificial Immune System Algorithm", IEEE Conference on Evolutionary Computation 2007, ISBN:1-4244-1340-0/07, DOI: 10.1109/cec.2007.4424908, 3377-3384

[95] Ankita Trivedi, Amit hrivastava, Aumreesh Saxena, Manish Manoria,"Survey Analysis On Immunological Approach To Intrusion Detection", IEEE International Conference on Advanced Computation and Telecommunication, ISBN:978-1-5386-5367-8, DOI: 10.1109/ICACAT.2018.8933710

[96] Kevin Song, Paul Kim, Shivani Rajasekaran, Vedant Tyagi, "Artificial Immune System (AIS) Based Intrusion Detection System (IDS) For Smart Grid Advanced Metering Infrastructure (AMI) Networks",2018, http://hdl.handle.net/10919/83203

[97] Obinna Igbe Ihab Darwish Tarek Saadawi "Distributed Network Intrusion Detection System: An Artificial Immune System Approach", IEEE First Conference on Connected Health: Applications, Systems, and Engineering Technologies, 2016, ISBN: 978-1-5090-0943-5, DOI 10.1109/CHASE.2016.36

[98] Galina Samigulina, Zarina Samigulina, "Development of Industrial Equipment Diagnostics System Based on Modified Algorithms of Artificial Immune Systems and AMDEC Approach Using Schneider Electric Equipment", IEEE International Conference on Industrial Engineering, Applications and Manufacturing, ISBN: 978-1-7281-4590-7, DOI: 10.1109/ICIEAM48468.2020.9111977

[99] Sahar Aldhaheri , Daniyal Alghazzawi, Li Cheng, Bander Alzahrani, Abdullah Al-Barakati, "Deep DCA: Novel Network-Based Detection of IoT Attacks Using Artificial Immune System", Article,AppliedScience,2020, Doi:10.3390/App10061909

[100] Shang Rong-Hua, Jiaoli-Cheng, Li Yang-Yang, Wu Jian-She, "Quantum Immune Clonal Selection Algorithm For Multi-Objective 0/1 Knapsack Problems", Chinese Physics Letters Chinese Physical Society and IOP Publishing Ltd, 2010, DOI:10.1088/0256-307X/27/1/010308

[101] Xiao-Zheng Deng, Li-Cheng Jiao, Shu-Yuan Yang, Qiu-Yi Wu, "Color Image Segmentation In A Multidimensional Space Based On Clonal Selection Algorithm", Journal Of Electronics Information & Technology, 2010, DOI:10.3724/SP.J.1146.2009.00922.

[102] A.Merve Acilar, Ahmet Arslan, "Optimization of Multiple Input-Output Fuzzy Membership Functions Using Clonal Selection Algorithm", An International Journal of Applications, 2010, 1374-1381.

[103] Designlucas S. Batista, Diogo B. Oliveira, Frederico G. Guimaraes, Elson J. Silva, Jaime A. Ramirez, "Dynamic Multiobjective Clonal Selection Algorithm for Engineering", IEEE Transactions on Magnetics, 2010, 3033-3036

[104] Khaled A. Al-Sheshtawi, H. M. Abdul-Kader, Nabil A. Ismail, "Artificial Immune Clonal Selection Classification Algorithms for Classifying Malware and Benign Processes Using API Call Sequences", International Journal of Computer Science and Network Security, 2010, 31-39

Table 2. Domains based on AIS

S. No.	The domain makes use of the concept of AIS to reach the objective	Year	References
1.	Feature Detection	2008	[1]
2.	Anomaly detection	2003,2019	[59,67]
3.	Information System Security	2010	[6,75]
4.	Task Allocation	2013	[37]
5.	Project Scheduling (AIS+Fuzzy)	2013	[39]
6.	Critical Information Protection	2012	[40]
7.	Fraud Detection in credit card	2014	[41]
8.	Risk Early Warning Model	2007	[42]
9.	Complex Software System/self-healing system	2021	[45]
10.	Detection and Diagnosis of faults	2019,2015,2021	[46, 58,90,84]
11.	Credit Scoring (AIS+Fuzzy)	2010	[47]
12.	Self-healing Swarm Robotic system	2016	[48]
13.	Control system for interruption flow of signals	2017	[49]
14.	Database Security	2020	[51]
15.	Anomaly-based Intrusion Detection System	2010	[53]
16.	Data Mining	2002	[54]
17.	Malware Detection	2012	[55]
18.	Intrusion Detection System	2014,2014	[44, 56,63]
19.	Executive Decision (AIS+fuzzy)	2008	[57]
20.	Network Traffic Anomaly detection	2019	[59]
21.	Cloud Computing	2008	[60]
22.	Network Layer Security	2020	[61]
23.	Detection IoT attacks	2020	[97]
24.	Prediction and Control System	2020	[66]
25.	Urban Traffic Control	2006	[68]
26.	Securing Computers	2015	[71]
27.	Web Structure Mining	2019	[7]
28.	Perception Of Risk Assessment	2015	[73]
29.	Digital Virtual Assets	2020	[74]
30.	E-Commerce Risk Assessment	2009	[76]
31.	Supply Chain	2010	[79]
32.	Refrigeration fault detection	2003	[86]
33.	EEG Signals	2018	[87]
34.	Motor Fault detection	2010	[89]
35.	Industrial Equipment diagnosis system	2020	[97]
36.	Knapsack Problem	2010	[100]
37.	Color Image Segmentation in Multidimensional Space	2010	[101]
38.	Constrained multi-objective problems in dynamic environments	2010	[102]
39.	Optimization of multiple input/output fuzzy membership functions	2010	[103]
40.	Dynamic Multi-objective algorithm	2010	[104]
41.	Flow Shop Scheduling Problem	2016	[69]
42.	Risk management in IT systems	2018	[81]

Table 3. Proposed approaches

S. No.	Proposed system/model/algorithm	Year	References
1.	Autonomous self-healing software	2021	[45]
2.	Proposed immune-based database IDS based on Danger theory and Negative selection algorithm inspired by AIS mechanism	2020	[51]
3.	Study of AIS to secure IoT environment	2020	[61,62,64]
4.	An intelligent and adaptive traffic signal control system (TSCS) that adapts traffic signals (both phase sequencing and duration) to traffic disturbances at a single signalized intersection	2017	[49]
5.	A different agent-based IDS based on natural killer cells	2014,2016, 2017,2019	[43,44,56,63,93,94]
6.	Recovery of faults, errors, and failures in the Manufacturing system	2015,2019	[46,58]
7.	AIS-based fault detection model (AFDM)	2014	[41]
8.	Self, non-self-theory, danger theory for the malware detection system	2012	[55]
9.	Clonal selection is used in combination with a fuzzy logic approach to estimate the credit risk of loan applicants. (Proposed credit scoring system) Models to estimate credit risk of loan applicants	2010	[47]
10.	Risk evaluation in the information system security.	2010	[6]
11.	Inspired by the feature of AIS, a novel risk assessment approach for network security (IRAA) is proposed	2009	[78]
12.	The analogy between the immune system/the decision system. AED algorithm and negative selection to deal with the problem. Fuzzy logic is also used to extend AED	2008	[57]
13.	Model construction process and testing results with data from a real test in risk assessment of the managerial field (food safety risk assessment model) using immune network theory	2008	[77]
14.	Novel Intelligent alerting Model	2007	[42]
15.	Improving the Risk Analysis process by investigating Immune System activity and current procedures of Risk Management methodologies.	2015,2011	[23,25]
16.	Investigated different AIS algorithms to classify fault-prone modules to simplify quality assurance activities for software development projects	2007	[4,19]
17.	AIS computational paradigm and introduces different AIS models and techniques developed in the literature	2009,2010	[2,7]
18.	Developing a new optimization algorithm proposed concept	2016,2021	[52,69]
19.	Proposed theory to improve Risk Analysis process in an organization	2015,2020	[73,80,81]
20.	Best Classification algorithm	2003,2021, 2016,2010	[4,7,27,33,52,69]
21.	Modified Artificial Immune Algorithm	2013	[39]
22.	Proposed Clonal Selection Optimization Algorithm	2010,2011	[98,102]

Table 4. Methodologies used

S. No.	Methodologies or algorithms used
1.	AIS (adaptive and Self-learning system)
2.	A danger theory-based hybrid immune algorithm is presented to apply different countermeasures that can preserve the secrecy of data
3.	The AIS approaches have been divided into three main categories based on IoT layers, and detailed classifications have also been included based on different parameters
4.	The AIS approaches have been divided into three main categories based on IoT layers, and detailed classifications have also been included based on different parameters
5.	Concepts of BIS used to build new learning algorithm for case base and optimize with traffic disturbances and suggested combination of simulation –optimization, condensed nearest neighbour algorithm, and rule-based system
6.	NSA algorithm used to create NK cell detectors and Confusion matrix to find out response delay of the system
7.	AIS mechanisms and techniques are applied to fault detection, diagnosis, and recovery problem.
8.	Use an immune system inspired algorithm (AIRS)and improve it for fraud detection Use an immune system inspired algorithm (AIRS)and improve it for fraud detection
9.	Danger theory self–nonself approach to the problems of detecting the new malware and decreasing the amount of false positive alarms
10.	The proposed AIS-based classifier has high accuracy and interpretability, making it competitive with several well-known classification systems.
11.	The mechanisms of immature evolving into mature and mature evolving into memory embody the self-adaptation and self-learning of the immune model for recognition of harmful antigens (threats).
12.	Theoretical analysis and experimental results show that Risk Assessment Approach is valid
13.	Decision evaluation Assemble helpful executive decision systems that may be easily deployed to reduce some of the risks inherent in strategic decision making.
14.	Explores the feasibility of constructing a risk assessment model based on immune network theory
15.	The negative selection algorithm to create a nonself subset and detect risk Immune matching help in identifying and detecting nonself coming from outside
16.	User-defined parameters have been optimized to reach the classification accuracy
17.	Models are mainly based on immune network theory, clonal selection principles, and negative selection mechanisms.

Table 5. Strength of AIS

S. No.	The strength of AIS extracted
1.	Anomaly detection and diagnosis capabilities. Quantitative methods such as AISs are well-suited for FDDR, which strengthens our belief that they will suit self-healing software systems as well
2.	Dynamic, automated, memorization, and adaptive defense tools to obtain effective outcomes of aggregation, integration, and individualization.
3.	Desirable properties of the AIS provide flexible decision-making mechanisms for dynamic environments such as IoT, specifically in security situations (Timmis, 2004)
4.	Artificial Immune Systems (AIS) often use the idea of memory cells to retain good solutions to the problem under consideration. Immune memory, and the mechanism of affinity to control traffic at a signalized intersection
5.	AIS is used as anomaly-based detection model, build a model for nonself data using real-time data
6.	AIS are sources of pattern recognition that use qualitative methods considered as a data-based method.
7.	Based on AIS we can increase the accuracy and speed of both fault detection models, and cost functions to get better results for improved AIRS. We create more memory cells for those records which contain critical fields, and then the overall number of Fraud Memory Cells is higher than base AIRS
8.	The immune system is a notable learning system. Through the use of the innate immune components, B-cells and T-cells
9.	High accuracy and interpretability. One of the most compromises in evolutionary algorithms like AIS is balancing between exploration and exploitation. In this algorithm, exploring is done by mutation of B-cells, and exploiting is applied with the age formula. After cloning when fitness is increased, the age is increased.
10.	Researchers apply AIS to resolving problems of information security and gain achievements.
11.	AIS has the features of self-adaptive, distributed, and real-time. Therefore, it provides a good solution to risk assessment for network security.
12.	Quality of the executive approach and reduced uncertainty. Experimental results suggest that AIS and Fuzzy hybrid approach to executive decision-making could be used to assemble helpful executive decision systems that may be easily deployed to reduce some of the risks inherent in strategic decision making
13.	Practical, reliable, and capable of providing strategic decision-making tool
14.	The theory of Artificial immunology abstracts the attributes from the real estate evaluation market and codes them to build an abnormal detecting set
15.	The immune system is complete and could be the best model for simulating it with Risk management in the organization. Used in improving risk analysis process.
16.	Automatic, efficient, objective, and adaptive for new datasets. Efficiently, and accurately given remarkable results
17.	Artificial Immune Systems (AIS) have been investigated to classify fault-prone modules. AIS algorithms such as AIRS1, AIRS2, AIRS2 Parallel, Immunos1, Immunos2, Immunos99, CSCA, and CLONALG are investigated by varying user-defined parameters for best classification accuracy

Table 6. Future Aspects

S. No.	Future aspects of the study
1.	More research on data-driven self-healing software systems can be made using the AIS paradigm
2.	A danger Theory-based intrusion detection system for securing Vehicular ad-hoc networks VANETs could achieve satisfactory results.
3.	AIS theory must be very helpful in research on Securing IoT
4.	The system can be extended using other concepts and mechanisms inspired by biological immunity. The immune network theory can inspire mechanisms for multi-criteria decision-making to select a case among several candidate cases. The clonal selection theory provides optimization mechanisms that can improve the performance of antibodies and their sensitivity to abnormal traffic situations and disturbances
5.	Combine the concepts of AIS with other biologically inspired algorithms for designing better intrusion detection models. This will be a hot topic for future surveys in AIS.
6.	AIS approach or algorithm for FDDR. Mitigation procedure for manufacturing system using biological immunity.
7.	Cloud computing misuse detection using AIRS
8.	If we combine the two methods to increase the accuracy of detection and decrease the false positive alarms. And can use other techniques in AIS
9.	Improving the accuracy and performance of the AIS algorithms.
10.	Some researchers proposed some immunity-based ways for ISRE and Further searched for removing threats and vulnerabilities etc.
11.	In the future, we can take into account other related security facts such as network flows, vulnerabilities, attacks, etc.
12.	Using variables as to benefits, impacts, and urgency of a decision, other principles of AIS, different fuzzy sets, and rule matrices could be used to further increase the reliability and quality.
13.	Using variables as to benefits, impacts, and urgency of a decision, other principles of AIS, different fuzzy sets, and rule matrices could be used to further increase the reliability and quality.
14.	A relationship between detectors for various real-time problems is not made and can be used as a future study
15.	Risks to a company could happen in different forms, and they are not all computer-related. This study wants to focus on IT/IS risk management. Then in that case information risk management is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level.
16.	Concentrate on AIRS1 and try to develop a hybrid algorithm to enhance the performance of faulty module classification
17.	Motivation to continue exploring the AIS field and contribute to the development of new AIS models and techniques