IRJAEH

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 02 February 2025
Page No: 164-171
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0022

Neural Network Model Using An Enhanced Whale Optimization Method For Cyber Threat Detection

Asra Sarwath[1], Dr. Raafiya Gulmeher[2], Zeenath Sultana[3]

[1,2,3] Assistant Professor, Dept. of CS&E, Khaja Bandanawaz University, Kalaburagi, Karnataka, India

Emails: sarwath@kbn.university[1], raafiya@kbn.university[2], zeenath@kbn.university[3]

Abstract

In our modern, highly-connected society, cybersecurity is of the utmost importance. With the rapid advancement and increasing integration of technology into our daily lives, the need of cyber security cannot be emphasized enough. Cybersecurity is vital for individual's protection. Credential stuffing is a sort of cyber assault whereby attackers use previously obtained usernames, keywords and passwords to unlawfully invoke user accounts across many websites. This is plausible as many individuals utilize identical passwords and usernames across several websites. The proposed Enhanced Whale Optimization Algorithm Neural Network (EWOA-NN) model may address the issues of failure detection, prediction, and credential stuffing attacks. A unique optimization method called the neural network is trained using EWOA. After confirming the efficacy of the proposed attack identification model, we will conduct an empirical comparison with respect to certain security research.

Keywords: *Cyber-attack, Neural Network (NN), Credential stuffing.*

1. Introduction

The increasing use of internet-connected digital gadgets has elevated the significance of cybersecurity as an academic discipline. The extensive interconnectedness has facilitated customers' lives, although it has concurrently rendered them more vulnerable to cybersecurity issues. To develop defenses against threats posed by attackers, researchers are focusing on this domain. Organizational networks, information systems, infrastructures, and personal gadgets are often targeted by hackers. Cyber assaults have evolved considerably since the late 1980s, paralleling technical advancements. Unfortunately, this increases the possible vulnerability to cyber assaults. The impact or harm inflicted by a hostile assailant correlates with the element of spectacle. Damages may include a reduction in the losses incurred by an individual or organization. A Denial of Service attack would result in revenue loss by disrupting the platforms of significant e-commerce platforms such as Amazon etc. The following consideration pertains to an individual or organization's vulnerability. Certain enterprises may be functioning with outdated infrastructure and security technologies, leaving them vulnerable to attackers. A cyber attack termed "credential stuffing" exploits the tendency of individuals to use same login credentials across several distinct websites. Attackers systematically and expeditiously input extensive lists of usernames and passwords into various websites, applications, and automated methods and bots. Attacks succeed due of widespread password reuse across several platforms. Given that 64% of individuals recycle credential stuffing attacks exploit users' credentials across numerous accounts represent a prevalent cause of data breaches. Credential stuffing accounts for almost 50% of all daily attempts to login on platform. To protect against attacks involving credential stuffing, enabling two-factor authentication (2FA), users must adhere to robust security policies, including using unique passwords, regularly updating passwords, and monitoring accounts. Attackers may use compromised user credentials to gain access to other websites or services associated with the individual's accounts after a data breach. To safeguard themselves against credential stuffing attacks, consumers should activate two-factor authentication (2FA), use unique passwords, change their passwords often, and carefully review their accounts. Most researchers depend on the encryption-based network authentication. The authentication procedure does not indicate the presence of an attacker; it only confirms the legitimacy of the nodes. Consequently, machine learning-based attack detection is essential. Diverse strategies using Optimization Techniques have been used to tackle the challenges of identifying attack vulnerabilities. These methodologies may be used to analyze attack datasets and improve classifier precision. Consequently, these techniques for detecting attacks and anomalies are reliable and appropriate. These strategies assess the multi-objective variable to get optimal results. There are many motivations for the integration of optimization methods with neural networks. Integrating machine learning (ML) into the network has emerged as a critical topic [1]. Proposes an approach for attack identification with ML, accompanied by optimization help. Elucidates the notion of optimization for identifying attack procedures executed within the constraints of penalty, time, and energy. Maintains the confidentiality aspect of the proposed attack detection system to guarantee secure and unimpeded network interactions. Proposes an advanced iteration of the traditional WOA algorithm [2], an innovative Enhanced Whale Optimization model, for addressing the designated optimization challenges. The subsequent sections of the paper are organized as follows: The second deals with Literature Review, next section with methodology later section with Results and Discussions Finally Conclusion section.

2. Literature Survey

A multitude of scholars have analyzed extensive research to identify incursion in this study. Panda et al[3]. propose an intrusion detection system that utilizes several characteristics of node behavior. The authors devised an effective methodology for identifying network assaults by integrating efficient sensor data fusion with accurate attack behavior detection as illustrated in Figure 1. The authors use a lightweight protocol interaction method between the client and server to consolidate real-time status information, therefore minimizing false alarms and lowering network overhead. Hoque et al. [4] devised a genetic algorithm for the intrusion detection system. The authors used the KDD99 benchmark dataset to utilize information for filtering traffic data and streamlining the procedure. Mangrulkar et al. used DDoS attacks to integrate four independent detection approaches. No dependable application layer detection technique exists; this method is only used for network layer protocols. Cusack and Almutairi developed a security architecture to combat DoS attacks in peer-to-peer networks. Zho et al. [5] suggested a hypothesis to ascertain the behavior of natural text samples. This method is designed to identify aberrant network behavior that diverges from conventional grammar norms, using a novel hidden Markov model. Whale Optimization Algorithm (WOA) [6] to address the inherent drawback of premature convergence. The integration of a modified bilateral phase with WOA enhances the algorithm's equilibrium, allowing a more extensive investigation of searching space while mitigating the wasteful use of computational resources via over exploitation. Computer scientists and people throughout the world are understandably terrified by the studies presented by Abiodun et al. and Omolara et al. , which show that cyber-attacks have developed into an asymmetrical kind of warfare. Abiodun et al. Proposed artificial neural network models for research focus on feedforward and feedback propagation, emphasizing data analysis factors like processing speed, accuracy, convergence, performance, latency, scalability, volume and fault tolerance. Alawida et al. A study reveals variations in cyber-attack methodologies, with hacking assaults being the most prevalent, totaling 330 out of 895 incidents, which constitutes 37%. The subsequent category was spam email attacks at 13%, followed by emails also at 13%, and harmful domains at 9%. Mobile applications accounted for 8%, phishing constituted 7%, malware represented 7%, browsing applications included 6%, DDoS attacks were at 6%, website applications also were at 6%, and MSMM was 6%. Taofeek et al. provide a Cognitive Deception Model (CDM) based on a neural framework that processes an input message to produce syntactically cohesive and semantically coherent decoy messages that seem independent but are reasonable and persuasive, aimed at mentally burdening and deceiving opponents. Giluka et al. [7] provide an intrusion detection method for network traffic termed “Correlation-based Feature-Selection-Bat-Algorithm” (CFSBA). This method is trained and tested using features from the KDDCup99 dataset. Figure 1 shows Credential of Stuffing Attacks

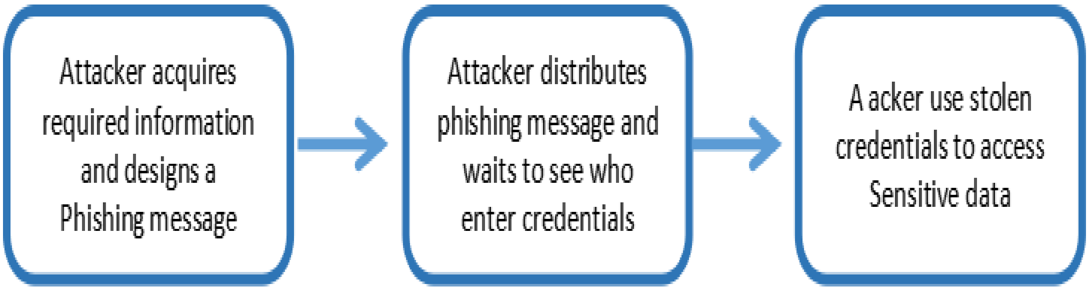

Attacker acquires required information and designs a Phishing message
Attacker distributes phishing message and waits to see who enter credentials
A acker use stolen credentials to access Sensitive data

Figure 1 Credential of Stuffing Attacks

3. Methodology

3.1 Proposed architecture for the identification and detection of attacker nodes in a cyber-network using machine learning

The suggested structure for the network attack detection approach is shown in Fig. 2. The KDD Cup dataset has 200 attacker nodes and 200 safe nodes, all of which are registered on the server using distinct biometric data. The CHs are selected from these nodes with a unique Enhanced Whale Optimization algorithm. Furthermore, four variables are considered in the decision-making process: "energy, delay, distance, and penalty." The node exhibiting the highest energy, minimal distance, lowest penalty, and reduced latency is likely to serve as a Cluster Head (CH). A lack of closeness to CH and energy levels below the CH threshold are characteristics that define the CH-based clusters. Additionally, the most effective cluster head and node data are both preserved by the blockchain [8]. Upon the enrollment of nodes into the system, clusters are formed to mitigate the network's burden; nevertheless, if a malicious node is detected during this procedure, pinpointing the exact node amongst the many nodes becomes challenging.

3.2 A Proposed Method for Detecting Attacks Via Optimization Method to Safeguard Against Credential Stuffing Attacks

- **Optimal Cluster Head Selection:** This research considers limits like distance, security penalties, energy, and time in the selection of the CH. The objective is to discover a CH node characterised by minimal distance, penalty, and delay, while maximising energy.
- **Distance Measurement (D):** clusters are generated when the nodes approach the cluster head. Consequently, clusters arise. The distance matrix D(m * n) is mathematically represented by Eq. (1).

$$D(m*n)=\begin{bmatrix} d_{Mc1,x1} & d_{Mc1,xn} \\ d_{Mc2,x1} & d_{Mc2,xn} \\ & \\ d_{Mcm,x1} & d_{Mcm,xn} \end{bmatrix} \text{---------1}$$

dMc represents the Euclidean distance between the cluster head (Mc) along with each node displayed in Equation (1). Y1, Y2,..., Yn are the designations given to the sensors located at nodes in an LTE network. Additional notation for node locations is y and z, whereas the Euclidean distance dr,q is calculated using Equation (2).

$$d_{r,q}=\sqrt{(r_y-q_y)^2+(r_z-q_z)^2} \text{ ----2}$$

Every component in Eq. (1) represents the distance from the node to the rth CH. The threshold distance, in numerical terms, denotes the maximum distance a qth node can connect to a cluster

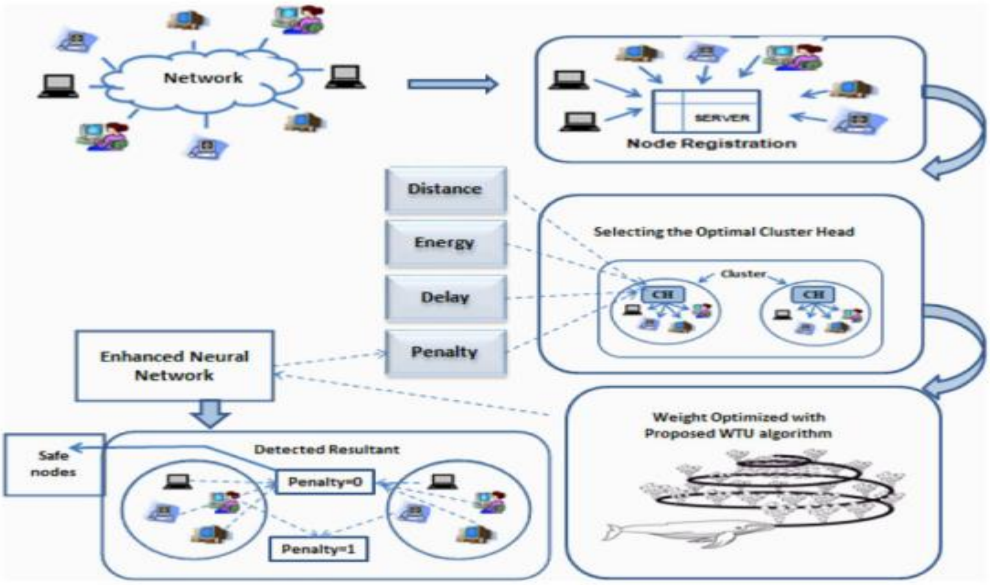


Figure 2 **Proposed Framework for The Identification of Attacks**

Energy model (En): A major criterion for selecting CH is energy consumption. The energy consumption model delineates a network framework that minimizes energy use across numerous functions, including reception, transmission, aggregation, and sensing. Equation (2) specifies the numerical value network the total energy (EnTX(M : d)) required for the dissemination of N bits of data across the dth distance between nodes and the cluster head, and vice versa.

$$En_{RX}(M:d) = En_e M \quad \text{--------}\ 3$$

The punishment function, established by a Neural Network, is essential for detecting attackers inside nodes. The binary nature of the penalty function (1 or 0) dictates the elimination of a node from the MTC process. The effectiveness of the punishment functionality is shown by its suitability, and the outcomes of the Neural Network are crucial to this evaluation. Proposed advanced whale optimisation algorithm Proposed modifications to the algorithm aim to enhance the convergence rate along with the efficiency of the current WOA20. The Whale Optimization Algorithm [9] is designed towards rapid convergence to solutions that are close to

including the Firefly algorithm (FF25) [16] , Jaya algorithm (JA24) [17], Grey Wolf [18] with Jaya algorithm (WI-JA26), and Grey Wolf algorithm

optimal. This quick convergence is beneficial in situations involving limited processing resources or when prompt decision-making is essential. Self-improvement has been shown to be beneficial in traditional optimisation methods[10-15]. This is a concise elucidation of the mathematical modelling of the proposed EWOA algorithm.

Prey Encirclement: The whales can identify their prey and encircle them. The coefficient matrices are B and H, with ongoing iteration represented by t; provide the contextual behaviors of humpback whales.

$$G = \left| H.Rp(t) - R(t) \right| \quad \text{-------------}4$$

$$R(t+1) = Rp(t) - B.G \quad \text{------------}5$$

Furthermore, R denotes the position of the vector, whereas Rp indicates the best position identified so far. The evaluation of the exploratory phase for Prey is provided.

4. Results and Discussion

The proposed approach for identifying cyber network threats using an optimisation strategy was tested in MATLAB, and the results are recorded. The proposed model is compared to known models,

(GWO19) [19], regarding active nodes and network longevity. The presented work is beneficial for evaluating active nodes and prolonging network longevity. Analysis of active nodes The nodes that remain at the conclusion of each cycle are termed the live nodes. A thorough 100-round evaluation of the planned and existing works is conducted, with the conclusive results shown in Fig. 2. The quantity of active node at the end of each round is ascertained by modifying the counts of attackers and cluster heads. Figure 3a illustrates the quantity of active nodes at the conclusion of the 100th iteration, contingent upon the variation in the amount of attackers inside the network. The proposed approach maintains a greater number of active nodes when the attacker count hits 20. superior than the traditional models such as JA, WI-JA,FF,and GWO in that sequence. Figure 3 shows Analysis of Active Nodes. (a) Number of Attackers and (b) Number of CH

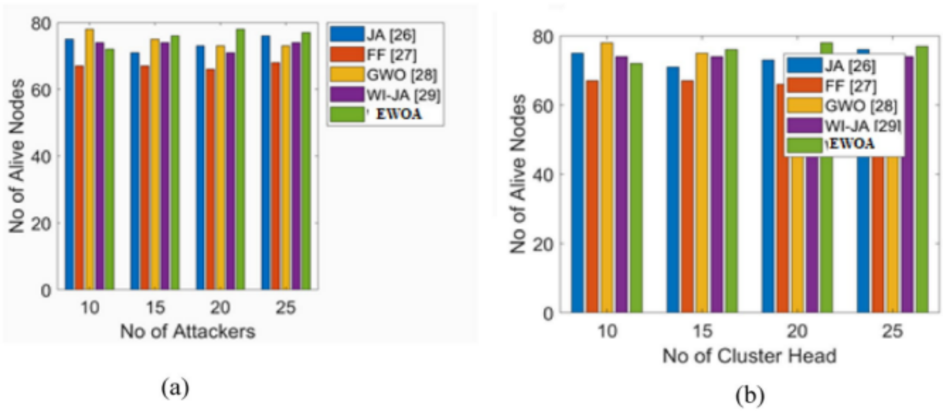
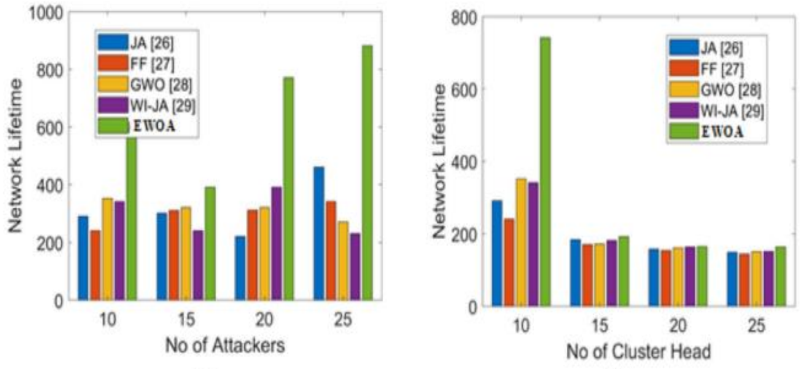


Figure 3 Analysis of Active Nodes. (a) Number of Attackers and (b) Number of CH

The research indicates that the quantity of active nodes produced by the task stays high despite the presence of supplementary attackers. Additionally, the number of active nodes corresponding to different counts of CHs is shown in Fig. 3b. The quantity of CH fluctuates as nodes use their energy and cease functioning, while other nodes continuously join the network. With 100 nodes selected for this assignment, the number of Cluster Heads must be at least 10. The quantity of active nodes in the suggested study increases when the number of CH reaches 15, relative to prior techniques in that sequence. The evaluation clearly demonstrates that, for the designated task including a fluctuating quantity of CHs, the count of active nodes is elevated. Evaluation on network lifetime The lifespan ratio is computed to ensure network stability and sufficient capacity for data packet transmission inside the network. The longevity ratio is a crucial factor in evaluating performance. Figure 4 illustrates the performance assessment of the performed work in comparison to the conventional approach, with variations in the number of attackers and CHs. Figure 3a illustrates the network performance outcomes for varying numbers of attacker nodes. Compared to previous common models, the network longevity using the proposed method is enhanced, even with a higher number of attacker nodes present. The proposed approach attains an extended network lifespan when the number of attackers is 25. Additionally, Fig. 4b depicts the network lifetime analysis across various CH counts based on the provided study. The offered work exhibits the longest network lifespan compared to the typical models, as shown by the overall findings of the study. Statistical performance evaluation Given the stochastic nature of the meta-heuristic method, each algorithm is conducted normalized network energy, ten times to get data, and the objective cost to be minimized, so ensuring a fair comparison. This assessment is conducted for a different number of CHs, and the results are shown in Table 1. The study is conducted across many scenarios, including worst, best, standard deviation, mean and median. In the optimal situation, the proposed work outperforms established models such as JA, WI-JA, FF and GWO by 3.2%, 1.4%, 5.3%, and 3.1%, respectively. The average performance of the proposed work surpasses that of existing methods, namely JA, FF, GWO, and WI-JA, by 2.3%, 5.1%, 3.1%, and 1.2%, respectively. Consequently, the appraisal indicates that the precision of attack detection in neural networks is superior. According to the comprehensive examination, the suggested model exhibits a reduced computation time when juxtaposed with conventional methodologies such as the Jaya algorithm (JA), firefly algorithm (FF), grey wolf algorithm (GWO), and grey wolf with Jaya algorithm (WIJA). Cybersecurity is a dynamic domain in which threats and vulnerabilities always change as depicted in Table 2. Figure 4 shows Examination of Network Longevity. (a) Number of Attackers, (b) Number of CHs. Table 1 Statistical Assessment of the Proposed Study in Comparison to Previous Studies: Precision Table 2 Shows Comparison of Computational Analysis.



(a) (b)

Figure 4 Examination of Network Longevity. (a) Number of Attackers, (b) Number of CHs

Table 1 Statistical Assessment of the Proposed Study in Comparison to Previous Studies: Precision

CH count	JA[24]	FF[25]	GWO[19]	WI-JA[26]	EWOA
Best Performance					
CH=10	0.002887	0.002782	0.002751	0.002658	0.002653
CH=15	0.004040	0.004411	0.004063	0.004138	0.004106
CH=20	0.005562	0.005327	0.005813	0.00466	0.004084
CH=25	0.006822	0.006047	0.006688	0.006831	0.007048

Table 2 Comparison of Computational Analysis

Models	Time of Computation
JA	2496.2
FF	6168.8
WIJA	2842.6
GWO	2782.4
FF	5868.9
WIJA	2842.7
EWOA	2142.9

Conclusion

This study presents an attack detecting model using mutual knowledge, optimized and combined with a cluster-based identification system. The methodologies for attack detection as well as clustering both used the notion of optimization [21]. Four key characteristics were evaluated in the selection of CH: energy, distance, delay and penalty. The proposed attack detection technique ensures a reliable and uninterrupted network connection. The EWOA, an innovative methodology, was created to tackle the identified optimization challenges. The efficacy of the suggested attack detection system was shown, while a comparison was conducted concerning certain security evaluations. The proposed approach attains significant network longevity with 25 attackers, surpassing previous models by 54%, 59%, 64%, and 69%. The quantity of active nodes in the given work is substantial when the count of CH is 15; it exceeds others by 12.4%, 18.74%, 6.24%, and 4% respectively. The proposed EWOA-ANN model effectively addresses the issues of, failure detection, prediction, and credential stuffing attacks. Data availability: The data supporting the results of this inquiry are included inside the text.

References

[1]. Onu, I. J. et al(2023). “Author correction: Detection of Ponzi scheme on Ethereum using machine learning algorithms” Sci. Rep. 13, 20952, 2023.

[2]. S. S. Sudheesh, M. S. Joseph and S. S. Kumar, "Color Image Segmentation Using Multiobjective Whale Optimization Algorithm", *IEEE Access*, vol. 8, pp. 130299-130308, 2020.

[3]. Panda, P. K. and Chattopadhyay, S. “An improved authentication and security scheme for LTE/LTE-A networks” J. Ambient Intell. Humaniz. Comput. 11, 2163–2185. https:// doi.org /10.1007/ s12652-019-01248-8 (2019).

[4]. Haque et al, “An Implementation Of Intrusion Detection System Using Genetic Algorithm”, IJNSA, Vol.4, No.2, March 2012, Doi: https://arxiv.org/pdf/1204.1336.

[5]. Zho et al(2019), “Predicting overall customer

[6]. Sanjoy Chakraborty et al, “An enhanced whale optimization algorithm for large scale optimization problems”, Knowledge-Based Systems, Volume 233, 2021, 107543, https:/ /doi.org/ 10.1016/j .knosys. 2021.107543.

[7]. Giluka et al., “Enhanced class based dynamic priority scheduling to support uplink IoT traffic in LTE-A networks”, JNCA,2018,

[8]. Sana Amjad et al, “Blockchain based Authentication for end-nodes and efficient Cluster Head selection in Wireless Sensor Networks”, Distributed Computing, 2021.

[9]. Deng, H et al, “Ranking-based biased learning swarm optimizer for large-scale optimization”, Inf. Sci. 2019, 493, 120–137.

[10]. Aziz, M. A. E., Ewees, A. A., & Hassanien, A. E. (2018), “ Multi-objective whale optimization algorithm for content- based image retrieval”, Multimedia Tools and Applications, 1–38.

[11]. Cui, D. (2017). Application of whale optimization algorithm in reservoir optimal operation. Advances in Science and Technology of Water Resources, 37(3), 72–79, 94.

[12]. Evirgen, F. and Yavuz, M. , “An alternative approach for nonlinear optimization problem with Caputo-Fabrizio derivative”, ITM Web of Conferences,2018, 01009.

[13]. Karthikeyan, S. and Christopher, T, “A hybrid clustering approach using artificial bee colony (ABC) and particle swarm optimization”, International Journal of Computer Applications, 2014, 100(15).

[14]. Houssein, E.H.; Saber, E.; Ali, A.A.; Wazery, Y.M, “Centroid mutation-based Search and Rescue optimization algorithm for feature selection and classification”, Expert Syst. Appl. 2022, 191, 116235.

[15]. Ahmadianfar, I et al, “ INFO: An Efficient Optimization Algorithm based on Weighted Mean of Vectors”, Expert Syst. Appl. 2022, 195, 116516.

[16]. Nur Farahlina Johari et al, “Firefly Algorithm for Optimization Problem”, Applied Mechanics and Materials Vol. 421, 2013.

[17]. R. Venkata Rao, “Jaya: A simple and new optimization algorithm for solving constrained and unconstrained optimization problems”, IJIEC, 2016.

[18]. Abdullah Alzaqebah, “A Modified Grey Wolf Optimization Algorithm for an Intrusion Detection System”, Mathematics 2022, 10, 999. https://doi.org/10.3390/ math10060999.

[19]. Dixit, P et al, “Comparing and Analyzing

Applications of Intelligent Techniques in Cyberattack Detection",. Secur. Commun. Netw. 2021, 2021, 5561816.

[20]. Asra Sarwath, Dr.Raafiya Gulmeher and Zeenath Sultana, "Spark Mllib intrusion detection mechanism using machine learning models", IJEECS, Vol 33,No 2, Feb 2024.

[21]. http://dx.doi.org/10.11591/ijeecs.v33.i2.pp1235-1242.

[22]. Zeenath Sultana, Dr.Raafiya Gulmeher and Asra Sarwath, "Methods for optimizing the assignment of cloud computing resources and the scheduling of related tasks", IJEECS, Vol 33,No 2, Feb 2024. http://dx.doi.org/10.11591/ijeecs.v33.i2.pp1092-1099