International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Optimized Weighted Trust Evaluation Based Intrusion Detection System in WSN

Dr. S. Suganthi
Assistant Professor, Department of Computer Science, Tagore Govt Arts and Science College, Puducherry, India

ARTICLEINFO

Article History:

Accepted: 05 April 2023
Published: 28 April 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
711-718

ABSTRACT

The individual nodes of a wireless sensor network (WSN) implemented in a hostile atmosphere might be readily penetrated by an adversary owing to restrictions such as short-term battery lifespan, storage capacity, and processing capabilities. It is vital to recognise and separate infected nodes with the goal to prevent being misled by the opponent's fake information provided through hacked nodes. However, due of their low flexibility and high communications cost, flat topological networks are difficult to protect effectively. In this research, we suggested an optimised based on weighted-trust assessment to identify malicious networks on top of hierarchy WSN architecture. In this study, we suggested an optimised weighted trust assessment-based intrusion detection system in WSNs, which makes use of a highly adaptable hierarchical trust administration method for clustering wireless sensor networks. To begin, a reliable assessment framework for trust perceptions is offered, which can calculate the node's trusted value based on its activity in order to successfully detect and isolate harmful nodes. Secondly, the trust evaluation model is introduced into an optimized path selection to increase security measures for data forwarding. The simulations of the outputs indicate that the suggested method greatly improves efficiency with respect to of packet loss percentage, end-to-end latency, efficiency, and use of energy, and also that it is resistant to black hole attacks.

Keywords: Wireless sensor networks, Optimized path selection, Weighted trust evaluation, Intrusion Detection, Sensor Node.

I. INTRODUCTION

As a result of the wide availability towards transmission, wireless sensor networks (WSNs) are now vulnerable to a range of assaults, including DoS incidents, manipulating attacks, sinkholes attacks, and so on. We explore putting up a matching system for intrusion detection around the outermost layer using edge computing to address the wireless sensor network

(WSN), taking into account the integrated features belonging to the wireless sensor network [1].

Detecting along with analysing wireless network breaches and assaults has grown into a significant and critical concern [2]. However, owing to the restricted capabilities of wireless devices, the employment of monitoring sites in WSNs to prevent & identify intrusion and assaults is virtually non-existent [3]. Network persistence has received significant study interest because of its usefulness in extending the lifespan of charging-restricted wireless sensor networks, with the renewable WSN surfacing as a possible alternative [4].

Because of the extensive use of wireless sensor networks in domains such as medical treatment, the war, and so on, encryption has emerged as a top priority for delivering signals without data modification [5]. Every node's overall trust score (OTS) is calculated using parameters such as explicit trust, oblique trust, energetic trust, Continuous neighbour Recommendations Trust, authenticating trust, and link reliability trust. This OTS aids in the detection of potentially dangerous nodes [6].

The intrusion detection model, at the other hand, struggled to retrieve typical information about user behaviours entirely and had various drawbacks, including weak generalisation capabilities, a high False Alarm Rate (FAR), and a lack of responsiveness [7]. Intrusion detection is a method capable of identifying cyber-attacks and networks irregularities. So far, many IDS techniques have been proposed [8]. Nonetheless, there are several aspects of their work that might be improved [9]. An intrusion detection model struggled to obtain typical user behaviour information entirely and had various shortcomings, including weak generalisation capabilities, a high False Alarm Rate (FAR), and poor Effectiveness [10].

II. RELATED WORKS

Through monitoring the history and development of network methods and the web, the intrusion detection system is able to determine the nature of the assault. In addition, traditional methods of intrusion identification often include mining associate rules in order to identify intrusion behaviours.

It is vital to have an effective system in place in order to identify the intrusions in WSN. A unique intrusion detection system (IDS) is the goal of the research presented in article [11], which uses a DL model as its basis. In the beginning, the ideal cluster head (CH) is chosen from across the sensor nodes. Based on this pool of sensor nodes, that possess an elevated level of energy can be given priority to serve as CH. An efficient defence system for a wireless sensor network (WSN) may be provided by an intrusion detection system (IDS), which is a preventative network security prevention solution. A WSN cognitive intrusion detection model was presented in this article [12], which may be found here.

A network intrusion detection system that uses feature selection is suggested in the current study [13]. This system is based on a mix of the Whale optimisation algorithm (WOA) and the genetic algorithm (GA), and it uses sample-based classification. In this study [14], a unique technique of a trust-based mechanism for increased security combined with an energy utility and re-usability model is suggested using software-defined networking (SDN) to maximise energy utilisation. The goal of this research is to maximise the amount of energy that can be used.

As a result, an MCDM framework is being developed as part of this project [15] in order to standardise and assess the ML-based IDSs that are used inside the FL architecture of IoMT systems. The model that was suggested [16] may be broken down into three distinct stages, which are as follows: (a) trust-based clustering; (b) cluster head selection; and (c) optimum data routing. At the beginning, the sensors are dispersed in a haphazard manner over the area in which the nodes have the same amount of energy.

In this framework that was introduced in [17], the whale procedure was utilised for the purpose to adjust the high-level parameters of the deep long short-term memories in addition to obtain both a low processing cost and excellent performance. This multiple levels intrusion detection procedure is addressed in detail in this study [18], which employs a hybrid optimization-based DL approach. To begin, the Fisher coefficient score method is used to determine which characteristics are most significant. The amount of the data is then raised before moving on to the data enhancement step.

The Naive Bayes classifier was surpassed by the model that was presented [19], both in terms of its accuracy in making predictions and its rate of inaccurate results. In comparison to other current classifiers, the recommended model was successful in performing well while using just 59% of the whole dataset's features. Tuning the variables of the ML system is an important issue to discuss since doing so may lead to increased detection quality [20]. The preliminary processing is a further field that has room for improvement in terms of quality.

III. APROPOSED METHODOLOGY

Intrusions must be identified under a variety of conditions. This study explores two such instances in which intrusion detection seems critical. To begin, a reliable assessment framework for trust impression is offered, which allows for estimating the node's credibility value based on its activity in order to successfully detect and isolated nodes that are malicious. Secondly, the trust evaluation model is introduced into an optimized path selection to improve the security for data forwarding. Because the suggested method is built on confidence, intruders are recognised according to their trust ratings.

Intrusion detection becomes necessary during path configuration. Only by establishing the most reliable path among the point of origin and the intended destination could excellent service be guaranteed. When exchanging Route Request and Route Reply packets, the level of trust of sites must be taken into account.

3.1 Optimized Weighted Trust Evaluation Method

As a result, the sensor nodes might have been hacked or taken out of service, providing inaccurate data that may misleading the entire network. It is known as the Byzantine issue. A hacked sensor node might regularly broadcast incorrect data to subsequent tiers. Because of the influence of the malicious node, an aggregator on the upper layer may provide incorrect aggregation results. Detecting rogue endpoints at sensor networks, notwithstanding the Byzantine problem, becomes an essential challenge and the hierarchy network of sensors with a weighted network is shown in fig 1.

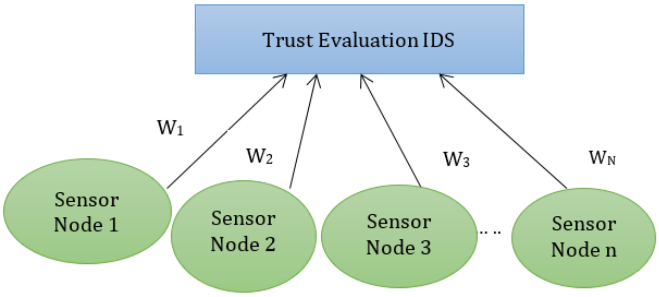

Figure 1. A hierarchy network of sensors with a weighted network

As an initial step towards to an approach, we represent the issue as a weighted network, as illustrated in Figure 2. In the framework, the relationship is customised between a collection of nodes with sensors and their processing node. Every device in the sensor is allocated a weight of W, as illustrated in the picture. The FN receives all SN data and computes an aggregate result based on the weights given to every SN:

$$E = \sum_{n=0}^{M} W_n \times U_n \qquad (1)$$

While E is aggregate value and Wn represents an amount of weight between 0 and 1. The defining of the sensor nodes produces Un. In practise, the output data Un can represent "false" or "true" details, or it could be a continuous integer, which could be a temp measurement. As a result, the precise meaning of results Un is generally determined by the process in which the sensor network is utilised.

The next problem is to adjust the dimensions of every sensor nodes depending on the accuracy of the data given. The weight of every sensor node is updated for two reasons. Initially when a sensor node is hacked and regularly delivers reports that contradict the final decision-making, its weight is going to be reduced.

Following that, the weight of a sensor node becomes less than a particular threshold, we may classify it as being a node that is malicious. Furthermore, the weight determines the extent to which a report may influence the ultimate decision. This is logical since if a sensor node's response is often inaccurate, it might be weighted less heavily in the conclusion.

The section that follows equation reflects this reasoning.

$$W_m = \begin{cases} W_n - \theta \times r_m & \text{if } (U_n \neq e) \\ W_n & \text{elsewise} \end{cases} \qquad (2)$$

Whereas θ is a penalise weighted proportion. Whenever a sensor node's outputs do not match the end result, its overall weight is lowered by the weight penalties multiplied by rn. The value of rn is described as follows:

$$r_m = m / s \qquad (3)$$

Although m is amount of nodes in the cluster providing distinct reports to the FN, whereas s is the entire amount of cluster networks under the equivalent FN. A normalisation process, as stated in the equation that follows, is also performed to ensure that the weight remains within the range of 0 to 1.

$$W_n = W_n / \max(W_1, \ldots . W_N) \qquad (4)$$

According to the modified weights, the transmission node may identify a node as hostile if it's weight is less than a particular threshold. This kind of detection technique has a broad range of applications in many kinds of sensor networks. The technique, for example, allows the total amount of sensor nodes to change, making it ideal for both huge and extremely small systems. Although in order to accomplish effective and superior precision detection, the characterization of sensor node outputs and the frequency of the scalability factor, which varies depending on the actual application, must be properly specified.

Algorithm for Optimized IDS

1. The source creates Route Request (RREQ) packets to start the route discovery process.
2. Whenever the node gets an RREQ packet, it passes the data packet to the nearest one-hop neighbour that it trusts foremost on the path to the destination.
3. To its one-hop neighbours, the node transmits Trust Request packets.
4. Each neighbour responds with details regarding its own forwarding of packets and its one-hop neighbours' Trust information.
5. The Trust Request packet's source assesses the level of trust among all of its one-hop neighbours.

The RREQ packet is transmitted to the neighbour with the highest level of trust.

7. A node sends the RREQ packet to its destination if it determines that the destination is one of its neighbours.
8. The pre-destination node assesses the destination's trust value.
9. A Route Reply (RREP) packet is sent in response from the destination. The from before-destination node either passes the RREP packet or sends a "Cancel

Application" message back to the source, according to how well the destination is trusted.

The fundamental concept is to choose node i's subsequent hop neighbour node j based on pheromone, monitoring sensor residue energy, and estimated trust rating. Typically, the following node must be chosen with greater confidence level and more leftover energy. Considering that m originates from the starting point node, the pathway's starting pheromone with the nodes's energies are equal. Every ant attempts to choose the best route with the lowest cost, and the rate of transition of ant k travelling between node i to j for the subsequent hop may be expressed as:

$$p_{ij}^{k}(t) = \begin{cases} \frac{\left[r_{ij}(t)\right]^{\alpha} . \left[\eta_{ij}(t)\right]^{\beta} . \left[\psi_{j}(t)\right]^{\gamma}}{\sum_{u \epsilon N_k(i)} [r_{iu}(t)]^{\alpha} . [\eta_{iu}(t)]^{\beta} . [\psi_u(t)]^{\gamma}}, j \epsilon N(i) \\ 0, \qquad otherwise \end{cases} \quad (5)$$

where τij(t) signifies the concentration of pheromones in the route at time t, ηij(t) represents the pathway's heuristic score, and ψj(t) is the residual efficiency coefficient of j node. α, β, γ are the pheromones value significance, heuristics value, and remaining power factor, accordingly. They must meet the requirement that 0 < α, β, γ ≤1 and α + β + γ = 1.

The Heuristic element will be computed as follows by picking the single node using the greatest extensive trust score from the neighbour nodes selected as the following hop:

$$\eta_{ij}(t) = \arg max_{j \epsilon N(i)} \{\theta T_{dir} + (1 - \theta) T_{ind}\} \quad (6)$$

Because every sensor node's capacity is limited, the energy that remains of the networks in the route, as well as the connection length, must be considered while in the pheromone update phase. It is capable of successfully balancing network energy demand and reducing the accumulated energy gap among nodes. Whenever the residual value of nodes on various links is equal, the shortest route routing is used. As a result, once k ants arrived to the aggregating node, the pheromone augmentation may be calculated as follows:

$$\Delta T_k(t) = \frac{\sum_{res}^{(t)}(i) \,/\, avg_{s \epsilon N(i)}\left(E_{res}(S)\right)}{E_0 - max_{s \epsilon N(i)}\left\{\left(E_{res}(S)\right)\right\}} \quad (7)$$

Where $avg_{s \epsilon N(i)}\left(E_{res}(S)\right)$ and $max_{s \epsilon N(i)}\left\{\left(E_{res}(S)\right)\right\}$ indicate the average and highest residual value of all networks node i, appropriately. The starting energy of every sensor node is represented by E_0.

The calculation will be utilised for updating the pheromone effect on the way (8).

$$T_{ij}(t) = (1 - \rho) T_{ij}(t) + \Delta T_k(t) \quad (8)$$

Where ρ symbolizes the pheromone volatilizing factor and $0 \leq \rho \leq 1$.

$\Delta T_k(t)$ signifies the pheromone's increase throughout the present round.

IV. Results and discussions

The simulation tests are carried out using MATLAB to validate the performance of the suggested method for protected routing. In this experiment, certain nodes were selected randomly assigned greater trust levels than others. The suggested approach effectively establishes routes between highly trustworthy nodes. Three measures are established to assess the recognition algorithm's efficiency. The reaction time, that is the mean detection process for accurately discovered malicious nodes, demonstrates how quickly harmful nodes may be identified. The identification rate, defined as the ratio of identified malicious nodes to the overall malicious nodes, reflects the efficiency of our approach. Figure 2 depicts an examination of trust values in the absence of an assault. In the lack of malevolent nodes, the amount of nodes that communicate successfully grows significantly over time. Figures 3 and 4 demonstrate the level of confidence in the event of a malicious node's assault.

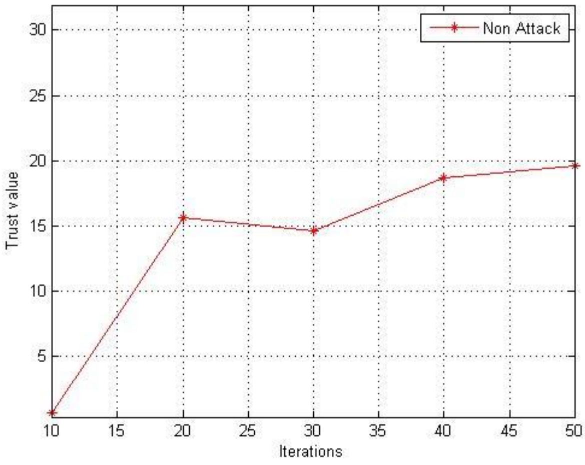

Figure 2. Trust value in a non-attack scenario

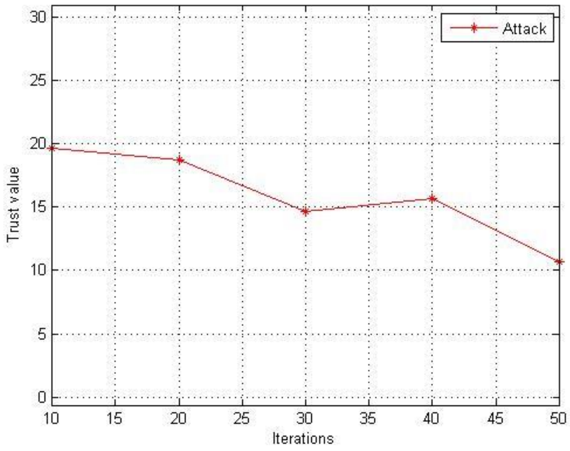

Figure 3. Trust value during a malicious node

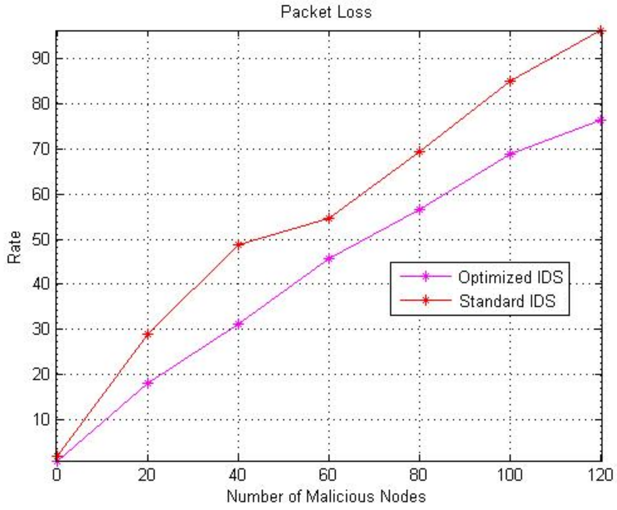

Figure 4. Rate of packet loss

As seen in Fig. 4, the overall tendency of packet loss rates of all methods increases as the number of malicious nodes exhibiting aggressive behaviours increases.

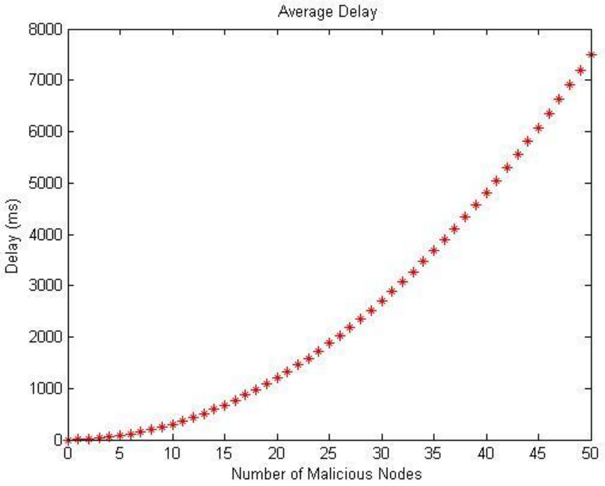

Figure 5. The average time Delay

Figure 5 depicts an average lag in time and the increase in the quantity of malicious nodes. Figure 6 depicts the network's performance comparison.

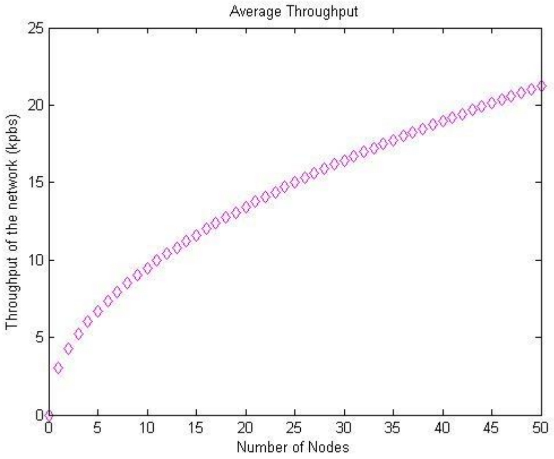

Figure 6. The performance of the Network

V. Conclusion

To protect against internal assaults from harmful nodes, this paper suggests an optimized weighted trust evaluation based intrusion detection system in WSN in WSNs enabling secure route that employ the trust sensing approach. To begin, a reliable assessment framework for trust perceptions is offered, that can calculate the node's trust level based on its activity in order to successfully detect and isolate nodes that are malicious. Secondly, the trust evaluation model is introduced into an optimized path selection to increase the safety for data transmission. Simulation findings indicate that the suggested method greatly improves efficiency in terms of losing packets rate, throughout its entirety latency, efficiency, and usage of energy, and additionally it is resistant to black holes attacks.

VI. REFERENCES

[1]. Ngueajio, M. K., Washington, G., Rawat, D. B., & Ngueabou, Y. (2022, September). Intrusion Detection Systems Using Support Vector Machines on the KDDCUP'99 and NSL-KDD Datasets: A Comprehensive Survey. In Intelligent Systems and Applications: Proceedings of the 2022 Intelligent Systems Conference (IntelliSys) Volume 2 (pp. 609-629). Cham: Springer International Publishing.

[2]. Li, Y., Ghoreishi, S. M., & Issakhov, A. (2022). Improving the Accuracy of Network Intrusion Detection System in Medical IoT Systems through Butterfly Optimization Algorithm. Wireless Personal Communications, 126(3), 1999-2017.

[3]. Shi, L., & Li, K. (2022). Privacy Protection and Intrusion Detection System of Wireless Sensor Network Based on Artificial Neural Network. Computational Intelligence and Neuroscience, 2022.

[4]. Thakkar, A., & Lohiya, R. (2022). A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. Artificial Intelligence Review, 55(1), 453-563.

[5]. Li, W., Wang, Y., & Li, J. (2022). Enhancing blockchain-based filtration mechanism via IPFS for collaborative intrusion detection in IoT networks. Journal of Systems Architecture, 127, 102510.

[6]. Emil Selvan, G. S. R., Daniya, T., Ananth, J. P., & Suresh Kumar, K. (2022). Network Intrusion Detection and Mitigation Using Hybrid Optimization Integrated Deep Q Network. Cybernetics and Systems, 1-17.

[7]. Srividya, P., & Devi, L. N. (2022). An optimal cluster & trusted path for routing formation and classification of intrusion using the machine learning classification approach in WSN. Global Transitions Proceedings, 3(1), 317-325.

[8]. Alamleh, A., Albahri, O. S., Zaidan, A., Alamoodi, A. H., Albahri, A. S., Zaidan, B. B., ... & Al-Samarraay, M. S. (2022). Multi-attribute decision-making for intrusion detection systems: A systematic review. Int J Inf Technol Decis Mak, 10.

[9]. Alzubi, O. A. (2022). A deep learning-based frechet and dirichlet model for intrusion detection in IWSN. Journal of Intelligent & Fuzzy Systems, 42(2), 873-883.

[10]. Imanbayev, A., Tynymbayev, S., Odarchenko, R., Gnatyuk, S., Berdibayev, R., Baikenov, A., & Kaniyeva, N. (2022). Research of Machine Learning Algorithms for the Development of Intrusion Detection Systems in 5G Mobile Networks and Beyond. Sensors, 22(24), 9957.

[11]. Kagade, R. B., & Jayagopalan, S. (2022). Optimization assisted deep learning based intrusion detection system in wireless sensor network with two-tier trust evaluation. International Journal of Network Management, 32(4), e2196.

[12]. Liu, G., Zhao, H., Fan, F., Liu, G., Xu, Q., & Nazir, S. (2022). An enhanced intrusion detection model based on improved kNN in WSNs. Sensors, 22(4), 1407.

[13]. Mojtahedi, A., Sorouri, F., Souha, A. N., Molazadeh, A., & Mehr, S. S. (2022). Feature selection-based intrusion detection system using genetic whale optimization algorithm and sample-based classification. arXiv preprint arXiv:2201.00584.

[14]. Sahoo, S. K., Mudligiriyappa, N., Algethami, A. A., Manoharan, P., Hamdi, M., & Raahemifar, K.

(2022). Intelligent trust-based utility and reusability model: Enhanced security using unmanned aerial vehicles on sensor nodes. Applied Sciences, 12(3), 1317.

[15]. Alamleh, A., Albahri, O. S., Zaidan, A. A., Albahri, A. S., Alamoodi, A. H., Zaidan, B. B., ... & Jasim, A. N. (2022). Federated learning for IoMT applications: a standardisation and benchmarking framework of intrusion detection systems. IEEE Journal of Biomedical and Health Informatics.

[16]. Sajan, R. I., Christopher, V. B., Kavitha, M. J., & Akhila, T. S. (2022). An energy aware secure three-level weighted trust evaluation and grey wolf optimization based routing in wireless ad hoc sensor network. Wireless Networks, 28(4), 1439-1455.

[17]. Ramana, K., Revathi, A., Gayathri, A., Jhaveri, R. H., Narayana, C. L., & Kumar, B. N. (2022). WOGRU-IDS—An intelligent intrusion detection system for IoT assisted Wireless Sensor Networks. Computer Communications, 196, 195-206.

[18]. GSR, E. S., Azees, M., Vinodkumar, C. R., & Parthasarathy, G. (2022). Hybrid optimization enabled deep learning technique for multi-level intrusion detection. Advances in Engineering Software, 173, 103197.

[19]. Gautam, S., Henry, A., Zuhair, M., Rashid, M., Javed, A. R., & Maddikunta, P. K. R. (2022). A Composite Approach of Intrusion Detection Systems: Hybrid RNN and Correlation-Based Feature Optimization. Electronics, 11(21), 3529.

[20]. Sarkar, A., Sharma, H. S., & Singh, M. M. (2023). A supervised machine learning-based solution for efficient network intrusion detection using ensemble learning based on hyperparameter optimization. International Journal of Information Technology, 15(1), 423-434.

Cite this article as :

Dr. S. Suganthi, "Optimized Weighted Trust Evaluation Based Intrusion Detection System in WSN", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 2, pp. 711-718, March-April 2023.
Journal URL : https://ijsrset.com/IJSRSET23102113 |