International Journal of Information Security and Privacy
Volume 17 • Issue 1

Optimized Deep Neuro Fuzzy Network for Cyber Forensic Investigation in Big Data-Based IoT Infrastructures

Suman Thapaliya, Department of IT, Lincoln University College, Malaysia*

Pawan Kumar Sharma, Department of Faculty of Science Health and Technology, Nepal Open University, Nepal

ABSTRACT

Forensic skills analysts play an imperative support to practice streaming data generated from the IoT networks. However, these sources pose size limitations that create traffic and increase big data assessment. The obtainable solutions have utilized cybercrime detection techniques based on regular pattern deviation. Here, a generalized model is devised considering the MapReduce as a backbone for detecting the cybercrime. The objective of this model is to present an automatic model, which using the misbehavior in IoT device can be manifested, and as a result the attacks exploiting the susceptibility can be exposed by newly devised automatic model. The simulation of IoT is done such that energy constraints are considered as basic part. The routing is done with fractional gravitational search algorithm to transmit the information amongst the nodes. Apart from this, the MapReduce is adapted for cybercrime detection and is done at base station (BS) considering deep neuro fuzzy network (DNFN) for identifying the malwares.

KEYWORDS

big data, Cyber forensic investigation, Deep neuro fuzzy network, Internet of Things, MapReduce framework

1. INTRODUCTION

The IoT devices link the static or mobile devices and objects using the sensors and actuator and offers smooth communication through network. IoT provides the widespread utilization of several modern technologies and models using the transmission control protocol (TCP) /internet protocol, which emerges in the model of interconnecting devices considering the physical platform. The main aspect adapted in routing considering IoT is efficiency of energy, safe communication, and scalability. The routing and data transmission using sophisticated services provides a key problem in IoT. The online business and Mobile commerce are emerging IoT application. The security considering IoT includes in-depth assessment as a basic need to preserve the network and is essential task. The genuine susceptibility in the IoT platform is insecure web interface, mobile interface and deficiency of security

DOI: 10.4018/IJISP.315819 *Corresponding Author

configurability. The aspects to avert cyber-attacks are devised by specified authors (Chhabra et al., 2020). A major IoT model accumulates large quantity of data known as big data and it transmits to layer that performs processing. The big data are devised with three features, such as volume, variety and velocity (Srinivasan et al., 2012). The big data is growing each year and thus the rebellion in the technology and scientific face influenced the size of data to maximize the lucrative tasks (Triguero et al., 2016 ; Venugopal et al., 2021). The database of big data is complex to accumulate, split, sort, envisage and examine the contemporary techniques (Terzi et al., 2015 ; Suthaharan, 2014 ; Venugopal et al., 2021).

Classically, the majority of data contained in big data represents streaming data, because of the connections, capacity, and events of the data modeling, which progress through the internet. The data are produced considering the time instance (Zhang et al., 2012 ; Venugopal et al., 2021). Cybercrime represents a crime through computer in which the computers are utilized for prohibited tasks, such as child pornography, theft, fraudulent behavior, intellectual possessions. The Cybercrime is progressively growing in internet technologies because of the computer operations, like commerce, entertainment and government. The server can conceal its data by foraging sender address, which are transmitted through unidentified server or channel. The detection of cybercrime is a basic domain in the retrieval of information, processing language and machine learning (Venugopal et al., 2021). Cybercrime is digital crime caused by considering network as weapon. The multiple cybercrime domains are extended from uncomplicated credential risks to geopolitical crime in recent days (Guarino, 2013). The report of crime survey reveals that 49% of global CEOs pose issues over the emerging network and figures out way to avert its institutions from risks (Meidan et al., 2017). The cybercrime requires coherent and logically effective technique for managing the crime space (Fahdi et al., 2013). Here, the cyber-attacks on IoT devices tend to be emerging. Some of the IoT attacks pose a hit in IoT platform in several years due to attacks, like Mirai botnet and Brickerbot (Chhabra et al., 2020).

The major problem in forensic relies in three classes, named legal, technical and resource issues. Amongst them, the technical issues provide a huge class of real-time live examination of anti-forensics data. The resource issues involve processing time and volume to attain and evaluate probable evidence item. The legal factors or issues include deficiency of legislation principles, simulation, reconstruction and other admissible problems (Fahdi et al., 2013). Generally, one requires meeting critical problems ranges to search for proving the evidence (Chhabra et al., 2020). The deep model is utilized for designing cyber security solutions and it has gained huge focus from both industry and academia. The DL method has huge ability to generate improved outcomes from big data of industrial models (Aljawarneha et al., 2018). However, the development of feasible and effectual attack detection methods for IoT is a major issue (Huma et al., 2021). Several machine learning models are utilized for performing analysis of big data and it includes several classifier, like Naive Bayes (NB), support vector machine (SVM), and k-nearest neighbors (KNN). The images and text are utilized in analyzing the big data whereas the cyber assessment contains elastic learning and flexible techniques (Wang and Jones 2021; Liu et al., 2013 ; Venugopal et al., 2021).

The purpose is to devise novel deep technique using MapReduce for cyber attack discovery. The inclusion of deep model helps to offer more accuracy and fast processing. It aimed at devising a new malware detection model based on DNFN for enabling the detection of attacks in IoT. The model performed routing amidst IoT devices to transmit data. The routing is done using FGSA for sending the accumulated data towards BS. The DNFN is trained with MSSO for detecting the malware wherein the MSSO is obtained by combining Mayfly Algorithm (MA) and Shuffled Shepherd Optimization Algorithm (SSOA). The proposed model was capable to discover and classify the cyber-attacks of IoT networks.

The major contributions involves

- **MSSO-based DNFN for discovering cybercrime in IoT with big data**. The proposed MSSO-based DNFN is adapted for detecting cybercrime in IoT platform using big data. Here, the DNFN

training is done using proposed MSSO, wherein the process of weight update in DNFN is done with MSSO, obtained byblending MA and SSOA.

The rest of the sections include Section 2 reveals prior cyber forensic discovery techniques in IoT. Section 3 exposes IoT configuration. Section 4 illustrates designed technique for cyber forensic detection. Section 5 confers competence of prior strategies, and Section 6 offers conclusion.

2. MOTIVATIONS

Due to quick extension of intellectual resource-based devices and high-speed techniques, the IoT has gained considerable attention. However, the platforms of IoT are susceptible to cyber-attacks because of certain constraints, like communication capacity, storage, and computation of end devices. Hence, motive is to devise a new framework for cyber-attack detection in IoT.

2.1. Literature Survey

The eight previously devised cyber-attack detection strategies are enlisted. Chhabra et al., (2020) presented generalized forensic model, which utilized Google's programming model and MapReduce model for detecting the cybercrime. The method utilized open-source tools and handled parallel processing and scalability. However, this technique suffers due to elevated processing time. To reduce time taken for processing, Huma et al., (2021) presented hybrid deep random neural network (HDRaNN) for detecting the cyberattack in IIoT. The method contained multilayer perceptron deep random neural network to regularize dropouts, but it was not capable to resist new attacks. To resist other attacks, Venugopal et al., (2021) developed a technique, namely Sunflower Jaya Optimization-based Deep stacked autoencoder (SFJO-based Deep SAE) for detecting the cyber attack. Here, the basic element of Sunflower optimization was combined with control attributes of Jaya optimization for addressing the problems of cyber forensic models. However, this technique suffered, due to elevated computational complexity. To minimize complexity, Cai et al., (2021) devises smart crime prevention and control big data analysis model on the basis of IoT for detecting the cyber-attacks. The method had elevated rate of data collection and crime avoidance and it effectively controlled the efficiency, but it was complex to analyze the prior faults. To reduce faults, Rajeswari et al., (2021) developed hyper-heuristic model for bi-objective optimization to detect the cyber-attacks. The method contained a low-level heuristics and high-level strategy for solving this issue. The high-level method utilized the search efficiency for controlling and low-level heuristics utilized various rules for SVM configuration. However, this technique limited the passkeys for accessing the details. To access details, Rahaman, (2020) devised a technique considering Hadoop by inspecting the geological zones for cybercrime detection. The method utilized topographical cybercrime mapping algorithm for differentiating the areas, which has elevated cybercrime cases. The available data was not consistent and it made the process more complex. To reduce complexity, Li and He, (2020) developed quantitative analysis technique for detecting the cybercrime and devised mathematical to analyze the behavior of network. A factor space research method was formed with medium scale and factor detection of cybercrime behavior was devised considering neural network. Then, the learning method was devised with factor discovery principle to guide decisions. However, this technique did not differentiate secondary and primary behavior of network. To differentiate primary and secondary behavior, Karimi et al., (2021) devised pseudo-label technique for optimizing the neural network and modelled it to semi-supervised classification. Here, the dataset was splitted into two classes, namely labeled and unlabelled, but it was not clever to control text and images dataset.

2.2. Challenges

The issues tackled by priorly provided cyber-crime detection methodologies are enlisted.

- In (Chhabra et al., 2020), a generalized forensic framework is devised to perform cybercrime detection. However, this methoddid not explore feature selection techniques. Hence, the major issuerelies on maximizing model accuracy.
- To increase accuracy, HDRaNN is devised, which attained effective performance with certain epochs with best rate of learning. However, this method did not select precise rate of learning for implementation (Huma et al., 2021).
- To choose precise learning rate, SFJO-based Deep stacked autoencoder is utilized. However, to accumulate and process large data is a complex task as it surpasses the processing abilities of memory and consumption of time (Venugopal et al., 2021).
- To reduce memory and time, a Semi-Supervised Neural Network is devised in (Karimi et al., 2021) for detecting the cyber crime. It took less time for building the labeled data. However, the main issue is that did not discover the probability of crime prior to its occurrence and this led to performance bottleneck.
- A forensic inspection of IoT with big data contains complex process as devices of IoT are modelled to work in a platform that works passively and autonomously.

3. SYSTEM MODEL

The devices of IoT links the mobile nodes and objects with sensors via internet for initiating the data exchange process. The major aspect employed in IoT routing is efficiency of energy and secure communication. The secured routing and data transmission with advanced services contains a key problem in IoT network. Security of IoT contains in-depth assessment as it needs to preserve network. The forensic expert's skills are in risk to operate with the streaming data in IoT infrastructures. However, the problems, such as different formats of traffic, steganography, anti-forensics, and encrypted data may degrade the efficiency of cyber forensic models. Hence, the motive is to devise an effective cyber forensic model considering IoT platforms. Figure 1 displays the basic IoT model. Here, the IoT model (Dhumane and Prasad, 2019) consists of various sensor nodes and they are linked with wireless network. In addition, the IoT model poses three types of nodes, namely normal nodes, Cluster head (CH) and Global System for Mobile (GSM) tower or Base Station (BS). The normal nodes exchange the accumulated data with its CH and CH are responsible to send data to GSM tower or BS. It comprises one BS E_f, CH N_p and r IoT nodes. The maximum communication radio range of an IoT node is consistently distributed in dimension of G_k and H_k meters. The optimum position of sink node in IoT is given by $\left\{0.5G_k, 0.5H_k\right\}$. The coordinate values of G_l and H_l indicates each IoT node position.

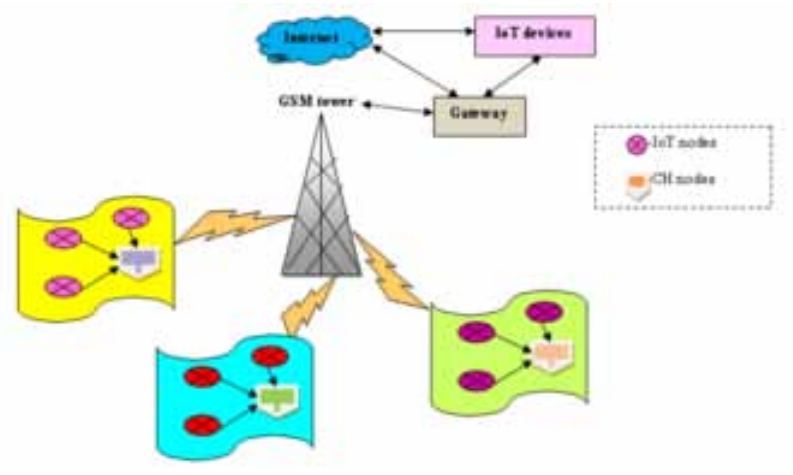
3.1 Energy model

The IoT comprises huge nodes wherein each node is liable to acquire some initial energy which is expressed by D_0, but nodes energy in IoT is not rechargeable (Dhumane and Prasad, 2019). During communication, the information loss can occur. In IoT, each node comprises hardware transmitter and receiver that help in dissipating the energy. Hence, the radio electronics are adapted for measuring the indulgenced energy. The two energy techniques are adapted to evaluate dispersed energy, one represents distance amidst nodes and other indicates nature of nodes that helps to describe if node represents normal or CH. Here, the indulgence of energy considering normal node is given by,

$$F_{emt}\left(E_n^m\right) = F_{ele} * M_Q + F_{pa} * M_Q * \left\| E_n^m - E_s^t \right|^4; If \left| E_n^m - E_s^t \right| \geq j_0 \tag{1}$$

$$F_{emt}\left(E_n^m\right) = F_{ele} * M_Q + F_{fs} * M_Q * \left\| E_n^m - E_s^t \right|^4; If \left| E_n^m - E_s^t \right| < j_0 \tag{2}$$

Figure 1. IoT model



$$j_0 = \sqrt{\frac{F_{fs}}{F_{pa}}} \tag{3}$$

where, F_{fs} represent free space energy, M_Q signifies packet size, F_{pa} express amplification of multipath fading, $\left\| E_n^m - E_s^t \right\|$ refers distance amidst CH and normal node. The electronic energy is producedbecause of electronic units, such as modulator, amplifier, filtering and formula of electronic energy is expressed by,

$$F_{ele} = F_{txr} + F_{DA} \tag{4}$$

where, F_{txr} is energy produced by transmitter, F_{DA} signifies energy produced while aggregating data. When CH node admit M_Q data bytes, then energy dissipation in CH is obtained and is modelled by,

$$F\left(E_s^m\right) = F_{ele} * M_Q \tag{5}$$

After completing broadcast and data reception considering CH, the IoT node energy is rehabilitated with $F_{u+1}\left(E_n^m\right)$ and $F_{u+1}\left(E_s^m\right)$ can be given by,

$$F_{u+1}\left(E_n^m\right) = F_u\left(E_n^m\right) - F_{emt}\left(E_n^m\right) \tag{6}$$

$$F_{u+1}\left(E_s^m\right) = F_u\left(E_s^m\right) - F_{emt}\left(E_s^m\right) \tag{7}$$

The update of energy in node is repeateduntilcomplete nodes in network turns to dead node.

3.2. Routing with FGSA

In IoT, the data routing using optimal route is not simple and owes energy issues, due to limited battery capacities. The energy problem occurred while transmission is mitigated by Fractional Gravitational

search algorithm (FGSA) technique (Dhumane and Prasad, 2019). The FGSA is obtained by combining the benefits of both GSA and fractional theory. The benefit of choosing effectual path is to minimize the energy and delay that improves lifetime of network. Here, selection of CH is done using FGSA for attaining effective routing. While sending data, the communication is achieved by optimum path by reducing the user of nodal power. The update expression obtained with FGSA is given by,

$$K_w^v\left(x+1\right) = DK_w^v\left(x\right) + \frac{1}{2}XK_w^v\left(x-1\right) + y_w^v\left(x+1\right) \tag{8}$$

where, $K_w^v\left(x+1\right)$ symbolize agent w location in v^{th} cluster at time $x+1$, $K_w^v\left(x\right)$ refers w^{th} agent location at current iteration x, and $K_w^v\left(x-1\right)$ symbolize agent w location in prior iteration, and $y_w^v\left(x+1\right)$ symbolize velocity computed by GSA in $(x+1)^{th}$ iteration considering agent w location in v^{th} cluster at time. Hence, the best paths are chosenwith FGSA for exchanging the accumulated data. The acquired data through optimum multipath is expressed by T.

4. MSSO-BASED DNFN FOR CYBERCRIME DISCOVERY IN IOT USING BIG DATA

Cybercrime uses network as tool to initiate crime. The multiple cybercrime area has broadened from easier credential risks to geopolitical risks. Moreover, the cyber-attacks in IoT devices tend to be increasing and caused various threats. Thus, the goal is to present effective method for cybercrime discovery with big data considering IoT using MSSO-based DNFN. Initially, the nodes are simulated in IoT and these nodes are responsible for collecting information. After that, routing process is accomplished by transferring the sensed data to the BS using FGSA (Dhumane and Prasad, 2019). Then the cybercrime detection is carried out at the BS using following steps: At first, the input data are acquired from the specific dataset (UCSD Network Telescope Aggregrated DDoS Metadata) and is forwarded to the MapReduce framework, which consists of two phases namely mapper phase and reducer phase. At the mapper phase, feature selection process is done for selecting the significant features using mutual information, whereas malware detection is performed at the reducer phase using DNFN (Javaid et al., 2019). Furthermore, the network classifier is trained with MSSO. Here, the MSSO is devised by combining MA (Zervoudakis and Tsafarakis, 2020) and SSOA (Kaveh and Zaerreza, 2020). Figure 2 reveals structure of the cybercrime detection model using proposed MSSO-based DNFN.

4.1. Acquisition of Data

Assume a database J having various number of data samples, and is given by,

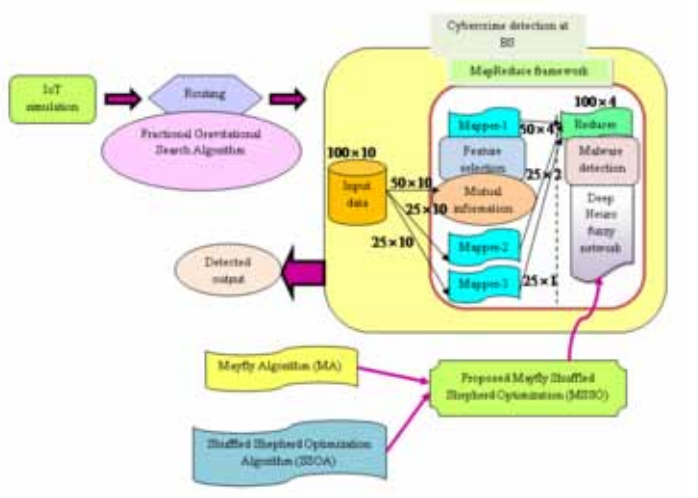
$$J = \left\{S_1, S_2, \ldots S_o, \ldots, S_z\right\} \tag{9}$$

where, z symbolize total number of data, and S_o signifies o^{th} data. Assume each data is of 100×10 dimension.

4.2. MapReduce Framework for Cybercrime Detection in IoT

MapReduce model represents programming technique, which consists of mapper and reducer. It performs cybercrime detection by operating the data in parallel. Hence, it helps to manage huge-scale data with MapReduce by sharing process amongst mappers and reducers. Here, the feature selection

Figure 2. Structure of proposed MSSO-based DNFN for Cybercrime detection in IoT



is done in mapper while the cyber crime detection is done in reducer. The input data S_o is fed to MapReduce model wherein the accumulated input data is divided into a specific number, which is equivalent to the total count of mappers.Figure 3 depicts the MapReduce model for cybercrime detection in IoT.

4.2.1. Mapper phase

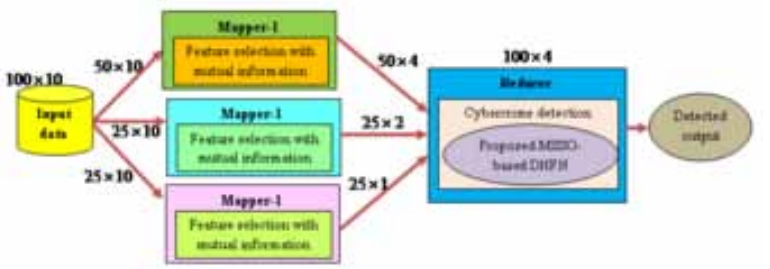
In mapper phase, the selection of imperative features is carried out. The feature selection is an imperative process for attaining effectual outcomes and it helps to deal with huge data.

4.2.1.1. Choosing significant feature with mutual information using mappers

The feature selection is carried out with mutual information (MI). The MI(Learned-Miller, 2013) assists in computing the data wherein one variable depends on other. Moreover, the information theory states that MI amidst two attributes is zero if two features are sovereign. The MI evaluates the relation amidst features that are sampled simultaneously. Here, the partitioned data obtained from input data S_o with dimension 100×10 is expressed as,

$$S_o = \left\{ \ell_\kappa \right\}; 1 \le \kappa \le \vartheta \tag{10}$$

Figure 3. MapReduce model for cybercrime detection in IoT



where, ϑ refers total mappers. Assume ϑ mappers be given by,

$$I = \left\{I_1, I_2, \ldots, I_\kappa, \ldots, I_\vartheta\right\}; 1 \le \kappa \le \vartheta \tag{11}$$

Thus, input to κ^{th} mapper are given by,

$$\ell_\kappa = \left\{q_{h,i}\right\}; 1 \le h \le \rho_\kappa; 1 \le i \le \upsilon \tag{12}$$

where, $q_{h,i}$ refers partitioned data provided to κ^{th} mapper to perform feature selection, and ρ_κ refers count of data in κ^{th} mapper. Each partitioned data is of dimension 50×10, 25×10, and 25×10 respectively. The MI is adapted to choose imperative features with the partitioned data $q_{h,i}$. The MI amidst feature O and target L whose joint distribution is given by $P\left(O, L\right)$ is formulated by,

$$MI\left(O, L\right) = \sum\nolimits_{L \in U} \sum\nolimits_{O \in V} P_{O,L}\left(U, V\right) \log \frac{P_{(O,L)}\left(U, V\right)}{P_O\left(U\right).P_L\left(V\right)} \tag{13}$$

where, $P_{(O,L)}\left(U, V\right)$ signifies joint probability mass function of O, and L, P_O and P_L refers marginal probability mass function, O is feature and L symbolize target. After computing mutual information amidst feature, it chooses top "m" features having highest MI value. The features chosen with MI is expressed as C which is of dimension 50×4, 25×2, and 25×1 and is given as an input to reducer which is denoted as I and is of dimension 100×4.

4.2.2. Reducer Phase

In reducer phase, the cyber crime detection is done with proposed MSSO-based DNFN considering reducer I. Here, the DNFN training is done considering proposed MSSO, and is obtained by unifying benefits of both SSOA and MA. The DNFN structure and training steps of proposed MSSO is explained below.

4.2.2.1. DNFN Structure

DNFN (Javaid et al., 2019) is the hybridization of fuzzy principle in deep neural network (DNN) and it is extensively adapted to offer effective optimization considering the less cost. Here, the DNN is employed as first phase, whereas fuzzy standard is used in second stage for estimating the needs of model. The DNFN poses three layers, namely hidden, input and output layer. Figure 4 reveals DNFN structure.

Each input or output is spotlighted using specific rate and input sent to DNFN is selected features, which is expressed as C. Here, the feature selected is fed to determine output which is either malware detected or no malware. Consider there exist two premises such as α and β, and one consequent χ, which are defined by,

$$I_{1,l} = \gamma.\hbar_l\left(\alpha\right) or I_{1,l} = \gamma\varpi_{l-2}\left(\upsilon\right), \forall l = 1, 2, 3, 4 \tag{14}$$

Here, α and β indicates inputs to individual l^{th} entity, $\gamma.\hbar_l$ and $\gamma\varpi_{l-2}$ is antecedent membership functions, whereas $I_{1,l}$ refers degree of membership.

$$\gamma\hbar_l\left(\alpha\right)=\frac{1}{1+\left|\frac{\alpha-\lambda_l}{\kappa_l}\right|2\tau_l} \tag{15}$$

where, τ_l, λ_l, and κ_l express membership outcomes of premise attributeswhich are optimized with training. Thus, values of membership deliberates strength of firing, and is formulated by,

$$I_{2,l}=\zeta_l=\gamma\hbar_l\left(\alpha\right)\gamma\varpi_{l-2}\left(\beta\right),\forall l=1,2 \tag{16}$$

Layer 3 refers normalization layer. ζ_l express generic network factor. The output of rule is modelled by,

$$I_{3,l}=\overline{\zeta}_l\varepsilon_l=\overline{\zeta}_l\left(\psi_l\alpha+\xi_l\beta+\omega_l\right),\forall l=1,2 \tag{17}$$

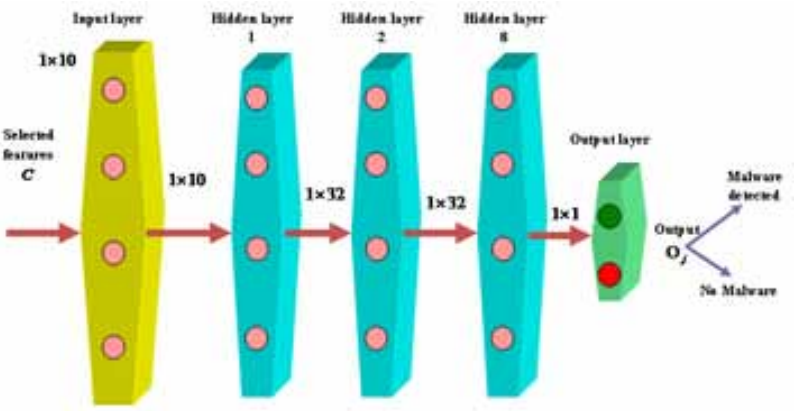
Here, ψ, ξ, and ω deliberates group of consequent aspects. Then, last layer is supposed as summation, and itexpress total number of previous outputs of layer. The final output is expressedby,

$$\mathrm{O}_j=I_{4,l}=\sum_l\overline{\zeta}_l\varepsilon_l=\frac{\sum_l\zeta_l\varepsilon_l}{\sum_l\varepsilon_l} \tag{18}$$

4.2.2.2. DNFN Training with MSSO

The DNFN training is done using MSSO, and produced by blending benefits ofSSOA and MA. The MA (Zervoudakis & Tsafarakis, 2020) is inspired from the behavior of mayfly mating. The convergence

Figure 4. DNFN Structure



rate and convergence speed tend to be better. The random flight and nuptial dance assists to offer improved balance amidst exploitation and exploration and assists to run away from local optima. Meanwhile, the SSOA (Kaveh and Zaerreza, 2020) is inspired from the shepherd behavior. It poses the ability to discover best solution with little assessment. Moreover, the optimization issues and engineering design issues can be handled by SSOA. Hence, the hybridization of SSOA and MA aids to augment overall rate of performance. The MSSO steps are enlisted below.

i) Initialization:

Initially, two mayfly's sets are randomly generated by modeling male and female population. Every mayfly is randomly located in d -dimensional vector $B = \left(B_1,\ldots,B_d\right)$ and its effectiveness is calculated on particular fitness function $f\left(B\right)$. The velocity $C = \left(C_1,\ldots,C_d\right)$ of mayfly is defined as location variation and flying direction. The personal best position is denoted by pb and global best position is expressed as gb.

ii) Find error:

The error amidst each solution is determined for attaining best solution and formulated as,

$$MSE = \frac{1}{o}\left[\sum\nolimits_{z=1}^{o} \ell_z - \mathrm{O}_j\right] \tag{19}$$

where, ℓ_z deliberates output estimated and O_j is DNFN output, and o express total data.

iii) Male mayfly's progress:

As per MA (Zervoudakis & Tsafarakis, 2020), the position of male mayfly is changed with its own experience and its experience of neighbor's. Assume B_a^y is present position of a^{th} mayfly on search space at iteration y and position is altered by summing velocity C_a^{y+1} to present position and provided as,

$$B_a\left(y+1\right) = B_a\left(y\right) + C_a\left(y+1\right) \tag{20}$$

The male mayfly velocity is expressed by,

$$C_a\left(y+1\right) = C_a\left(y\right) + b_1 e^{-\beta r_p^2}\left(pb_a - B_a\left(y\right)\right) + b_2 e^{-\beta r_g^2}\left(gb_a - B_a\left(y\right)\right) \tag{21}$$

where, $C_a\left(y\right)$ is velocity of a^{th} mayfly at iteration y, $B_a\left(y\right)$ refers present mayfly position, b_1, b_2 is positive attraction constants, pb_a refers personal best solution of a^{th} mayfly, and gb_a signifies global best solution of a^{th} mayfly.

Thus, the personal best solution is expressed as,

$$pb_a = \begin{cases} B_a\left(y+1\right); Iff\left(B_a\left(y+1\right)\right) < f\left(pb_a\right) \\ keptsameOtherwise; \end{cases} \tag{22}$$

The global best solution is expressed as,

$$gb \in \left\{pb_1, pb_2, \ldots, pb_N \mid f\left(cb\right)\right\} = \min\left\{f\left(pb_1\right), f\left(pb_2\right), \ldots, f\left(pb_N\right)\right\} \tag{23}$$

where, N is total mayflies.

The distance is expressed as,

$$\left\|c_a - B_a\right\| = \sqrt{\sum_{v=1}^{n}\left(c_{a,v} - B_{a,v}\right)^2} \tag{24}$$

where, $c_{a,v}$ is v^{th} element of mayfly a, and B_a refers linked to pb_a or gb.

The optimum mayflies keep changing its velocity, and is expressed by,

$$C_{a,v}\left(y+1\right) = C_{a,v}\left(y\right) + e * \nu \tag{25}$$

where, e refers nuptial dance coefficient, and ν signifies arbitrary number amidst $\left[-1,1\right]$.

By substituting equation (21) in (20),

$$B_a\left(y+1\right) = B_a\left(y\right) + C_a\left(y\right) + b_1 e^{-\beta r_p^2}\left(pb_a - B_a\left(y\right)\right) + b_2 e^{-\beta r_g^2}\left(gb_a - B_a\left(y\right)\right) \tag{26}$$

$$B_a\left(y+1\right) = B_a\left(y\right) + C_a\left(y\right) + b_1 e^{-\beta r_p^2} pb_a - b_1 e^{-\beta r_p^2} B_a\left(y\right) + b_2 e^{-\beta r_g^2} gb_a - b_2 e^{-\beta r_g^2} B_a\left(y\right) \tag{27}$$

$$B_a\left(y+1\right) = B_a\left(y\right)\left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right] + C_a\left(y\right) + b_1 e^{-\beta r_p^2} pb_a + b_2 e^{-\beta r_g^2} gb_a \tag{28}$$

The SSOA assist to acquire the best values rapidly. According to SSOA (Kaveh and Zaerreza, 2020), the equation is expressed as,

$$B_a^{temple} = B_a^{old} + \Delta_a \tag{29}$$

where, Δ_a refers step size. Assume $B_a\left(y+1\right) = B_a^{temple}$ and $B_a\left(y\right) = B_a^{old}$

$$B_a\left(y+1\right) = B_a\left(y\right) + \Delta_a \tag{30}$$

where, $B_a\left(y+1\right)$ symbolize position of a^{th} solution at iteration $\left(y+1\right)$, $B_g\left(y\right)$ and $B_o\left(y\right)$ is solution vectors at iteration $\left(y+1\right)$, $rand$ signifies random number between (0,1).

The step size is formulated by,

$$\Delta_a = R \times rand \circ \left(B_g\left(y\right) - B_a\left(y\right)\right) + Y \times rand \circ \left(B_o\left(y\right) - B_a\left(y\right)\right) \quad (31)$$

Here, R is given by,

$$R = R_0 - \frac{R_0}{\max iter} \times iter \quad (32)$$

Here, Y is given by,

$$Y = Y_0 + \frac{Y0_{max}}{\max iter} \quad (33)$$

After substituting step size Δ_a value, the equation becomes,

$$B_a\left(y+1\right) = B_a\left(y\right) + R \times rand \circ \left(B_g\left(y\right) - B_a\left(y\right)\right) + Y \times rand \circ \left(B_o\left(y\right) - B_a\left(y\right)\right) \quad (34)$$

$$B_a\left(y+1\right) = B_a\left(y\right) + R \times rand \circ B_g\left(y\right) - R \times rand \circ B_a\left(y\right) + Y \times rand \circ B_o\left(y\right) - Y \times rand \circ B_a\left(y\right) \quad (35)$$

$$B_a\left(y+1\right) = B_a\left(y\right)\left[1 - R \times rand - Y \times rand\right] + R \times rand \circ B_g\left(y\right) + Y \times rand \circ B_o\left(y\right) \quad (36)$$

$$B_a\left(y\right) = \frac{B_a\left(y+1\right) - rand\left(R \circ B_g\left(y\right) + Y \circ B_o\left(y\right)\right)}{\left[1 - R \times rand - Y \times rand\right]} \quad (37)$$

Substitute equation (37) in equation (28),

$$B_a(y+1) = \left[\frac{B_a(y+1) - rand\left(R \circ B_g(y) + Y \circ B_o(y)\right)}{\left[1 - R \times rand - Y \times rand\right]}\right]\left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right] + C_a(y) + b_1 e^{-\beta r_p^2} pb_a + b_2 e^{-\beta r_g^2} gb_a \quad (38)$$

$$B_a(y+1) = \frac{B_a(y+1)}{\left[1 - R \times rand - Y \times rand\right]}\left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right] - \frac{rand\left(R \circ B_g(y) + Y \circ B_o(y)\right)}{\left[1 - R \times rand - Y \times rand\right]}\left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right] + C_a(y) + b_1 e^{-\beta r_p^2} pb_a + b_2 e^{-\beta r_g^2} gb_a \quad (39)$$

$$B_a(y+1) - \frac{B_a(y+1)}{\left[1 - R \times rand - Y \times rand\right]}\left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right] = -\frac{rand\left(R \circ B_g(y) + Y \circ B_o(y)\right)}{\left[1 - R \times rand - Y \times rand\right]}\left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right] + C_a(y) + b_1 e^{-\beta r_p^2} pb_a + b_2 e^{-\beta r_g^2} gb_a \quad (40)$$

$$B_a(y+1)\left(1 - \frac{\left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right]}{\left[1 - R \times rand - Y \times rand\right]}\right) = -\frac{rand\left(R \circ B_g(y) + Y \circ B_o(y)\right)}{\left[1 - R \times rand - Y \times rand\right]}\left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right] + C_a(y) + b_1 e^{-\beta r_p^2} pb_a + b_2 e^{-\beta r_g^2} gb_a \quad (41)$$

$$B_a(y+1)\left(\frac{1-R\times rand-Y\times rand-\left[1-b_1e^{-\beta r_p^2}-b_2e^{-\beta r_g^2}\right]}{\left[1-R\times rand-Y\times rand\right]}\right)=$$
$$-\frac{rand\left(R\circ B_g(y)+Y\circ B_o(y)\right)}{\left[1-R\times rand-Y\times rand\right]}\left[1-b_1e^{-\beta r_p^2}-b_2e^{-\beta r_g^2}\right] \tag{42}$$
$$+C_a(y)+b_1e^{-\beta r_p^2}pb_a+b_2e^{-\beta r_g^2}gb_a$$

$$B_a(y+1)\left(\frac{1-R\times rand-Y\times rand-1+b_1e^{-\beta r_p^2}+b_2e^{-\beta r_g^2}}{\left[1-R\times rand-Y\times rand\right]}\right)=-\frac{rand\left(R\circ B_g(y)+Y\circ B_o(y)\right)}{\left[1-R\times rand-Y\times rand\right]} \tag{43}$$
$$\left[1-b_1e^{-\beta r_p^2}-b_2e^{-\beta r_g^2}\right]+C_a(y)+b_1e^{-\beta r_p^2}pb_a+b_2e^{-\beta r_g^2}gb_a$$

$$B_a(y+1)\left(\frac{-R\times rand-Y\times rand+b_1e^{-\beta r_p^2}+b_2e^{-\beta r_g^2}}{\left[1-R\times rand-Y\times rand\right]}\right)=-\frac{rand\left(R\circ B_g(y)+Y\circ B_o(y)\right)}{\left[1-R\times rand-Y\times rand\right]} \tag{44}$$
$$\left[1-b_1e^{-\beta r_p^2}-b_2e^{-\beta r_g^2}\right]+C_a(y)+b_1e^{-\beta r_p^2}pb_a+b_2e^{-\beta r_g^2}gb_a$$

$$B_a\left(y+1\right)=\frac{\left[1-R\times rand-Y\times rand\right]}{-R\times rand-Y\times rand+b_1e^{-\beta r_p^2}+b_2e^{-\beta r_g^2}}\left[\begin{array}{c}-\frac{rand\left(R\circ B_g\left(y\right)+Y\circ B_o\left(y\right)\right)}{\left[1-R\times rand-Y\times rand\right]}\left[1-b_1e^{-\beta r_p^2}-b_2e^{-\beta r_g^2}\right]\\ +C_a\left(y\right)+b_1e^{-\beta r_p^2}pb_a+b_2e^{-\beta r_g^2}gb_a\end{array}\right] \tag{45}$$

The final MSSO update is given by,

$$B_a\left(y+1\right)=\frac{\left[1-R\times rand-Y\times rand\right]}{b_1e^{-\beta r_p^2}+b_2e^{-\beta r_g^2}-R\times rand-Y\times rand}\left[\begin{array}{c}C_a\left(y\right)+b_1e^{-\beta r_p^2}pb_a+b_2e^{-\beta r_g^2}gb_a\\ -\frac{rand\left(R\circ B_g\left(y\right)+Y\circ B_o\left(y\right)\right)}{\left[1-R\times rand-Y\times rand\right]}\left[1-b_1e^{-\beta r_p^2}-b_2e^{-\beta r_g^2}\right]\end{array}\right] \tag{46}$$

iv) Female mayfly's progress:

The female mayflies do not collect in swarms. It flies in breeding direction. Assume δ_a^y is current female mayfly position of a at time y and location is altered by changing velocity C_a^{y+1} to present position, and is expressedas,

$$\delta_a^{y+1}=\delta_a^y+C_a^{y+1} \tag{47}$$

Hence, velocity is represented by,

$$C_{a,v}^{y+1}=\begin{cases}C_{a,v}^y+b_2e^{-\beta r_{mf}^2}\left(B_{a,v}^y-S_{a,v}^y\right);Iff\left(S_a\right)>f\left(B_a\right)\\ C_{a,v}^y+fl*\nu;Iff\left(S_a\right)\le f\left(B_a\right)\end{cases} \tag{48}$$

where, β refers visibility coefficient, r_{mf} express Cartesian distance amongst male and female mayfly, fl is random walk, and ν signifies arbitrary value amidst [-1, 1].

v) Mayflies Mating:

Crossover operator expresses procedure of mating amidst two mayflies. The crossover is expressed by,

$$offspring1 = \mathfrak{R} * male + \left(1 - \mathfrak{R}\right) * female \tag{49}$$

$$offspring \rightleftarrows 2 = \mathfrak{R} * female + \left(1 - \mathfrak{R}\right) * male \tag{50}$$

where, $male$ is male parent, $female$ deliberates female parent, $\mathfrak{R}$ refers random value.

vi) Find feasibility:

The error is found and solution generating less error is chosen as optimum solution.

vii) Termination:

The above steps are continueduntiloptimum solution is produced. Table 1examines pseudo code of MSSO.

Hence, the output of MSSO-based DNFN is cybercrime detection output, which is denoted by O_j.

Table 1. Pseudo code of MSSO

Sl. No	Pseudo code of MSSO
1	**Input:**Mayfly Population B
2	**Output:** $B*$
3	Initialize male and female mayfly population
4	Estimate error with equation (19)
5	Find gb with equation (23)
6	**Do**
7	**While stopping criteria is not met**
8	Update male and female mayflies solution with equation (46) and (47)
9	Mate mayflies
10	Estimate offspring with equation (49) and (50)
11	Estimate feasibility with error using equation (19)
12	**End while**

5. RESULTS AND DISCUSSION

The proficiency of MSSO+DNFN is defined with precision, F-measure, and recall. The assessment is performed by altering data of training.

5.1. Experimental Set-Up

The functioning of MSSO+DNFN is done in Python considering PC with Windows 10 OS, Intel i3 core processor and 8GB RAM.

5.2. Dataset Description

The assessment is performed with UCSD Network Telescope Aggregated DDoS Metadata (UCSD Network Telescope Aggregrated DDoS Metadata). This dataset indicates the activities of DDoS and is noted by through the UCSD Network Telescope. It is collected through raw Telescope data with the criterions defined in Internet Denial-of-Service based activities.

5.3. Evaluation Metrics

The efficacy of MSSO+DNFN is evaluatedconsideringvariousmetrics.

5.3.1 Precision

It referred nearness degree of several dimensions amidst each other, and formulated as,

$$P_r = \frac{\ell_p}{\ell_p + \eta_p} \tag{51}$$

where, ℓ_p refers true positive, and η_p is false positive.

5.3.2 Recall

It evaluates actual positives in which model attains true positive label and is expressed by,

$$R_e = \frac{\ell_p}{\ell_p + \eta_f} \tag{52}$$

where, η_f is false negative.

5.3.3 F-measure

It specifies harmonic mean amongst recall and precision, and formulated as,

$$F_m = 2 \times \left(\frac{P_r * R_e}{P_r + R_e} \right) \tag{53}$$

5.4. Performance Assessment

Figure 5 depicts evaluation of MSSO+DNFN by altering data of training and is inspectedwith certain metrics. The precision investigation is portrayed in figure 5a). For 60% data, the precision evaluated by MSSO+DNFN with iteration 5, 10, 15, 20 are 0.817, 0.821, 0.825, and 0.829. Besides, for 90%

data, the precision evaluated by MSSO+DNFN with iteration 5, 10, 15, 20 are 0.921, 0.923, 0.929, and 0.933. The recall investigation is portrayed in figure 5b). For 60% data, the recall evaluated by MSSO+DNFN with iteration 5, 10, 15, 20 are 0.852, 0.856, 0.861, and 0.867. Besides, for 90% data, the recall evaluated by MSSO+DNFN with iteration 5, 10, 15, 20 are 0.946, 0.950, 0.954, and 0.957. The F-measure investigation is portrayed in figure 5c). For 60% data, the F-measure evaluated by MSSO+DNFN with iteration 5, 10, 15, 20 are 0.775, 0.778, 0.782, and 0.786. Besides, for 90% data, the F-measure evaluated by MSSO+DNFN with iteration 5, 10, 15, 20 are 0.907, 0.913, 0.916, and 0.921.

5.5. Algorithm Utilized

The algorithms used for the assessment includes ChoA+DNFN, MA+DNFN, SSOA+DNFN, and proposed MSSO+DNFN.

5.6. Algorithm Assessment

The evaluation of algorithms by changing population size is inspected with certain metrics and is expressed in Figure 6. The precision analysis is explained in figure 6a). Considering population size=5, the precision obtained by ChoA+DNFN is 0.893, MA+DNFN is 0.896, SSOA+DNFN is0.900, and MSSO+DNFN is0.905. Similarly, for population size=20, the precision obtained by

Figure 5. Assessment of MSSO+DNFN with a) Precision b) Recall c) F-measure

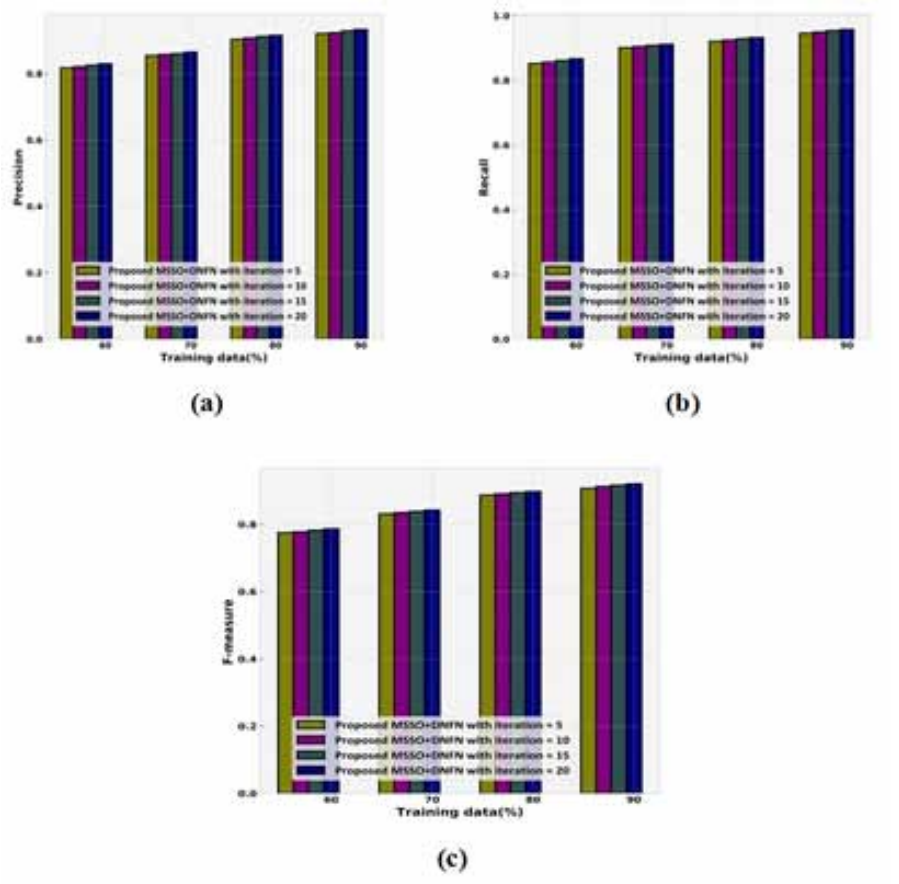
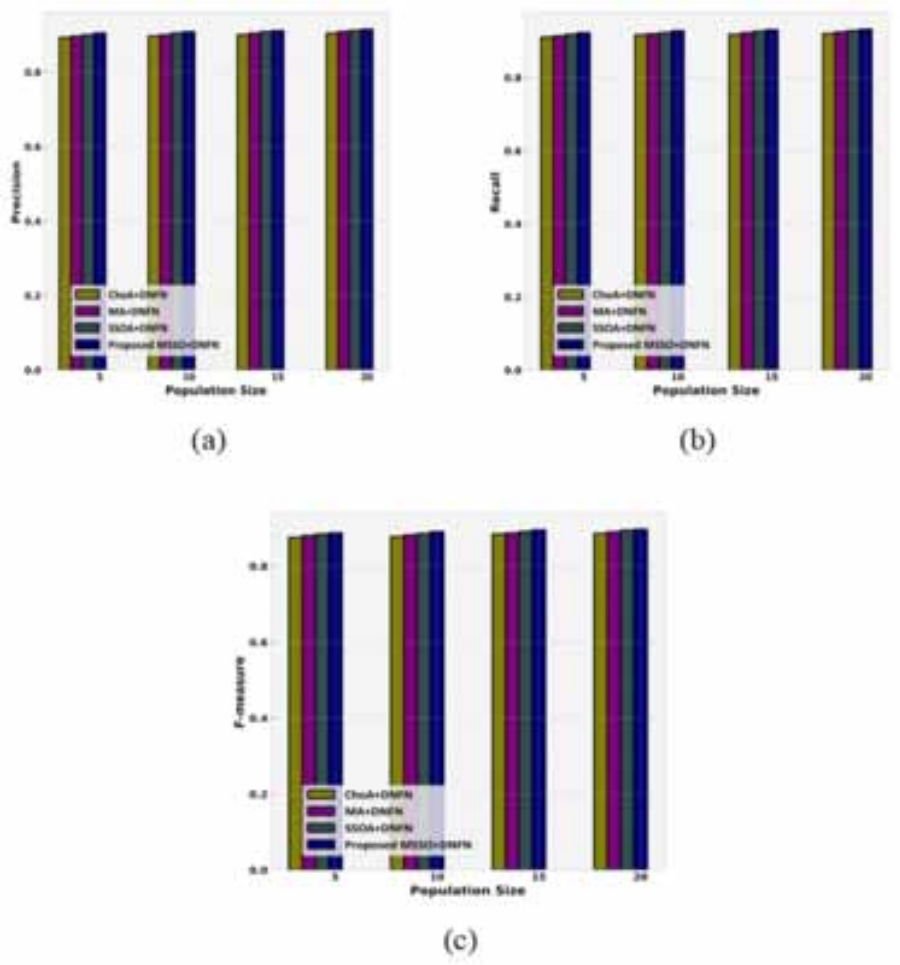
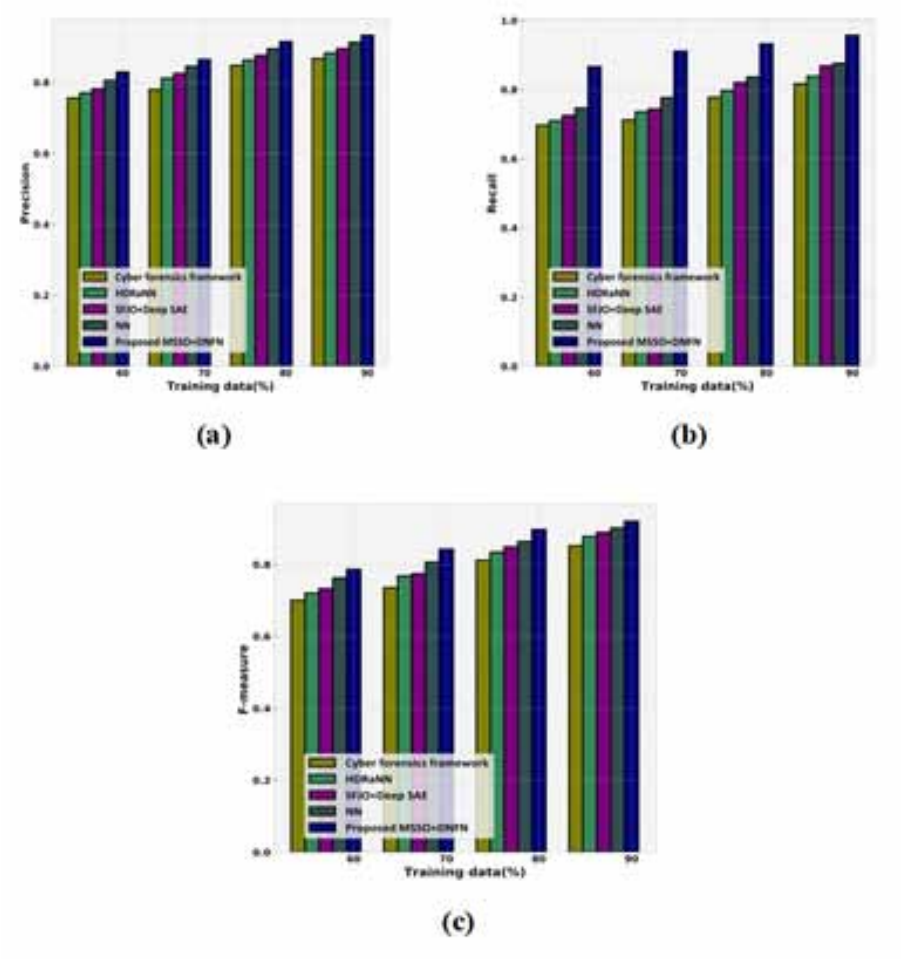


Figure 6. Assessment of algorithms with DNFN with a) Precision b) Recall c) F-measure



ChoA+DNFN is 0.905, MA+DNFN is 0.909, SSOA+DNFN is 0.912, and MSSO+DNFN is 0.915. The efficiency of Cyber forensics framework, HDRaNN, SFJO+Deep SAE, NN in contrast to proposed MSSO+DNFN using precision is 1.092%, 0.655%, 0.327%. The recall analysis is portrayed in figure 6b). For population size=5, the recall evaluated by ChoA+DNFN is 0.911, MA+DNFN is 0.914, SSOA+DNFN is 0.918, and MSSO+DNFN is 0.923. Similarly, considering population size=20, the recall evaluated by ChoA+DNFN is 0.920, MA+DNFN is 0.925, SSOA+DNFN is 0.928, and MSSO+DNFN is 0.932. The efficiency of Cyber forensics framework, HDRaNN, SFJO+Deep SAE, NN in contrast to proposed MSSO+DNFN using recall is 1.287%, 0.751%, 0.429%. The F-measure analysis is portrayed in figure 6c). Considering population size=5, the F-measure evaluated by ChoA+DNFN is 0.876, MA+DNFN is 0.881, SSOA+DNFN is 0.885, and MSSO+DNFN is 0.888. Similarly, considering population size=20, the F-measure evaluated by ChoA+DNFN is 0.887, MA+DNFN is 0.891, SSOA+DNFN is 0.895, and MSSO+DNFN is 0.897. The efficiency of Cyber forensics framework, HDRaNN, SFJO+Deep SAE, NN in contrast to MSSO+DNFN using F-measure is 1.114%, 0.668%, and 0.222%.

Figure 7. Assessment of techniques with a) Precision b) Recall c) F-measure



5.7. Comparative Methods

The techniques considered for assessment involves Cyber forensics framework (Chhabra et al., 2020), HDRaNN (Huma et al., 2021), SFJO+Deep SAE (Venugopal et al., 2021), NN (Karimi et al., 2021), and proposed MSSO+DNFN.

5.8. Comparative Analysis

The valuation of techniques by changing data of training is inspected in figure 7. The precision assessment is explained in figure 7a). With 60% data, the precision obtained by Cyber forensics framework, HDRaNN, SFJO+Deep SAE, NN are 0.756, 0.770, 0.782, 0.806whereas proposed MSSO+DNFN is0.829. As well, for 90% data, the precision obtained by Cyber forensics framework, HDRaNN, SFJO+Deep SAE, NN are 0.867, 0.883, 0.895, 0.913, whereas proposed MSSO+DNFN is0.933. The efficiency of Cyber forensics framework, HDRaNN, SFJO+Deep SAE, NN in contrast to proposed MSSO+DNFN using precision is 7.073%, 5.359%, 4.072%, 2.143%. The recall assessment is portrayed in figure 7b). For 60% data, the recall obtained by Cyber forensics framework, HDRaNN, SFJO+Deep SAE, NN are 0.697, 0.710, 0.725, 0.747, whereas proposed MSSO+DNFN is0.867. As well, for 90% data, the recall obtained by Cyber forensics framework, HDRaNN, SFJO+Deep SAE,

NN are 0.817, 0.839, 0.869, 0.876, whereas proposed MSSO+DNFN is0.957. The efficiency of Cyber forensics framework, HDRaNN, SFJO+Deep SAE, NN in contrast to proposed MSSO+DNFNusing recall is 14.629%, 12.330%, 9.195%, 8.463%. The F-measure assessment is portrayed in figure 7c). For 60% data, the F-measure obtained by Cyber forensics framework, HDRaNN, SFJO+Deep SAE, NN are 0.700, 0.720, 0.733, 0.763, whereas proposed MSSO+DNFN is0.786. As well, for 90% data, the F-measure obtained by Cyber forensics framework, HDRaNN, SFJO+Deep SAE, NN are0.852, 0.878, 0.889, 0.901, whereas proposed MSSO+DNFN is0.921. The efficiency of Cyber forensics framework, HDRaNN, SFJO+Deep SAE, NN in contrast to proposed MSSO+DNFNusing F-measure is 7.491%, 4.668%, 3.474%, 2.171%.

5.9. Comparative Discussion

The assessment of techniques is done with algorithms considering DNFN and techniques using F-measure, recall and precision.

a) Assessment with algorithms

Table 2 exposes algorithms assessment with DNFN using certain measures. The utmost precision of 0.915 is produced by proposed MSSO+DNFN whereas precision of ChoA+DNFN, MA+DNFN, and SSOA+DNFN are 0.905, 0.909, and 0.912. The utmost recall of 0.932 is produced by proposed MSSO+DNFN whereas recall of ChoA+DNFN, MA+DNFN, and SSOA+DNFN is 0.920, 0.925, and 0.928. The utmost F-measure of 0.897 is produced by proposed MSSO+DNFN whereas F-measure of ChoA+DNFN, MA+DNFN, and SSOA+DNFN are 0.887, 0.891, and 0.895.

b) Assessment with techniques

Table 3 presents techniques assessment using certain measures. The utmost precision of 0.933 is produced by MSSO+DNFN, whereas precision of Cyber forensics framework, HDRaNN, SFJO+Deep SAE, NN are 0.867, 0.883, 0.895, and 0.913. The utmost recall of 0.957 is produced by MSSO+DNFN, whereas recall of Cyber forensics framework, HDRaNN, SFJO+Deep SAE, NN is 0.817, 0.839, 0.869, and 0.876. The utmost F-measure of 0.921 is produced by MSSO+DNFN whereas F-measure of Cyber forensics framework, HDRaNN, SFJO+Deep SAE, NN are 0.852, 0.878, 0.889, and 0.901.

Table 2. Assessment of algorithms with DNFN

Metrics	ChoA+DNFN	MA+DNFN	SSOA+DNFN	Proposed MSSO+DNFN
Precision	0.905	0.909	0.912	**0.915**
Recall	0.920	0.925	0.928	**0.932**
F-measure	0.887	0.891	0.895	**0.897**

Table 3. Assessment of techniques

Metrics	Cyber forensics framework	HDRaNN	SFJO+Deep SAE	NN	Proposed MSSO+DNFN
Precision	0.867	0.883	0.895	0.913	**0.933**
Recall	0.817	0.839	0.869	0.876	**0.957**
F-measure	0.852	0.878	0.889	0.901	**0.921**

6. CONCLUSION

The huge count of organizations using IoT devices has contributed to an elevation in size, frequency, and severity of cyber-attacks against IoT and hence creates an arms race amidst the attackers and defenders. Here, a modified DNFN is devised for detecting the cyber-attacks in IoT over the network traffic. The model had showed successful adaption of deep model to cyber security and developed and executed the model for detecting the malware in distributed IoT model. The routing in IoT is performed with FGSA to transmit the collected data to BS and perform cybercrime detection at BSusing proposed MSSO-DNFN. The DNFN training is done with proposed MSSO wherein the optimal tuning of DNFN weights is performed. In addition, the method poses the ability to offer a detailed structure to improve the transparency of developed model. The experiment has deliberated that the malware detection can better discover the cyber-attacks compared to previous algorithms due to sharing of attributes that can prevent local minima. The proposed MSSO-based DNFN granted better efficiency with utmost precision of 93.3%, recall of 95.7% and F-measure of 92.1%.The future work involves the inclusion of other advanced datasets to validate flexibility of designed tactic.

REFERENCES

Aljawarneha, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science*, *25*, 152–160.

Cai, Y., Li, D., & Wang, Y. (2021). Intelligent crime prevention and control big data analysis system based on imaging and capsule network model. *Neural Processing Letters*, *53*(4), 2485–2499.

Chhabra, G. S., Singh, V. P., & Singh, M. (2020). Cyber forensics framework for big data analytics in IoT environment using machine learning. *Multimedia Tools and Applications*, *79*(23), 15881–15900.

Dhumane, A. V., & Prasad, R. S. (2019). Multi-objective fractional gravitational search algorithm for energy efficient routing in IoT. *Wireless Networks*, *25*(1), 399–413.

Fahdi, M.A., Clarke, N.L and Furnell, S.M. (2013). Challenges to digital forensics: A survey of researchers &practitioners attitudes and opinions. In *Information Security for South Africa, 1-8.*

Guarino, A. (2013). Digital forensics as a big data challenge. In ISSE securing electronic business processes, 197-203, Springer.

Huma, Z. E., Latif, S., Ahmad, J., Idress, Z., Ibrar, A., Zou, Z., Alqahanti, F., & Baothman, F. (2021). A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things. *IEEE Access: Practical Innovations, Open Solutions*, *9*, 55595–55605.

Javaid, S., Abdullah, M., Javaid, N., Sultana, T., Ahmed, J & Sattar, N.A. (2019). Towards Buildings Energy Management: Using Seasonal Schedules Under Time of Use Pricing Tariff via Deep Neuro-Fuzzy Optimizer, In *15th International Wireless Communications & Mobile Computing Conference (IWCMC),* 1594-1599.

Karimi, A., Abbasabadei, S., Torkestani, J. A., & Zarafshan, F. (2021). Cybercrime Detection Using Semi-Supervised Neural Network. *Computer Science Journal of Moldova*, *86*(2), 155–183.

Kaveh, A., & Zaerreza, A. (2020). Shuffled shepherd optimization method: A new meta-heuristic algorithm. *Engineering Computations*.

Learned-Miller, E. G. (2013). *Entropy and mutual information*. Department of Computer Science, University of Massachusetts.

Li, J., & He, P. (2020). Detection and Prevention of Cyber Crime Based on Diamond Factor Neural Network. *Journal of Physics: Conference Series*, *1437*(1), 012011.

Liu, B., Blaschy, E., Chenz, Y., Shen, D and Chen, G. (2013). Scalable sentiment classification for big data analysis using naive bayes classifier. In *international conference on big data,* 99-104. IEEE .

Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J. D., Ochoa, M., Tippenhauer, N. O., & Elovici, Y. (2017). ProfilIoT: A machine learning approach for IoT device identification based on network traffic analysis. In *Proceedings of the symposium on applied computing*, 506-509.

Rahaman, H. A. (2020). A Proposed Model for Cybercrime Detection Algorithm Using A Big Data Analytics [IJCSIS]. *International Journal of Computer Science and Information Security*, *18*(6).

Rajeswari, P. V. N., Susmitha, M., & Kumar, V. S. M. (2021). A Multi-Objective Hyper-Heuristic Improved Particle Swarm Optimization Based Configuration of SVM for Big Data Cyber Security. *European Journal of Molecular & Clinical Medicine*, *7*(11), 7552–7560.

Srinivasan, A., Faruquie, T. A., & Joshi, S. (2012). Data and task parallelism in ILP using MapReduce. *Machine Learning*, *86*(1), 141–168.

Suthaharan, S. (2014). Big data classification: Problems and challenges in network intrusion prediction with machine learning. *Performance Evaluation Review*, *41*(4), 70–73.

Terzi, D. S., & Terzi, R. and Serefsagiroglu. (2015). A survey on security and privacy issues in big data, In *10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 202-207.

Triguero, I., Galar, M., Merino, D., Maillo, J., Bustince, H., & Herrera, F. (2016). Evolutionary undersampling for extremely imbalanced big data classification under apache spark, In *Congress on Evolutionary Computation (CEC)*, 640-647. IEEE.

CAIDA. (2008). UCSD Network Telescope Aggregrated DDoS Metadata. "https://catalog.caida.org/details/dataset/telescope_ddos.

Venugopal, S., Sathianesan, G.W and Rengaswamy, R. (2021). Cyber forensic framework for big data analytics using Sunflower Jaya optimization-based Deep stacked autoencoder. *International Journal of Numerical Modelling: Electronic Networks, Devices and Fields,* e2892.

Wang, L., & Jones, R. (2021). Big data analytics in cyber security: Network traffic and attacks. *Journal of Computer Information Systems*, *61*(5), 410–417.

Zervoudakis, K., & Tsafarakis, S. (2020). A mayfly optimization algorithm. *Computers & Industrial Engineering*, *145*, 106559.

Zhang, C., Li, F., & Jestes, J. (2012). Efficient parallel kNN joins for large data in MapReduce, In *Proceedings of the 15th international conference on extending database technology*, 38-49.

Suman Thapaliya finished his undergraduate studies of "Computer Science" from London Metropolitan University, UK in 2013. Since then he has worked as Network/System Engineer in one of leading ISP of Nepal, worked under core experienced and professional's ICT team. He has in-depth understanding for Network planning and operations, Wireless Technologies, Telecommunications, Computer Networks and Video Surveillance. To refine his knowledge, hone his skills and prepare himself for the ever-increasing challenges of the competitive world, he left his job in 2015 and continued my postgraduate education. Thapaliya finished his master's in information technology with thesis title "Implementation and adaptation of software engineering in software development," a comparative analysis between Nepal and India from London Metropolitan University, UK 2017. He started his Ph.D. in 2018 in Information Security (IS) Audit with research work entitled as 'Information Security Audit: A Study for Security and Challenges in Financial Sector in Nepal – Comparative study between Nepal and India'. With strong academic qualification, having sound working experience in ICT sector and skilled to inputs in Security Domain. He is also decorated with global recognition certifications like CISA, CHFI, CEH, CEI, ISO 27001:2013, CCNA, RHCE, CISO and CISCO IT Essentials Instructor. Also, Thapaliya is contributing at Udemy and Cybrary as Instructor and Mentor respectively. He has extensive technical and management experience in information systems technology with a solid academic background in computer information systems, excellent command over communication and leadership skills, and the ability to build cohesive, productive teams while fostering and encouraging creativity and individual expression. His area of expertise: CISA Certified, Digital Forensic (CHFI) Certified, Digital Forensic (CHFI) Instructor, CCNA Certified, CCNA Instructor, Certified Ethical Hacker (CEH), Ethical Hacking Instructor (CEH), Lead Auditor ISO 27001:2013, CISCO IT Essentials Instructor, Cybrary Mentor, and Udemy Instructor.

Dr. Pawan Kumar Sharma is the Co-founder at Three Monks, is solutions-oriented IT Software/Public Cloud/ICT-related enterprise strategy Consultant highly regarded for more than 28 years of progressive experience developing, implementing, and supporting complex business infrastructures and technical solutions for leaders in the Banking, Insurance, Enterprises, Education, Fintech, ICT, Management Industry, Cyber Security auditing/consulting. He is also one of the ambassadors of Agora International for Nepal. He has authored and published numerous books, journals, and blogs. Pawan is a creative problem-solver who excels in team settings. He bridges business and technological concepts to boost profits and cut expenses through ongoing innovation and smart IT infrastructure planning. Pawan holds a Ph.D. from Singhania University, an MCA and MBA from Sikkim Manipal University, and has demonstrated skill and experience in delivering cutting-edge IT solutions while meeting goals and expectations for quality, time, and cost. With regard to development methodology, developer management, and customer interactions, Pawan is exceptionally skilled. He is also a Project manager with influence and motivation who excels at leading in circumstances with tight deadlines. When not working at Three Monks, Pawan is an avid public speaker and is associated with various clubs. He also enjoys socializing with technologists.