International Journal of Wireless Information Networks (2023) 30:16–29
https://doi.org/10.1007/s10776-022-00586-3

Cyber Forensic Investigation in IoT Using Deep Learning Based Feature Fusion in Big Data

Suman Thapaliya[1] · Pawan Kumar Sharma[2]

Received: 18 May 2022 / Revised: 15 July 2022 / Accepted: 2 November 2022 / Published online: 6 December 2022

Abstract
The Internet of Things (IoT) device is becoming universal domain and its success cannot be ignored, but its threats on IoT devices increases concurrently. The Cyber-attacks are becoming the component of IoT affecting user's life. The professionals are forced to sift huge data to unveil and manage litigations. Hence, secure IoT is required for comprehending attacks. A model is presented for discovering cyber attack considering feature fusion. The routing of data towards Base Station (BS) is done with the Fractional gravitational search algorithm (FGSA). At BS, cybercrime detection is done, wherein data is splitted with enhanced Fuzzy c-means clustering (FCM) considering the MapReduce model. In mapper, the feature fusion is done with mutual information and the Deep Quantum Neural Network (DQNN), while reducer performs cybercrime detection. The Fractional Mayfly Shepherd Optimization (FrMSO)-based Deep Belief Network (DBN) is devised for describing the digital examination to notice and trace behaviors of attacks in IoT. Here, the training of DBN is done by the proposed FrMSO algorithm, which is developed by integrating the Fractional Calculus (FC), Mayfly Optimization Algorithm (MA), and the Shuffled shepherd optimization Algorithm (SSOA). The developed model helps to employ the weights of DBN with FrMSO for determining and tracing the abnormal aspects in IoT. The FrMSO-based DBN presented elevated precision of 96.4%, recall of 98.3% and F-measure of 95.4% respectively.

Keywords Cybercrime detection · MAPREDUCE · Internet of things · Deep belief network · Deep quantum neural network

1 Introduction

Due to the emergence of communication technologies and incursion of several networking tools and services in day-to-day lives employed an omnipresent IoT model for empowering the automation that holds self-directed functions and dispersed computations in huge-scaled networks. With physical platform, the IoT model includes communication network for accumulating and exchanging beneficial data to fully provide the IoT benefits. Inspite huge number of IoT tools and deployments, the feasibility of IoT is far and owes to the existence of theoretical description. The functionality of network and robustness are directly based on the structure of network and disturbance of some devices in IoT platform can acquire terrible threats to operation, which is a major issue of IoT [1]. IoT can offer several advantages and it also maximizes the danger of exposure to several privacy and security risks. Considering IoT, the risks of security go far away from information risk or DoS. These risks are now based on real lives that include physical security. Other issues are based on privacy [2]. The emergence in count and erudition of unidentified cyber-attacks has shed a shadow in employment of smartest devices. It originates a way that heterogeneity and allocation of IoT tools and services made the IoT security a complex process. Moreover, the detection of attack in IoT is fundamentally different compared to classical techniques due to special service needs of IoT [3].

Cyber security is an imperative factor to be employed throughout the world and all the promising technologies as communications networking, and information processing. In addition, other important techniques as cloud computing, social networks and barcodes utilized in IoT raises cyber security issues. The applications of IoT, such as Smart Home suffered the majority from cybercrimes and hence evaluated by several countries, such as China, U.K and U.S.A. These

✉ Suman Thapaliya
sumanthapali096@gmail.com

[1] Department of IT, Lincoln University College, Petaling Jaya, Malaysia

[2] Department of Faculty of Science Health and Technology, Nepal Open University, Lalitpur, Nepal

countries have highlighted extraordinary laws for ensuring IoT security. The risk of cyber security n IoT maximizes the devices count linked to network. These devices make the data as target for creating an attack by hackers [4]. Due to quick emergence of IoT devices, a huge number of cyber-attacks occur, which targets these kinds of devices. It considered that majority of IoT attacks include botnet-based attacks. In addition, several classical rule-based detection models are modelled by the attackers, but the classical Intrusion Detection System (IDS) are not capable to be deployed in IoT platforms because of resource issues in these devices [5]. If IoT platform is violated, then attackers pose the capability to disperse the data of IoT to unauthenticated parties, which can influence the reliability and accuracy of IoT data over the complete life cycle. Hence, such cyber-attacks required to be solved for safer IoT usage. Presently, various measures are taken for managing the security problems in IoT model, which are done in recent days. The majority of cyber security techniques are devised by coupling the domains of machine learning and cyber security [6].

Recently, there is huge attention in revealing the usage of Artificial Intelligence (AI) methods, like Deep Learning (DL), and Machine Learning (ML) on developing solutions of cyber security that includes detection of malware, privacy-preserving methodologies, forensic examination and threat intelligence. The DL-based techniques involve a learning strategy with various layers and each layer poses an imperative count of computational nodes. However, the design of good AI-based IoT attack discovery model remained a major issue [7]. The major machines learning techniques are utilized for predicting the cyber security attacks, like Naïve Bayes, Random Forest (RF) and so on. The DL is a sophisticated ML, which expands artificial neural network techniques [4]. In [8], a cyber-attack detection model is devised for dealing with sinkhole attacks, which targeted the IoT devices. They obtained elevated accuracy of detection on mobile cases with its learning's. In [9], a battery exhausted prevention model is devised on the basis of mask network and Bluetooth low energy (BLE). In [10], a DDoS attack detection model is devised for handling the big data to detect the attacks. In [11], an entropy-based DDoS attack measurement is devised based on packet size and it helped to find the DDoS attack with Software defined networking (SDN). The majority of techniques revealed to discover the cyber-attacks in IoT, but it mostly focuses detection model for particular threats of IoT [5].

A method is devised for Cyber forensic investigation using deep learning-based feature fusion in big data-based IoT. The simulation of IoT network is done and the accumulated data are routed towards the BS using FGSA. Subsequent to routing, the cybercrime detection is performed at BS where the data is partitioned using an eFCM. The MapReduce is employed wherein the mappers are responsible for performing the feature fusion using mutual information and DQNN, while reducer is used for cyber crime detection using the DBN with proposed FrMSO algorithm.

The main contributions:

- **FrMSO-based DBN for Cyber attack discovery**: The FrMSO-based DBN is considered to identify cyber attack. Here, the update of DBN weight is performed with FrMSO to generate best weights for tuning DBN in order to attain effective outcomes.
- **FrMSO**: It is developed by integrating the Fractional Calculus (FC), Mayfly Optimization Algorithm (MA), and the Shuffled shepherd optimization Algorithm (SSOA).

The rest of sections includes: Sect. 2 exposes prior cyber attack discovery models. Section 3 presents IoT structure. Section 4 presents devised methodology for detecting the cyber attack. Section 5 presented ability of developed technique in contrast to other methodologies. Section 6 gives conclusion.

2 Literature Review

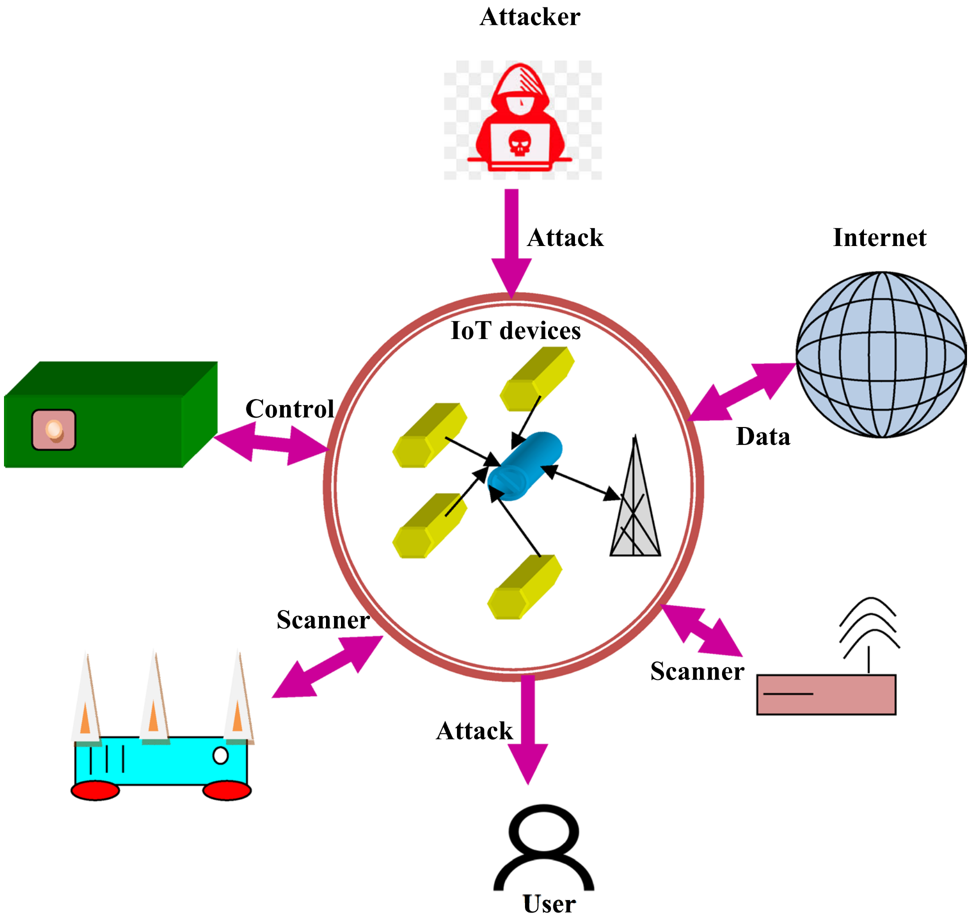
The eight priorly presented cyber attack discovery methodologies are inspected. Soe et al. [12] developed correlated-set thresholding on gain-ratio (CST-GR) for choosing essential features for determining the cyber-attacks. The detection model was lightweight and utilizes Raspberry Pi modules. The essential features linked with each attack were utilized to make the classifier to process quickly. However, the method was unable to discover other types of attacks on real platform. To identify other attacks, Samy et al. [13] devised a comprehensive attack detection module for detecting various types of cyber-attacks in IoT with DL. The developed model executed on attack detector considering the fog nodes, due to its disseminated nature, elevated capacity of computation and nearness amongst the edge devices. However, it poses a major issue in data labeling accumulated from edge layer and makes the process complicated. To reduce complexity, Gopalakrishnan et al. [14] developed DL-based traffic prediction with a data offloading mechanism with cyber-attack detection (DLTPDO-CD). Here, the bidirectional long short term memory (BiLSTM) was utilized for offloading data. Thereafter, the Adaptive Sampling Cross Entropy (ASCE) was utilized for increasing network throughput to make effective decisions. At last, the DBN trained with Barnacles Mating Optimizer (BMO) algorithm was adapted for detecting the cyber-attacks. However, the relaxation process may destroy the performance. To improve performance, Kumar et al. [15] devised hybrid feature reduced model for detecting the cyber attack in attack. Ranking of feature was done with correlation coefficient and the Random Forest (RF) was utilized for offer various sets of feature, which was integrated with AND operation. However, the method did not able to increase the accuracy.To elevate accuracy, Gurpal Singh Chhabra et al. [16] developed generalized forensic model with Google's programming model and MapReduce for detecting the cyber attack. Here, the tools, like Hive, Hadoop, R and Mahout were utilized for attaining parallel processing. Moreover, this method is scalable, but it suffered from elevated time of processing. To reduce processing time, Huma et al. [17] devised hybrid deep random neural network (HDRaNN) for detecting the cyber attack in IoT, but it was unable to defy other attacks. To handle other attacks, Sabaresan Venugopal et al. [18] developed Sunflower Jaya Optimization-based Deep stacked autoencoder (SFJO-based Deep SAE) for detecting the cyber attacks. The Deep SAE training was done using SFJO, which was devised by blending the control parameters of Jaya optimization to Sunflower optimization algorithm, but it suffered from elevated computational complexity. To reduce computational complexity, Abbas Karimi et al. [19] developed pseudo-label technique for optimizing the neural network to identify cyber attacks. Database was split into two modules, namely unlabelled and labeled, and then trained module was utilized for evaluating the labeling of unlabelled samples with pseudo-labels, but this technique did not examine images and text databases.

3 System Model

Due to the emerging technologies, new issues raises and one of them are cyber attacks. The hacks on web or the viruses spreading are heard by each of us and these bring attacks in IoT. Moreover, the extensive usage of IoT raises cyber security problems owing to the rise in attacks. Thus, the intention is to develop an effectual cyber forensic using IoT infrastructures. Figure 1 reveals IoT structure for malware detection. The IoT [20] comprises several sensor nodes, and it is connected using a wireless network. Furthermore, the IoT model contains three kinds of nodes, named normal nodes, Cluster head (CH) and BS. The normal nodes transmit data to CH and it sends the accumulated data to BS.

The IoT model consists of one BS F_j, CH K_l and g nodes. The highest range of radio communication considering node is constantly dispersed in size of M_q and N_q meters. The best position of sink node in IoT is expressed as $\{0.5M_q,\ 0.5N_q\}$.

Fig. 1 IoT model



The coordinate values of M_o and N_o express each IoT node position.

3.1 Energy Model

The IoT contains large number of nodes in which each node is responsible to attain some initial energy, and is represented as Q_0, but energy of nodes in IoT is non-rechargeable [20]. The energy dissipation with normal node is formulated as,

$$T_{emt}(\varepsilon_y^x) = T_{ele} * O_n + F_{pa} * O_n * ||\varepsilon_y^x - \varepsilon_z^w||^4 \quad ;If \ ||\varepsilon_y^x - \varepsilon_z^w|| \ge s_0 \tag{1}$$

$$T_{emt}(\varepsilon_y^x) = T_{ele} * O_n + T_{fs} * O_n * ||\varepsilon_y^x - \varepsilon_z^w||^4 \quad ;If \ ||\varepsilon_y^x - \varepsilon_z^w|| < s_0 \tag{2}$$

$$s_0 = \sqrt{\frac{T_{fs}}{T_{pa}}} \tag{3}$$

where,T_{fs} is energy obtained in free space, O_n refers packet size, T_{pa} deliberates multipath fading amplification, $||\varepsilon_y^x - \varepsilon_z^w||$ is distance amidst CH and normal node. The electronic energy is given as,

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

where,T_{txr} refers energy generated by transmitter, T_{DA} symbolize energy generated while collecting data. Whenever CH node confess O_n data bytes, then dissipation of energy in CH is produced, and is given as,

$$T(\varepsilon_z^x) = T_{ele} * O_n \tag{5}$$

After data broadcast and receive with CH, the IoT node energy is renewed with $T_{\ell+1}(\varepsilon_y^x)$ and $T_{\ell+1}(\varepsilon_z^x)$ and is formulated by,

$$T_{\ell+1}(\varepsilon_y^x) = T_{\ell}(\varepsilon_y^x) - T_{emt}(\varepsilon_y^x) \tag{6}$$

$$T_{\ell+1}(\varepsilon_z^x) = T_{\ell}(\varepsilon_z^x) - T_{emt}(\varepsilon_z^x) \tag{7}$$

The update energy considering each node is repeated until complete nodes in network set out to dead node.

3.2 Routing Using FGSA

Considering IoT, the routing of data with best path is not an easy task and initiates energy problems, because of less battery capability. The energy crisis happens whilst transmission and these issues can be mitigated with FGSA [20]. The FGSA is generated by blending advantages of both GSA and fractional theory. By transmitting data, the exchange of data is attained by best route and it reduces node power. The update of FGSA is represented as,

$$H_i^h(k+1) = XH_i^h(k) + \frac{1}{2}XH_i^h(k-1) + u_i^h(k+1) \tag{8}$$

where, $H_i^h(k+1)$ is agent i location in hth cluster at time $k+1$,$H_i^h(k)$ signifies ith agent location at present iteration k and $H_i^h(k-1)$ refers agent i position in previous iteration, and $u_i^h(k+1)$ signifies velocity evaluated by GSA in $(k+1)^{th}$ iteration using agent i location in hth cluster at time, and X is constant, such that $0 \le X \le 1$. The obtained data through best path is given as J.

4 Proposed FrMSO-Based DBN for Cyber Forensic Investigation in IoT

The huge expansion in IoT has resulted into huge data and analysis of these data through internet becomes a complex task, and thus the big data technology is utilized. The quick increase in data and hacking methods availability made the devices of IoT susceptible to cyber-attacks. The exploration Cyber forensic aimed to inspect data violations by mining data from devices through network. The goal is to devise a model for cyber forensic investigation with deep learning-based feature fusion in big data-based IoT platform. Here, the IoT network is simulated initially, and then the devices collect the information and thereafter the collected information is routed to the BS using FGSA [20]. Once routing is done, cybercrime detection are performed at the BS where the data is partitioned using an enhanced FCM (eFCM) [21]. After data partitioning, the partitioned data are then provided to the MapReduce framework in which the map reduce contains two stages, like mapper and reducer. In the mapper phase, the feature fusion is done with the help of mutual information and the DQNN [22]. On the other hand, in the reducer phase, malware detection is performed using the DBN [23]. Here, the DBN is trained with proposed FrMSO algorithm, which is newly devised by integrating the FC [24], MA [25] and the SSOA [26]. Figure 2 reveals the structure of malware detection model using proposed FrMSO-based DBN.

4.1 Data Acquisition

Assume database L having several data samples, and is expressed by,

$$L = \{T_1, T_2, \dots T_r, \dots, T_u\} \tag{9}$$

where, u refers total number of data and T_r refers rth data, which is of dimension 100000 × 100.

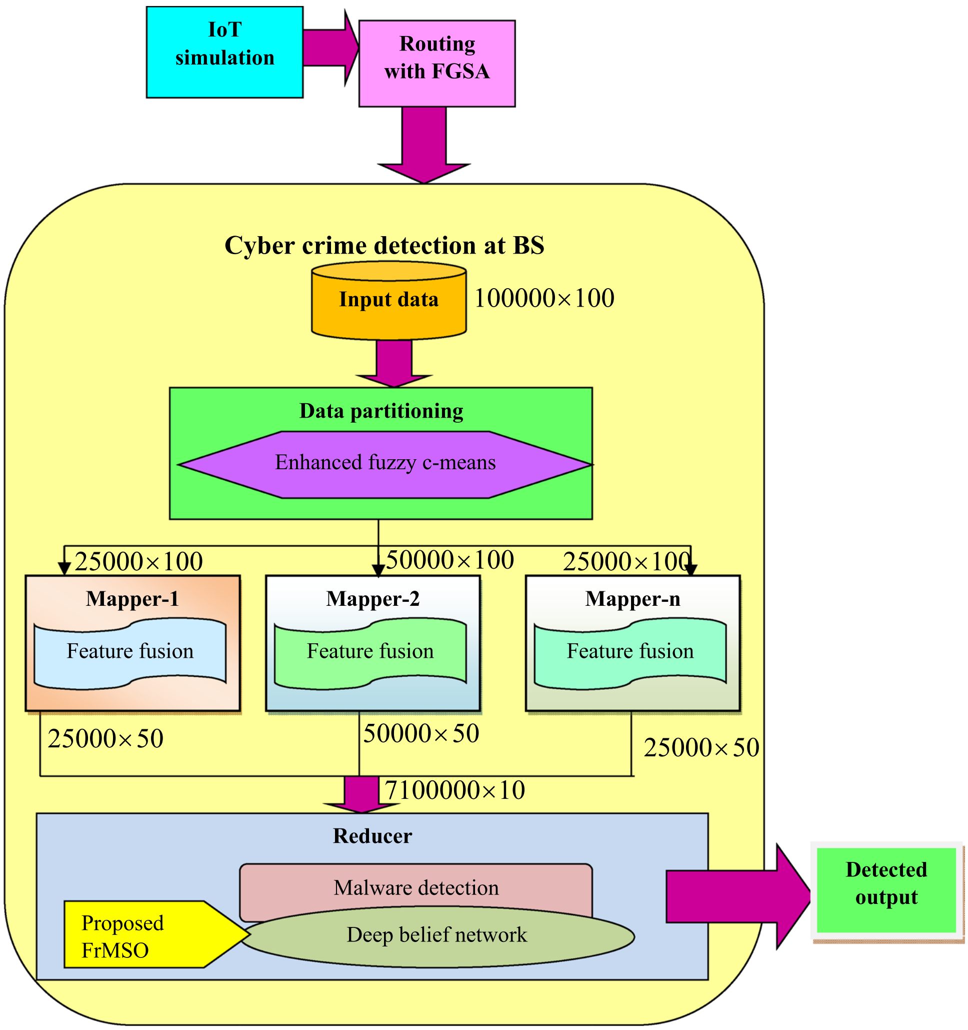


Fig. 2 Configuration of cyber-crime detection using FrMSO-based DBN

4.2 Partitioning of Data with eFCM

The partioining of dataset L is done using eFCM [21]. The aim of eFCM is to overwhelm the probable local optimum, and it enhances the computational efficiency of traditional FCM. The objective function considered for eFCM is stated as,

$$A(D) = \sum_{a=1}^{E} \sum_{b=1}^{D} \left(U_{a,b}\right)^{t} f_{a,b}^{2} \tag{10}$$

where, D refers number of clusters such that $1 \leq b \leq D$, $f_{a,b}$ symbolize distance from ath point to bth centroid, $U_{a,b}$ signifies membership value from ath point to bth cluster and t express fuzzifier and E refers total points such that $1 \leq a \leq E$.

The membership function is given by,

$$U_{a,b} = \frac{1}{\sum_{m=1}^{D} \frac{f_{a,b}^{\frac{2}{t-1}}}{f_{a,m}}} \tag{11}$$

where, $f_{a,m}$ symbolize distance from ath point to mth centroid, m refers cluster index.

The cluster centroid matrix is expressed by,

$$S_b = \frac{\sum_{a=1}^{E} U_{a,b}^{t} \cdot e_a}{\sum_{a=1}^{E} U_{a,b}^{t}} \tag{12}$$

where, e_a refers $a$thdata.

The steps considered in eFCM are stated below.

(i) The membership matrix is initialized such that $R = \left[U_{a,b}\right]$ with starting value $R^{(0)}$.

(ii) Initialize centroids.

a) The point is sampled uniformly consider data as first centroid.

b) Sample next centroid using data by considering probability proportional to squared distance.

c) Continue above steps repeatedly till the count of centroids is similar to needed number of clusters.

(iii) Evalaute matrix of cluster centroid considering Eq. (11) and Eq. (12)

(iv) Evaluate $R^{(\ell+1)}$.

(v) If $||R^{(\ell+1)} - R^{(\ell)}|| < \omega$, then coverage else goto step (iii).

Hence, the partitioned data obtained with input data T_r considering eFCM is givenby,

$$T_r = \left\{\rho_v\right\}; 1 \le v \le \eta \tag{13}$$

where,η is total partitioned data. Here, the partitioned data obtained in mapper-1 is of dimension 25000 × 100 and mapper-2 is of dimension 50000 × 100 and mapper-n is of dimension 25000 × 100 EFCM

4.3 Mapper and Reducer Phase

MapReduce indicates the programming method that comprises a set of mapper and reducer. It carries out detection of cybercrime by processing data parallelly. hus, it assists to control large data using MapReduce. Here, the feature fusion is done in mapper using DQNN [22], and the cyber crime detection process is performed in reducer. The partitioned data ρ_v is provided to MapReduce in which partioned data is splitted into particular number, which is equal to total mappers. Figure 3 reveals MapReduce for identifying cybercrime.

4.3.1 Mapper Phase

In mapper, the partitioned data ρ_v is adapted for performing feature fusion that includes two steps, such as features sorting and fusion of features with DQNN.

4.3.1.1 Feature Fusion Once data partitioning is done, features are acquired through data and sorted using mutual information (MI) in accordance with number of features to be selected, and are formulated by,

$$F_k^{new} = \sum_{i=1}^{N} \frac{\beta}{i} F_i \tag{14}$$

$$i = 1 + \frac{p}{q} \tag{15}$$

$$q = \frac{p}{N} \tag{16}$$

where, N signifies number of features to be chosen such that $i = i\ to\ q$, and p represents number of features in total, and β refers optimal parameter.

4.3.1.2 Generating β Using DQNN In DQNN [22], the training data and the feature size of 100 × 10 are considered. All the features are fed to DQNN for attaining the target value. Here, the training data is splitted into two classes namely class 0 and class 1. Here, the class 0 contains 60 × 10 and class 1 comprises 40 × 10. The mean of class 0 and class 1 is computed and modelled to 1 × 10.

Meanwhile, optimum value for factor β is discovered with DQNN. During training process, the value of optimal parameter β is evaluated as,

$$\beta = MI\left(d_i, \lambda_i\right) \tag{17}$$

Here, λ_i refers average of d_i that belongs to the same class, d_i depicts data instance, and MI symbolize MI. The MI amongst feature λ_i and target d_i whose joint distribution is provided as $P(\lambda_i, d_i)$ and is formulated by,

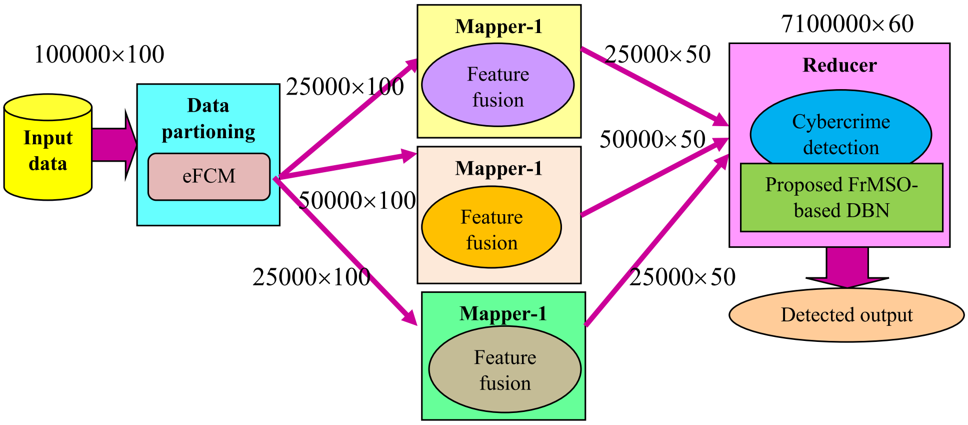


Fig. 3 MapReduce for cybercrime discovery

$$MI(\lambda_i, d_i) = \sum_{\lambda_i \in B} \sum_{d_i \in C} P_{\lambda_i, d_i}(B, C) \log \frac{P_{(\lambda_i, d_i)}(B, C)}{P_{\lambda_i}(B).P_{d_i}(C)} \tag{18}$$

where, $P_{\lambda_i, d_i}(B, C)$ signifies joint probability mass function of λ_i and d_i, P_{λ_i} and P_{d_i} refers marginal probability mass function, λ_i is feature and d_i symbolize target. After computing MI of each feature, it selects top "m" features with elevated value of MI. The features chosen with MI are expressed as ϑ, and is given as an input to reducer which is denoted as γ.

Figure 4 depicts the process of training adapted in discovering optimum parameter β. Thus, class label in training is expressed as α in such a way that optimum value of β is evaluated for each data instance with aforementioned formula.

4.3.1.3 Structure of DQNN The optimum value for parameter β is evaluated with DQNN [22] considering total features (p) as input.

Assume quantum perceptron considering input qubits as R and output qubits as V. The perceptron represents random unitary operator adapted to $(R + V)$ input and output qubits in such a way that it relies on $\left(2^{R+V}\right)^2 - 1$ attributes. Thus, the inputted qubits are described using unknown mixed state G^{in} wherein the output qubits are indicated in fiducial product state $|0...0\rangle_{out}$. This network represents quantum circuit that contains I hidden layers, and relies on initial state G^{in} of input and produces a mixed state G^{out} for output and is formulated by,

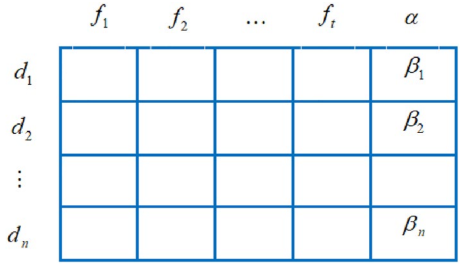
$$G^{out} = J_{in,hid}\left(W\left(G^{in} \otimes |0...0\rangle_{hid,out}\langle 0...0|\right)W^{+}\right) \tag{19}$$

where, $W = V^{out}V^{Q}V^{Q-1}...V^{1}$ is quantum circuit, V^{λ} represent layer unitaries which comprises product of quantum perceptrons, which relies on layers $(\varphi - 1)$ and φ. A fundamental feature is that output is described by combination of positive layer series to layer transition maps P^{φ}.

$$G^{out} = P^{out}\left(P^{I}\left(...P^{2}\left(P^{1}\left(G^{in}\right)\right)...\right)\right) \tag{20}$$

where,

$$P^{\varphi}\left(H^{\varphi-1}\right) \equiv J_{\varphi-1}\left(\prod_{\delta=S_\lambda}^{1} W_{\delta}^{\varphi}\left(H^{\varphi-1} \otimes |0\ldots0\rangle_{\varphi}\langle 0\ldots0|\right)\prod_{\delta=1}^{S_\lambda} W_{\delta}^{\varphi+}\right) \tag{21}$$



	f_1	f_2	...	f_t	α
d_1					β_1
d_2					β_2
⋮					
d_n					β_n

Fig. 4 Training procedure for evaluating β

Here, W_{δ}^{φ} reveals δ^{th} perceptron, which relies on layers $(\varphi - 1)$ and φ, S_{λ} signifies total perceptrons, which acts on layers $(\varphi - 1)$ and φ, and W refers controlled unitary. Thus, the output G^{out} acquired by network reveals optimal value for β. Hence, the feature fusion produced from mapper-1, mapper-2 and mapper-n are $A_1, A_2, \ldots, A_n$, which are further fed as an input to reducer.

4.3.2 Reducer Phase

Here, the detection of cyber crime is performed with FrMSO-based DBN using reducer γ which adapts feature fusion produced from mapper-1, mapper-2 and mapper-n are $A_1, A_2, \ldots, A_n$, as an input to reducer. The DBN [23] training is performed with FrMSO, and is obtained by integrating the advantages of FC [24], SSOA [26] and MA [25]. The DBN and training with FrMSO is illustrated below.

4.3.2.1 Structure of DBN The DBN [23] is a type of Deep Neural Network (DNN) that contains several layers of Multilayer Perceptrons (MLPs) and Restricted Boltzmann Machines (RBMs). It considers the selected features denoted as f_t as its input. RBMs comprise visible and hidden units which are linked using weighted connections. It can be utilized for solving the unsupervised learning tasks for minimizing the feature dimensionality and can be used for solving the supervised learning tasks.

The input fed to visible layer indicates features and first RBM hidden layer is modelled by,

$$\varepsilon^{1} = \left\{\varepsilon_1^1, \varepsilon_2^1, \ldots, \varepsilon_g^1, \ldots, \varepsilon_l^1\right\}; 1 \le g \le \ell \tag{22}$$

$$\kappa^{1} = \left\{\kappa_1^1, \kappa_2^1, \ldots, \kappa_e^1, \ldots, \kappa_v^1\right\}; 1 \le e \le v \tag{23}$$

where, ε_g^1 express gth visible neuron contained in first RBM layer, κ_e^1 signifies eth hidden neuron and v express total hidden neurons. Assume ρ express bias of visible layer and E signifies bias of hidden layer and is represented by,

$$\rho^{1} = \left\{\rho_1^1, \rho_2^1, \ldots, \rho_g^1, \ldots, \rho_{\ell}^1\right\} \tag{24}$$

$$\mu^{1} = \left\{\mu_1^1, \mu_2^1, \ldots, \mu_e^1, \ldots, \mu_v^1\right\} \tag{25}$$

where, ρ_g^1 signifies bias associated to gth neuron, and μ_e^1 symbolize bias associated with eth hidden neuron. The weights employed in first RBM are given by,

$$\varpi^{1} = \left\{\varpi_{g,e}^{1}\right\}; 1 \le g \le 4; 1 \le e \le v \tag{26}$$

where, $\varpi^{1}_{g,e}$ express weight amidst gth visible neuron and eth hidden neuron. The output of hidden layer considering first RBM is represented by,

$$\kappa^{1}_{e} = \alpha\left[\mu^{1}_{e} + \sum_{g} \varepsilon^{1}_{g}\varpi^{1}_{g,e}\right] \tag{27}$$

where, α symbolize activation function. The output produced through first RBM are given by,

$$\kappa^{1} = \left\{\kappa^{1}_{e}\right\}; 1 \le e \le v \tag{28}$$

The count of visible neurons is expressed by,

$$\varepsilon^{2} = \left\{\varepsilon^{2}_{1}, \varepsilon^{2}_{2}, \ldots, \varepsilon^{2}_{\ell}\right\} = \left\{\kappa^{1}_{e}\right\}; 1 \le e \le v \tag{29}$$

where, $\left\{\kappa^{1}_{e}\right\}$ refers first RBM layer output.

The hidden layer considering second RBM is formulated by,

$$\kappa^{2} = \left\{\kappa^{2}_{1}, \kappa^{2}_{2}, \ldots, \kappa^{2}_{e}, \ldots, \kappa^{2}_{v}\right\}; 1 \le e \le v \tag{30}$$

The biases of visible layer and hidden layer considering second RBM layer is expressed in Eqs. (24) and (25),denoted as ρ^{2} and μ^{2}. The weight vector of second RBM is modelledby,

$$\varpi^{2} = \left\{\varpi^{2}_{ee}\right\}; 1 \le e \le v \tag{31}$$

where,ϖ^{2}_{ee} refers weight amidst eth neuron, and eth hidden neuron. The output of eth hidden neuron is expressedby,

$$\kappa^{2}_{e} = \alpha\left[\mu^{2}_{e} + \sum_{g} \varepsilon^{2}_{g}\varpi^{2}_{ee}\right]\forall\varepsilon^{2}_{g} = \kappa^{1}_{e} \tag{32}$$

where,y^{2}_{u} refers bias linked with uth hidden neuron. Hence, the output of hidden layer generated is modelled as,

$$\kappa^{2} = \left\{\kappa^{2}_{e}\right\}; 1 \le e \le v \tag{33}$$

The MLP input is modelled by,

$$Y = \left\{Y_{1}, Y_{2}, \ldots, Y_{e}, \ldots, Y_{v}\right\} = \left\{\kappa^{2}_{e}\right\}; 1 \le e \le v \tag{34}$$

where,v refers count of neurons in input layer.

The hidden layer of MLP is given by,

$$Z = \left\{Z_{1}, Z_{2}, \ldots, Z_{N}, \ldots, Z_{o}\right\}; 1 \le N \le o \tag{35}$$

where,o signifies total hidden neurons. The MLP output is modelled by,

$$O = \left\{O_{1}, O_{2}, \ldots, O_{i}, \ldots, O_{j}\right\}; 1 \le i \le j \tag{36}$$

where,j refers count of neurons. Consider $\omega^{'}$ indicates a weight vector, and is formulated by,

$$\varpi^{'} = \left\{\varpi^{'}_{eN}\right\}; 1 \le e \le v; 1 \le N \le O \tag{37}$$

where,$\omega^{'}_{eN}$ refers weight amidst eth input neuron, and Nth hidden neuron. The hidden layer output is expressed by,

$$Z_{N} = \left[\sum_{e=1}^{v} \varpi^{'}_{eN} * I_{e}\right] L_{N} \forall Y_{e} = \kappa^{2}_{e} \tag{38}$$

where,L_{N} refers bias of hidden neuron. The weights amidst hidden layer and output layer is expressed as $\varpi^{''}$, and is modelled as,

$$\varpi^{''} = \left\{\varpi^{''}_{ei}\right\}; 1 \le e \le v; 1 \le i \le j \tag{39}$$

Hence, the output vector with weight $\varpi^{''}$ and hidden layer output is given by,

$$O_{i} = \sum_{N=1}^{O} \varpi^{''}_{eN} * Z_{N} \tag{40}$$

where,$\varpi^{'''}_{eN}$ signifies weight amidst eth hidden neuron, and Nth output neuron and Z_{N} signifies hidden layer output. The DBN output is given by υ.

4.3.2.2 DBN Training with FrMSO The DBN [23] training is performed with FrMSO, and is produced by integrating the advantages of FC, and MSSO. The MSSO is obtained by acquiring the benefits of MA [25] and SSOA [26]. The MSSO helps to effectively balance exploration and exploitation and helps to run off from local optimum. It can effectively manage engineering design issues and optimization issues. On the other hand, FC [24] can effectively deal with infinite parameters and poses the ability to solve differential and integral equation. Hence, the hybridization of MSSO and FC aids to produce global optimum solution. The FrMSO steps are enlisted below.

i) Initialization:

The foremost step is initialization, and is formulated as,

$$D = \left\{D_{1}, D_{2}, \ldots, D_{\tau}, \ldots, D_{\hbar}\right\} \tag{41}$$

where, $\hbar$ refers total solutions, and D_{τ} is τ^{th} solution.

ii) Find error:

The error is discovered to acquire most excellent solution and is produced by,

$$MSE = \frac{1}{o}\left[\sum_{z=1}^{o} \ell_{z} - \upsilon\right] \tag{42}$$

where, ℓ_{z} is output calculated and υ refers DBN output, and o symbolize total data.

iii) Update equation of proposed FrMSO

The update of MSSO is given by,

$$D_a(y+1) = \begin{bmatrix} C_a(y) + b_1 e^{-\beta r_p^2} pb_a + b_2 e^{-\beta r_g^2} gb_a \\ -\dfrac{rand\left(R \circ D_g(y) + Y \circ D_o(y)\right)}{[1 - R \times rand - Y \times rand]} \left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right] \end{bmatrix} * \frac{[1 - R \times rand - Y \times rand]}{b_1 e^{-\beta r_p^2} + b_2 e^{-\beta r_g^2} - R \times rand - Y \times rand} \tag{43}$$

where, R and Y is parameter, $rand$ signifies random number between (0,1), b_1, b_2 is positive attraction constants,$C_a(y)$ refers velocity of a^{th} mayfly at iteration y,pb_a is personal best solution of a^{th} mayfly, and gb_a signifies global best solution of ath mayfly, $D_g(y)$ and $D_o(y)$ is solution vectors at iteration $(y+1)$, e refers nuptial dance coefficient,

Subtract $D_a(y)$ on both sides,

$$D_a(y+1) - D_a(y) = \begin{bmatrix} C_a(y) + b_1 e^{-\beta r_p^2} pb_a + b_2 e^{-\beta r_g^2} gb_a \\ -\dfrac{rand\left(R \circ D_g(y) + Y \circ D_o(y)\right)}{[1 - R \times rand - Y \times rand]} \left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right] \end{bmatrix} * \frac{[1 - R \times rand - Y \times rand]}{b_1 e^{-\beta r_p^2} + b_2 e^{-\beta r_g^2} - R \times rand - Y \times rand} - D_a(y) \tag{44}$$

$$D_a(y+1) - D_a(y) = \begin{bmatrix} C_a(y) + b_1 e^{-\beta r_p^2} pb_a + b_2 e^{-\beta r_g^2} gb_a \\ -\dfrac{rand\left(R \circ D_g(y) + Y \circ D_o(y)\right)}{[1 - R \times rand - Y \times rand]} \left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right] \end{bmatrix} * \frac{[1 - R \times rand - Y \times rand]}{b_1 e^{-\beta r_p^2} + b_2 e^{-\beta r_g^2} - R \times rand - Y \times rand} - D_a(y) \tag{45}$$

For dealing with infinite terms, the FC concept is utilized. As per FC [24], the equation is written as,

$$M^{\alpha}\left(D_a(y+1)\right) = \begin{bmatrix} C_a(y) + b_1 e^{-\beta r_p^2} pb_a + b_2 e^{-\beta r_g^2} gb_a \\ -\dfrac{rand\left(R \circ D_g(y) + Y \circ D_o(y)\right)}{[1 - R \times rand - Y \times rand]} \left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right] \end{bmatrix} * \frac{[1 - R \times rand - Y \times rand]}{b_1 e^{-\beta r_p^2} + b_2 e^{-\beta r_g^2} - R \times rand - Y \times rand} - D_a(y) \tag{46}$$

$$D_a(y+1) - \alpha D_a(y) - \frac{1}{2}\alpha D_a(y-1) - \frac{1}{6}(1-\alpha) D_a(y-2) - \frac{1}{24}\alpha(1-\alpha)(2-\alpha) D_a(y-3) = \begin{bmatrix} C_a(y) + b_1 e^{-\beta r_p^2} pb_a + b_2 e^{-\beta r_g^2} gb_a \\ -\dfrac{rand\left(R \circ D_g(y) + Y \circ D_o(y)\right)}{[1 - R \times rand - Y \times rand]} \left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right] \end{bmatrix} * \frac{[1 - R \times rand - Y \times rand]}{b_1 e^{-\beta r_p^2} + b_2 e^{-\beta r_g^2} - R \times rand - Y \times rand} - D_a(y) \tag{47}$$

$$D_a(y+1) = \alpha D_a(y) + \frac{1}{2}\alpha D_a(y-1) + \frac{1}{6}(1-\alpha) D_a(y-2) + \frac{1}{24}\alpha(1-\alpha)(2-\alpha) D_a(y-3) + \begin{bmatrix} C_a(y) + b_1 e^{-\beta r_p^2} pb_a + b_2 e^{-\beta r_g^2} gb_a \\ -\dfrac{rand\left(R \circ D_g(y) + Y \circ D_o(y)\right)}{[1 - R \times rand - Y \times rand]} \left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right] \end{bmatrix} * \frac{[1 - R \times rand - Y \times rand]}{b_1 e^{-\beta r_p^2} + b_2 e^{-\beta r_g^2} - R \times rand - Y \times rand} - D_a(y) \tag{48}$$

The update of FrMSO is provided as,

$$D_a(y+1) = \begin{bmatrix} C_a(y) + b_1 e^{-\beta r_p^2} pb_a + b_2 e^{-\beta r_g^2} gb_a \\ -\dfrac{rand\left(R \circ D_g(y) - Y \circ D_o(y)\right)}{[1 - R \times rand - Y \times rand]} \left[1 - b_1 e^{-\beta r_p^2} - b_2 e^{-\beta r_g^2}\right] \end{bmatrix} * \frac{[1 - R \times rand - Y \times rand]}{b_1 e^{-\beta r_p^2} + b_2 e^{-\beta r_g^2} - R \times rand - Y \times rand} - D_a(y)(1-\alpha) + \frac{1}{2}\alpha D_a(y-1) + \frac{1}{6}(1-\alpha) D_a(y-2) + \frac{1}{24}\alpha(1-\alpha)(2-\alpha) D_a(y-3) \tag{49}$$

iv) Check feasibility:

The error is discovered and solution producing less error is chosen as optimum solution.

v) Termination:

The aforesaid steps are repeated until optimum solution is acquired. Table 1 inspects pseudo code of FrMSO.

5 Results and Discussion

The competence of FrMSO + DBN is obtained by altering data considered for training.

5.1 Experimental Set-Up

The modeling of FrMSO + DBN is operated in Python with PC having Windows 10 OS, Intel i3 core processor and 8 GB RAM.

5.2 Dataset Description

The assessment is done considering UCSD Network Telescope Aggregated DDoS Metadata [27]. This dataset represents the tasks of DDoS and is observed through the UCSD Network Telescope. It is accumulated with raw Telescope data considering the criterions described in Internet DoS based tasks.

5.3 Performance Analysis

Figure 5 provides valuation of FrMSO + DBN by changing the data taken for training and is modelled using

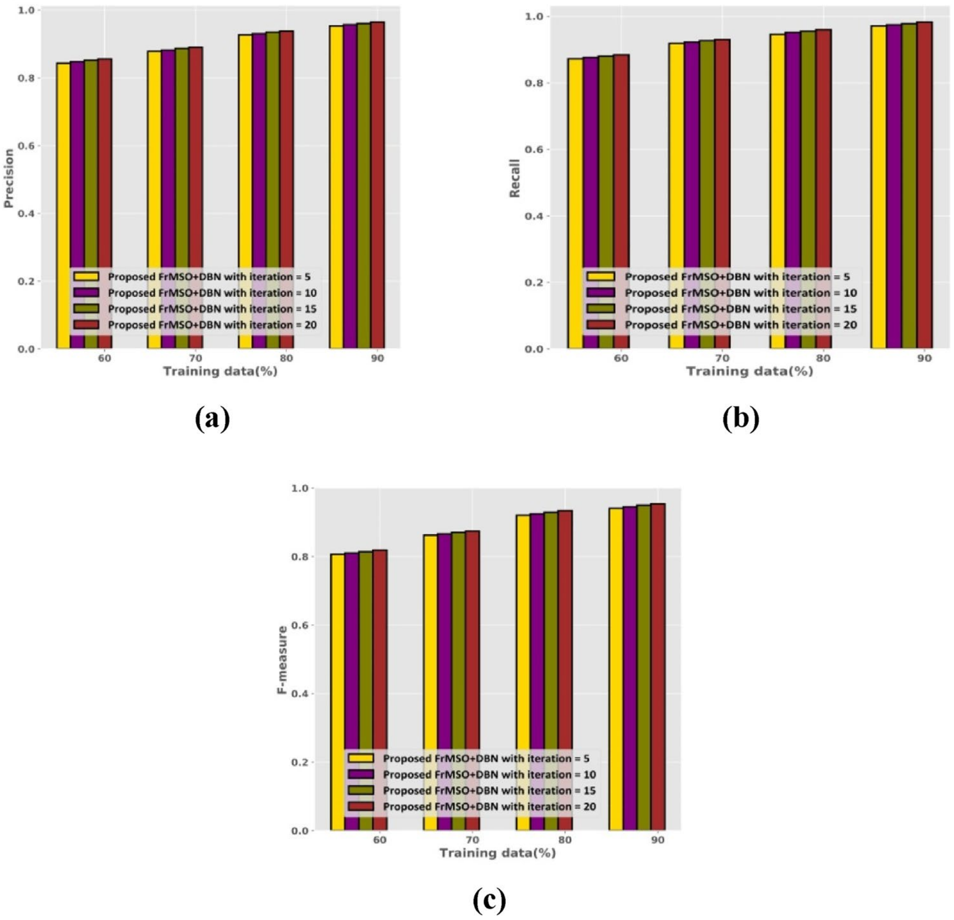
Table 1 Pseudo code of FrMSO

```
Input: Solutions $B$
Output: Best solution $B*$
Begin
Estimate error with Eq. (42)
While stopping criteria is not satisfied
Update solution using Eq. (49)
Enumerate achievability with error considering expression (42)
End while
Return Best solution
End
```

specific measures. The precision investigation is represented in Fig. 5a. For 60% data, the precision deliberated by FrMSO + DBN with iteration 5, 10, 15, 20 are 0.843, 0.848, 0.852, and 0.856. Correspondingly, for 90% data, the precision deliberated by FrMSO + DBN with iteration 5, 10, 15, 20 are 0.953, 0.957, 0.960, and 0.964. The recall inspection is demonstrated in Fig. 5b. For 60% data, the recall deliberated by FrMSO + DBN with iteration 5, 10, 15, 20 are 0.872, 0.877, 0.881, and 0.884. Correspondingly, for 90% data, the recall deliberated by FrMSO + DBN with iteration 5, 10, 15, 20 are 0.971, 0.975, 0.978, and 0.983. The F-measure inspection is demonstrated in Fig. 5c. For 60% data, the F-measure deliberated by FrMSO + DBN with iteration 5, 10, 15, 20 are 0.807, 0.810, 0.814, and 0.819. Correspondingly, for 90% data, the F-measure deliberated by FrMSO + DBN with iteration 5, 10, 15, 20 are 0.941, 0.945, 0.950, and 0.954.

5.4 Algorithm Analysis

The estimation considering DBN is defined in Fig. 6. The precision examination is illustrated in Fig. 6a. With population size = 5, the precision acquired by ChoA + DBN is 0.907, MA + DBN is 0.913, SSOA + DBN is 0.917, MSSO + DNFN is 0.922 and FrMSO + DBN is 0.927. Equally, for population size = 20, the precision acquired by ChoA + DBN is 0.919, MA + DBN is 0.923, SSOA + DBN is 0.929, MSSO + DNFN is 0.933 and FrMSO + DBN is 0.938. The efficiency of ChoA + DBN, MA + DBN, SSOA + DBN, MSSO + DBN with FrMSO + DBN considering precision is 2.025%, 1.599%, 0.959%, 0.533%. The recall inspection is rendered in Fig. 6b. For population size = 5,



(a)

(b)

(c)

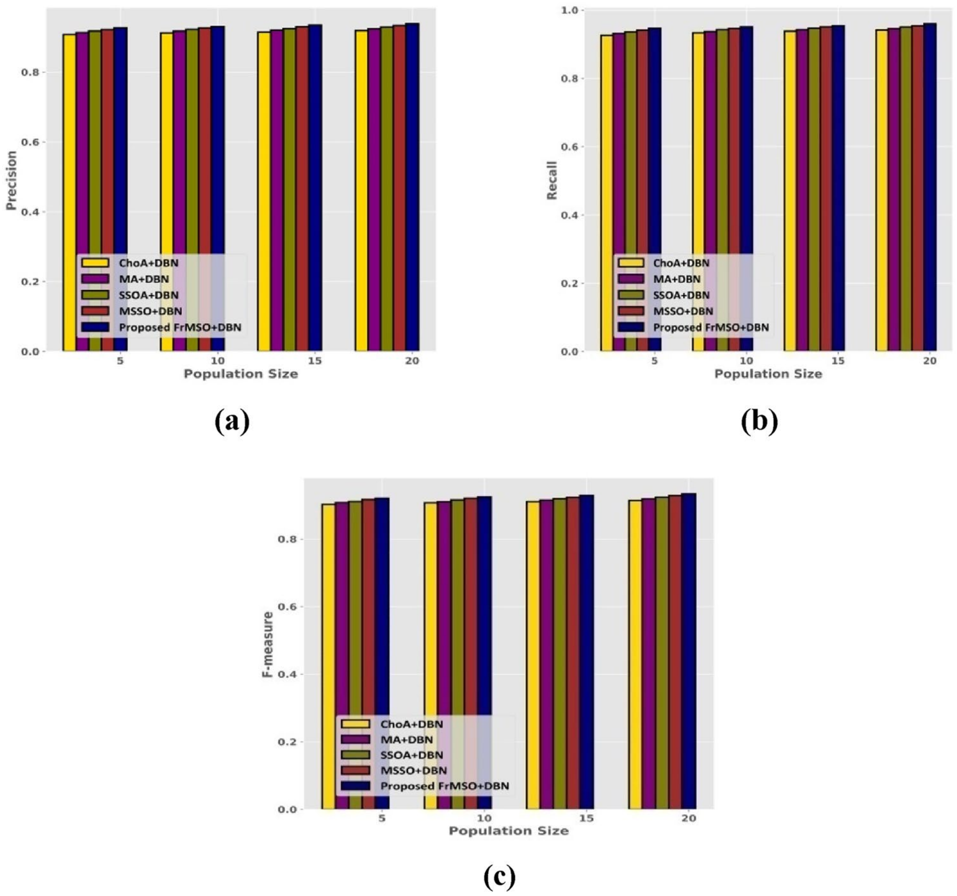
Fig. 5 Assessment of FrMSO + DBN considering **a** Precision **b** Recall **c** F-measure

the recall acquired by ChoA + DBN is 0.926, MA + DBN is 0.932, SSOA + DBN is 0.936, MSSO + DNFN is 0.941 and FrMSO + DBN is 0.947. Equally, considering population size = 20, the recall acquired by ChoA + DBN is 0.942, MA + DBN is 0.945, SSOA + DBN is 0.950, MSSO + DNFN is 0.954 and FrMSO + DBN is 0.960. The efficiency of ChoA + DBN, MA + DBN, SSOA + DBN, MSSO + DBN with FrMSO + DBN using recall is 1.875%, 1.562%, 1.041%, 0.625%. The F-measure examination is rendered in Fig. 6c. Considering population size = 5, the F-measure acquired by ChoA + DBN is 0.902, MA + DBN is 0.908, SSOA + DBN is 0.911, MSSO + DNFN is0.917 and FrMSO + DBN is 0.920. Equally, considering population size = 20, the F-measure acquired by ChoA + DBN is 0.914, MA + DBN is 0.918, SSOA + DBN is 0.924, MSSO + DNFN is 0.929 and FrMSO + DBN is 0.934. The efficiency of ChoA + DBN, MA + DBN, SSOA + DBN, MSSO + DBN with FrMSO + DBN using F-measure is 2.141%, 1.713%, 1.070%, 0.535%.

5.5 Comparative Assessment

The techniques considered for assessment involves Cyber forensics framework [16], HDRaNN [17], SFJO + Deep SAE [18], NN [19], MSSO + DNFN, and proposed FrMSO + DBN.

The techniques assessment is examined in Fig. 7. The precision investigation is shown in Fig. 7a. Using 60% data, the precision attained by existing are 0.756, 0.770, 0.782, 0.806, and 0.829 whereas FrMSO + DBN is 0.856. Besides, for 90% data, the precision attained by existing are 0.867, 0.883, 0.895, 0.913, and 0.933 whereas FrMSO + DBN is 0.964. The competence of existing with FrMSO + DBN considering precision is 10.062%, 8.402%, 7.157%, 5.290%, 3.215%. The recall investigation is shown in Fig. 7b. For 60% data, the recall attained by existing are 0.697, 0.710, 0.725, 0.747, 0.867 whereas FrMSO + DBN is 0.884. Also, for 90% data, the recall attained by existing are 0.817, 0.839, 0.869, 0.876, 0.957, whereas FrMSO + DBN is 0.983. The competence of existing with FrMSO + DBN considering recall is 16.887%, 14.649%, 11.597%, 10.885%, 2.644%. The F-measure investigation is shown in Fig. 7c. For 60% data, the F-measure attained by existing are 0.700, 0.720, 0.733, 0.763, 0.786, whereas FrMSO + DBN is 0.819. Also, for 90% data, the F-measure attained by existing are 0.852, 0.878, 0.889, 0.901, 0.921 whereas FrMSO + DBN is 0.954.

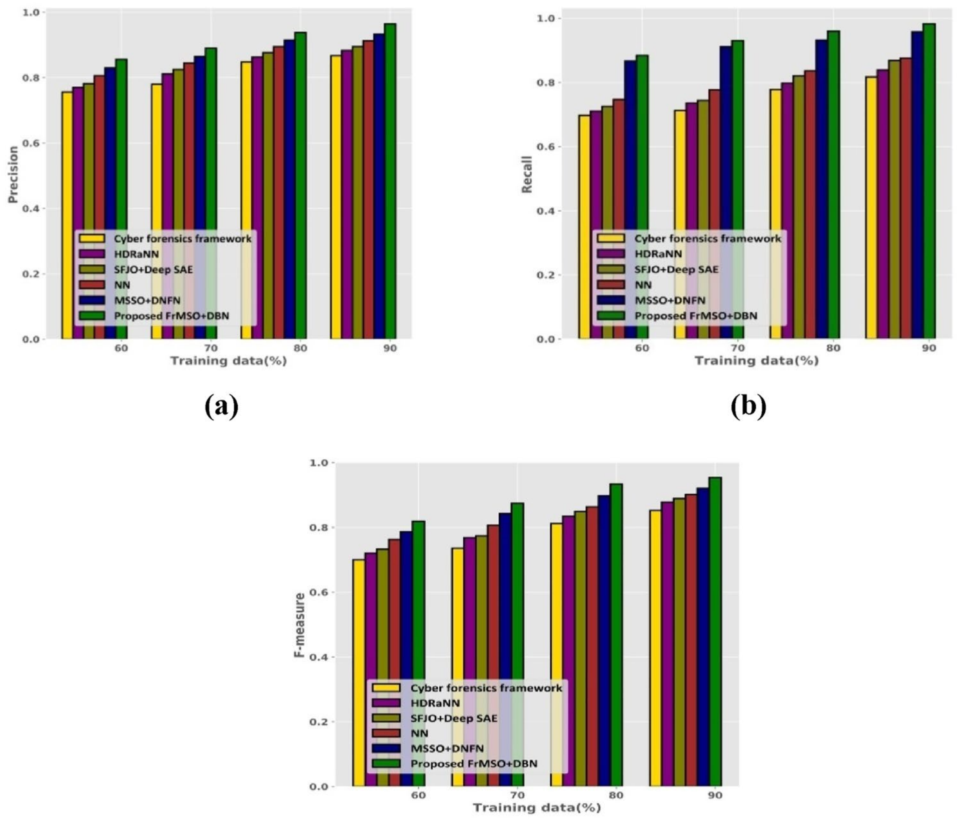


(a)

(b)

(c)

Fig. 6 Algorithms analysis with DBN considering **a** Precision **b** Recall **c** F-measure



(a)

(b)

(c)

Fig. 7 Assessment of techniques with **a** Precision **b** Recall **c** F-measure

The competence of existing with FrMSO + DBN considering F-measure is 10.691%, 7.966%, 6.813%, 5.555%, and 3.459%.

6 Conclusion

This paper presented a novel cyber forensics model, namely FrMSO-based DBN for identifying the cyber-attacks and traced them in IoT. It is due to the fact that the security aspects of IoT is in rise as an industry and public employs novel technologies with huge number of streaming data. Here, the network examination process is detailed and the proposed FrMSO-based DBN are briefly described. The total processing is performed with MapReduce framework wherein the mappers perform feature selection with mutual information and DQNN while the reducer performs cyber attack detection with proposed FrMSO-based DBN. Here, the FrMSO are utilized for adapting the best weights of DBN. In addition, the proposed model is validated with the datasets and certain evaluation measures for revealing the efficiency of proposed model. The method presented high precision with significant time-saving and provided better balance amidst the efficiency and detection time. The proposed FrMSO-based DBN give better performance with elevated precision of 96.4%, recall of 98.3% and F-measure of 95.4% respectively. The future works includes execution of this technique in real platform for preventing the cyber attacks and consider other databases to validate reliability of proposed technique.

Data Availability UCSD Network Telescope Aggregrated DDoS Metadata, "https://catalog.caida.org/details/dataset/telescope_ddos", accessed on January 2022.

References

1. P. Y. Chen, S. M. Cheng and K. C. Chen, Information fusion to defend intentional attack in internet of things, *IEEE Internet of Things Journal*, Vol. 1, No. 4, pp. 337–348, 2014.
2. E. F. Jesus, V. R. Chicarino, C. V. De Albuquerque and A. A. D. A. Rocha, A survey of how to use blockchain to secure internet of things and the stalker attack, *Security and Communication Networks*, 2018. https://doi.org/10.1155/2018/9675050.
3. A. A. Diro and N. Chilamkurti, Distributed attack detection scheme using deep learning approach for internet of things, *Future Generation Computer Systems*, Vol. 82, pp. 761–768, 2018.
4. K. Mohammed, A.H., Jebamikyous, H., Nawara, D. and Kashef, R, 2021 Iot cyber-attack detection: A comparative analysis, In *International Conference on Data Science, E-learning and Information Systems*, pp. 117–123

5. Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto and K. Sakurai, Machine learning-based IoT-botnet attack detection with sequential architecture, *Sensors*, Vol. 20, No. 16, pp. 4372, 2020.
6. Q. Abu Al-Haija and S. Zein-Sabatto, An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks, *Electronics*, Vol. 9, No. 12, pp. 2152, 2020.
7. M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K. K. R. Choo and R. M. Parizi, An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic, *IEEE Internet of Things Journal*, Vol. 7, No. 9, pp. 8852–8859, 2020.
8. Cervantes, C.; Poplade, D.; Nogueira, M.; Santos, A, Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things, In *Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management* (IM), 2015
9. Guo, Z.; Harris, I.G.; Jiang, Y.; Tsaur, L.F, An efficient approach to prevent battery exhaustion attack on BLE-based mesh networks, In *Proceedings of the International Conference on Computing, Networking and Communications* (ICNC), 2017
10. B. Jia, Y. Ma, X. Huang, Z. Lin and Y. Sun, A novel real-time DDoS attack detection mechanism based on MDRA algorithm in big data, *Math. Probl. Eng.*, 2016. https://doi.org/10.1155/2016/1467051.
11. K. J. Singh, K. Thongam and T. De, Entropy-based application layer DDoS attack detection using artificial neural networks, *Entropy*, Vol. 18, pp. 350, 2016.
12. Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto and K. Sakurai, Towards a lightweight detection system for cyber attacks in the IoT environment using corresponding features, *Electronics*, Vol. 9, No. 1, pp. 144, 2020.
13. A. Samy, H. Yu and H. Zhang, Fog-based attack detection framework for internet of things using deep learning, *IEEE Access*, Vol. 8, pp. 74571–74585, 2020.
14. T. Gopalakrishnan, D. Ruby, F. Al-Turjman, D. Gupta, I. V. Pustokhina, D. A. Pustokhin and K. Shankar, Deep learning enabled data offloading with cyber attack detection model in mobile edge computing systems, *IEEE Access*, Vol. 8, pp. 185938–185949, 2020.
15. P. Kumar, G. P. Gupta and R. Tripathi, Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for iot networks, *Arabian Journal for Science and Engineering*, Vol. 46, No. 4, pp. 3749–3778, 2021.
16. G. S. Chhabra, V. P. Singh and M. Singh, Cyber forensics framework for big data analytics in IoT environment using machine learning, *Multimedia Tools and Applications*, Vol. 79, No. 23, pp. 15881–15900, 2020.
17. Z. E. Huma, S. Latif, J. Ahmad, Z. Idress, A. Ibrar, Z. Zou, F. Alqahanti and F. Baothman, A hybrid deep random neural network for cyberattack detection in the industrial internet of things, *IEEE Access*, Vol. 9, pp. 55595–55605, 2021.
18. S. Venugopal, G. W. Sathianesan and R. Rengaswamy, 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*, 2021. https://doi.org/10.1002/jnm.2892.
19. A. Karimi, S. Abbasabadei, J. A. Torkestani and F. Zarafshan, Cybercrime detection using semi-supervised neural network, *Computer Science Journal of Moldova*, Vol. 86, No. 2, pp. 155–183, 2021.
20. A. V. Dhumane and R. S. Prasad, Multi-objective fractional gravitational search algorithm for energy efficient routing in IoT, *Wireless networks*, Vol. 25, No. 1, pp. 399–413, 2019.
21. S. Krinidis and V. Chatzis, A robust fuzzy local information C-means clustering algorithm, *IEEE transactions on image processing*, Vol. 19, No. 5, pp. 1328–1337, 2010.
22. K. Beer, D. Bondarenko, T. Farrelly, T. J. Osborne, R. Salzmann, D. Scheiermann and R. Wolf, Training deep quantum neural networks, *Nature communications*, Vol. 11, No. 1, pp. 1–6, 2020.
23. M. M. Hassan, M. G. R. Alam, M. Z. Uddin, S. Huda, A. Almogren and G. Fortino, Human emotion recognition using deep belief network architecture, *Information Fusion*, Vol. 51, pp. 10–18, 2019.
24. P. R. Bhaladhare and D. C. Jinwala, A clustering approach for thediversity model in privacy preserving data mining using fractional calculus-bacterial foraging optimization algorithm, *Advances in Computer Engineering*, 2014. https://doi.org/10.1155/2014/396529.
25. K. Zervoudakis and S. Tsafarakis, A mayfly optimization algorithm, *Computers & Industrial Engineering*, Vol. 145, pp. 106559, 2020.
26. Kaveh, A. and Zaerreza, A., "Shuffled shepherd optimization method: a new meta-heuristic algorithm", Engineering Computations, 2020
27. UCSD Network Telescope Aggregrated DDoS Metadata, https://catalog.caida.org/details/dataset/telescope_ddos, Accessed on January 2022

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

Suman Thapaliya: has completed his undergraduate studies of "Computer Science" from London Metropolitan University, UK in 2013. Since then he have started working as Network/System Engineer in one of leading ISP in Nepal. Worked under core experienced and professional's ICT team, he have 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 for postgraduate education. He Graduated in Information Technology with thesis title "Implementation and adaptation of software engineering in software development" comparative analysis between Nepal and India from London Metropolitan University, UK 2017. He started Ph.D. in 2018 in Information Security (IS) Audit with research work in Cyber Security Domain. 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, he is contributing at Udemy and Cybrary as Instructor and Mentor respectively.

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. He 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. He 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, he 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, he is an avid public speaker and is associated with various clubs. He also enjoys socializing with technologists.