

# Enhancing internet of things security against structured query language injection and brute force attacks through federated learning

Aigul Adamova<sup>1</sup>, Tamara Zhukabayeva<sup>1,2</sup>, Zhanna Mukanova<sup>3</sup>, Zhanar Oralbekova<sup>1</sup>

<sup>1</sup>Department of Computer Engineering, Astana IT University, Astana, Kazakhstan

<sup>2</sup>Faculty of Information Technology, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

<sup>3</sup>Department of Computer and Software Engineering, Turan University, Almaty, Kazakhstan

## Article Info

### Article history:

Received Jun 30, 2024

Revised Sep 6, 2024

Accepted Oct 1, 2024

### Keywords:

Brute force

Federated learning

Internet of things

Internet of things attack

Prediction

Security

Structured query language injection

## ABSTRACT

The internet of things (IoT) encompasses various devices for monitoring, data collection, tracking people and assets, and interacting with other gadgets without human intervention. Implementing a system for predicting the development and assessing the criticality of detected attacks is essential for ensuring security in IoT interactions. This work analyses existing methods for detecting attacks, including machine learning, deep learning, and ensemble methods, and explores the federated learning (FL) method. The aim is to study FL to enhance security, develop a methodology for predicting the development of attacks, and assess their criticality in real-time. FL enables devices and the aggregation server to jointly train a common global model while keeping the original data locally on each client. We demonstrate the performance of the proposed methodology against structured query language (SQL) injection and brute force attacks using the CICIOT2023 dataset. We used accuracy and F1 score metrics to evaluate the effectiveness of our proposed methodology. As a result, the accuracy in predicting SQL injection reached 100%, and for brute force attacks, it reached 98.25%. The high rates of experimental results clearly show that the proposed FL-based attack prediction methodology can be used to ensure security in IoT interactions.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Zhanar Oralbekova

Department of Computer Engineering, Astana IT University

Mangilik El Ave. 55/11, EXPO C.1, Astana 010000, Kazakhstan

Email: Zh.Oralbekova@astanait.edu.kz

## 1. INTRODUCTION

The internet of things (IoT) includes various devices for monitoring, collecting data, tracking people and assets, and interacting with other gadgets without human intervention. Many experts have noted the rapid development of the IoT. According to Statista, the global IoT market is expected to grow by 12.5% per year in 2024. Rapid growth is anticipated in various areas, including smart cities, healthcare, the agro-industrial sector, agriculture, and many other aspects of life where IoT continues to be deployed [1]. However, along with these great opportunities, IoT also brings security and privacy concerns. In addition, the development and implementation of the IoT should be accompanied by modern security and data protection measures. Any data analytics performed via the IoT necessitates the development of new methodologies to work within a limited computational resource. Moreover, one type of data analytics that finds states different from the norm in a system is real-time prediction and criticality assessment of detected attacks [2]–[5].

Therefore, it is important to note the increasing sophistication and number of attacks on IoT devices. Consequently, the rapid proliferation of vulnerable IoT devices and the ability of attackers to detect them have led to a steady increase in cyberattacks such as distributed denial-of-service (DDoS), phishing, spam, and click fraud. Among these cyberattacks, DDoS attacks are some of the most prominent, often originating from botnets based on vulnerable IoT devices. According to SonicWALL, the number of malware attacks in the first half of 2023 reached 77.9 million worldwide, compared with 57 million in the first half of 2022 [6]. There are different types of attacks on IoT, including physical attacks that target IoT device hardware, such as zero-day attacks, hijacking attacks, replay attacks, and data injection attacks [7], [8]. There are also denial of service, structured query language (SQL) injection, botnet attacks, DDoS attacks, man-in-the-middle attacks, malware attacks, credential attacks, firmware attacks, side-channel attacks, encryption attacks, and brute force password attacks [9]–[12]. Admittedly, the IoT has made its way into our daily lives by offering intelligent services and applications based on artificial intelligence. However, traditional artificial intelligence (AI) methods face difficulties related to the centralised management of processed data during IoT interactions. Therefore, we cannot rule out privacy issues. In this case, federated learning (FL) can help solve the problem by training AI in a distributed manner and storing data on the IoT devices themselves [13], [14].

The aim is to investigate FL for improving security by developing a technique for predicting the evolution of attacks and assessing their criticality in real-time. The major contributions of this article are as: basic machine learning methods, deep learning methods, and ensemble methods are presented; the potential of FL for improving security is analysed; and a methodology for predicting the development and assessing the criticality of detected attacks in real-time is developed. The article is structured as follows: section 2 contains the related work. Section 3 presents the research methodology, section 4 presents the proposed system for predicting the development and evaluating the criticality of detected attacks via FL, section 5 presents the experiments and results, and section 6 addresses unresolved issues and suggests new research perspectives.

## 2. RELATED WORK

There are many studies aimed at providing security for IoT devices. In this section, we review the research related to IoT attack detection via machine learning (ML) methods, deep learning (DL), and ensemble (EM) methods and note the promising use of FL. ML and DL methods often use centralised data processing techniques where there are risks regarding data privacy breaches. FL allows multiple devices to jointly train a model without sharing their raw data, increasing privacy. In addition, interest in using FL for IoT security is growing, but it is important to realise that there are still gaps in effectively applying FL to predict attacks in IoT environments.

The number of devices connected to the internet is increasing every day, offering many advantages, but it is crucial to remember that these advantages come with security issues. The IoT, which generates various types of information, can be targeted for various purposes, such as privacy breaches, identity theft, and physical damage. Attack detection is an important aspect of security in IoT interactions [15]. ML, DL, and combined methods have been successfully employed in this area. ML methods utilise algorithms to learn from historical data and identify patterns, which are then used to detect attacks [16]–[19]. As noted in studies [20]–[23], DL methods are based on neural networks and are trained on large volumes of data collected from different devices. Studies [24]–[26] highlight the use of EM that combine ML and DL models. To detect and predict attacks, a specific method is selected based on the task being solved and the available data. Table 1 presents the results of a review and analysis of the literature, showing the outcomes of applying ML, DL, and EM.

The papers in Table 1 discuss various aspects of improving security in IoT environments via innovative techniques such as ML, DL, dynamic quantization, hybrid learning models, and the integration of blockchain technology over the period from 2021 to 2024. They emphasise the importance of developing efficient, accurate, and scalable solutions to protect IoT networks from various cyber threats. Research in the area of security and privacy preservation in the interaction of IoT devices has demonstrated the successful implementation of methods for anomaly detection, attack detection, and prevention in wireless sensor networks. In this paper, we propose a method for attack prediction in the IoT using FL. FL is a machine learning method that allows training models on the devices themselves, without transmitting data to a server, which enhances data privacy [27]. Ensuring data privacy and security are critical issues for IoT devices.

To identify open questions and current issues related to the use of FL for attack prediction, we conducted a review of scientific publications. Our search revealed an increase in the number of publications over the period 2020–2023, Figure 1. During this period, a total of 702 documents were found in the Scopus database, including 40 publications in 2020, 89 in 2021, 208 in 2022, and 365 in 2023. The search was conducted using the keywords “FL” and “IoT security”.

Table 1. A review of research papers on the application of ML/DL/EM

Paper	Purpose	Methods	Dataset	Performance
[16]	A method for detecting DOS attacks in IoT	ML → decision trees (DT), random forest (RF), support vector machine (SVM), k-nearest neighbors (kNN)	IoTID20	Accuracy
[17]	To discuss evaluating trust in data collected by IoT sensors	ML → k-means, SVM via k-means, Gaussian mixture model (GMM), propagation, SVM, multi-layer perceptron (MLP)	Intel Lab	SVM 99.7%; RF 99.9%
[18]	A platform for intrusion detection in IoT using edge computing	ML → Long short-term memory (LSTM)	BoT-IoT N-BaIoTUNSW-NB15	DT 99.9%; kNN 99.8%
[19]	An attack and anomaly detection security system	ML → KNN, SVM, DT, RF, LR, MLP (ANN)	BoT-IoT	Accuracy
[20]	A comprehensive security framework	DL → hybrid LSTM-SVM classifier	NSL-KDD	MLP 91%
[24]	The method of anomaly detection using ensemble learning was present	EL → KNN, NB, SVM, LR, MLP, Voting, Boosting, Stacking, Bagging	Edge-IIoTset2023	Accuracy 99.41%; Detection rate 99.78%; Precision 98.50%
[27]	A method for combining attack candidates using FL is proposed		CICIoT 2023	Accuracy
[28]	Presents a comprehensive framework for a collaborative intrusion detection system	ML, FL → SVM, One-class SVM, FL	BoTIoT	DT 99.9%; RF 99.9%
[29]	Solves the problem of detecting faulty nodes in a wireless sensor network (WSN)	FL → FL-DNN	CICIOT 2023	Accuracy 97%; Specificity 98%; F1-score 91%; Sensitivity 82%
[30]	An approach for intrusion detection aimed at minimizing the required computational resources is presented	Centralized learning	-	Accuracy
[31]	Presenting a realistic and complex dataset	ML → SVM	CICIoT 2023	kNN 0.85; NB 0.77;
[32]	A hybrid optimized learning model is proposed to improve security in IoT networks	ML DL-BiLSTM	CICIoT 2023	SVM 0.88; LR 0.85;
[33]	The FedDetect method detects anomalous data on-device		CICIDS 2017	MLP 0.89; Voting 0.88;
[34]	An intrusion detection framework using EL	ML → RF, DNN, MLP, LR, AdaBoost	N-BaIoT	Stacking 0.89; Boosting 0.93; Bagging 0.89
[35]	The method using DL based on intrusion detection system (IDS)	ML → MLSTM	LANDER	
[36]	A hierarchical intrusion detection model based on IoT	FL → FedDetect	IoT-23 BoT-IoT Edge-IIoT	F1-score 81%
[37]	The decentralized and asynchronous FL infrastructure	EL → AdaBoost	KDD99	TNR 91%

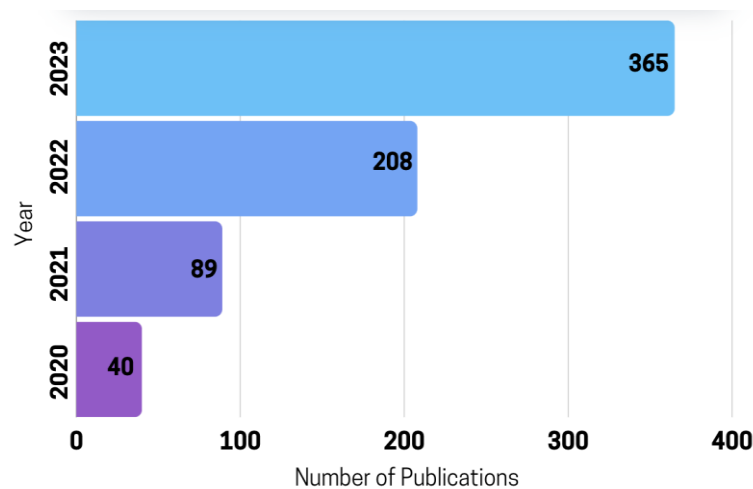


Figure 1. Growth of publications in the “Scopus” database

The annual growth of scientific publications demonstrates the promising application of FL in ensuring the security of IoT. Figure 2 presents the results of an analysis of the geographical distribution of these publications, highlighting scientific trends in the specified regions. The map uses a colour gradient from red to green, where red indicates a lower contribution and green indicates a higher contribution.

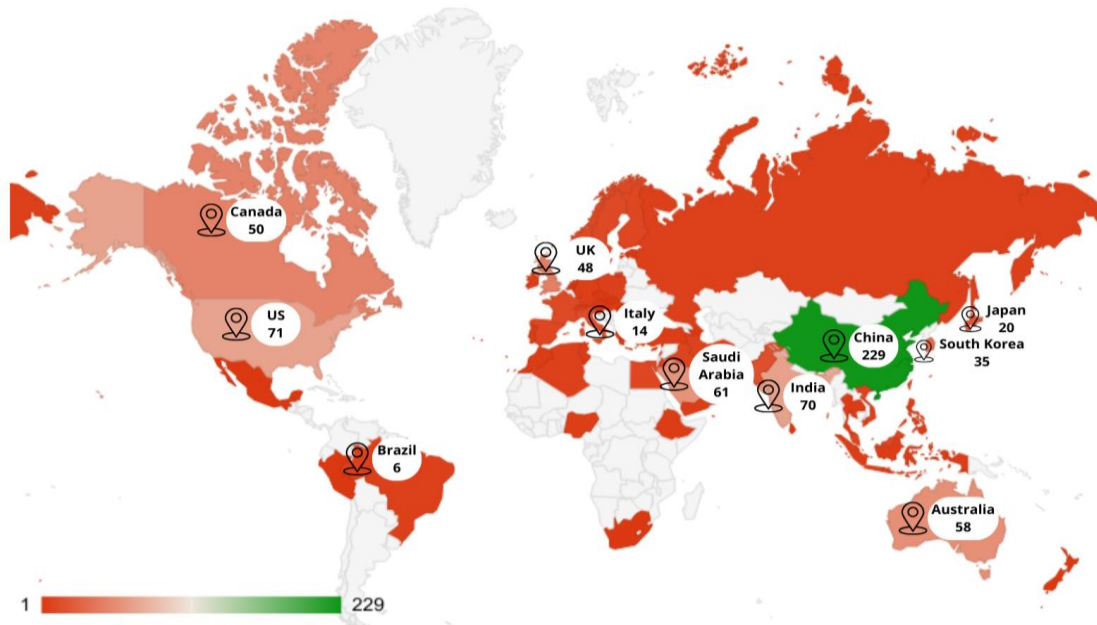


Figure 2. Geographical distribution of research papers

### 3. RESEARCH METHOD

In scientific databases, many studies related to FL for the IoT exist. In this part of our research, we present the methodology for searching and selecting the main literature to justify the relevance of our work. The key literature has focused on FL applications in IoT security, particularly on preserving data privacy while detecting attacks. Importantly, there are still unresolved issues related to data poisoning and attack patterns.

To date, researchers and practitioners have developed various approaches to protect data privacy in IoT systems. The approaches include the use of firewalls, intrusion detection systems, and other artificial intelligence solutions. Subsections of artificial intelligence, such as ML, DL, and FL have been proposed to address data privacy issues and predict potential threats in IoT interactions.

Our methodology for selecting the most relevant scientific publications for the literature review, as illustrated in Figure 3, is outlined as follows. The keywords used for the search were “IoT,” “security,” “attack,” and “FL.” The study period was from 2020 to 2024. The search was conducted in the IEEE Xplore, Google Scholar, Scopus, Springer, and ScienceDirect databases. An initial search of these databases yielded 354, 8540, 399, 1086, and 1631 documents, respectively. The following selection criteria were then applied: removal of duplicate articles, availability of open access, publication in journals, indication of the study’s purpose, level of citation, and alignment of the study title with the specified research questions.

The total number of selected research articles for the literature review on the application of FL in ensuring IoT security was 43. Figure 3 illustrates the general methodology for selecting relevant articles, which consist of two main stages: an initial search and the application of strict selection criteria. As a result, we obtained a set of relevant and high-quality research papers.

Kuppili and Jaidhan [38] presented a comparison of the effectiveness of centralised and FL paradigms in the context of a regression task using simulated data in an IoT interaction. The results show that FL, when used with a ML framework, has significant potential for preserving privacy in distributed networks [38]. Javeed *et al.* [39] demonstrated a horizontal FL model to address the issue of data diversity for attack detection evaluation, as well as the performance and scalability of devices connected to the network. Their approach for efficient intrusion detection combines elements of convolutional neural networks (CNNs) and bidirectional long short-term memory (BiLSTM). The performance of this approach is compared with that of a centralised federated intrusion detection system [39].

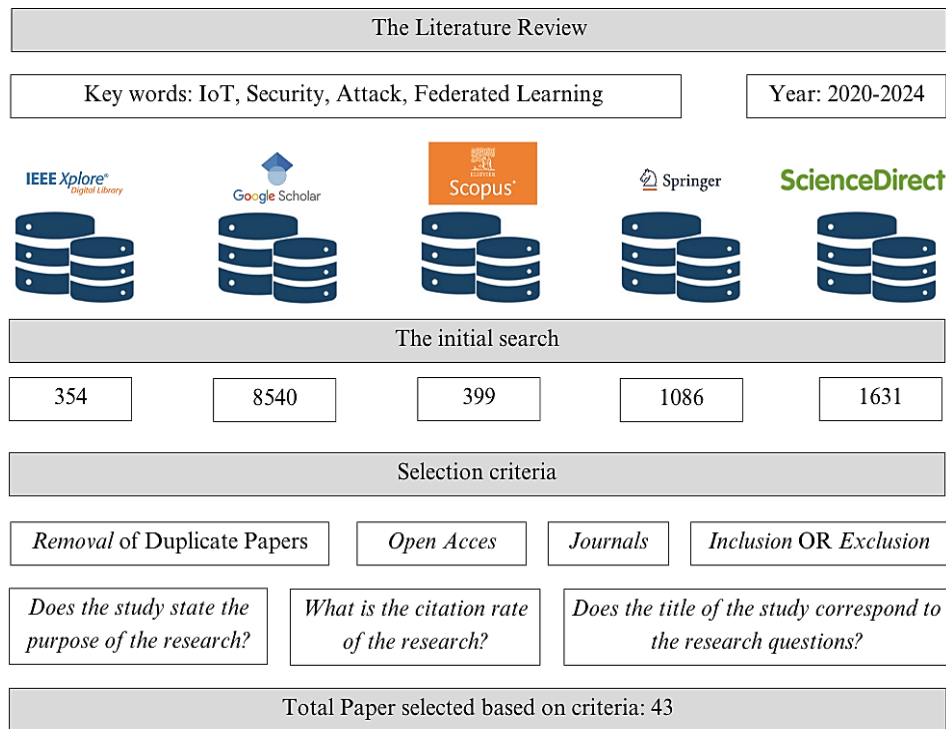


Figure 3. Process of literature review

Attota *et al.* [40] proposed a method for intrusion detection via FL, where learning was conducted in a decentralised format based on multiple perspectives of IoT network data to identify, classify, and protect against attacks. They considered the advantages of ensemble learning, particularly its ability to maximise training efficiency for various classes of attacks and the benefits of FL, where device data is processed locally. The authors compared the proposed approach with traditional centralised methods, demonstrating that the proposed approach achieves high accuracy [40]. Li *et al.* [41] reviewed major threats and challenges to the security and privacy of edge IoT data. They also discussed the concepts and principles of edge computing and FL, including the advantages and limitations of FL security models developed with different security technologies [41].

The paper by Chaurasia *et al.* [42] presents a unique approach for intrusion detection in industrial IoT networks based on ResNet and FL. This approach proposes a privacy-preserving collaborative learning framework. The experimental results demonstrate a high model accuracy of 99.16%. However, due to the limitations of the proposed approach, FL is vulnerable to attacks such as data and model poisoning. Attackers can inject corrupted data or models into the system, affecting the learning results. Additionally, the paper mentions privacy issues: although the proposed method provides greater privacy than centralised learning, it still exchanges a small portion of data to initialise a common model, which may lead to the leakage of confidential information. The authors are aware of these problems and plan to address them in the future [42].

The review paper by Gugueoth *et al.* [43] focuses on the application of ML algorithms, with an emphasis on FL and DL, for IoT security. This paper explores FL and DL methods for detecting various security threats and potential attacks on the IoT. It provides an overview of new methods and presents the results of the analysing multilevel attacks in the IoT. The open questions covered in this paper represent relevant areas for research in ensuring IoT security [43].

Yaacoub *et al.* [44] presented a comprehensive study of threats, limitations, and security, and privacy issues, and analysed the latest solutions to mitigate their impact and reduce their probability of occurrence. Several taxonomies have been proposed to explain different threats, attacks, and countermeasures for each component in FL-IoT [44]. By reviewing research studies on the application of FL for IoT security, we can recognize its great potential. Moreover, in Table 2, we present the main ideas of different studies and the limitations of various FL approaches. Additionally, as FL is still in the early stages of development, the list of reviewed works is not exhaustive but may be useful for researchers who want to learn more about FL in the internet of things.

Scientific research using FL to predict attacks in IoT has made significant progress in ensuring security and maintaining privacy. However, it is important to note that this area has not been sufficiently explored; therefore, further studies are needed to improve optimization, scalability, and practical applicability. Previous works [45], [46]–[49] have demonstrated relatively good results in ensuring the security and privacy of data in IoT via FL. Studies [49], [50], [51] have focused on developing models for detecting attacks and intrusions via FL. Proposals for optimising computational resources and increasing the efficiency of FL have been presented in studies [46]–[49], [50], [52]–[56]. To increase the reliability and security of FL, the studies [47], [48], and [51] integrate blockchain and other technologies.

Table 2. Research on FL

Paper	Main idea	Limitation
[45]	Was presented an FL property modification scheme that enhances data protection in FL by modifying data properties before data exchange	The proposed scheme may increase the computational cost due to additional data processing steps, potentially affecting the efficiency of the FL process
[50]	Was presented a Pelican optimization algorithm combined with FL for efficient attack detection in IoT environments, which improves detection accuracy and efficiency.	The performance of the proposed model may vary according to different types of IoT devices and network conditions, and its scalability in large-scale IoT networks requires further evaluation.
[52]	The integration of blockchain technology with FL and digital twins is being explored, highlighting the potential benefits of secure and efficient data management in IoT systems.	The research mainly provides a theoretical foundation and lacks empirical validation of the proposed integration in real IoT scenarios
[53]	An integrated approach to privacy-preserving learning based on data in IoT environments using fog nodes is proposed, enhancing data privacy and learning efficiency.	The proposed method requires further refinement to effectively address data imbalance and diversity issues.
[46]	A method for effective privacy-preserving FL with secure collaborative support verification is proposed.	The complexity of the structure and the potential computational load on resource-constrained IoT devices may limit its practical application.
[47]	A secure and reliable FL environment using trusted execution environments (TEE) to enhance the security and reliability of IoT applications is presented.	The use of TEE may restrict the deployment of the platform to IoT devices that support this technology, potentially reducing its versatility.
[48]	An FL framework that simultaneously preserves privacy and is resilient to chaotic errors, using a permissioned blockchain to ensure data integrity and security, is proposed.	However, implementing a permissioned blockchain may result in significant overhead in terms of processing time and computational resources, potentially affecting overall system performance.
[49]	Fed-Inforce-Fusion, a federated reinforcement model designed to enhance security and privacy in IoMT networks by providing robust protection against cyberattacks, is presented.	The use of reinforcement learning may require extensive training and computational resources, which can be challenging for resource-constrained IoT devices.
[54]	Vulnerabilities of FL models to data poisoning attacks in autonomous driving applications are explored, highlighting critical security issues.	The research focuses on a specific type of attack and application, which may limit the generalizability of its findings to other IoT use cases and attack vectors.
[55]	FedDiSC, an efficient FL computing environment designed to distinguish between power system failures and cyberattacks, enhancing reliability and security, is presented.	The effectiveness of the system may vary depending on different power system configurations and types of cyberattacks, requiring further validation in various scenarios.
[56]	A robust and resource-efficient ML method for monitoring IoT security, emphasizing a balance between performance and resource usage, is proposed.	The method may require customization for different IoT devices and environments, which could limit its out-of-the-box applicability.
[57]	A resilient FL platform using efficient encryption and the Quondam signature algorithm to enhance IoT security while minimizing energy consumption is proposed.	The reliance of the proposed platform on specific encryption and signature algorithms may limit its flexibility and applicability to other security solutions.
[58]	A federated transfer-ordered-personalized learning framework to address the above issues and tested on two real-world datasets with and without system heterogeneity is proposed.	The effectiveness of this approach in different driving conditions and driver behaviors needs further validation to ensure its reliability and adaptability.
[51]	A FL-based network intrusion detection system that improves the detection and prevention of cyberattacks in IoT networks is proposed.	The performance of the system may be affected by the quality and heterogeneity of data collected from different IoT devices, posing challenges for consistent and accurate intrusion detection.

#### 4. PROPOSED SYSTEM

In this section, we describe our FL-based approach, the dataset and its characteristics, and the evaluation metrics used in section 5 to evaluate performance. The proposed FL-based approach allows multiple devices to jointly train the model without sharing raw data, which preserves privacy and improves data security. For the experimental study, we used the CICIOT2023 dataset, which includes various attacks. The accuracy and F1 score were used to evaluate the performance of the proposed system.

### 4.1. Federated learning

Currently, FL is gaining popularity in applications for cyberspace security because it allows for collaborative learning without data leakage. FL is a decentralised approach to machine learning, where models are trained on distributed datasets stored on multiple devices [59]. Moreover, the data itself is not moved between devices; only the models are updated, which greatly improves security and privacy. One advantage of FL is that it allows for the quick development and updating of cyber defence models using information about different types of attacks (spoofing, hacking, anomalies, and DDoS) from the global network of devices. FL also provides security at the network and device levels, reducing the risk of cyberattacks.

Figure 4 shows the process of applying FL to protect against cyber threats. In the FL algorithm, the central server first provides the devices with the initial model, and then the devices train the model on their local data without revealing the data itself. In the next step, the updated model parameters are sent back to the central server. The central server then updates the model with the received parameters, and the cycle repeats; with each cycle, the model is improved. FL is a promising technology that can significantly improve cybersecurity during the IoT era.

FL is ideal for our task because it enables several clients to collaboratively train a single model without the need to share their local data. In this scenario, two clients use data attributes to construct the intended deep learning model. Initially, the client receives the data and preprocesses it to extract useful features. The clients then use the preexisting DL model.

Figure 5 shows the proposed model, which is based on a typical multilayer perceptron (MLP) architecture that has been successfully applied to classification problems. The neural network consists of six layers: one input layer, four hidden layers, and an output layer. The input layer transforms the input tensor into a flat vector [60].

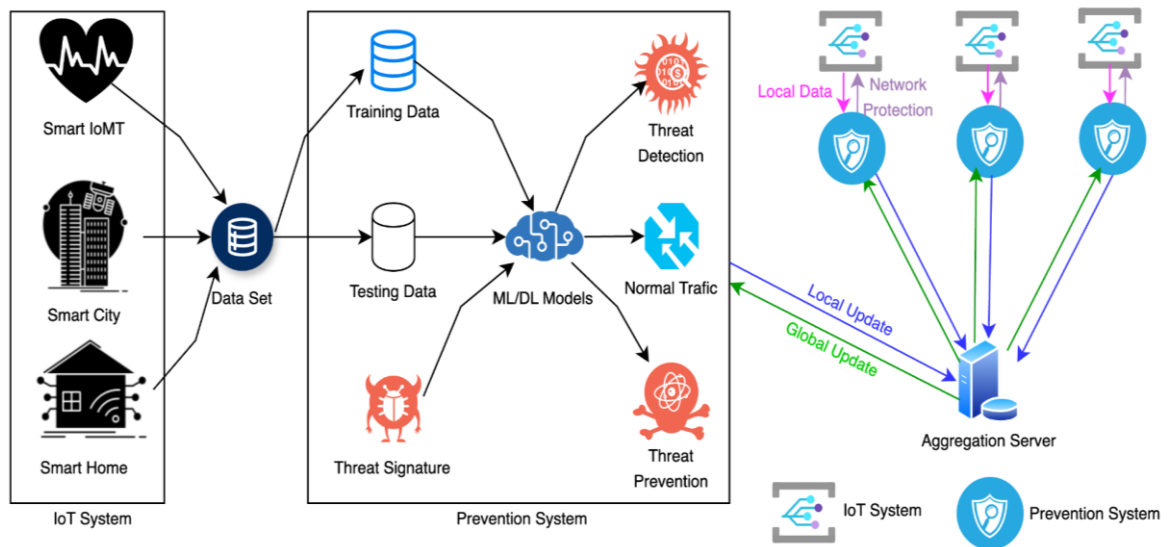


Figure 4. Methodology for using FL to defend against cyber threats

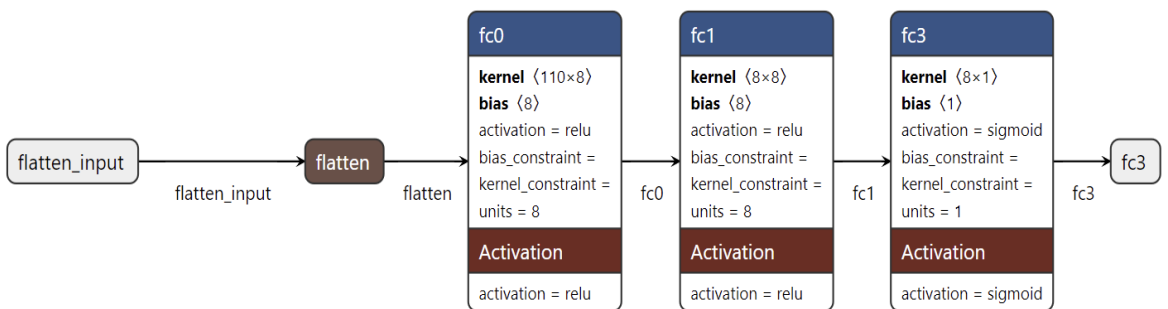


Figure 5. Layers of neural networks

Using the activation function, neural networks generate more informative feature descriptions, where the data are nonlinearly transformed. The nonlinear transformation is applied element by element to the incoming data, which is then passed to the input of the next layer. For accuracy, the correct choice of the activation function is necessary. The choice of a particular activation function depends on the specific task and how well it fits with the data. It is recommended to experiment with and test different activation functions to determine the best option for a particular case. The proposed neural network model solves the classification problem; therefore, the Softmax function was chosen as the activation function at the output layer [61]. The Softmax function generates probabilities for each class under consideration. The resulting probabilities are then used to calculate cross-entropy, which measures the model error. The rectified linear unit (ReLU) function was used as the activation function in the hidden layers of the neural network [62].

Model training takes place on a central server that aggregates information from clients and updates the model weights according to the received data. In each iteration, the model is improved by using the accuracy measure, the Adam optimizer, and binary cross-entropy as the loss function. The training is performed on 32 batches over 10 epochs, and the effectiveness of the proposed model is assessed via a 20% validation split. The validation split occurs both during and after training.

The presented process allows for the improvement of the model without disclosing the confidentiality of customer data, which is the main advantage of FL. The suggested model has been effectively applied to predict attacks in IoT interactions, demonstrating a high level of efficiency and priority in terms of security. While this subsection presents the theoretical background of the proposed model, the next subsection demonstrates the practical implementation of the model using a real dataset to address the problem of data privacy preservation through attack detection.

#### 4.2. Dataset

In part of the experimental study, the CICIOT2023 dataset, which was collected by the Canadian Cybersecurity Institute in 2023 [63], was used. Wireshark was used to monitor the network traffic, resulting in a file in “*pcap*” format. The dataset contains 46 features; normal data account for 38.3% of all the data, while the rest are abnormal data. The dataset includes various types of attacks, such as DDoS, SQL injection, brute force, and mirai. In our experimental study, two types of attacks—SQL injection and brute force—were selected [64], [65]. For each category of attack, specific scenarios were developed to cover all types of vulnerable devices. In each scenario, the attack activities were carried out via malicious IoT devices that target specific vulnerable IoT devices. For example, web-based attacks target web-enabled devices. Traditionally, IoT devices use a “login password” to connect to them. Often, most average users have no idea about security issues, and even if they change the default password, devices still have hidden coded accounts that are targeted after a leak. A brute force attack can guess the password and provide access to the device [65]. The SQL injection and brute force attacks analysed in the selected dataset have lower representativeness, which is a sign of imbalance, thereby constituting minor classes. This can cause attack prediction methods to be biased in favour of the dominant class (*e.g.* port scans), reducing their accuracy in detecting minor classes. The number of SQL injection instances in the selected dataset is 5,245, whereas the number of brute force instances is 13,064. Despite the problem of unbalanced data, we chose SQL injection and brute force attacks for our study because they are common types of attacks that can cause significant damage. We also choose a federated approach because it allows us to train the model on decentralised data collected from IoT devices. The selection of the above attack types plays an important role in ensuring the scalability of the proposed method and protecting users’ confidential data. The problem of data imbalance is addressed by applying the federated class weighting method. To better represent minor attack classes, the federated class weighting method dynamically adjusts the weights of the updated model, taking into account incoming data from different clients. As a result, we determined that the suggested method greatly enhanced our model’s accuracy in predicting minor attack types.

#### 4.3. Evaluation

The quality of the proposed system was measured via metrics such as accuracy and the F1 score. The performance on a balanced dataset is represented by accuracy, which is the proportion of correctly classified attack classes to the total number of predicted attacks. The F1 score is a measure that combines accuracy and completeness via the harmonic mean. The formulas used to compute these measurements are displayed in Table 3.

The metrics used provide a comprehensive evaluation of the proposed model’s ability to correctly identify different types of attacks, considering both accuracy and recall. By analysing these metrics, we can assess the overall performance of the proposed FL-based approach in detecting cyber attacks. The results of the study presented in section 5 were obtained using these metrics.



Table 3. Evaluation metrics

Metrics	Definition	Designation, formula
True Positive	The total number of all recordings that were categorized as an attack	$\rho$
True Negative	The total number of all recordings that are categorized as normal	$\eta$
False Positive	The total number of all recordings that were incorrectly categorized as an attack	$\xi$
False Negative	Total number of all recordings that were incorrectly categorized as benign	$\sigma$
Accuracy	The proportion of correctly categorized data	$\Lambda = \frac{\rho + \eta}{\rho + \eta + \xi + \sigma}$
Precision	The proportion of correctly categorized objects among all objects	$\theta = \frac{\rho}{\rho + \xi}$
Recall	The proportion of objects of the positive class out of all objects of the positive class	$\Pi = \frac{\rho}{\rho + \sigma}$
F1 score	The calculation of the harmonic mean between precision and recall	$\phi = 2 \times \frac{\theta \times \Pi}{\theta + \Pi}$

## 5. RESULTS AND DISCUSSION

To visually evaluate the performance of the proposed system across all clients for all rounds, loss and accuracy graphs for training and validation were plotted. For the experiment with Brute-Force attack data, round 5 yielded the best results. Figure 6 shows the accuracy and loss plots for training and validation.

The first graph in Figure 6 illustrates the change in training and validation losses with each epoch. The training and validation losses are 0.399% and 0.616%, respectively. The decrease in the training loss with each epoch demonstrates good learning properties. The validation error rate also decreases but in smaller steps. As a result, it can be argued that the model improves its predictions based on the validation sample. Importantly, if the difference between training and validation losses becomes less noticeable, this indicates the probability of overfitting in the last epochs.

Accuracy is measured as a percentage and represents the proportion of correctly classified samples. The maximum training accuracy was achieved in the last epoch and averaged 98.25%. The validation accuracy shows growth, indicating that the model continues to improve its ability to predict classes based on the validation data. Exceeding the training accuracy in the last epochs indicates the good generalisation ability of the model.

For the experiment with SQL injection data, the best results were obtained in round 2. Figure 7 shows the accuracy and loss plots for training and validation. The graph on the right in Figure 7 displays the training and validation loss curves. The training loss and validation loss are 0.062% and 0.063%, respectively. The training loss decreases significantly with each epoch, reflecting the effective training process of the model. The validation loss curve also decreases, indicating a good level of model fit to the validation data. The loss curves for both training and validation data decrease during validation, further suggesting a good model fit.

The training accuracy increases very quickly and reaches almost 100%. The validation accuracy also increases and reaches 100% at the last epoch, indicating an excellent fit of the model to the data. As a result, when predicting SQL injection and brute force attacks, the loss of training and validation data decreases with each epoch. In conclusion, the model was successfully trained. When working with brute force attacks, the loss of training and validation data was small, ultimately demonstrating a more effective model. The increase in accuracy during training and validation confirms that the model generalises well to previously unseen data. The second model achieves almost 100% accuracy, which may indicate its strong learning ability.

The second model achieves low loss and high accuracy faster, which may indicate a more efficient architecture. Both graphs of accuracy and training and validation loss graphs for the second model have smoother and more stable curves. Suggesting that the model is well-tuned and free of sharp fluctuations (*e.g.*, underestimation or overestimation of errors).

Overall, the created neural network model demonstrates high performance for the classification task under consideration. It successfully reduces loss and increases accuracy on both the training and testing data. The model used to predict brute force attacks performs at a high level, highlighting its ability to generalise and achieve excellent results with virtually no classification errors. A high score indicates a well-chosen architecture and correct model tuning for the task at hand.

The F1 score metric evaluates the model's performance in the presence of unbalanced data. The metric emphasises the accuracy of positive predictions and the identification of actual positive records. It can be used to determine how accurately the model reflects the results that matter to us. The F1 score attempts to balance precision and recall to find the harmonic mean between the two. Figure 8 shows a plot of the F1 score for all rounds for both clients. The F1 score reaches 1 in 30 rounds, indicating that the model exhibits perfect precision and recall, which is the highest quality measure for classification tasks. This means that the model not only correctly classifies most of the samples but also does so without missing any important classes, which is especially valuable in tasks requiring high accuracy.

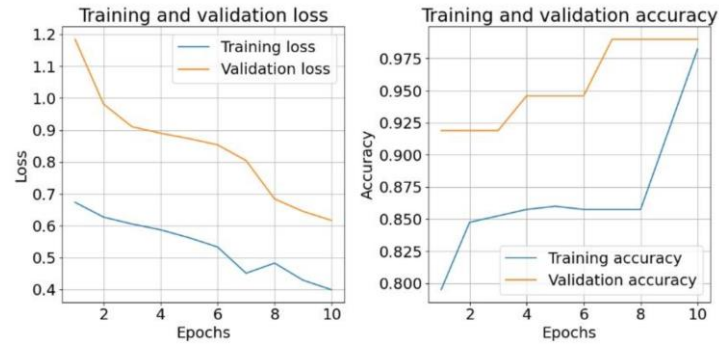


Figure 6. BruteForce training and testing results

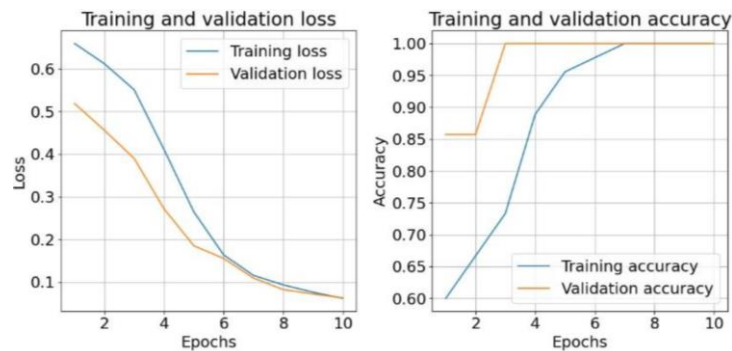


Figure 7. SQL-Injection training and testing results

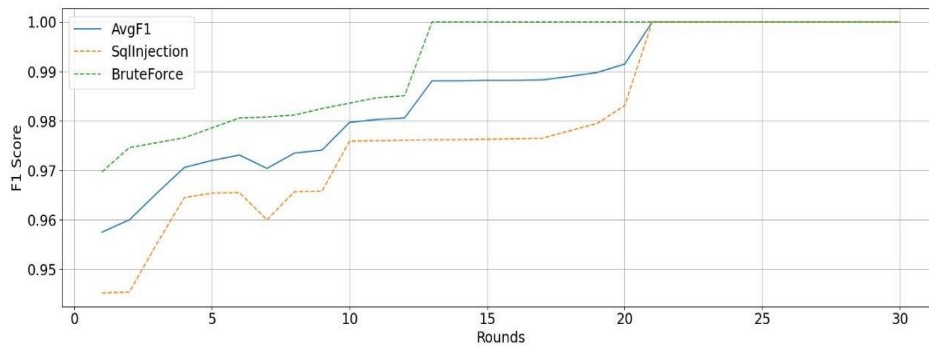


Figure 8. F1 score

## 6. CONCLUSION

FL presents a new perspective for providing a high level of security to IoT devices. This study introduced a methodology for predicting the development and assessing the criticality of detected attacks in the interaction of IoT devices. The analysis of existing methods revealed that ML techniques demonstrate high accuracy in detecting known attacks but are ineffective against new types of threats. DL methods show good resistance to new attacks but require significant computational resources and large amounts of data. Ensemble methods significantly improve the accuracy and reliability of attack detection, but they involve high computational complexity. In our study, FL was proposed as a high-quality and promising method for predicting attacks in IoT environments. FL enables the training of models on distributed data stored on IoT devices without centralised data collection, ensuring information privacy and security. The experiments demonstrate high accuracy in predicting the evolution of attacks, allowing for timely responses to cyber threats and minimising their consequences. This research represents an important step toward the development of robust cybersecurity systems for the IoT.

Further research will focus on improving the attack prediction algorithm through other FL approaches. By exploring different FL methodologies and utilising advanced ML algorithms, we aim to enhance the model's ability to predict a wide range of network attacks and adapt to various types of threats. This contributes to more resilient and secure interoperability of IoT devices.

## ACKNOWLEDGEMENTS

This research was funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP14973006).

## REFERENCES




- [1] "The tipping point: exploring the surge in IoT cyberattacks globally," *Check Point Research*, 2023. <https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the-education-sector/> (accessed Jun. 25, 2024).
- [2] N. Mishra and S. Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021, doi: 10.1109/ACCESS.2021.3073408.
- [3] M. Husak, J. Komarkova, E. Bou-Harb, and P. Celeda, "Survey of attack projection, prediction, and forecasting in cyber security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 640–660, 2019, doi: 10.1109/COMST.2018.2871866.
- [4] J. Su, S. He, and Y. Wu, "Features selection and prediction for IoT attacks," *High-Confidence Computing*, vol. 2, no. 2, Jun. 2022, doi: 10.1016/j.hcc.2021.100047.
- [5] T. Zhukabayeva *et al.*, "Towards robust security in WSN: a comprehensive analytical review and future research directions," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 36, no. 1, pp. 318–337, Oct. 2024, doi: 10.11591/ijeecs.v36.i1.pp318-337.
- [6] "Cyber threat report," *SonicWall*, 2024. Accessed: Jun. 25, 2024. [Online]. Available: <https://marlincomms.co.uk/wp-content/uploads/2024/03/SonicWall-Marlin-Cybersecurity-Threat-Report-compressed.pdf>
- [7] A. Alrefaei and M. Ilyas, "Using machine learning multiclass classification technique to detect IoT attacks in real time," *Sensors*, vol. 24, no. 14, Jul. 2024, doi: 10.3390/s24144516.
- [8] T. Zhukabayeva, A. Adamova, K. Ven-Tsen, Z. Nurlan, Y. Mardenov, and N. Karabayev, "Network attack detection using neuroevolution of augmenting topologies (NEAT) algorithm," *JOIV: International Journal on Informatics Visualization*, vol. 8, no. 1, Mar. 2024, doi: 10.62527/joiv.8.1.2220.
- [9] H. A. Noman and O. M. F. Abu-Sharkh, "Code injection attacks in wireless-based internet of things (IoT): a comprehensive review and practical implementations," *Sensors*, vol. 23, no. 13, Jun. 2023, doi: 10.3390/s23136067.
- [10] A. F. Otoom, W. Eleisah, and E. E. Abdallah, "Deep learning for accurate detection of brute force attacks on IoT networks," *Procedia Computer Science*, vol. 220, pp. 291–298, 2023, doi: 10.1016/j.procs.2023.03.038.
- [11] O. O. Amoo, F. Osasona, A. Atadoga, B. S. Ayinla, O. A. Farayola, and T. O. Abrahams, "Cybersecurity threats in the age of IoT: A review of protective measures," *International Journal of Science and Research Archive*, vol. 11, no. 1, pp. 1304–1310, Feb. 2024, doi: 10.30574/ijrsra.2024.11.1.0217.
- [12] M. Thakur, "Cyber security threats and countermeasures in digital age," *Journal of Applied Science and Education (JASE)*, vol. 4, no. 1, pp. 1–20, 2024, doi: 10.54060/a2zjournals.jase.42.
- [13] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for internet of things: recent advances, taxonomy, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1759–1799, 2021, doi: 10.1109/COMST.2021.3090430.
- [14] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. Vincent Poor, "Federated learning for internet of things: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1622–1658, 2021, doi: 10.1109/COMST.2021.3075439.
- [15] M. Anwer, S. M. Khan, M. U. Farooq, and Waseemullah, "Attack detection in IoT using machine learning," *Engineering, Technology & Applied Science Research*, vol. 11, no. 3, pp. 7273–7278, Jun. 2021, doi: 10.48084/etasr.4202.
- [16] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms," *Sensors*, vol. 24, no. 2, Jan. 2024, doi: 10.3390/s24020713.
- [17] T. Tadj, R. Arablouei, and V. Dedeoglu, "On evaluating IoT data trust via machine learning," *Future Internet*, vol. 15, no. 9, Sep. 2023, doi: 10.3390/fi15090309.
- [18] Y. K. Saheed, O. H. Abdulganiyu, and T. A. Tchakoucht, "Modified genetic algorithm and fine-tuned long short-term memory network for intrusion detection in the internet of things networks with edge capabilities," *Applied Soft Computing*, vol. 155, Apr. 2024, doi: 10.1016/j.asoc.2024.111434.
- [19] H. Tyagi and R. Kumar, "Attack and anomaly detection in IoT networks using supervised machine learning approaches," *Revue d'Intelligence Artificielle*, vol. 35, no. 1, pp. 11–21, Feb. 2021, doi: 10.18280/ria.350102.
- [20] S. Mishra and V. K. Chaurasiya, "Hybrid deep learning algorithm for smart cities security enhancement through blockchain and internet of things," *Multimedia Tools and Applications*, vol. 83, no. 8, pp. 22609–22637, 2023, doi: 10.1007/s11042-023-16406-6.
- [21] M. A. Amanullah *et al.*, "Deep learning and big data technologies for IoT security," *Computer Communications*, vol. 151, pp. 495–517, Feb. 2020, doi: 10.1016/j.comcom.2020.01.016.
- [22] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020, doi: 10.1109/COMST.2020.2988293.
- [23] Y. Li, Y. Zuo, H. Song, and Z. Lv, "Deep learning in security of internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22133–22146, Nov. 2022, doi: 10.1109/JIOT.2021.3106898.
- [24] N. Jeffrey, Q. Tan, and J. R. Villar, "Using ensemble learning for anomaly detection in cyber-physical systems," *Electronics*, vol. 13, no. 7, Apr. 2024, doi: 10.3390/electronics13071391.
- [25] Y. Alotaibi and M. Ilyas, "Ensemble-learning framework for intrusion detection to enhance internet of things' devices security," *Sensors*, vol. 23, no. 12, Jun. 2023, doi: 10.3390/s23125568.
- [26] M. Mohy-Eddine, A. Guezzaz, S. Benkirane, M. Azrou, and Y. Farhaoui, "An ensemble learning based intrusion detection model for industrial IoT security," *Big Data Mining and Analytics*, vol. 6, no. 3, pp. 273–287, 2023, doi: 10.26599/BDMA.2022.9020032.

- [27] T. Ohtani, R. Yamamoto, and S. Ohzahata, "IDAC: federated learning-based intrusion detection using autonomously extracted anomalies in IoT," *Sensors*, vol. 24, no. 10, May 2024, doi: 10.3390/s24103218.
- [28] A. A. Wardana, G. Kołaczek, and P. Sukarno, "Lightweight, trust-managing, and privacy-preserving collaborative intrusion detection for Internet of Things," *Applied Sciences*, vol. 14, no. 10, May 2024, doi: 10.3390/app14104109.
- [29] Y. Mardenov, A. Adamova, T. Zhukabayeva, and M. Othman, "Enhancing fault detection in wireless sensor networks through support vector machines: a comprehensive study," *Journal of Robotics and Control (JRC)*, vol. 4, no. 6, pp. 868–877, Dec. 2023, doi: 10.18196/jrc.v4i6.20216.
- [30] Z. Wang, H. Chen, S. Yang, X. Luo, D. Li, and J. Wang, "A lightweight intrusion detection method for IoT based on deep learning and dynamic quantization," *PeerJ Computer Science*, vol. 9, Sep. 2023, doi: 10.7717/peerj-cs.1569.
- [31] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: a real-time dataset and benchmark for large-scale attacks in IoT environment," *Sensors*, vol. 23, no. 13, p. 5941, 2023, doi: 10.3390/s23135941.
- [32] S. Rajarajan and M. G. Kavitha, "Enhanced security for IoT networks: a hybrid optimized learning model for intrusion classification," *Sādhanā*, vol. 49, no. 2, May 2024, doi: 10.1007/s12046-024-02535-7.
- [33] T. Zhang, C. He, T. Ma, L. Gao, M. Ma, and S. Avestimehr, "Federated learning for internet of things," in *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, Nov. 2021, pp. 413–419, doi: 10.1145/3485730.3493444.
- [34] C. Hazman, A. Guezaz, S. Benkirane, and M. Azrou, "IIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning," *Cluster Computing*, vol. 26, no. 6, pp. 4069–4083, Dec. 2023, doi: 10.1007/s10586-022-03810-0.
- [35] A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, and S. A. Bahaj, "Deep learning for intrusion detection and security of internet of things (IoT): current analysis, challenges, and possible solutions," *Security and Communication Networks*, vol. 2022, pp. 1–13, Jul. 2022, doi: 10.1155/2022/4016073.
- [36] Z. Lv, L. Qiao, J. Li, and H. Song, "Deep-learning-enabled security issues in the internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9531–9538, Jun. 2021, doi: 10.1109/JIOT.2020.3007130.
- [37] L. Cui *et al.*, "Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3492–3500, May 2022, doi: 10.1109/TII.2021.3107783.
- [38] Y. K. Kuppli and B. John Jaidhan, "Federated learning for IoT: ensuring privacy and security in distributed networks," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 1s, pp. 171–179, 2024.
- [39] D. Javed, M. S. Saeed, M. Adil, P. Kumar, and A. Jolfaei, "A federated learning-based zero trust intrusion detection system for Internet of Things," *Ad Hoc Networks*, vol. 162, Sep. 2024, doi: 10.1016/j.adhoc.2024.103540.
- [40] D. C. Attota, V. Mothukuri, R. M. Parizi, and S. Pouriyeh, "An ensemble multi-view federated learning intrusion detection for IoT," *IEEE Access*, vol. 9, pp. 117734–117745, 2021, doi: 10.1109/ACCESS.2021.3107337.
- [41] H. Li, L. Ge, and L. Tian, "Survey: federated learning data security and privacy-preserving in edge-Internet of Things," *Artificial Intelligence Review*, vol. 57, no. 5, Apr. 2024, doi: 10.1007/s10462-024-10774-7.
- [42] N. Chaurasia, M. Ram, P. Verma, N. Mehta, and N. Bharot, "A federated learning approach to network intrusion detection using residual networks in industrial IoT networks," *The Journal of Supercomputing*, vol. 80, no. 13, pp. 18325–18346, Sep. 2024, doi: 10.1007/s11227-024-06153-2.
- [43] V. Gugueoth, S. Safavat, and S. Shetty, "Security of internet of things (IoT) using federated learning and deep learning — recent advancements, issues and prospects," *ICT Express*, vol. 9, no. 5, pp. 941–960, Oct. 2023, doi: 10.1016/j.ict.2023.03.006.
- [44] J.-P. A. Yaacoub, H. N. Noura, and O. Salman, "Security of federated learning with IoT systems: issues, limitations, challenges, and solutions," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 155–179, 2023, doi: 10.1016/j.iotcps.2023.04.001.
- [45] S. Xu, H. Xia, P. Liu, R. Zhang, H. Chi, and W. Gao, "FLPM: a property modification scheme for data protection in federated learning," *Future Generation Computer Systems*, vol. 154, pp. 151–159, May 2024, doi: 10.1016/j.future.2023.12.030.
- [46] A. Alamer, "A privacy-preserving federated learning with a secure collaborative for malware detection models using internet of things resources," *Internet of Things*, vol. 25, Apr. 2024, doi: 10.1016/j.iot.2023.101015.
- [47] Y. Cao, J. Zhang, Y. Zhao, P. Su, and H. Huang, "SRFL: a secure and robust federated Learning framework for IoT with trusted execution environments," *Expert Systems with Applications*, vol. 239, Apr. 2024, doi: 10.1016/j.eswa.2023.122410.
- [48] H. Kasyap and S. Tripathy, "Privacy-preserving and byzantine-robust federated learning framework using permissioned blockchain," *Expert Systems with Applications*, vol. 238, Mar. 2024, doi: 10.1016/j.eswa.2023.122210.
- [49] I. A. Khan *et al.*, "Fed-inforce-fusion: a federated reinforcement-based fusion model for security and privacy protection of IoMT networks against cyber-attacks," *Information Fusion*, vol. 101, Jan. 2024, doi: 10.1016/j.inffus.2023.102002.
- [50] F. N. Al-Wesabi *et al.*, "Pelican optimization algorithm with federated learning driven attack detection model in internet of things environment," *Future Generation Computer Systems*, vol. 148, pp. 118–127, Nov. 2023, doi: 10.1016/j.future.2023.05.029.
- [51] J. Oliveira, G. R. Filho, R. Meneguette, V. Gonçalves, D. Guidoni, and R. T. de Sousa Junior, "F-Nids - a network intrusion detection system based on federated learning." 2023, doi: 10.2139/ssrn.4469457.
- [52] K. Liu, Z. Yan, X. Liang, R. Kantola, and C. Hu, "A survey on blockchain-enabled federated learning and its prospects with digital twin," *Digital Communications and Networks*, vol. 10, no. 2, pp. 248–264, Apr. 2024, doi: 10.1016/j.dcan.2022.08.001.
- [53] M. Abdel-Basset, H. Hawash, N. Moustafa, I. Razzak, and M. Abd Elfattah, "Privacy-preserved learning from non-i.i.d data in fog-assisted IoT: a federated learning approach," *Digital Communications and Networks*, vol. 10, no. 2, pp. 404–415, Apr. 2024, doi: 10.1016/j.dcan.2022.12.013.
- [54] S. Wang, Q. Li, Z. Cui, J. Hou, and C. Huang, "Bandit-based data poisoning attack against federated learning for autonomous driving models," *Expert Systems with Applications*, vol. 227, Oct. 2023, doi: 10.1016/j.eswa.2023.120295.
- [55] M. A. Husnoo *et al.*, "FedDiSC: a computation-efficient federated learning framework for power systems disturbance and cyber attack discrimination," *Energy and AI*, vol. 14, Oct. 2023, doi: 10.1016/j.egyai.2023.100271.
- [56] I. Zakariyya, H. Kalutarage, and M. O. Al-Kadri, "Towards a robust, effective and resource efficient machine learning technique for IoT security monitoring," *Computers & Security*, vol. 133, Oct. 2023, doi: 10.1016/j.cose.2023.103388.
- [57] T. Aljrees, A. Kumar, K. U. Singh, and T. Singh, "Enhancing IoT security through a green and sustainable federated learning platform: leveraging efficient encryption and the quondam signature algorithm," *Sensors*, vol. 23, no. 19, Sep. 2023, doi: 10.3390/s23198090.
- [58] L. Yuan, L. Su, and Z. Wang, "Federated transfer-ordered-personalized learning for driver monitoring application," *IEEE Internet of Things Journal*, vol. 10, no. 20, pp. 18292–18301, Oct. 2023, doi: 10.1109/JIOT.2023.3279273.
- [59] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1–19, Mar. 2019, doi: 10.1145/3298981.
- [60] Z. Mukanova, S. Atanov, and M. Jamshidi, "Intelligent hardware-software processing of high-frequency scanning data," *Journal of Robotics and Control (JRC)*, vol. 4, no. 5, pp. 600–611, Sep. 2023, doi: 10.18196/jrc.v4i5.18915.




- [61] W. Chen, K. Bhardwaj, and R. Marculescu, "FedMAX: mitigating activation divergence for accurate and communication-efficient federated learning," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12458 LNAI, 2021, pp. 348–363.
- [62] M. Hartmann, G. Danoy, M. Alswaitti, and P. Bouvry, "JoVe-FL: a joint-embedding vertical federated learning framework," in *Proceedings of the 15th International Conference on Agents and Artificial Intelligence*, 2023, pp. 416–426, doi: 10.5220/0011802600003393.
- [63] A. I. Jony and A. K. B. Arnob, "A long short-term memory based approach for detecting cyber attacks in IoT using CIC-IoT2023 dataset," *Journal of Edge Computing*, vol. 3, no. 1, pp. 28–42, May 2024, doi: 10.55056/jec.648.
- [64] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Ethical hacking for IoT: security issues, challenges, solutions and recommendations," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 280–308, 2023, doi: 10.1016/j.iotcps.2023.04.002.
- [65] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, and R. Budiarto, "Investigating brute force attack patterns in IoT network," *Journal of Electrical and Computer Engineering*, vol. 2019, pp. 1–13, Apr. 2019, doi: 10.1155/2019/4568368.

## BIOGRAPHIES OF AUTHORS






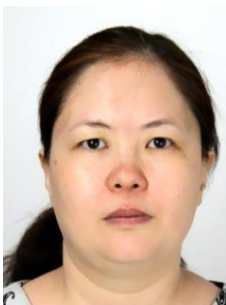
**Aigul Adamova**    received the M.S. degree in informatics from L. Gumilyov Eurasian National University, Kazakhstan, in 2006 and the Ph.D. degrees in computing and software from L.N. Gumilyov Eurasian National University, Kazakhstan, in 2016. Currently, she is a postdoctoral researcher and an assistant professor at Department of Computer Engineering, Astana IT University, Kazakhstan. She has about 40 published papers in refereed journals and conferences. She served as a reviewer for international conferences, including IEEE: SIST 2023, SIST 2024. Her research areas are information security of internet of things, wireless sensor network, embedded system, cyberphysical system, and computer vision. She can be contacted at email: aigul.adamova@astanait.edu.kz.






**Tamara Zhukabayeva**    received the Ph.D. degree from Satbayev University, Kazakhstan. She is currently an associate professor in informatics, computer engineering and management, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan. She is also an associate member of the universal association of computer and electronics engineers, has membership in scientific societies in The Society of Digital Information and Wireless Communications (SDIWC) and universal association of computer and electronics engineers. She has published over 70 scientific and educational-methodical works: in the Republic of Kazakhstan, and in countries of far and near abroad, including a foreign edition from the Clarivate analytics database, Scopus. She is the author and coauthor of educational publications and scientific monographs, has an innovative patent and copyright certificates for intellectual property rights. She can be contacted at email: tamara.kokenovna@gmail.com.



**Zhanna Mukanova**    received her bachelor's degree in informatics from E.A. Buketov Karaganda State University in 2004 and her master's degree in informatics from L.N. Gumilyov Eurasian National University in 2006. In 2021, she graduated from the PhD program of L.N. Gumilyov Eurasian National University in the specialty 6D070400-computer science and software. Her dissertation topic was "Development of software and hardware system of high-frequency scanning with intelligent data processing." She is currently a senior lecturer at the Computer and Software Engineering Department of the Digital Technologies and Art Faculty at Turan University. She has published more than 30 scientific works, including 5 copyright certificates for computer programs and 2 patents. Her research interests include artificial intelligence, robotics, and signal processing. She can be contacted at email: Zhanna.Mukanova.83@mail.ru.



**Zhanar Oralbekova**    received the B.S. and M.S. degrees in applied mathematics and informatics from Al-Farabi Kazakh National University, in 2003 and the Ph.D. degree in mathematics from the same university, in 2013. From 2005 to 2010, she was a senior teacher with Information Systems in Education Department, Abay Kazakh National Pedagogical University. Since 2014, she has been an assistant professor with the Computer and Software Engineering Department, L.N. Gumilyov Eurasian National University. Since 2023, she has been associate professor of Astana IT University. She is the author of 3 books and more than 40 articles. Her research interests include computer modeling and applications, robot technics, and ecological monitoring systems. Dr. Oralbekova's awards and honors include the Bolashak fellowship (Kazakhstan) and the ministry of education and science of the Republic of Kazakhstan Young Scientist Award for Excellence in 2014. She can be contacted at email: Zh.Oralbekova@astanait.edu.kz.