International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol. 8 Issue 1 January 2022

Survey Paper of Immune System based Intrusion Detection System using Neural Network

Ms. Sapna Thakur[1], Prof. Chetan Gupta[2], Dr. Ritu Shrivastava[3]
thakursapna0087@gmail.com[1], chetangupta.gupta1@gmail.com[2], ritushrivastava08@gmail.com[3]
M.Tech Research Scholar, Dept. of CSE[1], Asst. Prof., Dept. of CSE[2], HOD Dept. of CSE[3]
SIRTS, Bhopal India[1], SGI, Bhopal India[2], SGI, Bhopal India[3]

Abstract- Various approaches from different fields have been proposed to improve the security of computer system. One such approach is Intrusion detection system monitors computer system in real-time for activities indicating attempted or actual access by unauthorized users. To build an effective intrusion detection system many techniques are available which gathers and analyze information from different areas within a computer system or network and identify various security threats, including both intrusions anomaly i.e. attacks from outside the organization and misuse i.e. attacks from within the organization. Artificial Immune System (AIS) which is inspired by the robust and flexible nature of Human Immune System (HIS) can be incorporated in current Intrusion Detection Systems (IDS) thereby improving their efficiency and performance. This paper gives a review of various artificial immune system approaches that can be used for the development of an Intrusion Detection System.

Keywords- Immune System, Intrusion Detection System, Neural Network, artificial immune system

I. INTRODUCTION

Anomaly-based intrusion detection systems (IDS) have been broadly researched as defensive techniques to address the detection of unknown or zero-day attacks. Unlike misuse-based or signature based types of IDS, which take advantage of the predetermined signature of known attacks, anomaly based IDS deals with the detection of new types of attack that are unknown to the system. This process is done by detecting variation in the systems' behavior from a previously defined normal system profile. However, it is subject to false alarms as a result of the difficulty in defining the normal state during training. An increasing detection rate with fewer false alarms became an important challenge in the design of anomaly-based IDS.

The artificial immune system (AIS) comprises promising techniques in the form of biologically inspired computing that is applied to solving various problems in the information security field. The AIS is inspired by the human immune system (HIS), which has the ability to distinguish internal cells and molecules of the body from foreign pathogens, so called self and non-self respectively, and protects the body against diseases [1].

In the human body the HIS mainly does this without any prior knowledge of attacking pathogens and their structure. As self and non-self-discrimination is a significant attribute in the AIS, it is proposed that it is utilized in designing efficient anomaly-based IDS [2]–[4]. The AIS suggests a multi-layered protection structure for protecting computer networks against attack, like HIS protection against foreign pathogens in the human body [5]. This protection is accomplished through Innate or Adaptive mechanisms. Innate immunity is immediate; it is the first line of defense for the HIS and provides non-specific protection. Therefore, it has no prior knowledge of specific outsiders. The adaptive immune response, on the other hand, is antigen-specific and is trained using a pre-defined profile of specific attacks [6]. Adaptive immunity also includes a "memory" that makes future responses against a specific antigen more efficient [7].

Like other abnormality based discovery procedures, the AIS additionally exploit checking varieties of the framework's conduct as indicated by a pre-characterized typical movement profile as a versatile invulnerable system. This is done through a learning deliberately ease in which an informational index containing these profiles is used for this reason. Thus, the productivity of peculiarity location in the AIS is profoundly reliant on the learning informational index. Significant examination has been directed such a long ways in the

improvement and use of AIS-based IDS, most of which have used a pre-characterized and disconnected informational collection as learning information for preparing the IDS. This will decrease the proficiency of the IDS by restricting its knowledgebase to that specific learning informational collection. Additionally, it is amazingly hard to make an informational collection of self-tests with all varieties. To adapt to this issue, in this paper we have proposed an inborn insusceptible component by involving solo learning strategies as the principal line of safeguard in AIS based IDS. The inborn resistant framework in our proposed design gives on the web and dynamic order of organization streams to self and non-self, which is then utilized by the versatile insusceptible framework to create assault explicit locators.

II. LITERATURE REVIEW

Inadyuti Dutt et al. [1], this paper investigates the immunological model and carries out it in the space of interruption recognition on PC organizations. The principle objective of the paper is to screen, log the organization traffic and apply location calculations for identifying interruptions inside the organization. The proposed model copies the normal Immune System (IS) by considering both of its layers, natural safe framework and versatile resistant framework individually. The current work proposes Statistical Modeling based Anomaly Detection (SMAD) as the primary layer of Intrusion Detection System (IDS). It functions as the Innate Immune System (IIS) point of interaction and catches the underlying traffic of an organization to discover the direct weakness. The subsequent layer, Adaptive Immune-based Anomaly Detection (AIAD) has been considered for deciding the elements of the dubious organization bundles for discovery of peculiarity. The SMAD model yields as high as 96.04% genuine positive rate and around 97% genuine positive rate utilizing continuous traffic and standard informational indexes. Exceptionally dubious traffic recognized in the SMAD model is additionally tried for weakness in the AIAD model. Results show huge genuine positive rate, closer to practically almost 100% of precisely recognizing the document based and client based irregularities for both the ongoing traffic and standard informational indexes.

W. Wang et al. [2], the advancement of an abnormality based interruption recognition framework (IDS) is an essential examination course in the field of interruption identification. An IDS learns ordinary and peculiar conduct by dissecting network traffic and can distinguish obscure and new assaults. Nonetheless, the presentation of an IDS is exceptionally reliant upon highlight plan, and planning a list of capabilities that can precisely describe network traffic is as yet a continuous examination issue. Irregularity based IDSs likewise have the issue of a high bogus alert rate (FAR), which genuinely limits their useful applications. In this paper, we propose a clever IDS called the progressive spatial-worldly highlights based interruption location framework (HAST-IDS), which initially learns the low-level spatial elements of organization traffic utilizing profound convolutional neural organizations (CNNs) and afterward learns undeniable level transient elements utilizing long momentary memory organizations. The whole course of component learning is finished by the profound neural organizations consequently; no element designing methods are required. The naturally scholarly traffic includes viably lessen the FAR. The standard DARPA1998 and ISCX2012 informational collections are utilized to assess the presentation of the proposed framework. The test results show that the HAST-IDS beats other distributed methodologies as far as precision, discovery rate, and FAR, which effectively exhibits its adequacy in both element learning and FAR decrease.

M. H. Ali et al. [3], administered interruption identification framework is a framework that has the ability of gaining from models about the past assaults to identify new assaults. Utilizing fake neural organization (ANN)- based interruption location is promising for decreasing the quantity of bogus negative or bogus up-sides, on the grounds that ANN has the capacity of gaining from real models. In this paper, a created learning model for quick learning organization (FLN) in light of molecule swarm streamlining (PSO) has been proposed and named as PSO-FLN. The model has been applied to the issue of interruption discovery and approved in light of the popular dataset KDD99. Our created model has been analyzed against a wide scope of meta-heuristic calculations for preparing outrageous learning machine and FLN classifier. PSO-FLN has beated other learning approaches in the testing exactness of the learning.

L. Ma et al. [4], a superior Dynamic Clonal Selection Algorithm (IDCSA) is proposed in this paper which is utilized in appropriated network interruption recognition framework (NIDS). It expects to further develop the identifier's capacity to perceive both the known and obscure interruptions by utilizing the techniques of setting up rules of master information, programmed advancement of genetic stocks, and streamlining of finder age process. The exploratory outcomes show that the proposed IDCSA can decrease FP (bogus positive) and further develop TP (genuine positive), viably

further develop the identification execution and flexibility of the framework.

C. Yin et al. [5], counterfeit invulnerable framework builds a dynamic and versatile data guard framework through a capacity like the organic resistant framework. To oppose the outside attack of pointless and unsafe data and guarantee the adequacy and the innocuousness of gotten data. Because of the low precision and the high bogus positive pace of the current clonal determination calculations applied to interruption recognition, in this paper, we propose a superior clonal choice calculation. The better strategy identifies the interruption conduct by choosing the best individual generally and cloning them. Trial results show that the better calculation accomplishes excellent execution when applied to interruption recognition. What's more it is shown that the calculation is superior to BP neural organization with its 99.5 % precision and 0.1 % bogus positive rate.

C. Yin et al. [6], interruption location assumes a significant part in guaranteeing data security, and the key innovation is to precisely recognize different assaults in the organization. In this paper, we investigate how to show an interruption recognition framework in view of profound learning, and we propose a profound learning approach for interruption discovery utilizing repetitive neural organizations (RNN-IDS). Additionally, we concentrate on the exhibition of the model in parallel arrangement and multiclass grouping, and the quantity of neurons and different learning rate impacts on the presentation of the proposed model. We contrast it and those of J48, counterfeit neural organization, arbitrary backwoods, support vector machine, and other AI techniques proposed by past scientists on the benchmark informational index. The test results show that RNN-IDS is truly appropriate for demonstrating a characterization model with high exactness and that its exhibition is better than that of customary AI grouping techniques in both twofold and multiclass order. The RNN-IDS model works on the precision of the interruption location and gives another examination strategy to interruption discovery.

S. J. Xu et al. [7], another organization interruption location model in light of resistant multi-specialist hypothesis is set up and the idea of multi-specialists is progressed to understand the legitimate design and running component of safe multi-specialist just as staggered and disseminated identification instrument against network interruption, utilizing the versatility, variety and memory properties of fake insusceptible calculation and brushing the power and dispersed person of multi-specialists framework structure. The examination results reason that this framework is functioning admirably in network security discovery.

W. M. Alshara et al. [8], in the space of PC security, Intrusion Detection (ID) is an instrument that endeavors to find strange admittance to PCs by investigating different collaborations. There is a ton of writing about ID, however this concentrate on just studies the methodologies in light of Artificial Immune System (AIS). The utilization of AIS in ID is an engaging idea in current methods. This paper sums up AIS based ID strategies from another view point; also, a structure is proposed for the plan of AIS based ID Systems (IDSs). This structure is broke down and talked about in view of three center perspectives: immunizer/antigen encoding, age calculation, and advancement mode. Then, at that point, we examine the generally utilized calculations, their execution qualities, and the advancement of IDSs into this structure. At last, a portion of things to come difficulties in this space are likewise featured.

III. PROBLEM FORMULATION

Following are the problems which are to be considering as identify from the base paper [1]:

1. The number of accuracy and false-positives are quite high in some specific cases, which can be further reduced.
2. To increase the complexity in the case of high dimensional data.
3. Immune memory refers to a secondary response, meaning a similar and more rapid response is elicited should the same attack occur again, irrespective of the time between the attacks.
4. Features to identify the texture and amplify the difference between true/fake frame blocks, which can be further increased.
5. Algorithms for Immune System based Intrusion Detection System has much to be researched.

IV. INTRUSION DETECTION SYSTEM

IDS detect malicious activity in computer systems and perform forensics after the attack is complete. Check network resources to detect intrusions and attacks that have not been blocked by preventive techniques (firewall, router packet filtering, and proxy server). Intrusion is an attempt to compromise the confidentiality, integrity or availability of a system. Intrusion detection systems can be regarded as a rough analogy with true intruder detectors. Misuse based IDS (as shown in Figure 1) is designed to detect violations of

predefined security policies. But things get complicated both with the introduction of possible harmful behaviors that cannot be predetermined [9-11]. An example would be a developer in a company that transfers large amounts of data in a short period of time. This may be a potential data leakage problem, but it may not be detected by the admittance policy because it is allowed to transfer files [12]. For this specific reason, the detection of statistical anomalies has been introduced, in which a profile of a user or a system is created and deviations from the profile are reported. While both kinds of systems are independently useful, a hybrid of the two can reduce but not eliminate the individual disadvantages. An important factor that defines the kind of implementation inherited from IDS is the source of audit data. The two primary sources are host-based protocols used by host-based IDSs and data packets that exist on a network that are exploited by network IDSs. Host protocols can be kernel logs, application logs, or device-related logs [11].

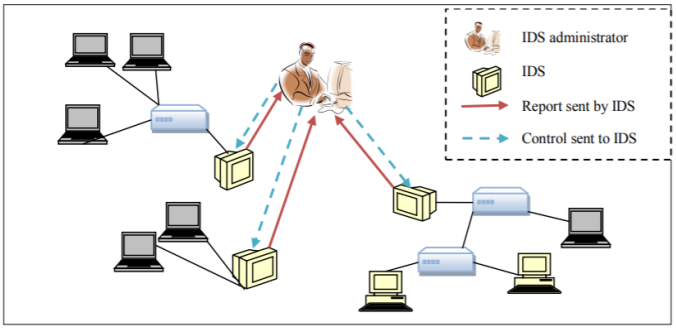

Fig. 1: Intrusion Detection System [11]

There are several problems with IDS based on host and network IDS. They include:

- Heterogeneous operating systems make the enumeration of system-specific detection parameters extremely long for any system.
- Increasing the number of critical nodes in the network increases performance.
- Performance degradation in the host system due to additional security activities, such as B. Registration.
- Difficulty in detecting attacks at the network level.
- Host with insufficient computing power to offer a complete host-based IDS.

In contrast, network-based intrusion detection systems can have a central system with a network connection to passively monitor network traffic. They have no impact on system performance and can easily detect network-level attacks when installed at the edge of the network. Network-based ID implementation is too simple [13]. Host based IDs in a critical performance-sensitive host network must be carefully selected so as not to unduly restrict the performance of each system [26][27][28].

V. NEURAL NETWORK

The human brain consists of approximately 1011 highly connected elements which are called neurons.

Table 1: Artificial Neural Networks and Biological Neural Networks

Biological Neural Networks	Artificial Neural Network
It works on serial processing. Processing of instructions and problem rules takes place at one time	It works on parallel processing that means various processes work at the same time in parallel
The functionality of these networks based on rule based approach like if & else rules	Their functionality depends on learning algorithms
Dendrites	Weighted inputs
Cell body	Artificial neurons
Axon	Outputs

These neurons have mainly 3 components: Dendrites, Cell body, and Axon. Dendrites are tree-like structures that carry electrical signals to the cell body. The cell body then sums and thresholds these signals. Axon is a single long fiber which transfers the signal from one cell body to another. The point of contact of an axon of a cell and a dendrite of another cell is called synapse. Artificial Neural Network (ANN) is somehow based on this neural network structure of the human brain [11, 14]. They are not entirely the same but have some similarities with each other. ANN is formed by artificial neurons which are in turn having the same functionality as biological neurons.

Table 1 shows the difference and similarities between Artificial Neural Networks and Biological Neural Networks. Fig. 2 shows the structure of biological neurons and basic terminologies attached with it and Fig. 3 shows the artificial neuron and its basic functions and parts.

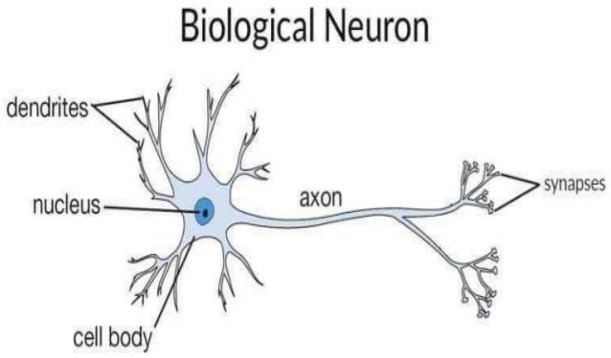

Fig. 2: Biological Neuron [12]

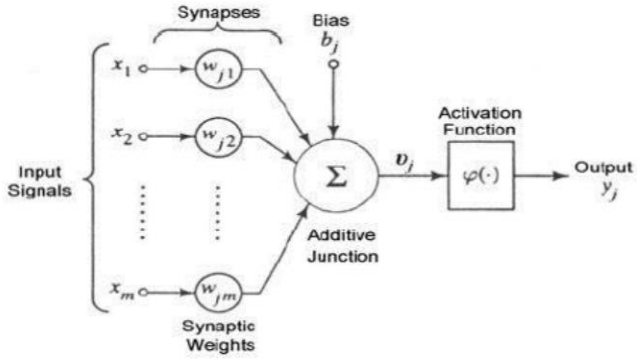

Fig. 3: Artificial Neuron [13]

In the artificial neural networks, the information comes into the body through inputs which have some weights associated with them. ANN is also called a weighted directed graph in which artificial act as nodes. Each input is multiplied with the weight associated with it. Weights are the processed form of data that work as a strength to solve the particular problem in the neural network [15]. The body of artificial neuron sums the weighted inputs and if it is zero, then bias values are added to make it non-zero and then, processes the sum with a transfer function. An activation function linear or non-linear is set to transfer function to limit the responses arrive at the desired output point. In the end, the processed information is then transferred through output [16, 17]. The neural network is robust and has fault tolerance property.

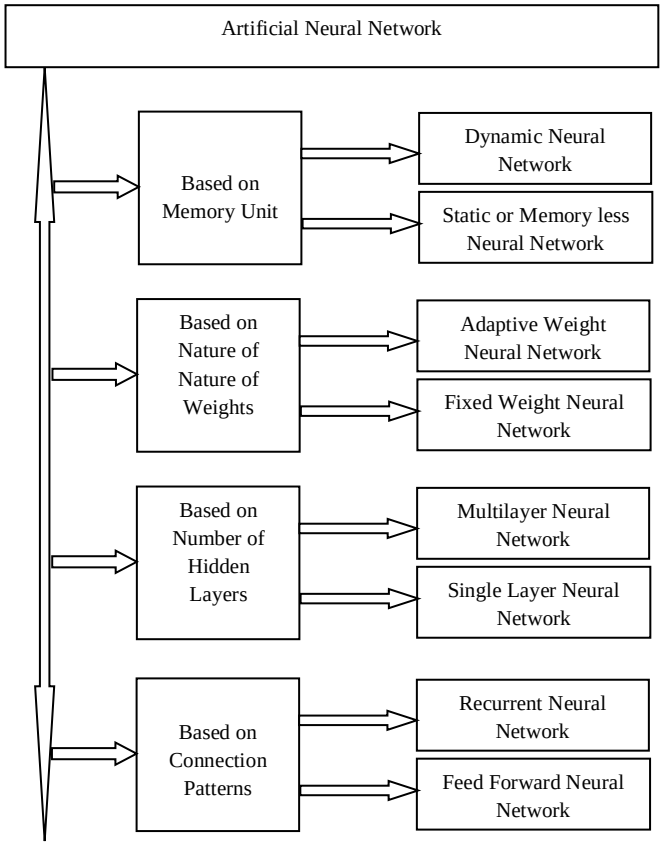

Fig. 4: Types of Artificial Neural Network

Types of Artificial Neural Networks: - ANNs can be of many types depending upon the various parameters like connection patterns, hidden layers, weights, and memory units. Figure 4 shows the various types of ANNs depending on which we have different architectures of ANNs.

Their brief introductions are as follows [16, 18]:

Single Layer Perceptron Neural Network: The feed-forward connection of one input layer to one output layer is known as the single-layer perceptron neural network. In this type of network, there is no feed-back connection of neurons.

Multi-layer Perceptron Neural Network: The feed-forward connection of one input layer, one output layer, and one or more hidden layers is known as multi-layer perceptron neural network [19]. In this type of network, there is no feed-back connection of neurons.[20][21][22]

Layer Recurrent Neural Network: A network that has at least one backward connection is known as the recurrent neural network[23][24][25]

VI. CONCLUSION

The various IDS tools developed till now were constraint to the detection of known intrusions and most of them suffer from the accuracy of the attack. The inability of the IDS inspired us to analyses these tools in such a manner so that we can overcome the accuracy of the attack. According to specification of various techniques we observed that by using concepts of artificial immune system we can even detect the unknown attacks. Thus it is believed that if these remarkable features of human immune system are applied to Intrusion detection Systems (IDS), then it would produce highly efficient and versatile Intrusion detection systems which can be referred as expert systems.

REFERENCES-

[1] Inadyuti Dutt, Samarjeet Borah, and Indra Kanta Maitra, "Immune System Based Intrusion Detection System (IS-IDS): A Proposed Model", IEEE Access 2020.

[2] W. Wang, Y. Sheng, J. Wang, X. Zeng, X. Ye, Y. Huang, and M. Zhu, "HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection", IEEE Access, vol. 6, pp. 17921806, 2018.

[3] M. H. Ali, B. A. D. Al Mohammed, A. Ismail, and M. F. Zolkipli, "A new intrusion detection system based on fast learning network and particle swarm optimization," IEEE Access, vol. 6, pp. 2025520261, 2018.

[4] L. Ma, J. Qu, Y. Chen, and S.Wei, ``An improved dynamic clonal selection algorithm using network intrusion detection," in Proc. 14th Int. Conf. Comput. Intell. Secur. (CIS), Nov. 2018, pp. 250253.

[5] C. Yin, L. Ma, and L. Feng, ``Towards accurate intrusion detection based on improved clonal selection algorithm," Multimedia Tools Appl., vol. 76, no. 19, pp. 19397_19410, Oct. 2017.

[6] C. Yin, Y. Zhu, J. Fei, and X. He, ``A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, vol. 5, pp. 21954_21961, 2017.

[7] S. J. Xu and Y. Li, ``Multi-agent intrusion detection system based on immune principle," Int. J. Innov. Res. Comput. Commun. Eng., vol. 3, no. 4, pp. 26812689, 2015.

[8] W. M. Alshara_ and M. N. Omar, ``A detector generating algorithm for intrusion detection inspired by artificial immune system," ARPN J. Eng. Appl. Sci., vol. 10, no. 2, pp. 608_612, 2015.

[9] N. Afzali Seresht and R. Azmi, ``MAIS-IDS: A distributed intrusion detection system using multi-agent AIS approach," Eng. Appl. Artif. Intell., vol. 35, pp. 286_298, Oct. 2014.

[10] F. Hosseinpour, S. Ramadass, A. Meulenberg, P. Vahdani Amoli, and Z. Moghaddasi, ``Distributed agent based model for intrusion detection system based on artificial immune system," Int. J. Digit. Content Technol. Appl., vol. 7, no. 9, p. 206, 2013.

[11] T. Stibor, J. Timmis, and C. Eckert, ``On the appropriateness of negative selection dened over hamming shape-space as a network intrusion detection system," in Proc. IEEE Congr. Evol. Comput., vol. 2, Dec. 2005, pp. 100995.

[12] T. Stibor, ``Phase transition and the computational complexity of generating r-contiguous detectors," in Artificial Immune Systems (Lecture Notes in Computer Science), L. N. de Castro, F. J. Von Zuben, H. Knidel, Eds. Berlin, Germany: Springer, 2007, pp. 142155.

[13] F. Hosseinpour, S. Ramadass, A. Meulenberg, P. Vahdani Amoli, and Z. Moghaddasi, ``Distributed agent based model for intrusion detection system based on artificial immune system," Int. J. Digit. Content Technol. Appl., vol. 7, no. 9, p. 206, 2013.

[14] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, ``Self-nonself discrimination in a computer," in Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy, Dec. 2002, pp. 202_212.

[15] Y. Otsuki, M. Ichino, S. Kimura, M. Hatada, and H. Yoshiura, ``Evaluating payload features for malware infection detection," J. Inf. Process., vol. 22, no. 2, pp. 376_387, 2014.

[16] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R. P. Liu, ``RePIDS: A multitier real-time payload-based intrusion detection system," Comput. Netw., vol. 57, no. 3, pp. 811_824, Feb. 2013.

[17] K. Kato and V. Klyuev, ``Large-scale network packet analysis for intelligent DDoS attack detection development," in Proc. 9th Int. Conf. for Internet Technol. Secured Trans. (ICITST), Dec. 2014, pp. 360_365.

[18] F. Iglesias and T. Zseby, ``Analysis of network traffic features for anomaly detection," in Machine Learning, vol. 101, no. 1. Cham, Switzerland: Springer, 2015, pp. 59_84.

[19] I. M. Iqbal and R. A. Calix, ``Analysis of a payload-based network intrusion detection system using pattern recognition processors," in Proc. Int. Conf. Collaboration Technol. Syst. (CTS), Oct. 2016, pp. 398_403.

[20] Chetan Gupta, Dr. Amit Sinhal, Prof. Rachna Kamble "Intrusion Detection based on K-Means Clustering and Ant Colony Optimization: A Survey", has been published in International Journal of Computer Applications (IJCA

ONLINE) (0975 – 8887), Volume 79 – No6, Foundation of Computer Science, New York, USA, October 2013.

[21] Chetan Gupta, Dr. Amit Sinhal, Prof. Rachna Kamble "An Enhanced Associative Ant Colony Optimization Technique based Intrusion Detection System", International Conference on Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, ICAEES-2014, Published in Springer (Serial no 12563 (ISSN -18761100)) at Kanyakumari 23-24 April 2014.

[22] Sushmita Sagar, Prof. Amit Shrivastava, Prof. Chetan Gupta "Comparative Analysis of Different Data Mining Technique Based Intrusion Detection System: A Review" is published in International Journal of Creative Research Thought (IJCRT) , Volume 6, Issue 2, May 2018, ISSN: 2320–2882 Impact Factor 5.97.

[23] Ms. Sushmita sagar, Prof. Chetan Gupta "Feature Reduction and Selection Based Optimization for Hybrid Intrusion Detection System Using PGO followed by SVM" is Accepted for publication in International Conference On Advanced Computation And Telecommunication (ICACAT-2018), ISBN: 978-1-5386-5472-9, IEEE 2018.

[24] Ms. Surbhi Solanki, Prof. Chetan Gupta, "An Efficient HIDS System Using Machine Learning Algorithm and Evidence Theory" in 2nd International Conference on Artificial Intelligence: Advances and Applications, MARCH 27-28, 2021 SPRINGER (ICAIAA 2021).

[25] Ms. Tanushri Jain, Prof. Chetan Gupta, "Multi-Agent Intrusion Detection System using Sparse PSO K-means Clustering and Deep Learning" in 2nd International Conference on Artificial Intelligence: Advances and Applications, MARCH 27-28, 2021 SPRINGER (ICAIAA 2021).

[26] Ms. Tanushri Jain, Prof. Chetan Gupta "A Review on Intrusion Detection System using Deep Learning" in International Journal of Creative Research Thoughts (IJCRT), Volume 8, Issue 7 July 2020.

[27] Ms. Shivangi Soni, Prof. Chetan Gupta, Prof. Shivendra Dubey "A Detailed Survey on Intrusion Detection System based on NSL-KDD Dataset using Various Approach" in "International Journal of Creative Research Thoughts (IJCRT)" Volume 9, Issue 5 Page No : 408-412, on 18 May 2021.

[28] Ms. Swikrati Dubey, Prof. Chetan Gupta, Prof. Shivendra Dubey "A Survey on Intrusion Detection Systems for Detecting Networking Attacks using NSL-KDD Dataset", International Journal of Engineering Technology and Applied Science (IJETAS)Vol. 7 Issue 6 June 2021.