Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 2, 2020

Review Article

ARTIFICIAL IMMUNE SYSTEM BASED FRAMEWORKS AND ITS APPLICATION IN CYBER IMMUNE SYSTEM: A COMPREHENSIVE REVIEW

Bejoy B J[1], Bijeesh TV[1], S Janakiraman[2]

[1]Assistant Professor,Department of Computer Science and Engineering,Christ (Deemed to be University)
[2]Assistant Professor,Department of Banking Technology,Pondicherry University

Received:24.11.2019 *Revised: 16.12.2019* *Accepted: 11.01.2020*

Abstract
Computer science has always mixed the concepts of biology and computers to enhance the way in which systems are designed. Artificial Immune System (AIS) is a Computational Intelligence strategy dependent on an organically enlivened computational system that can be utilized for taking care of complex computational issues. It tends to be seen that AIS is an incredibly various locale of research, going from the modeling immune systems to complex algorithms for specific applications. This paper exhibits an exhaustive survey of different frameworks developed in the artificial immune system and its application. Reviews of frameworks in AIS are uncommon and henceforth this paper gives an inside out audit of progressing research and challenges in AIS. We start by presenting AIS and give a thorough survey of different systems in AIS and its application in anomaly detection. We investigate the utilization of AIS in the Intrusion Detection System named the Cyber Immune System(CIS) and compares various AIS works applied to CIS. We conclude with various future extensions in the area of AIS research.

Keywords: Artificial Immune System; Intrusion Detection System; Cyber Immune System; AIS Framework.

DOI: http://dx.doi.org/10.31838/jcr.07.02.103

INTRODUCTION

The Internet and its remarkable advancement have added to the usage of the web by practically all fundamental administrations. A considerable volume of huge information, for instance, individual profiles and financial data is scattered and traded through the web. As the enthusiasm for the internet grows, so as the triggering of pernicious codes and assaults in the internet environment. This advancement has exposed infrastructures to a raising measure of security dangers from digital gatecrashers who modify and steal basic data that affect the integrity, confidentiality, and availability of services.

Artificial immune systems(AIS) is a computational approach that is propelled by the procedure and instruments of the human immune system. AIS is a Computational Intelligence technique based on a biologically inspired computational technique that can be used for resolving multifaceted computational glitches. Present-day Artificial Immune frameworks are enlivened by four sub-fields: Negative Selection(NSA) [1], Clonal Selection(CSA) [2,3], Immune network(INA) [4] and Danger Theory(DT) [5,6]. The systems are usually utilized for pattern recognition, clustering, and other optimization problems.

An intrusion detection system(IDS) is a scheme that screens the network as well as hosts to ascertain unauthorized activities that affect the confidentiality, integrity, and availability(CIA) of the data. IDS has a nearby association with the procedures and instruments of Human Immune Systems(HIS)which assists with recognizing pathogens that can cause destructive infections in individuals. So clearly systems motivated by HIS can be utilized in IDS likewise whose essential capacity is to recognize malignant bundles. Thus AIS is the prime contender for actualizing IDS as AIS is mapped from the Human immune system that is well known for battling pathogens and other non-self cells going into the human framework. Cyber immune system(CIS) is defined as "An immune framework that can be spawned in a network or host using the notions of artificial immune system that encourages the network/host to recognize and react to malicious entities like viruses, worms and so forth that when entered into the framework can inimically influence the ordinary functioning of the system". Cyber Immune System try to mimic the flexibility of HIS to fend off new and disguised viral polluted cells or tumor cells. So in this review, the AIS based approach used for Intrusion detection is called Cyber Immune System.

RELATED WORKS IN FRAMEWORKS BASED ON AIS

The initial conceptual framework for an Artificial Immune System was proposed by De Castro [7]. The methodology depicted was a layered strategy that contains layers like Representation, Affinity Measures and Immune calculations delineated in Fig 2.1. The premise is a Representation layer that is utilized to create an intellectual structure associated with immunity like organs, molecules, etc. and so forth together with a course of action of partiality counts to gauge the relationship of these artificial components and a plan of comprehensively helpful algorithms to signify the components of AIS. The representation layer represents the domain for which the model is to be intended which includes a presentation area or an object domain. Utilizing the premise, a depiction of the system's parts is chosen.

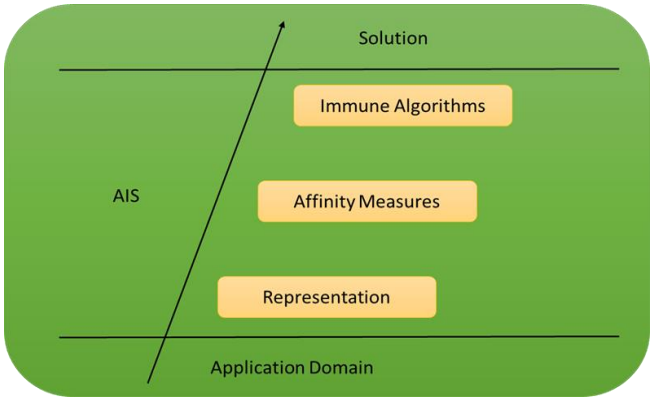

Fig 2.1: AIS framework based on [7]

The representation might be network traffic on the off chance that we picked IDS as the domain. The portrayal may fluctuate for every domain. When the representation is picked, an affinity or similarity measures are utilized to assess the associations of the components of the structure. The affinity measures are subject to the representation that is utilized. The most generally utilized similitude measures are fixated on Hamming distance and Euclidean distance. The concluding layer utilizes various immune-based algorithms like the Negative selection algorithm (NSA), Clonal Selection(CSA), Positive Selection(PSA) and Immune Network Algorithm(INA). The algorithms used has their own specific scope of services.

Stepney et al. [8] projected a conceptual framework with regards to the AIS model which can be utilized for multiple domains to create a meta-system. The proposed work states that bio-propelled algorithms are paramountly formed and dismembered with regards to an interdisciplinary framework that oblige modern organic models and very much established systematic standards. This methodology unites a couple of spaces into an ordinary meta-structure, with respect to AIS populace prototypes. The proposed work indicates the probability of a unique appearance of a meta-model, thus permitting the working of a precise calculation structure that is bio-prompted, yet not constrained to a specific biotic zone. Probes are utilized to give a (fractional and boisterous) perspective of the complex organic framework. From this confined view, the conceptual biological model is gathered and verified. From these biological models, an indicative computational framework is gathered and approved.

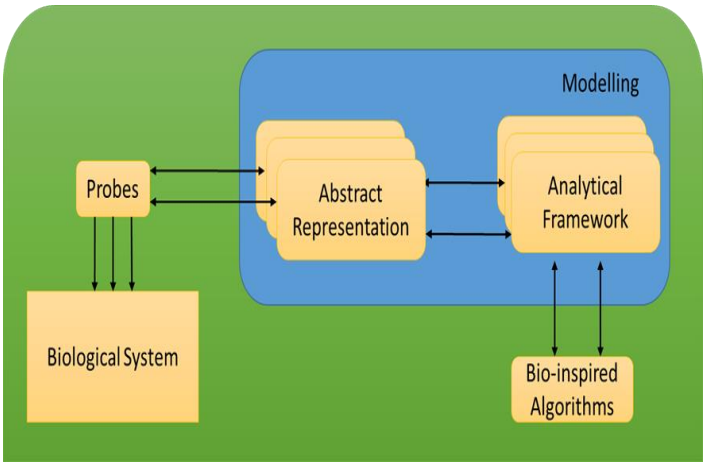

Fig 2.2: A Conceptual Framework for the bio-inspired system [8]

This approval uses numerical examination, standard issues, and structuring demonstrators. These structures give models for delineating and analyzing bio-enlivened calculations relevant to non-biological issues, maybe custom-fitted to an extent of issue territories, and substance to such a degree or as small natural genuineness as legitimate. This is basically a multidisciplinary technique, requiring participation between naturalists, mathematicians, and system specialists to construct a complete framework. A hypothetical model for the bio-affected zone is given in Fig 2.2. The proposed work likewise recommends a Meta-structure utilizing meta-tests, meta-portrayal, and meta-system for summing up the methodology offered above to incorporate multi-disciplinary models.

Twycross and Aickelin [9] applied the meta-framework used in [8] to be utilized in Artificial Immune frameworks combining contemplations from innate resistance. AIS system models have, all things considered, been energized by adaptive immunity as opposed to innate immunity. The purpose of this methodology is to chart meta-structure models utilizing innate insusceptibility. The recommended strategy uses the meta-structure to separate natural models. Structures of specialists shape a beneficial meta-depiction of a framework based on artificial systems, and various artificial structures rely upon the masses of companion specialists. Cells are seen as autonomous agents that form the foundation of the meta-structure. Signals which empower combinations of agents to control the limits and state of particular groups of agents are significant right now. A crucial piece of nature where these

specialists occur is named artificial tissue, where the arrangement plan of a domain wherein specialists can relate by methods of signaling. The depiction of the irresistible specialists at various stages offers an additional procedure that copied tissue desires to provide. The copied tissue licenses experts of AIS to utilize different phases of information around procedures. While underlining the piece of innate immunity, in fact, the innate and adaptive immunity are consolidated together and collaborate to form a secure framework. Fitting together the properties proposed with those of the ordinary populace and framework models would engage AIS to mimic their natural accomplices.

Ahmed [10] recommended a hypothetical system that assimilates the conceptual structure of AIS proposed in [7] and produce an engineering structure to make a crossbreed system for improving AIS. The created crossbreed model is used to develop a use for AIS based invasion deterrence and self-repairing structure as portrayed in Fig 2.3. At first, the area of utilization ought to be resolved. Then comes the objectives that need to be worked out for the plan. Afterward, the necessities to accomplish the objectives should be set up. This is trailed by requests for a natural plan followed by examining and observing such a plan, that would present to achieving the objectives. After this, the differentiation and resemblances among the natural and calculational structures must be developed. These connections will be the principles in the improvement of the conceptual framework, which ought to be shown numerically. This numerical structure easily changed over into a calculational portrayal and can be resolved as an algorithm. To finish up this algorithm must be reenacted or recreated to get the ideal yield that the AIS creator pursuits for. The AIS creator would then be able to go over and reuse the calculations until the point that the objectives for the new AIS are proficient.

Khan et al. [11] proposed a structure that utilizes multi-robot frameworks for participation among robots to finish complex jobs. The harmonization and correspondence amongst diverse robots in this approach are achieved by exploiting the possibility of the AIS system and a great Idiotypic network model. In this anticipated framework, two main sorts of robots are used, P robots and B robots. P robots are institutionalized and utilized for surveillance and probing. P robots examine the area for complex tasks existing after that light up the capable B robots who can assist the P robots for that task. It sends the region and competence criteria of the perceived jobs to B robots. B robots are assorted in nature and are utilized for tasks examining and completing those tasks. In any case, if B robot can't complete a job independently and cannot manage the task, it sends an assistance communication to scan for help from supplementary B robots. The robot that begins the assistance communication is named commencing robot and the capable robots which can manage the endeavor will calculate their " binding affinity " and a proper robot having the most noteworthy binding affinity value among them will be picked to contribute to the errand. Binding affinity is figured by the speed of the robot, the detachment amongst a robot and a precise errand, the execution pace of the robot and hindrances amongst the robot and the endeavor. The picked robot is called a serving robot and will sort out with the commencing robot to achieve the job compliantly.

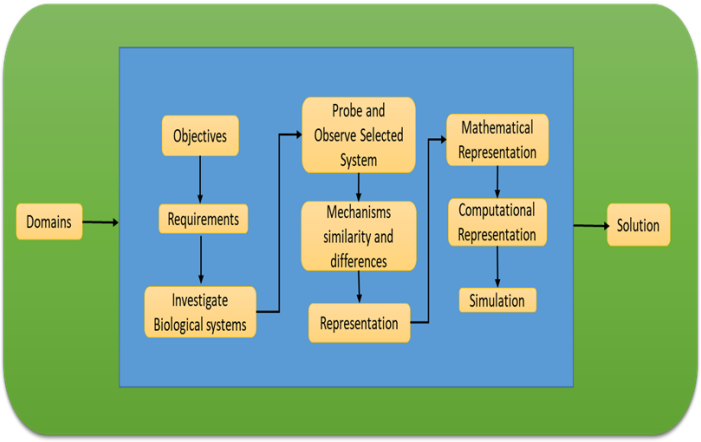

Fig 2.3: A Hybrid Conceptual framework portrayed in [10]

Lau et al. [12] depicted a control system that exemplifies how an AIS agent functions independently in a changing domain by mimicking the segments of the Human Immune System(HIS). The proposed control structure is described by multi-administrator frameworks. Awakened from HIS, each AIS administrator has its own specific practices and they organize through data correspondence and distribution remembering the ultimate objective to achieve shared objectives. Experts of the AIS-focused controller framework take part by hailing each other using the 'interest for' and 'respond to' signals. The coupling likeness is indicated utilizing partition among an expert and a specific task, task event repeats and administrator nature with such an endeavor. The master from the outset considers if it will deal with a standard task or to respond to a demand. In case the target needs the achievement of a supportive task, the expert around then interconnects with the entreated specialist and plays out idle responses. The structure is depicted in Fig 2.4.

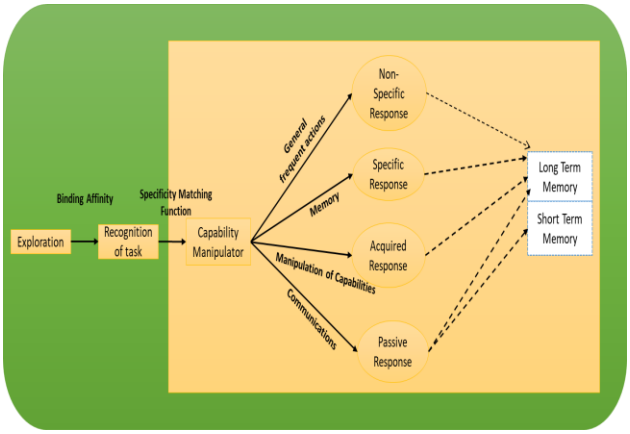

Fig 2.4: Control framework for each AIS agents [12]

An idle answer is undifferentiated from vaccination where the enquiring for administrator brings about trading significant capacities to the band together with a particular ultimate objective to complete the task. Mimicking the building of an antigen, two or three chains are utilized known as heavy and light chains. The heavy ones decide the class of responses and use a separate reply. The light one involves a progression of nuclear capacities and the nuclear capacity gathering is obvious for each reply. On the off chance that the specialist encounters a standard target, the specialist will from the outset check the capacity of the non-specific and acquired chains. In case anything can't be facilitated, the expert will control its nuclear capacities in the vague one to give a definite response. The gained response is indistinguishable from the auxiliary response in HIS where a speedier and more grounded answer will be realized in the occasion of a previously occurred antigen.

Ko et al. [13] proposed a framework focused on the concealment component of immunity. A distributed control framework considering the proposed framework is planned to manage a specific robot organized into placoid controller support**.** The components produce increased gathering presenting intense or tolerant behavior when there is an environmental change. The parts of this system are Similarity Surveyor, Cell Discriminator, Cell Container, Inhibition Modulator and Native Location (Fig 2.5). Similarity Surveyor evaluates information having a place with Native Location against the objective and yield a comparability record. The limit of this fragment resembles the immune segregation work, which isolates among self and non-self-cells. Cell discriminator evaluates commitments from the Similarity Surveyor and Inhibition Modulator to pick the kind of behavior to alter. The chosen behavior is sent to the Cell Container using cell flagging. Cell Container reacts to the signs from the Cell Discriminator and plays out the matching practices which produce results about the Native Location. The inhibition Modulator is an assembly of Suppressor Cells, which will respond to different impelling's and demonstrate specific camouflage effects on Cell Differentiators' decision strategy. Local Environment is the spot where interchanges between different parts take place. The essentialness of this fragment inside the structure is to go about as an edge that associates with the Global Location which contains other Native Locations with different courses of action of Inhibition Modulators.

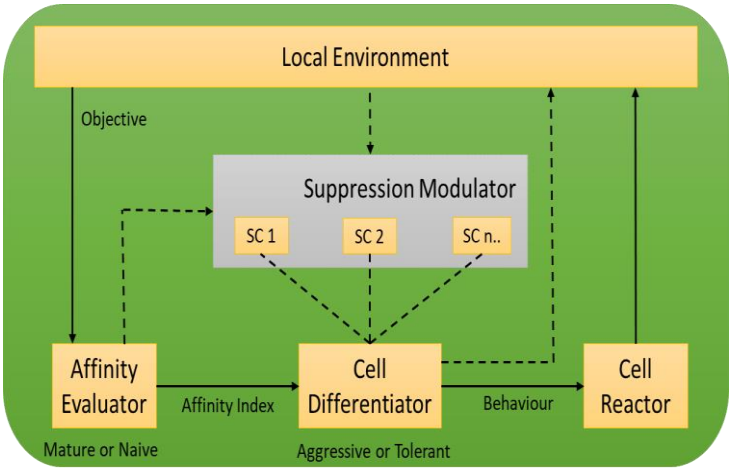

Fig 2.5: A General Suppression Framework [13]

Tan et al. [14] proposed a generic framework utilizing an immune-based methodology that was used for spam sifting. According to the framework, union focused component courses are extricated from messages by figuring match intermingling of acknowledgment. Categorizer is then founded on the union courses of preparing quantity. Finally, moving toward messages can be requested by utilizing the Danger Theory based Ensemble (DTE) technique. The framework is shown in Fig 2.6. In like manner, categorizers are invigorated continually considering the importance of messages and characterization execution. Echoing

the Danger Theory hypothesis, counterfeit signs and risk locales, and categorizers were combined using them were described. Initially, two sorts of signals, direct signals (Signal 1) and danger signals, were exclusively created using two independent categorizers. Dependent upon the categorizers results, negative or positive pointers are created. Consequent to the formation of pointers, the two categorizers were interfaced using the correspondence of the signals. Mimicking the Danger Theory system, the correspondence of the signals was intended to be dissimilar. An incited signal 1 is coordinated to a specific area, where the signal was ascended and to remaining all sections an enacted risk signal is coordinated. The result was obtained in perspective on the relationship among categorizers. All the testing information is arranged by the two categorizers if the two signals agree with each other. If not, another categorizer is utilized to handle the dispute aroused and testing samples are classified. The three categorizers are combined in a successive manner dependent on enactment on preparing data. The traits of the DTE strategy lies in the joint effort among categorizers by using the risk zone and the signals.

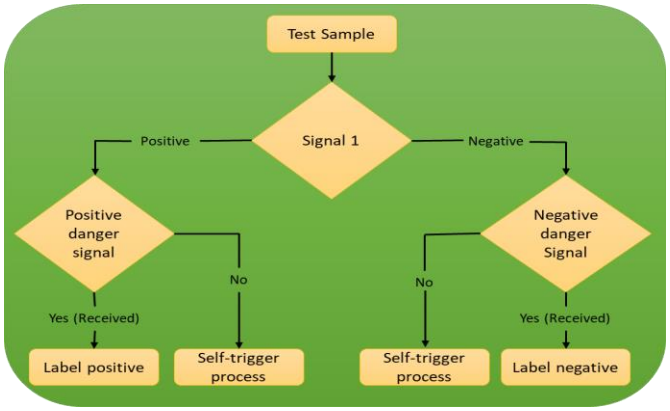

Fig 2.6: Generic framework using immune-based approach [14]

Chen et al. [15] proposed a framework for film recommendation consolidating immune network and collaborative filtering technique. There are two phases in this framework; preparation stage and the other is a testing stage (Fig 2.7). In the preparation stage, each record of client rating data is considered as an antigen and the similarity is described as the affinity. It is figured by using the Pearson correlation coefficient. Right when the antigens assault the immune framework, antibodies are generated. In light of the underlying K antibody agent made, an immune network is generated. At that point, the affinity of the created framework and each training data is computed. In case the affinity is higher than a point of confinement, the antigen will widen the immune framework. If not, the antigen will shape another safe framework. Incidentally, there will be various increasingly safe frameworks created in the preparation stage. After all the safe frameworks are made in the preparation stage, a co-operative oriented filtering methodology to predict a customer's evaluation is applied. To achieve this, the structure finds a course of action of the nearest neighbor to the target customer and the related immune system. By then the affinities of the target customer to its nearest neighbors and its related resistant frameworks are generated and the framework is used to foresee the rating by using the enlisted likenesses as the expectation weighting.

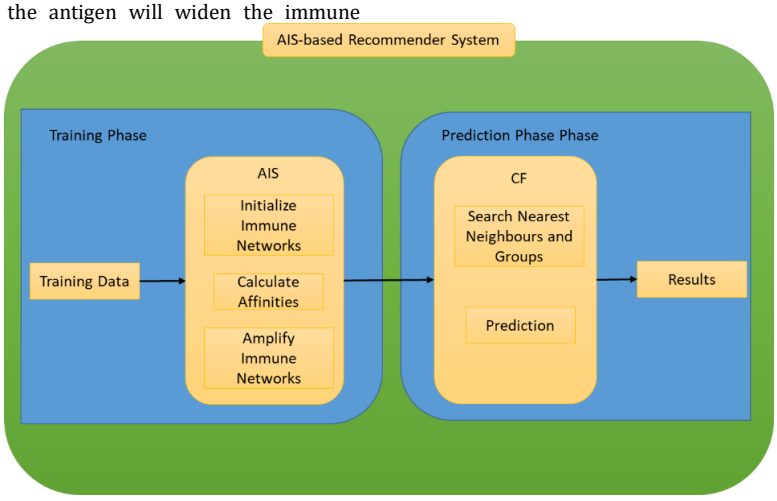

Fig 2.7: Framework for AIS based recommender system in [15]

Yang et al. [16] proposed the fundamental components that guide an AIS based generic framework that could be utilized for IDS. To apply the AIS system for IDS, three phases are anticipated that is portrayed in Fig 2.8. The initial stage is to denote the IDS components based on immunity by making dynamic models of T-cells, B-cells and so on. The relationship between these segments is assessed dependent on affinity measure. For example, the anomaly behavior in IDS is shown as an antigen in AIS. In IDS, affinity infers to the similarity among indicators and data. Diverse depictions can get a distinctive affinity portion. The following stage is the utilization of the immune algorithm for creating indicators. Making precise and capable locators is basic when AIS is associated with an identification issue. An average locator should not recognize self-information and should have a minimal

overlay with different indicators. A few systems ought to be utilized to limit the overlay in this manner making minimum identifiers with most extreme productivity. In long term usage, the number of identifiers will increase yet ought to have a maximum number of indicators instead of an infinite number that will influence the unpredictability of the framework. Those detectors that fail to meet the expectations ought to be killed when new advance locators are made to adjust the number of inhabitants in identifiers.

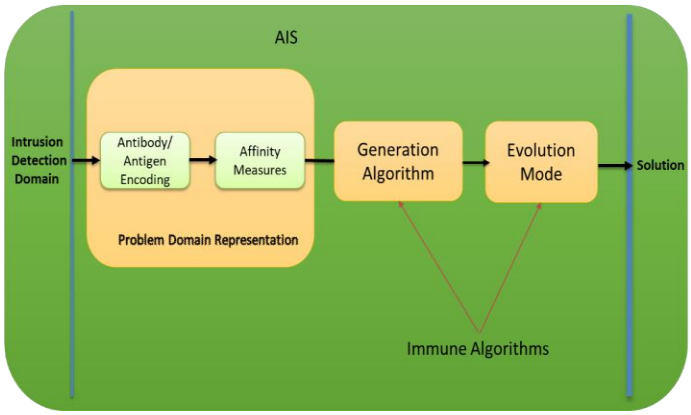

Fig 2.8: AIS framework applied to IDS [16]

RELATED WORKS IN AIS BASED CYBER IMMUNE SYSTEMS

Artificial Immune Systems(AIS) are generally utilized to generate IDS based on Anomaly Detection. Be that as it may, rather than constructing prototypes for the normal, the method created non-self (strange) designs by yielding typical information just. Some coordinating to non-self is assumed to be an oddity. A detailed review of AIS based IDS models will be given in the forthcoming sections.

Seresht and Azmi [17] proposed MAIS-IDS which utilized a multi-agent approach in IDS that was implemented on Virtual machines. Three types of agents were utilized in this approach Detector agent, Antigen agents and Orchestra Agent. Detector agents were versatile operators that distinguish and perceive normal from foreign antigens. Antigen agents were specialist portable operators that drift to additional VM and change into detector agents. Orchestra Agents is the focal specialist for overseeing and regulating correspondence between other agents. Hu et al. [18] depicted a dynamic algorithm known as DIDIAN which utilizes an immune network for correspondence between agents. These agents become mature and are updated dynamically. The clonal selection algorithm is utilized to clone high fitness agents that diminish the False Alarm Rate (FAR). The detector radius of a mature detector that is ineffective to perceive a non-self was effectively resized to improve the effectiveness of that detector to recognize new attacks.

Chung-Ming Ou [19] proposed a Multi-operator based methodology known as ABIDS that used danger theory to implement an IDS using AIS. The methodology was utilized in recognizing intrusions in hosts based on peril signals discharged by them. The concept of danger and safe signals were used in this approach that utilized four agents namely Antigen agent, Dendritic Cell agent, T-Cell agent and Responding agent to evaluate and evade intrusion in hosts. Yang et al. [20] utilized a hierarchical framework known as DAMIDAIS which utilized disseminated agents for detecting intrusions in a real-time environment. Multiple agents viz. Sensor agent, Analyser agent, Manager Agent, Message agent, and alert agent were used to implement real-time intrusion detection. Vidal et al. [21] used a methodology that relies upon building networks of scattered sensors appropriate to the essentials of the environment. This methodology was used for recognizing and alleviating DoS flooding assaults by methods for the human immune system model. Two types of detectors were utilized- DH detector that is linked to innate immunity and a DA detector that accomplishes adaptive immunity tasks.

Zeng et al. [22] depicted a novel IDS approach dependent on the Antibody focus called NIDAAC. Novel operational discoverers are made dependent on the genetic chronicle which stores subtleties of successful groupings. In the event that the recently created detector distinguishes any self-design for example typical traffic design, it is expelled from the system utilizing the negative selection. Saurabh et al. [23] proposed a concept called EPAADPS that utilizes AIS that separates self and non-self to recognize inconsistencies. This work gives a thought of self-tuning of detectors and their control in the Negative Selection Algorithm with the desire to impact an identifier to progress and energize better and perform self and non-self determination.

Sobh and Mostafa [24] depicted a flexible multi-layered structure utilizing AIS that can change with the alterations in condition. It utilizes a blend of danger theory and self and non-self theory. The framework continually sniffs data accessible in the system and examines data from two databases. The primary database contains self-identifiers that are assembled and inspected in watched conditions to shape the crucial game plan of bundles and data that the framework may oversee. The subsequent database contains profiles of system resources (connections, ports and so on.). To revive the knowledge of the system, a vaccination component was utilized. Sobh [25] anticipated a blend of a few AIS standards called HAIP. The mix of those techniques helped in shaping a multi-layered resistance system that could modify with steady incorporating changes. Generally, the framework used self/non-self speculation and Danger Theory, besides an immunization unit additionally animated from characteristic immunology.

Laurentys et al. [26] proposed the AIS Multi-Operational Algorithm(MO) considering the Negative Selection Algorithm. The MO Algorithm was made with the arrangement to propel the better extent of non-self space with increasingly imperative efficiency, which implies the most insignificant number of detectors with the greatest range possible. In the wake of making the detector, its overlaying is assessed by the overlay estimation

system. If it is over a threshold limit, the detector is moved multiple times to decrease the overlaying. On the off chance that this action isn't satisfactory to decrease the overlay, the scope of the detector perseveres through dynamic decays until there is a minimum or no overlay. Zhang and Tan [27] proposed another framework called ICL which used the idea of an immune collaboration of the biological immune system where sample information is expressed as an antigen-specific component vector and an antigen-nonspecific element vector, individually, emulating the antigenic determinant and risk includes in the biological immune system. The antigen-specific and antigen-vague classifiers score the two vectors and charge Signal1 and Signal2, correspondingly. With the contribution of these twin signals, the instance is clustered by the collaboration classifier, that resolves the signal scuffle issue.

Tabatabaefar et al. [28] depicted an AIS based IDS that used two sorts of antibodies—positive and negative that are made for normal and attack tests independently using negative selection and positive assurance speculations to produce detectors for recognizing intrusions. Particle Swarm Optimization (PSO) is used for formulating recently made identifiers to improve their disclosure rate. Other than a scope of antibodies is logically chosen through creation and planning algorithms. Detectors from the two sorts, the positive and negative markers, which can perceive a greater amount of elements in the related dataset, are acknowledged as developed while remaining is believed to be premature. Fuyong and Deyu [29] proposed an algorithm named PSCA for recognizing malware utilizing the idea of positive selection in AIS. This algorithm works by grouping packets dependent on I/O Request bundles by different programs. Utilizing positive determination, arbitrary detectors are made and these detectors just recognize self-information. Detectors that can identify self-information are encompassed in the set and those detectors that don't recognize self-information are disposed of.

Fu et al. [30] introduced the idea of using Natural Killer Cells to AIS. A HIDS has developed dependent on Natural Killer (NK) Cells that was proposed to recognize disguised spyware. The idea utilized three significant concepts. Inhibitory signal, Activating signal and Induction cytokines. Inhibitory signals are that which block NK inception. On the off chance that the programs carry on conventionally, at that point Inhibitory signs are actuated. Initiating signals are signs that advance NK activation. Bejoy and Janakiraman [31] proposed an Intrusion Prevention System based on Natural Killer Cells of AIS. Here Negative Selection was used for creating NK Cells and high fitness NK cells were proliferated used Clonal Selection Algorithm. Based on a threshold level, high fitness NK cells that detect a large number of attacks were migrated to an intrusion prevention system where the original packet dropping happens.

Luther et al. [32] utilized an incredible facilitated exertion between singular AIS masters to address the remarkable false positive issue in anomaly-based discovery. The AIS administrators use a game plan of detectors gained through NSA in the midst of a readiness stage and trade status information and detectors on a periodical and event-driven premise, independently. Dal et al. [33] used a technique of applying an Artificial Immune System Nearby Genetic calculation to Develop an Intrusion Detection System. Far from making Primary Immune Response, as most of the related works, do, it tries to propel this Primary Immune Response to a Secondary Immune Response using the possibility of memory cells dominating in Natural Immune Systems.

Zheng et al. [34] showed a self-adaptable negative selection algorithm known as ANSA. The methodology can create a legitimate profile of the framework just by using a subset of typical components and can alter the collections of self/non-self-space. It can moreover adaptively change self territory, the distinguishing proof range and amounts of detectors to reconsider the fabricated profile of the framework. A more detailed review of the Artificial Immune System based Intrusion Detection System is presented in Bejoy and Janakiraman [35]. The main points of the works in AIS is portrayed in Table 1.

CONCLUSION

A comprehensive survey of AIS based frameworks and its applications on the Intrusion detection system termed Cyber Immune System was presented in this paper. The survey primarily centers around utilizing the artificial immune system frameworks and its utility in the Intrusion detection system termed Cyber Immune System. Section 2 gives a prologue of predominantly utilized frameworks in AIS that evolved from De Castro [7]. Segment 3 gives some thorough works of AIS that are utilized for IDS for the most part focusing on distributed autonomous agents. These concepts are grouped under the key term Cyber Immune System which defines the systems of AIS used for IDS. Although many surveys are there based on AIS based IDS, a comprehensive review of the AIS framework and its utilization is rare from the literature.

This overview surveys some current ideas which may have a few downsides and give some new headings in AIS based IDS. Utilizing Natural Killer Cells is one such of an exploration course. The future work can include additional components of the immune system like Natural Killer Cells and its application in AIS. The future AIS works will incorporate various machine learning techniques that will boost the usage in real-time cyber immune systems. This will be an intriguing issue for the future works in AIS.

Table 1: AIS based Cyber Immune Systems

Title	AIS Algo					Mon src	Dataset	Parameters	Remarks
	NS	CS	IN	DT	Other				
Seresht [17]	*	*	*			N/W	NSL KDD	✓Accuracy ✓False Alarm ✓Detection Rate	✓Used in virtual machines
Ching [19]				*	*	Host	-	-	✓Dendritic cell algorithm ✓Experimental Evaluation
Xinlei [18]	*		*			N/W	KDD Cup99	✓False Alarm ✓Detection Rate	✓Immune Network
Yang [20]		*				N/W	Experimental Evaluation / Real-time	-	✓Dynamic immunological surveillance
Zeng [22]	*				*	N/W	KDD Cup99	✓False Alarm ✓Detection Rate	✓Antibody Concentration
Sobh [24]	*			*		N/W	Real-time	✓False Positive rate	✓Vaccination Module
Sobh [25]	*			*		N/W	KDD Cup99	✓False Alarm Rate	✓Dynamic Response ✓Vaccination Unit
Pengtao [27]					*	Host	CLIPKU08, Henchiri, and VXHeanvens (Malware datasets)	✓Average detecting time	✓Immune cooperation (IC) mechanism
Tabatabaefer [28]	*				*	N/W	KDD Cup99	✓Precision ✓FPR ✓True Negative	✓Positive selection ✓PSO used with AIS
Fuyong [29]		*			*	Host	VX heavens	✓Accuracy ✓TPR ✓FPR	✓Positive Selection ✓K-NN for hole avoidance
Fu- [30]				*		Host	Real-time (Actual Spy and Spybot)	✓Detection Rate	✓Natural Killer cell ✓Limited to host
Luther [32]					*	N/W & Host	Tcpdump data	✓Detection Rate ✓False Positive Rate	✓Positive Selection
Laurents [26]	*					DC Motor	DC motor Error	✓Detection Rate ✓Detection time	✓Detector Moving
Saurabh [23]	*	*	*		*	N/W	KDD Cup99	✓Detection Rate ✓False Alarm Rate	✓Extending NSA
Bejoy [31]	*	*	*		*	N/W	NSL KDD	✓Detection Rate ✓ False Alarm Rate ✓ Accuracy	✓NK cell-based IPS
Vidal [21]	*	*			*	N/W	KDD Cup99 CAIDA'07	✓False Alarm Rate ✓TPR	✓Limited to DoS flooding attacks
Dal [33]	*				*	N/W	DARPA	✓Detection Rate	✓AIS and GA
Zheng [34]	*					-	Various Biomedical dataset	✓Detection Rate ✓False Alarm Rate	✓Enhanced NSA ✓Detector radius adjusted

NS- Negative Selection
CS- Clonal Selection
IN- Immune Network
DT- Danger Theory

REFERENCES

1. S. Forrest, A. S Pereslon, L. Allen, R, Cherukuri, "Self-nonself discrimination in a computer" in Proceedings of the 1992 IEEE Symposium on Security and Privacy, pages 202-212.IEEE Computer Society Press, 1994.
2. F. M. Burnet. The clonal selection theory of acquired immunity, Vanderbilt University Press, 1959.
3. L. N. de Castro, F. J. Von Zuben. "Learning and optimization using the clonal selection principle", IEEE Transactions on Evolutionary Computation, 6:239-251, 2002.
4. N. K. Jerne, "Towards a network theory of the immune system", Ann. Immunol. (Inst. Pasteur), 125C, 373-389, 1974.
5. P. Matzinger, "The danger model: A renewed sense of self", Science,296(5566):301-305,2002.

6. J Greensmith, U Aickelin, S Cayzer, "Introducing dendritic cells as a novel Immune-Inspired algorithm for anomaly detection". In: Lecture Notes in Computer Science, 3627. Berlin, Heidelberg: Springer; 2005
7. L. N. de Castro, J. Timmis. Artificial Immune Systems: A New Computational Intelligence Approach. Springer, 2002
8. S. Stepney, R. E. Smith, J. Timmis, and A. M. Tyrrell, "Towards a conceptual framework for artificial immune systems," Int. Conf. Artif. Immune Syst., pp. 53–64, 2004.
9. J. Twycross and U. Aickelin, "Towards a Conceptual Framework for Innate Immunity", Int. Conf. Artif. Immune Syst., pp. 112–125, 2005.
10. M. E. M. Ahmed, "Hybrid conceptual framework for artificial immune system," Int. Conf. Comput. Electr. Electron. Eng. ICCEEE 2013, pp. 249–252, 2013
11. M. T. Khan, Izhar, F. Nasir, M. U. Qadir, and J. Iqbal, "Artificial immune system based framework for multi- robot cooperation," Proc. 9th Int. Conf. Comput. Sci. Educ. ICCCSE 2014, no. Iccse, pp. 50–55, 2014
12. H. Y. K. Lau, V. W. K. Wong, M. S. Engineering, P. Road, and H. Kong, "Immunologic Responses Manipulation of AIS Agents," Int. Conf. Artif. Immune Syst., pp. 65–79, 2004.
13. T. L. L. Albert Ko, H.Y.K Lau, "An Immuno Control Framework for Decentralized Mechatronic Control", Int. Conf. Artif. Immune Syst., pp. 255–280, 2004.
14. Y. Tan, G. Mi, Y. Zhu, and C. Deng, "Artificial Immune System Based Methods for Spam Filtering," IEEE pp. 2484–2488, 2013.
15. M. H. Chen, C. H. Teng, and P. C. Chang, "Applying artificial immune systems to collaborative filtering for a movie recommendation," Adv.Eng. Informatics, vol. 29, no.4, pp. 830–839, 2015.
16. H. Yang, T. Li, X. Hu, F. Wang, and Y. Zou, "A survey of artificial immune system based intrusion detection," Sci. World J., vol. 2014, 2014.
17. Neda Afzali Seresht, Reza Azmi, "MAIS-IDS: A distributed intrusion detection system using multi-agent AIS approach", Engineering Applications of Artificial Intelligence Elsevier,2014.
18. Xinlei HU, Xiaojie LIU, Tao LI, Tao YANG, Wen CHEN, Zhengjun LIU, "Dynamically Real-time Intrusion Detection Algorithm with Immune Network", Journal of Computational Information Systems, 2015.
19. Chung-Ming Ou, "Host-based intrusion detection systems adapted from agent-based artificial immune systems", Neurocomputing, Elsevier, 2012.
20. Jin Yang, XiaoJie Liu, Tao Li, Gang Liang, SunJun Liu, "Distributed agents model for intrusion detection based on AIS", Knowledge-Based Systems 22, 2008.
21. J.M. Vidal, A.L.S. Orozco, L.J.G Villalba, "Adaptive artificial immune networks for mitigating DoS flooding attacks", Swarm Evol. Comput., vol. 38, no. July 2017, pp. 94–108, 2018.
22. J. Zeng, X. Liu, T. Li, G. Li, H. Li, and J. Zeng, "A novel intrusion detection approach learned from the change of antibody concentration in biological immune response," Appl. Intell., vol. 35, no. 1, pp. 41–62, 2011.
23. P. Saurabh and B. Verma, "An efficient proactive artificial immune system based anomaly detection and prevention system," Expert Syst. Appl., vol. 60, pp. 311–320, 2016.
24. T. S. Sobh and W. M. Mostafa, "A cooperative immunological approach for detecting network anomaly," Appl. Soft Comput. J., vol. 11, no. 1, pp. 1275–1283, 2011.
25. T. S. Sobh, "Anomaly detection based on hybrid artificial immune principles", Information Management & Computer Security, Vol. 21 Issue: 4, pp.288-314.
26. C.A. Laurentys, G. Ronacher, R.M. Palhares, W.M Caminhas, "Design of an Artificial Immune System for fault detection: A Negative Selection Approach", Expert Systems with Applications, 2010.
27. Pengtao Zhang, Ying Tan, "Immune cooperation mechanism based learning framework", Neurocomputing 148, 2015.
28. M. Tabatabaefar, M. Miriestahbanati, J. C. Gregoire, and Ieee, "Network Intrusion Detection through Artificial Immune System", 11th Annu. Ieee Int. Syst. Conf., pp. 334–339, 2017.
29. Z. Fuyong and Q. Deyu, "Run-time malware detection based on positive selection," J. Comput. Virol., vol. 7, no. 4, pp. 267–277, 2011.
30. Jun Fu, Huan Yang, Yiwen Liang, and Chengyu Tan, "Bait a Trap: Introducing Natural Killer Cells to Artificial Immune System for Spyware Detection", Springer-ICARIS 2012.
31. B.J. Bejoy, S. Janakiraman. "An Intrusion Detection and Prevention System Using AIS—An NK Cell-Based Approach". In International Conference on ISMAC in Computational Vision and Bio-Engineering 2018 May 16 (pp. 883-893). Springer, Cham.
32. K. Luther, R. Bye, T. Alpcan, A. Müller, and Ş. Albayrak, "A cooperative AIS framework for intrusion detection," IEEE Int. Conf. Commun., pp. 1409–1416, 2007.
33. D. Dal, S. Abraham, A. Abraham, S. Sanyal, and M. Sanglikar, "Evolution induced secondary immunity: An artificial immune system based intrusion detection system," Proc. - 7th Comput. Inf. Syst. Ind. Manag. Appl. CISIM 2008, pp. 65–70, 2008.
34. J. Zeng, X. Liu, T. Li, C. Liu, L. Peng, and F. Sun, "A self-adaptive negative selection algorithm used for anomaly detection," Prog. Nat. Sci., vol. 19, no. 2, pp. 261–266, 2009.
35. B.J. Bejoy, S. Janakiraman. "Artificial immune system based intrusion detection systems-a comprehensive review". Int J Comput Eng Technol. 2017;8(1):85-95.
36. Prashant Tiwari, Puravi Nayak, Shakti Ketan Prusty, Pratap Kumar Sahu. "Phytochemistry and Pharmacology of Tinospora cordifolia: A Review." Systematic Reviews in Pharmacy 9.1 (2018), 70-78. Print. doi:10.5530/srp.2018.1.14