scientific reports

Check for updates

OPEN

Hybridization of synergistic swarm and differential evolution with graph convolutional network for distributed denial of service detection and mitigation in IoT environment

Chukka Ramesh Babu[1], M. Suneetha[2], Mohammed Altaf Ahmed[3], Palamakula Ramesh babu[4], Mohamad Khairi Ishak[5], Hend Khalid Alkahtani[6]✉ & Samih M. Mostafa[7,8]

Enhanced technologies of the future are gradually improving the digital landscape. Internet of Things (IoT) technology is an advanced technique that is quickly increasing owing to the development of a network of organized online devices. In today's digital era, the IoT is considered one of the most robust technologies. However, attackers can effortlessly hack the IoT devices employed to generate botnets, and it is applied to present distributed denial of service (DDoS) attacks beside networks. The DDoS attack is the foremost attack on the system that causes the complete network to go down. Thus, average consumers may need help to get the services they need from the server. The compromised or attackers IoT devices want to be perceived well in the system. So, presently, Deep Learning (DL) plays a prominent part in forecasting end-users' behaviour by extracting features and identifying the adversary in the network. This paper proposes a Synergistic Swarm Optimization and Differential Evolution with Graph Convolutional Network Cyberattack Detection and Mitigation (SSODE-GCNDM) technique in the IoT environment. The main intention of the SSODE-GCNDM method is to recognize the presence of DDoS attack behaviour in IoT platforms. Primarily, the SSODE-GCNDM technique utilizes Z-score normalization to scale the input data into a uniform format. The presented SSODE-GCNDM approach utilizes synergistic swarm optimization with a differential evolution (SSO-DE) approach for the feature selection. Moreover, the graph convolutional network (GCN) method recognizes and mitigates attacks. Finally, the presented SSODE-GCNDM technique implements the northern goshawk optimization (NGO) method to fine-tune the hyperparameters involved in the GCN method. An extensive range of experimentation analyses occur, and the outcomes are observed using numerous features. The experimental validation of the SSODE-GCNDM technique portrayed a superior accuracy value of 99.62% compared to existing approaches.

[1]Department of Electrical Communication Engineering, Vignan Institute of Information Technology, Visakhapatnam, India. [2]Department of Information Technology (IT), VR Siddhartha Engineering College (A), Siddhartha Academy of Higher Education (Deemed to be University), Vijayawada, India. [3]Department of Computer Engineering, College of Computer Engineering & Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia. [4]Department of Information Technology, Chaitanya Bharathi Institute of Technology, Hyderabad, India. [5]Department of Electrical and Computer Engineering, College of Engineering and Information Technology, Ajman University, Ajman, United Arab Emirates. [6]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia. [7]Computer Science Department, Faculty of Computers and Information, South Valley University, Qena 83523, Egypt. [8]Faculty of Industry and Energy Technology, New Assiut Technological University (N.A.T.U.), New Assiut City 71684, Egypt. ✉email: Hkalqahtani@pnu.edu.sa

Keywords Graph Convolutional Network, Internet of things, Synergistic Swarm optimization, Distributed denial of service, Northern Goshawk optimization, Deep learning

The industrialized achievement of the IoT presents various military and civilian applications for developing the connectivity of millions of novel smart devices. These millions of risky internet-connected smart devices cause a dangerous security risk in the existence of uncountable cyberattacks. These insecurely protected devices are the doorways for hackers' intrusion and cause problems with the industrialized achievement of IoT[1]. These IoT-prepared devices devise hotspots for attackers to initiate volumetric attacks in the system of Denial-of-Service (DoS), Distributed DoS (DDoS), spamming, click fraud, etc. Among these cyberattacks, DDoS is the most well-known attack created with the help of botnets equipped with unprotected IoT devices[2]. DDoS attacks are often undergone owing to the development of botnets that affect millions of IoT devices. DDoS security attacks constantly threaten organizations and individual and company service providers. A DDoS attack utilizes various computers to unveil the distributed attack against one or more targets. The dispersed nature of the attack upsurges its actual ability and is very hard to identify[3]. Figure 1exemplifies the general structure of DDoS attacks in IoT platforms. With the developments of cloud computing (CC), Artificial Intelligence (AI), and IoT, attackers could launch huge-scale DDoS attacks at a lower cost. It is very challenging to identify and protect DDoS attacks. In many cases, DDoS network traffic is comparable to the usual one[4]. Thus, identifying and detecting DDoS from massive network traffic is challenging. Many standard mechanisms to identify and inhibit DDoS include attack reaction, attack prevention, and attack detection. Network intrusion detection system (NIDS) has become an essential module of security creation[5].

It identifies unusual system utilization by observing and analyzing the behaviour of a system to identify the attack. There are dual kinds of NIDS, specifically, Anomaly-based NIDS and Signature-based NIDS. Signature-based recognition identifies attacks by gathering and identifying whether there is a particular signature or pattern of previous attacks in traffic. However, it could be more effective in DDoS attack recognition because attackers frequently change the methods and kinds of attacks. Therefore, it is challenging to identify the signature or pattern of an attack[6]. When a DDoS attack arises on a system, the related traffic will result in unusual system behaviour. Therefore, NIDS could attain the equivalent attacks. To overwhelm the limits of these dual techniques, hybrid solutions based on either Anomaly-based or Signature-based methods are presented[7]. Research has presented numerous methods for handling DDoS attacks. The common methods utilize multiple machine learning (ML) methods to conquer DDoS attacks. Furthermore, hybrid solutions that integrate the two or more ML methods are presented. ML models are measured to be a feasible method of identifying DDoS attacks. These methods study the patterns behind attacks to identify them before network resources become inaccessible[8]. Current security methods use ML and other detection methods containing host-based IDS (HIDS) and IDS to respond to intricate cyber-attacks like DDoS attacks efficiently. The rapid proliferation of smart devices in diverse sectors has created unprecedented opportunities for innovation, but it also exposes critical vulnerabilities in network security[9]. As these interconnected devices become integral to daily operations, the potential for cyber threats, specifically DDoS attacks, intensifies. These attacks can disrupt services and compromise sensitive data, resulting in substantial financial and operational losses. Therefore, enhancing detection and mitigation strategies for such threats is crucial to safeguard the integrity of IoT ecosystems. Addressing these threats protects organizations and fosters trust in the ongoing adoption of smart technologies[10].

This paper proposes a Synergistic Swarm Optimization and Differential Evolution with Graph Convolutional Network Cyberattack Detection and Mitigation (SSODE-GCNDM) technique in the IoT environment. The main intention of the SSODE-GCNDM method is to recognize the presence of DDoS attack behaviour in IoT platforms. Primarily, the SSODE-GCNDM technique utilizes Z-score normalization to scale the input data into a uniform format. The presented SSODE-GCNDM approach utilizes synergistic swarm optimization with a differential evolution (SSO-DE) approach for the feature selection. Moreover, the graph convolutional network (GCN) method recognizes and mitigates attacks. Finally, the presented SSODE-GCNDM technique implements the northern goshawk optimization (NGO) method to fine-tune the hyperparameters involved in the GCN method. An extensive range of experimentation analyses occur, and the outcomes are observed under numerous features. The major contribution of the SSODE-GCNDM technique is listed below.

- The SSODE-GCNDM model employs Z-score normalization to standardize input data, which improves the technique's performance and stability. This approach allows for improved comparability among features, ultimately enhancing the overall efficiency of the model. Confirming that data is uniformly scaled eases more accurate training and evaluation.
- The SSODE-GCNDM technique utilizes the SSO-DE for efficient feature selection, substantially improving the chosen features' relevance. This methodology allows the model to concentrate on the most impactful data, enhancing its predictive accuracy. Employing the merits of both optimization methods effectively streamlines the feature selection process.
- The SSODE-GCNDM method effectively utilizes the GCN model to detect and reduce potential attacks, integrating the merits of graph-based learning. This enables the model to capture intrinsic relationships within the data, resulting in enhanced detection accuracy. By employing GCN, the technique improves its capability to detect patterns indicative of attacks, thereby strengthening overall safety measures.
- The SSODE-GCNDM technique implements the NGO method to fine-tune hyperparameters in the GCN, resulting in improved model performance and precision. This optimization method assists in systematically exploring the hyperparameter space, resulting in more effective learning results. By enhancing the tuning process, the technique substantially improves the capability of the GCN model to handle complex attack scenarios.

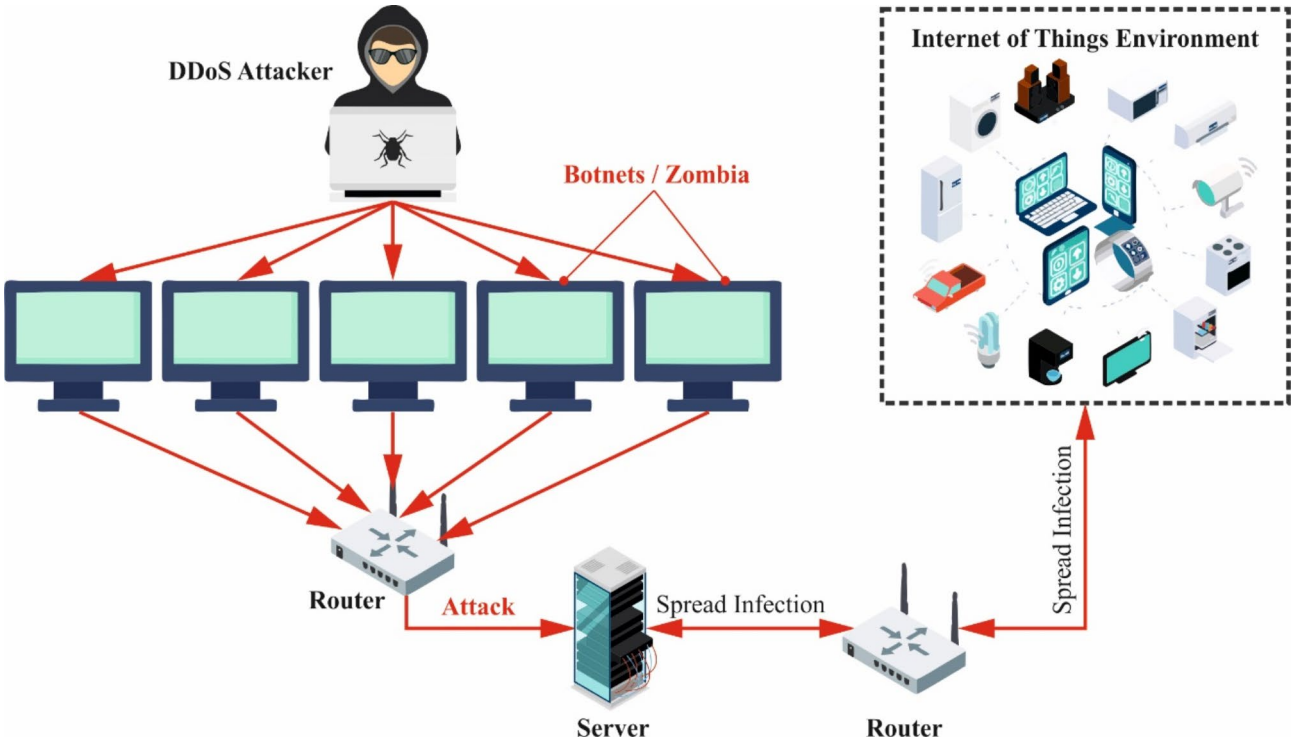

Fig. 1. General structure of DDoS attack in IoT.

- Incorporating SSO-DE for feature selection and NGO for hyperparameter tuning within a GCN framework underscores a novel and cohesive strategy for improving attack detection accuracy. This novel integration employs the merits of diverse optimization techniques, confirming both relevant feature detection and optimal model performance. By synergizing these methods, the approach enhances detection rates and sets a new standard for tackling complex security threats in network data analysis.

Review of literature

Sanlı[11] proposes a novel approach for mitigating and detecting DoS attacks in IoT systems. The presented technique is executed on an FPGA-based platform and tested for performance against various DoS attacks. Abid et al.[12]present a new technique for identifying and classifying DDoS attacks, which is enhanced significantly for this atmosphere. As part of the method, the author incorporates CNNs and LSTM methods into a multi-level deep neural network (DNN) model. With this hybrid structure, intricate temporal and spatial forms are spontaneously extracted from raw network traffic data to enable the widespread study and precise recognition of DDoS attacks. Kumar and Kumar Keshri[13] developed a smart GT-AS numerical method to maximize the DDoS attack mitigation efficiency. Furthermore, this tactic could intensely develop the five parameters: memory, intruder, hybrid, and energy channel. These could attain a strong security position against DDoS attacks from the recently devised IoT. Subsequently, the RB method is advanced to categorize the nodes into dual classes, such as malicious and trusted. Furthermore, the presented methods analyze how defence efficiency and energy consumption interrelate while estimating the adaptable security methods. Nisa et al.[14]propose a new method named TwophaseVerification for Attack Recognition, which aims to improve SDN security by mitigating DoS attacks. The method also contains the execution of packet filtration and ML classifier methods that are consequently monitored by the pursued limit of malicious network traffic. Rather than entirely disabling the host, the prominence reclines on averting dangerous communication. SVM and K-NN methods are used for effectual recognition on the CICDoS 2017 dataset. The method has been used in an atmosphere intended for threat recognition in SDN. Kavitha and Ramalakshmi[15] propose an effectual DDoS attack recognition and inhibition methodology utilizing ML methods. The study analyses the SDN's performance in IoT networks, integrating a massive group of computation devices which utilize multi-controllers.

Musa et al.[16] proposed tackling the intrinsic security susceptibilities of SDN atmospheres and emerging automatic methods for identifying and mitigating system attacks. Traditional network measuring methods have been restricted in the context of SDNs, and the goal of the presented DL and ML methods is to overcome these restrictions by offering more precise and effective mitigation and detection of DDoS attacks. This study aims to provide a complete analysis of associated studies in SDN anomaly detection current developments, classified into dual classes by DLand ML techniques. Aslam et al.[17] present an AMLSDM method. The presented AMLSDM method advances an SDN-enabled security mechanism for IoT devices with the help of an adaptable ML classifier method to attain the effective mitigation and recognition of DDoS attacks. The proposed structure uses ML techniques in an adaptable multi-layered feed-forwarding system to effectively recognize DDoS

attacks by inspecting the static features of the studied network traffic. Ahmim et al.[18] presented method goals to identify all DDoS attacks with their particular subgroup. This hybrid method integrates the various categories of DL methods, containing CNNs, LSTM, Deep AE, and DNNs. The presented method is composed of dual vital levels. The initial one comprises various equivalent sub-NN trained with particular methods. The next level utilizes the unmoving initial output integrated with the first data as input. Al Hwaitat and Fakhouri et al.[19]propose a novel Multi-Layer Perceptron (MLP) trainer that utilizes evolutionary computation methods. Benlloch-Caballero, Wang, and Calero[20] present a new cognitive closed-loop system to present distributed dual-layer self-protection capabilities to battle against DDoS attacks. Huang et al.[21]propose BDE-IDS, a bidirectional differential evolution-based system for unknown cyberattack detection. This work presents an intelligent Game Theory-based Adaptive Security (GT-AS) model to enhance DDoS attack mitigation. Sureshkumar, Venkatesan, and Santhosh[22] introduce a technique by using Density Peak Clustering Algorithms (DPCAs) to partition training sets for size and imbalance reduction.

Anoop et al.[23]present an Optimized Graph Transformer with a Molecule Attention Network (OGTMAN), which incorporates Secure Multi-party Computation (SMC) and differential privacy for enhanced security. The model utilizes min-max normalization, N-Tuple Contrastive Learning for feature extraction, and optimized feature selection using chi-square statistics. Al-Dunainawi, Al-Kaseem, and Al-Raweshidy[24]introduce an optimized model by using Mininet, Ryu controller, and a 1D-Convolutional Neural Network (1D-CNN) to detect and reduce DDoS attacks in SDN environments. Hekmati and Krishnamachari[25] introduce a robust solution by utilizing the capabilities of GCN. The study also presents a detection mechanism capable of operating efficiently even in lossy network environments. Various graph topologies are introduced for modelling IoT networks and evaluating them to detect tunable futuristic DDoS attacks. Ali et al.[26] present a reactive recovery strategy for link failures using a TOPSIS module in an SDN controller to choose alternative paths based on multiple criteria. A DDoS detection and mitigation mechanism are also presented by employing blockchain (BC) and ML in SD-IoT. Rizvi et al.[27]propose an innovative and highly efficient approach that integrates diverse classification models comprising Random Forest (RF), Decision Tree (DT), Gradient Boosting, Linear SVM, Logistics, K-nearest neighbours (KNN), and AdaBoost for DDoS attack detection. Kostas, Just, and Lones[28] present a model for IoT attack detection. This method uses isolated train and test datasets, evaluates various ML models, and applies explainable AI to identify key detection features. Sadhwani et al.[29] present a scalable system that integrates ML and DL methods with optimized data processing to secure IoT devices against DDoS attacks. Aswad et al.[30] propose integrating three deep DL methods, namely recurrent neural network (RNN), LSTM-RNN, and CNN, to build a bidirectional CNN-BiLSTM DDoS detection model. Pawar et al.[31]investigate attacks in IoT and SDN environments, exploring the incorporation of BC for enhanced security. The model also utilizes Attention-based Convolutional LSTM (At-C-L) to improve detection capabilities. Oladele and Jimoh[32] analyze six DNN models, exhibiting that LSTM outperforms the other algorithms.

Ma et al.[33] provide a comprehensive survey on DDoS defense solutions in Multi-access Edge Computing (MEC) networks, exploring security threats, attack types, and current defense strategies. Vincent et al.[34] proposes a GCN framework to detect FDI attacks by analyzing power network topology and fluctuating state estimations. Yang et al.[35] propose STMIR, a secure and traceable multikey image retrieval system utilizing privacy-preserving Mahalanobis distance comparison, CNN-based feature extraction, and encrypted watermarking for secure retrieval and user tracking. Feng et al.[36] introduces a learning-based DDoS detection approach using an enhanced k-nearest neighbors (KNN) approach with a k-dimensional (KD)-tree for faster detection and fine-grained classification of DDoS sources by IP risk level. Chen et al.[37] propose an efficient and secure content-based image retrieval scheme for Cloud-assisted IoT, utilizing lattice-based homomorphic encryption, CKKS batch processing, and Private Information Retrieval to improve privacy and reduce computational overhead, with proven security and efficiency. Lo et al.[38] proposes XG-BoT, an explainable deep GNN for botnet node detection. It also utilizes a reversible residual connection and graph isomorphism network for accurate detection and includes an explainer for automatic forensics, highlighting suspicious network flows and botnet nodes. Ma et al.[39] presents a DDoS defense using a Graph Convolutional Neural Network (GCNN) for accurate attack detection and dynamic whitelist-based reduction with fast traffic rerouting to ensure service continuity. Li et al.[40] presents AT-GCN, a DDoS attack path tracing system using a knowledge base and GCN, with a Tracing-Sample algorithm and dynamic traceability algorithm recommendations based on user needs. Qian et al.[41]proposes a distributed botnet detection methodology by using graph partitioning and GCNs, with METIS for efficient traffic division and diagonal enhancement to ensure accurate detection. Jemal, Cheikhrouhou, and Haddar[42] improves IoT security by using CNNs to detect and counter DDoS and DoS attacks. Abinesh et al.[43] introduces a Deep GCNN for effectually botnet detection, particularly for Mirai and Bashlite attacks, which are similar to DDoS attacks.

Lee and Han[44]propose a causal attention graph convolutional network (CAGCN) that utilizes node and neighbor attention to reduce bias from attacks, ensuring robust performance even under stronger attacks. Sanap and Aher[45] proposes a DCNN-based SVMAK for DDoS detection and mitigation, utilizing WSMOTE to address data imbalance and HGSO for feature selection. Khalid Alkahtani et al.[46] presents an Optimal GCNN based Ransomware Detection (OGCNN-RWD) technique for IoT environments, using learning enthusiasm for teaching learning-based optimization (LETLBO) for feature selection and the GCNN model with hyperparameters optimized by harmony search algorithm (HSA). Saunders et al.[47] presents the design of a GCN-based DDoS detection system. Kisanga et al.[48] introduces an Activity and Event Network (AEN)-based supervised Graph Convolutional Network (GCN) model. Altaf et al.[49]introduces a GGCN framework for botnet detection in IoT networks, employing time-stamped multi-edge graphs and a gated graph model to capture temporal patterns in network traffic. Alhayani and Murphy[50]presents an efficient ML-based DDoS detection approach by employing chi-square for feature selection to ensure efficiency with minimal input features. Thota, Prathibhavani, and Venugopal[51] present a new hybrid approach, called GNN-WGAN, to efficiently detect bots

in IoT-based smart city networks by integrating Graph Neural Network (GNN) and Wasserstein Generative Adversarial Network (WGAN). Barsellotti et al.[52] introduces a two-level hierarchical graph representation and GNN method to integrate traffic- and flow-level relationships, maximizing information from the traffic structure without needing stateful features.

The existing studies for mitigating and detecting DDoS attacks portray diverse limitations. One model employs an FPGA-based platform, which may deter scalability and adaptability across several IoT environments, concentrating primarily on DoS attacks while neglecting other potential threats. A hybrid model incorporating CNNs and LSTMs may be computationally intensive, impacting real-time detection capabilities. Moreover, reliance on a limited set of parameters might oversimplify mitigation strategies, and specific methods could face difficulty with high volumes of malevolent traffic, resulting in false negatives. The complexity of some hybrid models may result in longer training times and extensive resource requirements. Additionally, conventional measurement methods may only effectually address some security vulnerabilities in dynamic conditions, and the efficiency of specific models could diminish when faced with growing DDoS attack strategies. Lastly, while some approaches underscore multi-criteria decision-making, they risk oversimplifying intrinsic scenarios, potentially resulting in suboptimal outcomes. Despite enhancements in DDoS attack detection and mitigation, crucial research gaps remain in the adaptability and scalability of these methods across various IoT environments. Many existing approaches concentrate on specific attack vectors or depend on limited parameters, which can oversimplify complex threat landscapes. Additionally, there is a need for more robust models that effectually balance computational efficiency with high detection accuracy in real-time scenarios. Enhanced integration of explainable AI techniques could also improve trust and transparency in detection mechanisms.

Proposed Method

This manuscript proposes the SSODE-GCNDM methodology in the IoT environment. The main intention of the SSODE-GCNDM method is to recognize the presence of DDoS attack behaviour in IoT platforms. It encompasses four phases: data normalization, feature selection, classification, and parameter tuning, as demonstrated in Fig. 2.

Phase I: Z-score normalization

Primarily, the SSODE-GCNDM technique involves Z-score normalization to scale the input data into a uniform format[53]. The Z-score normalization is a powerful technique for standardizing data, as it converts features to have a mean of zero and a standard deviation (SD) of one. This method is specifically beneficial when dealing with datasets that exhibit varying scales, confirming that all features contribute equally to the model's performance. By reducing the influence of outliers, Z-score normalization improves optimization algorithms' stability and convergence speed. Compared to other normalization methods, namely min-max scaling, Z-score normalization is less sensitive to extreme values, making it a more robust choice in various applications. Its capability to facilitate better interpretability of results also assists in more precise insights during model evaluation. Overall,

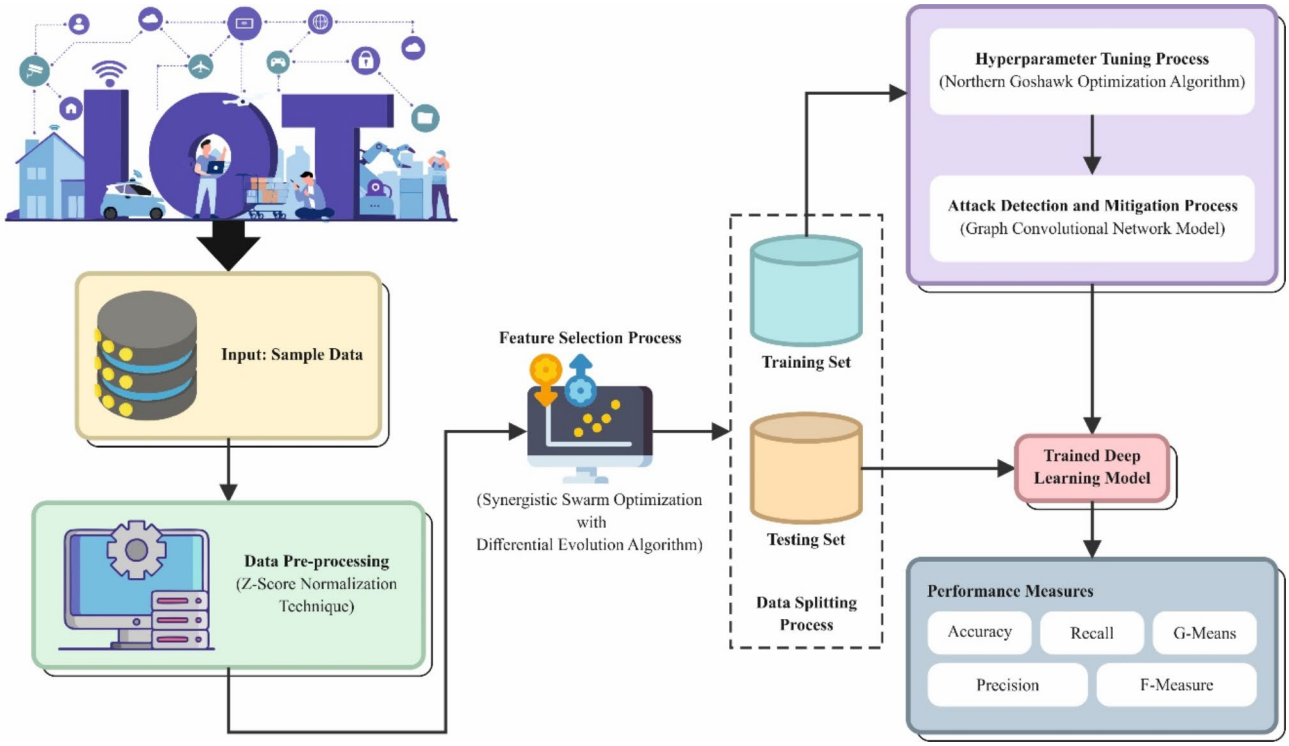

Fig. 2. Overall process of SSODE-GCNDM technique.

its efficiency in preparing data for complex models makes it an excellent choice in scenarios needing precision and reliability.

Z-score normalization is an arithmetical model employed to regulate data by converting it into a mutual scale, usually with a mean of 0 and an SD of 1. Z-score normalization aids in equating and examining network traffic patterns by removing the effects of opposing units and scales. This procedure includes deducting the mean of the data and isolating it by its SD, permitting a more uniform depiction of traffic features. Using Z-score normalization, anomalous behaviour indicative of DDoS attacks is more easily identified as deviations from the norm. This technique enhances the effectiveness of anomaly detection algorithms by providing a consistent basis for comparison across diverse IoT devices and network conditions. Consequently, it aids in improving the overall accuracy and efficiency of DDoS recognition and mitigation strategies.

Phase II: feature selection

For the feature selection process, the presented SSODE-GCNDM technique utilizes the SSO-DE approach[54]. This method presents a unique merit by integrating the strengths of both optimization models. The SSO model effectually explores the solution space through collaborative swarm intelligence, endorsing diversity and adaptability, while Differential Evolution (DE) improves convergence speed and robustness in finding optimal feature subsets. This hybrid approach is specifically useful for high-dimensional datasets, where conventional techniques may need to assist computational efficiency and overfitting difficulty. Compared to other feature selection methods, SSO-DE balances exploration and exploitation, resulting in more relevant and compact feature sets. Its capacity to dynamically adjust to the data landscape confirms a more tailored feature selection process, ultimately enhancing the model's performance. This synergy enhances predictive accuracy and simplifies model interpretation and implementation. Figure 3 illustrates the structure of the SSO-DE model.

Natural swarms' synergistic and cooperative behaviour stimulates the advanced optimization approach SSOA. This model utilizes an agent swarm that collaborates to solve complex issues successfully. The key process of the suggested SSOA approach is presented below. The optimization process begins with selecting candidate solutions in Eq. (1).

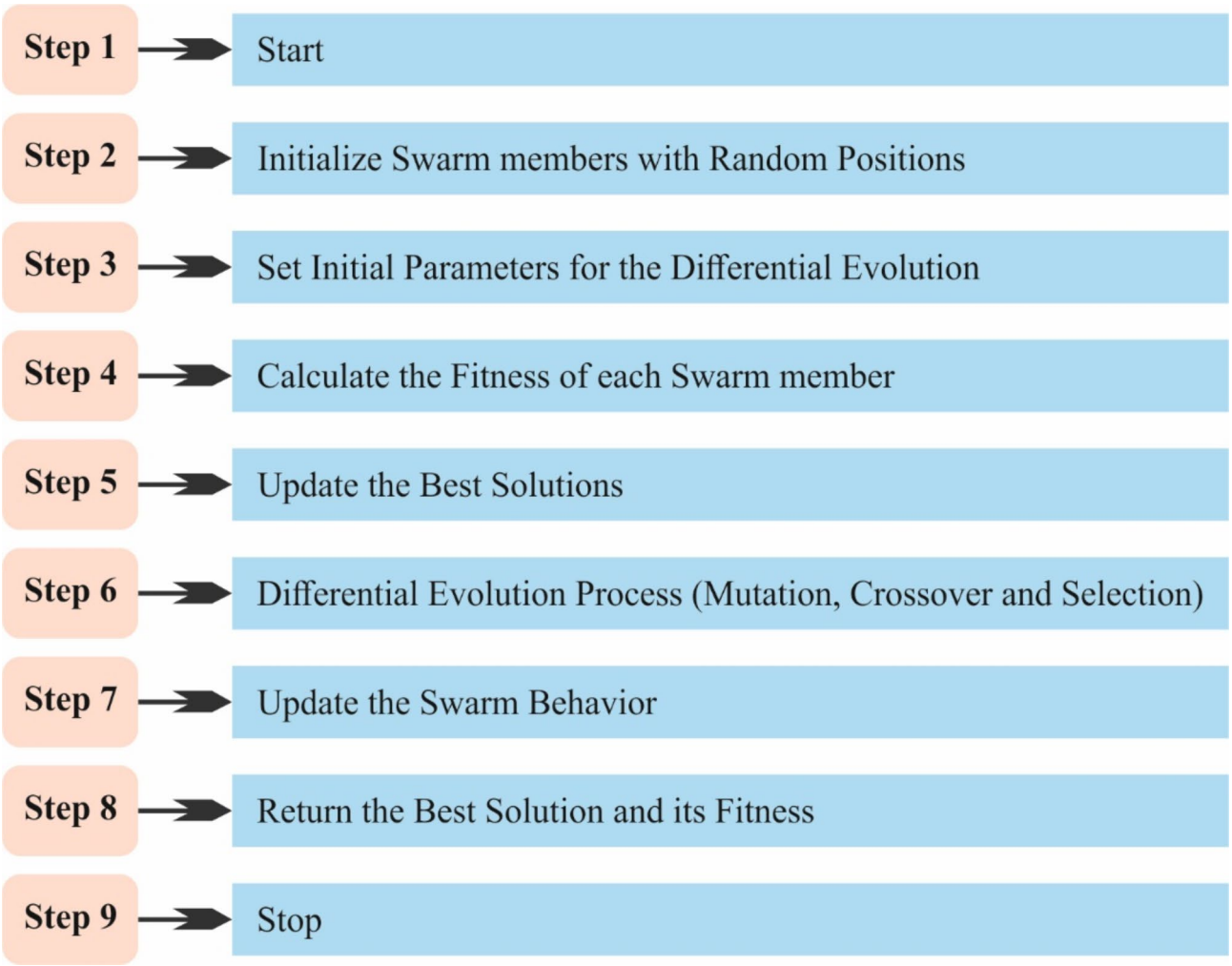

Fig. 3. Structure of the SSO-DE model.

$$X = rand\,(N,\ Dim) * (UB - LB) + LB \tag{1}$$

Equation (1) makes a matrix X of size $(NxDim)$ with randomly generated values inside known ranges. The framework of these matrices is assumed in Eq. (2)

$$X = \begin{bmatrix} x_{1,1} & \cdots & x_{1,Dim} \\ \vdots & \ddots & \vdots \\ x_{N,1} & \cdots & x_{N,Dim} \end{bmatrix} \tag{2}$$

whereas N characterizes solutions or particles, Dim symbolizes variables or dimensions of the known problem, $and\,UB$ and LB represent upper and lower limit vectors for every problem space dimension.

The candidate solutions (X) are upgraded using the Eq. (3).

$$Xnew\ (i,j) = X\,(i,j) + v\,(i,j) \tag{3}$$

Now, $Xnew(i,\ j)$ signifies the original optimization position j of the ith candidate solution, $X\,(i,\ j)$ stands for present position j of the ith candidate solution, $v\,(i,\ j)$ characterizes the position j of the ith value of the candidate solution.

Additionally, the velocity updated equation introduces a dynamic attraction equation that impacts the particles' movement near more favourable areas of the search space. These equations are calculated to adaptably guide the particles depending on the global and local attraction of the positions.

$$v_{new}\,(i,j) = IWV + PBC + GBC + DAC + ANIC + MDC \tag{4}$$

The subsequent equations design the vnew(i, j) values. The inertia weight value (IWV) is computed in the following:

$$IWV = w\,(t) * v\,(i,j) \tag{5}$$

Here, w represents an adaptable method for controlling the balance between dynamical exploitation and exploration using the inertia weight parameter (w).

The adaptable neighbourhood communication equation encourages a concentrated search space exploration by providing more weight to particles with greater fitness, permitting the swarm to meet more powerfully. Present an equation that dynamically adjusts the interaction power between particles depending on their fitness values. This equation allows particles with superior fitness to have a robust inspiration for the movement of their neighbours. The inertia weight is upgraded at every iteration via an adaptable equation:

$$w\,(t+1) = w\,(t) * (1 - exp\,(-k*t)) \tag{6}$$

Now, k denotes the constant that regulates the decline in the inertia weight rate, and t symbolizes the present iteration. This model slowly moves from exploration to exploitation by decreasing the inertia weight on time, encouraging convergence, and fine-tuning near the optimum solution. The personal best coefficient (PBC) is computed in the following:

$$PBC = r1 * (eps * rand\ (pbest) - X_i) \tag{7}$$

Here, $r1$ represents a value of random, eps provides a smaller value, $rand\,(pbest)$ denotes a random solution from the present candidate solutions, and X_i offerings the $i\,th$ solution number. The global best coefficient (GBC) is computed in the following:

$$GBC = r2 * gbest_t - X_i \tag{8}$$

Whereas $r2$ denotes random value, $gbest_t$ signifies the globally best solution (at several iterations t), and X_i gives the number of solutions. Consists of a diverse conservation equation that inspires the exploration of varied areas inside the search space. The dynamic attraction coefficient (DAC) is computed in the following:

$$DAC = r3 * \frac{attract_i}{c1} - X_i \tag{9}$$

Here, $r3$ represents randomized value, $attract_i$ characterizes the position with the greater local attraction value inside the neighbourhood of the particle i, cl denotes the added acceleration coefficient for the dynamically attracted word, and X_i provides the number of solutions i. The dynamically attracted word leader's particles near high attracted positions, endorsing fast convergence near optimum solutions. The adaptive neighbourhood interaction coefficient (ANIC) is computed in the following:

$$ANIC = r4 * rand\,(bestf) - bestf_i \tag{10}$$

Now, $r4$ signifies a randomly generated value, $rand\,(bestf)$ denotes a randomly selected fitness value from the present fitness solutions, and $bestf_i$ represents the fitness value of the ith solution. The diversity maintenance coefficient (DMC) is measured as below:

$$DMC = r5 * \frac{diversity_i}{c2} - X_i \tag{11}$$

Whereas $r5$ stands for randomly formed value, $c2$ is an added accelerated coefficient for the term of diversity. $diversity_i$ characterizes a position inside the swarm that increases the diversity during the ith particle neighbourhood.

DE Model.

The DE model presented by Storn and Price is an efficient and robust search model intended to challenge complicated, constant, non-linear functions[55]. The Conventional DE (method begins by initializing a population of N individuals signified as vector $\overrightarrow{X}_i$, whereas $\overrightarrow{X}_{\mathrm{i}} = (X_{i1}, X_{i2}, X_{i3}, \ldots, X_{in}), i = 1,2,3,\ldots,N$, and n represent the dimension of the problem. The DEA technique has integrated three main operators: crossover, selection, and mutation. The mutation and crossover operators are used to give new candidate vectors. Simultaneously, a selection approach has been applied to control the survival of both the parent and the offspring in the following generation.

Stage of mutation

An individual with genetic mutations has been characterized based on Eq. (12) whereas $\overrightarrow{V}_{\mathrm{i}} = (v_{i1}, v_{i2}, v_{i3}, v_{in})$ and is made using a mutation operator. Numerous mutation models are recognized in this work. A unique often applied operator is 'DE/best/1', which is described as:

$$\overrightarrow{V}_{\mathrm{i}}(t) = \overrightarrow{X}^{*}(t) + F\left(\overrightarrow{X}_{\alpha}(t) - \overrightarrow{V}_{\beta}(t)\right) \tag{12}$$

Where t characterizes the present iteration, $\overrightarrow{X}^{*}(t)$ symbolizes the finest individual with the lower $f\left(\overrightarrow{X}\right)^{*}$. Now, α and β are two indices selected at random between the range $[1, N]$, whereas a, b, and i are all distinct from one another $\alpha \neq \beta \neq i \in 1 \ldots, N)$. In addition, $F \in [0,1]$ characterizes a mutation scaling factor manipulating the discrepancy variation among two individuals.

Stage of crossover

The crossover parameter has been applied to every mutation individual, and it is related to a targeted individual $\overrightarrow{X}_i$ to offer an experimental vector, $\overrightarrow{U}_{\mathrm{i}} = (u_{i1}, u_{i2}, u_{i3}, \ldots, u_{i,n})$. Binomial and exponential crossovers are regularly used crossover tactics. The binomial crossover has been stated based on Eq. (13):

$$u_{i,j}(t) = \begin{cases} v_{i,j}(t), & if\ r_j \leq CR\ or\ j = R; \\ xi,j(t), & Otherwise \end{cases} \tag{13}$$

The index R symbolizes a dimensionally selected random number from the set $1, 2, \ldots, n$. This is completed to promise that at the smallest one dimension from $\overrightarrow{V}_{\mathrm{i}}(\mathrm{t})$, current is current in the individual $\overrightarrow{U}_i$, which varies from its targeted vector, $\overrightarrow{V}_i$. The crossover rate (CR) represents the value ranging between 0 and 1, and $r_j \in [0,1]$ stands for a randomly formed number distributed uniformly among 0 and 1.

Stage of selection

A one-to-one greedier selection has been applied in DE to regulate when the experimental individual $\overrightarrow{U}_{\mathrm{i}}(\mathrm{t})$ will be incorporated into the targeted population for the following generation. The one-to-one selection approach controls by defining the survival of the more suitable person among the experimental individual $\overrightarrow{U}_{\mathrm{i}}(\mathrm{t})$ and its targeted counterpart $\overrightarrow{X}_i$. The expression for minimization problems has been based on Eq. (14):

$$\overrightarrow{X}_{\mathrm{i}}(t+1) = \begin{cases} \overrightarrow{U}_{\mathrm{i}}(t), & if\ f\left(\overrightarrow{U}_{\mathrm{i}}(t)\right) \leq f\left(\overrightarrow{X}_{\mathrm{i}}(t)\right) \\ \overrightarrow{X}_{\mathrm{i}}(t), & otherwise \end{cases} \tag{14}$$

Here, f denotes the function of the objective. The process mentioned above is iterated till an end requirement is attained.

The SSOA integration with DE influences the balancing powers of both models to improve optimization performance. SSO outshines exploring the searching space using the cooperative interaction and behaviour of swarm agents, which allows efficient exploration of different areas. DE, alternatively, concentrates on developing these areas over crossover operations and differential mutation. SSO is initially applied to recognize and encourage search space regions during this hybrid model. After identifying this region, DE has been used to fine-tune the solutions. This grouping increases the exploration or exploitation stages, leading to a more effectual searching method and improved optimizer outcomes. The incorporation is mathematically defined in the following:

Updating the position of all agents in the swarm using:

$$x_i(t+1) = x_i(t) + \alpha \cdot (x_{best}(t) - x_i(t)) + \beta \cdot (x_j(t) - x_k(t)), \tag{15}$$

Here, $x_i\,(t)$ represents the position of the $i-th$ agent at time $t, x_{best}\,(t)$ denotes the best position founded by the swarm, $x_j\,(t)$ and $x_k\,(t)$ are positions of agents selected at random, and α and β are coefficients adjusting the impact of the best agent and the changes among other agents.

Afterwards, exploration of SSO, use DE for local refinement:

$$v_i = x_r1 + F\cdot\ (x_r2 - x_r3)\,, \tag{16}$$

Here, v_i represents the mutant vector for the $i-th$ individual, x_r1, x_r2, $and\, x_r3$ are individuals selected randomly from the population, and F represents a scaling factor. Create the experimental vector u_i using crossover and choose the best individuals for the following generation. These hybrid models associate the wide-ranging searching abilities of SSO with the accurate optimization algorithms of DE, resulting in an efficient and robust technique for composite optimizer difficulties.

In the SSO-DE method, the objectives are combined into a solitary objective formula such that a current weight classifies every objective's importance. In this study, a fitness function (FF) that incorporates both objectives of FS is utilized and shown in Eq. (17).

$$Fitness\,(X) = \alpha\ \cdot\ E\,(X) + \beta\ *\left(1 - \frac{|R|}{|N|}\right) \tag{17}$$

Whereas Fitness(X) signifies the fitness rate of subset $X, E\,(X)$ denotes the classification rate of error by utilizing the chosen features within the X subset. $|R|$ and $|N|$ are the counts of selected features and novel features within the dataset. Correspondingly, α and β are the weights of the classification error and the decrease ratio, $\alpha\ \in\ [0,1]$ and $\beta\ = (1-\alpha\,)$.

Phase III: attack detection using GCN technique

Moreover, the GCN technique recognizes and mitigates DDoS attacks[56]. This model for attack detection utilizes the ability to model complex relationships and dependencies in data, which is particularly advantageous in network security contexts. GCNs capture the structural data inherent in graph-structured data, allowing them to detect patterns and anomalies that may indicate potential attacks. Unlike conventional techniques that treat features independently, GCNs integrate the interconnections between data points, giving a richer understanding of the overall system. This capability enhances detection rates, mainly in scenarios with intricate attack patterns. Moreover, GCNs are adaptable to varying data types and can scale well with increasing data complexity. Their performance extracting meaningful insights from relational data makes GCNs a superior option for enhancing security measures in dynamic environments. Figure 4 depicts the architecture of the GCN model.

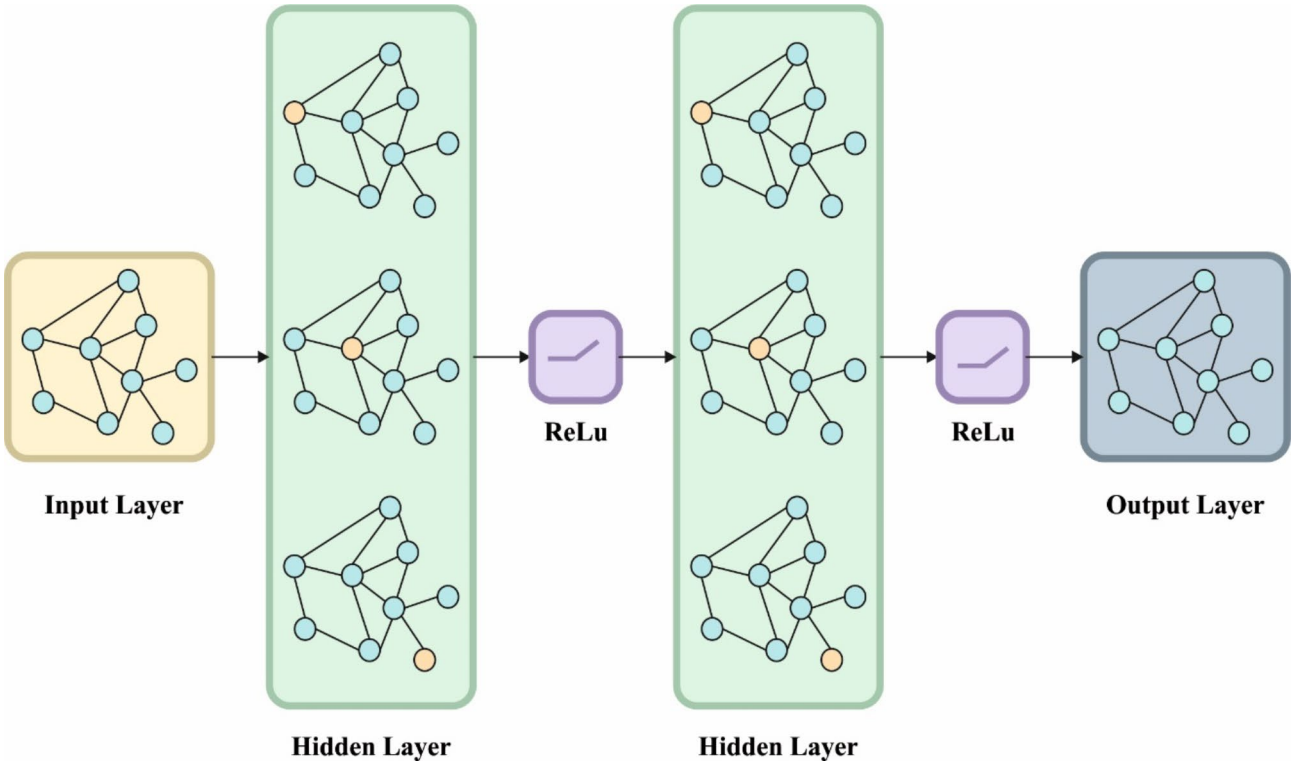

Fig. 4. Structure of GCN.

During these studies, layers of GCN were selected according to the graphical convolution operator. The operator was presented to extract features from molecular fingerprints. GCNs are notorious for their capacity to make node embeddings that take necessary structural information from the graph. This is mainly helpful in tasks requiring understanding objects' connections and relationships. GCNs use a convolution process similar to traditional CNNs to combine information from adjacent nodes but also slot in distanced information of the local area. The sharing of parameters enables the GCN scalability, for the parameters are shared uniformly through each node. The operator of GCN follows the layer-to-layer rule of propagation that is described as:

$$H^{(l+1)} = \sigma\left(\widetilde{D}^{-\frac{1}{2}}\ \widetilde{A}\ \widetilde{D}^{-\frac{1}{2}} H^{(l)} W^{(l)}\right) \tag{18}$$

Here, $H^{(l)}$ signifies the input graph by $l\ th$ layer, and $H^{(l+1)}$ symbolizes the output by $the\ l+1\ \underset{\sim}{\text{th}}$ layer. The matrix $\widetilde{A}= A + I_N$ is the adjacent matrix with additional self-loops to every node. The matrix $\widetilde{D}$ signifies a diagonal matrix delineated as $\widetilde{D}_{\text{ii}} = \Sigma_{\ j}\left(\widetilde{A}\right)$. The training matrix precise to the layer is denoted as $W^{(l)}$, and σ symbolizes the activation function implementation. Equation (18) is inspired by an initial-order estimate of training local spectral filters g_θ on graphs. A spectral convolution (meant as *) from the input graph $\widetilde{x}$ using a filter g_θ parametrized by θ within the Fourier domain is specified as:

$$g_\theta *x = U g_\theta\, U^{Tx} \tag{19}$$

Now, U symbolizes the eigenvectors matrix, with its eigenvalues signified as Λ, gained from $L = I_N - D^{-\frac{1}{2}} A D^{-\frac{1}{2}} = U \Lambda\, U$, whereas $D_{ii} = \sum_{\ j}(A)$ denotes the diagonal matrix. By stating g_θ for Λ function and estimating it over Chebyshev polynomials truncation equal to the K^{th} order, the L eigendecomposition is calculated, resulting in:

$$g_\theta *x \approx \sum_{k=0}^{K} \theta'_k T_k\left(\widetilde{L}\right) x \tag{20}$$

Here, θ' denotes the Chebyshev coefficients vector, and $T_k\left(\widetilde{L}\right)$ represents $the\ k^{th}$ Chebyshev polynomial utilized to $\widetilde{L}= \frac{2}{\lambda_{\max}} L - I_N$ with $\lambda_{\max}$ indicating the maximal matrix eigenvalue Λ.

Decreasing the parameter counts helps address streamlining and overfitting operations in each layer. By limiting the order of Chebyshev to $K = 1$ and estimating the $\lambda_{\max}$ value to 2 (assuming that neural network parameters regulate these scale changes in training), Eq. (20) facilitates:

$$g_\theta *x \approx\ \theta\ \left(I_N + D^{-\frac{1}{2}} A D^{-\frac{1}{2}}\right) x \tag{21}$$

Continual implementation of these operators can lead to numerical variabilities, producing both vanishing gradients and exploding, mainly in connection with DNN techniques. Renormalization habits have been suggested to address these problems. Over continuous pooling operation applications, information from a node is transmitted over progressively different areas. For example, with k_l concatenation layers of GCN, inspiration is extended to the k_l^{th}-order area near node i. Finally, the GCN layer output is served over an activation function σ to present non-linearity. Hence, the operation at every layer l contains the operator of GCN in Eq. (18) using the PReLU operator applied by the activation function:

$$f_a(y) = \begin{cases} y & if\ y \geq 0 \\ \beta\, y & if\ y < 0 \end{cases} \tag{22}$$

Phase IV: NGO-based parameter tuning

Finally, the presented SSODE-GCNDM model implements the NGO method to fine-tune the hyperparameters involved in the GCN method[57]. This method is an efficient parameter-tuning technique motivated by goshawks' hunting behaviours, enabling it to explore the solution space effectively. Its adaptive search mechanism is specifically beneficial for optimizing hyperparameters in complex models, resulting in improved performance and accuracy. The capability of the NGO model to balance exploration and exploitation assists in preventing premature convergence, a general problem in conventional optimization methods. Compared to other techniques, namely grid or random search, NGO presents a more systematic and intelligent approach, often needing fewer evaluations to attain optimal settings. This efficiency not only saves computational resources but also accelerates the tuning process. Moreover, NGOs can be easily integrated with diverse ML models, making it a versatile choice for diverse applications in model optimization. Its efficiency in attaining high-quality solutions distinguishes it from conventional tuning methods. Figure 5 demonstrates the structure of the NGO model.

Stimulated by the predatory behaviour of the northern goshawk, the NGO captures every northern goshawk as an individual of a population and extracts the predatory behaviour into 2 phases. The initial phase is to attack and explore prey that replicates the group behaviour by recognizing the location of the present best solution and inducing every individual to update their position over the optimal solution, demonstrating the global exploration abilities. The next phase represents the escaping behaviour of prey, implying the local exploitation abilities.

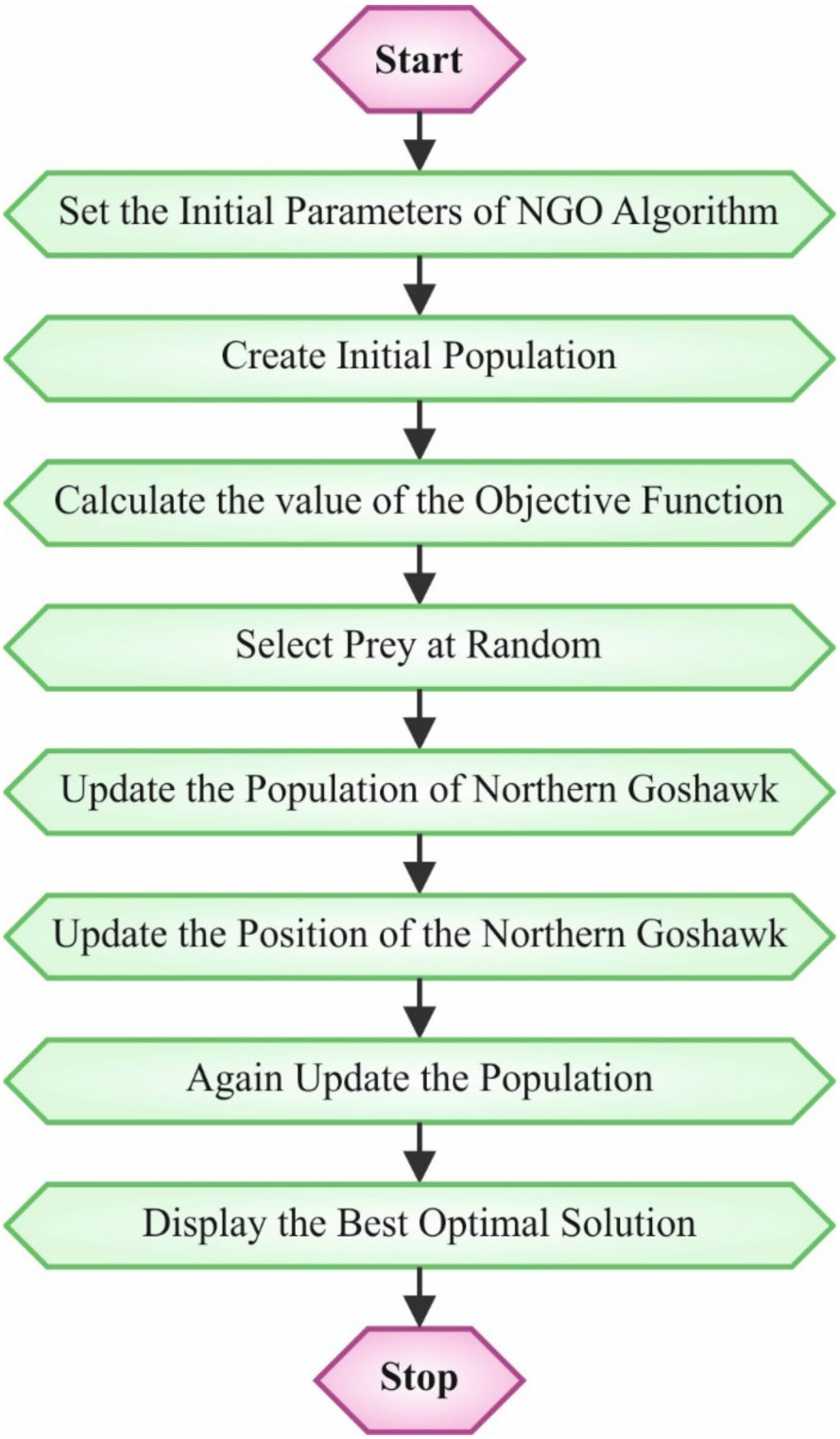

Fig. 5. Architecture of the NGO approach.

Initialization.

NGO believes every northern goshawk is an individual of a population that is a possible solution, searching for the finest value in the potential solution space by transferring. Similarly, in swarm intelligence algorithms (SIA), NGO makes initial populations by randomly generating earlier populations. During the mathematical approach, every individual symbolizes a D-dimensional vector, N individuals establish the complete population, and the population is an $N \times D$ matrix. The population's mathematical technique is depicted in the following equation.

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_i \\ \vdots \\ X_N \end{bmatrix}_{N\times M} = \begin{bmatrix} x_{1,1} & \cdots & x_{1,j} & \cdots & x_{1,M} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{i,1} & \cdots & x_{i,j} & \cdots & x_{i,M} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{i,1} & \cdots & x_{i,j} & \cdots & x_{i,M} \end{bmatrix}_{N\times M} \tag{23}$$

Now, the population N and the individual's position are characterized by X and X_i. Individually, $X_{i\ and\ j}$ represent the value of the j_{th} dimension, and M denotes individual counts and the larger dimension. The FF signifies the objective function.

Attack and Identification of Prey.

The prey attack and search is the primary phase of the NGO in every iteration, which pretends the optimal solution as prey and every individual presents the attack. During these phases, each individual recognizes the position of the present best solution and upgrades their position depending on these optimum solutions. The leading resolution is to allow the northern goshawk individual to more commonly hunt the possible solution space. Hence, a global search has been performed. Eqs. $(24)-(26)$ characterize the mathematical representation for the first stage.

$$P_i = X_Z \tag{24}$$

$$x_{i,j}^{new1} = \begin{cases} x_{i,j} + r\left(p_{i,j} - I * x_{i,j}\right), F_{p_i} < F_i \\ x_{i,j} + r\left(x_{i,j} - p_{i,j}\right), F_{p_i} \geq F_i \end{cases} \tag{25}$$

$$X_i = \begin{cases} x_i^{new1}, F_i^{new1} < F_i \\ X_i, F_i^{new1} \geq F_i \end{cases} \tag{26}$$

Here, $i = 1,2,\cdots,N$, I value is 1 or 2, and $r = rand\,(0,1)$. P_i denotes the candidate solution. F_{P_i} represents the value of an objective function. x_i^{new1} symbolizes the new position of the initial phase and $x_{i,j}^{new1}$ is its j_{th} dimension. F_i^{new1} characterizes the value of the objective function of the initial phase.

Operation of Escape and Chase.

The 2nd phase represents escaping and chasing prey, and the local exploitation is performed by mimicking the local actions of prey to affect the individual position of the northern goshawk. The position updating equation of the 2nd phase has been exposed in Eqs. $(27)-(28)$:

$$x_{i,j}^{new2} = x_{i,j} + R\,(2r-1)\,x_{i,j} \tag{27}$$

$$X_i = \begin{cases} x_i^{new2}, F_i^{new2} < F_i \\ X_i, F_i^{new2} \geq F_i \end{cases} Z = 1,2,\cdots I,\cdots N \tag{28}$$

Now, x_i^{new2} stands for an original position in the 2nd phase and $x_{i.j}^{new2}$ represents its value in $the\ j_{th}$ dimension. F_i^{new2} characterizes the value of the objective function of 2nd phase. R denotes the searching radius. The R expression is shown below

$$R = 0.02\left(1 - \frac{t}{T}\right) \tag{29}$$

whereas t signifies the number of iterations, T indicates the maximum number. R should reduce as the number of iterations upsurges, demonstrating that the searching radius of the NGO bonds in the advanced iteration phases, thus improving the model's local exploitation proficiency. These methods have been essential to NGOs' achieving better optimization accuracy than others. Every iteration of the NGO process includes these two stages. Upon accomplishment of the maximal iteration boundary, the algorithm ends.

Fitness selection is a substantial feature that induces the performance of the NGO method. The hyperparameter choice process includes the encoding methodology to assess the efficiency of the candidate results. In this study, the NGO method studies precision as the primary criterion for designing the FF.

$$Fitness = \max\,(P) \tag{30}$$

$$P = \frac{TP}{TP + FP} \tag{31}$$

TP implies the true positive, and FP signifies the false positive value.

Performance validation

The simulation validation of the SSODE-GCNDM technique is studied utilizing the dataset[58]. The dataset contains 1600 samples under dual-class labels, as represented in Table 1. The ten features are Represents the total duration of the captured packets (tot_dur), Placeholder for nanoseconds part of the duration (dur_nse), Time difference between consecutive packets (dt), Duration between consecutive packets (dur), received kilobits per second (rx_kbps), Determines the packet protocol (Protocol), Transmitted kilobits per second (tx_kbps), Rate of packet arrival per second (pktrate), Total kilobits per second (tot_kbps), and Port number (port_no). But, only six features are selected: Time difference between consecutive packets (dt), Rate of packet arrival per second

Class	No. of Samples
DDoS Attack	1000
Normal	600
Total Samples	**1600**

Table 1. Details of dataset.

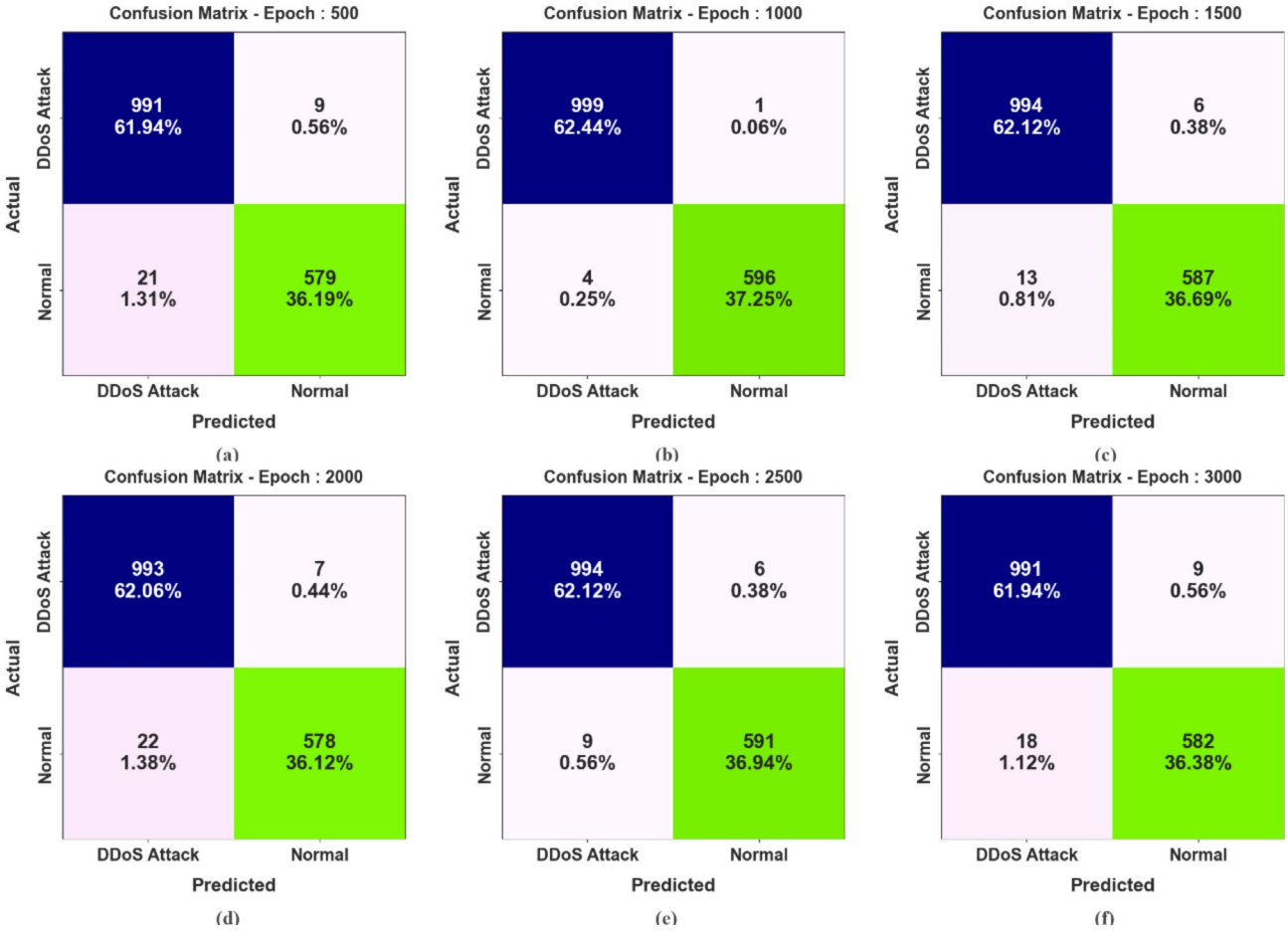

Fig. 6. Confusion matrices of SSODE-GCNDM technique (a-f) Epochs 500–3000.

(pktrae), Total kilobits per second (tot_kbps), Duration between consecutive packets (dur), Transmitted kilobits per second (tx_kbps), and received kilobits per second (rx_kbps).

The suggested technique is simulated using the Python 3.6.5 tool on a PC with an i5-8600k, 250GB SSD, GeForce 1050Ti 4GB, 16GB RAM, and 1 TB HDD. The parameter settings are learning rate: 0.01, activation: ReLU, epoch count 50, dropout: 0.5, and batch size: 5.

Figure 6 reports a set of confusion matrices produced by the SSODE-GCNDM method on different epochs. On 500 epochs, the SSODE-GCNDM model has identified 991 samples as DDoS attacks and 579 samples as normal. In addition, on 1000 epochs, the SSODE-GCNDM method has identified 999 samples as DDoS attacks and 596 samples as normal. Followed by, on 1500 epochs, the SSODE-GCNDM model has identified 994 samples into DDoS attack and 587 samples as normal. Finally, on 2500 epochs, the SSODE-GCNDM technique has approached 994 samples into DDoS attack and 591 samples into normal.

The DDoS recognition outcomes of the SSODE-GCNDM method are determined under distinct epochs in Table 2; Fig. 7. The table values state that the SSODE-GCNDM method correctly recognized DDoS attacks and normal samples. On 500 epochs, the SSODE-GCNDM method provides an average $accu_y$ of 97.80%, $prec_n$ of 98.20%, $reca_l$ of 97.80%, $F_{measure}$ of 97.99%, and G_{Means} of 98.00%. Likewise, on 1000 epochs, the SSODE-GCNDM methodology offers an average $accu_y$ of 99.62%, $prec_n$ of 99.72%, $reca_l$ of 99.62%, $F_{measure}$ of 99.67%, and G_{Means} of 99.67%. Moreover, on 1500 epochs, the SSODE-GCNDM methodology gains an average $accu_y$ of 98.62%, $prec_n$ of 98.85%, $reca_l$ of 98.62%, $F_{measure}$ of 98.73%, and G_{Means} of 98.73%.

Class	$Accu_y$	$Prec_n$	$Reca_l$	$F_{measure}$	G_{Means}
Epoch – 500					
DDoS Attack	99.10	97.92	99.10	98.51	98.51
Normal	96.50	98.47	96.50	97.47	97.48
Average	**97.80**	**98.20**	**97.80**	**97.99**	**98.00**
Epoch – 1000					
DDoS Attack	99.90	99.60	99.90	99.75	99.75
Normal	99.33	99.83	99.33	99.58	99.58
Average	**99.62**	**99.72**	**99.62**	**99.67**	**99.67**
Epoch – 1500					
DDoS Attack	99.40	98.71	99.40	99.05	99.05
Normal	97.83	98.99	97.83	98.41	98.41
Average	**98.62**	**98.85**	**98.62**	**98.73**	**98.73**
Epoch – 2000					
DDoS Attack	99.30	97.83	99.30	98.56	98.56
Normal	96.33	98.80	96.33	97.55	97.56
Average	**97.82**	**98.32**	**97.82**	**98.06**	**98.06**
Epoch – 2500					
DDoS Attack	99.40	99.10	99.40	99.25	99.25
Normal	98.50	98.99	98.50	98.75	98.75
Average	**98.95**	**99.05**	**98.95**	**99.00**	**99.00**
Epoch – 3000					
DDoS Attack	99.10	98.22	99.10	98.66	98.66
Normal	97.00	98.48	97.00	97.73	97.74
Average	**98.05**	**98.35**	**98.05**	**98.19**	**98.20**

Table 2. DDoS attack recognition outcome of SSODE-GCNDM technique under distinct epochs.

Finally, on 3000 epochs, the SSODE-GCNDM methodology provides an average $accu_y$ of 98.05%, $prec_n$ of 98.35%, $reca_l$ of 98.05%, $F_{measure}$ of 98.19%, and G_{Means} of 98.20%.

In Fig. 8, the training (TRA) and validation (VLA) accuracy outcomes of the SSODE-GCNDM approach under epoch 1000 are displayed. The accuracy values are computed for 0–1000 epochs. The figure highlighted that the TRA and VLA accuracy values display a rising tendency, which indicates the ability of the SSODE-GCNDM model to improve performance over several iterations. Also, the TRA and VLA accuracy remains closer over the epochs, showing low minimal overfitting and enhanced performance of the SSODE-GCNDM model, guaranteeing consistent prediction on unseen samples.

Figure 9 displays the TRA and VLA loss graph of the SSODE-GCNDM model at epoch 1000. The loss rates are computed for 0–1000 epochs. It is signified that the TRA and VLA accuracy rates display a lower trend, notifying the ability of the SSODE-GCNDM method to balance a trade-off between data fitting and generalization. The continual reduction in loss values guarantees the enhanced performance of the SSODE-GCNDM methodology and tunes the prediction results over time.

In Fig. 10, the precision-recall (PR) curve analysis of the SSODE-GCNDM approach under epoch 1000 interprets its performance by plotting Precision against Recall for all the classes. The figure shows that the SSODE-GCNDM approach continuously accomplishes improved PR values across different class labels, representing its capability to maintain a significant portion of true positive predictions amongst each positive prediction (precision) while capturing a large proportion of actual positives (recall). The steady rise in PR results among all classes depicts the effectiveness of the SSODE-GCNDM technique in the classification process.

In Fig. 11, the ROC curve of the SSODE-GCNDM model is studied. The outcomes imply that the SSODE-GCNDM model reaches enhanced ROC outcomes over each class under epoch 1000, representing a significant ability to discriminate the classes. This reliable tendency of improved ROC values over various classes indicates the efficient performance of the SSODE-GCNDM approach in predicting classes, emphasizing the robust nature of the classification process.

The comparative analysis of the SSODE-GCNDM methodology with existing approaches is illustrated in Table 3; Fig. 12[59–63]. The simulation result indicated that the SSODE-GCNDM approach outperformed better performances. Regarding $accu_y$, the SSODE-GCNDM approach has a better $accu_y$ of 99.62%. In contrast, the Logistic Regression (LR), KNN, RF, DT, AdaBoost, XGBoost, Multi-Layer Perceptron (MLP), and DNN, Quantum CNN (QCNN), global search strategy of the coyote optimization algorithm with Improved deep neural network (COA-GS-IDNN), Grey Wolf Optimizer and Long Short-Term Memory (GWO-LSTM), and Autoencoder (AE) methods have the lowest $accu_y$ of 91.10%, 97.00%, 98.54%, 98.36%, 98.09%, 98.34%, 98.98%, 99.37%, 99.25%, 98.71%, 99.10%, and 98.95%, correspondingly. Likewise, for $prec_n$, the SSODE-GCNDM method has a high $prec_n$ of 99.72%, while the LR, KNN, RF, DT, AdaBoost, XGBoost, MLP, DNN, QCNN, COA-GS-IDNN, GWO-LSTM, and AE methodologies have minimal $prec_n$ of 91.00%, 97.00%, 98.52%, 98.64%, 98.08%, 98.65%,

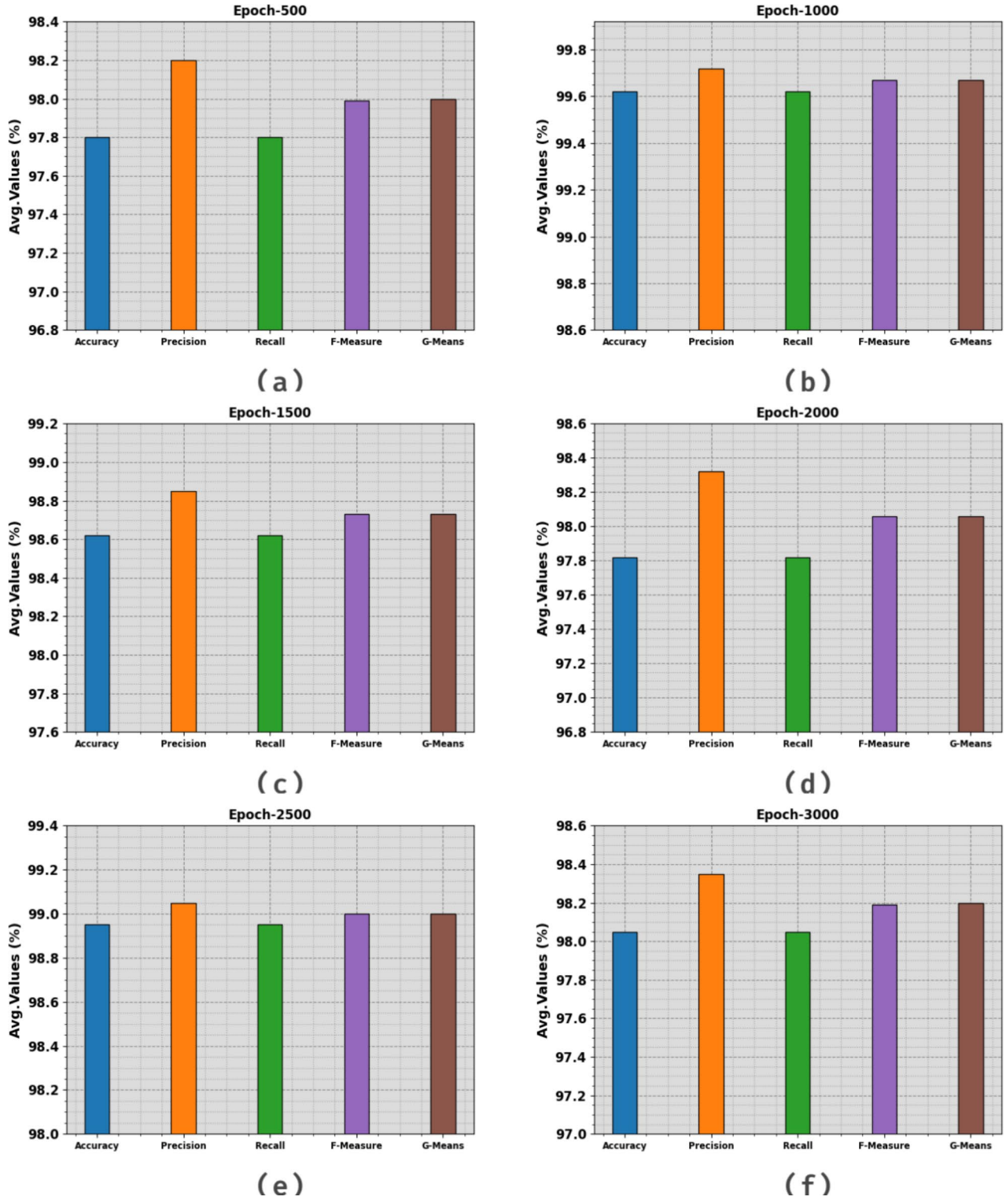

Fig. 7. Average outcome of SSODE-GCNDM technique (a) Epochs 500, (b) Epochs 1000, (c) Epochs 1500, (d) Epochs 2000, (e) Epochs 2500, (f) Epochs 3000.

98.67%, 99.17%, 99.12%, 99.41%, 98.87%, and 98.82%, respectively. Finally, based on $F_{measure}$, the SSODE-GCNDM method has superior $F_{measure}$ of 99.67% while the LR, KNN, RF, DT, AdaBoost, XGBoost, MLP, DNN, QCNN, COA-GS-IDNN, GWO-LSTM, and AE techniques exhibited the lowest $F_{measure}$ of 91.00%, 97.00%, 98.79%, 97.82%, 98.35%, 98.46%, 98.61%, 98.82%, 98.59%, 98.70%, 98.82%, and 98.82%, respectively.

In Table 4; Fig. 13, the comparative results of the SSODE-GCNDM approach are specified in terms of computational time (CT). The outcomes suggest that the SSODE-GCNDM approach gets better performance.

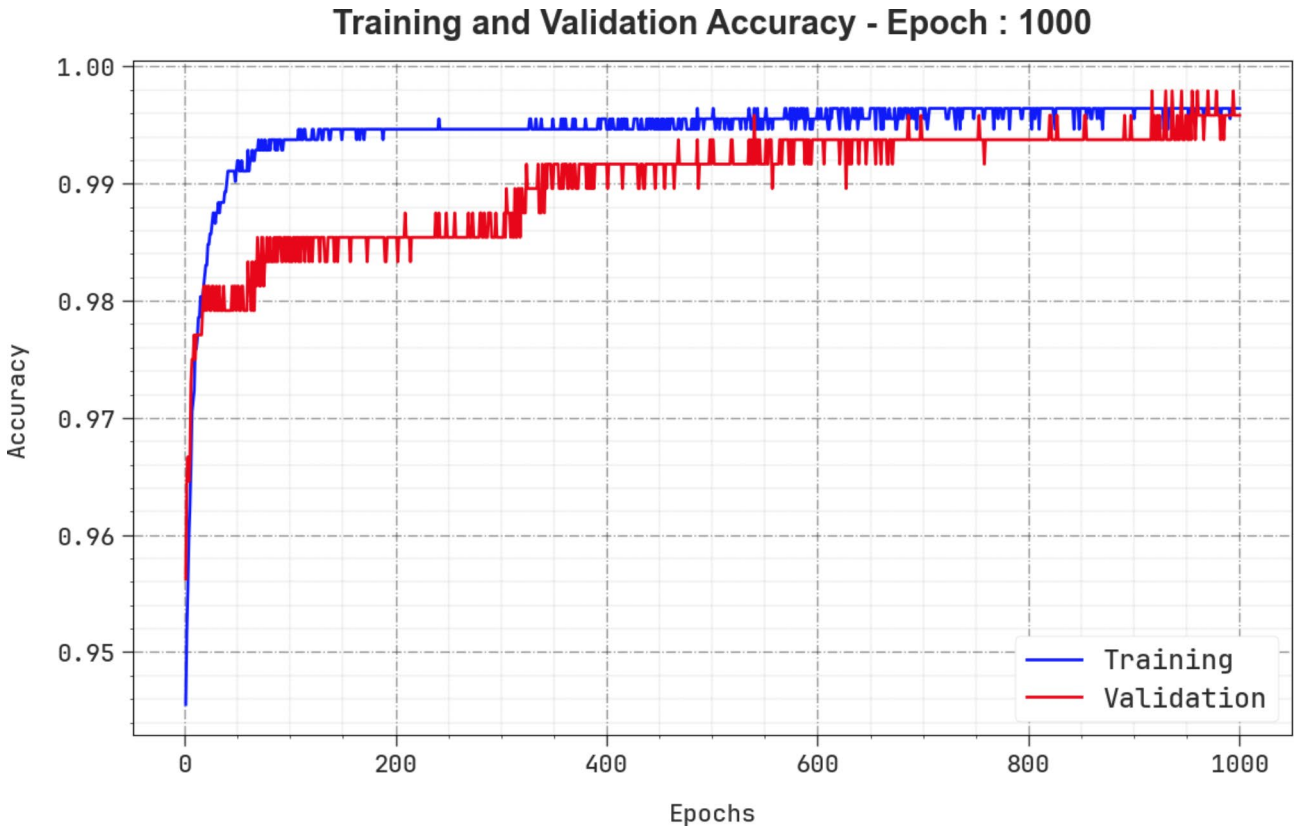

Fig. 8. $Accu_y$ curve of SSODE-GCNDM technique on Epoch 1000.

Based on CT, the SSODE-GCNDM approach offers a reduced CT of 05.92s whereas the LR, KNN, RF, DT, AdaBoost, XGBoost, MLP, DNN, QCNN, COA-GS-IDNN, GWO-LSTM, and AE models attain better CT values of 11.68s, 10.61s, 14.17s, 09.91s, 07.42s, 11.96s, 11.14s, 12.45s, 10.07s, 09.12s, 13.11s, and 12.20s, correspondingly.

Conclusion

This manuscript proposes the SSODE-GCNDM technique in the IoT environment. The main intention of the SSODE-GCNDM method is to recognize the presence of DDoS attack behaviour in IoT platforms. Primarily, the SSODE-GCNDM technique involves Z-score normalization to scale the input data into a uniform format. The presented SSODE-GCNDM technique utilizes the SSO-DE method for the feature selection process. Moreover, the GCN technique is employed to recognize and mitigate attacks. Finally, the presented SSODE-GCNDM model implements the NGO method to fine-tune the parameters involved in the GCN method. A wide range of experimentation analyses occur, and the outcomes are observed in numerous aspects. The experimental validation of the SSODE-GCNDM technique portrayed a superior accuracy value of 99.62% compared to existing approaches. The presented SSODE-GCNDM approach has limitations, such as sensitivity to data quality and potential overfitting when working with high-dimensional datasets. The reliance on specific optimization algorithms may also restrict adaptability to diverse problem domains. Future work should focus on enhancing model robustness through enhanced data preprocessing and combining ensemble techniques to reduce overfitting. Furthermore, exploring unsupervised learning methods could give valuable insights when labelled data is scarce. Examining the transfer learning (TL) model application may improve performance across varying contexts. Expanding the framework to accommodate real-time attack detection could enhance practical applicability in dynamic environments.

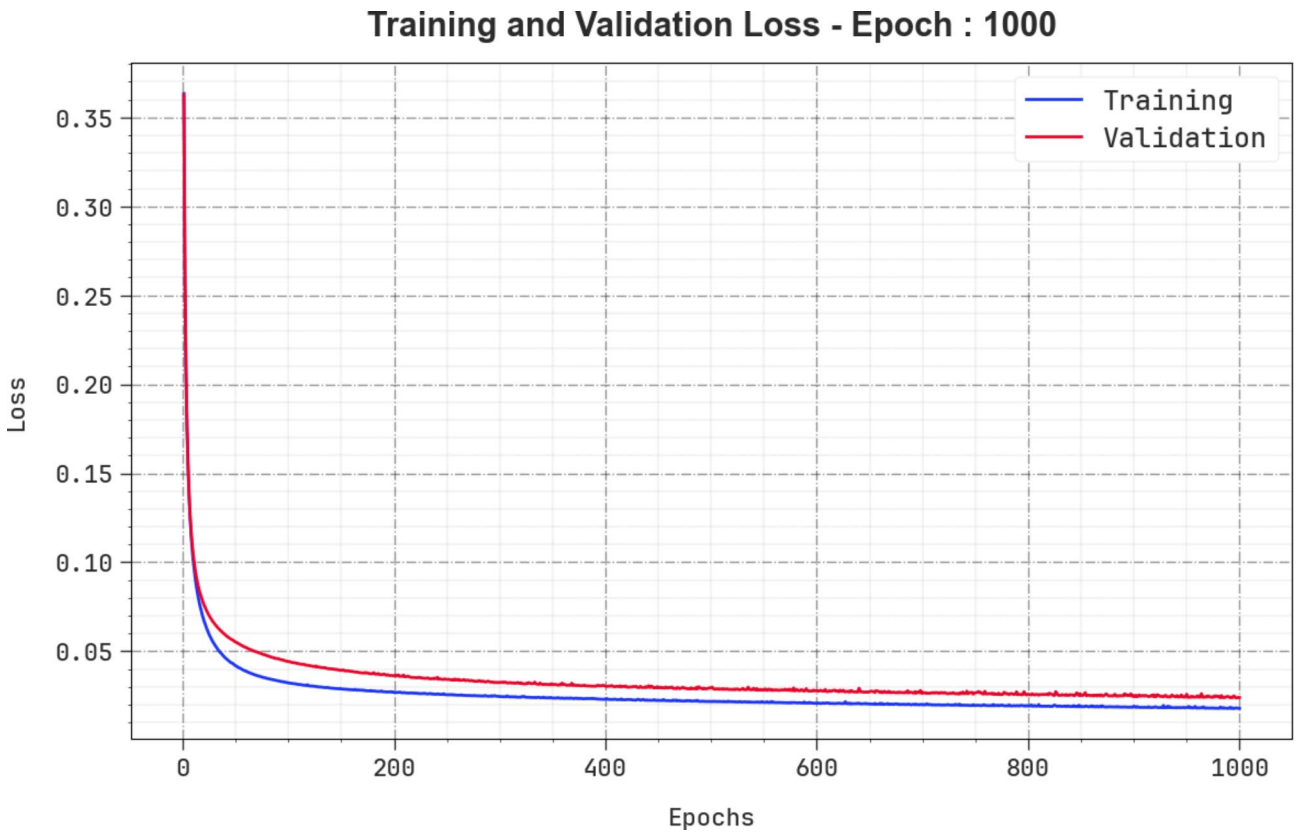

Fig. 9. Loss curve of SSODE-GCNDM technique on Epoch 1000.

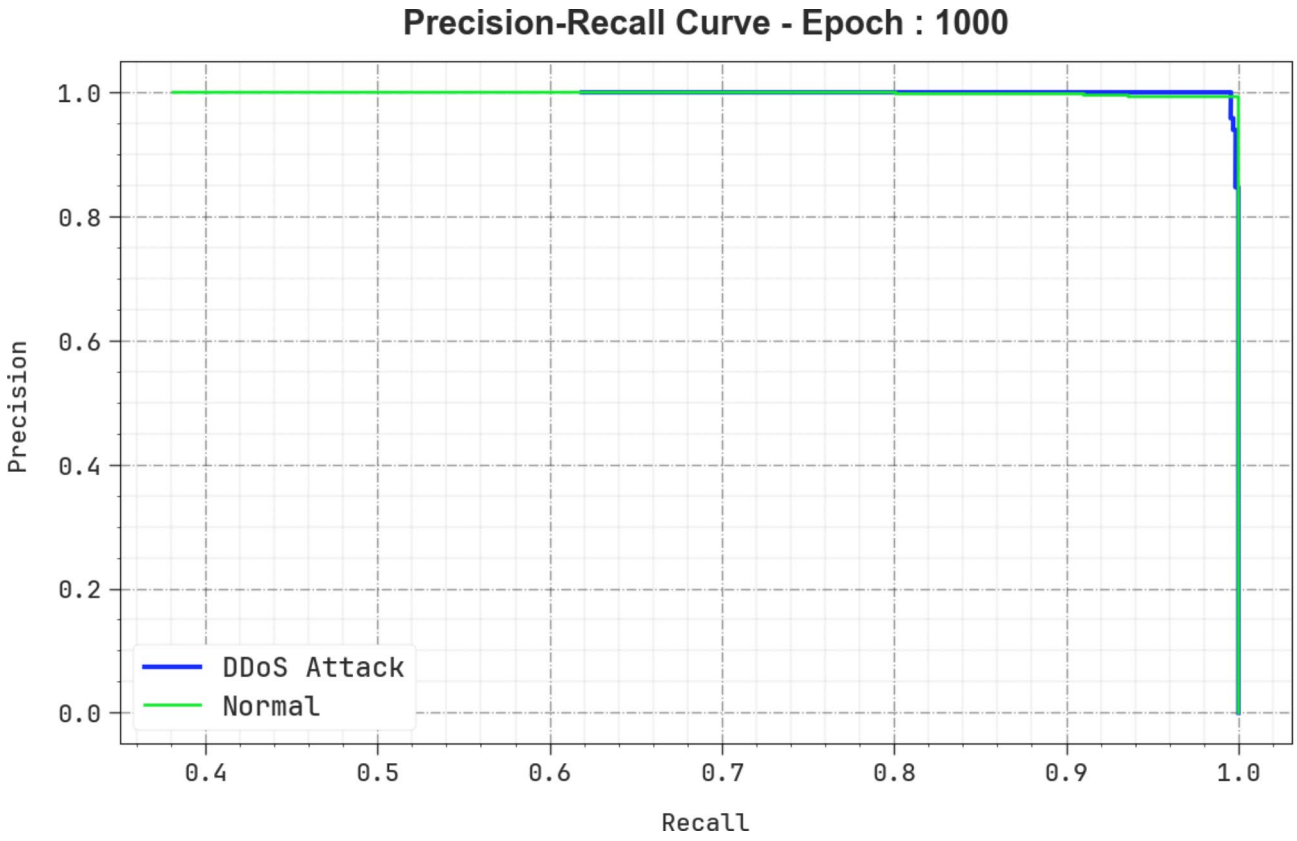

Fig. 10. PR curve of SSODE-GCNDM technique on Epoch 1000.

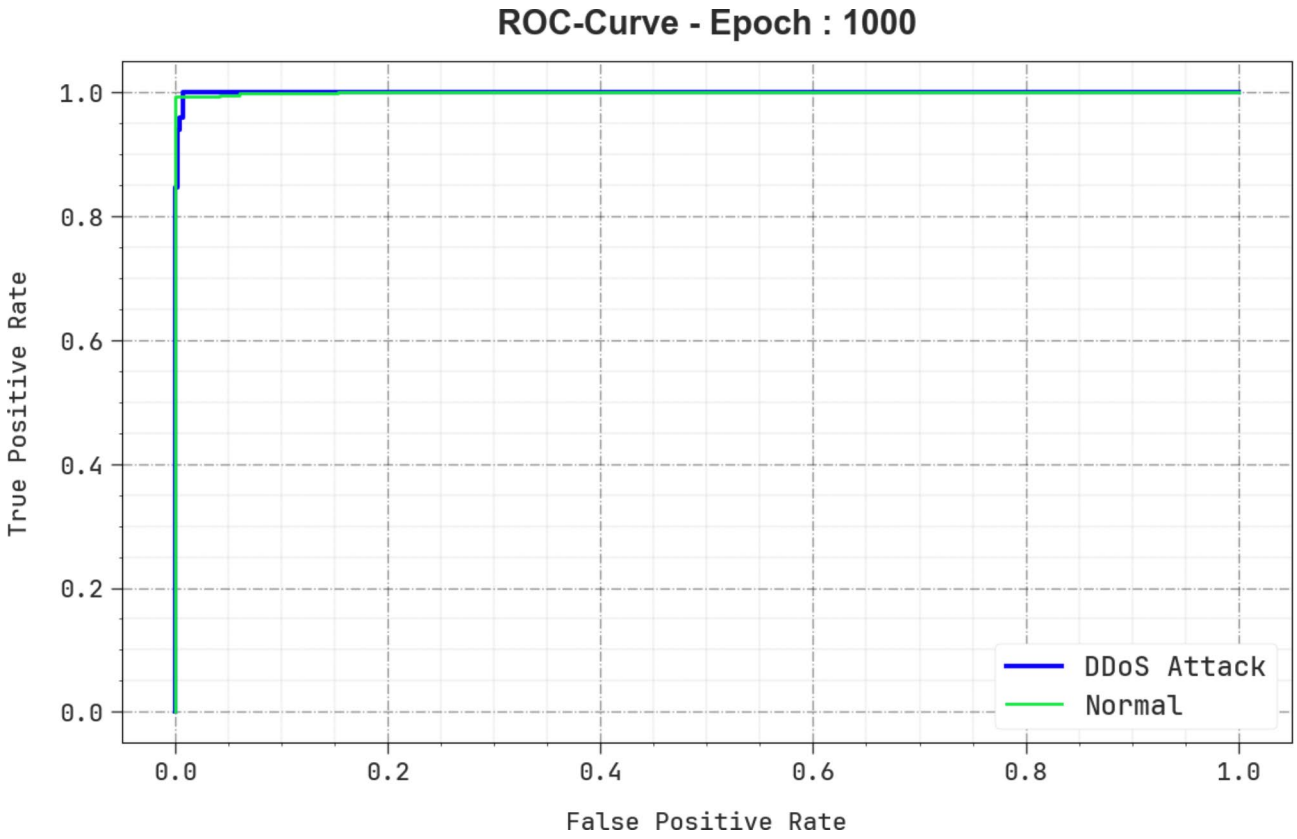

Fig. 11. ROC curve of SSODE-GCNDM technique on Epoch 1000.

Classifiers	$Accu_y$	$Prec_n$	$Reca_l$	$F_{measure}$
LR	91.10	91.00	91.00	91.00
KNN	97.00	97.00	97.00	97.00
RF	98.54	98.52	98.22	98.79
DT	98.36	98.64	98.24	97.82
AdaBoost	98.09	98.08	98.24	98.35
XGBoost	98.34	98.65	98.51	98.46
MLP Classifier	98.98	98.67	98.47	98.61
DNN	99.37	99.17	98.97	98.82
QCNN	99.25	99.12	99.15	98.59
COA-GS-IDNN	98.71	99.41	98.48	98.70
GWO-LSTM	99.10	98.87	98.70	98.82
AE	98.95	98.82	99.17	98.82
SSODE-GCNDM	99.62	99.72	99.62	99.67

Table 3. Comparative analysis of SSODE-GCNDM approach with recent models[59–63].

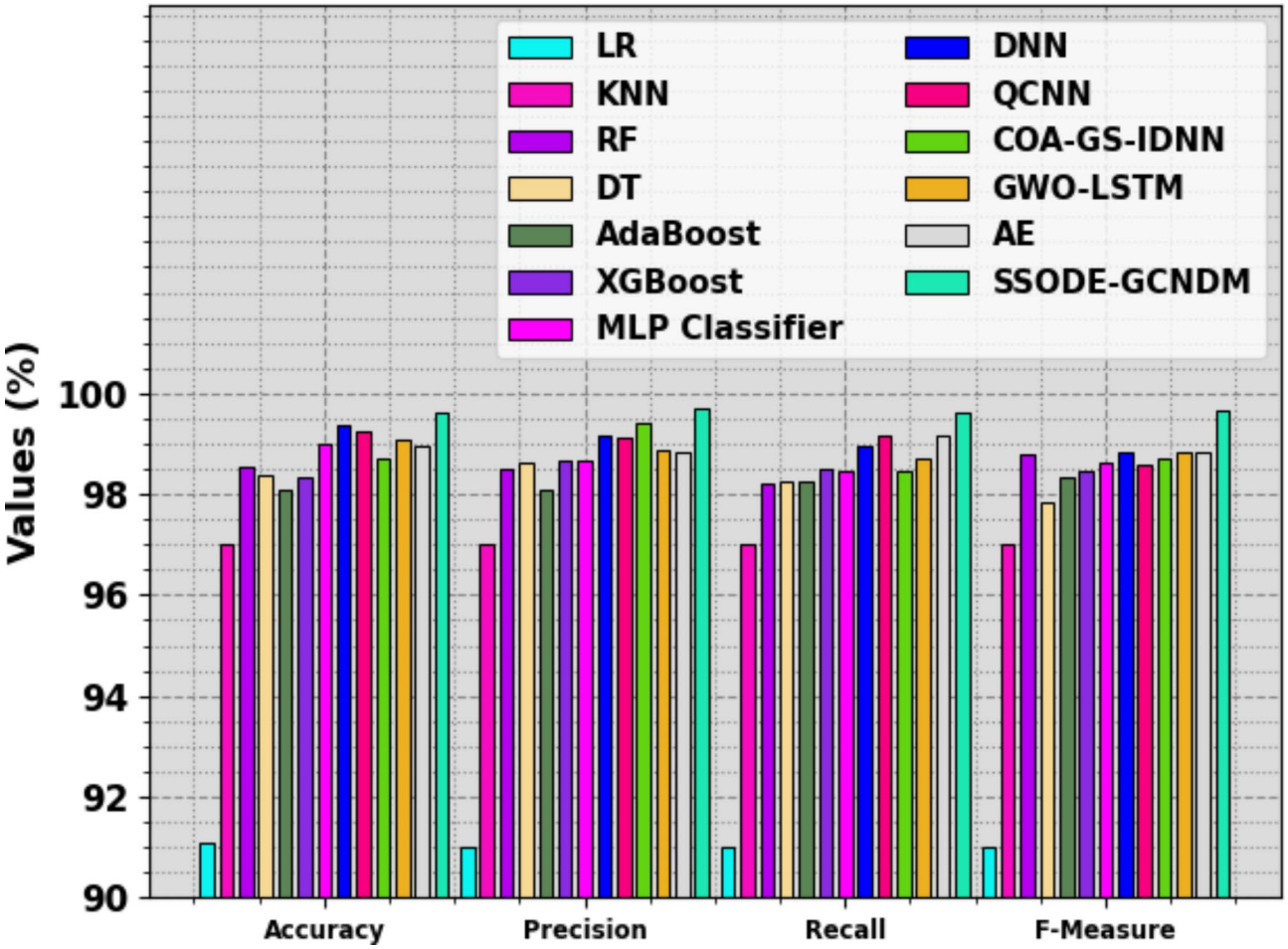

Fig. 12. Comparative analysis of SSODE-GCNDM approach with recent models.

Classifiers	CT (sec)
LR	11.68
KNN	10.61
RF	14.17
DT	09.91
AdaBoost	07.42
XGBoost	11.96
MLP Classifier	11.14
DNN	12.45
QCNN	10.07
COA-GS-IDNN	09.12
GWO-LSTM	13.11
AE	12.20
SSODE-GCNDM	05.92

Table 4. CT outcome of SSODE-GCNDM method with recent models.

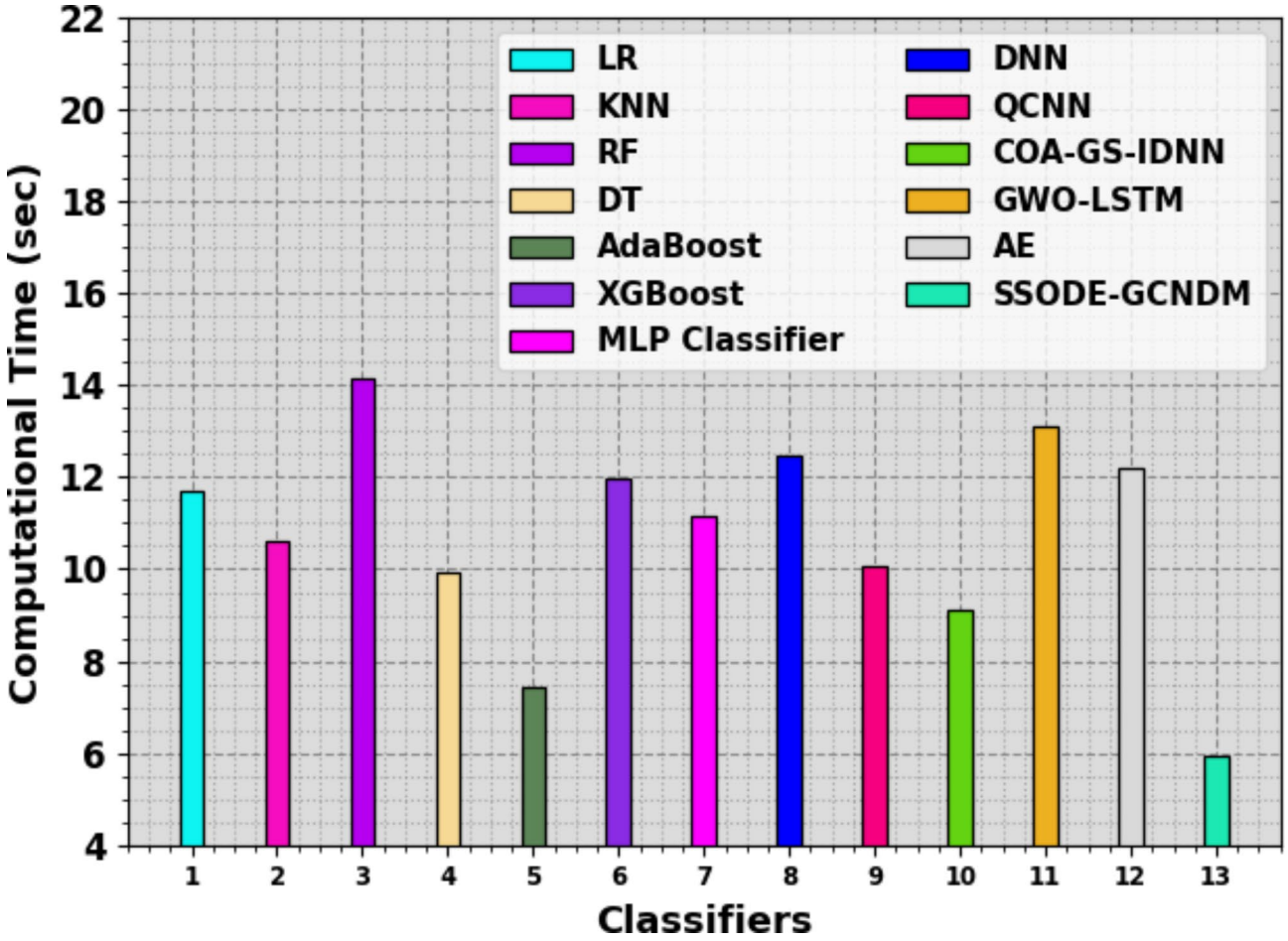

Fig. 13. CT outcome of SSODE-GCNDM technique with recent models.

Data availability

The datasets used and analyzed during the current study available from the corresponding author on reasonable request.

Received: 11 September 2024; Accepted: 25 November 2024
Published online: 28 December 2024

References

1. Karmous, N., Aoueileyine, M. O. E., Abdelkader, M., Romdhani, L. & Youssef, N. Software-Defined-Networking-Based One-versus-Rest Strategy for Detecting and Mitigating Distributed Denial-of-Service Attacks in Smart Home Internet of Things Devices. *Sensors*, *24*(15), p.5022. (2024).
2. Ramprasath, J., Krishnaraj, N. & Seethalakshmi, V. Mitigation services on SDN for distributed denial of service and denial of service attacks using machine learning techniques. *IETE J. Res.* **70** (1), 70–81 (2024).
3. Arachchige, K. G., Branch, P. & But, J. An Analysis of Blockchain-Based IoT Sensor Network Distributed Denial of Service Attacks. *Sensors*, *24*(10), p.3083. (2024).
4. Kumar, G. & Pragya IPv6 addressing with hidden duplicate address detection to mitigate denial of service attacks in the internet of drone. *Concurrency and Computation: Practice and Experience*, p.e8131. (2024).
5. Hnamte, V., Najar, A. A., Nhung-Nguyen, H., Hussain, J. & Sugali, M. N. DDoS attack detection and mitigation using deep neural network in SDN environment. *Computers & Security*, *138*, p.103661. (2024).
6. Zaki, A. M., Abdelhamid, A. A., Ibrahim, A., Eid, M. M. & El-Kenawy, E. S. M. Enhancing K-Nearest neighbors Algorithm in Wireless Sensor networks through Stochastic Fractal Search and particle swarm optimization. *J. Cybersecur. Inform. Manage.*, **13**(1). (2024).
7. Varma, A., Kumar, A. T. & Yamini, B. April. Detection and Prevention of Distributed Denial of Service (DDoS) Attacks Using Machine Learning Techniques. In *2024 2nd International Conference on Networking and Communications (ICNWC)* (pp. 1–5). IEEE. (2024).
8. Kumar, A. & Singh, D. Detection and prevention of DDoS attacks on edge computing of IoT devices through reinforcement learning. *Int. J. Inform. Technol.* **16** (3), 1365–1376 (2024).
9. Shah, Z., Ullah, I., Li, H., Levula, A. & Khurshid, K. Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. *Sensors*, *22*(3), p.1094. (2022).
10. Ali, M. H. et al. Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT). *Electronics*, *11*(3), p.494. (2022).
11. Sanlı, M. Detection and mitigation of denial of service attacks in internet of things networks. *Arab. J. Sci. Eng.*, pp.1–11. (2024).

12. Abid, Y. A., Wu, J., Xu, G., Fu, S. & Waqas, M. Multi-level Deep Neural Network for Distributed Denial-of-Service Attack Detection and classification in Software-defined networking supported internet of things networks. *IEEE Internet Things J.* (2024).
13. Kumar, S. & kumar Keshri, A. An effective DDoS attack mitigation strategy for IoT using an optimization-based adaptive security model. *Knowledge-Based Systems*, *299*, p.112052. (2024).
14. Nisa, N., Khan, A. S., Ahmad, Z. & Abdullah, J. Two-phase authentication system for denial of service attack detection and mitigation using machine learning in software-defined network. *Int. J. Network Manage.* **34** (3), e2258 (2024).
15. Kavitha, D. & Ramalakshmi, R. Machine learning-based DDOS Attack Detection and Mitigation in SDNs for IoT environments. *J. Franklin Inst.*, p.107197. (2024).
16. Musa, N. S., Mirza, N. M., Rafique, S. H., Abdallah, A. & Murugan, T. Machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks-current research solutions. *IEEE Access.* (2024).
17. Aslam, M. et al. Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT. *Sensors*, *22*(7), p.2697. (2022).
18. Ahmim, A., Maazouzi, F., Ahmim, M., Namane, S. & Dhaou, I. B. Distributed denial of service attack detection for the internet of things using hybrid deep learning model. *IEEE Access.* **11**, 119862–119875 (2023).
19. Al Hwaitat, A. K. & Fakhouri, H. N. Adaptive Cybersecurity Neural Networks: An Evolutionary Approach for Enhanced Attack Detection and Classification. *Applied Sciences*, *14*(19), p.9142. (2024).
20. Benlloch-Caballero, P., Wang, Q. & Calero, J. M. A. Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks. *Computer Networks*, *222*, p.109526. (2023).
21. Huang, H., Li, T., Li, B., Wang, W. & Sun, Y. A bidirectional Differential Evolution based unknown Cyberattack Detection System. *IEEE Trans. Evol. Comput.* (2024).
22. Sureshkumar, S., Venkatesan, G. P. & Santhosh, R. Detection of DDoS attacks on Cloud Computing Environment using altered Convolutional Deep Belief Networks. *Int. J. Comput. Netw. Inform. Secur.* **15** (5), 63–72 (2023).
23. Anoop, M., Mary, L. W., Wilson, A. J. & Kiran, W. S. Optimized graph transformer with molecule attention network based multi class attack detection framework for enhancing privacy and security in WSN. *Multimedia Tools and Applications*, pp.1–32. (2024).
24. Al-Dunainawi, Y., Al-Kaseem, B. R. & Al-Raweshidy, H. S. Optimized artificial intelligence model for DDoS detection in SDN environment. *IEEE Access.* (2023).
25. Hekmati, A. & Krishnamachari, B. Graph-Based DDoS Attack Detection in IoT Systems with Lossy Network. *arXiv preprint arXiv:2403.09118*. (2024).
26. Ali, J., Shan, G., Gul, N. & Roh, B. H. An intelligent blockchain-based secure link failure recovery framework for software-defined internet-of-things. *Journal of Grid Computing*, *21*(4), p.57. (2023).
27. Rizvi, F. et al. An evolutionary KNN model for DDoS assault detection using genetic algorithm based optimization. *Multimedia Tools Appl.*, pp.1–24. (2024).
28. Kostas, K., Just, M. & Lones, M. A. IoTGeM: Generalizable Models for Behaviour-Based IoT Attack Detection. *arXiv preprint arXiv:2401.01343*. (2023).
29. Sadhwani, S., Mathur, A., Muthalagu, R. & Pawar, P. M. 5G-SIID: an intelligent hybrid DDoS intrusion detector for 5G IoT networks. *Int. J. Mach. Learn. Cybernet.*, pp.1–21. (2024).
30. Aswad, F. M., Ahmed, A. M. S., Alhammadi, N. A. M., Khalaf, B. A. & Mostafa, S. A. Deep learning in distributed denial-of-service attacks detection method for Internet of Things networks. *Journal of Intelligent Systems*, *32*(1), p.20220155. (2023).
31. Pawar, P. P., Kumar, D., Ananthan, B., Pradeepa, A. S. & Selvi, A. S. May. An efficient ddos attack detection using attention based hybrid model in blockchain based SDN-IOT. In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1–5). IEEE. (2024).
32. Oladele, T. O. & Jimoh, E. R. Analysis of deep neural networks algorithms for mitigating distributed denial of service attacks in Software defined networks. *FUW Trends Sci. Technol.* **8** (3), 353–360 (2023).
33. Ma, Y. et al. A Survey of DDoS Attack and Defense technologies in Multi-access Edge Computing. *IEEE Internet Things J.* (2024).
34. Vincent, E., Korki, M., Seyedmahmoudian, M., Stojcevski, A. & Mekhilef, S. Detection of false data injection attacks in cyber–physical systems using graph convolutional network. *Electric Power Systems Research*, *217*, p.109118. (2023).
35. Yang, T. et al. Secure and traceable multikey image retrieval in cloud-assisted internet of things. *IEEE Internet Things J.* (2024).
36. Feng, Y., Li, J., Sisodia, D. & Reiher, P. On Explainable and Adaptable Detection of Distributed Denial-of-Service Traffic. *IEEE Transactions on Dependable and Secure Computing*. (2023).
37. Chen, L. et al. Efficient and secure content-based image Retrieval in Cloud-assisted internet of things. *IEEE Internet Things J.* (2024).
38. Lo, W. W., Kulatilleke, G., Sarhan, M., Layeghy, S. & Portmann, M. XG-BoT: An explainable deep graph neural network for botnet detection and forensics. *Internet of Things*, *22*, p.100747. (2023).
39. Ma, J., Su, W., Li, Y. & Peng, Y. Synchronizing DDoS detection and mitigation based graph learning with programmable data plane, SDN. *Future Generation Comput. Syst.* **154**, 206–218 (2024).
40. Li, K., Zhou, H., Tu, Z., Liu, O. & Zhang, H. AT-GCN: A DDoS attack path tracing system based on attack traceability knowledge base and GCN. *Computer Networks*, *236*, p.110036. (2023).
41. Qian, K. et al. Distributed Detection of Large-Scale Internet of Things Botnets Based on Graph Partitioning. *Applied Sciences*, *14*(4), p.1615. (2024).
42. Jemal, I., Cheikhrouhou, O. & Haddar, M. A. October. IoT DOS and DDOS Attacks Detection Using an Effective Convolutional Neural Network. In *2023 International Conference on Cyberworlds (CW)* (pp. 373–379). IEEE. (2023).
43. Abinesh, R. & Nandhini, S. VG, Y., TJ, S. and October. Deep Graph Convolution Neural Network based Intrusion Detection System towards Early Detection of Malicious Attacks. In *2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 549–554). IEEE. (2024).
44. Lee, Y. & Han, S. W. CAGCN: Causal attention graph convolutional network against adversarial attacks. *Neurocomputing*, *538*, p.126187. (2023).
45. Sanap, Y. B. & Aher, P. G. February. Deep Learning Method for Detecting and Mitigating Distributed Denial of Service Attacks with Imbalanced Data. In *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)* (pp. 1–8). IEEE. (2024).
46. Khalid Alkahtani, H. et al. optimal graph convolutional neural network-based ransomware detection for cybersecurity in IoT environment. *Applied Sciences*, *13*(8), p.5167. (2023).
47. Saunders, B. J., Kisanga, P., Carvalho, G. H. & Woungang, I. April. A Graph Convolutional Networks-Based DDoS Detection Model. In *2024 IEEE International Systems Conference (SysCon)* (pp. 1–5). IEEE. (2024).
48. Kisanga, P., Woungang, I., Traore, I. & Carvalho, G. H. February. Network anomaly detection using a graph neural network. In *2023 International Conference on Computing, Networking and Communications (ICNC)* (pp. 61–65). IEEE. (2023).
49. Altaf, T. et al. GNN-Based Network Traffic Analysis for the Detection of Sequential Attacks in IoT. *Electronics*, *13*(12), p.2274. (2024).
50. Alhayani, S. & Murphy, D. R. A machine learning-based distributed denial of Service Detection Approach for early warning in Internet Exchange points. *Computers Mater. Continua*, **76**(2). (2023).
51. Thota, M. K., Prathibhavani, P. M. & Venugopal, K. R. June. The Graph Neural Network with Wasserstein Generative Adversarial Network for botnet detection in smart city IoT. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1–6). IEEE. (2024).

52. Barsellotti, L., De Marinis, L., Cugini, F. & Paolucci, F. June. FTG-Net: Hierarchical flow-to-traffic graph neural network for DDoS attack detection. In *2023 IEEE 24th International Conference on High Performance Switching and Routing (HPSR)* (pp. 173–178). IEEE. (2023).
53. Geem, D. et al. Progression of Pediatric Crohn's disease is Associated with anti–tumor necrosis factor timing and body Mass Index Z-Score normalization. *Clin. Gastroenterol. Hepatol.* **22** (2), 368–376 (2024).
54. Alzoubi, S. et al. (2024). Synergistic swarm optimization algorithm.
55. Alshinwan, M. et al. Enhanced Prairie Dog Optimization with Differential Evolution for Solving Engineering Design Problems and Network Intrusion Detection System. *Heliyon*. (2024).
56. Immordino, G., Vaiuso, A., Da Ronch, A. & Righi, M. Predicting Transonic Flowfields in Non-Homogeneous Unstructured Grids Using Autoencoder Graph Convolutional Networks. *arXiv preprint arXiv:2405.04396*. (2024).
57. Zeng, L., Hu, M., Zhang, C., Yuan, Q. & Wang, S. A Multi-strategy-improved Northern Goshawk optimization algorithm for global optimization and Engineering Design. *Computers Mater. Continua*, **80**(1). (2024).
58. https://data.mendeley.com/datasets/8dns3xbckv/1
59. Becerra-Suarez, F. L., Fernández-Roman, I. & Forero, M. G. Improvement of Distributed Denial of Service Attack Detection through Machine Learning and Data Processing. *Mathematics*, *12*(9), p.1294. (2024).
60. Fathima, A., Devi, G. S. & Faizaanuddin, M. Improving distributed denial of service attack detection using supervised machine learning. *Measurement: Sensors*, *30*, p.100911. (2023).
61. Vaisakhkrishnan, K., Ashok, G., Mishra, P. & Kumar, T. G. Guarding Digital Health: deep learning for attack detection in Medical IoT. *Procedia Comput. Sci.* **235**, 2498–2507 (2024).
62. Ramadass, P. et al. BSDN-HMTD: A blockchain supported SDN framework for detecting DDoS attacks using deep learning method. *Egyptian Informatics Journal*, *27*, p.100515. (2024).
63. Sedhuramalingam, K. & Saravanakumar, N. A novel optimal deep learning approach for designing intrusion detection system in wireless sensor networks. *Egyptian Informatics Journal*, *27*, p.100522. (2024).

Author contributions

Chukka Ramesh Babu: Conceptualization, methodology development, experiment, formal analysis, investigation, writing. M. Suneetha: Formal analysis, investigation, validation, visualization, writing. Mohammed Altaf Ahmed: Formal analysis, review and editing. Palamakula Ramesh babu : Methodology, investigation. Mohamad Khairi Ishak: Review and editing. Samih M. Mostafa: Discussion, review and editing. Hend Khalid Alkahtani: Conceptualization, methodology development, investigation, supervision, review and editing.All authors have read and agreed to the published version of the manuscript.

Funding

details.

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNUR-SP2024R384), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Declarations

Competing interests

The authors declare no competing interests.

Conflict of interest

The authors declare that they have no conflict of interest. The manuscript was written with the contributions of all authors, and all authors have approved the final version.

Ethics approval

This article contains no studies with human participants performed by any authors.

Consent to participate

Not applicable.

Informed consent

Not applicable.

Additional information

Correspondence and requests for materials should be addressed to H.K.A.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.