Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

CIA Triad Validation in Intrusion Detection Using ACO Algorithm with RNN based Cognitive Mechanisms

Jayaganesh Jagannathan [#1], M.Y. Mohamed Parvees [*2]

[#1 & *2] Department of Computer and Information Science, Faculty of Science
Annamalai University, Annamalai Nagar, India
[#1]everjays@gmail.com, [*2]yparvees@gmail.com

Article Info
Page Number: 4198 - 4207
Publication Issue:
Vol 71 No. 4 (2022)

Abstract

Confidentiality is the process of verifying the one's identity to allow them for the usage of registered application which is available in the remote place and serve the same to different end users. Integrity is the process of examining the supplied data is altered by someone or not. Availability ensuring the data supply to legitimate user. Intrusion detection is a key parameter to stop malicious action immediately at the same time it should be validated against CIA. Cognitive is the nascent technology which is strongly applying the concepts of it against discovery of malicious event. Bio Inspired algorithms are mainly applied to obtain optimized result in the process. Proposed solution for validating CIA along with intrusion detection named as ACO- RNN-C model to verify the CIA measurement. We have compared CIA validations against our previous findings and proved that ACO-RNN-C has given reasonable improvement in performance.

Article History
Article Received*: 25 March 2022*
Revised*: 30 April 2022*
Accepted*: 15 June 2022*
Publication*: 19 August 2022*

Keywords: - Integrity, Confidentiality, Availability, Recurrent Neural Network , Bio Inspired Algorithms, Ant Colony Optimization, Cognitive Model, Intrusion Detection System.

Introduction

Securing data is an art at the same time sometimes it can be consider as science because which involves many computing algorithms to secure data and its relevant applications. Data is very important asset of any organization if any variation or manipulation in existing data leads to a big issue for the specific organization. The following figure 1 shows the way to protect an organization

data with great support of best optimized bio inspired concepts and strong deep learning neural networks concept. Data can be collected in one common place to analyze its nature later because data collection and accumulation one place is basic step for any research findings. The collected data can be applied to different way to secure its application. Bio inspired concepts are derived from nature and specifically observed from nature of bird and animal life style. The behavior of several animals and birds obtained to apply it in complicated problems to choose an effective strategy.

Malware is a sort of unsafe programming that is utilized to get unapproved admittance to network foundations, secure individual data, or disturb PC activities and offices. Any occasion taking care of cycles, for example, source code, dynamic contents, or other dynamic substance, can be utilized. Creative malware variations can muddle and stay undetected by utilizing complex techniques like befuddling filenames, record highlight changes, or working under the appearance of authentic programming and administrations to keep away from location and erasure. Moreover, by dodging antivirus programming and clouding running tasks, network administrations, and strings from dubious URLs or vault passages, the noxious movement every now and again attempts to upset the whole framework [1,2].

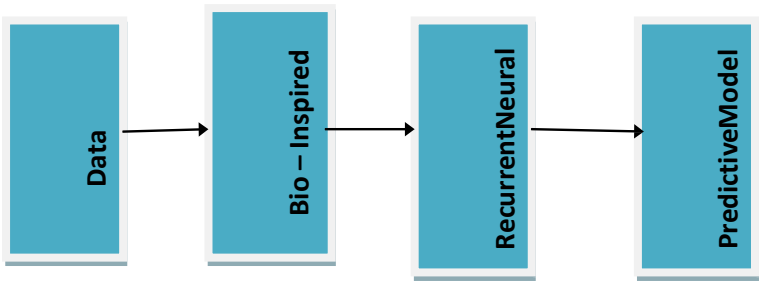

Fig. 1 Concepts of Data security procedure

Program details that indicate the planned conduct of safety basic applications are utilized in determination based identification. Maybe than recognizing the presence of certain attack types, observing executing programs remembers distinguishing varieties for their conduct from these determinations. Therefore, regardless of whether an attack has never been distinguished, it would now be able to be recognized. Early endeavors focused on consecutive projects, whose proposed conduct was characterized by a decent arrangement of activities [3,4].

Validation questions require specific keen abilities for breaking down confounded examples, just as fast moving consideration, speedy reaction, and aptitude information in explicit logical or expert fields. Such components ought to guarantee an undeniable degree of safety and permit just talented clients with specific information to effectively pass the confirmation procedure. Traditional validated codes have a similar high-security highlight as cognitive check measures. Because of the trouble in appropriately understanding or perceiving things on foggy or contorted examples, standard

confirmation are secure. We can use a similar component while executing staggered cognitive systems that require master information or encounters to be fruitful [5].

Information confirmation, security conventions, and data insurance are the three most significant parts of enormous data security. The objective of conveyed processing security the executives is to deal with colossal data the board hardships, keep up with framework respectability, and defend the internet from risks. Enormous data security is worried about continuous unique security perceptions to recognize any expected danger/weakness or even peculiar movement. There is consistently a danger of classified information spilling while at the same time keeping data access speed at a healthy level [6-8].

These frameworks are based on request, they are not unified, they come up short on an appropriate geography, and they as often as possible change their geography as they are fabricated utilizing cell phones. Moreover, the powerlessness of every gadget to communicate data over a significant distance compels them to pass on data in numerous means, utilizing middle of the road hubs as transports. The battery force of the gadgets that are added to the network upholds these network capacities. Subsequently, the network's life span is controlled by the measure of force accessible in every gadget added to the network. The convenient hubs in Ad Hoc networks that impart through remote medium are consequently figured out and set to naturally broaden and shield the whole network The proposed strategy in the paper utilizes the GBC calculation to choose the most energy-proficient gadgets with the least portability, greatest energy accessibility, and briefest distance to the objective, and the ACO to figure out the courses with the most limited distance to have an energy-effective correspondence that works on the network's life span and administration quality [9,10].

Methodology

This section explains various methodology of network security which takes concern over in detection of misconduct in existing applications. Mostly we have discussed the existing findings of security model and cognitive concepts in searching misbehavior identification in the application. Finally discussed few bio inspired algorithms and its different variant also considered to meet the objective of our research. While expanding the edge presented to a bunch of direct limitations, the SVM utilizes a reiterative preparing way to deal with produce an optimal hyper plane where the mistake work is limited. This methodology can be considered as a quadratic programming answer for an enhancement issue.

To accomplish direct detachment, nonlinear data is normally meant a higher measurement. The part stunt, for instance, is a proficient strategy for changing the first data space into a high-dimensional space with an express isolating boundary between data classes. Since there are not many tuning choices, the customary technique is to work in two stages: track down the best improvement boundaries and train the SVM utilizing them [11].

The models are made using the ACT-R cognitive engineering's standards, and they figure out how to perceive malware tests utilizing a restricted preparing plan like that of a human expert. The model builds likelihood dissemination over an assortment of malware families dependent on a malware test, then, at that point gathers a bunch of conceivable malware expectations dependent on that dispersion. The speculations depend on the sub symbolic instruments of the ACT-R design, explicitly the actuation analytics that supports recovery from long haul revelatory memory. Each example's static and dynamic credits are utilized to address it [12].

The OH-BAC calculation was created as a component for VM position. For their exploration, they considered the accompanying components: load balance, CPU usage, memory, transfer speed, stockpiling size, and memory. They had the option to track down the best PM with minimal measure of force use utilizing OH-BAC techniques. Their suggested arrangement, then again, requires more Service Level Agreement time per Active Host [13].

The source gadget decides the briefest way between the source and objective, refreshes the database with the subtleties of the way, and specifies the briefest way utilizing the ACO, which chooses the briefest way by choosing ways improved with gadgets with the greatest, least, and disposes of the remaining. Once the best gadgets have been picked and the network has been set up, the source that demands the transmission of data to an area past the arrive at attempts to track down an appropriate way with minimal measure of transfer speed utilization, correspondence overhead, and distance to the objective, to save energy. The next section derived from idea of all above methodology [9,14,15].

Implementation

The below Fig. 2 is the entire process of our proposed mechanism and named as ACO- RNN-C model. Here server is used to collect all the data pertaining to transmission and packet flow of various nodes and routers. The purpose of the server is analyzing collected data from dynamic array which restricts memory constraint of network components. The traffic and content information is taken for subsequent step to check the flow is normal or harmful. Further the content of normal and affected path will be forwarded to Hierarchical Clustering.

Hierarchical clustering is a category of unsupervised Learning model to group certain parameters. Here confidentiality group, Availability group, Integrity group is formed using above unsupervised mechanisms to identify quantity of manipulation in these parameters after intrusion finding in the current environment. Besides for finding abnormality in path RNN used to take decision with great extent support of its internal memory capacity and also it is quickly iterates between ACO algorithm and Predictive model mentioned in Fig. 2.

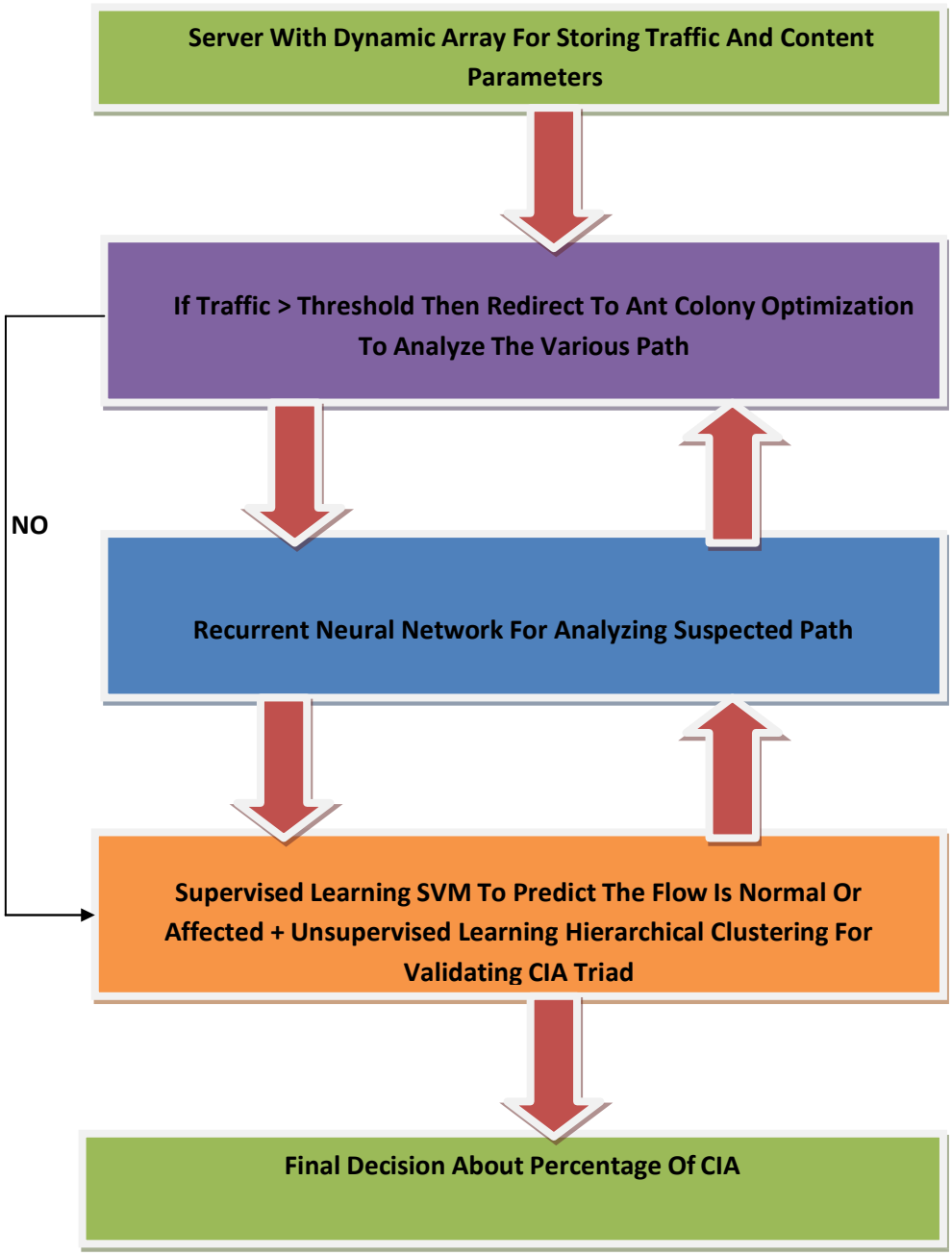

Fig. 2. Cognitive based ACO-RNN-C model

Ant Colony Optimization applied to guess the high dense path where more number of packets flow in the network like ants are rushing to a specified path based on its huge storage of pheromone. ACO finds exactly best optimization and it easily will track the surge flow of different packets rather than less packet flow path in network.ACO algorithm steps also mentioned clearly in the next section. High dense path data analyzed using RNN again for tuning the result in vulnerability detection. SVM used as supervised model for finding best result.

Algorithm (AC-RNN-C)

Step 1: Let we consider the various nodes are participating in network as Node1 to Node n and routers functioning between the different Local Area Networks are consider as Rt_1 to Rt_i.

Step 2: Server with dynamic array container is used to hold all the values in the entire network named as Sv and it can able to store the data of all possible nodes transmission details and router information mentioned in below equation.

$Sv = \sum Rt_1$ to Rt_i.

Where Rt_1 to Rt_i. Consists $\sum Node_1$ to $Node_n$

Step 3: Dynamic Array container release the series of data to the Ant Colony Optimization Algorithm to find affected path using threshold validation.

a. Initially a small verification will be done in beginning of ACO process which is given here as If Traffic > Threshold then pass this flow to ACO algorithm
b. Once the flow greater then threshold value ACO will consider that as input for its processing.
c. ACO algorithm easily can track flooded path by its own capacity based on heavy flow on same route which may caused by botnet. Light density flow also analyzed quickly but concentration will be given to highly dense route
d. Highly dense route can be collected and that parameters are forwarded to next level RNN to decide the flow using predictive models
e. If Traffic < Threshold then directly forward this flow to check CIA triad validation without ACO and RNN process.

Step 4: RNN process starts here to decide further step with the help of many layers according to the training for the result of step 3.

Step 5: Supervised Learning model SVM for prediction process followed by Unsupervised Learning of Hierarchical clustering is done for the purpose of measuring the percentage of deviation in terms of three important concepts which are confidentiality, Availability and Integrity after intrusion detection.

Step 6: Final decision on the abnormal path to avoid further transmission and affected information will be passed to all intermediate routers.

The Algorithm is implemented using python keras because this contains keras API for RNN .The reason behind choosing above tools its readymade methods for implementing algorithm given above and Fig. 2 diagram. The KDD 99 data set was taken to validate the result of CIA with support of clustering procedure using hierarchical approach.

Finally we have implemented the above and DRNN method to verify the performance in terms of intrusion detection and the CIA parameter measurement. The compared result are clearly depicted in Fig. 3 and Fig. 4 and also the graph shows that proposed ACO-RNN-C (Ant Colony Optimization –

Recurrent Neural Network – Cognitive) model is proved as improvement in analysis of IDS and CIA.

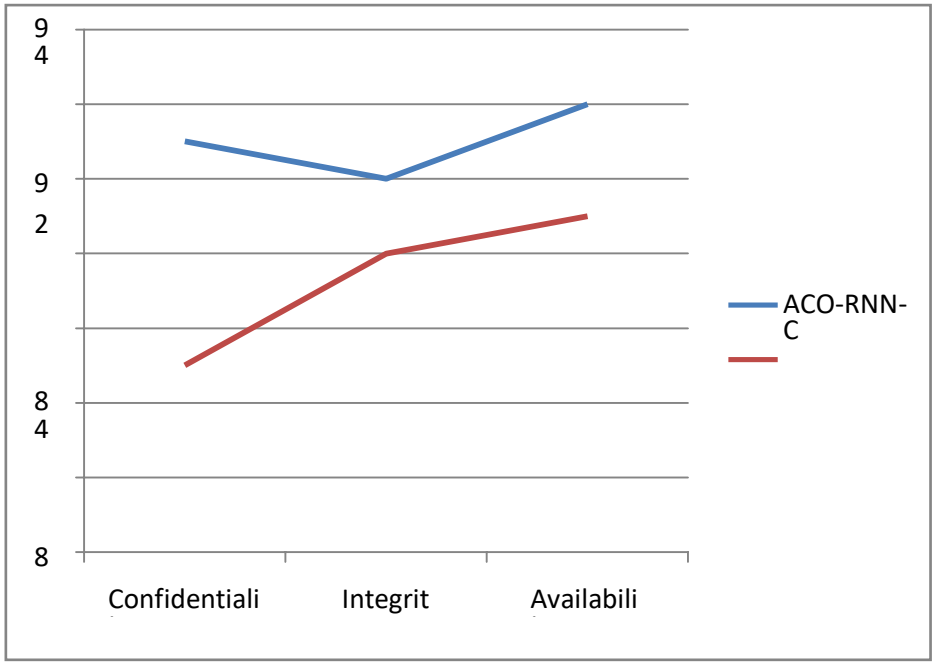

Fig. 3. Comparison of CIA measurement using DRNN and ACO-RNN-C

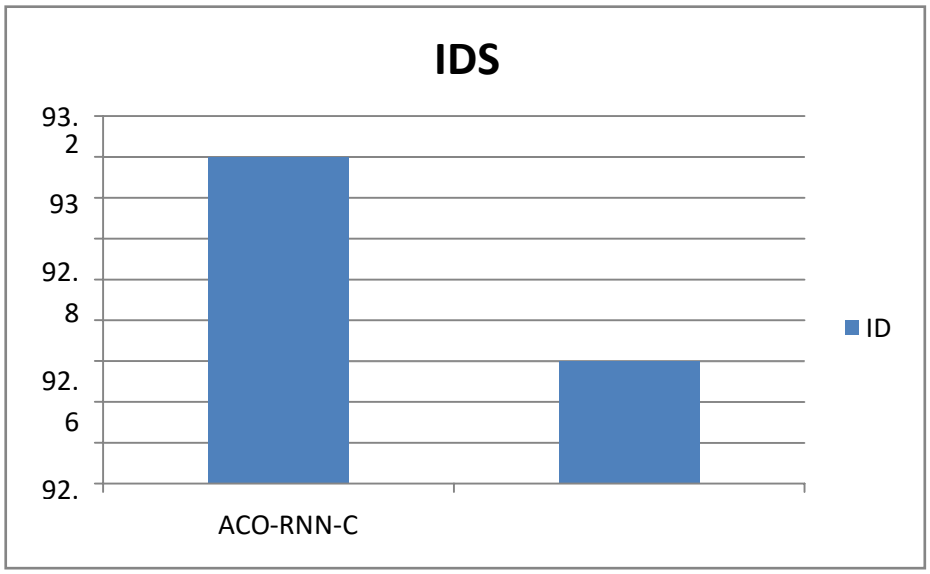

Fig. 4. Comparison of cognitive based IDS

Comparison

Our early proposed methods are taken for evaluating its performance in terms of vulnerability detection and resultant graph shown in Fig. 5. First we have applied in Traditional cryptography it provides reasonable support in finding vulnerability in traffic parameters and content verification. Then cognitive cryptography is taken and applied for the same purpose. Similarly we approached other methodology of our implementation of cognitive Convolutional Neural Network, Dynamic Array – Recurrent Neural Network and ACO-RNN-C. The final methodology discussed in this article shows relatively good increased value when considered to other four approaches.

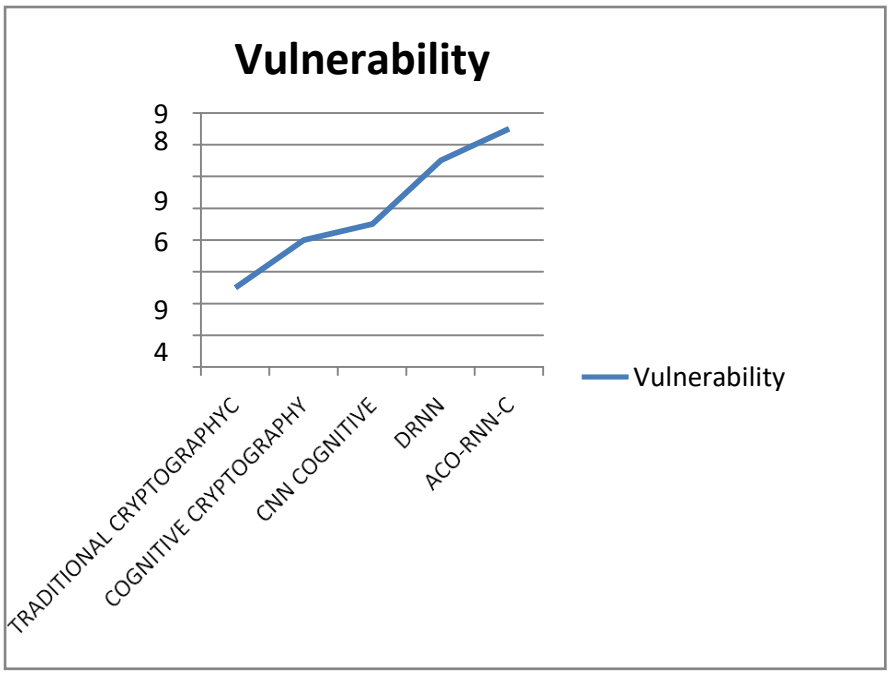

Fig. 5. Comparisons of vulnerability detection using our methodologies

Conclusion

There are several mechanisms being adopted by us to find intrusion detection in an environment. Still many shortfalls retaining in validation against three important key parameters in security concern which are called as CIA Triad. These three parameters are essential to introspect to analyze how far the data affected by hacker during malicious action in the existing set up. Bio inspired concepts pretty useful to bring optimized outcome in any sort of application belongs to client-server based. Cognitive methodology will improve in producing tuned result with the help of neural network. Bio inspired concept along with cognitive model produce better result in terms of predicting the flow is normal or attack flow. Thus the accuracy can be improved when we apply validation against CIA in intrusion detection step.

References

[1] K. Demertzis, P. Kikiras, N. Tziritas, S.L. Sanchez, and L. Iliadis, “The Next Generation Cognitive Security Operations Center: Network Flow Forensics Using Cyber Security Intelligence”, *Big Data Cogn. Comput. 2*, 35, 2018. https://doi.org/10.3390/bdcc2040035

[2] E. Rudd, A. Rozsa, M. Gunther, and T. Boult, “A Survey of Stealth Malware: Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions”, arXiv 2016, arXiv:1603.06028

[3] C. Ko, M. Ruschitzka and K. Levitt, "Execution monitoring of security-critical programs in distributed systems: a specification-based approach," *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097)*, pp. 175-187, 1997, doi: 10.1109/SECPRI.1997.601332.

[4] C. KO, G. Fink, and K. Levitt, “Automated Detection of Vulnerabilities in Privileged Programs Using Exe- cution Monitoring,” in Proceedings of the 10th Computer Security Application Conference, (Orlando, FL), December 5-9, 1994.

[5] Ogiela and Urszula, “Cognitive cryptography for data security in cloud computing”, 32 10.1002/cpe.5557, Concurrency and Computation: Practice and Experience, 2019/11/01.

[6] M. M. Ahsan, K. D. Gupta, A. K. Nag, S. Poudyal, A. Z. Kouzani and M. A. P. Mahmud, "Applications and Evaluations of Bio-Inspired Approaches in Cloud Security: A Review," in *IEEE Access*, vol. 8, pp. 180799-180814, 2020, doi:10.1109/ACCESS.2020.3027841.

[7] T. Lu, X. Guo, B. Xu, L. Zhao, Y. Peng, and H. Yang, “Next big thing in big data: The security of the ICT supply chain”, in Proc. Int. Conf. Social Comput., pp. 1066–1073, Sep. 2013.

[8] S.-H. Kim, N.-U. Kim, and T.-M. Chung, “Attribute relationship evaluation methodology for big data security”, in Proc. Int. Conf. IT Converg. Secur. (ICITCS), pp. 1–4. Dec. 2013.

[9] Dr. Subarna Shakya, “Intelligent and Adaptive Multi-Objective Optimization in WANET Using Bio Inspired Algorithms”, Journal of Soft Computing Paradigm (JSCP) Vol.02 / No.01 Pages: 13-23, http://irojournals.com/jscp, 2020, DOI:https://doi.org/10.36548/jscp.2020.1.002

[10] Malar, A. Christy Jeba, M. Kowsigan, N. Krishnamoorthy, S. Karthick, E. Prabhu, and K. Venkatachalam, "Multi constraints applied energy efficient routing technique based on ant colony optimization used for disaster resilient location detection in mobile ad-hoc network", Journal of Ambient Intelligence and Humanized Computing , 1-11, 2020.

[11] H. William, S.A. Teukolsky, W.T. Vetterling, and B.P. Flannery, “Support Vector Machines, In Numerical Recipes: The Art of Scientific Computing”, 3rd ed.,Cambridge University Press: New York, NY, USA, 2007, ISBN 978-0-521-88068-8.

[12] C. Lebiere, S. Bennati, R. Thomson, P. Shakarian, and E. Nunes, “Functional Cognitive Models of Malware Identification”, In N. Taatgen (Ed), Proceedings of the 13th Annual Conference on Cognitive Modeling. Groningen, Netherlands, 2015.

[13] M. Gamal, R. Rizk, H. Mahdi, and B. E. Elnaghi, “Osmotic bio-inspired load balancing algorithm in cloud computing”, IEEE Access, vol. 7, pp. 42735–42744, 2019.

[14] Alshamlan, M. Hala, Ghada H. Badr, and Yousef A. Alohali, "Genetic Bee Colony (GBC)

algorithm: A new gene selection method for microarray cancer classification", Computational biology and chemistry 56, 49-60, 2015.

[15] Haoxiang, and Wang, "Multi-Objective Optimization Algorithm For Power Management In Cognitive Radio Networks", Journal of Ubiquitous Computing and Communication Technologies (UCCT) 1, no. 02, 97-109, 2019.