Federated LSTM Model for Enhanced Anomaly Detection in Cyber Security: A Novel Approach for Distributed Threat

Dr. Aradhana Sahu[1], Prof. Ts. Dr. Yousef A.Baker El-Ebiary[2], Dr.K.Aanandha Saravanan[3], Dr.K.Thilagam[4], Gunnam Rama Devi[5], Dr. Adapa Gopi[6], Ahmed I. Taloba[7]

Associate Professor, Department of Computer Science and Engineering, Rungta College of Engineering and Technology, Bhilai, Chhattisgarh, India[1]

Faculty of Informatics and Computing, UniSZA University, Malaysia[2]

Associate Professor, VelTech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, India[3]

Associate Professor, Department of ECE, Velammal Engineering College, Chennai, India[4]

Assistant Professor, Department of Computer Science and Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur District, Andhra Pradesh, India[5]

Associate Professor, Dept.of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur Dist, Andhra Pradesh, India[6].

Department of Computer Science, College of Computer and Information Sciences, Jouf University, Saudi Arabia[7]

Information System Department-Faculty of Computers and Information, Assiut University, Assiut, Egypt[7]

***Abstract*—Technological improvements have led to a rapid expansion of the digital realm, raising concerns about cyber security. The last ten years have seen an enormous rise in Internet applications, which has greatly raised the requirement for information network security. In the realm of cyber security, detecting anomalies efficiently and effectively is paramount to safeguarding digital assets and infrastructure. Traditional anomaly detection methods often struggle with the evolving landscape of cyber threats, particularly in distributed environments. To address this challenge, the research proposes a novel approach leveraging federated learning and Long Short-Term Memory (LSTM) networks. Federated learning permits training models across decentralised data sources without sacrificing data privacy, and LSTM networks are highly effective in identifying temporal correlations in sequential data, which makes them suitable for analysing cyber security time-series data. In this paper, the study presents the federated LSTM model architecture tailored for anomaly detection in distributed environments. By allowing model updates to be performed locally on individual devices or servers without sharing raw data, federated learning mitigates privacy concerns associated with centralized data aggregation. This decentralized approach not only safeguards sensitive information but also fosters collaboration among diverse stakeholders, empowering them to contribute to model improvement without relinquishing control over their data. Python software is used to implement the method. The research demonstrate its effectiveness through experiments on real-world cyber security datasets, showcasing improved detection rates compared to traditional methods. When compared to RNN, SVM, and CNN, the suggested Fed LSTM method exhibits superior accuracy with 98.9%, which is 2.28% more advanced. Additionally, the research discuss the practical implications and scalability of our approach, highlighting its potential to enhance cyber security measures in distributed threat scenarios.**

***Keywords*—Federated learning; LSTM; anomaly detection; cyber security; distributed threats; privacy-preserving model training**

I. Introduction

It is projected that by 2030, there will be 500 billion devices linked to the Internet. For businesses, limitless Internet connectivity offers enormous convenience and opportunity [1]. But it also poses significant dangers to network security, as evidenced by the sharp rise in cybercrimes and network intrusions that has been documented in recent years. Gaining understanding of the typical sequence of attacks on networks and developing robust solutions to guarantee network security are essential in addressing concerns about network security [2]. AI and data science techniques are developing at a rapid pace, and these technologies have shown to be effective in resolving complicated problems [3]. Many AI-based networks anomaly recognition methods have been put forth in current years to show how data science and AI techniques can be combined to address network security issues [4]. Big Data presents a huge opportunity in transforming the current manufacturing paradigm into smart manufacturing, as the volume of data generated in production continues to expand. It also enables us to have based on artificial intelligence IIoT solutions 5 that operate in real-time, are more precise and efficient, and work in real-time. A lot of attention is paid to robot technology. Inanimate creatures frequently carry out tasks without human assistance, such as gathering data from the surroundings, interacting with one another, and exchanging data. The machinery will be outnumbered when the human component takes control in the future. Applications of artificial intelligence can also be assessed; these show advancement by mimicking human mental processes [5]. In this context evaluating which of the options computer systems favor in order to concentrate on correct or incorrect outcomes, modifying them in accordance with these decisions, and ultimately dressing them

up as a "humanized" structure as an idea. Sensors keep an eye on a smart manufacturing system, which uses sophisticated computing technology to oversee operations and increase system performance and product quality while cutting costs. Modern industrial control systems like these are essential to the functioning of national infrastructure like electricity grids and natural gas pipelines [6]. ICSs can be used to control power switches, hydraulic valves, and other devices by issuing commands. As a result, any ICS malfunction could result in catastrophic financial loss or environmental damage. However, the rapid expansion of IIoT presents both enormous advantages and formidable obstacles to the development and deployment of ICSs pertaining to cyber-security issues.

Therefore, it would have dire repercussions if hackers managed to take over the computer network and take the data that is crucial to security, or if viruses and worms were to infiltrate and wipe out a factory's operating system. One of the main industries being attacked by various attacks nowadays is the IIoT-based Factory Control Systems. As a result, the issue of safeguarding IIoT systems from cyber-attacks is becoming more crucial to their architecture. Numerous methods have been suggested, including intrusion detection systems (IDS), firewalls, and antivirus software. But as threats get more complex, a method for detecting anomalies is required that can identify attacks promptly and precisely, but is also small enough to be used in industrial settings with IoT devices that have limited processing capability [7]. The primary source of an attack on security is intrusion, wherein a malevolent person can quickly take or damage important data from the network system. Additionally, it may result in significant harm to IT infrastructure and additional financial losses. The challenge of keeping an eye on and distinguishing these types of network movements and actions from the typical behaviour of a network, which can have a negative effect on information system security, is known as network intrusion detection [8]. Intrusion prevention and detection are now at the forefront of the information security scene due to governments' and businesses' need for trustworthy solutions to safeguard the data they hold from unlawful accesses and disclosures. Denning [9] suggested using artificial intelligence approaches to analyse security events and discover anomalous usage patterns and invasions to construct an intrusion detection system. This concept gave rise to a new class of intrusion recognition systems, which relied less on constantly updating intrusion signatures and more on learning techniques. In the past thirty years, the traditional method of creating network anomalous detection models has been the application of ML techniques [10]. Deep Learning is a branch of ML that uses mathematical constructs resembling neurons to accomplish learning tasks. The research community has been using neural networks for many years, and its opinions have fluctuated over time.

Traditional approaches often fall short in addressing the dynamic nature of cyber threats, especially in distributed environments where data is generated and stored across various locations and devices. In response to these challenges, the concept of federated learning has emerged as a promising paradigm for collaborative model training across decentralized data sources while preserving data privacy and security. This paper presents a novel approach leveraging federated learning and LSTM networks for enhancing anomaly detection in cyber security. LSTM, a type of RNN, is well-applicable for taking temporal dependencies in sequential data, making it an ideal candidate for modelling complex patterns in cyber security datasets. Unlike standard RNNs, which suffer from the vanishing gradient problem due to the repeated multiplication of gradients during backpropagation, LSTM networks incorporate specialized memory cells and gating mechanisms to retain information over extended time intervals. LSTM networks are proficient in learning and recalling information over long sequences, making them particularly well-suited for tasks involving sequential data such as time series prediction, natural language processing, and, importantly, cyber security anomaly detection [11]. The ability of LSTM networks to capture temporal dependencies and recognize complex patterns in sequential data makes them an essential component of advanced anomaly detection systems in cyber security, enabling the detection of subtle deviations from normal behaviour that may indicate potential security threats. By integrating LSTM with federated learning, our proposed model enables distributed threat detection without the need to centralize sensitive data, thereby addressing privacy concerns and regulatory requirements. The core aim of the research is to create a robust anomaly detection system capable of effectively identifying malicious activities across distributed networks while ensuring data privacy and confidentiality. By harnessing the collective intelligence of edge devices and network nodes through federated learning, our approach empowers organizations to leverage their distributed data assets for enhancing cyber threat detection without compromising individual privacy or data sovereignty. This improves the model's stability and accuracy in dispersed contexts while adhering to strict data confidentiality regulations.

The key contribution of the proposed Federated LSTM study is as follows:

- Creation of an Innovative deep learning Federated - LSTM system that cleverly blends federated learning and long short-term memory. This approach improves the ability to precisely detect various types of network intrusion, marking a major advancement in predictive modelling for cyber security.
- Conducting extensive experiments using real-world datasets, including KDD 99, UNSW-NB15, and NSL-KDD, to assess the effectiveness and performance of the Federated LSTM architecture in detecting anomalies in distributed environments.
- Provide a framework for federated learning for the Fed - LSTM approach, leveraging creative approaches to data privacy to allow nodes to train together on models without exchanging sensitive raw data. This methodology represents a revolutionary advance in the preservation of data privacy, especially important in situations where substantial levels of confidentiality of information are required.
- Conduct a thorough assessment of the Federated-LSTM system using multiple structured datasets. This thorough testing confirms the model's resilience and efficacy in

identifying a variety of network intrusions by evaluating key performance metrics like recall, accuracy, precision, and F1 score.

The rest of the sections of this article are ordered as follows: In Section II, a synopsis of pertinent studies is provided. Section III contains the problem statement for the current system. The suggested Federated LSTM architecture and methodology for anomaly detection are explained in Section IV of the paper. Section V presents the study's findings together with the debate that followed. The conclusion of the proposed model and its potential uses are covered in Section VI.

II. Related Works

Elsayed et al. [12] suggested a hypermethod using the LSTM automatic encoding device and One-class SVM to identify anomalies-based assaults in an unstable dataset. The LSTM-auto encoder is trained to detect the latent characteristics, or compacted form of the information being provided, and recognize a typical traffic pattern before sending the input information to an OC-SVM technique. The drawbacks of the standalone OC-SVM, such as its limited capacity to function with large and high-dimensional datasets, are addressed by the hybrid model. Furthermore, we run our tests using the latest Intrusion Detection System (IDS) dataset for SDN settings, called InSDN. The findings demonstrate that the suggested model offers a greater detection rate and greatly shortens processing times. Therefore, we can be very confident that our approach will protect SDN networks from traffic that is malicious. While this is a frequent practice in anomaly detection techniques, it could make it more difficult for the model to identify new or unknown threats that deviate significantly from the typical traffic patterns found during training.

The effectiveness of network behaviour anomaly detection (NBAD) has been greatly enhanced by the use of ML as well as deep learning techniques. However, the hand-picked feature vectors used by the current machine learning-based NBAD algorithms to identify network behaviours are not adaptable enough to new attack categories or changing cyber environments, which leads to low accuracy. Low scalability has also been caused by the large-scale and high-dimensional data sets, which have greatly increased the training, retraining, and detection times. An effective NBAD method that utilizes DBNs and LSTM networks was suggested by Chen et al. [13]. Initially, a DBN is used in a nonlinear reduction of dimension technique to automatically train features in order to minimize the dimensions of the initial information while maintaining accuracy. Then, an LSTM network with a straightforward topology is used to acquire the categorization results. The results of multiple trials show that the proposed method is effective in acquiring characteristics with high accuracy, generates results rapidly, and changes the model easily. The disadvantage is that, in order to train these models, significant processing power and volumes of data are usually needed, which may not be practical or accessible in all network setups.

An ensemble approach based on the stacking generalization principle and deep models like the DNN and LSTM is presented by Dutta et al. [14]. The method applies a two-step process to the detection of network anomalies in order to increase the capacity of the suggested methodology. For the feature engineering experiment, a Deep Sparse Auto Encoder is used in the first stage of data pre-processing. For classification, an ensemble stacking learning strategy is used in the second phase. The effectiveness of the technique presented in this article is evaluated using a diversity of datasets. The findings from the assessment of the suggested methodology are spoken about. The statistical significance is examined and contrasted with the most advanced methods available for detecting network anomalies. The key disadvantage is that integrating different learning algorithms may increase system complexity, which could make it harder to understand and maintain.

An Intrusion Detection System (IDS) specifically created for SG settings utilizing the Transmission Control Protocol, or TCP, and DNP3 protocols is presented by Siniosoglou et al. [15]. A unique Auto encoder-GAN architecture is used by the proposed intrusion detection system (IDS) MENSA to identify operational irregularities and categorize DNP3 and Modbus/TCP cyber-attacks. Specifically, MENSA incorporates the previously described DNNs into a shared architecture while accounting for the reconstruction discrepancy and adversarial loss. The suggested IDS is tested in four actual SG assessment environments: the SG lab, substations, hydro power plant, and power plant. It successfully resolves a difficult multiclass classification problem with 14 classes and an outlier identification (also known as anomaly detection) problem. Moreover, MENSA is able to distinguish between five cyber-attacks directed at DNP3. The evaluation's findings show that MENSA is more effective than other ML and DL techniques in terms of metrics. The disadvantage is that for implementation and adjustment, the architectures usually ask for a large amount of processing power and knowledge. Furthermore, MENSA's efficacy in identifying cyber-attacks and operating irregularities in SG contexts is promising; however, this may be constrained by the caliber and accessibility of training data.

In order to create a reliable anomaly detection model, Ikram et al. suggested stacking a variety of DNN models, including LSTM, MLP, and Back propagation Network. The UNSW-NB15 and a campus-generated dataset are the two datasets used to analyse the ensemble model's performance. The VIT_SPARC20 dataset contains additional categories of traffic, such as encryption and decrypted malicious traffic, regular encrypted traffic, and unencrypted normal traffic. Deep learning models classify encrypted normal and illicit traffic of VIT_SPARC20 without first decrypting its contents, protecting the transmitted data's confidentiality and integrity. XGBoost combines every deep learning model's output to attain greater accuracy. It is deduced from the experimental study that UNSW_ NB yields a maximum accuracy of 99.5%. In regards to accuracy, precision, and recall, VIT_SPARC20 performs at a 99.4% level. 98% and 97%, in that order. Without having to decrypt the contents of the packets, LSTM can be incredibly useful in classifying the packets into different categories. Furthermore, it does not impose any constraints on the variables being used and has the ability to predict new forms of assaults for which the model has not been trained through learning from complicated relations between the features. In order to

demonstrate efficiency and other derived metrics, the suggested model is contrasted with the current deep learning ensembles.

Liu et al. [16] developed a new-fangled communiqué-efficient on-device FL-based anomaly recognition structure. To be more precise, the FL framework was created to allow distributed edge devices to jointly train an anomaly recognition method that enhances the model's capacity for generalization. Second, in order to precisely identify anomalies, we suggest a CNN-LSTM model based on the Attention Mechanism. By capturing significant fine-grained characteristics using CNN units based on attention mechanisms, the AMCNN-LSTM model avoids gradient dispersion issues and memory loss. Additionally, this model keeps the benefits of the Long Short-Term Memory unit for time series data prediction. To enhance communication efficiency and better align the suggested framework with the timeliness of commercial detection of anomalies, a gradient compression technique that utilizes Top-k selection was proposed. Comprehensive experiment investigations on four real-world data sets show that, in comparison to the federated learning system that lacks the gradient compression technique, the suggested framework can detect anomalies reliably and promptly while also reducing the communication cost by 50%. Variations in the distribution or quality of data among edge devices affect the model's performance and capacity for generalization, which could result in inconsistent anomaly detection accuracy between various contexts or devices.

In the Du et al.[17], NIDS-CNNLSTM is developed for the IIoT wireless sensing scenario. Its purpose is to efficiently separate and recognize network traffic data and guarantee the safety of the IIoT's equipment and operation. NIDS-CNNLSTM learns and classifies the features chosen by the CNN, integrates the potent learning capabilities of neural networks with long-term short-term memory in time series data, and validates the applicability based on binary categorization and multi-classification situations. The three dataset's verification accuracy, training loss, and accuracy rate all exhibit excellent convergence and level, and the precision rate while classifying different types of traffic is high. The models suggested in earlier research have not been able to match the overall efficacy of NIDS-CNNLSTM. Experimental results demonstrate a low false alarm rate, a high discovery rate, and grouping accuracy. Large-scale, multi-scenario network information in the IIoT is better suited for it. The main drawback is that deep learning models like CNN-LSTM were computationally intensive, especially when dealing with large-scale and high-dimensional data such as network traffic data.

The reviewed literature showcases various approaches to network anomaly detection utilizing ML and deep learning techniques. While these methods demonstrate promising results in enhancing detection rates and reducing processing times, they come with several limitations. One common challenge is the adaptability of models to new or unknown threats, as they heavily rely on training data reflecting typical traffic patterns. Additionally, scalability issues arise with large-scale and high-dimensional datasets, leading to increased training and detection times. Integration of multiple learning algorithms can elevate system complexity, hindering understanding and maintenance efforts. Moreover, implementing deep learning models may demand significant processing power and data volumes, posing practical constraints in certain network setups. Distribution variations among edge devices in federated learning frameworks could lead to inconsistent anomaly detection accuracy across contexts or devices. Despite their effectiveness, deep learning models like CNN-LSTM can be computationally intensive, especially when dealing with extensive network traffic data.

III. Problem Statement

Conventional anomaly detection techniques encounter many difficulties in the field of cyber security, especially in distributed contexts where data is dispersed among several devices or locations. Scalability, flexibility against new threats, and communication efficiency are common problems with current techniques. The problem statement revolves around the need for robust and privacy-preserving anomaly detection in distributed environments, particularly within the realm of cyber security [18]. Traditional approaches face difficulties related to data privacy and scalability, prompting the exploration of federated learning techniques. Thus, a novel technique that tackles these problems and offers improved anomaly detection capabilities in distributed cyber security environments is desperately needed. The goal is to develop an architecture that leverages Federated LSTM models to collaboratively train across decentralized nodes while safeguarding sensitive data. This involves addressing issues such as varying feature scales, vanishing and exploding gradients, and ensuring effective anomaly detection in time series data. The objective is to devise a methodology that enhances detection accuracy while maintaining data privacy, scalability, and suitability for real-world cybersecurity applications.

IV. Proposed Federated LSTM Model for Enhanced Anomaly Detection in Cyber Security

The methodology begins with the data collection process whereby data is obtained from three specified datasets that have some pertinent attributes for anomaly detection study. Follow-up pre-processing includes normalization of the data especially the numerical data through min-max normalization hence making the training of the model even more effective. Next, the structure of Federated LSTM for Anomaly Detection is explained to train models at the edge nodes, prevent the leakage of data and implement differential privacy and encryption. FL is proposed to address privacy challenges by performing model construction on smart devices and synchronizing only the model parameters with a central server. Containment of gradients is done in Federated LSTM architecture through memory block and gate structures that are alluded for optimum the anomaly detection in the time series data. Anomaly detection is done by computing anomaly scores from the reconstruction errors vectors and is considered anomalous if it meets certain threshold values. In general, this methodology combines an acquisition of the data, the pre-processing of the data, and architectural distinctive features that provide an efficient and privacy-preserved anomaly detection in the environments discussed above. The block diagram of the federated LSTM is described in the below Fig. 1 hereby is presented.

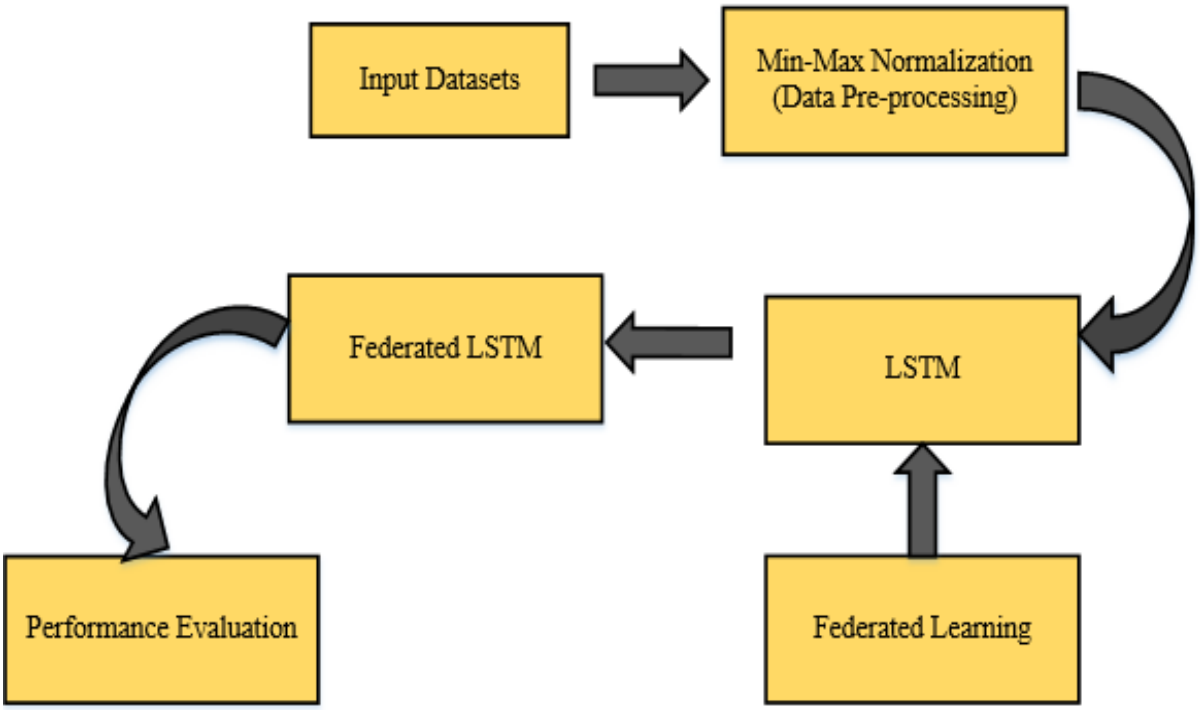


Fig. 1. The conceptual block diagram of the proposed methodology.

A. *Dataset Collection*

1) NSL-KDD Dataset 1: The secondary source is where this dataset was obtained [19]. It is made up of particular entries from the KDD 99 data set. Random sampling is not necessary because of the smaller dataset size. The percentage of entries in the KDD99 dataset is inversely related to the chosen records in every category of the NSL-KDD dataset. Diverse ML techniques have varying degrees of accuracy over a wider range, which leads to a more precise assessment for various models. There are 125,970 instances in the training dataset and 22, 5440 samples in the test dataset. There are four types of attacks in it: DoS, R2L, U2R, Probe, and a Standard class.

2) KDD-99 Dataset 2: The Kaggle website provided the dataset [13]. It is an extremely widely used dataset in IDS studies. This dataset is a subset of DARPA-98 and consists of 41 feature vectors with both category and numeric properties. There are five classes in the dataset: R2L, U2R, DoS and Probe Assault. With the exception of the Normal class, the other four groups represent assault instances.

3) UNSW-NB15 Dataset 3: This dataset is taken from the secondary source [20]. The UNSW Canberra Cyber Range Lab's IXIA Perfect Storm tool formed the fresh packets from the UNSW-NB 15 dataset's network in order to create a combination of real-world modern normal activities and manufactured modern attack behaviours. There are nine different kinds of attacks in this dataset: worms, reconnaissance, shell code, DoS, backdoors, fuzzers, and exploits. In order to produce a total of 49 features with the class label, twelve algorithms are constructed and the Argus and Bro-IDS tools are utilized.

B. *Min-Max Normalization for Data Pre*-Processing

By removing the effects of varying scales among features, normalization shortens the time it takes to train a model. Following the relocation of outliers, the min-max normalization is applied. Min-max normalisation, also known as features scaling, is a method for converting mathematical data into a range, usually between 0 and 1. This process is applied to each feature, or column, in the dataset [21]. Min-max normalization, a basic data preparation technique used in identifying anomalies in the sets of data provided using a federated LSTM Model, is the scaling of numerical data within a specific range, often between 0 and 1. This method ensures that any additional data values are rescaled linearly with respect to this range and that, in the absence of an explicit equation, the dataset's lowest and maximum values are transformed to 0 and 1, respectively [22]. By calculating the feature or column's lowest and maximum values, eliminating the minimal value, and dividing by the range of values, the normalization procedure adjusts each data point independently. The min-max normalization is represented by Eq. (1) and Eq. (2).

$$Y_{std} = \frac{Y - Y_{min}}{Y_{max} - Y_{min}} \quad (1)$$

$$Y_{scaled} = Y_{std} * (max - min) + min \quad (2)$$

By doing this, you can be sure that the values that fall between will be scaled linearly to match the transformation of the lowest value to 0 and the highest value to 1. This normalization method is particularly useful when features have different scales since it ensures uniformity among the features and supports the performance of the ML model during training.

C. Architecture of Federated LSTM for Anomaly Detection

The federated approach enables us to train the LSTM model collaboratively across multiple decentralized nodes, each retaining its own sensitive data, without the want to share the raw data centrally. Federated learning guarantees data privacy and safety while harnessing the collective understanding from various resources to improve the model's robustness and generalization capability. The study appoint a sequential studying strategy wherein each nearby node trains its LSTM model on its respective information subset and periodically exchanges version updates with a central coordinator. This coordinator aggregates the local version updates to iteratively refine the global LSTM model, which encapsulates insights from the whole federated network. The Federated LSTM model presents a novel approach to anomaly detection in cyber security, comprising client-side and server-side components. At the client-side, individual devices or network nodes host their LSTM models, processing and analysing local data streams consisting of logs, network traffic, and system events. The privacy of sensitive data is maintained as it remains on the client-side, with continuous learning facilitated by the LSTM model. Concurrently, the server orchestrates federated learning, ensuring model updates without direct access to raw data. It distributes global model parameters to all participating clients, which are then used to train local LSTM models. Updated parameters, or gradients, are sent back to the server for aggregation, facilitating iterative model improvement over multiple rounds. This process, devoid of centralized data, enhances cyber security while preserving privacy. Efficient communication protocols are pivotal for secure parameter exchange between the server and clients, minimizing overhead. Model aggregation techniques, such as averaging or Federated Averaging, consolidate parameters received from diverse clients, augmenting the global model's efficacy. Continuous evaluation and monitoring, gauging metrics like accuracy and false positive rates, ensure the model's efficacy in detecting anomalies, fostering adaptability to evolving threats.

Additionally, strategies such as differential privacy and encryption were incorporated to the addition of safeguard sensitive information in the course of version aggregation and communication. This novel federated LSTM framework not only effective enhances anomaly detection accuracy but also additionally addresses the scalability and privacy concerns inherent in conventional centralized processes, making it well-suited for real-world cyber security applications in distributed environments.

To perform at their best, deep learning models require an adequate supply of training data. This data is frequently utilized to create a global model by transmitting information from distributed sensors to a centralized server. Concerns regarding data protection, however, might make data exchange difficult, if not impossible, across numerous locations and companies. It becomes more challenging to create efficient algorithms with multi-party data while preserving data privacy. In recent years FL has been proposed as a potential solution to these privacy issues. FL was first suggested by McMahan et al. in 2016. Essentially, FL uses a distributed learning methodology to minimize the risk of data leakage while facilitating team training across numerous devices. Edge computers have the capacity to carry out more computing tasks as a result of the growth of edge computing, creating an environment that is inherently FL-friendly. Since everyone involved trains the local model using local data, the FL task avoids the need to gather a sizable amount of raw data. Only the model weights are sent to a central server. After multiple iterations, a global design is generated, eliminating any potential privacy issues.

A certain quantity of private data must be combined and examined at central servers in order to use LSTM during the training phase utilizing conventional deep learning techniques. This raises the possibility of data privacy breaches throughout the training phase. In order to overcome these privacy concerns, federated deep learning a jointly distributed deep learning paradigm was presented as a way for edge devices to build a global model without sharing raw training data, all while retaining the training datasets locally. Initialization, Aggregation, and Update phases make up the three stages of the FL method. During the setup stage, let's say that FL has N edge devices, and each edge device receives a pre-trained global models ω_t from the public datasets via a parameter aggregator, also known as a cloud aggregator. After that, each device trains and refines the global model ω_t in every iteration using a local dataset $B_k$of size B_k. The aggregator gathers local gradients provided by the edge nodes during the aggregation phase. To do this, the following Eq. (3) represents the loss function to be improved is used.

$$\min_{y \in Rd} P_k(y) = \frac{1}{B_k} \sum_{i \in Dk} Ez_i \sim B_k \, f(y;\, z_i) + \lambda h(y) \qquad (3)$$

Where h (•) serves as a regularize functions of k, f () represents the local loss function for k, and z_i is a sample taken from the localized dataset B_k on the k device. Additionally, ∀λ ∈ [0, 1]. A different global model ω_{t+1} is obtained for the following repetition by the cloud aggregator using the Fed AVG procedure during the update phase. As a result, in Eq. (4)

$$\omega_{t+1} \leftarrow \omega_t + \frac{1}{n} \sum_{n=1}^{N} P_{t+1}^n \qquad (4)$$

Where $\frac{1}{n} \sum_{n=1}^{N} P_{t+1}^n$ indicates an average aggregation (i.e., Fed AVG method) and $\sum_{n=1}^{N} P_{t+1}^n$ indicates the aggregation of model updates. The aforementioned procedure is repeated by the cloud aggregator and edge devices till the global model converges. Through the decoupling of training models from direct accessibility to the raw data used for training on edge nodes, this approach dramatically lowers the risks associated with privacy leaks. Fig. 2 shows the architectural diagram of the federated LSTM is given below.

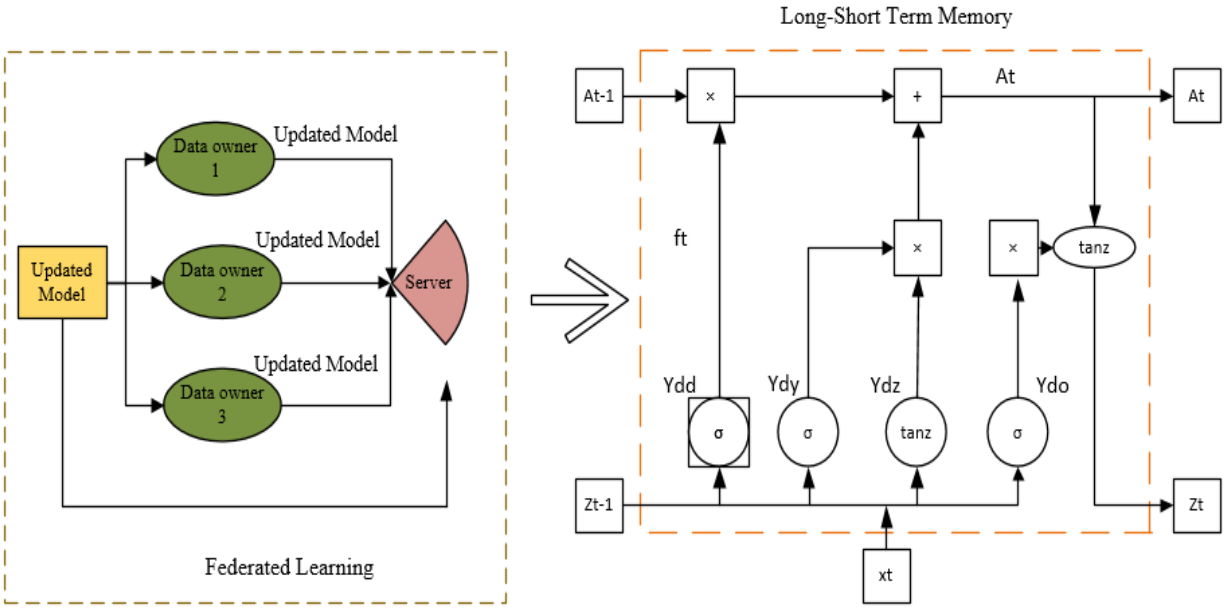


Fig. 2. Architecture of federated LSTM.

Long short-term memory has been added to RNNs through improvements. As a substitute to conventional RNN units, the LSTM proposes memory blocks to handle the problem of expanding and disappearing gradients. The study employ LSTM variation of a RNN to enable accurately anticipate the sensing time series data to sense anomalies. A well-constructed "gate" structure is used by LSTM to add or delete information from the cell's state. Information can be passed selectively using the "gate" structure.

An LSTM network can recall information from the past and draw connections with present data. An input to the gate, a gate to forget, and a gate for output are connected to an LSTM [23]. The input is denoted by x_t, by A_t and A_{t-1}, denotes new and last state respectively, and the recent and prior outputs by z_t and z_{t-1}.

The following forms illustrate the LSTM input gate idea.

$$j_t = \sigma(\mathrm{Y}_i \cdot [z_{t-1}, y_t] + b_j) \quad (5)$$

$$\tilde{A}_t = \tanz(Y_j \cdot [z_{t-1}, \mathrm{y}_t] + \mathrm{b}_j) \quad (6)$$

$$\mathrm{A}_t = f_t \mathrm{A}_{t-1} + j\tilde{A}_t \quad (7)$$

where, z_{t-1} and y_t are passed via a sigmoid layer in Eq. (5) to identify which bit of information ought to be added. After z_{t-1} and y_t have passed through the tanz layer, more information is obtained using Eq. (6) in this case. The currently available information,$\tilde{A}_t$, and the long-term storage data, A_{t-1} into A_t are combined in Eq. (7). A sigmoid output is indicated byY_i, while a tanz output is shown by$\tilde{A}_t$. In this case, Y_i represents the weight matrices, while $b_t$is the bias of the LSTM input gate. The resultant dot and sigmoid layer can then selectively pass information through the LSTM's forget gate. The decision to remove pertinent data from a previous cell is made with a given probability. To decide whether to save pertinent data from a previous cell with a specific possibility, apply Eq. (8) The weight matrix is represented by Y_f, the offset by b_f, and the sigmoid function by σ. Q_t is represented in Eq. (9)is the output gate at time step t. $z_t$is the cell state represented in Eq. (10).

$$f_t = \sigma(Y_f \cdot [z_{t-1}, y_t] + \mathrm{b}_f) \quad (8)$$

$$Q_t = \sigma(X_o \cdot [Z_{t-1}, y_t] + b_o) \quad (9)$$

$$z_t = P_t \tanz(\mathrm{A}_t) \quad (10)$$

Where the weighted matrices Y_o and the LSTM bias b_o, respectively, represent the output gate. It is represented in Eq. (11) and Eq. (12).

$$y^{\,j}_{n-T+1}, y^{\,j}_{n-T+2}, \cdots, y^{\,j}_{n} \;\rightarrow^{f(\cdot)}\; [y^{\,j}_{n+1}, y^{\,j}_{n+2}, \cdots, y^{\,j}_{n+T}] \quad (11)$$

$$B_n = (\beta_n - \mu)^T \sigma^{-1} (\beta_n - \mu) \quad (12)$$

A point in a sequence can be predicted to be "anomalous" or "normal" in an unsupervised scenario if $B_n > \varsigma$ ($\varsigma = max\ F_\theta = (\frac{1+\theta^2)\times P \times R}{\theta^2 P + R}$). Fig. 3 shows the mechanism of the proposed Federated LSTM and Fig. 4 shows the flow chart of the proposed model is given below.

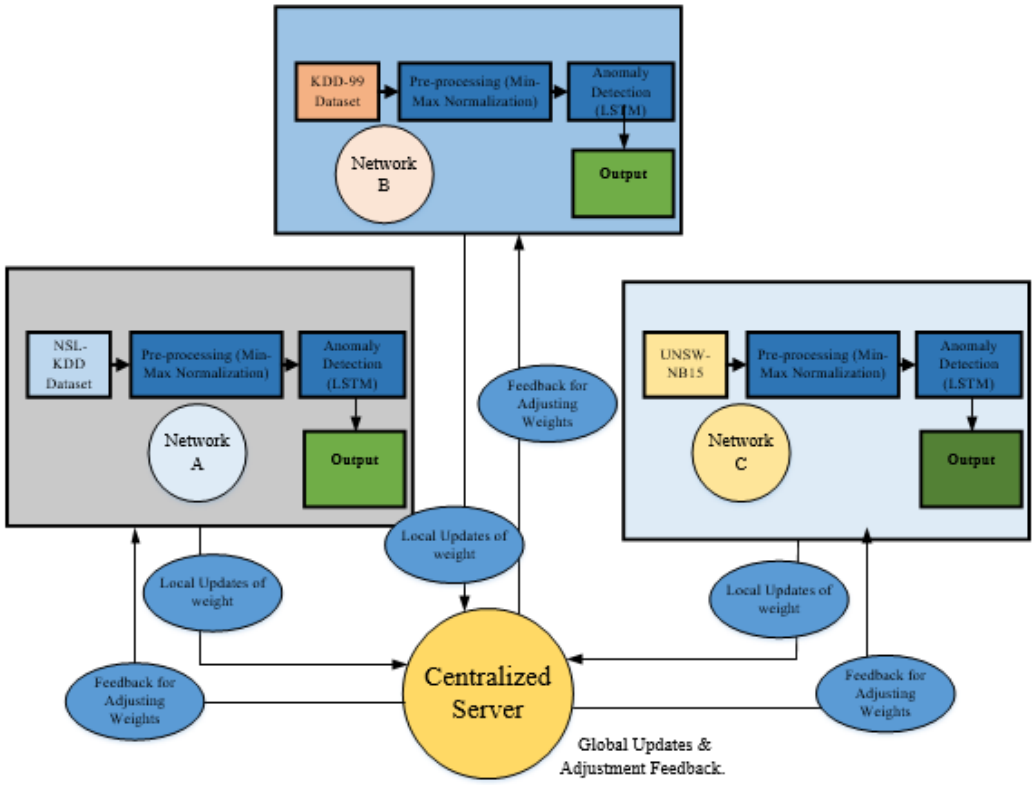


Fig. 3. Mechanism of the federated LSTM.

Federated Averaging Algorithm (Fed Avg.)

Initialize weights ω_0 of the global model N

for each round t do

$S_t \leftarrow$ randomly selected n clients

Send model N to S_t clients

for each client k do

ω k t+1 ← Update client (wt , k)

$\omega_{t+1} \leftarrow$ PM m=1 nm n Lm(ω)

end

Send model N to all clients

At client: Client Update(k, wt) procedure

B ← P_k is split into batches B of size bS

for every epoch e < E do

for batch b ∈ B do

ω ← ω − η1L(ω)

end

send ω to server

end

end

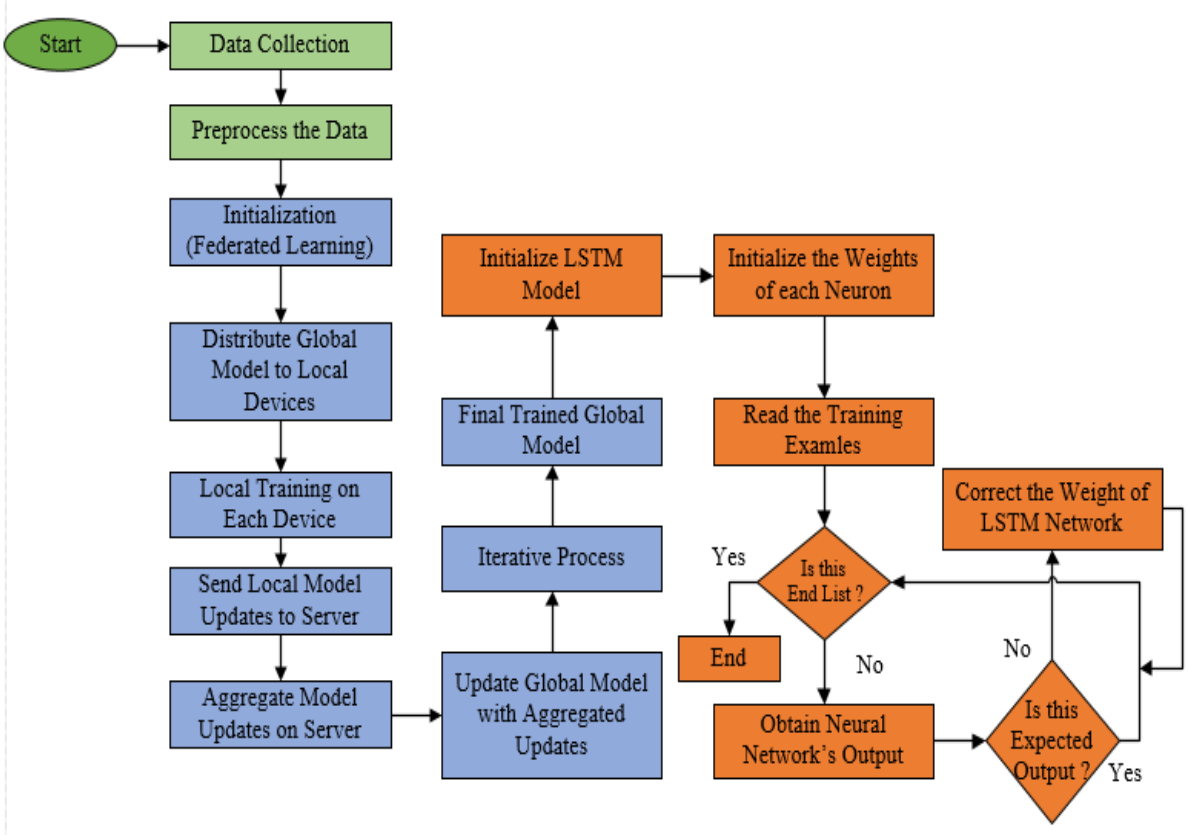


Fig. 4. Flowchart of the proposed federated LSTM.

V. Results and Discussion

A comprehensive analysis of the conclusions and findings from the experimental assessment of anomaly identification to improve cyber security is provided in the results section. The results and discussion section of the study encompasses the findings obtained from empirical evaluations, comparisons with existing approaches, and the implications of the proposed Federated LSTM architecture for anomaly detection in distributed environments. To locate the anomaly, three distinct datasets are consulted. Python programming language and the Windows 10 operating system are being used. This next statistic was used to assess the efficiency of the model.

A. Performance Metrics

1) Accuracy: Comparing the actual labels for the test dataset with the predicted class labels produced by LSTM in order to determine the accuracy. If the projected label matches the actual label f in the test dataset, increase the "Number of Correct Predictions" then divide this count by the "Total Number of Predictions".

Accuracy is determined by the following Eq. (13)

$$Accuracy = \frac{RN+RP}{RP+AP+RN+AN} \quad (13)$$

2) Precision: Precision is a frequently assessed metrics in detection problems, primarily in ML and statistics. It assesses a system's ability to make optimistic calculations about the future. The ratio of correct estimates to all reliable estimates is known as precision.

The precision in expressed in Eq. (14) is as follows:

$$Precision = \frac{True\ Positives}{(True\ Positives+False\ Positives)} \quad (14)$$

The accuracy level is a number between 0 and 1, where 1 represents complete precision and 0 represents no right positive predictions.

3) Recall: True positive rate and sensitivity are other names for recall. The model's capacity to accurately recognise each pertinent instance of a given class that exists in the dataset is necessary for effective detection. Out of all actual positive occurrences for a class, it calculates the proportion of true positive predictions, or accurately identified cases of that class. Recall is described mathematically by Eq. (15).

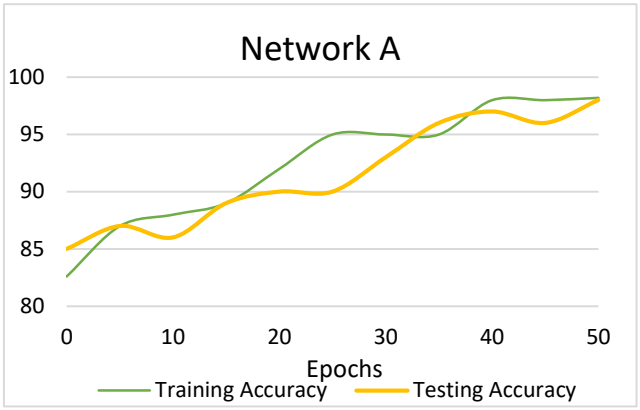
$$Recall(sensitivity) = \frac{True\ Positives}{True\ Positives+False\ Negatives} \quad (15)$$

4) F1-Score: A popular metric for assessing sorting models' performance in detection tasks is the F1 score, which is particularly useful for models that perform well in anomaly identification and prediction. When a dataset is imbalanced—that is, when one class greatly outnumbers the other—the F1 score comes in handy. The F1 score is evaluated using the Eq. (16)

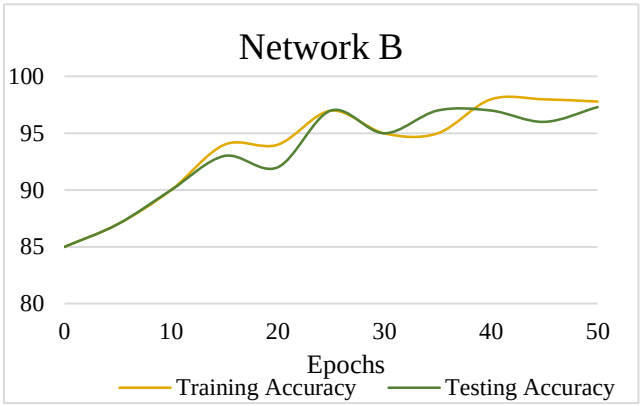
$$F1\ Score = 2 \times \frac{(Precision*Recall)}{(Precision+Recall)} \quad (16)$$

The F1 score provides a neutral and useful measure of both recall and precision that one should consider in your evaluation. It is a valuable statistic to employ when deciding between precision and recall, as is often the case in detection tasks.

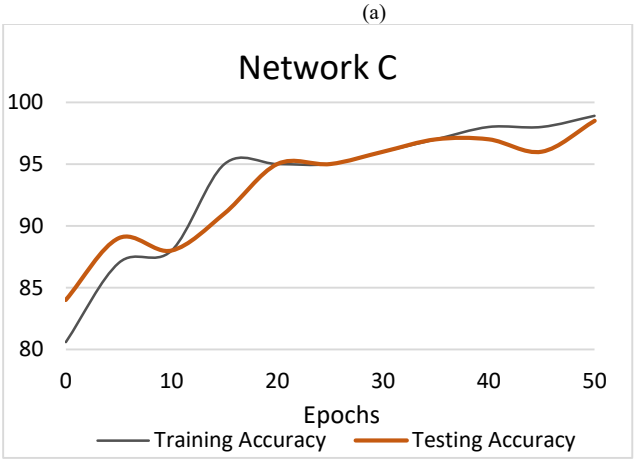
Fig. 5 illustrates the training and testing accuracy of LSTM models for three distinct networks, labelled as Network A, Network B, and Network C, along with the Federated LSTM (Fed-LSTM) Model. In Fig. 5(a), (b), and (c), the study can observe the performance of individual LSTM models trained and tested on different network datasets. Each network likely represents a specific environment or context within the cyber security domain. The training accuracy measures how well the LSTM models fit the training data, while the testing accuracy indicates their performance on unseen data. Generally, the research aim for high testing accuracy to ensure the model's efficiency in real-world scenarios.



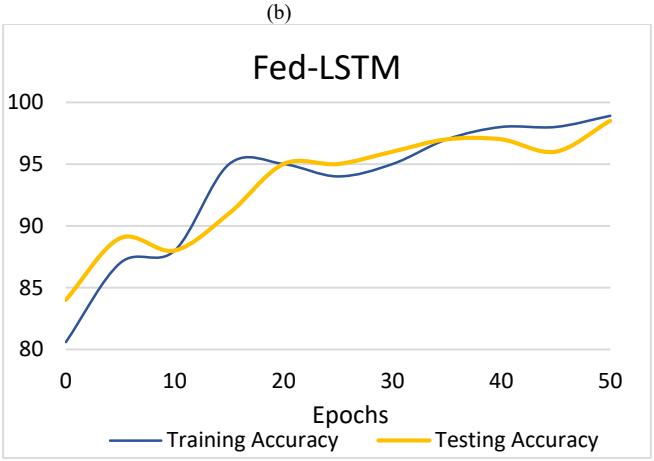
(a)



(b)

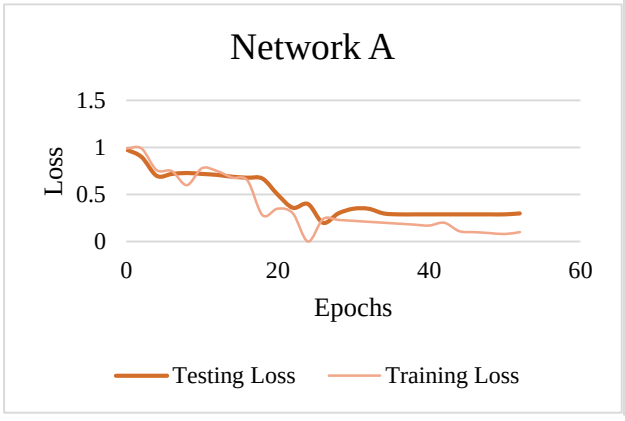


(c)

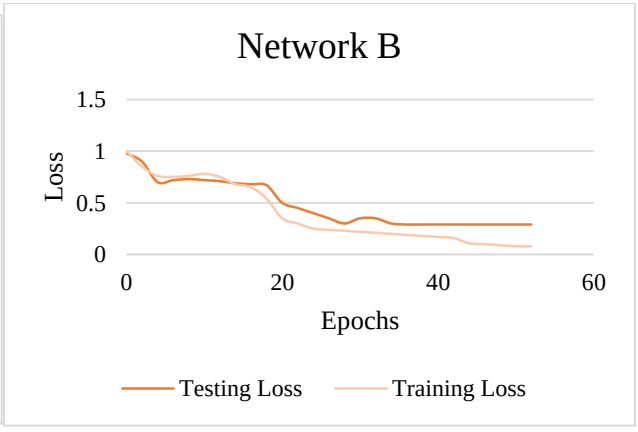


(d)

Fig. 5. Training and testing accuracy of LSTM model for (a) Network A, (b) Network B, and (c) Network C and (d) Fed-LSTM model.



(a)



(b)

(c) (d)

Fig. 6. Training and testing loss of LSTM model for (a) Network A, (b) Network B, and (c) Network C and (d), Fed-CNN model.

Fig. 6 illustrates the training and testing loss curves for three individual LSTM models trained on Network A, Network B, and Network C, respectively, as well as the Fed-CNN model. The training loss represents the error incurred during the model's training phase, while the testing loss reflects the model's performance on unseen data, providing insights into its generalization capabilities. In Fig. 6(a), (b), and (c), loss curves for the individual LSTM models on Networks A, B, and C using three different datasets shows the convergence of the models during training. Ideally, both training and testing losses decrease over successive epochs, indicating that the models are effectively learning the underlying patterns in the data without over fitting. Discrepancies between the training and testing loss curves may indicate potential over fitting or under fitting issues, highlighting the importance of proper regularization techniques and model tuning.

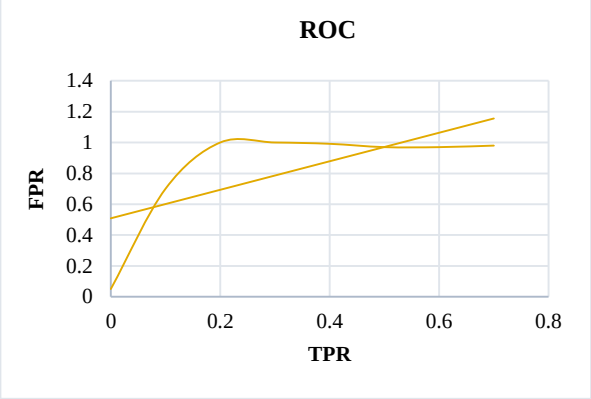


Fig. 7. ROC of the proposed fed LSTM model.

Fig. 7 presents the ROC of the Federated LSTM model. The ROC is a representation that illustrates the trade-off between the sensitivity and the specificity across different threshold values for detection tasks. In anomaly detection in cyber security, the ROC curve of the Fed LSTM model provides insights into its discrimination ability between normal and anomalous network activities. The curve plots the TPR against the FPR at various decision thresholds.

TABLE I. COMPARISON OF THE PERFORMANCE METRICS OF EXISTING METHODS AND SUGGESTED METHOD

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1Score (%)
RNN [24]	94.64	93.60	92.24	92.42
SVM [25]	97.00	96.78	94.08	94.21
CNN [26]	98.43	96.20	96.50	96.78
Proposed Federated LSTM	98.9	98.2	98.80	98.08

The suggested model's metrics are displayed in Table I and it is graphically illustrated in Fig. 8. It shows the Accuracy (98.9%), Precision (98.2%) Recall (98.80%) and F1-score (98.08%) of the fed LSTM approach with other methods. The accuracy of the suggested method Federated LSTM is greater than the traditional approaches RNN (94.64%), SVM (97.00%), CNN (98.43%) and Proposed Federated LSTM (98.9%).

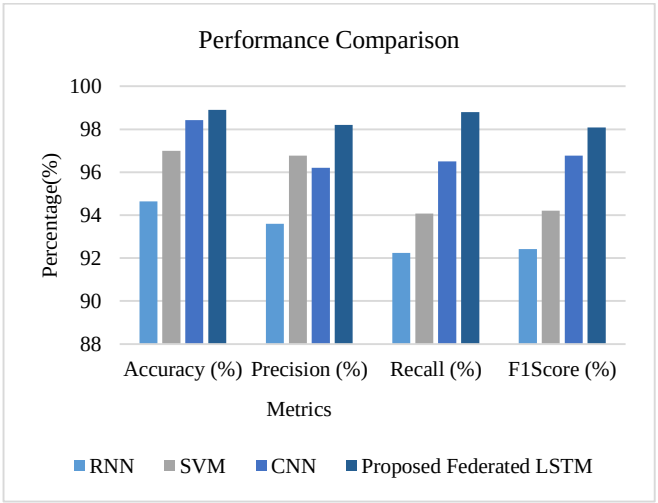


Fig. 8. The performance measures of the suggested method using traditional methods.

TABLE II. ACCURACY OF EXISTING METHODS AND SUGGESTED METHOD ARE COMPARED WITH THREE DATASETS

Accuracy			
Methods	**NSL-KDD (Network A)**	**KDD-99 (Network B)**	**UNSW-NB15 (Network C)**
RNN	92.18	94.21	94.67
CNN	82.83	97.34	98.43
Auto encoder, SVM	96.56	96.01	97.00
Federated LSTM	98.2	97.8	98.9

Table II presents accuracy scores of different anomaly detection methods on various datasets: NSL-KDD, KDD-99, and UNSW-NB15. However, the Federated LSTM model outperforms all methods, achieving the highest accuracies across all networks, showcasing its effectiveness in collaborative learning while preserving data confidentiality and safety, making it a promising approach for enhancing cyber security in distributed environments.

B. Discussion

The results presented in the study showcase the effectiveness of the proposed Federated LSTM architecture for anomaly detection in distributed environments. Through empirical evaluations and comparisons with existing approaches, the Federated LSTM model demonstrates greater performance in terms of metrics across multiple datasets, including NSL-KDD, KDD-99, and UNSW-NB15 networks. Notably, the Federated LSTM model outperforms traditional methods such as RNN, SVM, and CNN, achieving higher accuracies and demonstrating its potential in enhancing cyber security measures. The graphical representations further support these findings, illustrating the training and testing accuracy, loss curves, and ROC curve of the Federated LSTM model, which collectively highlight its robustness and effectiveness in identifying anomalies while preserving data privacy and security in distributed environments. Overall, these results underscore the promising prospects of the Federated LSTM approach for improving anomaly detection and bolstering cyber security in complex network infrastructures.

VI. CONCLUSION AND FUTURE SCOPE

One potential approach to addressing the difficulties associated with distributed threat detection is the Federated LSTM Model for Enhanced Anomaly Detection in Cyber Security. The model shows enhanced anomaly detection capabilities across remote networks while maintaining data confidentiality and privacy by utilizing federated learning approaches and LSTM neural networks. It has been demonstrated through testing and assessment to perform better than conventional centralized methods, providing more scalability and effectiveness in identifying cyber threats. Through experimentation and evaluation, using real-world datasets, to assess the effectiveness and performance of the Federated LSTM architecture in detecting anomalies in distributed environments. The model has demonstrated superior anomaly detection capabilities compared to traditional centralized approaches, while ensuring data privacy and security across distributed networks. Future refinements could include optimizing model architectures, adapting it for real-time detection scenarios, integrating with edge computing infrastructure for localized processing, and enhancing adversarial robustness. Additionally, exploring collaborative threat intelligence sharing and interoperability standards would further enhance the model's effectiveness and facilitate wider adoption in cyber security applications. Overall, continued research and development in this area hold great promise for improving cyber security posture and mitigating evolving threats in our increasingly interconnected digital landscapes.

REFERENCES

[1] H. Allioui and Y. Mourdi, “Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey,” *Sensors*, vol. 23, no. 19, Art. no. 19, Jan. 2023, doi: 10.3390/s23198015.

[2] A. M. Rahmani, S. Bayramov, and B. Kiani Kalejahi, “Internet of Things Applications: Opportunities and Threats,” *Wireless Pers Commun*, vol. 122, no. 1, pp. 451–476, Jan. 2022, doi: 10.1007/s11277-021-08907-0.

[3] J. M. Górriz *et al.*, “Artificial intelligence within the interplay between natural and artificial computation: Advances in data science, trends and applications,” *Neurocomputing*, vol. 410, pp. 237–270, Oct. 2020, doi: 10.1016/j.neucom.2020.05.078.

[4] M. M. Saeed, R. A. Saeed, M. Abdelhaq, R. Alsaqour, M. K. Hasan, and R. A. Mokhtar, “Anomaly Detection in 6G Networks Using Machine Learning Methods,” *Electronics*, vol. 12, no. 15, Art. no. 15, Jan. 2023, doi: 10.3390/electronics12153300.

[5] J.M. Górriz et al., “Computational approaches to Explainable Artificial Intelligence: Advances in theory, applications and trends,” *Information Fusion*, vol. 100, p. 101945, Dec. 2023, doi: 10.1016/j.inffus.2023.101945.

[6] M. Majid *et al.*, “Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review,” *Sensors*, vol. 22, no. 6, Art. no. 6, Jan. 2022, doi: 10.3390/s22062087.

[7] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, “Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications,” *IEEE Access*, vol. 8, pp. 151019–151064, 2020, doi: 10.1109/ACCESS.2020.3016826.

[8] João Vitorino et al., “SoK: Realistic adversarial attacks and defenses for intelligent network intrusion detection,” *Computers & Security*, vol. 134, p. 103433, Nov. 2023, doi: 10.1016/j.cose.2023.103433.

[9] D. E. Denning, “An Intrusion-Detection Model,” *IIEEE Trans. Software Eng.*, vol. SE-13, no. 2, pp. 222–232, Feb. 1987, doi: 10.1109/TSE.1987.232894.

[10] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, “Cybersecurity data science: an overview from machine learning perspective,” *J Big Data*, vol. 7, no. 1, Art. no. 1, Dec. 2020, doi: 10.1186/s40537-020-00318-5.

[11] N. Oliveira, I. Praça, E. Maia, and O. Sousa, “Intelligent Cyber Attack Detection and Classification for Network-Based Intrusion Detection Systems,” *Applied Sciences*, vol. 11, no. 4, p. 1674, Feb. 2021, doi: 10.3390/app11041674.

[12] M. Said Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, “Network Anomaly Detection Using LSTM Based Autoencoder,” in *Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, Alicante Spain: ACM, Nov. 2020, pp. 37–45. doi: 10.1145/3416013.3426457.

[13] A. Chen, Y. Fu, X. Zheng, and G. Lu, “An efficient network behavior anomaly detection using a hybrid DBN-LSTM network,” *Computers & Security*, vol. 114, p. 102600, Mar. 2022, doi: 10.1016/j.cose.2021.102600.

[14] V. Dutta, M. Choraś, M. Pawlicki, and R. Kozik, “A Deep Learning Ensemble for Network Anomaly and Cyber-Attack Detection,” *Sensors*, vol. 20, no. 16, p. 4583, Aug. 2020, doi: 10.3390/s20164583.

[15] I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, "A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments," *IEEE Trans. Netw. Serv. Manage.*, vol. 18, no. 2, pp. 1137–1151, Jun. 2021, doi: 10.1109/TNSM.2021.3078381.

[16] Y. Liu *et al.*, "Deep Anomaly Detection for Time-series Data in Industrial IoT: A Communication-Efficient On-device Federated Learning Approach," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6348–6358, Apr. 2021, doi: 10.1109/JIOT.2020.3011726.

[17] J. Du, K. Yang, Y. Hu, and L. Jiang, "NIDS-CNNLSTM: Network Intrusion Detection Classification Model Based on Deep Learning," *IEEE Access*, vol. 11, pp. 24808–24821, 2023, doi: 10.1109/ACCESS.2023.3254915.

[18] Fargana Abdullayeva, "Cyber resilience and cyber security issues of intelligent cloud computing systems," *Results in Control and Optimization*, vol. 12, p. 100268, Sep. 2023, doi: 10.1016/j.rico.2023.100268.

[19] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," *IEEE Symposium. Computational Intelligence for Security and Defense Applications, CISDA*, vol. 2, Jul. 2009, doi: 10.1109/CISDA.2009.5356528.

[20] V. Kumar, D. Sinha, A. K. Das, S. C. Pandey, and R. T. Goswami, "An integrated rule based intrusion detection system: analysis on UNSW-NB15 data set and the real time online dataset," *Cluster Comput*, vol. 23, no. 2, pp. 1397–1418, Jun. 2020, doi: 10.1007/s10586-019-03008-x.

[21] S. Yu, J. Wang, J. Liu, R. Sun, S. Kuang, and L. Sun, "Rapid Prediction of Respiratory Motion Based on Bidirectional Gated Recurrent Unit Network," *IEEE Access*, vol. 8, pp. 49424–49435, 2020, doi: 10.1109/ACCESS.2020.2980002.

[22] A. Soleimani and S. E. Khadem, "Early fault detection of rotating machinery through chaotic vibration feature extraction of experimental data sets," *Chaos, Solitons & Fractals*, vol. 78, pp. 61–75, Sep. 2015, doi: 10.1016/j.chaos.2015.06.018.

[23] Md. Z. Islam, Md. M. Islam, and A. Asraf, "A combined deep CNN-LSTM network for the detection of novel coronavirus (COVID-19) using X-ray images," *Informatics in Medicine Unlocked*, vol. 20, p. 100412, 2020, doi: 10.1016/j.imu.2020.100412.

[24] I. Ullah and Q. H. Mahmoud, "Design and Development of RNN Anomaly Detection Model for IoT Networks," *IEEE Access*, vol. 10, pp. 62722–62750, 2022, doi: 10.1109/ACCESS.2022.3176317.

[25] K. Yang, S. Kpotufe, and N. Feamster, "An Efficient One-Class SVM for Anomaly Detection in the Internet of Things." arXiv, Apr. 22, 2021. Accessed: Mar. 08, 2024. [Online]. Available: http://arxiv.org/abs/2104.11146.s

[26] S. A. V. Shajihan, S. Wang, G. Zhai, and B. F. Jr. Spencer, "CNN based data anomaly detection using multi-channel imagery for structural health monitoring," *Smart Structures and Systems*, vol. 29, no. 1, pp. 181–193, Jan. 2022, doi: 10.12989/SSS.2022.29.1.181.