User Activity Analysis Via Network Traffic Using DNN and Optimized Federated Learning based Privacy Preserving Method in Mobile Wireless Networks

Dr.R. Udayakumar[1*], Dr. Suvarna Yogesh Pansambal[2], Dr. Yogesh Manohar Gajmal[3], Dr.V.R. Vimal[4] and Dr.R. Sugumar[5]

[1*]Dean, CS & IT, Kalinga University, India. rsukumar2007@gmail.com, deancsit@kalingauniversity.ac.in, Orcid: https://orcid.org/0000-0002-1395-583X

[2]Associate Professor, Department of Computer Engineering, Atharva College of Engineering, University of Mumbai, India. suvarna.atharv@gmail.com, Suvarnashirke@atharvacoe.ac.in, Orcid: https://orcid.org/0000-0002-8920-1102

[3]Associate Professor, Finolex Academy of Management and Technology, Ratnagiri, Maharashtra, India. yogesh.gajmal@famt.ac.in, Orcid: https://orcid.org/0000-0002-0562-0423

[4]Professor, Institute of CSE, Saveetha School of Engineering, Saveetha Institute of Medical & Technical Sciences, Thandalam, Chennai, India. vimalraman2004@gmail.com Orcid: https://orcid.org/0000-0001-9401-4507

[5]Professor, Institute of CSE, Saveetha School of Engineering, Saveetha Institute of Medical & Technical Sciences, Thandalam, Chennai, India. sugu16@gmail.com, Orcid: https://orcid.org/0000-0002-0801-6600

Received: March 14, 2023; Accepted: May 20, 2023; Published: June 30, 2023

Abstract

Mobile and wireless networking infrastructures are facing unprecedented loads due to increasing apps and services on mobiles. Hence, 5G systems have been developed to maximise mobile user experiences as they can accommodate large volumes of traffics with extractions of fine-grained data while offering flexible network resource controls. Potential solutions for managing networks and their security using network traffic are based on UAA (User Activity Analysis). DLTs (Deep Learning Techniques) have been recently used in network traffic analysis for better performances. These previously suggested techniques for network traffic analysis typically need voluminous information on network usages. Hence, this work proposes OFedeMWOUAA (optimal federated learning-based UAA technique with Meadow Wolf Optimisation) and DNN (deep Neuron Networks) for minimizing risks of data leakages in MWNs (Mobile Wireless Networks). In the proposed OFedeMWOUAA, the need to submit data to cloud servers does not arise because it trains DLTs locally and only uploads model gradients or knowledge weights. The OFedeMWOUAA approach effectively decreases dangers to data privacies with very minor performance losses in simulations.

Keywords: User Activity Analysis, Network Traffic, Deep Neural Network, Optimized, Federated Learning, Meadow Wolf Optimization and Mobile Wireless Networks.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 14, number: 2 (June), pp. 66-81. DOI: *10.58346/JOWUA.2023.I2.006*

*Corresponding author: Dean, CS & IT, Kalinga University, India.

1 Introduction

MWNs which have recently received significant interest from both academia and industry are combinations of wireless communication networks and mobile devices (Fang, D., 2017) (Tilson, D., 2012) (Zhang, X., 2018). MWNs consist of MNs (Mobile Nodes), multiple APs (Access Points), and an Authentication Server where MNs denote users' mobile devices including laptops or smart phones. These devices have constrained resources in terms of storage, computation, and communication capabilities (Jo, H.J., 2013) (Alzahrani, B.A., 2020) (Papadimitratos, P., 2021). Users in MWNs access the Internet anytime and anywhere using APs provided by remote providers. The movements of MNs result in frequent handovers between APs due to restricted geographical coverage of APs. For practical applications in MWNs, secure authentication during data transmissions is a necessity for guaranteeing that only authorised MNs access MWNs and prevent adversaries from accessing MWNs during connections. UAA techniques are appropriate for securing mutual authentications between MNs and APs. Fig. 1 depicts typical MWNs independent of underlying UAA implementation specifics.

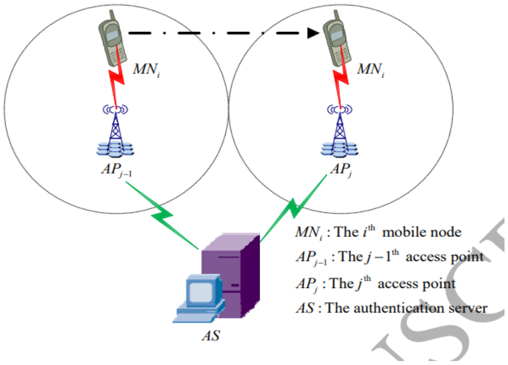

MN_i
MN_i
AP_{j-1}
AP_j
AS
MN_i : The i^{th} mobile node
AP_{j-1} : The $j-1^{th}$ access point
AP_j : The j^{th} access point
AS : The authentication server

Figure 1: A Typical MWN

A general architecture of applications in MWNs is shown in Fig. 2. In addition to offering conventional voice and data connections, MWNs can also connect wide ranges of innovative societal gadgets and applications (5G security, 2015). Specific 5G application cases include connectivity between vehicles and infrastructures, industrial automations, health services and smart cities/homes (Global Mobile Suppliers Association, 2015). It is anticipated that large IoT (Internet of Things) and vital services offered by 5G wireless networks would improve mobile broadband (Leading the World to 5G, 2016). There are multiple challenges in terms of security in these new architectures, technologies, and use cases of 5G wireless networks (5G security, 2015).

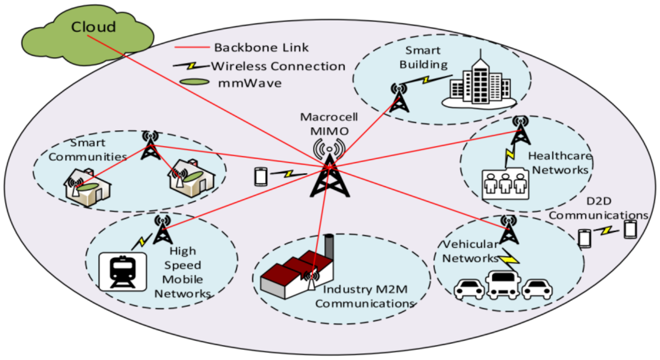


Figure 2: Generic Architecture of Applications of MWNs (Fang, D., 2017)

Future communication systems need to assess user characteristics and offer a variety of high-quality services in addition to be able to watch and spot malevolent users who can deter network securities. UAA is suggested as a potential method based on network traffics to evaluate user characteristics, identify user activities, and find user anomalies (Pacheco, F., 2018). DLTs have been included into many communication situations recently, including the physical, network, and data connection layers due to performances of classifications or regressions on ultra-high dimensional data. DLTs have been used in physical layers (Huang, H., 2019), auto encoder-based end-to-end communication system designs (Ye, H., 2020), and automated modulation recognitions (Wang, Y., 2020). signal detections (Li, C., 2021), and beamforming designs (Huang, H., 2019). In network layers (Liu, L., 2018) (Mao, Q., 2018) (Zhang, C., 2019), routing establishments, optimizations (Zhao, L., 2019), and network securities (Guo, Y., 2021) (Xia, J., 2019) have been enhanced by DLTs.

Numerous studies on data link layers (Sun, H., 2017), channel resource allocations (Li, Y., 2017) and link assessments (Feltrin, L., 2018) have been based on DLTs. One of the most important strategies for network security is UAA based on DLTs and MLTs (Machine Learning Techniques) (Parwez, M.S., 2017) . These UAA techniques, also known as CentUAA, are centralised techniques where user network traffic data must be transferred to cloud servers. However, when data includes users' private information, CentUAA techniques may not be secure. This work suggested an OFL (optimal federated learning) based UAA approach, known as OFedeMWOUAA for 4G networks where users need not upload their network traffic data but train local models using data local network traffic data. The learned knowledge, which may take the form of mode weight or model gradient, should then be uploaded onto a cloud server for the aim of gathering and enhancing this information (Yang, J., 2022).

The remainder of this paper is structured as follows. Network traffic and FL related works are detailed Section 2 followed by a system model and network traffic dataset regarding in Section 3. The suggested FedeUAA technique is presented in section 4 while results of simulations are presented in Section 5. This paper concludes with Section 6.

2 Related Work

The goal of suggested predictive techniques for mobile networks was to improve overall efficacies in accuracies and innate traffic/mobility dynamics of systems. For lowering the danger of data leakage in MWNs, Guo et al. (Guo, L., 2021) presented a federated learning-based UAA approach (known as FedeUAA). When using the FedeUAA approach, directly trains DNN models on local devices. It is not necessary to send data to a cloud server; instead, just information like models' weights or gradients must be transferred. According to simulation studies, FedeUAA minimizes the risks in data privacy leakage while incurring very minimal performance degradations. The possibility of data privacy exposure is one of these approaches' main concerns, though.

Fazio et al., (Fazio, P., 2023) defined the dynamics of mobile nodes in advance with anticipated knowledge about their stability (in terms of mobility) by analysing mobility grade trends for mobile ad-hoc networks and their comprehensions apriori. Their simulations included mobility on geographic maps where their results confirmed the relevance of their proposed schema. However, additional dynamics result in considerable changes in the values of routing tables as the network is constructed with many nodes.

Chowdhury & De (Chowdhury, A., 2020) suggested MSLG-RGSO (Movement Score based Limited Grid-mobility approach using Reverse Glowworm Swarm Optimization) algorithm for MWNs to achieve maximum sensor movement efficiencies and minimal energy usages. The suggested schema enhanced sensor network performances by restricting sensor movements based on movement scores and careful placements of nodes on significant grid-points. Calculations determined sensor node velocity changes with respect to proximity of other nodes. Their simulation findings show that, in compared to current Reverse Glowworm Swarm Optimisation technique, the suggested approach decreased energy usage by 14 to 70%. The simulation's conclusion showed that total distances travelled by sensor nodes are reduced between 14-45%, in comparison to conventional techniques. As a result, this suggested technique is implemented in wireless sensor networks as an energy-efficient method. The mobility of the sensors must be effective if MWNs are to use lesser energies. However, balancing energy usages and sensors coverage ranges may be extremely difficult.

Ding et al., (Ding, A.Y., 2014) advocated the use of SDN (Software Defined Networking) and its benefits were fully used to address problems. They concentrated on the security elements and looked into enhancing security with SDN for MWNs as security problems in networks pose severe challenges. Due to the growing demand and the counts of mobile users, the current legacy infrastructure is already in need of an upgrade to address its current network management and security shortcomings.

Wanalertlak et al., (Wanalertlak, W., 2011) reduced scanning overheads of IEEE 802.11 networks using Behavior-based Mobility Prediction technique. This was achieved by taking into account not just location data but also categories of users, durations and time of day as characteristics. They could identify mobile users' recurrent behaviours within a short time and provided accurate next-cell forecasts. When compared to other location-only based approaches, this campus network’s simulations and local wireless networks showed that their recommended technique reduced average handoff times by 24-25 ms and boosted next-cell prediction accuracies by 23-43%. However, lowering handoff delay is particularly crucial as their size and complexity keep expanding.

He et al., (He, D., 2011) developed straightforward vertical handoff operations for heterogeneous wireless mobile networks. Battery capacities of mobile nodes are significant factors and this study was the first to distinguish mobile nodes with scarce or abundant battery resources in vertical handoffs. It is now more practical in the actual world thanks to this new functionality. In addition, this article introduces a dynamic new call blocking probability to help with wireless network handoff decision-making. According to the results of their experiments, the proposed algorithm outperforms existing algorithms in terms of bandwidth utilisation, handoff dropping rate, and handoff frequency. One of the major barriers to seamless mobility is the lack of simple and reliable vertical handoff solutions that allow a mobile node to roam between different wireless networks.

In order to anticipate user purchasing behaviours, Zhang & Dong (Zhang, H., 2020) presented multi-perspective features based on sample balances. Their data acquisition of users’ historical purchases and behaviours involved ensemble learning. The effective features of users’ purchase behaviours were extracted based on three perspectives namely users, commodities, and interactions for enhancing dimensions of features. Meanwhile, the XGBSFS method was used to pick features. On the Alibaba M-Commerce platform, experiments with sizable actual datasets were conducted. The experimental findings demonstrate that the suggested approach has improved prediction performance across a range of assessment indices, including precision and recall rate. The aforementioned models, however, suffer from limitations in their inability to accurately represent features and their low accuracy while processing the intricate past behavioural data of users.

Parwez et al., (Parwez, M.S., 2017) proposed two different methods. First, we use call detail records from mobile network data (Big Data) to examine the strange behaviour of the mobile wireless network. We employ hierarchical and k-means clustering as unsupervised clustering algorithms for the purpose of anomaly identification. To confirm the accuracy of the observed anomalies, we compare them to data from the real world. From the comparison study, we see that the network recognises an anomaly when there is an abruptly high (unusual) traffic demand at any location and time.

This aids in locating key network areas that require extra attention for things like resource allocation and fault-finding techniques. Second, we use both anomaly-containing and anomaly-free data to demonstrate how anomalies affect eural network-based predictive capacities to learn from data. In this stage, anomalous data was transformed into anomaly-free data and discovery of errors in predictions dramatically decreased when the models were trained on anomaly-free data as opposed to abnormal data. The first layer of the usual model comprises multiple basic learners, but because they all utilise the same training data, the changes in their output values are minimal, which results in poor model generalisation performance.

Lee et al., (Lee, J., 2013) assessed input data after every two hours with data distributions (as measures of connections) across mobile (cellular) and wireless LAN networks based on data distribution (as a connection indicator), application network activity durations, and device-level network traffic volumes. For device-level data volumes, we find usually homogenous values with negligible autocorrelation or long-range dependence, although we notice a possible self-similarity for positively correlated cumulative application network usage periods. We may also see distinctive patterns for both the day of the week and the hour of the day in the average distribution of cellular interface usage. These lessons taken together will be helpful in future attempts to mimic mobile device usage.

Ma & Lin (Ma, J., 2019) proposed novel MBD (mobile big data) architecture with four layers: Three layers made up the application, storage, and fusion layers. They provided a data-driven user experience prediction based on the MDB architecture as an illustration of how to implement their suggested MBD design in wireless networks. The suggested user experience prediction may pre-evaluate user experience through network performance and user behaviour characteristics in a data-driven manner by utilising machine learning methodologies. First, we conduct a preliminary study of data on customer complaints gathered from a significant Chinese MNO's (mobile network operator) network monitoring system. The excessively unbalanced negative and positive samples are then corrected by combining up- and down-sampling. The results reveal that the suggested automated machine learning technique improved prediction accuracy when measured against two baselines that the MNO frequently uses: empirical criteria and a rule-based expert system. In conclusion, there are many outstanding studies on network traffic analysis using FL, however other areas, like the best FL-based UAA, have not yet been fully researched. Consequently, concentrated on the usage of opimal FL in UAA.

3 Proposed Methodology

Because user data does not need to be stored on the cloud server, the danger of privacy leakage is significantly decreased. DNN based UAA using balanced cross entropy losses is proposed for identifying user activities from network traffics of MWNs and assuming the condition of class imbalances. In terms of identification performance, our technique surpassed previous UAA methods based on MLTs. Based on the research efforts stated above, FL is added to UAA to safeguard security and privacy, and the FL-based UAA approach is called as OFedeMWOUAA. Introduce two different optimisation techniques for OFedeMWOUAA, namely MA (model averaging) and SPGD (stochastic parallel gradient descent), as illustrated in Fig. 3. According to simulation findings, the OFedeMWOUAA method can lessen the danger of data privacy leakage and performs similarly to the centralised method in terms of performance.

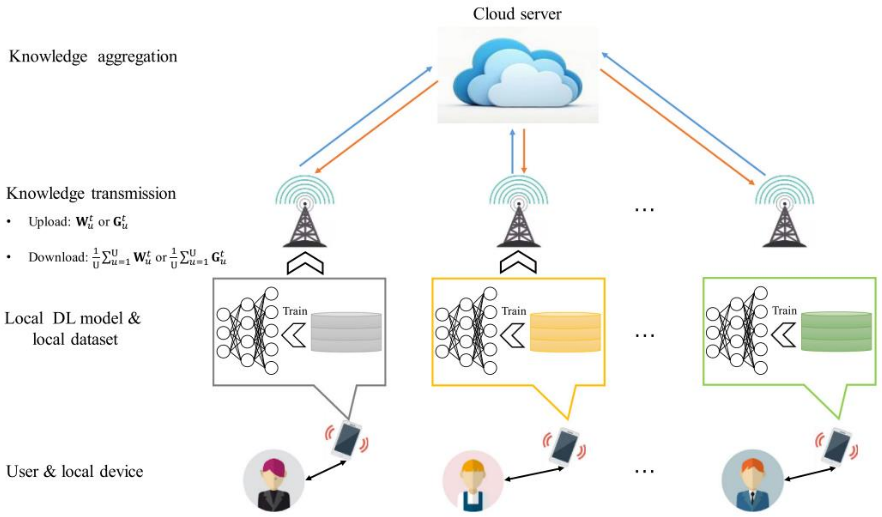

Cloud server
Knowledge aggregation
Knowledge transmission
• Upload: $\mathbf{W}_u^t$ or $\mathbf{G}_u^t$
• Download: $\frac{1}{\mathrm{U}}\sum_{u=1}^{\mathrm{U}}\mathbf{W}_u^t$ or $\frac{1}{\mathrm{U}}\sum_{u=1}^{\mathrm{U}}\mathbf{G}_u^t$
Local DL model & local dataset
Train
Train
Train
User & local device
…
…
…

Figure 3: The Architecture of OFedeMWOUAA

4 Input Dataset

In this study, just three user behaviours were considered: viewing videos, listening to audio, and exploring the webs. One network traffic sample contains the time stamp, source IP, destination IP, protocol, and packet size. It should be noted that the protocol, source IP address, and destination IP address are all transformed to countable serial numbers. All classes in the dataset are distributed as follows: video is represented by 21386, audio is represented by 13026, and web is represented by 3868. It should be mentioned that the dataset has a problem with class imbalance, particularly in the class "Video." The dataset is split into a training dataset and a test dataset in a 9:1 ratio in centralised systems, with the remaining 30% of the training dataset being used for validation and the remaining 70% for training. In order to implement federated solutions, the dataset is also split into a training dataset and test dataset with a 9:1 ratio, but the training dataset is randomly divided into nine parts as the local datasets to simulate nine users.

The structure of DNN: DNN is made up of several fully-connected (FC) layers, each of which has 512, 256, 128, 64, 32, 16, 8, and 3 neurons. Additionally, to prevent overfitting, the majority of FC layers employ ReLU (rectified linear unit) as the activation function and l2 regularization with a factor of 0.0001, while the last FC layer uses Softmax. Given that UAA is modeled as a multi-classification issue, CE (cross entropy) often serves as the problem's loss function.

$$f_{\mathbb{CE}}(\{\mathbb{S}_i, \mathbb{a}_i\}\mathbb{N}\ i = 1\,; \mathbb{W}) = -\frac{1}{\mathbb{N}}\sum_{i=1}^{\mathbb{N}} a_i\ log[f_{\mathbb{DNN}}(\mathbb{S}_i; \mathbb{W}], \tag{1}$$

where $\{\mathbb{S}_i, \mathbb{a}_i\}_{i=1}^{\mathbb{N}}$ i=1 stands for training sample sets, and $\mathbb{W}$ represents weights of DNN. However, taking into account the dataset's class imbalance problem, a unique loss function called balanced CE, which can be stated as, is created to balance the difference between various classes.

$$f_{Balanced\mathbb{CE}}(\{\mathbb{S}_i, \mathbb{a}_i\}_{i=1}^{\mathbb{N}} = 1\,;\ \mathbb{W})\ = \tag{2}$$

$$-\frac{1}{\mathbb{N}}\sum_{j=1}^{3} r^j \sum_{i=1}^{\mathbb{N}^j} a_i^j\, log[f_{\mathbb{DNN}}(\mathbb{S}_i^j; \mathbb{W})], \tag{3}$$

where $\left\{\mathbb{S}_i^j\ , a_i^j\right\}_{i=1}^{\mathbb{N}}\ , j\ \in\ \{1, 2, 3\}$ represents the set of samples and its labels about the jth class, and $\sum_{j=1}^{3}\mathbb{N}^j\ = \mathbb{N};\ r^j, j\ \in\ \{1, 2, 3\}$ is the ratio of the jth class, which can be expressed as

$$r^{j} = \frac{\frac{1}{\mathbb{N}^{i}}}{\sum_{i=1}^{3}\frac{1}{\mathbb{N}^{j}}}. \tag{4}$$

This work uses SGD (stochastic gradient descent) to reduce loss function and shown below:

$$\mathbb{W}^{t+1} = \mathbb{W}^{t} - \eta \cdot \mathbb{G}^{t}, \tag{5}$$

where $\mathbb{W}^{t}$s refers to model weights at tth epochs; η implies learning rates; $\mathbb{G}^{t}$ stands for gradient at t th epochs.

The architecture of FedeUAA: FedeUAA consists of four main steps, which are shown as follows.

- Train local DLTs: The first stage is to train local DLTs based on users' datasets, which often contain users' private information and cannot be shared;
- Upload obtained knowledge: The knowledge, which may be the weights or gradients of DLTs, is transferred from these local DLTs to the cloud server;
- Aggregate obtained knowledge: The uploaded knowledge is compiled on a cloud server using an aggregation algorithm that determines the average gradient or weight;
- Save information: Each user receives a download of the aggregated weight or gradient, which updates their local DLTs. Repeat the previous stages until convergence.

For FedeUAA, there are two optimisation techniques: MA and SPGD (stochastic parallel gradient descent). The gradients from local DLTs, on which SPGD is built, can be represented as

$$\mathbb{W}^{t,b+1} = \mathbb{W}^{t,b} - \eta \cdot \left(\frac{1}{\mathbb{U}}\sum_{u=1}^{\mathbb{U}}\sum \mathbb{G}_{u}^{t,b}\right), \tag{6}$$

where b represents the bth batch, where U is the counts of FedeUAA users and t is the counts of epochs. MA is based on local DLT weights, which may be expressed as

$$\mathbb{W}_{u}^{t+1} = \mathbb{W}_{u}^{t} - \eta \cdot \mathbb{G}_{u}^{t}, \tag{7}$$

$$\mathbb{W}^{t+1} = \frac{1}{\mathbb{U}}\sum_{u=1}^{\mathbb{U}} W_{u}^{t+1}. \tag{8}$$

It is clear that the uploaded information distinguishes MA from SPGD. All users must update their local models using their local datasets, and the SPGD method aggregates these local model weights to generate the global model weight. Each user computes his or her own local gradients, which are subsequently used to update the global model.

OFedeMWOUAA: OFedeMWOUAA detected UAA in WMN based on Algorithm 1. Servers that coordinated the training of DNNs for choosing iteration/epoch counts and batch sizes were utilised in the framework, which also utilised mobile devices to access model parameter servers. A popular method for improving the accuracy of DNNs models is increasing the depth of the model layers. Weight characteristic counts that necessitate training rise. When the model created on client computers is sent to servers in Florida, the cost of network transmission climbs significantly. Due to this, OFede leveraged on MWO's chosen capabilities to communicate regardless of sizes and acquired clients with the highest weights in order to prevent their transmissions. The lowest loss value discovered after teaching the user is used to determine the best score.

First, the approach determines the initial solution of MWs by defining it as a crowd of embedding places, which requires $\mathbb{N}_{pop} \in \mathbb{N}^{*}$packs, each holding $\mathbb{N}_{MW} \in \mathbb{N}^{*}$MW. Distribution among the packets at the outset is arbitrary. The social conditions that are taken into account while making decisions are denoted by the symbol "sc," and the quantities of the MWth MW in the jth aspect at period intervals are defined as follows:

$$scd_{MW,j}^{\mathbb{p},\mathbb{t}} = \mathfrak{l}w\mathfrak{b}_{j} + rand_{j} \cdot \left(\mathfrak{u}p\mathfrak{b}_{j} - \mathfrak{l}w\mathfrak{b}_{j}\right) \tag{9}$$

Where $\mathfrak{l}w\mathfrak{b}_j$ and $up\mathfrak{b}_j$are the limits of the j th parameter, and $rand_j$∈ [0, 1] is just a random integer with the same probability for each value. Step two entails using accuracy to determine the values of the goal function for each group of choice variables.

$$fit_{MW,j}^{\mathbb{p},\mathbb{t}} = \max(accuracy) \tag{10}$$

Eq. 5 is used to determine how well the final emerges; as a result, image fits the criteria for the embedding sites of interest. The MWO considers the probability with which a Meadow Wolf (MW) moves from one pack to another, which depends on the counts of MWs in the population $\mathbb{N}_{MW}$, and is given by: Prob=0.005*$\mathbb{N}_{MW}$ (Chi, Mingwen., 2019). Additionally, the MW algorithm considers the alpha, which is the $\mathbb{N}_{MW}$ with the lowest optimal solution unit cost in the $\mathbb{p}$th pack at the $\mathbb{t}$th timestamp, and is defined as:

$$\mathfrak{alpha}^{\mathbb{p},\mathbb{t}} = \left\{scd_{MW,j}^{\mathbb{p},\mathbb{t}} \,|\, \arg_{MW=\{1,2,\ldots,MW\}} \max(accuracy)\right\} \tag{11}$$

The MWO also takes into account the cultural practice $\mathfrak{C}l\mathfrak{R}$, which is calculated as follows based on estimates made inside each pack:

$$\mathfrak{C}l\mathfrak{R}_j^{\mathbb{p},\mathbb{t}} = \begin{cases} \mathbb{R}ef_{\left(\frac{\mathbb{N}_{MW}+1}{2}\right),j}^{\mathbb{p},\mathbb{t}} & \mathbb{N}_{MW} \ is\ odd \\ \frac{\mathbb{R}ef_{\left(\frac{\mathbb{N}_{MW}}{2}\right),j}^{\mathbb{p},\mathbb{t}} + \mathbb{R}ef_{\left(\frac{\mathbb{N}_{MW}+1}{2}\right),j}^{\mathbb{p},\mathbb{t}}}{2} & otherwise \end{cases} \tag{12}$$

Specifically, for any j in the range [1, SD], wherein SD is the size of the solution space,$\mathbb{R}ef^{\mathbb{p},\mathbb{t}}$ reflects the ordered social circumstances of all MWs of the $\mathbb{p}$th packs at the j time point. The birth and death of MWs are coordinated by the algorithm based on the values of the target function and also the MWs' ages, which are determined in years and defined as.

$$age_{MW}^{\mathbb{p},\mathbb{t}} \in N \tag{13}$$

The Algorithm 1 describes this process, where OF stands for the set of MWs with the lowest values for the objective function and o for the maximum population of MWs in this category. The young MW designated the pup YMW and all the MWs in the pack are compared for their objective function values to create the group of OFMWs. The social interactions of two randomly selected parents and an environmental component are combined to produce the pups. No of their social standing, the parents are chosen. The pups are therefore described as:

$$YPW_j^{\mathbb{p},\mathbb{t}} = \begin{cases} scd_{PW_1,j}^{\mathbb{p},\mathbb{t}} & urand_j > Prob_{sp} \text{ or j} = \mathrm{j}_1 \\ scd_{PW_2,j}^{\mathbb{p},\mathbb{t}} & urand_j \geq Prob_{im} + Prob_{ap}\ or\ j = j_2 \\ rand_j & otherwise \end{cases} \tag{14}$$

where PW_1 and PW_2 are the two MWs from the $\mathbb{p}$th pack who are selected to undertake the diversity of the MWs. j_1 and j_2 are randomly generated measurements of the optimization process,$Prob_{sp} = \frac{1}{diversity}$ is used for calculating the scatter probability, $Prob_{ap} = \frac{(1-Prob_{im})}{2}$ represents the association probability $rand_j$is a random number between 0 and m restricted to the limits of the jth timeline's objective functions, and $urand_j$is a consistently generated random number. Additionally, $Prob_{im}$ imbalances the creative effect evenly across both parents. The MWs are written as follows under the entire pack motivation (mot_w) and the alpha motivation (mot_a):

$$mot_w = \mathfrak{C}l\mathfrak{R}_j^{\mathbb{p},\mathbb{t}} - scd_{cdiff_1,j}^{\mathbb{p},\mathbb{t}}$$
$$mot_a = \mathfrak{alpha}^{\mathbb{p},\mathbb{t}} - scd_{cdiff_2,j}^{\mathbb{p},\mathbb{t}} \tag{15}$$

where the terms $cdiff_1$" and " $cdiff_2$" stand for "differences in cultures from a random MW" and "clash of cultures between a unique MW of the group and the alpha MW," respectively. The MW's new social state is updated by applying the formula below, where $\mathfrak{w}_w$ and $\mathfrak{w}_a$are the collection and alpha involvement weights, respectively, and are evenly spread random values ranging ∈ [0, 1].

$$newscd_{MW,j}^{\mathbb{p},\mathbb{t}} = scd_{MW,j}^{\mathbb{p},\mathbb{t}} + \mathfrak{w}_w \cdot mot_w + \mathfrak{w}_a \cdot mot_a \tag{16}$$

The algorithm's final solution is the best solution out of all the packs since it's based on the best social condition, which is reserved using eq, (10).

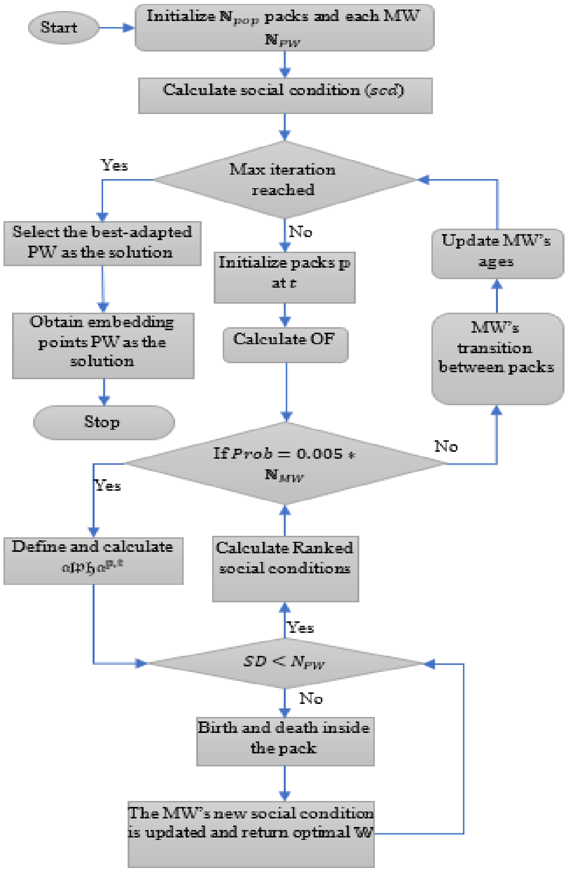
$$scd_{MW,j}^{\mathbb{p},\mathbb{t}+1} = \begin{cases} new\mathbb{s}scd_{MW,j}^{\mathbb{p},\mathbb{t}} & newfit_{MW,j}^{\mathbb{p},\mathbb{t}} < fit_{MW,j}^{\mathbb{p},\mathbb{t}} \\ scd_{MW,j}^{\mathbb{p},\mathbb{t}} & otherwise \end{cases} \tag{17}$$

$\mathbb{N}_{MW}$ can be calculated in terms in the range, and $\mathbb{N}_{pop}$ can then be changed to provide the algorithm's overall population size. The steps are followed higher than or equal till a large iteration count. As a result, the produced private shares might be sent as give the appearance of UAA for protected data.

Algorithm 1: The Pseudocode of OFedeMWOUAA

```
Input: The numbers of the MW, fitness, max iterations
Output: Produce better embedding points.
Algorithm 1 FedeUAA (DNN, Balanced CE, SPGD).
Input: Network traffic samples and their corresponding user activities $\{\mathbb{S}_i, \mathbb{a}_i\}_{i=1}^{\mathbb{N}}$ ;
Output: Model weight W;
Condition 1: when SPGD usage
    • Construct DNN and set loss function, learning rate and other key parameters;
    • for$t = 1,2,\dots,\mathbb{T}$do:
    • for$b = 1,2,\dots,\mathbb{B}$do:
    • Users calculate their local gradients $\mathbb{G}_u^{t,b}$ at the $b$ −th epoch of the $t$-th epoch;
    • Users upload their local gradients to the cloud server;
    • The cloud server calculates the average of these local gradients as the global gradient;
    • The cloud server downloads the global gradient to every user for updating the global model
      weight $\mathbb{D}$Eq.(6);
Condition 2: when SPGD usage
    • 2: for t = 1, 2, ..., T do:
    • 3: Users update their local model weight $\mathbb{W}_u^t$by their local datasets and Eq. (6);
    • 4: Users upload their model weight to the cloud server;
    • 5: The cloud server aggregates these local model weight by Eq. (7);
    • 6: The cloud server downloads the aggregated model weights to every user;
Procedure call MWO ()
Initialize the social conditions of nodes all MWs
Calculate the $\mathbb{s}$scd of all MWs
Calculate the objective function based on PSNR
Also takes into account the alpha MW and calculate age
Sort objective function's values in ascending order $OF$ based on $Y$MW
If $urand_j < Prob_{sp} and \geq Prob_{im}$then
For each MW of the $new\mathbb{s}\mathrm{scd}_{\mathrm{MW},j}^{\mathbb{p},\mathbb{t}}$ do
Update the social conditions of MWs
```

```
If a random number $Prob = 0.005 * \mathbb{N}_{\mathrm{MW}}$, then
The MW leaves its packs and becomes lonely or enters other packs
Endif
Return globalminSC as optimal $\mathbb{W}$
Follow the steps until a large count of iterations have been attained.
The produced private shares were transferable as steganography pictures for protected input images.
End for
end for
end for
```


Start
Initialize $\mathbb{N}_{pop}$ packs and each MW $\mathbb{N}_{PW}$
Calculate social condition (scd)
Max iteration reached
Yes
No
Select the best-adapted PW as the solution
Obtain embedding points PW as the solution
Stop
Initialize packs p at t
Calculate OF
Update MW's ages
MW's transition between packs
If $Prob = 0.005 * \mathbb{N}_{MW}$
Yes
No
Define and calculate $alpha^{p,t}$
Calculate Ranked social conditions
Yes
$SD < N_{PW}$
No
Birth and death inside the pack
The MW's new social condition is updated and return optimal $\mathbb{W}$

Flowchart of MWO for Secure Transaction

5 Experimental Results and Discussion

While previous DLTs in this study are built on the Scikit-learn toolkit, the simulation of OFedeMWOUAA is based on Keras with Tensorflow as a backbend. In Table 3, further simulation parameters are listed. DNN's learning rate is 0.001, its training epochs are 500, and its batch sizes are all obtained using MWO. The accuracy, precision, recall, and F1-score metrics are also included in this study, and the findings are contrasted with those of other established models as FedeUAA (Guo, L., 2021) and neural-network (Parwez, M.S., 2017).

$$Accuracy = \frac{TP + TN}{number\ of\ test\ set} \times 100\% \tag{18}$$

$$Precision \ = \frac{TP}{TP + FP} \times \ 100\% \quad (19)$$

$$Recall \ = \frac{TP}{TP + FN} \times \ 100\% \quad (20)$$

$$F1 \ - \ score \ = \frac{2}{1/Precision + 1/Recall} \times \ 100\% \quad (21)$$

where TP is the counts of samples that are both positive and assessed to be in the positive class, and FP is the counts of samples that are both negative and judged to be in the positive class. The counts of samples that belong to a positive class but are assessed to be in the negative class is called FN, while the counts of samples that belong to a negative class but are also judged to be in the negative class is called TN.

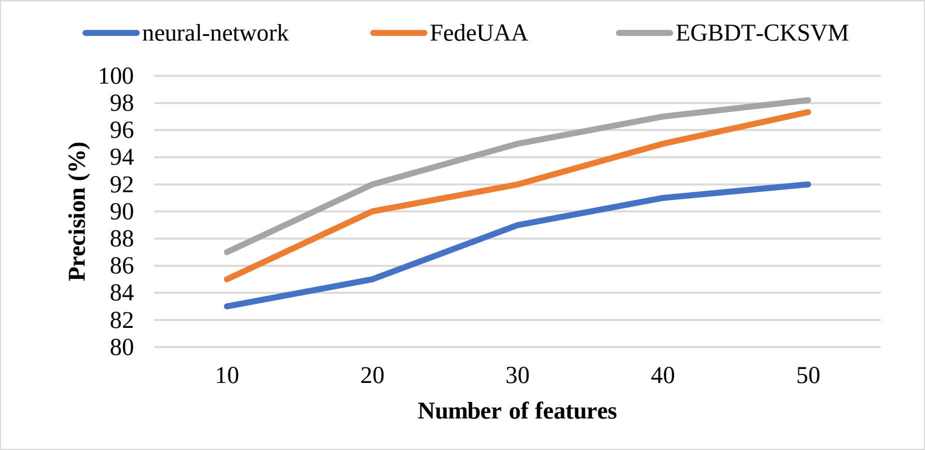


Figure 4: Precision Comparison

Figure 4 displays the accuracy of recommended and existing models for the number of features in a certain database. The precision that comes along with it increases as the counts of features increase. In contrast to the FedeUAA and neural network, the OFedeMWOUAA, for instance, has an accuracy of 98.21%. This is done so that the OFedeMWOUAA may identify a little better sorted collection of input within a set amount of time without using derived factors or high-dimensional features. Compared to existing models, the suggested model performs better. Additionally, by choosing the highest-ranking security characteristics, we were able to decrease overfitting and computation complexity (i.e., the quantity of security features).

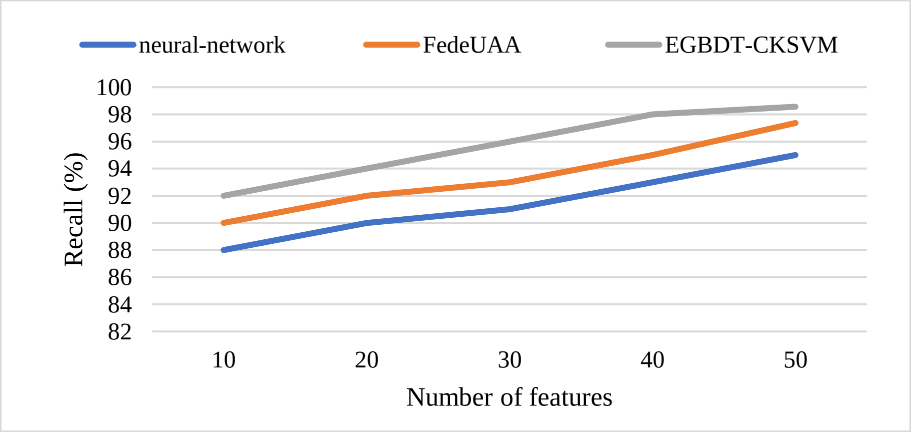


Figure 5: Recall Comparison

The recall of suggested and current models in Fig. 5 display attributes counts in a certain database. As the number of attributes rises, recall is maximised. For instance, when compared to the FedeUAA and neural network, the OFedeMWOUAA gets a recall of 98.56%. This is because the MWO speeds up the computation of the derived factors, making FedeUAA more adaptable. As a consequence, the proposed network might be used to accurately detect UAA.

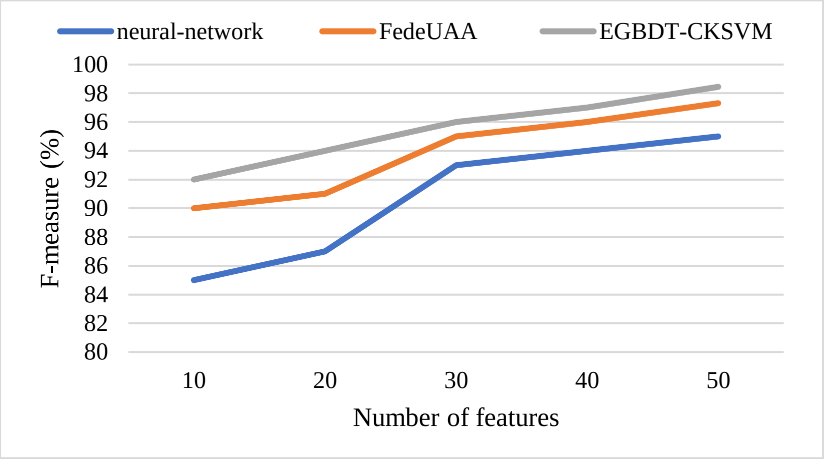


Figure 6: F-measure Comparison

The f-measure of proposed and current models for characteristics counts in a specific database are shown in Fig. 6. The f-measures are maximised while the counts of features maximised. For instance, the OFedeMWOUAA offers an f-measure of 98.45% when compared to all other models, including FedeUAA and neural networks. MWO employs random values for the parameters and reaches a predetermined ending point based on parameters, time, or performance goals. This prevents the data from being overfitted and makes it useful for real-time situations with good performance outcomes.

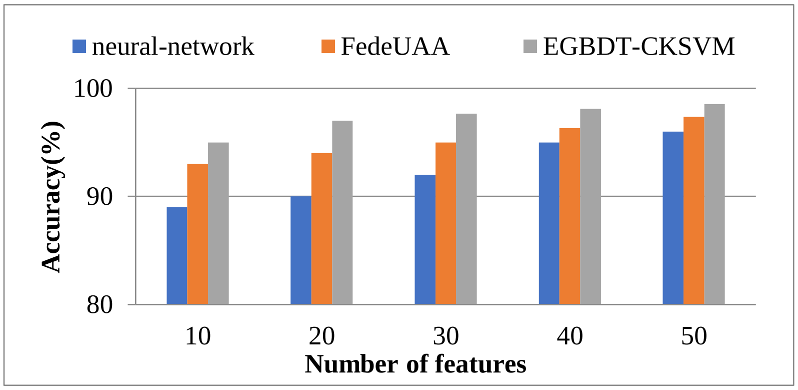


Figure 7: Result of Accuracy Comparison

The accuracy of suggested and current models for the amount of characteristics in a particular database is shown in Fig. 7. The OFedeMWOUAA shortens the processing time while improving accuracy. Since the OFedeMWOUAA only needs a small count of derived components during pre-processing, it achieves an accuracy of 98.56% when compared to all other models. By simultaneously optimising the Fede and improving output classification results, the suggested OFedeMWOUAA framework may greatly increase the performance of UAA classification.

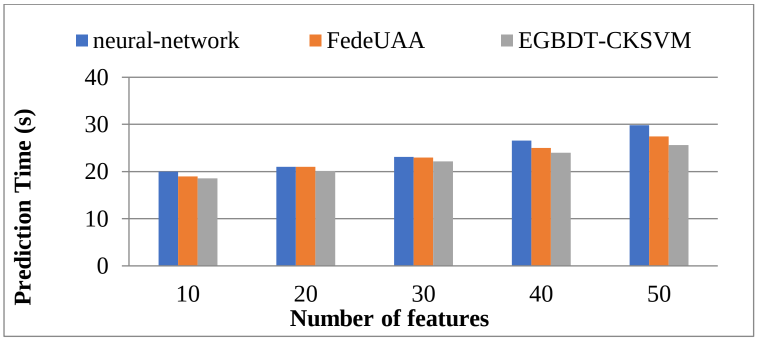


Figure 8: Result of Prediction Time Comparison

As seen in Fig. 8, the OFedeMWOUAA tree outperforms the competition by requiring the least amount of time to train the model—25.64 seconds—while the neural-network based approach requires the most time. After linked characteristics were removed, it is evident that all training times for the schemes decreased. The time it takes to forecast a cyberattack using FedeUAA, OFedeMWOUAA, and neural networks has also dropped. FedeUAA predicts a cyberattack in roughly 27.44 seconds, whereas FedeUAA and neural networks take somewhat longer. It is obvious that the DNN-based UAA method with balanced CE loss function may be more capable of identifying the activity "Video" than the DNN-based UAA method with CE loss function, indicating that the balanced CE loss function is effective for the DNN-based UAA method.

6 Conclusion and Future Work

In order to maintain data privacy, this work presented the OFedeMWOUAA method, which only requires users to contribute newly acquired knowledge rather than actual data. Furthermore, a balanced CE loss function—a sort of CE loss function variant—was developed in response to the data's class imbalance problem. Experiment findings demonstrated that, when compared to the CE loss function, the balanced CE loss function can somewhat improve identification performance. Additionally, there is a slight performance difference between the OFedeMWOUAA approach and existing methods, but it is thought that this performance difference is worth it in order to lower the danger of privacy leaking. It is clear that the OFedeMWOUAA method's convergence speed is a little bit faster than that of the other two types of techniques. Additionally, the loss value of the OFedeMWOUAA method is marginally lower than that of the other two techniques, which again illustrates how well the UAA methods identify objects. In the future, the FL algorithm will be used to other network traffic-related subjects, such as classification and recognition tasks. We will also focus on decreasing communication costs and enhancing training efficacy, which will reduce the cost of FL algorithms in actual applications.

References

[1] 5G security, Ericsson, Stockholm, Sweden, White Paper, Jun. 2015.

[2] 5G security: Forward thinking Huawei white paper, Huawei, Shenzhen, China, White Paper, 2015.

[3] Alzahrani, B.A., Chaudhry, S.A., Barnawi, A., Al-Barakati, A., & Alsharif, M.H. (2020). A privacy preserving authentication scheme for roaming in IoT-based wireless mobile networks. *Symmetry*, *12*(2), 1-18.

[4] Chi, Mingwen (2019). An improved wolf pack algorithm. In *Proceedings of the International Conference on Artificial Intelligence, Information Processing and Cloud Computing*, 1-5.

[5] Chowdhury, A., & De, D. (2020). MSLG-RGSO: Movement score based limited grid-mobility approach using reverse Glowworm Swarm Optimization algorithm for mobile wireless sensor networks. *Ad Hoc Networks*, *106*.

[6] Ding, A.Y., Crowcroft, J., Tarkoma, S., & Flinck, H. (2014). Software defined networking for security enhancement in wireless mobile networks. *Computer Networks*, *66*, 94-101.

[7] Fang, D., Qian, Y., & Hu, R.Q. (2017). Security for 5G mobile wireless networks. *IEEE access*, *6*, 4850-4874.

[8] Fazio, P., Mehic, M., Voznak, M., De Rango, F., & Tropea, M. (2023). A novel predictive approach for mobility activeness in mobile wireless networks. *Computer Networks*, *226*.

[9] Feltrin, L., Buratti, C., Vinciarelli, E., De Bonis, R., & Verdone, R. (2018). LoRaWAN: Evaluation of link-and system-level performance. *IEEE Internet of Things Journal*, *5*(3), 2249-2258.

[10] Global Mobile Suppliers Association. (2015). The road to 5G: Drivers, applications, requirements and technical development. *A GSA Executive Report from Ericsson, Huawei and Qualcomm*.

[11] Guo, L., Wang, S., Yin, J., Wang, Y., Yang, J., & Gui, G. (2021). Federated user activity analysis via network traffic and deep neural network in mobile wireless networks. *Physical Communication*, *48*.

[12] Guo, Y., Zhao, Z., He, K., Lai, S., Xia, J., & Fan, L. (2021). Efficient and flexible management for industrial internet of things: A federated learning approach. *Computer Networks*, *192*.

[13] He, D., Chi, C., Chan, S., Chen, C., Bu, J., & Yin, M. (2011). A simple and robust vertical handoff algorithm for heterogeneous wireless mobile networks. *Wireless Personal Communications*, *59*, 361-373.

[14] Huang, H., Guo, S., Gui, G., Yang, Z., Zhang, J., Sari, H., & Adachi, F. (2019). Deep learning for physical-layer 5G wireless techniques: Opportunities, challenges and solutions. *IEEE Wireless Communications*, *27*(1), 214-222.

[15] Huang, H., Peng, Y., Yang, J., Xia, W., & Gui, G. (2019). Fast beamforming design via deep learning. *IEEE Transactions on Vehicular Technology*, *69*(1), 1065-1069.

[16] Jo, H.J., Paik, J.H., & Lee, D.H. (2013). Efficient privacy-preserving authentication in wireless mobile networks. *IEEE Transactions on Mobile Computing*, *13*(7), 1469-1481.

[17] Leading the World to 5G, QualComm, San Diego, CA, USA, Feb. 2016.

[18] Lee, J., & Seeling, P. (2013). An overview of mobile device network traffic and network interface usage patterns. *In IEEE International Conference on Electro-Information Technology, EIT,* 1-5.

[19] Li, C., Xia, J., Liu, F., Li, D., Fan, L., Karagiannidis, G.K., & Nallanathan, A. (2021). Dynamic offloading for multiuser muti-CAP MEC networks: A deep reinforcement learning approach. *IEEE Transactions on Vehicular Technology*, *70*(3), 2922-2927.

[20] Li, Y., Gursoy, M.C., Velipasalar, S., & Tang, J. (2017). Joint mode selection and resource allocation for D2D communications via vertex coloring. *In GLOBECOM IEEE Global Communications Conference*, 1-6.

[21] Liu, L., Yin, B., Zhang, S., Cao, X., & Cheng, Y. (2018). Deep learning meets wireless network optimization: Identify critical links. *IEEE Transactions on Network Science and Engineering*, *7*(1), 167-180.

[22] Ma, J., & Lin, S. (2019). Big data enabled anomaly user detection in mobile wireless networks. *In IEEE 5th International Conference on Computer and Communications (ICCC)*, 479-484.

[23] Mao, Q., Hu, F., & Hao, Q. (2018). Deep learning for intelligent wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *20*(4), 2595-2621.

[24] Pacheco, F., Exposito, E., Gineste, M., Baudoin, C., & Aguilar, J. (2018). Towards the deployment of machine learning solutions in network traffic classification: A systematic survey. *IEEE Communications Surveys & Tutorials*, *21*(2), 1988-2014.

[25] Papadimitratos, P. (2021). Mix-Zones in Wireless Mobile Networks. *Encyclopedia of Cryptography, Security and Privacy*, 1-5.

[26] Parwez, M.S., Rawat, D.B., & Garuba, M. (2017). Big data analytics for user-activity analysis and user-anomaly detection in mobile wireless network. *IEEE Transactions on Industrial Informatics*, *13*(4), 2058-2065.

[27] Parwez, M.S., Rawat, D.B., & Garuba, M. (2017). Big data analytics for user-activity analysis and user-anomaly detection in mobile wireless network. *IEEE Transactions on Industrial Informatics*, *13*(4), 2058-2065.

[28] Sun, H., Chen, X., Shi, Q., Hong, M., Fu, X., & Sidiropoulos, N.D. (2017). Learning to optimize: Training deep neural networks for wireless resource management. *In IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 1-6.

[29] Tilson, D., Sorensen, C., & Lyytinen, K. (2012). Platform complexity: Lessons from mobile wireless.

[30] Wanalertlak, W., Lee, B., Yu, C., Kim, M., Park, S.M., & Kim, W.T. (2011). Behavior-based mobility prediction for seamless handoffs in mobile wireless networks. *Wireless networks*, *17*, 645-658.

[31] Wang, Y., Yang, J., Liu, M., & Gui, G. (2020). Light AMC: Lightweight automatic modulation classification via deep learning and compressive sensing. *IEEE Transactions on Vehicular Technology*, *69*(3), 3491-3495.

[32] Xia, J., Fan, L., Xu, W., Lei, X., Chen, X., Karagiannidis, G.K., & Nallanathan, A. (2019). Secure cache-aided multi-relay networks in the presence of multiple eavesdroppers. *IEEE Transactions on Communications*, *67*(11), 7672-7685.

[33] Yang, J., Wang, L., & Shakya, S. (2022). Modelling Network Traffic and Exploiting Encrypted Packets to Detect Stepping-stone Intrusions. *Journal of Internet Services and Information Security (JISIS)*, *12*(1), 2-25.

[34] Ye, H., Liang, L., Li, G.Y., & Juang, B.H. (2020). Deep learning-based end-to-end wireless communication systems with conditional GANs as unknown channels. *IEEE Transactions on Wireless Communications*, *19*(5), 3133-3143.

[35] Zhang, C., Patras, P., & Haddadi, H. (2019). Deep learning in mobile and wireless networking: A survey. *IEEE Communications surveys & tutorials*, *21*(3), 2224-2287.

[36] Zhang, H., & Dong, J. (2020). Application of sample balance-based multi-perspective feature ensemble learning for prediction of user purchasing behaviors on mobile wireless network platforms. *EURASIP Journal on Wireless Communications and Networking*, *2020*, 1-26.

[37] Zhang, X., & Zhu, Q. (2018). Scalable virtualization and offloading-based software-defined architecture for heterogeneous statistical QoS provisioning over 5G multimedia mobile wireless networks. *IEEE Journal on Selected Areas in Communications*, *36*(12), 2787-2804.

[38] Zhao, L., Wang, J., Liu, J., & Kato, N. (2019). Routing for crowd management in smart cities: A deep reinforcement learning perspective. *IEEE Communications Magazine*, *57*(4), 88-93.

Authors Biography

Professor. Dr. Udayakumar Ramanathan is serving in Teaching community for more than two decades, he successfully produced 5 Doctoral candidates, he is a researcher, contribute the Research work in inter disciplinary areas. He is having h-index of 27, citation 2949(Scopus). He associated as Dean –Department of computer science and Information Technology, Kalinga University, Raipur, Chhattisgarh.

Dr. Suvarna Yogesh Pansambal had received B.E. degree in Computer Engineering and from Pune University, M.E. Degree in Computer Engineering from Pune University and was awarded Ph.D. degree from Bharath Institute of Higher Education and Research, Chennai. Currently, she is working as Associate Professor in Department of Computer Engineering in Atharva College of Engineering, University of Mumbai. She has published 80+ technical papers in various international journals/conferences. She has 16 years of teaching experience on graduate level. Her research interests include Artificial Intelligence, Image Processing, Machine learning, Cyber Security, Digital Forensics.

Dr. Yogesh Manohar Gajmal is an Associate Professor in the Finolex Academy of Management and Technology, Ratnagiri, Maharashtra, India. He received his PhD in CSE from Bharath Institute of Higher Education and Research, Chennai and M-Tech in CSE from Bharati Vidyapeeth Deemed University, Pune. He is working as reviewer for SCI, ESCI, WoS and Scopus journals. He has teaching experience of 13 years in the area of Computer Engineering, Information Technology etc. His core teaching and research interests are in Blockchain, Information Security, and Cryptography. He has published his work in reputed SCI, ESCI, Web of Science and Scopus journals. He has collaborated actively with researchers in several other disciplines of computer science.

Dr. V.R. Vimal has received his B.E., degree from the Manonmaiam Sundaranar University, Tirunelveli, India in 2005, M.E., degree from Anna University, Chennai, India, in 2007, and Ph.D., degree from Anna University, Chennai, India, in 2022. For past 16 years from 2007, he has worked at different positions like Assistant Professor, Associate Professor, Professor & HOD in various reputed engineering colleges across India. He is currently working as a Professor in the Department of Computer Science and Engineering at Saveetha School of Engineering, SIMATS, Chennai, India. His research interests include Network Security, Image Processing and Machine Learning. He has published more than 20 research articles in various international journals and conference proceedings. He is acting as a reviewer in various national and international journals. He has chaired various international and national conferences. He is a life time member of ISTE and CSI.

R. Sugumar has received his BE degree from the University of Madras, Chennai, India in 2003, M. Tech degree from Dr. M.G.R. Educational and Research Institute, Chennai, India, in 2007, and PhD degree from Bharath University, Chennai, India, in 2011. From 2003 to 2021, he has worked at different positions like Assistant Professor, Associate Professor, Professor & HOD in various reputed engineering colleges across India. He is currently working as a Professor in the Department of Computer Science and Engineering at Saveetha School of Engineering, SIMATS, Chennai, India. His research interests include data mining, cloud computing and networks. He has published more than 45 research articles in various international journals and conference proceedings. He is acting as a reviewer in various national and international journals. He has chaired various international and national conferences. He is a life time member of ISTE and CSI.