Received: 3 July 2024 | Revised: 29 September 2024 | Accepted: 19 October 2024 | Published online: 31 October 2024

Journal of Computational and Cognitive Engineering
2025, Vol. 4(2) 223–235
DOI: 10.47852/bonviewJCCE42023751
BON VIEW PUBLISHING

RESEARCH ARTICLE

An Advanced Cyber Security Model Using Federated Machine Learning Approach for Intrusion Detection in Networks

Mahantesh Laddi[1,*], **Shridhar Allagi**[2], **Rashmi Rachh**[3], **Kuldeep Sambrekar**[4] **and Shrikant Athanikar**[5]

[1] *KLE College of Engineering and Technology, Visvesvaraya Technological University, India*

[2] *KLE Institute of Technology, Visvesvaraya Technological University, India*

[3] *Department of Computer Science and Engineering, Visvesvaraya Technological University, India*

[4] *KLS Gogte Institute of Technology, Visvesvaraya Technological University, India*

[5] *VSM's Somashekhar R. Kothiwale Institute of Technology, Visvesvaraya Technological University, India*

Abstract: The intelligent cyber security model for intrusion detection with federated machine learning is based on distributed learning protocols for processing data and training models while preserving data security and privacy. Data owners can use the federated machine learning architecture to create a standard intrusion detection system by transferring their data without revealing private information. Taking a global approach to fraud management, models based on predictive analysis and anomaly detection are developed using a federated learning model. By leveraging unsupervised machine learning algorithms, the system can find new and unconventional ways fraudsters make a move by recognizing intricate relationships within them. In addition, the system can develop an adaptive intrusion detection solution with current new profile downloads and model training. This model is a handy and effective mechanism culminating in distributed architectures and proper data processing protocols to develop radical improvements in security systems to counter cyberattacks. Also, the model seeks to enhance cyber security systems since federated learning combines the strength that comes with advances in data analysis techniques, which helps in the detection and response to cyberattacks.

Keywords: cyber security, intrusion detection, machine learning, centralized detection, malicious behavior, fraud management

1. Introduction

Adversarial attacks are capable of causing obvious and widespread harm to today's organizations. The machine learning (ML) models to present times are falling vulnerable to adversarial attacks at an alarming rate, and this vulnerability can go a long way in redefining the way modern organizations operate. All you need to know is that an adversarial attack is when an attacker creates bad data such that an ML model predicts a test point wrong. Such an attack could result in bad decisions or even harm end users [1]. These organizations must have some input processing or filtering mechanism to protect against the input features that contain adversarial examples, which could be used to attack them. Always tracking the input features of the model is one strategy that seems to work well. It is also possible to find features that show malicious intention when using data in the model [2]. Identify those features, and you can remove or split them from your model. A permutation is used to use multiple ML models as a supplement to find malicious input. For instance, an ensemble of various models, random forest, logistic regression, and possibly even a straightforward support vector machine will have its features. The malicious intent can be laid bare by any of these [3]. When an attacker tries to manufacture an input that would lead to a misclassification of a test point, the models should be trained to detect the attack and refuse the input, blocking the attacker from attacking the end user. In addition to the techniques described above, organizations must ensure their ML is safeguarded from how it was built [4]. For instance, every model should include rigid input validation methods that will help ensure the input is not malicious. Finally, organizations need to continually patch and monitor ML models to maintain their security and safety. Organizations should inoculate themselves, as it were, against an attack on their ML models [5]. Organizations can protect themselves against adversarial attacks by carefully monitoring input features, using different ML models, and watching for design flaws in real production environments. No single "minimal feature set" can be used to classify malicious code reliably [6]. However, several characteristics must be considered to properly categorize a specific piece of malware rather than just one. First, some feature sets should be derived from malicious code properties. The type of threat can be identified by properties like size, configuration, code logic, etc., of any given malware sample. Moreover, signs, for example, John Hancocks, encryption keys, or other manifest

*Corresponding author: Mahantesh Laddi, KLE College of Engineering and Technology, Visvesvaraya Technological University, India. Email: mahanteshl@klecet.edu.in

© The Author(s) 2024. Published by BON VIEW PUBLISHING PTE. LTD. This is an open access article under the CC BY License (https://creativecommons.org/licenses/by/4.0/).

attributes (marks), can also help to distinguish malicious code [7]. After researching the features of the code, the second process is to examine the behavior generated by the malicious code. Some behaviors that can be examined include trying to call out external domains, processes created by the malware, and files that malware may have dropped [8]. The impact of the misbehavior can be one of the ways to create an end-to-end threat, and it can generate a full threat profile using this. This might include changes made to the system (e.g., altered registry, creating new files) and information or data stolen [9]. This set of attributes, characteristics, and behaviors can then create a rich feature set for each attribute to correctly classify any particular malware sample. Such an awareness is crucial to deterring new threats, and because threats evolve, how they are addressed must also do so [10]. Real data is data that has not been altered in any form. By its correspondence with what is going on, one can be assured of the accuracy and the reliability of the results of their investigations referred to in the data. Decision-making is impossible without accurate data as it is a trustworthy source of information on which decisions are made. However, maliciously augmented data is the augmented data that has been intentionally manipulated and changed to have the desired results [11]. People have done this for many reasons, whether abhorrent or to move the needle a little in one direction. If there were no sound to accompany the visual images, it could easily look like straight footage taken at a riot, and that is hugely dangerous: augmented data used to make claims or decisions. Data can be either real, similar, but modified or deliberately forged, and the cost of entangling the false state of affairs might be extremely severe [12]. Understanding the differences and validating the data are essential, as all the business branches will rely on it for future-planned decisions. This has been the years of a new era, an era of cyberattacks on different kinds of organizations and industries all over the world. A great incident response community is an essential part of defending against these types of attacks. While incident response is crucial in any security stance because new attacks can be found with little or no awareness, the growing number of attacks requires broader and more reactive countermeasures [13]. Federated machine learning (FML) is a hot research area that enables organizations to learn from collectively observed data from different data sources in a distributed manner without sharing these data sources in their raw (unprocessed) forms. With FML and distributed computing, organizations can create a stronger incident response model and more accurately flag future alerts on the fly. FML offers numerous benefits over traditional incident response techniques. It enables organizations to carry out ML-based data processing on data originating from multiple distributed sources more efficiently, enabling them to train prediction models on various data sources. Second, FML models can be trained from encrypted data and support the containment of privacy by design by ensuring that organizations can not only return the promise of privacy to user data but also do so while still allowing useful predictive features to be derived from the data [14]. FML further helps organizations build the models without sharing the data, reducing the risk of data breaches. FML further enables a response to the changing world of cyber as well. Organizations can then automate responding by collaboratively training models to iterate on the feedback into their incident response policies quickly. By allowing FML to automate incident response processes, automating human intervention can reduce human errors. The FML response process can be automated to reduce human errors due to manual handling [15]. FML presents a viable way to construct a more reactive joint defense strategy against adversarial threats. Nevertheless, a broad spectrum of these functionalities may also present privacy, scalability, and reliability issues. In developing effective incident response mechanisms based on FML, it is necessary to analyze existing ways to use FML and its shortcomings, design solutions, and control the model's performance. In summary, the main outcomes of this research are as follows:

1) Automated detection: FML simplifies automated detection by tokenizing the data and matching it with a predefined pattern for the adversarial attack. Feature-based detection such as this, when used for anomaly detection, can quickly respond to unusual activities so they can be identified.
2) Extensive monitoring of activity: FML means the system is heavily monitored, collecting data from multiple distributed sections. It offers complete visibility into activity, as well as the ability to detect anomalies sooner.
3) Enhanced data security: One of the primary advantages of FML is that the system allows the secure sharing of data among distributed sources without being concerned by data leaks or unauthorized acquiescing issues. Ensuring the system data is more secure.
4) Decrease alse positives: One of the features of ML is that it can improve incident response time by seeking lost people anytime and reducing false favorable rates using FML techniques. It mitigates the likelihood of false positives, which can result in higher costs and wasted time.
5) Faster issue response time: The decrease in the time it takes to identify suspicious activity results in quicker response time to address the issue. This helps the system efficiently respond to and break down harmful intrusion.

2. Literature Review

Verma et al. [16] discussed a type of artificial intelligence (AI) based method used for cyber security. Industrial sector AI is designed to detect and block attacks on linked systems in the intelligent manufacturing space. It does this through ML algorithms that look over data orientated from various angles to try and identify anomalies and hacker issues. The data that this algorithm uses is shared in a secure, distributed environment without being copied and updated continuously. It can detect intrusions and malicious activities, notify the security team, and respond to them immediately. This kind of AI approach also serves the intelligent manufacturing sector to improve security and threat detection. A study has defined an intrusion detection system (IDS) with ML applied to improve detection performance and reduce false alarms [17]. Federal Intrusion Detection System (FIDS) combines unsupervised learning and supervised learning and ML algorithms. Unsupervised learning helps detect anomalies: once supervised learning creates a model from the normal behavior of the network, unsupervised learning is used to find abnormal patterns. This robust set of ML algorithms enables FIDS to catch a new attack that traditional IDS behavioral patterns might miss. The best approach is to implement an acquisition IDS solution. Agrawal et al. [18] explored the approaches to detect cyber-attacks on a set of computer systems with intermittent or delayed connection to some real-time (streaming) data presented. It will assign a weight to each node based on whatever data it has processed. These weights are applied as multipliers in a sum formula, representing an average consensus of the system or network's attack level. This allows main updates on the overall security level of the system, even if, for example, some of them are lagging due to their connection or hardware. Friha et al. [19] conducted research on industrial Internet of Things (IoT) networks. A federated, privacy-preserving IDS using differential privacy and Differential Federated Learning (DFL) is proposed by Friha et al. [19].

The system uses federated learning to create distributed intrusion detection models rather than relying on centralized or shared data. In addition, differentially, private algorithms de-noise the input and thereby minimize the risk of privacy leakage for all nodes, which is beneficial for the privacy of all nodes. This allows for finding assaults at extraordinary levels without compromising the confidentiality of any touchy facts. It would detect and prevent multiple threat categories in industrial IoT environments, such as SQL injection and brute force. Naeem et al. [20] proposed a federated learning framework to enhance static anomaly intrusion detection models. Building on active learning and semi-supervised learning concepts is the solution. The library employs federated learning techniques to alleviate privacy concerns associated with models and exploits semi-supervised learning to leverage the labeled data requirement. Traditional ML approaches generally perform benefits; thus, this framework can outperform by utilizing edge node data collected from hundreds of meters away. The advancement provides a high-level security architecture in ZSM networks, allowing them to get more accurate intrusion detections via federated learning.

Tabassum et al. [21] proposed a system that uses federated learning for a distributed AI-enabled method to detect malicious threats without compromising user privacy. Specifically, this system utilizes GANs to generate simulated realistic malicious traffic to train a central intrusion detection model via federated learning. A central model is trained using federated learning, improving the detection of malicious threats while maintaining the users' privacy. Abdul Rahman et al. [22] explored an emerging security technology that could detect suspicious or unwanted behavior within the created IoT in more general devices. It's a proactive approach to discovering malicious IoT devices and network behavior. It leverages multi-sensory-based data collection, in-depth data analysis, and ML, among various others, to discover potential threats. The purpose of intrusion detection is to ensure that no malicious or unintended activity goes unnoticed and that no attacks are detected or thwarted. Liu et al. [23] explored that blockchain-centric consensus decomposition and isolated execution engine for trustworthy decentralized computing describe a distributed digital ledger system that allows secure peer-to-peer transactions without a central authority. The automotive sector is one of the sectors in which it is used. Federated learning is a decentralized ML technique that only uploads the updated model from the user to the server, thus allowing collaborative prediction model building without revealing user data. This method is well suited for edge computing applications, enabling cars to train models in conjunction with each other and preserving data privacy. Federated learning for collaborative intrusion detection to jointly achieve federated learning and vehicular sharing models to recognize malicious behaviors using the context and data in vehicular edge computing. To do that, in this approach, it could exchange the model changes (weights, model parameters, etc.) safely. Making these updates available to cars may help these detection algorithms be more precise in detecting security risks in the future. Moreover, blockchain technology ensures that data is in an open space. As a result, anyone can trust it because they can communicate through the immutable channel of the shared ledger; thus, no one can tamper with it. Khan et al. [24] explored a more detailed analysis of blockchain-based approach and the application of decentralized ML methods in enabling Unmanned Aerial Vehicle (UAVs) to cooperate to sense and avoid threats, including cyber intrusions that can become air-based attacks. The system comprises shared data exchange mechanisms to allow the collaboration of UAVs equipped with neural networks to identify and classify detecting/labeled intrusions. The system also uses a blockchain approach to store detected intrusions for access to them in the future, with the ability to keep records of the actions of drones. This also validates the information gathered from multiple UAVs, stores it securely, and collaborates between UAVs. Markovic et al. [25] have proposed an effective security approach that combines shared learning with distributed data to detect and prevent these malicious acts. It models a random decision tree to classify data from multiple sources and applies a federated learning algorithm to integrate and analyze the data. This will help advance IDSs with enhanced accuracy and user data privacy.

An advanced level of ML was also discussed by Sun et al. [26] in the network security domain. This way, elasticity trains each ML model, based on different LANs, to learn and share that know-how independently without moving confidential data. The divided federated learning and large-scale multiple LAN architectures can make intrusion detection more accurate. In this way, training data can be distributed across many LANs, making the ML models learn from each other's data and more accurately improve the detection system. Nguyen et al. [27] introduced a possible attack by maliciously injecting data into the training set, with the implication of classifying the IoT traffic mistakenly. The effects of the attacks could be dire, causing an apparent attack or non-attack, creating an attack vector for a malicious exploit. Federated learning-based IoT IDS must follow a well-access control system and a well-defined privacy and security policy. Mosaiyebzadeh et al. [28] reported an AI-based distributed ML framework to detect anomalous and malignant behavior in an IoT ecosystem. It identifies security events and evaluates inter-IoT device communication and behavior through federated learning. The system helps identify malicious activities, ensure data security, and secure IoT infrastructure. Vadigi et al. [29] have proposed an ML model for detecting cyberattacks (intrusions). In this system, using the dynamic attention mechanism and federated learning, we can detect malicious data patterns and the behaviors of malefic data downstream on remote networks, which will help identify and prevent hidden malicious activities. Its main role is to use the usual or malicious pattern-based data classification using unsupervised or semi-supervised methods. The system also tags the bad data patterns, reducing the effort to detect them. Furthermore, the dynamic attention mechanism focuses on the critical data patterns rather than the whole data, making it easy for the system to analyze and detect malicious patterns effectively. Popoola et al. [30] proposed a sort of ML utilizing multiple individual networks to cooperate and communicate to enhance the efficacy of detection of cyber threats. Multiple networks are trained with the same deep learning model locally over different segments of data using a decentralized architecture. The federated deep learning process aggregates separately created models within the different networks, which can be used to enhance a single IDS. This partnership yields deeper context about cyber threats, enables early alerting of attacks, and affords security personnel even more avenues for response.

2.1. Research gaps

1) Lack of an Integrated System scale intrusion detection and simulation tool that is quantifies the impact of multiple attack types on intrusion detection performance and poor understanding of individual cyberattack phases and the effect each phase has on an organization's cyber security performance.
2) Insufficient knowledge of advanced stealthy attack methods and the number of events to which an IDS must respond (in real time) to accommodate new attack modes, as well as the requirements for knowledge of network traffic types and patterns needed to detect malicious events.
3) More studies are required with anomaly-based detection systems that can detect intrusions in real time and analyze full data traf-

fic patterns. However, network traffic complexity requires more work to reduce false-positive output.

4) Developing secure multi-tier architectures to ensure data integrity and security are not novel nor do they advocate cloud protection as part of that work. Then, the job is essentially the same as that of previous research, and it also tries to integrate intrusion detection as a large-scale big data processing.
5) The limited use of IDSs to analyze big data encourages the study and implementation of secure multi-tier architectures to ensure data integrity and security. Weak studies that amalgamate threat intelligence integrating OSINT and CTI with IDSs and no empirical survey on the AI and ML for the advancement of the intrusion detection models.
6) However, the federated learning gives privacy benefits, scaling over the complicated and massive network introduces huge threats, namely, the overhead and communication delay. Effective communication optimization between the server and client still remains a vital challenge.

2.2. Research objectives

1) To develop and implement an enhanced federated learning framework tailored for intrusion detection, enabling collaborative model training across multifarious network nodes while preserving confidential information privacy as well as reducing the centralized data storage space.
2) To assess as well as optimize the suggested model's performance to determine distinct types of cyber threats, focusing on enhancing the detection accuracy by improved ML algorithms and feature selection approaches.
3) To systematically validate the suggested federated learning-based intrusion detection framework with conventional centralized detection techniques, highlighting improvements in scalability, adaptability, and real-time responsiveness to evolving threats.
4) To evaluate the security implications as well as computational efficiency of the federated learning technique, confirming that the suggested framework not only identifies the intrusions effectively but also operates efficiently in resource-constrained settings.

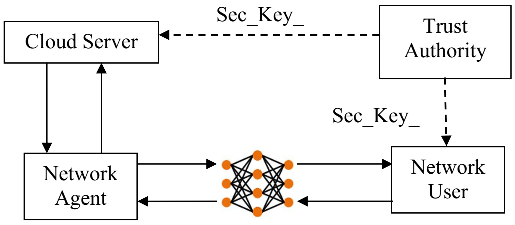
3. Research Methodology

FML is a concept of ML distributed via a network of agents that train multiple machines on their local datasets. FML can be used as a part of an intelligent cyber security model for intrusion detection to improve the system's security by training the models for anomaly and potential intrusion detection using the power of a distributed system (multiple computers). To use FML for this purpose, we first need to create a network of different machines. All these machines can be installed with a local machine-learning model, which should be able to learn from the data stored on the local machine. Suppose we train these local models on the data stored on each machine autonomously for known intrusions instead. In that case, the data each device saves can be capable of self-programming to detect known intrusions. Once we have implemented local models, the next step is to train federated models by combining all the local models to form a global one. This is where the genuinely global model is trained based on synthetic training data constructed by local models. When an attack is detected, the federated model can recognize a global anomaly in international data, leading to an alert in case of intrusion. One of the most valuable characteristics of FML, when used for intrusion detection, is that individual machines can benefit from the knowledge of all nodes in the system without sharing any dataset with them. It makes the system more secure as there is no data theft or manipulation risk. It also has the side effect of lowering the computation cost concerning training multiple models because only the federated model is trained.

3.1. System model

A system model for intelligent cyber security model for intrusion detection using FML is proposed. A distributed ML approach for providing an efficient and dependable IDS is vital. This approach cleverly integrates many ML algorithms to detect new threats or oddities. To allow unbiased training and prediction, it uses a federated structure that enables the sharing of multiple data fractions with multiple stakeholders to help the imperative need for federated analytics. Similarly, the model utilizes distributed training on multi-nodes, enhancing scalability and allowing accurate data prediction. It also uses a few other strategies, such as data fusion or anomaly detection, to improve the performance and accuracy of the model along with feature selection. Figure 1 expresses the model of the system.

Figure 1
Express the model of the system



This ML system employs the latest technology to detect and respond to hostile cyber activity and risks. It is designed to highlight potential vulnerabilities, flag anything that appears strange, and react swiftly and aggressively to any online attack. This technology could block networks from all kinds of hostile behaviors and be able to identify hidden cyber threats, which current security solutions would probably let pass. It can detect these things and take action against malicious or phishing, malware, or other illegal activities. The system can also provide real-time statistics, and it can monitor the performance of a network.

$$\frac{df}{de} = \frac{d}{de}\left(e^{e} * \sin Ef\right) \tag{1}$$

Let $E = e^{e}$ and $F = \sin Ef$; then we have the following:

$$G = E * F \tag{2}$$

Cloud Server: It is a cloud-native security solution that leverages automation and accuracy in detection using intelligence based on sophisticated analytics to detect and alert for threats or malicious activities in the IT network. It fuses AI, ML, and analytics on user and entity behavior to detect network threats, such as self-installing malware, malicious insiders, and external adversaries. It can automatically react to find and remove threats within seconds, such as blocking more entries or sending out a malware alert. Moreover, it can be integrated into existing security systems over an open-architecture platform so that organizations can react and coordinate faster, with all the events correlated in real time.

$$\frac{df}{de} = \left(E * \frac{dF}{de}\right) + \left(F * \frac{dE}{de}\right) \tag{3}$$

$$\frac{df}{de} = \left(e^{e} * \frac{d}{\mathrm{de}} \sin Ef\right) + \left(\sin Ef * \frac{d}{de}\left(e^{e}\right)\right) \tag{4}$$

$$\frac{df}{de} = \left(E * e^{e} \ \cos Ef\right) + \left(e^{e} \ \sin Ef\right) \tag{5}$$

Here, the active sink node comes at the fifth place, and the active source node arrives at the eighth place. It involves setting up a software application known as a "network agent" on computer networks to detect and respond to potential invasions. They detect cyber threats. The decision by admin from revenue companies to promptly identify and do away with the unwelcome task on their computer networks. It helps protect the data, the network, and the enterprise as a whole.

3.2. Threat model

These are essential components in a threat model for intelligent cyber security for intrusion detection:

Network mapping: Discovering the active devices on the network and generating a device-wise relationships map.

Anomaly detection: Discovering well-behaved and observing misbehaved usage patterns, thus defining good behavior and alerting when significant deviations have been detected.

Profile attacks: Incorporating profile attacks where actions from your environment are run against targets using real-world operational technologies.

Safe listing and deny listing: Allow lists and block lists to establish a compliance posture and detect malicious activities.

User and entity behavior analytics: ML algorithms process all the activity and perform advanced analysis of user and entity behavior for more precise detection of suspicious activities.

Access controls: Monitoring and limiting permitted user access to information and resources and ensuring unauthorized users are not exempt from controls that prevent access.

Security monitoring: Sending logs of activities and events to monitoring and alerting systems to detect the presence of organized attacks.

Intrusion detection: Detecting suspicious activities using behavioral analytics, rule-based logic, and ML models.

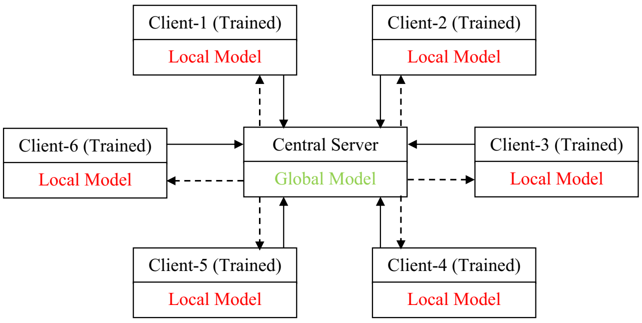
Patch management: Provide regular technology patching and updates on environmental security. Using a threat model for intelligent cyber security for intrusion detection helps identify and examine the potential threats reduced by malicious actors and attack vectors, including malicious software, unauthorized access, data infiltration, identity theft, and other harmful activities.

Furthermore, it helps businesses understand cyber security threats and potential weaknesses in their frameworks, technologies, and network architecture. Using a threat model, a company can minimize the probability of a successful attack and take a strategic approach to its security budget.

3.3. Proposed model

In this paper, we propose a novel iCyber system, which employs the concept of FML to design an intelligent cyber security system for intrusion detection. In the conventional model, data is collected from distributed organizations (i.e., in enterprise networks and cloud environments) and sent to an FML-based framework that conducts the analysis (detects cyber threats). The performance in the model processes data in a similar pattern to the distributed learning method and enables secure data sharing so that individual user privacy is maintained. Because it processes data from multiple sources, the FML model can catch suspicious activity and respond to it before it is too late simply because it has more than one vantage point. The AI-based threat detection system can also gain from past incidents, which results in detection that would even decrease the probability of figuring out unknown threats. The block diagram shown in Figure 2 depicts the proposed system.

Figure 2
Proposed block diagram



The Global Model Central Server manages and distributes global knowledge and information about security threats across all deployed detection models.

$$G = e(f) = g^{e} \tag{6}$$

The Global Model Central Server tracks and monitors global threat events from various sources, such as external threat intelligence databases and industry reports.

$$f'' = \lim_{e \to 0} \left(\frac{g(e+f) - g(e)}{f}\right) \tag{7}$$

This data is then used to update the real-time security models distributed throughout the network. It allows the detection models to more accurately identify and respond to security events and threats.

$$f'' = \lim_{e \to 0} \left(\frac{g^{e+f} - g^{e}}{f}\right) \tag{8}$$

$$f'' = \lim_{e \to 0} \left(\frac{\left(g^{e} * g^{f}\right) - g^{e}}{f}\right) \tag{9}$$

A local model (trained) is a software tool for training an ML model on local data. It allows organizations to develop a model specific to their use case and environment.

$$f'' = \lim_{e \to 0} \left(\frac{g^{e} * \left(g^{f} - 1\right)}{f}\right) \tag{10}$$

$$f'' = g^{e} * \lim_{e \to 0} \left(\frac{\left(g^{f} - 1\right)}{f}\right) \tag{11}$$

$$f'' = g^{e} * \ln(g) \tag{12}$$

The tool provides a convenient way to train the models since the local data is already available and labeled. It allows companies to easily tailor their models to the characteristics of their data and attack vectors.

3.3.1. Preprocessing

Preprocessing in the context of an intelligent cyber security model for intrusion detection using FML refers to the first stage of building an automated system to detect intrusions.

$$\left(\frac{E * E_e}{F_e}\right) = \frac{1}{2}E * f_e^2 \tag{13}$$

This process is fundamental, ensuring that data for detecting intrusions and other anomalous activity is appropriately formatted, cleaned, and structured for maximum input.

$$f_e^2 = \left(\frac{E * E_e}{F_e}\right) * \frac{2}{E} \tag{14}$$

It includes tasks such as normalizing data, eliminating duplicates, removing outliers, and transforming raw data into the desired shape and form to be more effectively utilized within the system's FML algorithm.

$$f_e^2 = \left(\frac{2 * E_e}{F_e}\right) * \frac{2}{E} \tag{15}$$

where, $g = \left(\frac{E_e}{F_e^2}\right)$;

Additionally, preprocessing determines which features are meaningful and which should be discarded, as well as what data is considered irrelevant to the task and what should be kept.

$$f_e^2 = 2 * f * F_e \tag{16}$$

$$f_e = \sqrt{2 * f * F_e} \tag{17}$$

The successful implementation of preprocessing ensures that the system can be consistently effective and receives input in a standardized format and that accuracy does not suffer due to too noisy or irrelevant data.

3.3.2. Feature extraction

Feature extraction is an essential step in the intelligent cyber security model for intrusion detection using FML.

$$g'(e) = \lim_{f \to 0}\left(\frac{g(e+f) - g(e)}{f}\right) \tag{18}$$

$$g'(e) = \lim_{f \to 0}\left(\frac{g^{e+f} - g^{e}}{f}\right) \tag{19}$$

The process of taking useful information out of a data collection and putting it in a format that can be utilized to train a model is called feature extraction. Accurately detecting, categorizing, and mitigating intrusions requires this procedure.

$$g'(e) = \lim_{f \to 0}\left(\frac{\left(g^{e} * g^{f}\right) - g^{e}}{f}\right) \tag{20}$$

$$g''(e) = e^{e} * \lim_{f \to 0}\left(\frac{\left(1 - e^{f}\right)}{f}\right) \tag{21}$$

Using pertinent aspects from the dataset, feature extraction helps identify important intrusions. The retrieved characteristics aid in the development of a successful intrusion detection and classification model. It guarantees that the FML-based intelligent cyber security model for intrusion detection is effective.

3.3.3. Attack detection

Attack detection in an intelligent cyber security model for intrusion detection using FML is a system-level approach to detect malicious activities within a federated network.

$$f = e^{e} - 1 \tag{22}$$

$$e^{e} = f + 1 \tag{23}$$

$$e = \ln(f + 1) \tag{24}$$

It combines ML, distributed processing, and data analysis techniques to detect security threats and anomalous activities.

As, $e \to 0 \;=>\; f \to 0$

$$g''(e) = e^{e} * \lim_{f \to 0}\frac{f}{\ln(f + 1)} \tag{25}$$

$$g''(e) = e^{e} * \lim_{f \to 0}\frac{f}{\frac{1}{f}\ln(f + 1)} \tag{26}$$

The objective is to user activity using distributed terminals to detect harmful actions using AI and distributed learning techniques.

$$g''(e) = e^{e} * \lim_{f \to 0}\frac{f}{\ln(f + 1)^{\frac{1}{f}}} \tag{27}$$

The distributed terminals work as a network, pushing collected data to the central server for analysis.

$$g''(e) = e^{e} * \frac{1}{\ln \lim_{e \to 0}(f + 1)^{\frac{1}{f}}} \tag{28}$$

The attacks will be detected through the ML algorithms, which will identify patterns and relationships among the collected data for better data security.

$$g''(e) = e^{e} * \frac{1}{\ln f} \tag{29}$$

Once detection is successful, the appropriate reaction will be taken to contain the threat and protect the system from future attacks.

3.3.4. Attack classification

An intelligent cyber security model for FML-based intrusion detection must include attack classification. The model's ability to precisely recognize and classify hostile behavior, such as intrusion attempts or malicious software, is made possible by attack classification.

$$E_1 = -F + \sum_{g=1} H_g = 0 => \frac{\partial E_1}{\partial F_g} = 1 \tag{30}$$

$$E_2 = F + \sum_{g=1} \beta_g * H_g = 0 => \frac{\partial E_2}{\partial F_g} = 1 \tag{31}$$

This component works using a combination of features such as behavioral analysis, packet header analysis, payload analysis, and other heuristics. Attack classification also enables the model to identify the malicious source, which may be used to determine the correct countermeasures or further investigate the attack.

$$\frac{\partial \ln(\sigma_d)}{\partial F_g} + \delta_1 * \frac{\partial E_1}{\partial F_g} + \delta_2 * \frac{\partial E_2}{\partial F_g} = 0 \tag{32}$$

$$\ln(H_g) - \ln(F_g) + \delta_1 - \delta_2 \sigma_g = 0 \tag{33}$$

The attack classification helps the security team better understand the threat's severity and scope. The classification can often be used to develop better detection strategies and accuracy of the model.

3.4. Proposed framework

The proposed framework is a more sophisticated system developed to detect and analyze malicious network traffic in real time. Using a range of techniques from anomaly-based detection and signature-based detection to ML algorithms. Focus point is designed to catch known and virtually unknown attacks, weakening the ability of a malicious hacker to work his way around prevention techniques. Automated responses also enable an immediate response for users to defend against an attack and work without hindrance to their network.

Data collection: The data is collected from various sources, including operating systems, applications, network devices, internet backbone, and user activity logs.

Preprocessing: The data is collected and then preprocessed to remove redundant or false data for better accurate results. The features can be frequency, intensity, duration, and many other attributes. To further strengthen the reliability of our study results, we have conducted an extensive preprocessing phase for cleaning and normalization of the data before feeding it into the federated learning model. This involved removing duplicates, handling missing values, and balancing the dataset to prevent any biases during training. We also performed cross-validation using K-fold cross-validation wherein the value of K is considered 10, to ensure that the model's performance metrics are not overly dependent on a particular subset of the data, thus increasing the robustness of our findings.

Abstract feature extraction: In this step, the features are extracted from data in various ways.

Model creation: Here, the features are applied to create a classifier model. This model of the classifier will identify the kind of malicious activities.

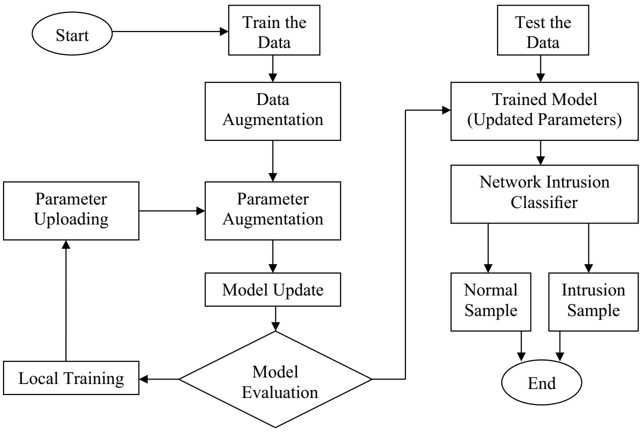
Anomaly detection: In this step, the system will learn to recognize any anomalies that may highlight malicious behavior.

Alerts: Once such activity is discovered, an alert will be triggered to inform your security staff to take action.

Assessment: This task measures how well the intrusion detection framework can identify intrusion activities.

These methods are considered to accurately detect the nature of the network malware as malicious activity. They automatically perform actions such as blocking the attack to prevent it from causing any damage. It also enables post-incident forensics, useful in a follow-up analysis for better incident response. Figure 3 shows flow of the proposed framework. The proposed framework contains many functionalities to identify and stop the intrusion. The model first builds an FML-based anomaly detection system. The model also employs an AI-driven cognitive monitoring system for oversight and action on suspicious activity items. This system can detect patterns in the activity of specific users and anomalies in user behavior to identify whether or not someone is trying to access the system without permission beginning with an automated, rule-based detection implemented on the model that can automatically identify known cyber threats and attacks based on a library of attack signatures. Together, these features give us deep security around cyberattack detection and handling.

Figure 3
Proposed flow diagram



4. Results and Discussion

4.1. Comparative analysis

The proposed Intelligent Cyber Security Model (ICSM) has been compared with the existing federated deep learning (FDL), federated learning aided long short-term memory (FLSTM), FML, and Fairness Federated Deep Learning Approach (FFDLA). Here, python is a simulation tool used to execute the results with the Network Intrusion Detection dataset. This proposed model has been implemented on the computer system integrated with the following settings: Processor: Intel 2.40GHz, 64 GB RAM, NVIDIA Tesla V100 GPU, 2 TB storage, and OS Ubuntu 20.04 LTS, TensorFlow Federated 0.18. Furthermore, the learning rate was set to 0.1, the decay rate was 0.8, and dropout was 0.2 for the elimination of overfitting.

4.2. Computation of accuracy

Accuracy measures how consistently and correctly the intelligent cyber security framework can detect an intrusion. Typically, the calculation involves dividing the total number of instances (all positives and all negatives) by the ratio of correctly classified cases (true positives and true negatives). Stated differently, it refers to the proportion of incursions or attacks that the system accurately detects. Since it can show how many attacks are missed or result in false negatives, it is an essential indicator of an IDS's performance. The accuracy performance comparison is displayed in Table 1 [31]. The accuracy of the proposed ICSM framework over the number of inputs 400 is obtained at 94.16%, while the existing method [31] obtains an accuracy level of 80.13%. Hence, it is evident from the comparative analysis of proposed and existing methods, that the proposed framework is more robust and provides improved accuracy performance.

Table 1
Comparative analysis of proposed and existing model in terms of accuracy (in %)

No. of inputs	FDL	FLSTM	FML	FFDLA	ICSM
100	63.12	65.78	67.07	75.53	91.29
200	62.79	64.28	66.48	73.66	92.28
300	61.45	63.17	65.50	72.83	93.12
400	60.31	62.79	64.29	71.92	94.16
500	59.26	61.78	63.15	71.00	95.59
600	58.55	60.85	62.04	69.67	97.39
700	57.25	59.85	61.34	68.80	98.24

Figure 4 shows the computation of accuracy. In a computation cycle, the existing FDL reached 60.31%, FLSTM reached 62.79%, FML reached 64.29%, and FFDLA reached 71.92% accuracy. The proposed ICSM obtained 94.16% accuracy.

4.3. Computation of precision

An algorithm's precision in detecting an intrusion is measured by the intelligent cyber security framework's IDS. The true positives are divided by the total of the true and false positives to compute it. It's employed to gauge how well the framework detects intrusions while avoiding raising false warnings. Precision's performance comparison is displayed in Table 2.

Table 2
Comparison of precision (in %)

No. of inputs	FDL	FLSTM	FML	FFDLA	ICSM
100	72.42	62.28	76.90	86.88	94.63
200	72.75	63.78	77.49	88.75	95.67
300	74.09	64.89	78.47	89.58	95.80
400	75.23	65.27	79.68	90.49	96.76
500	76.28	66.28	80.82	91.41	96.33
600	76.99	67.21	81.93	92.74	97.57
700	78.29	68.21	82.63	93.61	97.68

The precision computation is displayed in Figure 5. The current FDL achieved 75.23%, FLSTM 65.27%, FML 79.68%, and FFDLA 90.49% precision in a computing cycle. 96.76% precision was attained by the suggested ICSM.

4.4. Computation of recall

Remember that the accuracy of the system's capacity to identify attacks or malicious activities is a component of an intelligent cyber security framework in intrusion detection. It divides the total number of accurate positive attacks by the number of real positive attacks that were found. Stated differently, recall is the proportion of positives that the system correctly detects out of all the data points that could be attacked.

For example, if there are a total of 100 attacks in the dataset and 90 of them are correctly identified by the system, then the recall rate is 90%. It is important to note that recall is independent

Figure 4
Measured accuracy of the proposed framework

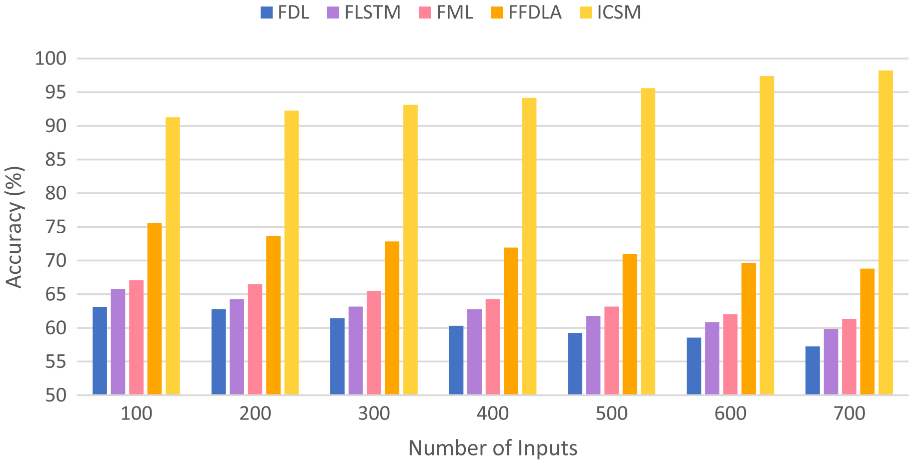
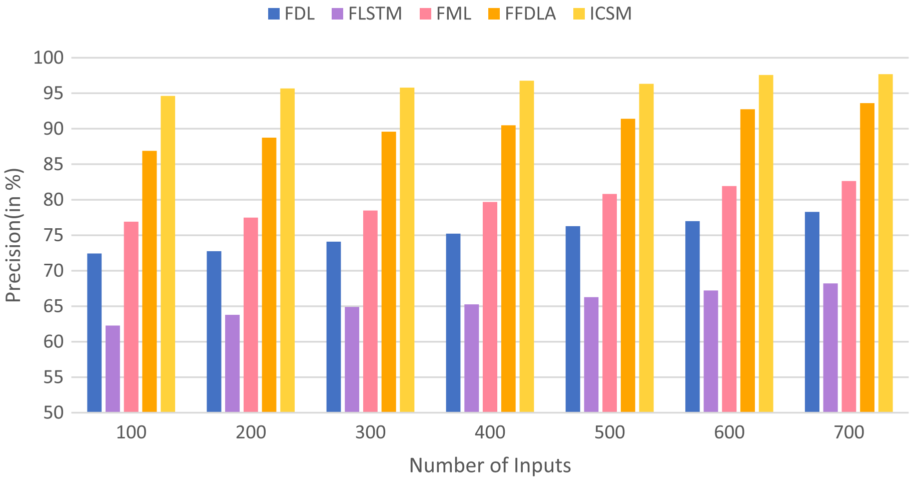


Figure 5
Measured precision value of the system



of false positives that may be produced as long as all true positives are detected. Table 3 shows the performance comparison of recall.

Table 3
Comparison of recall (in %)

No. of inputs	FDL	FLSTM	FML	FFDLA	ICSM
100	64.16	75.82	71.23	81.23	96.46
200	62.53	74.08	69.65	79.81	95.17
300	62.05	71.74	67.45	78.55	94.16
400	60.76	70.93	65.82	76.56	93.27
500	58.65	68.64	64.68	74.09	92.90
600	57.16	66.71	62.48	72.65	92.26
700	55.35	64.98	61.33	70.93	91.89

The computation of recall is shown in Figure 6. The current FDL achieved 60.76%, FLSTM reached 70.93%, FML reached 65.82%, and FFDLA reached 76.56% recall in a computation cycle. The projected ICSM has a recall rate of 93.27%.

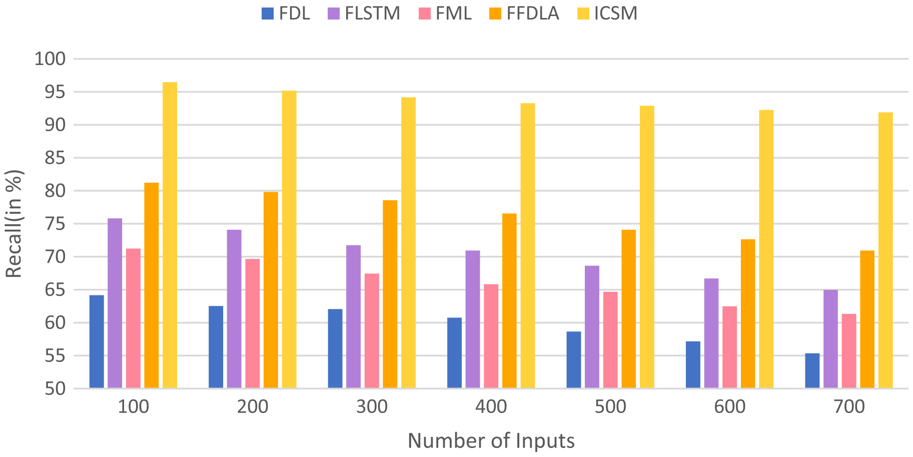
4.5. Computation of F1 score

A performance metric for binary classifiers that assesses a model's recall and precision is called the F1 score, sometimes known as the F-measure. It is computed as the harmonic mean of precision and recall, taking into account both erroneous positives and false negatives.

The precision of the model is calculated by dividing the total number of true positives by the total number of false positives. The model's recall is calculated by dividing the total number of true positives by the total number of false negatives and true positives.

The scores for each would be used to gauge the effectiveness of the IDS when utilizing the F1 score for an intelligent cyber security framework in intrusion detection. The system might have a high recall rate, which means it has successfully identified false negatives, and a high precision rate, which means it has correctly

Figure 6
Measured recall of the system



identified real positive intrusions. The total performance of the system would then be determined by taking the harmonic mean of these two ratings, which is known as the F1 score. The F1 score performance comparison is displayed in Table 4.

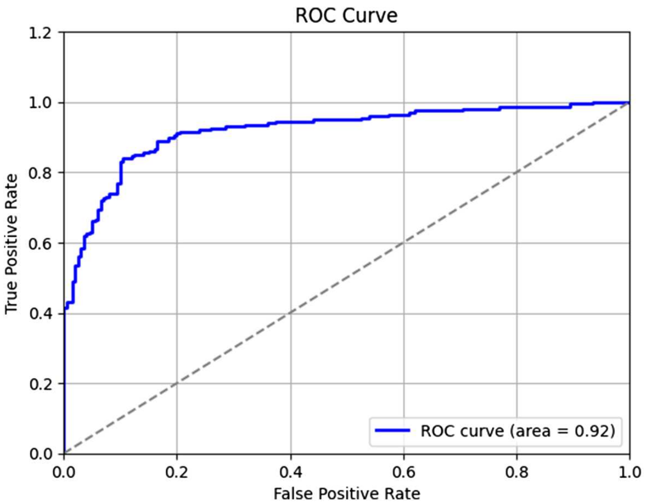
Table 4
Comparison of F1 score (in %)

No. of inputs	FDL	FLSTM	FML	FFDLA	ICSM
100	61.01	66.22	75.04	75.82	91.69
200	61.34	67.72	75.63	77.69	92.73
300	62.68	68.83	76.61	78.52	92.86
400	63.82	69.21	77.82	79.43	93.82
500	64.87	70.22	78.96	80.35	93.39
600	65.58	71.15	80.07	81.68	95.63
700	66.88	72.15	80.77	82.55	95.74

We have prolonged the proposed model performance analysis by incorporating the AUC-ROC curve analysis. This metrics assessment offers a detailed understanding of the suggested model's performance, particularly in the context of classification challenges, namely, the intrusion identification. Unlike distinct metrics that focused solely on a specified aspect of classification (for instance, precision for false positives as well as recall for true positives), the AUC-ROC curve effectively evaluates the model's capability to distinguish among the classes across all threshold levels. By evaluating both the true positive rate (sensitivity) as well as the false positive rate, the AUC-ROC metric gives a balanced overview of the suggested model's trade-offs, making it a noteworthy addition to the comparative analysis. This model analysis strengthens the complete evaluation of the suggested model as well as justifies its effectiveness for real-world applications. Figure 7 illustrates the proposed model ROC curve matrix.

The F1 score computation is displayed in Figure 8. The current FDL scored 63.82%, FLSTM scored 69.21%, FML scored 77.82%, and FFDLA scored 79.43% F1 score in a computation cycle. The suggested ICSM received an F1 score of 93.82%. Because intelligent cyber security systems are highly flexible and reactive to harmful activity, intrusion detection benefits from their use. These frameworks can identify malicious behavior, analyze patterns, and react swiftly to security concerns since they are built on AI and ML technology. Better defense against more sophisticated threats and zero-day attacks is provided by this cyber security framework. They are also capable of seeing unusual activity and sounding an alarm when they come across anything questionable. It can be used to strengthen the organization's security over time as well as assist in promptly responding to any possible assault. The following are a few of the suggested framework's shortcomings:

Figure 7
The proposed model ROC curve matrix



1) False positives: The algorithms used in an intelligent IDS can mistakenly raise an alarm if they recognize a pattern similar to a malicious attack, although the activity is harmless. This process is known as a false positive.
2) Require specific training: To design a practical cyber security framework, the developer must deeply understand the different types of malicious attacks, the technology, and the security protocols used by the cyber landscape.
3) Resource consumption: A component of an intelligent cyber security framework is resource consumption, which can impact its performance due to the extensive data analysis and processing.
4) Not always up to date with new threats: New digital threats and attack patterns are constantly evolving, which means that an intelligent cyber security framework may only sometimes be up to date with new sophisticated threat patterns.
5) Difficult to deploy and manage: The entire mechanism of deploying and managing an intelligent cyber security framework can be difficult and time-consuming for a more minor or even more extensive organization if it needs the proper infrastructure and data analytics team.

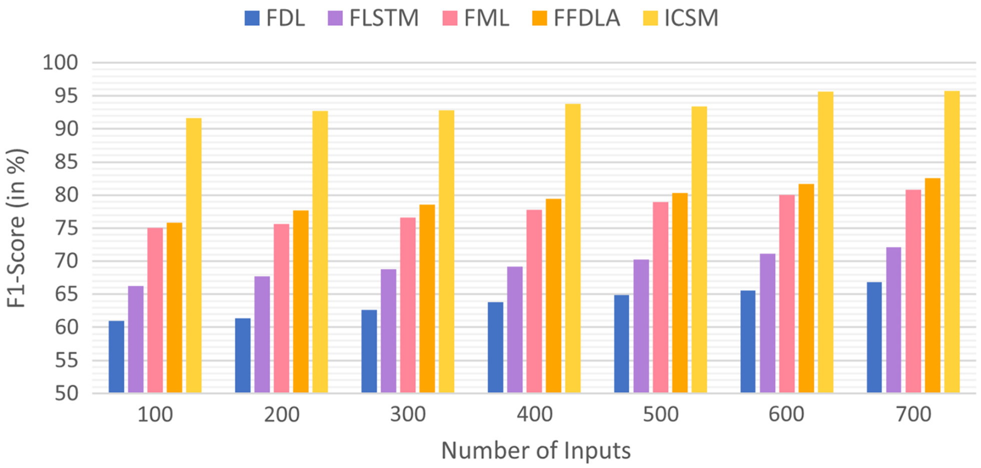
In our study, several confounding variables could potentially affect the results. We have identified confounding variables such as bias and data distribution to improve the overall model training.

The variation in computational power and network conditions across different clients can influence the training process. Clients with lower computational resources may struggle to contribute effectively to the global model, which could bias the results. To mitigate this, we implemented techniques, namely, asynchronous updates, and tested the impact of different client configurations on the overall performance.

The choice of model architecture and training algorithms can introduce biases. We have taken care to select the proposed model architecture that is generalizable across different types of data and have applied regularization techniques to minimize overfitting considering the dropout of 0.2. Additionally, we have employed cross-validation to assess the robustness of our model across different subsets of the data. The entire dataset is split into two categories: train set and test set into the 80:20 ratio. This data partition is done by K-fold cross-validation, wherein K is considered 10.

In federated learning systems, communication among the distributed clients as well as the central server may lead to significant overhead in real time. This is particularly true in large-scale networks where clients are geographically dispersed and may have altered network bandwidths. Frequent communication rounds, required for model updates and aggregation, can cause delays, increase latency, and strain network resources. To resolve these issues, the ICSM model is implemented, which is more robust in multifarious settings such as trade-offs, maintaining the

Figure 8
Measured F1 score of the proposed system



communication and model convergence and improving the overall performance of the model.

5. Conclusion

The intelligent cyber security framework for intrusion detection is that implementing such a system can provide essential defense against malicious attacks. By integrating different technologies and innovative approaches, an intelligent cyber security framework can detect anomalies in data communication, create alerts, and take action when malicious activities are detected. These measures can help minimize security threats and protect data from loss, unapproved entry, and modification. 94.16% accuracy, 96.76% precision, 93.27% recall, and 93.82% F1 score were attained by the suggested model. The creation of a powerful system that can instantly recognize and stop harmful network activity is the eventual goal of an intelligent cyber security framework for intrusion detection. To find anomalies in network activity, an IDS of this kind might include data mining, ML, and AI. Malicious activity including malware infections, ransomware assaults, and unwanted network access could be identified and stopped by it. The system should also be able to recognize harmful files, actions, and websites and notify users and system administrators of these risks. An intelligent cyber security framework for intrusion detection is required to keep up with evolving malware trends and guarantee network security as the sophistication of cyberattacks rises.

The proposed cyber security model using FML introduces significant practical benefits, especially in enhancing network security and maintaining data privacy. By leveraging decentralized learning, this model enables multiple organizations or nodes to collaboratively train a robust IDS without sharing sensitive data. Moreover, the model improves real-time detection capabilities by enabling continuous updates across distributed networks without compromising the secrecy of individual nodes. This decentralization also eliminates the risk of single-point failures, which is a common vulnerability in conventional centralized IDS models.

In terms of future applications, this model has the potential to revolutionize cyber security in distinct domains. For instance, it can be used in smart city infrastructures to protect connected systems, such as traffic control, power grids, and public safety networks, from cyberattacks. Similarly, in the context of the IoT, where billions of devices are interconnected, the FML method can aid in building more resilient and adaptive IDSs that can protect against increasingly sophisticated threats without exposing private data.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

The Network Intrusion Detection data that supports the findings of this study are openly available at https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection.

Author Contribution Statement

Mahantesh Laddi: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization. **Shridhar Allagi:** Validation, Resources, Writing – review & editing, Supervision, Project administration. **Rashmi Rachh:** Supervision. **Kuldeep Sambrekar:** Project administration. **Shrikant Athanikar:** Visualization.

References

[1] Li, B., Wu, Y., Song, J., Lu, R., Li, T., & Zhao, L. (2021). DeepFed: Federated deep learning for intrusion detection in industrial cyber-physical systems. *IEEE Transactions on Industrial Informatics, 17*(8), 5615–5624. https://doi.org/10.1109/TII.2020.3023430

[2] Zhao, R., Yin, Y., Shi, Y., & Xue, Z. (2020). Intelligent intrusion detection based on federated learning aided long short-term

memory. *Physical Communication, 42,* 101157. https://doi.org/10.1016/j.phycom.2020.101157

[3] Sanal Kumar, K. P., Nair, S. A. H., Guha Roy, D., Rajalingam, B., & Kumar, R. S. (2021). Security and privacy-aware artificial Intrusion Detection System using federated machine learning. *Computers & Electrical Engineering, 96,* 107440. http://dx.doi.org/10.1016/j.compeleceng.2021.107440

[4] Li, J. (2018). Cyber security meets artificial intelligence: A survey. *Frontiers of Information Technology & Electronic Engineering, 19*(12), 1462–1474. https://doi.org/10.1631/FITEE.1800573

[5] Cui, J., Sun, H., Zhong, H., Zhang, J., Wei, L., Bolodurina, I., & He, D. (2023). Collaborative intrusion detection system for SDVN: A fairness federated deep learning approach. *IEEE Transactions on Parallel and Distributed Systems, 34*(9), 2512–2528. https://doi.org/10.1109/TPDS.2023.3290650

[6] Friha, O., Ferrag, M. A., Shu, L., Maglaras, L., Choo, K. K. R., & Nafaa, M. (2022). FELIDS: Federated learning-based intrusion detection system for agricultural Internet of Things. *Journal of Parallel and Distributed Computing, 165,* 17–31. https://doi.org/10.1016/j.jpdc.2022.03.003

[7] Abdel-Basset, M., Moustafa, N., Hawash, H., Razzak, I., Sallam, K. M., & Elkomy, O. M. (2022). Federated intrusion detection in blockchain-based smart transportation systems. *IEEE Transactions on Intelligent Transportation Systems, 23*(3), 2523–2537. https://doi.org/10.1109/TITS.2021.3119968

[8] Sarhan, M., Layeghy, S., Moustafa, N., & Portmann, M. (2023). Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. *Journal of Network and Systems Management, 31*(1), 3. https://doi.org/10.1007/s10922-022-09691-3

[9] Logeshwaran, J., Shanmugasundaram, N., & Lloret, J. (2023). L-RUBI: An efficient load-based resource utilization algorithm for bi-partite scatternet in wireless personal area networks. *International Journal of Communication Systems, 36*(6), e5439. https://doi.org/10.1002/dac.5439

[10] Attota, D. C., Mothukuri, V., Parizi, R. M., & Pouriyeh, S. (2021). An ensemble multi-view federated learning intrusion detection for IoT. *IEEE Access, 9,* 117734–117745. https://doi.org/10.1109/ACCESS.2021.3107337

[11] Sarhan, M., Lo, W. W., Layeghy, S., & Portmann, M. (2022). HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection. *Computers and Electrical Engineering, 103,* 108379. https://doi.org/10.1016/j.compeleceng.2022.108379

[12] Liu, W., Xu, X., Wu, L., Qi, L., Jolfaei, A., Ding, W., & Khosravi, M. R. (2023). Intrusion detection for maritime transportation systems with batch federated aggregation. *IEEE Transactions on Intelligent Transportation Systems, 24*(2), 2503–2514. https://doi.org/10.1109/TITS.2022.3181436

[13] Ferrag, M. A., Friha, O., Maglaras, L., Janicke, H., & Shu, L. (2021). Federated deep learning for cyber security in the Internet of Things: Concepts, applications, and experimental analysis. *IEEE Access, 9,* 138509–138542. https://doi.org/10.1109/ACCESS.2021.3118642

[14] Chatterjee, S., & Hanawal, M. K. (2022). Federated learning for intrusion detection in IoT security: A hybrid ensemble approach. *International Journal of Internet of Things and Cyber-Assurance, 2*(1), 62–86. https://doi.org/10.1504/IJITCA.2022.124372

[15] Logeshwaran, J., Shanmugasundaram, N., & Lloret, J. (2023). Energy-efficient resource allocation model for device-to-device communication in 5G wireless personal area networks. *International Journal of Communication Systems, 36*(13), e5524. https://doi.org/10.1002/dac.5524

[16] Verma, P., Breslin, J. G., & O'Shea, D. (2022). FLDID: Federated learning enabled deep intrusion detection in smart manufacturing industries. *Sensors, 22*(22), 8974. https://doi.org/10.3390/s22228974

[17] Aouedi, O., & Piamrat, K. (2023). F-BIDS: Federated-Blending based Intrusion Detection System. *Pervasive and Mobile Computing, 89,* 101750. https://doi.org/10.1016/j.pmcj.2023.101750

[18] Agrawal, S., Chowdhuri, A., Sarkar, S., Selvanambi, R., & Gadekallu, T. R. (2021). Temporal weighted averaging for asynchronous federated intrusion detection systems. *Computational Intelligence and Neuroscience, 2021*(1), 5844728. https://doi.org/10.1155/2021/5844728

[19] Friha, O., Ferrag, M. A., Benbouzid, M., Berghout, T., Kantarci, B., & Choo, K. K. R. (2023). 2DF-IDS: Decentralized and differentially private federated learning-based intrusion detection system for industrial IoT. *Computers & Security, 127,* 103097. https://doi.org/10.1016/j.cose.2023.103097

[20] Naeem, F., Ali, M., & Kaddoum, G. (2023). Federated-learning-empowered semi-supervised active learning framework for intrusion detection in ZSM. *IEEE Communications Magazine, 61*(2), 88–94. http://dx.doi.org/10.1109/MCOM.001.2200533

[21] Tabassum, A., Erbad, A., Lebda, W., Mohamed, A., & Guizani, M. (2022). FEDGAN-IDS: Privacy-preserving IDS using GAN and Federated Learning. *Computer Communications, 192,* 299–310. https://doi.org/10.1016/j.comcom.2022.06.015

[22] Abdul Rahman, S., Tout, H., Talhi, C., & Mourad, A. (2020). Internet of Things intrusion detection: Centralized, on-device, or federated learning? *IEEE Network, 34*(6), 310–317. https://doi.org/10.1109/MNET.011.2000286

[23] Liu, H., Zhang, S., Zhang, P., Zhou, X., Shao, X., Pu, G., & Zhang, Y. (2021). Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing. *IEEE Transactions on Vehicular Technology, 70*(6), 6073–6084. https://doi.org/10.1109/TVT.2021.3076780

[24] Khan, A. A., Khan, M. M., Khan, K. M., Arshad, J., & Ahmad, F. (2021). A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs. *Computer Networks, 196,* 108217. https://doi.org/10.1016/j.comnet.2021.108217

[25] Markovic, T., Leon, M., Buffoni, D., & Punnekkat, S. (2022). Random forest based on federated learning for intrusion detection. In *Artificial Intelligence Applications and Innovations: 18th IFIP WG 12.5 International Conference,* 132–144. https://doi.org/10.1007/978-3-031-08333-4_11

[26] Sun, Y., Ochiai, H., & Esaki, H. (2020). Intrusion detection with segmented federated learning for large-scale multiple LANs. In *2020 International Joint Conference on Neural Networks,* 1–8. https://doi.org/10.1109/IJCNN48605.2020.9207094

[27] Nguyen, T. D., Rieger, P., Miettinen, M., & Sadeghi, A. R. (2020). Poisoning attacks on federated learning-based IoT intrusion detection system. In *Workshop on Decentralized IoT Systems and Security,* 1–7. https://dx.doi.org/10.14722/diss.2020.23003

[28] Mosaiyebzadeh, F., Pouriyeh, S., Parizi, R. M., Han, M., & Macêdo Batista, D. (2023). Intrusion Detection System

for IoHT devices using federated learning. In *IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops,* 1–6. https://doi.org/10.1109/INFOCOMWKSHPS57453.2023.10225932

[29] Vadigi, S., Sethi, K., Mohanty, D., Das, S. P., & Bera, P. (2023). Federated reinforcement learning based Intrusion Detection System using dynamic attention mechanism. *Journal of Information Security and Applications, 78,* 103608. https://doi.org/10.1016/j.jisa.2023.103608

[30] Popoola, S. I., Gui, G., Adebisi, B., Hammoudeh, M., & Gacanin, H. (2021). Federated Deep Learning for collaborative intrusion detection in heterogeneous networks. In *2021 IEEE 94th Vehicular Technology Conference,* 1–6. https://doi.org/10.1109/VTC2021-Fall52928.2021.9625505

[31] Kelli, V., Argyriou, V., Lagkas, T., Fragulis, G., Grigoriou, E., & Sarigiannidis, P. (2021). IDS for industrial applications: A federated learning approach with active personalization. *Sensors, 21*(20), 6743. https://doi.org/10.3390/s21206743

How to Cite: Laddi, M., Allagi, S., Rachh, R., Sambrekar, K., & Athanikar, S. (2025). An Advanced Cyber Security Model Using Federated Machine Learning Approach for Intrusion Detection in Networks. *Journal of Computational and Cognitive Engineering*, *4*(2), 223–235. https://doi.org/10.47852/bonviewJCCE42023751