International Journal of Electrical and Computer Engineering (IJECE)
Vol. 14, No. 1, February 2024, pp. 1058~1070
ISSN: 2088-8708, DOI: 10.11591/ijece.v14i1.pp1058-1070

Efficient network management and security in 5G enabled internet of things using deep learning algorithms

Sowmya Naik Poojari Thippeswamy[1], Ambika Padinjareveedu Raghavan[1], Manjunath Rajgopal[2], Annie Sujith[3]
[1]Department of Computer Science and Engineering, City Engineering College, Bengaluru, India
[2]Department of Computer Science and Engineering, R. R. Institute of Technology, Bengaluru, India
[3]Department of Computer Science and Engineering, Jyothy Institute of Technology, Bengaluru, India

Article Info

Article history:

Received Mar 6, 2023
Revised Aug 18, 2023
Accepted Sep 6, 2023

Keywords:

5G enabled IoT
Deep learning
Network management
Network security
Predictive modelling

ABSTRACT

The rise of fifth generation (5G) networks and the proliferation of internet-of-things (IoT) devices have created new opportunities for innovation and increased connectivity. However, this growth has also brought forth several challenges related to network management and security. Based on the review of literature it has been identified that majority of existing research work are limited to either addressing the network management issue or security concerns. In this paper, the proposed work has presented an integrated framework to address both network management and security concerns in 5G internet-of-things (IoT) network using a deep learning algorithm. Firstly, a joint approach of attention mechanism and long short-term memory (LSTM) model is proposed to forecast network traffic and optimization of network resources in a, service-based and user-oriented manner. The second contribution is development of reliable network attack detection system using autoencoder mechanism. Finally, a contextual model of 5G-IoT is discussed to demonstrate the scope of the proposed models quantifying the network behavior to drive predictive decision making in network resources and attack detection with performance guarantees. The experiments are conducted with respect to various statistical error analysis and other performance indicators to assess prediction capability of both traffic forecasting and attack detection model.

Corresponding Author:

Sowmya Naik Poojari Thippeswamy
Department of Computer Science and Engineering, City Engineering College
Bengaluru, Karnataka, India
Email: Sowmya.vturesearch@gmail.com

1. INTRODUCTION

The growth of internet of things (IoT) devices has created new opportunities for developing smart applications such as healthcare, smart cities, transportation, and industrial automation [1]. It is known that IoT is rapidly expanding with connected devices featuring electronics, software, sensors, and network connectivity. But effective functioning of IoT devices in smart applications requires high-speed, low-latency, and secure connectivity [2]. Fifth generation (5G) is the latest wireless technology offering faster speeds, lower latency, and greater capacity, making it essential for supporting widespread deployment of IoT devices and systems [3]. 5G is the latest iteration of wireless technology which offers significant improvements over previous generations, including faster speeds, lower latency, and increased capacity [4]. This makes 5G a key enabler technology for supporting the large-scale deployment of IoT devices and systems. Also, the integration of artificial intelligence (AI) technologies to 5G powered IoT has potential to enable more

autonomous and intelligent functions to revolutionize the way we live, work, and communicate [5], [6]. However, the increased connectivity offered by 5G networks and widespread adoption of IoT devices also brings new opportunities for cyberattacks [7]. It is due to the fact that more devices connected to the network, more the complicated network, more traffic congestion, and more personal data will be generated and communicated [8]. Effective network management is necessary to ensure efficient use of network resources and high-quality service delivery, while security is crucial to protect sensitive information and prevent cyberattacks. Although, the literature consists of various threat mitigation and security measures based on encryption, firewalls, intrusion detection systems, and secure protocols [9]. Most of these measures are designed according to the specific attack scenario and network models. Due to inherent dynamicity and heterogeneity, such traditional methods cannot be directly applied to the modern 5G IoT [10]. As a result, current 5G IoT system architectures are facing significant challenges in handling the security and privacy of an increasing number of devices and servers and protecting large volumes of data processed in real-time. The proposed study presents a novel unified framework that can jointly address both network management issue and security concerns in 5G IoT by leveraging the power of data analytics and learning-driven predictive functions.

However, literature analysis has shown a growing trend towards adopting machine learning (ML) and deep learning (DL) techniques for addressing security and various other problems in 5G IoT. Sharm *et al.* [11] presented interesting work on discovering various security issues, privacy concerns, and limitations imposed by existing approaches in the IoT context. The authors have also discussed the potential role of ML and DL techniques in securing 5G-enabled industrial IoT (IIoT). The work done by Wang *et al.* [12] presented an efficient routing mechanism for providing quality of services (QoS) and privacy-aware packet transmission in 5G driven IIoT using the application of reinforcement learning. However, this approach can be subjected to the curse of the dimensionality due to the large memory requirements to store the action-space values during route discovery in and large networks. Shin and Kwon [13] developed elliptic curve cryptography (ECC) oriented authentication and key-based mechanisms for ensuring privacy in wireless sensor networks (WSN) in 5G-driven IoT. This work is subjected to the scalability problem due to the security compatibility issue among heterogeneous IoT devices. In the work of Liang *et al.* [14], trust-aware algorithm is designed based on a code dissemination technique to establish on-demand routing mechanisms among trusted unmanned aerial vehicles (UAVs) in IIoT. This approach is suitable against internal attacks but is not much robust to dynamic and smart attacks based on self-exploration techniques. Esenogho *et al.* [15] conducted exhaustive literature on the applications of AI in smart grids assisted by IoT and 5G technologies. The authors have highlight potential challenges and probable solutions using numerical tools and simulation-based approaches. Manasreh *et al.* [16] have presented a detailed analysis of the telecommunication network's cryptology approaches. The analysis is conducted on the basis of scientific data and quantitative and statistical analysis. The study has shown a trend toward the adoption of various existing protocols in various industries to secure the network. Lin *et al.* [17] concentrated on ensuring low latency and QoS for the internet of health care things (IoHT).

A Nash bargaining game theory-based scheme is adopted to offload the healthcare services to edge computing systems. Further, Lyapunov-based proportional fairness followed optimization is implemented to perform optimal resource allocation. Similarly, Aljarah *et al.* [18] have explored the application of edge resources and presented cooperative layered edge computing for resource sharing in cloud-based mobile and IoT ecosystems. The adoption of blockchain technology is also seen in the work of Feng *et al.* [19] towards ensuring robust authentication in 5G-enabled internet of drones (IoD). This approach also implemented various signatures based on a threshold-sharing scheme, and smart contracts are used to achieve reliable communication. An intelligent resource placement mechanism is suggested by Chafi *et al.* [20] to optimize network resource utilization and latency in 5G-driven smart grid applications. An approach to IoHT for secure clustering is suggested by Yang *et al.* [21], where trusted-based evaluation is done using soft computing approaches. A fuzzy trust-based recommending system is developed to compute trust among cloud-assisted healthcare nodes, and a trust classification scheme does intrusion. A prediction model is developed by Ferreira *et al.* [22], where DL and ML approaches are implemented to predict multiple performance parameters such as slicing requirement and congestion probability to improve 5G networks' management. In the same line of research, He *et al.* [23] has employed a multi-agent algorithm to explore the state of 5G IoT on a real-time basis and perform suitable action towards congestion control. The attention mechanism is used for designing the agent algorithm, preventing it from slowing the convergence rate and dimension disaster problem. Ahmed *et al.* [24] presented DL-based spectrum agents which dynamically learn the spatial and temporal features towards estimating network congestion in advance for the vehicular network. However, this approach has not focused on security and takes a long search time. Najm *et al.* [25] implemented an ML classifier decision tree to predict the optimal parametric setting of the network to optimize congestions in the sensor network of 5G IoT. Although this works predicts traffic congestion but does not considered security aspects. Goswami *et al.* [26] considered both problems and used convolutional

neural network (CNN) to compute optimal channel state for different applications. However, the system can have stability issues when there is massive traffic and the system cannot handle it and eventually crashes.

All the above-mentioned existing research work have witnessed different variants of methods for solving different network problem, security, and privacy preservation. However, it has been analyzed that the researches in the context of 5G IoT is still in its infancy stage as there are many challenges that need to be resolved discussed as follows: i) The architecture of 5G networks is complex, requiring enhanced network management algorithms that can handle the increased demands of 5G networks. In previous works, dedicated channel states with respect to fixed resources have been considered. This presents great challenges to the security and resiliency of the network; ii) A few existing works have employed a statistical and probability distribution-based approach to predict traffic flow. In the 5G scenario, these approaches are insufficient in terms of context granularity because they are highly dependent on finite parameters; iii) As IoT devices collect and use personal data, security threats and privacy concerns are likely to grow. IoT networks powered by 5G require adaptive security and privacy-centric solutions that can ensure the safety of data and systems; iv) The literature reveals that ML and DL approaches are being increasingly used to perform predictive tasks in the context of network traffic prioritization, congestion control, resource allocation, and attack detection. One significant research gap is the failure to address both network management and security issues simultaneously. In existing works, the major focus is either on optimizing network resources or traffic management and less on security; and v) Learning-driven prior algorithms for traffic prediction and attack detection suffer from higher prediction errors, and those who claim higher accuracy are not much more computationally efficient.

In the proposed research work, all significant problems were considered, and effective predictive modeling is carried for addressing network management and security concerns in 5G IoT ecosystem. The research work reported in paper offers a significant contribution to address the following challenges particularly: i) networking modelling by considering the characteristics of 5G IoT to reduce surface of network congestion and attacks; ii) examining network data, relevant variables and identify correlations to get insights towards driving better decision variables in predictive modelling for future traffic conditions and network behavior patterns; iii) implementation of suitable deep learning models towards accurate forecasting of highly contextualized traffic demand and quantifying the network behavior to drive decision making in attack detection with performance guarantees.

Ultimately, the proposed research work aims to provide proactive approach towards ensuring reliable communication environment and optimizing network resources in a, service-based and user-oriented manner. The core agenda of this study model is to introduce a simplified framework towards offering better form of communication system adhering to norms of 5G service usage in IoT devices. The next section elaborates the proposed system design and implementation procedure adopted to accomplish network efficiency, reliability, and security in the face of increasing network complexity and growing security threats.

2. METHOD

The implementation of the proposed scheme is carried out using standard analytical research methodology which mainly emphasize towards the traffic-related attributes from the practical utilization viewpoint in IoT. The proposed methodology also emphasizes towards accomplishing a better equilibrium between computational efficiency and communication performance associated with resource-constrained IoT devices. Further, it emphasizes on using deep learning scheme for facilitating a better form of predictive model in IoT environment. A novel integrated framework is proposed using statistical methods and deep learning models to prioritize network traffic efficiently based on network demands and monitor the network to predict attacks. To gain control over computational complexity, the framework design does not include any complex operations in the execution of the algorithm, but instead includes appropriate data modeling, correlation analysis, and implementation of deep learning models with fewer learning attributes. The schematic architecture of the proposed integrated framework is shown in Figure 1.

The intuition of the proposed system is that the IoT devices with 5G connectivity generate massive amounts of data that contain rich metainformation related to users, applications, and network. Analyzing information with statistical methods and processing it through machine learning can result in efficient predictive models. As a result, it enables it to make predictions about future traffic patterns, dynamically allocate network resources, and take proactive action to prioritize traffic accordingly. Additionally, it improves overall visibility into network operations and identifies anomalies and potential threats before they become a serious problem or curse on the network. The implementation procedure adopted in the proposed system is discussed in the sub-sections.

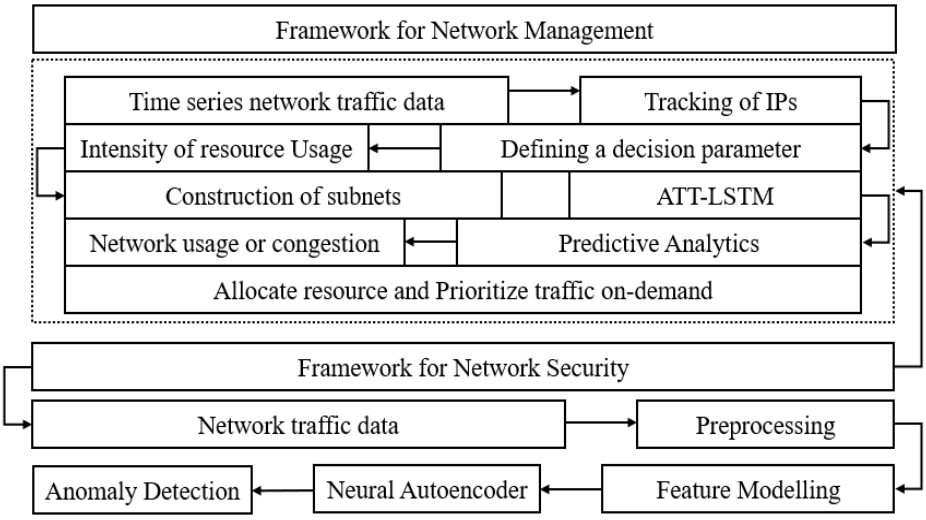

Figure 1. Architecture of the proposed integrated framework

2.1. Traffic forecasting system

As the number of devices in 5G IoT increases rapidly, the network cannot handle it and eventually collapses. Therefore, this phase of the proposed system is meant for implementing a deep learning predictive system on time series network traffic data to predict high traffic peak, congestion and allocate resources followed by the prioritization. The dataset used in this work is computer network traffic data [27] obtained in format of .csv consisting information about real traffic that covers local workstation internet protocols (IPs) over a three-month period. The dataset has approximately 21,000 samples in row and each row has four columns such as date, local IP (l_ipn encoded from 0 to 9), remote autonomous system number (r_asn) and flows (i.e., number of connections recorded on particular day). After loading the dataset into data frame, the study executes exploratory and statistical analysis towards identifying unique characteristics and correlation among the data. The first analysis is done towards tracking the IPs, autonomous system number (ASN) addresses and estimation of maximum and minimum traffic flow per day. Table 1 illustrates the insights obtained from exploratory analysis of dataset.

Table 1. Statistical insights of dataset

Insights	Value
Number of days for which data is available	92
Count of unique **l_ipn**	10
Count of unique **r_asn**	2,005
Minimum flow per day	1
Maximum flow per day	784,234

The data statistics shown in Table 1 illustrates that the dataset consists of traffic data recorded for total 92 days. Further tracking of local IP is done where it has been identified that total 10 IPs assigned to devices connected to a local network. These local IP addresses is used help concerned entity to identify the devices or number of user active with in the local network, which ultimately relates to the traffic or congestion in the network. Further, analysis is done towards identifying unique remote ASN which is total 2,005. This ASN is a unique identifier assigned to a network in the internet that is connected to multiple other networks. This helps to identify a specific network and its routing policies, which allows for more efficient communication between networks. Traffic congestion in a network can be estimated using the number of flows, which are the connections between devices sending and receiving data. Therefore, the exploratory study also reveals the flow count minimum value i.e., 1 and maximum i.e., 784,234 per day. A higher number of flows in a network can indicate that the network is congested, as there is limited bandwidth available for the traffic to flow.

For example, let F_c be the maximum number of flows that the network is capable of handling, and F_A be the number of active flows in the network. If $F_A > F_c$, the network is congested, Mathematically, this can be represented as:

$$Congestion\ (C) = (F_A > F_c) \tag{1}$$

where C is a binary variable with a value of 1 indicating that the network is congested and a value of 0 indicating that the network is not congested. Similarly, the intensity if resource usage based on the traffic congestion can be computed as (2).

$$Intensity\ of\ resource\ usage\ (R) = F \times (1 + C) \tag{2}$$

where R is the intensity of resource usage, F denotes traffic flow and C is a weight that represents the impact of congestion on the resource usage. If the network is congested, the value of C will be greater than 0, which will increase the value of R, thus reflecting the higher intensity of resource usage. However, forecasting network traffic based on flow count and network capacity can involve using time series analysis techniques to predict future trends in the number of active flows and the intensity of resource usage. In this regard, the exploratory analysis continues to identify the traffic pattern with sequence of traffic flow over time i.e., by day of week shown in Figure 2.

Figure 2(a) to (f) provides an analysis for 6 local IP which exhibits different traffic patterns and trends in the form of seasonality where number of active flows forming series of value that change in a predictable or unpredictable manner. All these analysis helps to derive decision variables towards identifying correlations for suitable data preparation for carrying out predictive tasks to train deep learning model to forecast future traffic conditions. Furthermore, the study implements attention-based long short-term memory (LSTM) learning model to perform predictive task for traffic forecasting. LSTM is a class of recurrent neural network stands for long short-term memory, it uses gating mechanism to capture long-term dependencies and predict future values of the traffic by learning non-linear pattern of historical sequential data. Consider X be the input data in fixed length interval obtained from the training time series traffic data such that: $X = \{x_1, x_2, \cdots x_c\}$, where x_c refers to congestion in network due to peak traffic at time t_p. The proposed model tries to forecast the peak traffic in advance such that x_{c+1} at time t_{p+1}. The working principle of a single LSTM neural unit or cell depends on (3) to accomplish this predictive task of traffic forecasting:

$$\begin{cases} f_t = \sigma\big(W_f \cdot \big[h_{g-1}, x_c\big] + b_f\big) \\ i_t = \sigma(W_i \cdot [h_{t-1}, x_c] + b_i) \\ \tilde{C}_t = \tanh\,(W_c \cdot [h_{t-1}, x_c] + b_c) \\ C_t = f_t \times C_{t-1} + i_t \times \tilde{C}_t \\ o_t = \sigma(W_o \cdot [h_{t-1}, x_c] + b_o) \\ h_t = o_t \times \tanh(C_t) \end{cases} \tag{3}$$

where, f_t denotes forget gate, i_t denotes input gate, C_t is the cell state, o_t refers to output gate, and h_t denotes hidden state of cell. W_f, W_i, b_f, b_i are the weight and biases for forget and input gate and σ sigmoid activation function. As an encoder-decoder model, LSTM requires that the encoder represents the whole input sequential time series traffic data as a single vector. This can lead to information loss. In order to improve traffic forecasting, the attention mechanism enables the encoder to examine all hidden states and exploit correlations between features. In other words, LSTM unit is responsible for capturing temporal dependencies in sequential data, while the attention mechanism allows the model to focus on relevant parts of the input sequence when making predictions. The attention mechanism works by computing attention scores for each step in the input sequence, which indicate the importance of each step in the prediction process. The attention scores are typically computed using a feedforward neural network that takes the current LSTM hidden state as input. Let us consider that the set of LSTM cell at i^{th} layer computes an output of hidden state h_t for each step t using (3). The attention mechanism then computes the α_t (attention score) numerically expressed as (4):

$$\alpha_t = softmax(x_t \cdot \tanh\,(W_1 \cdot h_t + b_1)\,) \tag{4}$$

where, x_t data feature, W_1 and b_1 trainable parameters.

Finally, the attention-weighted representation of the input sequence is computed as a weighted sum of the hidden states.

$$z\ =\ \textstyle\sum_t \alpha_t \cdot ht \tag{5}$$

The output of the learning model is typically computed using a feedforward neural network that takes z as input. Owing to the adoption of this learning mechanism, the predictive accuracy witnesses better improvement in its score. The implementation steps for training LSTM-attention learning model for traffic forecasting is discussed in Algorithm 1.

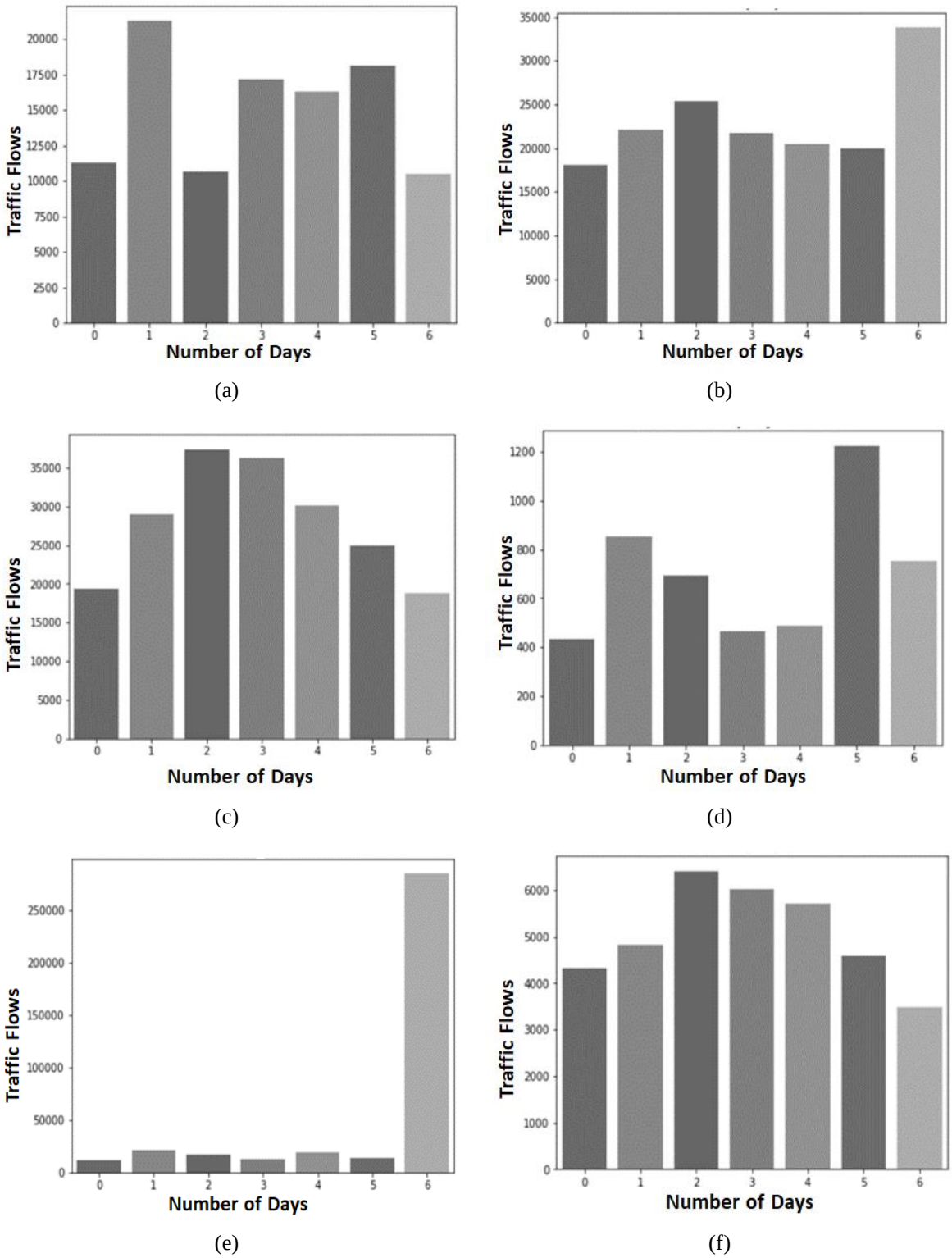

Figure 2. Illustration of traffic flow by day of week (a) local IP-1 flow, (b) local IP-2 flow, (c) local IP-3 flow, (d) local IP-4 flow, (e) local IP-5 flow, (f) local IP-6 flow

Algorithm 1. Training model for traffic forecasting

```
Input: D_t (traffic data), e (epoch), b (batch_size)
Output: forecast traffic, resource allocation
Start
    1. D̃_t ← normalize (D_t) ← (D_t − min(D_t)) / (max(x) − min(x))
    2. //Dataset split
    3. [Tr, Ts] ← train_test_split (D̃_t, 80:20)
    4. //Train model with Tr
    5. input ← Tr ∈ [X, Y]
    6. n = 100
    7. lstm = LSTM(n, activation = relu, return_sequences = True)(input)
                                                attention = Attention(1)(lstm)
                                                outputs = Dense(1)(attention)
                                              model = Model(inputs1, outputs1)
                                          model.compile(loss = MSE, optimizer = sgd)
    8. model.fit(X, Y, e, b)
    9. //Forecasting of traffic flow using trained model and test dataset Ts
    10. input ← Ts ∈ [x, y]
    11. forecast = model.predict(x)
    12. //Allocate resource
    13. resource (nR) → [B, L, R, Co]
    14. if P[s_id] == high
    15. nR[s_id] = forecast[s_id] × k
    16. elif P[s_id] == medium
    17. nR[s_id] = forecast[s_id] × k + 1
    18. else:
    19. nR[s_id] = forecast[s_id] × k + 1
    20. end
End
```

The above-mentioned algorithmic step takes necessary input to train attain-LSTM model and after execution is predicts the traffic and allocates network resources for different type of network in 5G IoT. The model is trained for 100 epochs and batch size considered is 16, mean square error as loss function (MSE) and stochastic gradient descent (sgd) as optimizer. The algorithm also allocates resources based on the priority of the communication required in different network discussed in section 2.3.

2.2. Network security system

This phase of the research work aims to implement an effective attack detection system to detect cyber-attacks with high detection accuracy. The proposed implements Algorithm 2 for utilizing a concept of an Auto-encoders mechanism which is a type of neural network architecture designed to learn a compact representation of an input data taken from [28]. By training an autoencoder on normal network behavior data, it can be used to identify deviations from the normal behavior that may indicate an intrusion. The autoencoder would produce higher reconstruction errors for inputs that are significantly different from the normal behavior data.

Algorithm 2. Training autoencoder for attack detection

```
Input: XTrain, e(epoch)
Output: Err (reconstruction error)
Start
   1. Initialize weights
   2. for each e

        encode x_i → h_i : f(x_i) = a((W x_i + b))  // a activation function, W (weights) and b (bias)

        decode h_i → x'_i : g(h_i) = a((W h_i + b))

   3. end for
   4. Compute

        Err ← f_1(x_i, x'_i)  // Err is reconstruction error, such that:

        Err = (1/n) Σ_{i=1}^{n} (x_i − x'_i)^2

End
```

2.3. Network modelling

5G networks are more complex than their 2G, 3G and 4G networks, but one of its key features is the ability to support virtualization and multiplexing of virtual networks. In technical terms, this process is referred to as network slicing, an advanced feature of 5G networks that enables independent logical separation of physical networks. A primary consideration from the perspective of network management is that if physical IoT network are split into more logical networks, the more efficient the management of its resources and complexities will be. Figure 3 presents a contextual depiction of network slicing in the context of 5G-driven IoT networks that are subdivided into mobile broadband, massive IoT, and critical IoT networks. Incorporating virtual sub-networks that can have varying traffic priorities based on the application, service, or use case. For example, in a critical IoT, network resources can be tailored to prioritize communications between surgeons and computer-aided automated diagnosis systems over those being used by patients. Thus, even during times of network congestion, emergency transmissions can be protected. Also, from the security perspective, network slicing is important because a single physical network has the maximum potential for attacks. As a result, dividing a single physical network into multiple slices reduces the attack surface and makes it difficult for attackers to use the IoT device as a single attack vector and to degrade performance. An Algorithm 3 for network slicing and virtualization is illustrated as follows:

Algorithm 3. IoT network slicing and virtual subnetwork construction

```
Initialize s_id, s_type
Initialize S→[ ]
def create_s(s_id, s_type, nR):
new_s = f1(s_id, s_type, nR)
S.append(new_s)
return new_s
//Split IoT physical network into different logical network or slices
s1 = nI.create_s(1, eMBB, [B, L])
s2 = nI.create_s(2, mMTC, [Co, R])
s3 = nI.create_s(3, uRLLC, [L, R])
for slice in nI.S:
plot network in format: S{s_id} ({s_type}) has resources: {s.nR}
// Create a virtual subnet
Input: addr ofnV ∈ S
Initialize subnet
Ip_net→f2(addr, subnet)
```

The algorithm initializes a variable such as s_id (identity of slice or logical network), s_type (a service category of 5G such as enhanced mobile broadband (eMBB), massive machine-type communications (mMTC), and ultra reliable low latency communications (uRLLC)) and S an empty vector to hold value of slices. The next step of algorithm is executed towards creating a user define function named create_s( ) which uses an implicit function $f1( )$ to create desired number of slices considering different input arguments such as s_id, , s_type and , nR (network resources). This function returns new_s (a new slice or network) for each unique inputs which is further appended into vector S. The execution of this function is shown in the subsequent steps of the algorithm which creates three different slices such that s1, s2, s3 with corresponding input arguments such for $s1\leftarrow$ the function $create\_s$ followed by network identity (nI), it takes value s_id equals 1 as its first input, s_type eMBB as its second input and the last input $nR \in \{B, L\}$ as its prime network resources, where B is bandwidth and L is latency. Similarly, the algorithm takes corresponding value for the next slices such that: *s2|s_id=2* and *s3|s_id=3*, s2|s_type→mMTC and s3|s_type→uRLLC, $s2|\text{nR} \in \{\text{Co}, \text{R}\}$ and $s3|\text{nR} \in \{\text{L}, \text{R}\}$, where Co is communication strength, R is reliability, and L is latency. The next step of the algorithm plots the network with all three different slices and their corresponding resources being allocated. Apart from the network slicing, another contribution is creating virtual subnets of virtual components subjected to slices. The previous steps of algorithm meant for dividing the physical IoT network into different unique logical slices (sub network) which enables higher-level abstraction in managing network resources for specific use cases. But the virtual subnets are a logical subdivision of virtual components to provide specific network services within a network slice there by more manageable sub-networks, more control in the flow of traffic by creating separate broadcast domains. The algorithm considers address (*addr*) of virtual networks (nV) belongs to particular network slice such that addr of $nV \in S$. It then initializes a size of subnets and uses a function $f2( )$ which basically calls '$netaddr$' from the python library converts the network address string to an IP network object and divide a network address into subnets. Figure 3 illustrates the contextual architecture of the proposed system. This part of the proposed system serves a complementary feature to proactively prioritizing traffic and optimal resource allocation to critical 5G-IoT application.

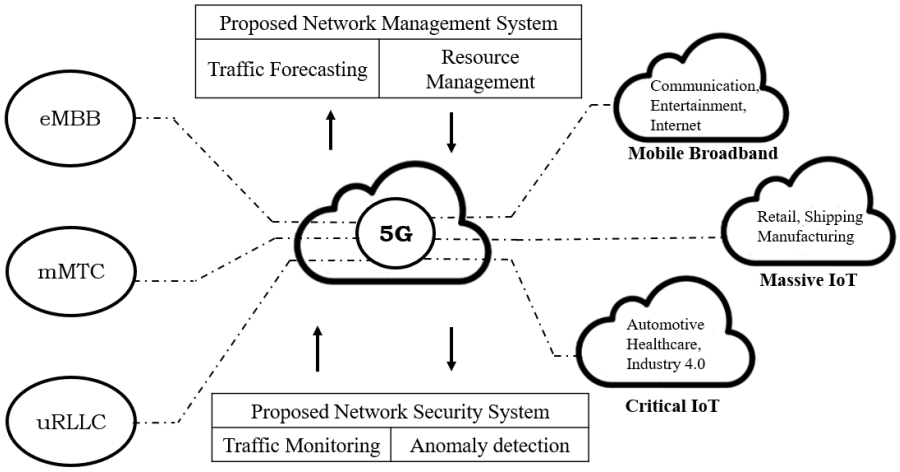

Figure 3. Contextual depiction of proposed system in 5G-IoT

3. RESULTS AND DISCUSSION

The design and development of the proposed system is carried out using Python programming language executed on Anaconda distribution. The assessment of the proposed systems is done in terms of various performance metrics and their outcomes are compared to similar existing predictive models. The entire performance assessments are carried out in two phases which are particular to both schemes of proposed traffic forecasting and attack detection.

3.1. Analysis of traffic forecasting model

In order to assess the prediction capability of the proposed attention-LSTM (ATT-LSTM) model various the statistical metrics are used mean absolute error (MAE), mean square error (MSE) and root mean square error (RMSE). This statistical error analysis is highly adopted in the literature towards analyzing the performance regarding prediction error and variance in predictions made by models and actual samples of the testing dataset. The study also considers two similar type of deep learning models namely gated recurrent unit (GRU) and LSTM for the comparative analysis. Both models are based on the similar principle of recurrent neural network. The study outcome for traffic forecasting model is exhibited in Figures 4 to 6.

The MSE score shown in Figure 4 obtained by proposed ATT-LSTM forecast network traffic with minimal error and higher accuracy compared to other sequence prediction models i.e., GRU and LSTM. Similarly, it can be seen from Figure 5 that ATT-LSTM shows best performance with respect to average absolute error i.e., MAE. The RMSE analysis shown in Figure 6 also exhibits effectiveness of the proposed system compared to LSTM and GRU. The reason behind achieving better performance by the proposed ATT-LSTM is that the attention mechanism allows the LSTM model to dynamically focus on the most relevant part of the input sequence while making predictions, whereas in a normal GRU and LSTM model, the entire sequence is considered equally important.

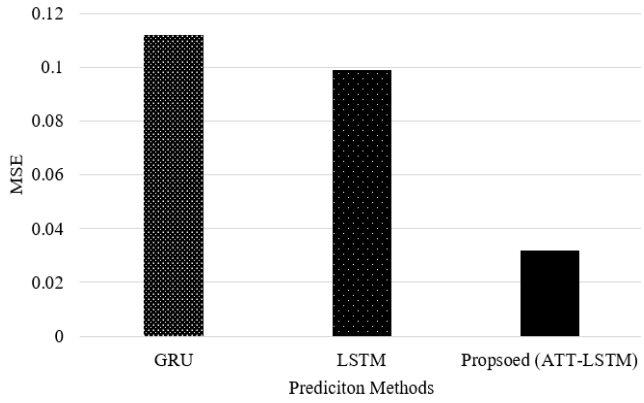

Figure 4. MSE score achieved by proposed ATT-LSMT and other similar models

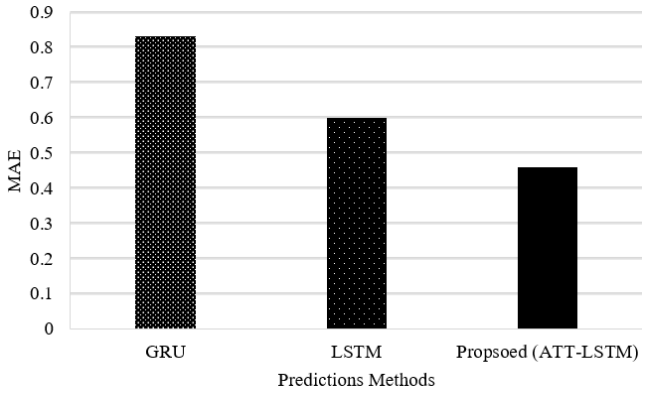

Figure 5. MAE score achieved by proposed ATT-LSMT and other similar models

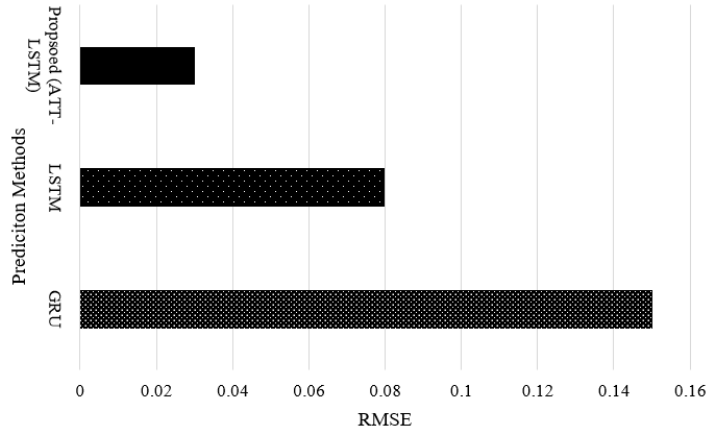

Figure 6. RMSE score achieved by proposed ATT-LSMT and other similar models

This results in improved performance on tasks where the important information is spread across the input sequence. On the other hand, GRU is a type of RNN that has fewer parameters compared to LSTM and are computationally more efficient. However, this reduction in complexity comes at the cost of modeling power. LSTMs have two memory cells that can retain information for a longer period of time compared to GRUs, which only have one memory cell. This makes LSTMs better suited for tasks that require the model to remember information for a longer period of time, whereas GRUs are more suited for tasks that require quick memorization and forgetting of information. Therefore, leveraging attention mechanism in LSTM model the proposed study implements better model that can forecast traffic in advance with higher accuracy and low false positive result.

3.2. Analysis of attack detection model

In order to assess the prediction performance of the proposed autoencoder model for anomaly detection in 5G-IoT various the performance metrics of confusion matrix are considered namely, accuracy, precision, recall rate and F1-score. The study also considers to implement two popular machine learning model such as support vector machine (SVM) and k-nearest neighbor (KNN) to conduct comparative analysis. The analysis shown in Figure 7 exhibits higher score obtained by the proposed predictive model with respect to accuracy, precision, re-call rate and F1 score. According to the result, the proposed autoencoder based attack detection model outperforms other methods such as SVM, and KNN. There are many reasons behind getting better performance by autoencoder. The proposed model is capable of learning non-linear relationships in the data, making them suitable for handling complex data such as network intrusion data, which can be highly non-linear. Another reason is that it does not rely on feature scaling, which makes them more robust to feature scaling issues compared to SVM and KNN, which are sensitive to feature scaling. The proposed model learns the normal patterns in the data and flag anything that deviates from the norm as an anomaly.

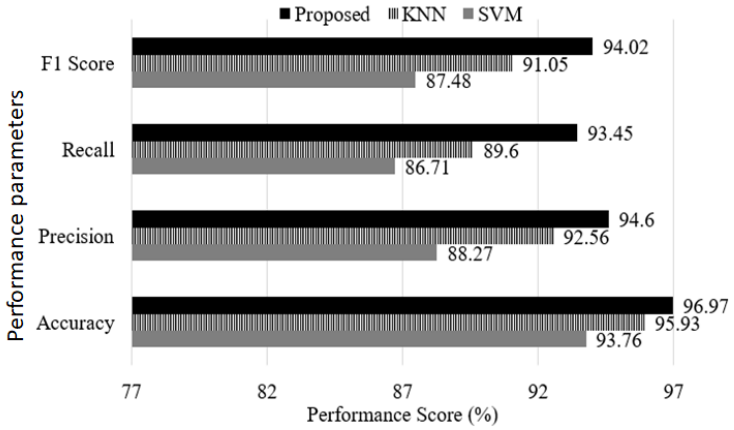

Figure 7. Prediction analysis of proposed autoencoder and other classifiers

4. CONCLUSION

The research work reported in this paper has considered a case scenario of an 5G IoT network and focuses on network traffic forecasting, resource management and security. The entire contribution is proposed in multifold. An analytical research approach has been adopted in design of the proposed system followed by computationally-efficient implementation mechanisms. The proposed system leverages the real time network data and applied data analytics to gain insight into user behavior, and network traffic. By utilizing statistical analysis and combination of deep learning algorithms such as attention mechanism with LSTM learning model, the proposed work constructed effective predictive models to anticipate future traffic patterns, optimize network resource allocation, and prioritize traffic proactively. Another important contribution of the proposed system is development of the compact attack detection system utilizing an autoencoder model to conduct real-time network security monitoring and identify potential attacks. The design of the security model strives to provide a full view of end-devices connected to the network. Last but not least, the proposed work also presented a conceptual architecture of 5G-IoT network where the entire physical network is divided into slices or sub-network which not only reduces the effort require in managing the network resources but it also reduces the possibility of getting compromised with attacks and avoids single point failure of the entire network. The experimental outcome justifies the effectiveness of the proposed system. In future work, the proposed research works willing to optimize the proposed system with self-exploration ability of reinforcement learning and addressing other network related problems.

REFERENCES

[1] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of internet of things (IoT): a survey," *Journal of Network and Computer Applications*, vol. 161, Art. no. 102630, Jul. 2020, doi: 10.1016/j.jnca.2020.102630.

[2] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber threats to industrial IoT: a survey on attacks and countermeasures," *Internet of Things*, vol. 2, no. 1, pp. 163–186, Mar. 2021, doi: 10.3390/iot2010009.

[3] A. Jurcut, T. Niculcea, P. Ranaweera, and N. A. Le-Khac, "Security considerations for internet of things: a survey," *SN Computer Science*, vol. 1, no. 4, Jun. 2020, doi: 10.1007/s42979-020-00201-3.

[4] J. Navarro-Ortiz, P. Romero-Diaz, S. Sendra, P. Ameigeiras, J. J. Ramos-Munoz, and J. M. Lopez-Soler, "A survey on 5G usage scenarios and traffic models," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2, pp. 905–929, 2020, doi: 10.1109/COMST.2020.2971781.

[5] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of things (IoT) for next-generation smart systems: a review of current challenges, future trends and prospects for emerging 5G-IoT Scenarios," *IEEE Access*, vol. 8, pp. 23022–23040, 2020, doi: 10.1109/ACCESS.2020.2970118.

[6] L. Chettri and R. Bera, "A comprehensive survey on internet of things (IoT) toward 5G wireless systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16–32, Jan. 2020, doi: 10.1109/JIOT.2019.2948888.

[7] P. Varga *et al.*, "5G support for industrial IoT applications – challenges, solutions, and research gaps," *Sensors (Switzerland)*, vol. 20, no. 3, p. 828, Feb. 2020, doi: 10.3390/s20030828.

[8] F. Al-Turjman, "Intelligence and security in big 5G-oriented IoNT: An overview," *Future Generation Computer Systems*, vol. 102, pp. 357–368, Jan. 2020, doi: 10.1016/j.future.2019.08.009.

[9] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the internet of things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2017, doi: 10.1109/ACCESS.2017.2779844.

[10] A. A. A. Solyman and K. Yahya, "Evolution of wireless communication networks: from 1G to 6G and future perspective," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 4, pp. 3943–3950, Aug. 2022, doi: 10.11591/ijece.v12i4.pp3943-3950.

[11] P. Sharma, S. Jain, S. Gupta, and V. Chamola, "Role of machine learning and deep learning in securing 5G-driven industrial IoT applications," *Ad Hoc Networks*, vol. 123, p. 102685, Dec. 2021, doi: 10.1016/j.adhoc.2021.102685.

[12] X. Wang *et al.*, "QoS and privacy-aware routing for 5G-enabled industrial internet of things: a federated reinforcement learning approach," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4189–4197, Jun. 2022, doi: 10.1109/TII.2021.3124848.
[13] S. Shin and T. Kwon, "A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated internet of things," *IEEE Access*, vol. 8, pp. 67555–67571, 2020, doi: 10.1109/ACCESS.2020.2985719.
[14] J. Liang, W. Liu, N. N. Xiong, A. Liu, and S. Zhang, "An intelligent and trust UAV-assisted code dissemination 5G system for industrial internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2877–2889, Apr. 2022, doi: 10.1109/TII.2021.3110734.
[15] E. Esenogho, K. Djouani, and A. M. Kurien, "Integrating artificial intelligence internet of things and 5G for next-generation smartgrid: A survey of trends challenges and prospect," *IEEE Access*, vol. 10, pp. 4794–4831, 2022, doi: 10.1109/ACCESS.2022.3140595.
[16] A. Manasreh, A. A. M. Sharadqh, J. S. Alkasassbeh, and A. Al-Qaisi, "Ensuring telecommunication network security through cryptology: A case of 4G and 5G LTE cellular network providers," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 6, pp. 4860–4865, Dec. 2019, doi: 10.11591/ijece.v9i6.pp4860-4865.
[17] X. Lin, J. Wu, A. K. Bashir, W. Yang, A. Singh, and A. A. Alzubi, "FairHealth: Long-term proportional fairness-driven 5G edge healthcare in internet of medical things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 8905–8915, Dec. 2022, doi: 10.1109/TII.2022.3183000.
[18] M. Aljarah, M. Shurman, and S. H. Alnabelsi, "Cooperative hierarchical based edge-computing approach for resources allocation of distributed mobile and IoT applications," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 296–307, Feb. 2020, doi: 10.11591/ijece.v10i1.pp296-307.
[19] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K. K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6224–6238, Apr. 2022, doi: 10.1109/JIOT.2021.3113321.
[20] S. E. Chafi, Y. Balboul, S. Mazer, M. Fattah, and M. El Bekkali, "Resource placement strategy optimization for smart grid application using 5G wireless networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 4, pp. 3932–3942, Aug. 2022, doi: 10.11591/ijece.v12i4.pp3932-3942.
[21] L. Yang, K. Yu, S. X. Yang, C. Chakraborty, Y. Lu, and T. Guo, "An intelligent trust cloud management method for secure clustering in 5G enabled internet of medical things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 8864–8875, Dec. 2022, doi: 10.1109/TII.2021.3128954.
[22] D. Ferreira, A. Braga Reis, C. Senna, and S. Sargento, "A forecasting approach to improve control and management for 5G networks," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1817–1831, Jun. 2021, doi: 10.1109/TNSM.2021.3056222.
[23] B. He *et al.*, "DeepCC: Multi-agent deep reinforcement learning congestion control for multi-path TCP based on self-attention," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4770–4788, Dec. 2021, doi: 10.1109/TNSM.2021.3093302.
[24] R. Ahmed, Y. Chen, B. Hassan, L. Du, T. Hassan, and J. Dias, "Hybrid machine-learning-based spectrum sensing and allocation with adaptive congestion-aware modeling in CR-assisted IoV networks," *IEEE Internet of Things Journal*, vol. 9, no. 24, pp. 25100–25116, Dec. 2022, doi: 10.1109/JIOT.2022.3195425.
[25] I. A. Najm, A. K. Hamoud, J. Lloret, and I. Bosch, "Machine learning prediction approach to enhance congestion control in 5G IoT environment," *Electronics (Switzerland)*, vol. 8, no. 6, p. 607, May 2019, doi: 10.3390/electronics8060607.
[26] P. Goswami, A. Mukherjee, M. Maiti, S. K. S. Tyagi, and L. Yang, "A neural-network-based optimal resource allocation method for secure IIoT network," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2538–2544, Feb. 2022, doi: 10.1109/JIOT.2021.3084636.
[27] Stanford HCI Group, "Dataset: Stanford.edu." Stanford HCI, Accessed: Feb. 02, 2023. [Online], Available: https://hci.stanford.edu/courses/cs448b/data/ipasn/cs448b_ipasn.csv
[28] S. Bhosale, "Dataset: network intrusion detection." [Online], Available: https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection (accessed Feb. 02, 2023).

BIOGRAPHIES OF AUTHORS

Sowmya Naik Poojari Thippeswamy completed her B.E. in computer science and engineering, in 2007 and M.Tech. in computer science and engineering in 2012. She obtained her Ph.D. Degree in computer science and engineering from Visvesvaraya Technological University (VTU), Belgaum, and Karnataka. Presently she is working as professor and HOD, Department of Computer Science and Engineering at City Engineering College, Bengaluru affiliated to Visvesvaraya Technological University (VTU), Belgaum, and Karnataka, India. She is a member of ISTE and MIE. Her areas of interest include wireless sensor networks, cloud computing big data, and machine learning. She published her papers in IEEE, Springer, and Elsevier. She can be contacted at email Sowmya.vturesearch@gmail.com.

Ambika Padinjareveedu Raghavan received her B.E. and M.Tech. in computer science and engineering from Visvesvaraya Technological University (VTU), Belgaum, Karnataka. She is a research scholar in the Computer Science and Engineering Department at BMS Institute of Technology and Management, Bengaluru affiliated with VTU. Currently, she is working as an assistant professor in the Department of CSE, City Engineering College, Bengaluru, and Karnataka, India. Her areas of interest include data mining, data science, big data analytics, and machine learning. She can be contacted at email ambikatanaji@gmail.com.

Manjunath Rajgopal received his bachelor's degree in computer science and engineering from University of Kuvempu, Karnataka, India, master's degree in computer science and engineering from Visvesvaraya Technological University, Karnataka India, a Master of Business Administration in Human Resources from Indra Gandhi National Open University, New Delhi, India and Ph.D. from Tumkur University, Karnataka, India. Currently working as professor and head in the Department of Computer Science and Engineering, at R R Institute of Technology, VTU. He has presented and published more than 40 papers in national and international Journal/Conferences. His areas of interest include data mining, data science and analytics, multimedia, cloud and grid computing, image processing, and business intelligence. He can be contacted at email drmanjunath.raj@gmail.com.

Annie Sujith received her master's degree from AMC Engineering College, affiliated to Visvesvaraya Technological University, Karnataka in the year 2009 and her bachelor's degree from the College of Engineering Badnera, Maharashtra in the year 2006. She obtained her Ph.D. degree in computer science and engineering from Visvesvaraya Technological University, Belgaum, Karnataka. India. She has 14 plus years of academic experience and 2 years of Industry experience. Currently, she is working as associate professor in the Department of CSE, Jyothy Institute of Technology, Bengaluru, and Karnataka. She has published and presented 21 papers in National/International Journals and Conferences and has one national level patents. Her areas of interest include computer networks, artificial intelligence, machine learning and IoT. She can be contacted at email annie.jithu@gmail.com.