A Hybrid Federated Learning Framework and Multi-Party Communication for Cyber-Security Analysis

Fahad Alqurashi
Computer Science Department-Faculty of Computing and Information Technology,
King Abdulaziz University, Jeddah 21589, Saudi Arabia

***Abstract*—The term "Internet of Things" (IoT) describes a global system of electronically linked devices and sensors capable of two-way communication and data sharing. IoT provides various advantages, including improved efficiency and production and lower operating expenses. Concern about data breaches is constantly present, for example, since devices with sensors capture and send confidential data that might have dire effects if leaked. Hence, this research proposed a novel hybrid federated learning framework with multi-party communication (FLbMPC) to address the cyber-security challenges. The proposed approach comprises four phases: data collection and standardization, model training, data aggregation, and attack detection. The research uses the UNSW-NB15 cyber-security dataset, which was collected and standardized using the z-score normalization approach. Federated learning was used to train the local models of each IoT device with their respective subsets of data. The MPC method is used to aggregate the encrypted local models into a global model while maintaining the confidentiality of the local models. Finally, in the attack detection phase, the global model compares real-time sensor data and predicted values to identify cyber-attacks. The experiment findings show that the suggested model outperforms the current methods in terms of accuracy, precision, f-measure and recall.**

Keywords*—*Federated learning; multi-party communication; cyber-security; machine learning; internet of things

I. INTRODUCTION

IoT defines the interconnection between physically moving objects through the internet integrated with the sensors, system memory, electronic chips, and other hardware [1]. In an IoT network, things interact with other nodes, which can be managed and controlled remotely [2]. This interconnectivity between the nodes enables them to gather and exchange information with other connected devices [3]. The IoT system provides ubiquitous connectivity to various intelligent systems, service industries, cloud computing, and applications [4]. Moreover, the IoT system enhances the number of communication networks and the amount of big data shared using the cloud architecture [5]. Recently, IoT-assisted approaches have had numerous applications in smart cities, online shopping, health care, banking, industries, etc., to protect human beings [6]. However, IoT systems are vulnerable to open attacks available on the network. Furthermore, the increased usage of IoT devices made them more vulnerable to cyber-attacks, making it essential to develop efficient mechanisms for predicting these threats [7]. The traditional techniques to detect and prevent cyber-attacks in IoT include conducting risk assessment, execution of authentication system, utilization of secure protocols, data encryption, etc., [8]. The risk assessment involves the evaluation of security controls to predict the vulnerabilities and cyber-attacks in the IoT system [9]. The implementation of the authentication system includes the usage of biometric authentication, password policies, and factor authentication technique to enable authorized user access in the IoT network [10].

In data encryption, the collected IoT data was encrypted using different algorithms during the data transmission [11]. However, conventional algorithms cannot offer higher security to IoT devices. Moreover, it cannot deal with the huge volume of data generated by IoT devices [12]. To address these challenges, Artificial Intelligent (AI) techniques are utilized to predict malicious events in the IoT network [13]. Machine learning (ML)-based methods are trained to identify data patterns and malicious events without requiring explicit protocols [14]. Hence, they have emerged as an effective attack detection tool in real-time IoT systems. Several types of ML techniques exist, such as supervised, unsupervised, and reinforcement learning [15]. The supervised learning technique utilizes a labeled database to train the algorithm to identify the patterns and categorize data into various classes, like benign or malicious [16]. But then, unsupervised learning does not require a labeled dataset to predict the data pattern or malicious data [17]. On the other hand, the reinforcement learning technique learns from experience and makes decisions to predict and prevent cyber-attacks in IoT networks [18].

Utilizing ML approaches in cyber-attack detection earned more advantages, like greater detection accuracy, improved speed, and faster response [19]. In addition, it enables the system to classify the types of cyber-attacks present in the data [20]. Moreover, it minimizes the human workload and allows them to detect complex cyber threats. However, the existing ML-based techniques face limitations and challenges, such as lack of labeled data, inconsistent data quality, storage, data privacy, etc. Moreover, recently various approaches such as supervised machine learning [21], false-data injection using ML model [22], Ensemble deep learning model [23], Deep learning-based IDS [24], Federated Learning-based IDS [26], etc., are designed to protect the network data from cyber-security attacks. However, these approaches are limited to generalizability that is these techniques cannot recognize the patterns of unknown attacks. Moreover, the performances of these models rely on dataset availability for training, and acquiring such a database is challenging. In addition, the techniques including deep learning and machine learning algorithms are computationally expensive and resource

intensive. Also, training and deploying these techniques require more computational power, memory, and time, thus making them less effective for resource-constrained environments. Addressing these issues and challenges is important to develop a reliable and robust cyber-security framework. To address these challenges, federated learning with an intelligent MPC system was developed in this article. The basic concept of the proposed model is combining the advantages of Federated Learning and MPC algorithms to predict attacks and malicious events in IoT networks. The key contributions of the presented research work are described below:

- We develop an integrated Federated learning-based Multi-Party Computation approach to protect the IoT network data from malicious attacks.
- The network data was pre-processed using the z-score normalization approach enabling data standardization and effective training across subsets.
- Each IoT device trains a local model on its subset of pre-processed data using the federated learning approach. Then, the local models are encrypted using the MPC to confirm data security.
- The central server collects the encrypted models, and secure model aggregation was performed using the intelligent MPC approach to ensure privacy of the individual models.
- Finally, the performances of the developed model were analyzed and evaluated with existing techniques in terms of accuracy, f-measure, recall, and precision.

The organization of the presented article is described as follows, the current research related to cyber-security is described in Section II, the existing cyber-security model and its challenges are illustrated in Section III, the proposed methodology is explained in Section IV, the outcomes of the proposed work is analyzed in Section V, and the conclusion of the article is summarized in Section VI.

II. Related Work

Some of the research articles related to the proposed work are listed below:

IoT defines the interconnection between different devices or objects, enabling the devices to collect, exchange and share information over the Internet. However, the tremendous growth of the IoT makes it more vulnerable to privacy and security risks. These security risks result in the limitation of energy resources and reduce the scalability of IoT devices. Hence, Yakub Kayode Saheed *et al.* [21] proposed an ML-supervised approach-based Intrusion Detection System (IDS) to address the security and privacy risks of the IoT. The developed model was tested and evaluated with the publicly available UNSW-NB15 dataset. The developed model utilizes the Principal Component Analysis technique to reduce the dataset dimensionality and minimum-maximum normalization concept to extract features. The implementation outcomes illustrate that the presented model earned greater accuracy of 99.9% for the UNSW-NB15 dataset. However, training the labeled dataset using the supervised technique consumes more time and increases the implementation cost.

The wide acceptance of the Industrial Internet of Things (IIoT) system resulted in various limitations like security, privacy, etc. The primary security threat affecting the IIoT system's function is the False Data Injection (FDI) attack. The primary concern of the FDI attacks is to mislead the industrial design by faking its sensor measurements. Mariam M. N. Aboelwafa *et al*. [22] developed an innovative FDI attack prediction algorithm. This method utilizes auto-encoders to detect the FDI attacks accurately. Initially, the sensor data was collected from the industrial sector and pre-processed to detect false data. Further, denoising auto-encoders are used to clean the falsified data. Finally, the performance of the developed design was evaluated and compared with existing techniques. The developed model is more effective in recovering the clean data from the injected dataset. However, the presented approach cannot handle highly dynamic and complex datasets.

The incorporation of IoT devices and communication networks in industrial control systems makes them vulnerable to cyber-attacks, making the system produce devastating results. Typically, IDS schemes are developed to assist the Information Technology (IT) system in predicting cyber-attacks. These models are pre-defined algorithms and are trained to identify the specific cyber threat. However, the traditional IDS design needs to consider the inconsistent nature of the industrial control system, which results in low accuracy and a high false positive rate. Abdulrahman Al-Abassi *et al.* [23] designed a Deep Learning (DL)-based IDS framework to overcome these issues. The proposed model builds a balanced demonstration of the imbalanced database and passes it to the ensemble DL attack prediction scheme. The developed algorithm integrates the deep neural network (DNN) and Decision tree classifier to predict cyber-attacks accurately. However, this approach cannot specify the cyber-attacks in the industrial control system.

The ultimate goal of the stakeholders from IIoT is its sustainability and trustworthiness to prevent loss. A secured IIoT network enables trust, security, privacy, safety, and reliability to the stakeholders. However, conventional security models are ineffective in protecting the network from security threats. Fazlullah Khan *et al*. [24] designed a reliable and accurate supervisory control and data acquisition (SCADA) system-based attack detection. The developed model integrates the DL-based recurrent units and decision tree classifier to predict the cyber-attacks in the IIoT system. The nonlinearity of the presented recurrent unit eliminates the irrelevant data. Thus it enhances the detection rate of the system. The proposed technique was validated with 15 different SCADA datasets. The experimental analysis illustrates that the presented algorithm outperforms the traditional attack detection schemes. However, it cannot process large-scale databases.

In the IIoT system, a tremendous amount of data processing occurs at the edge or cloud server to perform various analytics. Hence, various DL-based data analytic models are developed to effectively process the hue IIoT data. However, the learning process must be trustworthy and reliable to overcome the vulnerability of the IIoT networks. Therefore, Sharmistha

Nayak *et al.* [25] developed a DL-based routing algorithm for attack prediction in IIoT networks. This model deploys adversarial training to identify the injected attacks. Furthermore, the Generative Adversarial Network-Classifier (GAN-C) is designed to specify the type of attack that occurred in the IIoT system. The developed model utilizes parallel learning and prediction design to minimize the computational complexity of the system. The performance analysis demonstrates the usage of GAN-C significantly reduces the training time and increases accuracy. But the GAN-C is biased towards certain data types, making the system more complex.

Othmane Friha *et al.* [26] presented a federated learning (FL)-based IDS for providing security to the agricultural IoT architectures. The developed model protects the agricultural data through local learning in which the devices benefit the knowledge and share to enhance the detection accuracy. The presented model utilizes three different DL classifiers: convolutional neural network, recurrent neural network, and deep neural network. The performance of the developed algorithm was evaluated on other datasets such as InSDN, MQTTset, and CSE-CIC-IDS2018. The results illustrate that the presented technique outperforms the non-federated learning techniques. However, the communication cost in the proposed method is high compared to other techniques.

III. Problem Statement

Even though the Internet of Things (IoT) has undoubtedly improved our everyday lives in many ways, its dispersed and decentralized architecture has also opened the door to novel cybersecurity risks. Methods based on Machine Learning (ML) have shown a lot of promise in spotting these dangers. The limitations of the traditional approaches include dependency on central servers for data processing and transmission; hence, these models cannot perform in a decentralized IoT environment. The existing model faces privacy problems, as they share sensitive data with the central server; this leads to data unauthenticated access to user-sensitive information. Moreover, these models transfer the large volume of data to the server, which is time-consuming, poses computational overhead, large energy consumption, and leads to poor resource utilization. As a result, improved collaboration methods for threat detection across IoT devices that respect users' security and privacy are required. Federated learning with MPC may provide a safer and more private solution for IoT devices to work together on threat detection [27]. The motivation behind the proposed work is the benefits of federated learning and MPC to handle the decentralized and distributed nature of the IoT environment. The federated learning approach enables each IoT device in the network to train a local model using its data, confirming that the sensitive data remains on the device and is not shared with the central aggregator. This decentralized framework preserves data privacy and addresses the concerns interconnected with centralized data aggregation. Moreover, the distributed and decentralized feature of federated learning minimizes the amount of data transmission, thus it reduces the computational overhead and energy consumption issues faced by the existing models. Further, by aggregating the local models' knowledge through MPC, the global model benefits from the collective intelligence of all participating IoT devices. This collaboration enables the system to leverage diverse data sources and insights, leading to more accurate and robust threat detection. Moreover, the MPC approach confirms that the data transmitted during collaboration remains encrypted and makes it inaccessible to unauthenticated users. Thus, the designed framework addresses the problems faced by the existing models.

IV. Proposed FLbMPC Approach For Cyber-Attack Detection

A novel hybrid cyber-security framework was developed in this article to predict attacks or malicious events in the IoT network. This model integrates the Federated Learning algorithm [28] and intelligent multi-party computation (MPC) [29] technique to secure network data from cyber-security threats. The federated learning is an algorithm, which enables multiple IoT devices to collaboratively train the model without sharing the raw data. On the other hand, the MPC is a cryptographic algorithm, which allows secure collaboration and computation on encrypted data. Initially, the cyber-security dataset was collected from the standard site and imported into the system. The raw dataset was pre-processed using the z-score normalization technique, and the dataset was partitioned into multiple subsets in which different parties own each subset. Further, each IoT device trains a local model on its subset of pre-processed data.

The local model can be an ML design trained using the federated learning algorithm. After the completion of local model training, it is encrypted using the MPC to confirm that the privacy of the local model is preserved. Then, the encrypted local model is sent to the central server for aggregation.

The central server gathers the encrypted local models from all the IoT devices and aggregates them to form a global model. The proposed work performs the model aggregation using the MPC algorithm. Finally, the global model is utilized to predict cyber-attacks in real-time by comparing sensor readings from each IoT device to the expected values detected by the model. If there is a difference from the expected values, it is represented as a cyber-attack. Finally, the performances of the proposed work are estimated in model evaluation in terms of accuracy, precision, recall, and f-measure. The proposed framework is explained in Fig. 1.

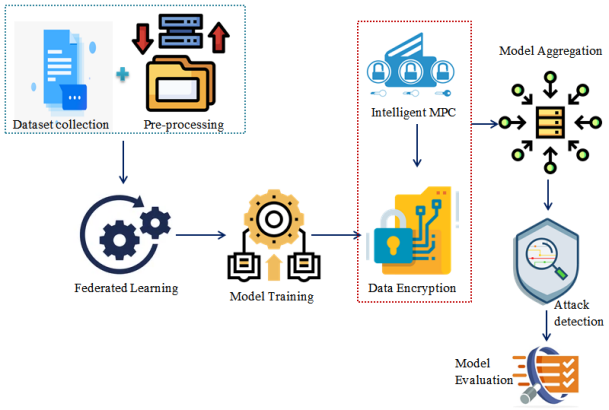

Fig. 1. Proposed hybrid federated learning framework with multi-party communication.

A. Data Pre-processing

The cyber-security dataset containing the network traffic logs from numerous IoT devices is initially collected. Each log contains information regarding the device, log time, port numbers, IP addresses, packet sizes, etc. In the proposed work, the UNSW-NB15 cyber-security dataset was collected from the Kaggle site and imported into the system. The dataset initialization is expressed in Eq. (1).

$$D_{un} = \{d_{a1}, d_{a2}, ...d_{an}\} \quad (1)$$

Where D_{un} denotes the input dataset, d_a the data present in the dataset, and n the number of data present in the dataset. Then the raw dataset was pre-processed using the z-score normalization technique. Z-score normalization is a data pre-processing approach deployed in ML to convert numerical attributes to mean and standard deviations of 0 and 1, respectively. The mean and standard deviation calculation for each feature in the dataset is expressed in Eq. (2), and (3).

$$M_e(D_{un}) = \frac{1}{n}\sum(f_i) \quad (2)$$

$$S_D(D_{un}) = sqrt\left(\frac{1}{n} * \sum(f_i - M_e)^2\right) \quad (3)$$

Here S_D represents the standard deviation, M_e denotes the mean value, and f_i indicates the value of the i^{th} feature. The dataset normalization is formulated in Eq. (4).

$$N(f_i) = \frac{(f_i - M_e)}{S_D} \quad (4)$$

In this approach, the mean of the feature is subtracted from each value in the feature, and the result is divided by the feature's standard deviation. The outcome values have a mean and standard deviation of 0 and 1, which enables the ML algorithms to learn easily from the data.

B. Model Training

The model training was performed using the federated learning algorithm in the proposed framework. Federated learning is a ML-based algorithm that performs model training using the data distributed across multiple devices without the necessity of centralized data collection. Initially, the pre-processed dataset was partitioned, and then local model training was performed to train the models for cyber-attack detection. The dataset was partitioned into multiple subsets and distributed across the IoT devices. In the developed work, random partitioning was deployed to divide the dataset into approximately equal sizes of subsets. The formulation of data partition is expressed in Eq. (5).

$$D_{un} = \{D_{un1}, D_{un2}, D_{un3}, ...D_{unK}\} \quad (5)$$

Where K denotes the number of IoT devices. In federated learning, the data is partitioned so that each party owns a data subset, and the subsets are non-overlapping. For example, the party p owns a subset of data D_{unp}.

The local training model begins after the completion of data partitioning. It is the process of training a ML design on the data subset owned by each party in the network.

In the proposed work, each party trains a local model on its own data subset without sharing the data with other parties. Here, each party p trains a local model M_p with its own data subset D_{unp} in a decentralized manner and L_p denotes the local model on the device.

C. Model Aggregation

After the completion of local model training, it is encrypted using the MPC approach to confirm the security and privacy of the model. The local model is encrypted using cryptographic techniques like MPC. The encryption of local models is expressed in Eq. (6).

$$E_n(L_p) = Ef_{Ke}(L_p) \quad (6)$$

Where E_n denotes the encryption process, Ef refers to the encryption function, and Ke represents the key. Further, the central server gathers the encrypted local models from all the IoT devices and aggregates them to form a global model. In the proposed work, the model aggregation was performed using MPC. The global model was utilized to predict cyber-attacks in real time by comparing sensor readings from each IoT device to the expected values detected by the model. If there is a variation from the expected values, it predicts a cyber-attack. It is represented in Eq. (7).

$$D'_p = \left|S_p - S'_p\right| \quad (7)$$

where D'_p indicates the deviation between the actual and expected values, S_p denotes the sensor reading on the device p, and S'_p the expected value detected by the global model. If the deviation value exceeds the predefined threshold value T_R, it is predicted as an attack. Otherwise, the central server updates the global model, which is expressed in Eqn. (8).

$$R' = R - \lambda\sum(D'_p - \nabla L_p) \quad (8)$$

Where R' denotes the updated global model, R indicates the previous global model, λ refers to the learning rate, and ∇L_p defines the gradient of the local model on the device p. This process continues until the global model achieves the desired accuracy.

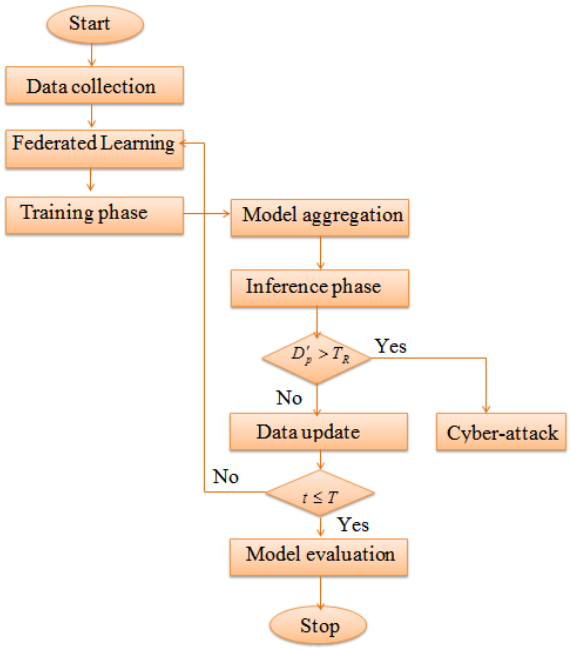

Fig. 2. Flowchart of the proposed framework.

The flowchart of the proposed work is displayed in Fig. 2. In addition, the step-by-step procedure of the proposed model is illustrated in pseudo code format in algorithm 1.

Algorithm pseudo-code of the proposed model (Algorithm 1)

start

{

1. Initialize the machine learning model with random weights R_w
2. Initialize the number of training rounds, IoT devices
3. Initialize the batch size and learning rate for local training
4. for $(t = 1, t \le T; t++)$

{

5 Partition the dataset: $D_{un1,}\, D_{un2}, D_{un3}, \ldots\ldots D_{unK}$

6 Each IoT device *p* trains the local model L_p with its subset. D_{unp}

7 $En = encrypt(L_p)$ *// encrypt the local model using the MPC algorithm*

8 Send the encrypted model to the central server.

9 $L_p = encrypt(En)/N$ *// aggregate the local model to form a global model*

10 $If(D'_p > T_R)$

11 {

12 **"Cyber-attack"** *//The system predicts a "cyber-attack."*

13 }

14 else **(data update);**

}

}

end

V. Results and Discussion

This research proposed a hybrid intelligent cyber-security mechanism to detect cyber-attacks in the IoT system. The model utilizes federated learning and MPC to predict cyber-attacks effectively. The input dataset was initially collected and pre-processed using the z-score normalization approach. Further, a federated learning algorithm was designed to partition the normalized dataset. Moreover, it enables the system to train the local model in a decentralized manner (without sharing the raw dataset). Moreover, an intelligent MPC was developed to encrypt the local models, enabling it to preserve the privacy of the local models.

Finally, the encrypted local models are sent to the central server for model aggregation. The model aggregator combines them to form a global model. The global model predicts cyber-attacks by analyzing expected and actual sensor readings deviation. The presented work was implemented in MATLAB software, version R2020a, and the results are analyzed. The parameters and their description are tabulated in Table I. In addition, a comparative assessment was carried out to manifest the effectiveness of the proposed work.

A. Dataset Description

The presented model was trained and tested with the UNSW-NB15 dataset. It is a cyber-security dataset that was developed to help the researchers on IDS and network security. It consists of a massive collection of network traffic data, including the different types of cyber-attacks such as DoS, Probe, U2R, R2L, etc. Table II illustrates the attack types and number of records in the UNSW-NB15 dataset. The dataset contains ten different attack types indicated by a separate class label.

TABLE I. Parameter and Specification

Parameters	Specification
Tool	MATLAB
Version	R2020a
OS	Windows10
Dataset	UNSW-NB15
Dataset size	1.9GB

TABLE II. Dataset Description

Attack Type	*Number of records*
Normal	221,876
Analysis	2,244
Backdoor	18
DoS	122,846
Exploits	445,104
Fuzzers	242,720
Generic	188,220
Reconnaissance	104,13
Shellcode	1,571
Worms	130

In addition, it includes 49 different features like port numbers, protocol types, source and destination IP addresses, byte counts, etc. The University of New South Wales researchers in Australia created the dataset. It comprises nearly 2.5 million network packets in which 175,341 records are selected for training and 82,332 records are chosen for testing.

B. Case Study

The working procedure of the proposed work is explained in this case study. Initially, the input cyber-security dataset was collected from the standard site and imported into the system. In the present study, the UNSW-NB15 dataset was collected and fed into the system for further processing. After data initialization, the raw dataset was pre-processed using the z-score normalization technique. Further, a federated learning setup was established for performing data partition and local model training. Initially, the pre-processed dataset was partitioned into approximately equal-sized subsets and distributed to IoT devices.

Federated learning helps the system divide the dataset so that each party owns a data subset, and the subsets are non-overlapping. In local model training, each party trains a local model with its own data subset without sharing the data with other parties. Further, the trained local models are encrypted using the MPC algorithm to ensure the privacy and security of the models. After encryption, the central server collects the encrypted local models from all the IoT devices and aggregates them into a global model. The global model was used to detect cyber-attacks by matching the real-time sensor reading with the expected values predicted by the model. If the difference between actual and estimated values is greater than the threshold value, it is predicted as Attack. Else, the central server updates the global model.

This process is continued until the system achieves the desired accuracy. Finally, the performances of the proposed technique were estimated by implementing it in the MATLAB tool. In addition, a comparative assessment was performed to validate the outcomes of the proposed work. The implementation results of the proposed work are tabulated in Table III.

The performance analysis illustrates that the proposed model earned greater performances, such as 99.98% accuracy, 100% precision, 99.8% recall, and 99.87% f-measure. In addition, the presented model achieved a less computational time of 2.34ms.

C. Performance Analysis

In this module, the performances of the proposed work are examined in terms of accuracy and loss relative to the increasing number of epochs. The training and testing accuracy of the proposed framework over increasing epochs count is demonstrated in Fig. 3. The training accuracy denotes the model accuracy on the train dataset which is how accurately the designed model detects the attacks on the train set. In addition, it measures how efficiently the designed model learns the attack patterns during the training phase. On the other hand, the testing accuracy measures how well this approach works on unseen data. The designed framework achieved an approximate training accuracy of 0.99, which demonstrates that the developed model works well on the training dataset and quickly learns the interconnection between the normal and attack data. Consequently, the presented approach attained an approximate testing accuracy of 0.97; this shows that the designed framework predicts cyber-attacks on unseen data effectively.

Similarly, the training and testing losses were over increasing epochs. Fig. 4 portrays the evaluation of training and validation losses. The training loss represents the difference between the actual and predicted results on the training dataset. It measures how well the proposed model fits the training set and learns the relationship between network data and attack patterns. This approach attained an average training loss of 0.003, which shows that the proposed model fits well on the training dataset.

TABLE III. PERFORMANCE ANALYSIS

Metrics	***Values***
Accuracy (%)	99.98
F-measure (%)	100
Recall (%)	99.8
Precision (%)	99.87
Processing time (ms)	2.34

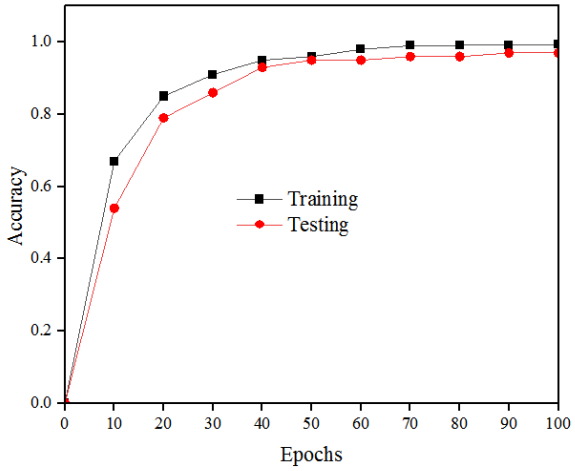

Fig. 3. Training and testing accuracy evaluation.

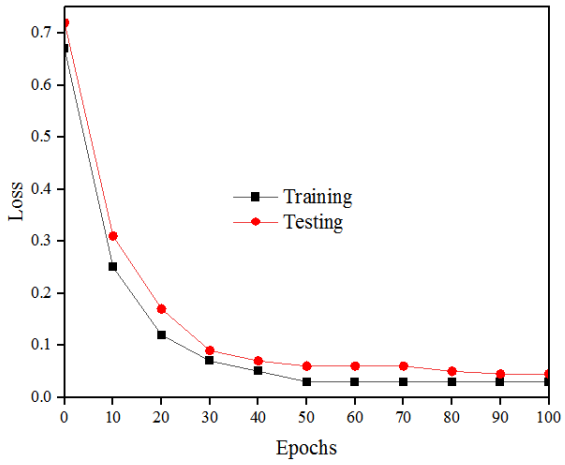

Fig. 4. Training and testing loss evaluation.

The testing loss defines the model's generalization ability on unseen data (unknown attack patterns). This approach earned a testing loss of 0.045, which indicates that the proposed model accurately classifies cyber-attacks in real-world scenarios.

Furthermore, to evaluate the effectiveness of the proposed work on real-world scenarios the system performances such as attack detection accuracy, computational time, and energy consumption are analyzed for increasing number of participants and data size in the network.

Here, the model accuracy was evaluated by increasing the data size and number of users in the IoT network and it is graphically represented in Fig. 5. When the network user count is 20, the proposed model earned an average accuracy of 99%. Further, on increasing the network users to 40, 60, 80, and 100, the designed model obtained an approximate accuracy of 99.5%, 99.6%, 99.7%, and 99.99%. The increase in system accuracy over increasing network users and data size is because of the ability of the proposed model to compare the sensor readings with the expected values. This makes the system more refined and attuned to the attack patterns owing to improved accuracy over increasing network users and data size.

Error rate defines the discrepancy between the actual and predicted results. This metric determines the efficiency of the model in detecting the attacks. Fig. 6 illustrates the error rate over increased network users and data size. The proposed model earned a minimum error rate of 1%, 0.9%, 0.8%, 0.6%, and 0.5%, respectively for 20, 40, 60, 80, and 100 network users at increasing data size from 50MB to 500MB. The lowering of the error rate illustrates that despite the increased network users and data size the proposed model correctly detects the attacks and normal events.

The computational complexity over increasing network users and data size is illustrated in Fig. 7, the computational time of the system was examined at different network user counts and the increasing data size (50 to 500MB). When a user in the network is 20, the proposed system consumed an average computational time of 1.75ms. Consequently, on increasing the network users to 40, 60, 80, and 100, the designed model consumed an approximate time of 2ms, 2.25ms, 2.5ms, and 2.75ms, respectively. From the analysis, it is observed that the computational time increases with increasing the number of users and data size in the IoT network. However, the computational time consumed by the presented model is relatively small, which is achieved by integrating federated learning and MPC. The local model training using the FL approach significantly reduces the amount of data transmission over the network; this minimizes the computational overhead and leads to faster communication. The integration of these techniques optimizes the computational process and reduces the time complexity.

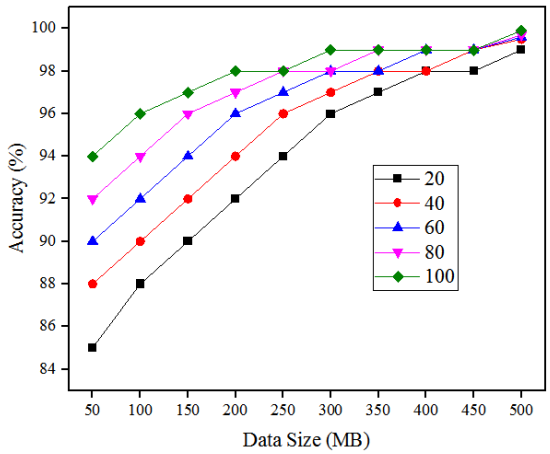

Fig. 5. System accuracy over the increasing number of network users and data size.

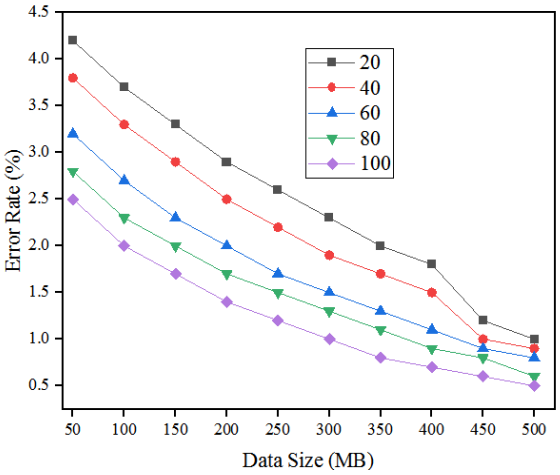

Fig. 6. Error rate over the increasing number of network users and data size.

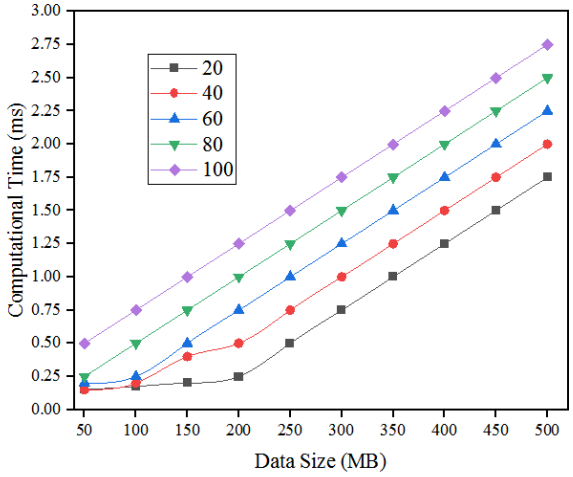

Fig. 7. Computational complexity over increasing network users and data size.

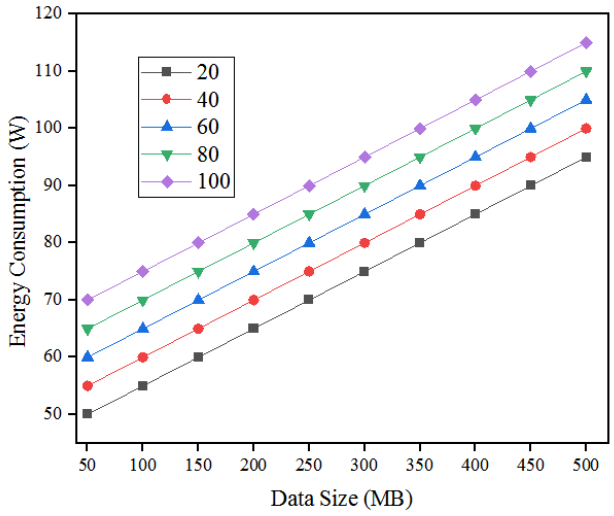

Fig. 8. Network energy consumption over increasing network users and data size.

The energy consumption of the system over increasing data size and network users is graphically represented in Fig. 8. Typically, on increasing the network user count and data size the energy consumption of the IoT network increases. Similarly, energy consumption increased with the increase in user count and dataset size. When the user count is 20, the model attained an average energy consumption of 95W over increasing data size (50 to 500). Consequently, the proposed model obtained an approximate energy consumption of 100W, 105W, 110W, and 115W, respectively for 40, 60, 80, and 100 network users. Similar to the traditional model the energy consumption of the network increases over increased network user and dataset size. However, the energy consumption of the system is comparatively lower than other models. This is due to the incorporation of the FL method in the proposed model. The FL technique in the designed model enables collaborative training that is it does not require a centralized server and instead of transferring the raw data to the central server, the proposed framework transmits only encrypted local models for aggregation. This process significantly reduces the energy consumption for data transmission. This comprehensive performance analysis manifests that the developed model efficiently predicts the attacks or malicious events on the IoT network.

D. Comparative Analysis

In this section, the performances of the proposed model are compared with existing techniques for validation purposes. The current methods such as Deep Belief Network-based Intrusion Detection System (DBN_IDS) [30], Deep Convolutional Generative Adversarial Network (DCGAN) [31], Distributed Convolutional Neural Network (DCNN) [32], Feed-forward neural network (FFNN) [33], and Vector convolutional deep learning (VCDL) [34] are used in comparative performance. The outcomes of these techniques are evaluated by implementing them in the MATLAB tool for the UNSW-NB15 dataset.

1) Accuracy: Accuracy defines the percentage of correct classification of instances. It is defined as the proportion of the sum of true positives and negatives to the total number of instances[35]. Moreover, it represents how exactly the system performs a cyber-attack detection function. The accuracy calculation is formulated in Eq. (9).

$$A_{sy} = \frac{w^+ + w^-}{w^+ + w^- + z^+ + z^-} \tag{9}$$

Where A_{sy} defines the system accuracy, w^+ w^- z^+ and z^- denotes the true positive, true-negative, false-positive, and false negative, respectively.

To manifest the accuracy of the proposed technique, it is compared with existing cyber-security models. Fig. 9 shows the comparison of accuracy. This section uses existing models such as VCDL, FFNN, DCNN, DCGAN, and DBN_IDS for comparative analysis. The accuracy earned by the conventional approaches is 94.72%, 89.43%, 95.45%, 91.78%, and 95.65%, respectively. But the developed technique attained greater accuracy of 99.98%, which is higher than existing techniques. The highest accuracy obtained by the designed model illustrates that it predicts cyber-attacks accurately.

2) Precision: Precision represents the proportion of true positives out of the total positive instances classified by the system[36]. It is also defined as the system's ability to correctly predict cyber-attacks without creating false positives. The precision calculation is represented in Eq. (10).

$$Pi_{cs} = \frac{w^+}{w^+ + z^+} \tag{10}$$

Where Pi_{cs} represent the precision percentage. The high precision defines that the proposed system accurately identifies the cyber-security threats with fewer false positives.

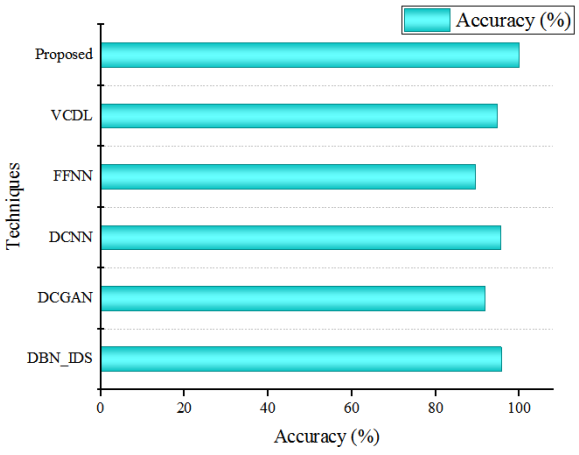

Fig. 9. Comparison of accuracy.

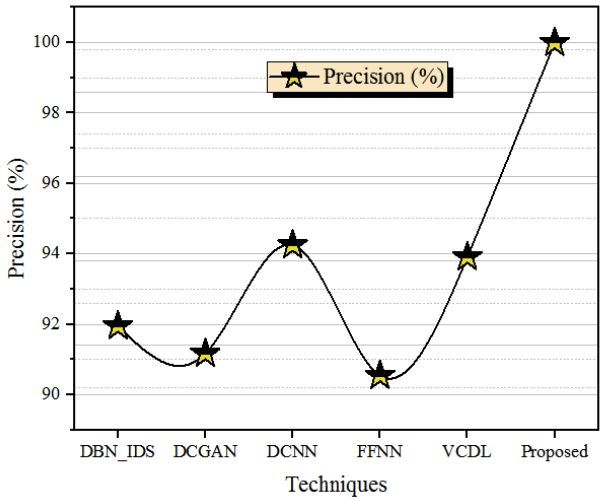

Fig. 10. Precision validation.

In model evaluation, a comparative analysis is important to identify the strength and weaknesses of the proposed techniques. Here, the precision percentage of different machine learning algorithms for predicting cyber-attacks on the UNSW-NB15 dataset was compared with the proposed technique. The existing ML techniques like VCDL, FFNN, DCNN, DCGAN, and DBN_IDS earned precision percentages of 93.91%, 90.54%, 94.25%, 90.17%, and 94.95%, respectively. However, the proposed technique obtained a higher precision percentage of 100%, which is comparatively greater than existing techniques. The comparison of precision is illustrated in Fig 10.

3) Recall: The recall is a performance metric that measures the proportion of true positives out of a total number of actual positive instances[37]. It denotes the system's capability to classify cyber-security threats irrespective of false positives correctly. The recall calculation is expressed in Eq. (11).

$$\mathrm{Re}_{ll} = \frac{w^{+}}{w^{+} + z^{-}} \tag{11}$$

Where Re_{ll} denotes the recall. The high recall rate defines that the system exactly predicts most of the actual cyber-attacks.

The comparison of recall is shown in Fig. 11. The recall is compared with the existing techniques such as VCDL, FFNN, DCNN, DCGAN, and DBN_IDS. The proposed technique attained a recall percentage of 99.8%. On the other hand, the recall percentage attained by the conventional methods is 92.24%, 88.56%, 93.41%, 91%, and 94.16%, respectively. The comparative performance of recall describes that the developed model achieved a better recall percentage than existing techniques.

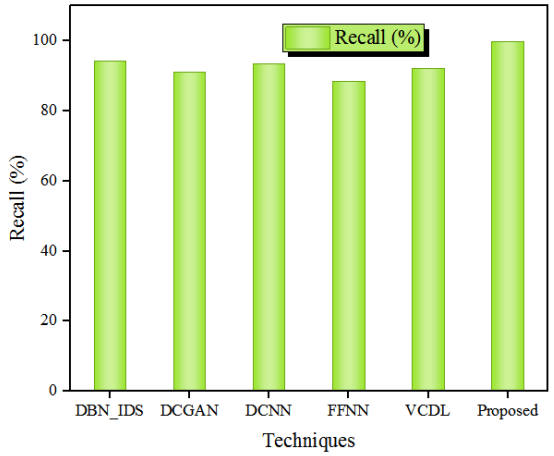

Fig. 11. Comparison of recall.

4) F-measure: F-measure is the metric that combines both precisions and recalls into a single score. It is evaluated as the harmonic mean of these two metrics[38]. The system achieves greater f-measure value only when both recall, and precision score is high. The f-measure calculation is represented in Eq. (12).

$$Fm_{sc} = 2\left(\frac{Pi_{cs} * \mathrm{Re}_{ll}}{Pi_{cs} + \mathrm{Re}_{ll}}\right) \tag{12}$$

Where Fm_{sc} refers to the f-measure.

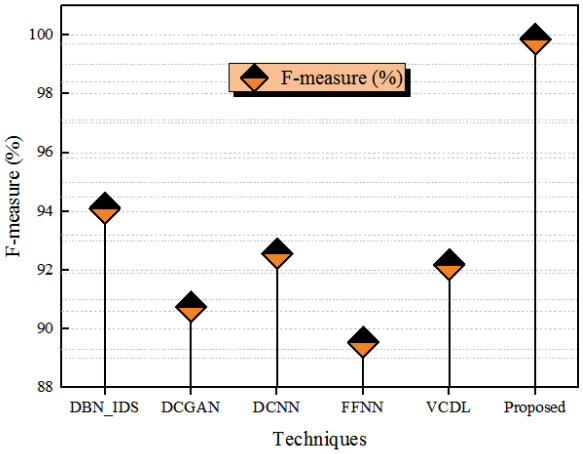

Fig. 12 Comparison of f-measure

To validate that the proposed model gained more f-measure, it is compared with existing techniques like VCDL, FFNN, DCNN, DCGAN, and DBN_IDS. Fig. 12 shows the comparison of the f-measure percentage. The f-measure obtained by the existing techniques is 92.18%, 89.54%, 92.56%, 90.75%, and 94.10%, respectively, less than the f-measure earned by the proposed model. This shows that the developed model balances the precision and recall metrics optimally.

TABLE IV. COMPARATIVE PERFORMANCE OF DIFFERENT MODELS

Techniques	*Accuracy (%)*	*Precision (%)*	*Recall (%)*	*F-measure (%)*
DBN_IDS	95.65	94.95	94.16	94.10
DCGAN	91.78	90.17	91.00	90.75
DCNN	95.45	94.25	93.41	92.56
FFNN	89.43	90.54	88.56	89.54
VCDL	94.72	93.91	92.24	92.18
Proposed	99.98	100	99.8	99.87

The comparative performance of different cyber-security models with the proposed technique is tabulated in Table IV.

5) Computational time: Computation time defines the time taken by the system to perform tasks such as data pre-processing, encryption, data transmission, decryption, etc. The computational time of the system is tabulated in Table V.

TABLE V. COMPUTATIONAL TIME EVALUATION

Component	*Time (ms)*
Encryption time	0.5
Key generation time	0.2
Decryption time	0.6
Data processing time	1.04
Total computational time	2.34

The computational time of the system was compared with an existing model including the VCDL, FFNN, DCNN, DCGAN, and DBN_IDS for validation purposes.

TABLE VI. COMPUTATIONAL COMPLEXITY OF DIFFERENT MODELS

Techniques	*Computational time (ms)*
DBN_IDS	16.02
DCGAN	21.96
DCNN	16.93
FFNN	20.5
VCDL	17.92
Proposed	2.34

Table VI lists the computational complexity of different models. The above-mentioned models consumed 16.02ms, 21.96ms, 16.93ms, 20.5ms, and 17.92ms, respectively. The time taken by the proposed model is 2.34ms, which is comparatively less than the existing techniques. The comprehensive comparative assessment proves that the developed model outperformed the existing techniques.

E. Discussion

This research article presents an integrated framework to detect attacks or malicious events in the IoT network. The developed strategy combines the advantages of Federated learning and MPC algorithms. To begin with, a cyber-security database was acquired from a standard source and fed into the system. This collected database acts as the basis for training the models and predicting potential cyber-attacks. Before training, the raw data was pre-processed using the z-score normalization method. The data normalization confirms that the data was standardized and ready for further analysis. Further, the standardized database was partitioned into multiple subsets, with each subset being owned by different parties (IoT devices). Each party trains the local model using the FL model on its subset of pre-processed data. The utilization of the FL approach for training ensures that the sensitive information owned by IoT devices remains secure and confidential. Moreover, this distributed training minimizes the computational overhead on individual IoT devices and overcomes the drawback of centralized training in which a single server is responsible for training the entire dataset. In addition, it improves scalability and ensures efficient resource utilization.

After local model training, these models are encrypted using the MPC algorithm; this ensures that the model's sensitive data remains confidential and prevents unauthorized data access. Consequently, the encrypted local models are transmitted to the central server for aggregation. The central server receives the encrypted local models from all IoT devices and combines them to form a global model using the MPC, without having direct access to the data. This step permits secure and privacy-preserving collaboration among the different parties. Finally, the global model containing the collective knowledge of all local models is employed to detect cyber-attacks. The real-time prediction ability of the global model improves the system's capacity to respond promptly to cyber-attacks and mitigate potential damages.

The presented approach was evaluated with the publically available network data named UNSW-NB15 and the performances are analyzed in terms of accuracy, computational time, error rate, and energy consumption. Moreover, the developed model performances are examined in real-time scenarios over increasing network users and data size. This intensive performance evaluation demonstrates the effectiveness of the proposed model in handling real-time applications. Thus, the integration of federated learning with the MPC permits the data to remain on the IoT devices, and only encrypted gradients are sent to the central server. This enables the system to preserve security by ensuring that sensitive information is not transmitted to the central server and reduces the risk of data breaches. In addition, the proposed model minimizes the latency, especially in scenarios with limited network connectivity. Moreover, it enhances the robustness to device failures. Since the training is distributed across multiple devices, the failure of one or more devices does not necessarily lead to the failure of the entire system. Furthermore, to manifest the robustness of the developed model the obtained results are compared with the existing techniques. The comparative analysis demonstrates that the proposed model outperformed the existing models in terms of accuracy, recall, f-measure, and precision.

VI. CONCLUSION

This paper proposed a ML-based cyber-security framework to secure IoT networks from attacks and malicious activities. The proposed framework integrates the FL technique and MPC algorithm to preserve security in the IoT. Federated learning

partitions the pre-processed data into equal size subsets. Further, each IoT devices train a local model on its subset of data. Then the trained local models are encrypted using the MPC approach to preserve the model's privacy. Finally, the central server gathers the encrypted local model and forms a global model to predict the cyber-attacks in the system. The developed model is implemented in the MATLAB tool on the UNSW-NB15 dataset. Moreover, a comparative analysis was performed to illustrate the robustness of the proposed algorithm. The comparative analysis shows that performance like precision, accuracy, recall, and f-measure are improved by 5.05%, 4.33%, 5.64%, and 5.77%, respectively. Thus, the designed model accurately predicts the cyber-attacks in IoT networks. Although the proposed framework provides high privacy, it cannot handle large-scale federated learning scenarios. In addition, the proposed framework is vulnerable to adversarial attacks, such as model poisoning or data poisoning attacks. Since IoT systems are composed of devices and sensors from different vendors and manufacturers, making interoperability a critical issue. Moreover, this approach may face scalability issues when handling large-scale federated learning scenarios, and maintaining the inherent trade-off between privacy and utility is a challenging factor. Therefore, in the future, developing ML-based techniques with multi-objective optimization and advanced privacy-preserving approaches will provide enhanced privacy and increases the scalability and efficiency of the system.

REFERENCES

[1] Chen, Wei. "Intelligent manufacturing production line data monitoring system for industrial internet of things." Computer Communications 151 (2020): 31-41.

[2] Ray, Abhay Kumar, and Ashish Bagwari. "IoT based Smart home: Security Aspects and security architecture." 2020 IEEE 9th international conference on communication systems and network technologies (CSNT). IEEE, 2020.

[3] Ahmed, Imran, et al. "A blockchain-and artificial intelligence-enabled smart IoT framework for a sustainable city." International Journal of Intelligent Systems 37.9 (2022): 6493-6507.

[4] Yunana, Kefas, et al. "Internet of things: Applications, adoptions, and components-a conceptual overview." Hybrid Intelligent Systems: 20th International Conference on Hybrid Intelligent Systems (HIS 2020), December 14-16, 2020. Springer International Publishing, 2021.

[5] Stergiou, Christos L., Konstantinos E. Psannis, and Brij B. Gupta. "IoT-based big data secure management in the fog over a 6G wireless network." IEEE Internet of Things Journal 8.7 (2020): 5164-5171.

[6] Heidari, Arash, Nima Jafari Navimipour, and Mehmet Unal. "Applications of ML/DL in the management of smart cities and societies based on new trends in information technologies: A systematic literature review." Sustainable Cities and Society (2022): 104089.

[7] Yazdinejad, Abbas, et al. "An ensemble deep learning model for cyber threat hunting in industrial internet of things." Digital Communications and Networks 9.1 (2023): 101-110.

[8] Rao, P. Muralidhara, and B. D. Deebak. "A Comprehensive Survey on Authentication and Secure Key Management in Internet of Things: Challenges, Countermeasures, and Future Directions." Ad Hoc Networks (2023): 103159.

[9] Kure, Halima Ibrahim, et al. "Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system." Neural Computing and Applications 34.1 (2022): 493-514.

[10] Alattar, Zaid Sh, Tarek Abbes, and Faouzi Zerai. "Smartphone-key: Hands-free two-factor authentication for voice-controlled devices using Wi-Fi location." IEEE Transactions on Network and Service Management (2023).

[11] Yaacoub, Elias, et al. "Secure transmission of IoT mHealth patient monitoring data from remote areas using DTN." IEEE Network 34.5 (2020): 226-231.

[12] Tripathi, Ashish Kumar, et al. "A parallel military-dog-based algorithm for clustering big data in cognitive industrial internet of things." IEEE Transactions on Industrial Informatics 17.3 (2020): 2134-2142.

[13] Bécue, Adrien, Isabel Praça, and João Gama. "Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities." Artificial Intelligence Review 54.5 (2021): 3849-3886.

[14] Sarhan, Mohanad, et al. "Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection." Journal of Network and Systems Management 31.1 (2023): 3.

[15] Sarker, Iqbal H. "Machine learning: Algorithms, real-world applications and research directions." SN computer science 2.3 (2021): 160.

[16] Singh, Jagsir, and Jaswinder Singh. "A survey on machine learning-based malware detection in executable files." Journal of Systems Architecture 112 (2021): 101861.

[17] Rajawat, Anand Singh, et al. "Suspicious big text data analysis for prediction—on darkweb user activity using computational intelligence model." Innovations in Electrical and Electronic Engineering: Proceedings of ICEEE 2021. Springer Singapore, 2021.

[18] Sarker, Iqbal H. "Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects." Annals of Data Science (2022): 1-26.

[19] Nayak, Janmenjoy, et al. "Extreme learning machine and bayesian optimization-driven intelligent framework for IoMT cyber-attack detection." The Journal of Supercomputing 78.13 (2022): 14866-14891.

[20] Müller, Nils, Charalampos Ziras, and Kai Heussen. "Assessment of Cyber-Physical Intrusion Detection and Classification for Industrial Control Systems." 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). IEEE, 2022.

[21] Saheed, Yakub Kayode, et al. "A machine learning-based intrusion detection for detecting internet of things network attacks." Alexandria Engineering Journal 61.12 (2022): 9395-9409.

[22] Aboelwafa, Mariam MN, et al. "A machine-learning-based technique for false data injection attacks detection in industrial IoT." IEEE Internet of Things Journal 7.9 (2020): 8462-8471.

[23] Al-Abassi, Abdulrahman, et al. "An ensemble deep learning-based cyber-attack detection in industrial control system." IEEE Access 8 (2020): 83965-83973.

[24] Khan, Fazlullah, et al. "Trustworthy and Reliable Deep-Learning-Based Cyberattack Detection in Industrial IoT." IEEE Transactions on Industrial Informatics 19.1 (2022): 1030-1038.

[25] Nayak, Sharmistha, Nurzaman Ahmed, and Sudip Misra. "Deep learning-based reliable routing attack detection mechanism for industrial Internet of Things." Ad Hoc Networks 123 (2021): 102661.

[26] Friha, Othmane, et al. "FELIDS: Federated learning-based intrusion detection system for agricultural Internet of Things." Journal of Parallel and Distributed Computing 165 (2022): 17-31.

[27] Ananthi, J. Vijitha, and P. Subha Hency Jose. "A perspective review of security challenges in body area networks for healthcare applications." International Journal of Wireless Information Networks (2021): 1-16.

[28] Khan, Latif U., et al. "Federated learning for internet of things: Recent advances, taxonomy, and open challenges." IEEE Communications Surveys & Tutorials 23.3 (2021): 1759-1799.

[29] Liu-Zhang, Chen-Da, et al. "MPC with synchronous security and asynchronous responsiveness." Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part III 26. Springer International Publishing, 2020.

[30] Wu, Yixuan, et al. "Intelligent intrusion detection for internet of things security: A deep convolutional generative adversarial network-enabled approach." IEEE Internet of Things Journal (2021).

[31] Balakrishnan, Nagaraj, et al. "Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things." Internet of things 14 (2021): 100112.

[32] Parra, Gonzalo De La Torre, et al. "Detecting Internet of Things attacks using distributed deep learning." Journal of Network and Computer Applications 163 (2020): 102662.

[33] Ge, Mengmeng, et al. "Towards a deep learning-driven intrusion detection approach for Internet of Things." Computer Networks 186 (2021): 107784.

[34] NG, Bhuvaneswari Amma, and S. Selvakumar. "Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment." Future Generation Computer Systems 113 (2020): 255-265.

[35] Alloqmani, A., Abushark, Y. B., Khan, A. I., & Alsolami, F. (2021). Deep learning based anomaly detection in images: insights, challenges and recommendations. International Journal of Advanced Computer Science and Applications, 12(4).

[36] Almalawi, A., Khan, A. I., Alsolami, F., Abushark, Y. B., Alfakeeh, A. S., & Mekuriyaw, W. D. (2022). Analysis of the Exploration of Security and Privacy for Healthcare Management Using Artificial Intelligence: Saudi Hospitals. Computational Intelligence & Neuroscience.

[37] Almalawi, A., Khan, A. I., Alsolami, F., Abushark, Y. B., & Alfakeeh, A. S. (2023). Managing Security of Healthcare Data for a Modern Healthcare System. Sensors, 23(7), 3612.

[38] Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. Symmetry, 12(5), 754.