Federated Learning framework for DDoS attacks detection in smart city: a systematic review

Given Name Surname
Department. name of organization
University name
City, Country
{email address or ORCID}

Given Name Surname
Department. name of organization
University name
City, Country
{email address or ORCID}

Abstract- **Smart cities are rapidly developing in the current era, with an increasing number of residents using smart applications such as medical, transportation, environmental, education, and so on, which enables a network security weakness vividly increase a number of cyber-threats, specifically, "distributed denial of service attacks (DDoS)" has significantly increased a risk in smart city IoT applications. Numerous research have suggested a variety of approaches, including machine learning, deep learning, and optimization techniques, which offer reliable detection and mitigation solutions. However, scalability and computing expense still make it difficult. State-of-the-art attack detection across "Federated Learning (FL)" techniques, which have lately gained prominence due to the substantial advantages of safeguarding clients' personal data, are critically evaluated in this systematic review. These articles provide a thorough analysis of the FL frameworks for DDoS attack detection in smart cities from 2022 to 2025 due to the significant expansion of this subject. The key drawbacks and benefits of the suggested framework and conventional models were discussed in this study in a variety of fields, such as "Internet of Things (IoT), Internet of Vehicles (IoV), blockchain-supported privacy, and edge cloud-based collaboration systems." Our research examines detection accuracy, methodology, and model architecture designs in the different smart city contexts. Overall, we offer a critical perspective on the state of the study on this subject, emphasizing and elucidating the main obstacles that FL and conventional models must overcome. We also offer future approaches to improve the security and accuracy of detection for the upcoming generation.**

Keywords- Federated Learning, smart cities, DDoS attack, Internet of Things (IoT), traditional models

1. Introduction

Globally, surveys have shown that cities are growing in size and population. The lack of resources and infrastructure, such as healthcare, transportation, education, and the environment, was making daily living in metropolitan areas more difficult. By controlling actual storage and distribution systems, the concepts of "smart cities" were employed to extend transportable computer technology to all of the city's sectors and components. The cities were concentrating on technology for managing distributed information through "Internet of Things, cloud computing, and big data analytics" in order to become more adaptable. Congestion control, environmentally friendly resource management, citizen satisfaction, and infrastructure development are just a few of the critical aspects of smart city organizations and operations that are being improved by these data handling mechanisms in urban areas that must handle the data by creative solutions that offer long-term viability [1]. This smart city delivers an efficient and improved service for large-scale, interdependent urban property development. The occupants were receiving dynamic, intelligent, and flexible services from these institutions [2, 3]. A range of IoT devices and sensor networks are used in smart cities to create apps that are aware of their surroundings. The various smart city applications are shown in Fig. 1. In this case, the research and designs of sensor networks were vulnerable to cyber-attacks. The enormous volume of data flow was raising the possibility of security problems, such as denial-of-service attacks and data availability. Additionally, the consequences of the compromised infrastructure included data loss, unreachable sensors, potential risk to the personal information of smart city citizens, and the use of malware programs to disseminate false information [4-6]. All of these concerns were emphasized as being essential for offering effective security measures to deal with possible security issues in the presence of the internet in extensive IoT environments, which promotes resolving the dynamic attack metrics in cybersecurity. It was still difficult to identify the vulnerable DDoS attacks quickly and precisely. Traditional models were put forth in numerous studies to address this issue however they are unable to detect attacks when the traffic is hidden. Thus, the novel mitigation strategy was created using cutting-edge machine learning and optimization techniques that identify and track the real-time network changes [7-9].

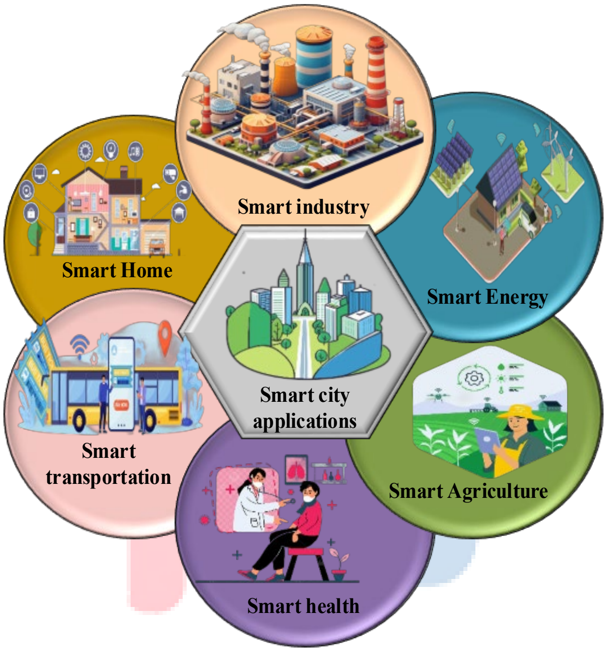


Fig.1. Smart city applications

Consequently, FL was created to address the aforementioned problems with the centralized approach [10]. "Horizontal FL, vertical FL, and federated transfer learning" were the three main categories into which FL was typically divided. Additionally, the FL is quite accurate and reliable in identifying cyber-attacks, such as "distributed denial of service (DDoS)". Because some controllers have been subjected to attack payloads while others only receive regular traffic, the aggregation methods in this FL model, such as FedAvg and weighted average, were modified to account for the different traffic intensities across diverse software-based communication networking fields. This was accomplished by using FL, which lowers the communication networks and safeguards local privacy while maintaining resistance to attack actions [11-13]. Although the FL has many benefits, such as improved DDoS detection and security, it has security flaws. For example, it only shares an updated model, which allows attackers to obtain personal information. It also lacks device capabilities, connectivity issues, and vulnerability because of malicious model changes. Additionally, some attackers are using poisoned updates to trick the global model, which has an impact on privacy and detection accuracy [14, 15].

In this study, we carried out a methodical analysis with an emphasis on the FL framework for DDoS attack detection in smart cities. In the present scenario, 2022–2025, our study integrates a thorough examination of DDoS assaults and kinds, mitigation measures, and preventative approaches gathered from the published studies. The following is a summary of this study's main goals:

- To improve security and accuracy, we examined current publications to recognize DDoS attacks with FL in smart cities.
- Examining the benefits and limitations of FL, prior studies can help address issues with smart IoT nodes.
- Traditional machine learning (ML) and deep learning (DL) model-based DDoS attack detection are compared, which highlights the difficulties mentioned in this study.
- Additionally, we made use of the model architecture DDoS attack types and smart city vulnerabilities described in this review.
- Using assessment measures, a performance analysis of all the examined research was carried out.

2. Background

Three important subjects that bolster our thesis are presented in this section. First, in recent research publications, we use DDoS assaults and their varieties in smart city environments. The architecture of the FL process modules in IoT devices is then shown. Lastly, the benefits of FL and the drawbacks of the conventional approach were also covered.

2.1 DDoS attacks and their types in smart cities

The IoT devices' ease of setup and feature extraction led to their implementation in numerous services and applications. More portable gadgets are routinely linked to the internet worldwide. Attackers are increasingly focusing on poorly configured networks and deploying DDoS assaults to destroy their data as a result. DDoS assaults have dramatically grown in recent years, according to the majority of study. In order to safeguard these gadgets, security measures and adequate defense against hackers were needed [16].

DDoS attacks in a smart city were divided into two categories: bandwidth depletion attacks and resource depletion attacks.

- **Broadband depleting assault:** By overloading the targeted networks with malicious traffic, bandwidth depletion attacks prevent users from accessing network services. "Amplification attack and Flood attack" is a subtype of this. An amplification attack occurs when an attacker sends a brief message to a server or broadcast address in the form of a spoof request. The server or broadcast addresses react with longer data than the anomalous request, which creates an amplifying circulation in the victim's direction. For instance, "Fraggle and Smurf." Then, flood assaults happen when an attacker transfers a significant volume of traffic to the target network service using a device that has been taken over, such as zombies**.**

- **Depletion of resources exploits:** These attacks prevented the victim's systems from processing, storing, or managing protocols in order to fulfill legitimate user requests. "Protocol exploitation and malformed packet attacks" are subcategories of this. PUSH+ACK, TCP SYN flood assaults, and weak signal network protocols are all used by the hijacker in this protocol manipulation attack. Additionally, by sending damaged or improperly constructed packets, malformed packet assaults confuse or crash the target. For instance, IP packet option fields and IP spoofing [13]. Fig.2 demonstrates the DDoS attack in smart cities.

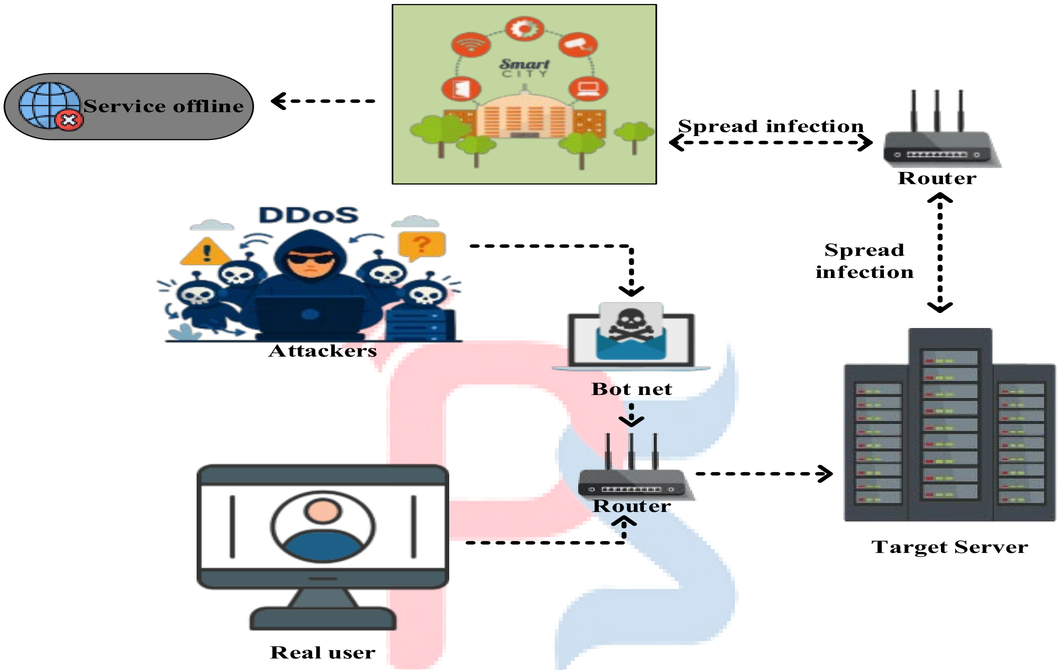
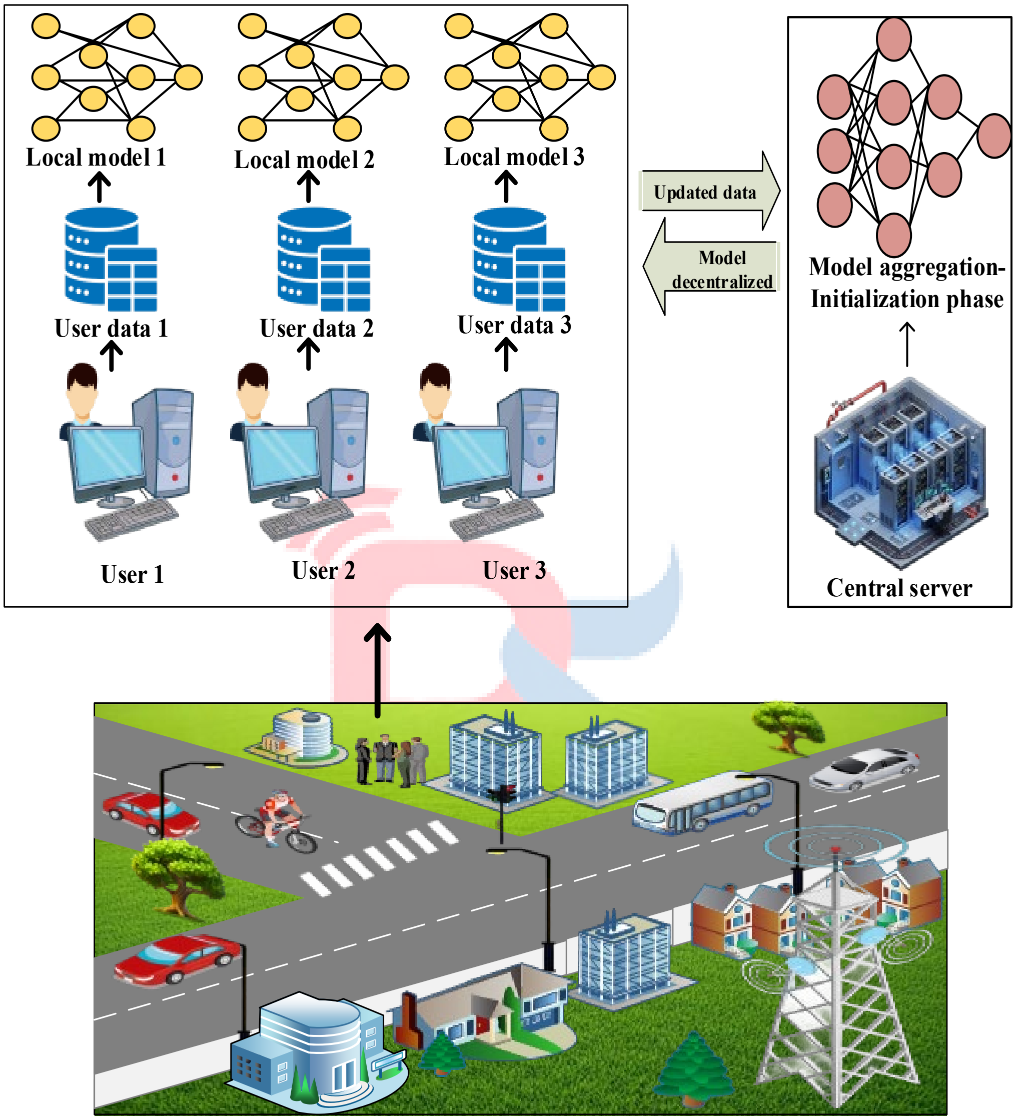


Fig.2 DDoS attack in smart city

2.2 Federated learning architecture

In order to build an initial local model for system training, each node gathered local traffic data and used that data to train its own local model. While this FL sent the nodes' model updates to centralized nodes for model accumulation, other models were sending raw data. Subsequently, the chief server integrated these changes to create an improved global model that duplicates all user data acquired. The global model was then sent back to the edge server for real-time DDoS attack detection. By eliminating the transmission of the biggest datasets, this FL procedure helps to minimize the problem of data outflow while protecting the privacy of personal information and conserving bandwidth [13]. The Fig.3 represents the federated model architecture in smart cities.



Smart city environment

Fig.3 Federated model architecture in smart cities

2.3 FL vs traditional models for DDoS attack detection

Because the FL permits training for its own data but only sends updated models to a central server, enabling distributed computing, it offers a viable answer for improving security and privacy preservation from the DDoS assault in smart cities. By not sending personal data, these decentralized devices improve data privacy preservation and lower computing resource costs. The FL's flexibility and scalability for real-time DDoS attack detection and mitigation make it ideal for decentralized IoT networks. Additionally, the efficacy of FL-based DDoS detection relied on their capacity to handle the many essential components.

The IoT devices were producing massive data streams, and the dynamic network services needed to quickly identify any new threats. However, the conventional detection approaches are centralized and vulnerable to scalability problems and single-point errors. Because the existing approaches compromise user privacy by transferring and storing important data in centralized systems. Improving the IoT security challenges impacted by malware attacks—which are made possible by FL—is required to address these problems [39].

3. Systematic Literature review

We examined recent research on identifying DDoS cyber threats in this area, which may be thoroughly discussed. A summary of the systematic literature review is shown in Table 1.

A novel "Outlier Exposure (OE)-enabled cross-silo FL framework (FedOE)" for identifying DDoS assaults in IoT devices is presented in this study [17]. Additionally, they employ a "OE-based Autoencoder (oAE)" to more effectively identify the abnormalities. An OE loss function is used to compare this encoder with the "traditional autoencoder." To show that they could generalize the 50 classified assaults at every edge level, they were assessing the OE with FedOE. When it comes to identifying the critical DDoS assaults in the IoT context, this suggested new model has a higher F1-score. Additionally, they suggested a model that needed further performance enhancement in order to effectively identify the unlabeled assaults.

In addition to applying three different gradient boosting, XGBoost, and RF models to give consumers localized and well-balanced data partitions, this study [18] attempts to use a hybrid federated principles framework for DDoS detection. The "synthetic minority oversampling technique (SMOTE)" was used in this case to lessen the imbalanced data. Additionally, they employ the "Down-sampling (Tomek links)" approach, which enhances performance and class distribution. This suggested federated approach preserves privacy and reduces communication cost by just transmitting model-updated data to aggregate rather than the complete data. Real-time attack implementation over additional network cells is guaranteed by these models. These models are remarkably accurate in identifying various DDoS attack types, such as SYN flood, HTTP GET flood, ICMP flood, UDP flood, and DNS amplification. The reported model's performance indicators were F1-score, accuracy, recall, and AUC-ROC. These measures showed that the suggested federated architecture is more accurate, minimizes latency, lowers computing cost, protects privacy, and increases the robustness of realistic threat detection in 5G networks. This suggested article does not cover the examination of privacy leaks, which impacts data privacy.

The author of [19] creates an adaptive FL model to identify DDoS assaults. In this case, the FL was a cybersecurity device solution based on an adaptive mechanism that controls the FL processes by dynamically allocating the numerous computational resources to members whose attacker profiles were more challenging to learn without requiring the sharing of tested data to monitor the performance of the trained model. The accuracy and convergence time across imbalanced data of various DDoS assaults are improved by this model, which uses a dataset of recent DDoS attacks. Additionally, while retraining the model to include new assaults on pretrained models, this suggested model exceeded resilience in a temporal scenario. While simulating the FL framework, they do not take into account potential harmful attacks on users' and servers' vital parameters, which they will take into account in their further work.

Author of [20] suggested a FL decentralized-based DDoS attack detection method that uses a convolutional neural network and DL techniques to successfully identify DDoS assaults. Data privacy was given top priority in this work by processing the data locally, which reduces the need for centralized data collecting and increases detection accuracy. The comparison reveals that the suggested federated paradigm outperforms the other alternatives for IoT networks. Nevertheless, this approach fails to attain consistent accuracy and lacks certain difficulties, processing overhead, and communication complexity.

While users produce network traffic at a low rate the author in [21] mitigates the most troublesome DDoS and their form of low-rate DDoS (LR-DDoS). They employed a weighted FL framework that identifies low-rate DDoS assaults for this purpose. These WFL models were tested using MATLAB, and the evaluation results showed that, in comparison to the other methods, their models had remarkable accuracy for LR-DDoS detection. Future work will use SDN to alleviate the inability of these models to govern IoT networks against malicious assaults.

FL for cyber security in IoT systems was suggested in this paper [22]. In order to teach the edge devices to safeguard the data, this approach guarantees decentralized data processing models across localized models. Anomaly assaults are detected by this "Gated Recurrent Unit (GRU) based recurrent neural network (RNN)." The suggested models exhibit remarkable accuracy in identifying DDoS assaults with lower computational overhead and power consumption than the conventional models, according to the experimental findings of these models. Nevertheless, this suggested model's ability to handle ultra-low energy IoT devices is restricted, and it is unable to identify sophisticated susceptible assaults in IoT settings to protect privacy.

The author of [23] focuses on recognizing the biggest assaults and utilizing a revolutionary FL strategy to produce dependable and improved performance in IoT nodes. The CIC_IoT2023 dataset was utilized in this study to detect DDoS attacks. In this case, the classification accuracy was being improved by the federated deep neural networks. In order to provide reliable fit data for classification, the models were also preprocessed using a variety of methods prior to the training stage. By using FL, the model carries out "feature normalization," "data balance," and "model prediction." Lastly, the experimental validation findings demonstrate that, in comparison to existing models, the innovative recommended technique has a remarkable DDoS attack detection accuracy. The suggested method in this novel does not examine communication overloads and privacy leaks, which are important aspects that will be taken into account in subsequent studies.

The goal of this study [24] is to identify DDoS assaults in the banking industry for financial institutions. To do this, they employ a variety of categorization models to forecast DDoS attacks with greater precision. To carry out the detection, they were gathering data from the bank. Additionally, the suggested study adds more complexity to the design of the generic models, which improves the performance of the model that is provided. "Random forest algorithms," "support vector machine (SVM)," and "K-Nearest Neighbors" models were used to carry out the categorization. Ultimately, the comparison of these various machine learning models reveals that the SVM outperforms the other KNN and RF models in terms of DDoS attack detection accuracy. This suggested model has several drawbacks that call for a more effective training procedure and significant computational energy consumption.

In order to reduce the network resources accessible to cybercriminals, the author of [25] concentrated on offering a solution for "Honeynet security tools with network slicing" capability. The IoT accessibility in 5G networks and future 6G networks is supported by this suggested solution. The precise results were obtained by evaluating the mMTC and eMBB traffic profiles using an emulated testbed. The findings of the suggested model demonstrated that a solution to the "Honeynet security tools" in the 5G network IoT smart city environment could be achieved. Additionally, the model has a significant implementation cost and computational overhead.

In this article [26], a "Gini index" for feature selection and FL for model training are used to develop a novel technique for more accurately identifying DDoS assaults. In order to increase the accuracy of the model, they chose essential elements and removed extraneous characteristics. In order to protect privacy and provide scalability, FL then made it possible for the model to be trained dispersed among a variety of devices. Ultimately, the experimental findings demonstrated that the suggested model for DDoS attack detection had remarkable accuracy and low computing cost. This method's sophisticated selection with FL offers a robust and effective answer for the IoV's contemporary cybersecurity systems. Additionally, by reducing consumption time and memory storage utilization, this study makes it possible for the lightest and quickest computers to run realistic Internet of Things applications. Additionally, they are not taking into account other important assaults that enhance the system's detection, such intrusion and anomaly detection.

In order to improve the accuracy and dependability of identifying assaults in IoT nodes, the author in [27] created a fog computing-enabled FL-based IDS that employs a DL technique called "convolutional neural networks (CNN)." This DL model was trained with improved data privacy and reduced latency guaranteed by fog computing, enabling a variety of IoT networks. They do this by using two different datasets, such as IIoT and CIC-IDS2017, which contain a variety of networks. The results of this model demonstrate its remarkable accuracy and strength in identifying susceptible DDoS assaults in Internet of Things applications. Furthermore, they suggested that in order to enhance performance, the model requires robust data handling techniques, energy-efficient systems, and adaptive learning machinery.

This study [28] use a block chain to detect DDoS assaults in IoT, enabling safe information to be disseminated by smart city applications. The relevance of the simulation in the suggested model was that it took into account a smart city and comprised a testbed of real-time IoT devices and "blockchain Ethereum." In processing these messages, the impacts of "transmission memory, time, and CPU" utilization were ascertained. Prior to being collected from IoT network data management apps, the messages were handled using the "Application programming interface sign, identify, and validation" methodology. Additionally, the model that is being provided has a problem with data leaking and lacks large-scale ecosystems.

In order to protect edge cloud settings from cyber threats including "Denial of Service (DoS), injection attacks, and DDoS," the author of [29] offers a "SecFedDNN" method that incorporates "federated deep learning approaches." The edge level pre-aggregations for the suggested SecFedDNN models were filtered using the "Layer-Adaptive Sparsified Model Aggregation," which identifies anomalous attacks and enables the well-balanced "multi-class evaluation for federated clients." Then, using the FedAvg protocol, which preserves the raw localized data, DNN was trained on several customers. Additionally, they tested the performance of the suggested DNN model using extended short-term memory. This outcome demonstrates that the suggested method outperforms other current models in terms of accuracy and computing resource costs. Advanced aggregation techniques like "Federated Proximal (FedProx) and Federated Curvature (FedCurv)," which enhance detection under shorter convergence times with varied and unbalanced data distributions, are not used by the model.

Hybrid FL and DL architecture for identifying DDoS attacks by building features on traffic data was proposed in this article [30]. This study reveals the relationship between abnormalities related to DDoS assaults and both short-term and long-term industrial traffic statistics. Additionally, they employed a "convolutional neural network (CNN)," which increased accuracy by identifying the temporal characteristics of industrial traffic. The subsequent optimization throughout FL made possible by this suggested global detection model trains the distributed data and aggregation mechanism that offers a safe environment for the data of industrial clients. Their method has a reduced convergence time and a greater accuracy, according to the model validation findings. The suggested paradigm in this study has synchronization delays and is not verified in other industrial control system situations.

In order to identify DDoS attacks, the author of [31] suggested a "distributed machine learning mechanism," sometimes known as federated machine learning. To precisely identify DDoS assaults, this suggested methodology is connected with the blockchain network. The various machine learning frameworks, such as "Random forest (RF), logistic regression (LR), and multilayer perceptron (MLP)," were used to evaluate the suggested models. According to their models' comparative results, the suggested federated machine learning combined with a blockchain network framework has outperformed previous methods in terms of DDoS attack detection accuracy. The suggested method does not mitigate the security mechanisms; it only detects the threat.

This study [32] uses a "Host Intrusion Detection and Prevention System" to identify cyber-attacks more accurately and in real time. By integrating this method with FL, the devices were able to assess the localized data and identify more unusual traffic. By employing an effective federated trained model and detection techniques across DL models, this suggested study seeks to reduce the computational burden and minimize the impact of the single point of failure. This approach offers a way to preserve data in IoT contexts and has remarkable accuracy. They suggested that although it offers numerous benefits, problems with malicious or poisoned client data updates still exist.

In order to safeguard IoT settings, the author of [33] proposed a FL framework for recognizing needless infiltration concerns. This suggested strategy uses federated training of localized data to provide a very private and secure data environment. Only updated parameters were shared by the localized IoT client data with the global server, which compiles and disseminates them to improve threat detection techniques. Every time the Fl model is trained, the clients receive updated local IoT data from the global server and use it to train their local data, protecting their personal data while improving the model as a whole. The suggested methodology performs dependably and effectively in identifying DDoS attack incursions in IoT settings with remarkable precision. The accuracy of the entire system is impacted by the suggested model's continued absence of a global model. The clients got irrelevant data, uploading and model changes were extremely sluggish, and the system had devices that were not working in the middle of the operation.

An asynchronous FL arbitration framework based on bidirectional LSTM (bi-LSTM) and attention mechanism (AsyncFL-bLAM) is used by the author in [34] to identify low-rate DDoS attacks. The leader node election algorithm" in the suggested paradigm was created to build the asynchronous FL framework. Additionally, the task of extracting the characteristics and arbiter for locally identifying low-rate DDoS attacks has been taken on by the provided bLAM. Furthermore, the bLAM models parameters are uploaded and aggregated asynchronously between the client and leader nodes using the suggested combined model. Their model has remarkable accuracy and generally lowers the communication overhead, according to the model experiment test results. The bi-LSTM and attention mechanism in the newly suggested model are computationally expensive, and the leader node has problems.

To successfully detect the infiltration, this study [35] suggests combining "horizontal FL with convolutional neural networks and bidirectional long short-term memory" models. This combination model aimed to overcome the current constraints of scalability and communication overhead while enhancing the efficacy of the FL technique in IoT nodes. In this case, the "BiLSTM model" captures the temporal and sequential patterns in the client's data while the suggested CNN model extracts the significant features. Additionally, they suggested a model that only sends the FL central server the learnt weights. By updating the aggregated models to optimize the diversified global model, this FL server increases accuracy. The experimental validations of these models show that they have effectively identified IoT device assaults. The communication overhead and computational cost have risen due to its combined FL with the CNN-BiLSTM model. Additionally, this is having scaling problems because there are so many different IoT networks.

In order to identify DDoS, DoS, and brute force cyber threats in IoT contexts, the author of [36] suggested a "optimized Isolation Forest model." In order to get improved accuracy results, they additionally employ XGBoost, SVM, LR, and RF as detecting classifiers. During the evaluation, the model's performance was assessed using "precision, recall, F1 scores, ROC curves, and precision-recall curves." Their models include data privacy and protection techniques together with a real-time anomaly detection system. They created a model that offers an IoT application solution, resulting in a safe and precise detection system. The suggested model has a problem with generalizability and requires a lot of computing resources to process. Table 2 demonstrates a comparison of overall literature survey.

Table 1
Summary of the overall literature review

References	Objectives	Advantages	Disadvantages
[17]	To emphasized crucial attacks and using various data in edge server.	• The model has higher F1-score to detect most vulnerable DDoS attacks.	• Need to improve the performance to detect unlabeled anomalies.
[18]	To using well-balanced data to identifying the cyber threats in 5G environments.	• The model achieves higher accuracy, minimal latency, and reduced computational overhead to detecting attacks in real-time 5G environments.	• Sensitive data leakage issue.
[19]	For provide the solution to dynamic cybersecurity to detecting the DDoS attacks.	• Handling the unbalanced data and providing robust real time attack detection.	• The model not addressed crucial malicious attacks.
[20]	To using decentralized method to improving the detection accuracy.	• Eliminating unnecessary data and improving the detection accuracy.	• High computational cost and communication complexity.
[21]	By mitigating the most challenged low rate DDoS attacks in IoT through FL models.	• Achieving impressive detection accuracy for low rate DDoS attacks.	• The model only detects the attacks not considered any mitigation strategies.
[22]	To ensuring secure and privacy by detecting the cyber-attacks in IoT environments	• Reducing computational overhead and energy consumption.	• Advanced cyber threats were not identified.
[23]	To developing new FL model to improving classification accuracy.	• The model has detecting the attacks with reliable and efficient performance and has impressive accuracy.	• Personal data leakage and not analysed communications overloads.
[24]	To detecting the cyber threats in banking sector by used multiple classifiers.	• Comparing diverse models to finding the higher accurately DDoS attack detection models which improving the performance.	• This model required high power consumption and better training process.

[25]	To providing a solution for Honeynet security tools to minimizing the network resources from the cyber-attacks.	• The models were provided an efficient solution to the Honeynet security tools in IoT environments.	• This has high computational overhead and deployment cost.
[26]	To developing a new model to improving the accuracy of DDoS attacks detection.	• This improving the accuracy and also, reducing consumption time and memory storage.	• The model restricted to detecting crucial attacks.
[27]	To designing the robust intrusion detection systems.	• Improving the scalability and security with efficient performance.	• Required additional mechanism and algorithms to make a feasible model.
[28]	To secure the data from the spread infection in smart city.	• Determining the transmission memory, CPU, and time while the messages were shared.	• Data leakage issue.
[29]	By combining new model to securing the edge cloud environments from DDoS attacks.	• The model has impressive accuracy and low computational resource cost	• To detecting the threats the model not used advanced aggregation models.
[30]	To creating novel combine FL and DL for cloud-edge to attack detection.	• That has lower convergence time and higher accuracy to detecting the attacks.	• Generalization inability and synchronization delay
[31]	To using novel model to detecting the attacks in IoT environments.	• The model has greater accuracy than existing approach.	• The model only providing the detection not addressing mitigation strategies.
[32]	By focusing the attacks mitigation and detection in IoT networks.	• Securing the clients data and has higher accuracy detection.	• Malicious attack and poisoned client updates were still lacking.
[33]	To developing a FL model to predicting unwanted intrusion attacks detection.	• Reliable and efficient performance and also has greater accuracy.	• The global model has issue on middle of the operation.
[34]	To designs a new model to ensuring satisfactory accurate low rate DDoS attacks.	• The models reducing the communication overheads and improving the accuracy.	• High computational cost and leader node has failed.
[35]	To design a combined model to improve the accuracy and scalability for detect attacks in IoT.	• Enhance the efficiency and accuracy to detecting the attacks higher performance.	• High computational cost and communication overhead. • Scalability issue.
[36]	To protecting the IoT devices and wireless networks by detecting anomalies.	• The model creates a safer and secured IoT environments by provide a solution to protection.	• High computational cost and generalizability issue.

Table 2

A comparison of the systematic literature survey

References	Domains	Accuracy	Precision	F1-score	Recall	Latency	cost
[17]	IoT networks	×	×	✓	×	×	×
[18]	5G networks in IoT environment	✓	✓	✓	✓	✓	✓
[19]	Cybersecurity community	✓	✓	✓	✓	×	×
[20]	IoT networks environments	✓	✓	✓	✓	×	✓
[21]	IoT networks environments	✓	✓	✓	✓	×	×
[22]	Cybersecurity framework for IoT network settings	✓	✓	✓	✓	×	✓
[23]	IoT infrastructures	✓	✓	✓	✓	×	×
[24]	Banking sector in IoT environments	✓	✓	✓	✓	×	×
[25]	Internet of Vehicles environments	✓	✓	✓	✓	✓	×
[26]	Large scale software defined network	✓	✓	✓	✓	×	×
[27]	Industrial internet of things environments.	✓	✓	✓	✓	×	×
[28]	Pre-6G smart city environments	×	×	×	×	✓	×
[29]	Edge cloud IoT environments	✓	✓	✓	✓	✓	✓
[30]	Cloud edge collaborative industrial control system	✓	✓	✓	✓	×	×
[31]	Blockchain network environment	✓	✓	✓	✓	×	×
[32]	IoT network settings	✓	×	×	×	×	×
[33]	Industrial IoT networks	✓	✓	✓	✓	×	×
[34]	Internet of things devices	✓	✓	×	✓	×	×
[35]	Internet of things (IoT) devices	✓	✓	×	✓	×	×

[36]	IoT and smart city wireless network environments	✓	✓	✓	✓	×	×

3.1 Federated Learning for DDoS attack detection in smart cities

The benefits and drawbacks of FL-based DDoS cyber threat detection in smart city settings were described.

This study [37] created a novel model and "FL-based lightweight intrusion detection systems (FL-LIDS)," which use DDoS attack detection in smart cities to offer realistic, safe client data. The optimized lightweight DL method was used in conjunction with this innovative FL-LIDS to identify the infiltration. An effective solution for smart city environments is offered by this innovative concept. The study [38] suggested a hybrid DL approach, and ResVGG-SwinNet for multi-label DDoS attack detection with FL. In Internet of Things applications, the FL model protects data privacy. These models are scalable and perform well in identifying DDoS assaults in the Internet of Things.

In order to detect and lessen DDoS assaults in IoT applications, the author in [39] suggested a decentralized FL architecture that used blockchain technology. Blockchain technology will improve the security of all data in the distribution center while also enabling people to apply FL (FL) techniques to prevent the leakage of raw data, guaranteeing data privacy. This method enhances DDoS attack detection and increases data security in smart cities. In order to improve data privacy and identify DDoS assaults, the author of [40] suggests a method based on federated and split learning. This novel method (federated/split learning) is considerably more accurate in detecting cyber-attacks and improving data privacy when compared to more conventional ML and DL.

In order to improve data security and accuracy while detecting assaults in IoT contexts, the author of [41] developed an approach based on FL. In this study, collaborative FL combines several learning levels, such as edge cloud, cloud, and device levels, to create smart services. Overall, this model performs well and increases the accuracy of DDoS attack detection. This study [42] offers state-of-the-art methods to guarantee security and privacy in many components. Among the recommended methods is FL, which improves security and the precision of attack detection. To guarantee real-time anomaly detection in smart cities, they were utilizing CNN, LSTM, and DL architecture. Additionally, they suggested "Multi-factor authentication (MFA)" as a reliable security-enabled real-time detection solution. These models have performed better than the current methods.

A FL strategy with intrusion detection systems is presented by the author in [43] to safeguard vehicle network data in Internet of Things settings. Using "Logistic regression and Convolutional neural networks" models in the Internet of Things, the ML and DL techniques are employed as classifiers to lessen the assault. To improve privacy in IoT networks, these algorithms identify various cyber threats. By utilizing the integrated DL models, "convolutional neural networks (CNNs), and long short-term memory (LSTM) networks," which identify the abnormalities, this study [44] tackles the scalability and robustness issues in real-time privacy preservation in IoT smart city networks. Additionally, they employed "FL and edge AI" to improve privacy protection while identifying cyber-attacks. In IoT smart city settings, these models provide scalable and effective immediate cyberattack detection and response.

The FL architecture was created by the author of [45] to increase the precision and effectiveness of intrusion detection in VANETs. This methodology improves the global intrusion detection system by working with SDN networks without directly sharing local data. These model trial findings demonstrate that their model performs the IDS more accurately and efficiently. An FL-based security improvement for IoT contexts is developed in this work [46]. Enhanced protection is offered by the model that detects several cyber-attacks in the IoT environment. Two different kinds of datasets are used to test this model. The test demonstrates that their model greatly improves detection accuracy. Table 4 displays the thorough analysis summery of FL based DDoS detection.

Table 3
Summary of the FL based DDoS detection

References	Objectives	Advantages	Disadvantages
[37]	To detecting the attacks in real-time with enhanced privacy and security.	• The model offering high scalable and robust security to smart cities.	• High computational overhead in edge devices and scalability issues while extensive the networks.
[38]	To using the hybrid models for detecting multi-label attacks with efficient privacy and security.	• Provide a scalable and safe DDoS attack detection for IoT devices.	• High communication overhead and computational cost issue.
[39]	To providing prevention strategies and detecting the attacks in IoT.	• Reducing the communication cost and resource consumption which increase the accuracy.	• The model required additional resources to handle the communication overhead.
[40]	To identifying anomalies for ensuring the security and privacy.	• Enabling the reliability and safety to the IoT environments devices.	• Diverse IoT data affects the model performance and communication overhead issue.
[41]	By using FL models to providing intelligent services for various learning level.	• Improving the efficient performance and accuracy.	• The model not considering the security concerns.
[42]	To providing a secure and privacy in UAV models by used FL approaches.	• This model enables higher performance and accuracy than existing methods.	• High latency and limited data for evaluation.
[43]	To enhancing security and preventing the transportation IoT environments from cyber threats.	• Enhancing the security and privacy against cyber-attacks.	• The model requiring longer training time.
[44]	To using hybrid DL and FL models to Real time DDoS attack detection in IoT driven smart city.	• Provide an enhanced security and mitigation strategies.	• High Computational overhead.
[45]	To ensure high efficient and accurate threats detection in SDN enabled IoT nodes.	• Improves the precision and adeptness of the model.	• The model lack on data resources.

[46]	To improving the detection performance and accuracy in IoT nodes.	• The model enhances the protection and accuracy.	• Diverse data sources affect the model generalization and communication.

Table 4

A comprehensive analysis for FL

References	Domains	Accuracy	Precision	F1-score	Recall	Latency	cost
[37]	Smart city environments	✓	✓	✓	✓	✓	✓
[38]	Industry wide IoT network	✓	✓	✓	✓	✓	×
[39]	IoT and smart city environment	✓	✓	×	✓	×	×
[40]	IoT cyber-attacks in smart city environment	✓	✓	✓	✓	×	×
[41]	6G networks in IoT applications	✓	×	×	×	×	×
[42]	Internet of UAVs smart city environments	✓	✓	✓	✓	×	×
[43]	Transportation IoT smart city devices	✓	×	×	×	×	×
[44]	5G enabled smart city applications	✓	✓	✓	✓	×	×
[45]	IoT networks in VANET	✓	✓	✓	✓	×	×
[46]	IoT applications	✓	×	✓	×	×	×

3.2 Traditional machine learning based DDoS attack detection in smart city

This section examines conventional machine learning techniques based on DDoS assaults in smart settings, noting their advantages and disadvantages. The Table 5 represents the summary of machine learning based DDoS detection.

A novel model for DDoS attack detection called "Adaptive Machine Learning based SDN-enabled DDoS Attacks Detection and Mitigation" is presented by the author in [47]. The methodology that was demonstrated successfully detected DDoS assaults by designing a "SDN-based security device" for IoT networks that maintained the AML standards. "Naive Bayes (NB), Random Forest (RF), Logistic Regression (LR), Support Vector Machine (SVM), and k-Nearest Neighbor (KNN)" are some of the models that use different classifiers. Lastly, testing findings demonstrate that their approach outperformed the other earlier techniques for attracting DDoS attacks. In order to provide reliable detection in large-scale networks with a challenging dataset, the author of [48] employed a machine learning technique. To identify DDoS threats in smart city IoT systems, they employed a variety of ML and DL models as classifiers. Compared to other models, their model is remarkably accurate.

ML-based attack detection techniques in smart city settings are developed in this work [49]. The intrusion detection systems architecture, fog computing, which operates in specialized modules to identify potential threats, has been integrated with the suggested machine learning model. Additionally, they employ "Deep neural networks (DNN)," a DL technique, to identify fraudulent communication within the IoT node. The findings of their suggested model showed that it performs well in identifying anomalous assaults. A very successful machine learning model to improve IoT device security was given by the author of [50]. To verify the suggested method, they employed "Message Driven-based Reinforcement Learning (MD-RL)" security of IoT Edge computing techniques. In particular, this concept offers a defense against DDoS assaults in smart cities. The findings showed that by improving attack detection accuracy and safeguarding data privacy, the proposed approach offers an effective solution for IoT networks.

In order to identify DDoS assaults in IoT-driven smart cities, this study [51] developed a "Machine learning-based ensemble technique." The security of IoT network data is therefore guaranteed by combining blockchain types. Compared to earlier classification techniques, these models have a reduced false rate and greater detection accuracy. In order to solve security problems and identify cyber threats in IoT networks, the author of [52] employs cutting-edge machine learning algorithms. The "L^2-Norm-based fuzzy model," which offers an accurate detection, identified the cyber threats. When compared to current methods, these models demonstrate effective performance in criteria including "accuracy, precision, sensitivity, and F1-score." Table 6 displays the whole analysis for machine learning.

Table 5

Summary of the machine learning based DDoS detection

References	Objectives	Advantages	Disadvantages
[47]	To using a SDN enabled ML model for reducing the communication overhead in IoT nodes.	• The models provide an efficient performance to detect the DDoS attack.	• High computational overhead and scalability issue on detecting the DDoS attack.
[48]	For enhancing the efficiency and security in IoT environment while detecting the cyber-attacks.	• The model ensures protection to the client's data and higher performance.	• The model required designed and build elements to secure the IoT nodes.
[49]	To using a ML model to detecting possible attacks in IoT with low latency.	• Improving the performance for diagnosing the traffic flow.	• Generalizability issue and not has capacity to identify the attacks.
[50]	To using collaborative detection systems to improving the accuracy.	• Reducing the false negative rate and enhancing detection accuracy.	• Lack on security key management and insecure alert communication.
[51]	By providing an efficient performance to secure the IoT environments.	• The models provide a solution to secure the IoT network.	• The model has restrict computational and capability to detect attacks.
[52]	To using a model to enhancing the security in IoT nodes.	• The model has higher accuracy and lower packet overhead than other models.	• Edge nodes restrict the process and computational resource capacity.

Table 6
A comprehensive analysis for machine learning

References	Domains	Accuracy	Precision	F1-score	Recall	Latency	cost
[47]	SDN enabled IoT environment	✓	✓	✓	✓	×	×
[48]	IoT system of smart city environment	✓	✓	✓	✓	×	×
[49]	IDs based IoT network	×	✓	✓	✓	×	×
[50]	IoT urban data node	✓	✓	✓	✓	×	×
[51]	Edge computing of IoT applications	✓	×	×	×	×	✓
[52]	IoT-driven smart city devices	✓	×	×	×	×	×

3.3 Traditional Deep learning based DDoS attack detection in smart city

This section addressed the benefits and drawbacks of the conventional deep learning architecture. In Table 7, we representing the summary of Deep learning based DDoS detection.

A DL method for detecting cyber threats in IoT settings is suggested in this study [53]. "Long short-term memory (LSTM) and feed forward neural network" are two different DL models that were employed in this. The assessment results of the suggested models demonstrate that they effectively identify various cyber-attacks, including DDoS threats, in smart cities. In [54], the author used "Long short-term memory (LSTM) and feature engineering" to create a novel IDS for IoT-driven smart city scenarios. The "tensor processing unit (TPU)" was used to evaluate their suggested model on the enhanced datasets. The comparison outcome demonstrates that their methodology is more accurate at effectively identifying assaults in IoT networks.

The author of [55] used the innovative "White Shark Equilibrium Optimizer" in conjunction with cybersecurity technologies based on "hybrid DL architecture" to identify DDoS threats in smart cities. This suggested methodology detects DDoS assaults and improves security. These models use the WSEO feature selection approach to extract the low-dimensional vector data. Additionally, they employ "stacked deep autoencoder (SDAE)" to identify the primary DDoS cyberattack in IoT nodes. The "GSA-gravitational search algorithm model" was used to adjust the model's hyperparameter. The results of their proposed model outperformed other existing techniques. A hybrid DL model is used in this study [56] to improve the accuracy of attack detection in IoT devices. The DL techniques "convolutional neural network (CNN)" and "quasi-recurrent neural network (QRNN)" were employed to identify the precise cyber threats. Two different datasets, "BoT-IoT and ToN_IoT," were used to test their models. The results of the validation test demonstrate that their model operates well and quickly lessens the dangers.

In order to identify all DDoS threats in IoT nodes, the author in [57] creates a unique DL model that combines "Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM), and Deep Autoencoder." When compared to "traditional ML and DL," these integrated models improve the accuracy of all forms of attack detection. This article [58] describes how hybrid DL models like "Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNNs), and Auto encoders" may identify DDoS attacks. In these hybrid models, CNN extracts the feature after the LSTM detects temporal danger patterns, and auto encoders compress the high-dimensional input. Their hybrid DL models perform better than the other methods, according to the model that used CICIOT2023 as a dataset during the validation procedure.

This study [59] offers an improved "two-level intrusion detection systems with long short-term memory" as a solution to the lower accuracy and scalability problem in identifying cyber-attacks in smart cities. This suggested model effectively detects assaults and identifies the kinds of sub-attacks. In order to increase efficiency, they are training and assessing the suggested models in real time using two different datasets. According to the experimental results, their model performs better than other models and has more accuracy. DDoS attacks on IoT networks are identified by the author in [60]. They improved security by using a DL-based strategy. The "CICIDS-2018 dataset" is used in this study to accurately identify the cyber threats. Compared to other models now in use, their suggested model offers a reliable attack detection system with more accuracy. Table 8 offers a thorough examination of DL. The Table 8 provides comprehensive analysis of DL.

Table 7
Summary of the deep learning based DDoS detection

References	Objectives	Advantages	Disadvantages
[53]	To preventing the IoT networks from various attacks.	• Detecting several types of attacks with higher accuracy.	• Limited robustness and performance was varying.
[54]	To design a model for detects IoT threats by smart intrusion detection system.	• The model provides better results within short time of training period.	• Inefficient classification time and worse performance.
[55]	To developing a novel WSEO-HDLCS for detects and securing the Data in smart cities.	• Detecting accurately false alarms and enabling automated mitigation strategies.	• The model requires better optimization and feature selection approaches.
[56]	To developing a hybrid models to detecting the attacks efficiently.	• Enhancing the classification accuracy and effectively analyse the attacks.	• Difficult to enabling privacy and security in real time IoT environment.
[57]	To creating a novel DL model for detecting attacks especially in fog and cloud level IoT nodes.	• The model was outperformed in accuracy, false alarm and true positive rate metrics.	• The model accuracy was not satisfactory due to model hyperparameter were not tuned.
[58]	To using a novel model to enhancing the security and dimensionality reduction.	• The model has outperformed than other existing models.	• The model not considering training time, class imbalance.

[59]	To addressing the lower accuracy and scalability in DDoS detection for IoT.	• Efficient performance and has higher accuracy.	• To detecting the attacks slowly and has scalability issue.
[60]	To ensuring networks security by zero touch networks that detecting the cyber threats.	• The model well performed to attack detection with high accuracy and robustness.	• The model need to consider real time detection

Table 8

A comprehensive analysis for deep learning

References	Domains	Accuracy	Precision	F1-score	Recall	Latency	cost
[53]	IoT smart devices	✓	✓	×	✓	✓	×
[54]	IoT driven Smart city environment	✓	✓	×	✓	×	×
[55]	Smart city environment	✓	✓	✓	✓	×	×
[56]	IoT smart city applications	✓	✓	✓	✓	×	×
[57]	Internet of things devices	✓	×	×	×	×	×
[58]	IoT networks	✓	✓	✓	✓	×	×
[59]	IoT system	✓	✓	✓	✓	×	×

4. Performance evaluation

4.1 QoS metrics:

The most popular performance metrics and confusion metrics were described in this section. It comprises True positive (TP), False positive (FP), True negative (TN), and False negative (FN) confusion measures and Accuracy, Precision, F1-score, Recall, and Mean squared error performance metrics.

4.1.1 Confusion metrics

A summary of the outcomes, known as confusion metrics, was anticipated by the categorization models and is shown below:

- **True positive (TP):** The total number of attacked sample data out of all sampled data that the assaults successfully identified was known as the true positive.

- **False Positive (FP):** This indicates that normal traffic was mistakenly identified, minimizing the needless mitigations.

- **True positive (TP):** The total number of attacked sample data out of all sampled data that the assaults successfully identified was known as the true positive.

- **False Positive (FP):** This indicates that normal traffic was mistakenly identified, minimizing the needless mitigations.

4.1.2 Performance metrics

The following metrics were commonly considered to evaluate the test validation.

- **Accuracy (*A*):** The accuracy quantifies the proportion of properly categorized numbers within the entire sample. Since the model performs better in classification, a larger accuracy ratio is taken into consideration. The calculation for this precision is as follows:

$$A = \frac{TP+TN}{TP+TN+FP+FN} \tag{1}$$

- **Precision (P):** It adds the proportion of positive categorized threats to the overall quantity of predicted assaults, indicating that the results are greater than those found by the successfully identified attacks. The following determined that.

$$\mathrm{P} = \frac{TP}{TP+FP} \tag{2}$$

- **Recall (*R*):** The overall real positive rate of attacks to all positive sample attack results is presented. This is referred to as the detection rate. The model's capacity to recognize DDoS assaults was determined by its greater recall. This has the following definition.

$$R = \frac{TP}{FP+FN} \tag{3}$$

- **F1-score (*F*):** Two criteria, such as "precision (P) and recall (R)," determine this F1-score. A model with a high F1-score has balanced, effective performance. This was ascertained as follows,

$$F = 2 \times \frac{\mathrm{P}.R}{\mathrm{P}+R} \tag{4}$$

- **Mean square error (MSE):** It is also known as the model's total loss function, which quantifies the difference between the expected output values and the actual input values. The model learning accuracy and consistency are excellent for the lower mean square error. This is computed as follows:

$$MSE = \sum(y_i - p_i)^2 n \tag{5}$$

Above mentioned equation, the y_i defined the actual values of the samples (i), and p_i represents predicted value for i. Also, n denotes total number of used samples for estimation.

4.2 Performance analysis

An analytical review based on the FL framework utilized in DDoS detection studies in smart cities is presented in this part. In this part, we highlight the widely dispersed research in a variety of smart city domains, learning methodologies, and assessment measures. This was an experimental comparison between QoS measurements and DDoS assaults based on FL. The effectiveness of many earlier studies that employed FL for DDoS detection in smart cities is assessed in this analysis.

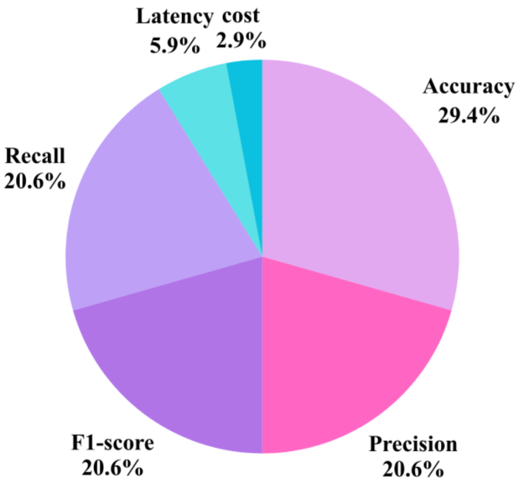


Fig.4 QoS metrics in FL based DDoS detection in smart city studies

A distribution of QoS measurements utilized by FL to identify DDoS assaults in smart city systems is shown in Fig. 4. This shows that many of the examined studies solely concentrate on an accuracy of 29.4%, while other metrics, such as "F1-score, precision, and recall," all share the same 20.6%, suggesting that current research has effective detection performance. These findings show that categorization efficiency is given precedence over organization-level considerations in the majority of the investigations. Furthermore, the criteria for cost (2.9%) and delay (5.9%) are given extremely little weight. This has an impact on the majority of current research by limiting related resources and failing to comprehensively evaluate in real time. These disparities highlight the accuracy-focused performance evaluation in recent publications. Additionally, it was unusual to test the critical elements like scalability, real-time adaptability, and communication overhead. These findings indicate that the deployment problems in large-scale smart city networks are not well covered by current research. This result highlights the need for additional QoS performance evaluation frameworks in future FL-based DDoS detection research.

5. Overall strength of Federated Learning

In particular, the federated learning frameworks provide several benefits for identifying DDoS assaults in smart cities, which are outlined below.

- **Improving data security:** By sending the revised model to the central node and storing the raw data at local nodes, personal information leakage is minimized.
- **Real-time adaptation:** The FL has adjusted to real-time DDoS patterns in order to continually update the distributed nodes.
- **Greater detection accuracy:** Compared to conventional models, the FL model's pooled information from several nodes improves the "DDoS attack detection" accuracy.
- **Reducing data transfer:** Compared to centralize model training, the FL only transmits the updated model, which lessens network overloads.
- **Resilience:** The FL model's ability to effectively identify different data from a range of domains increases the model's resilience.

6. Overall limitations of Federated Learning

The next section covered the main issues with FL frameworks for identifying DDoS assaults in large-scale smart city networks.

- **Significant computational cost:** In a smart city setting, the FL local model training involves a significant level of computer complexity.
- **Malicious Client Manipulation:** The effectiveness of DDoS attack detection is reduced when malicious attackers introduce contaminated data or mislead clients.
- **Communication overhead:** High bandwidth and latency are improved by the frequent transfers between the client and server model parameters, which results in communication overload.
- **Generalizability problems:** The local models are impacted by the different smart city environment data, which is often non-independent and identically distributed. The generalizability of many domains is delayed as a result.
- **Scalability issues:** Managing and organizing a wide variety of IoT devices in Florida was difficult. Systems experience inefficiency as a result, and the network grows due to aggregation latency.

- **Increased latency:** The server must wait for a large number of clients to report their modifications before processing the subsequent steps, which might take a considerable period of time, as the FL model was updated into the global model.

7. Conclusion & Future Work

In this study, we examined newly released studies on FL-based susceptible "DDoS attack detection" in IoT systems for smart cities. We used the DDoS attack categories and FL designs from previous studies in smart cities. In this study, we looked at a number of different methods, with an emphasis on data collecting, model training, outcomes, drawbacks, and assessment measures. These elements were utilized to offer a thorough comparison of the suggested FL to "traditional ML and DL models." This research shows that by storing the sensitive data, the FL method has successfully protected data privacy. The majority of the studies included standard assessment measures, such as "Accuracy, F1-score, precision, and recall," which emphasize FL's suitability for smart city networks. The total accuracy of the FL frameworks is 29.4%, according to this performance analysis, and each one achieves a "precision, recall, and F1-score" of 20.6%, which were mostly contributed to. However, the latency of 5.9% and the computational cost of 2.9% were not included in many studies. Some relevant areas that have been overlooked in this research are as follows: "White papers," "non-English papers," "thesis," "non-peer review papers," "chapter books," and "conference papers" with fewer than four pages. Overall, by our thorough investigation and effective evaluation, we have offered a methodical examination of a FL framework for identifying "DDoS attack" in smart cities. We looked at articles that show FL has several difficulties as well, such as high computational costs, malicious client manipulation, problems with generalizability and scalability, and communications overhead. In order to overcome these limitations, future research should be done using lightweight and adaptive FL frameworks. This will reduce the high computational cost and communication overloads, strengthen defense strategies against vulnerable attacks, and provide real-world adaptation with improved dependability, scalability, and effective performance in next-generation smart city security networks.

References

1. Lakshmi, V., & Rajkumar, S. (2025). Hybrid Ensemble FL Using SMOTE-Tomek for Efficient DDoS Detection on Constrained Edge Devices over 5G Networks. *Results in Engineering*, 107601.

2. Alshahrani, M. M. (2023). A Secure and intelligent software-defined networking framework for future smart cities to prevent DDoS Attack. *Applied Sciences*, *13*(17), 9822

3. Ali, H., Elzeki, O. M., & Elmougy, S. (2022). Smart attacks learning machine advisor system for protecting smart cities from smart threats. *Applied Sciences*, *12*(13), 6473.

4. Saveetha, D., Maragatham, G., Ponnusamy, V., & Zdravković, N. (2024). An integrated federated machine learning and blockchain framework with optimal miner selection for reliable ddos attack detection. *IEEE Access*, *12*, 127903-127915

5. Abou El Houda, Z., Brik, B., Ksentini, A., & Khoukhi, L. (2023). A MEC-based architecture to secure IoT applications using federated deep learning. *IEEE Internet of Things Magazine*, *6*(1), 60-63

6. Aslam, M., Ye, D., Tariq, A., Asad, M., Hanif, M., Ndzi, D., ... & Jilani, S. F. (2022). Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT. *Sensors*, *22*(7), 2697.

7. Priyadarshini, I. (2024). Anomaly detection of IoT cyberattacks in smart cities using FL and split learning. *Big Data and Cognitive Computing*, *8*(3), 21.

8. Babu, E. S., SrinivasaRao, B. K. N., Nayak, S. R., Verma, A., Alqahtani, F., Tolba, A., & Mukherjee, A. (2022). Blockchain-based Intrusion Detection System of IoT urban data with device authentication against DDoS attacks. *Computers and Electrical Engineering*, *103*, 108287.

9. Zia, T., Faheem, M. H., Shahzad, K., Imran, M., & Ahmed, Z. (2024). Zero-touch network security (ZTNS): A network intrusion detection system based on deep learning. *IEEE Access*.

10. Jullian, O., Otero, B., Rodriguez, E., Gutierrez, N., Antona, H., & Canal, R. (2023). Deep-learning based detection for cyber-attacks in iot networks: A distributed attack detection framework. *Journal of Network and Systems Management*, *31*(2), 33.

11. Zhukabayeva, T., Ahmad, Z., Adamova, A., Karabayev, N., Mardenov, Y., & Satybaldina, D. (2025). Penetration Testing and Machine Learning-Driven Cybersecurity Framework for IoT and Smart City Wireless Networks. *IEEE Access*.

12. Devi, M., Nandal, P., & Sehrawat, H. (2025). FL-Enabled Lightweight Intrusion Detection System for Wireless Sensor Networks: A Cybersecurity Approach Against DDoS Attacks in Smart City Environments. *Intelligent Systems with Applications*, 200553.

13. Al-Taleb, N., & Saqib, N. A. (2022). Towards a hybrid machine learning model for intelligent cyber threat identification in smart city environments. *Applied Sciences*, *12*(4), 1863.

14. Rahmati, M., & Pagano, A. (2025, July). FL-Driven Cybersecurity Framework for IoT Networks with Privacy Preserving and Real-Time Threat Detection Capabilities. In *Informatics* (Vol. 12, No. 3, p. 62). MDPI.

15. Batool, S., Aslam, M., Akpokodje, E., & Jilani, S. F. (2025). A Comprehensive Review of DDoS Detection and Mitigation in SDN Environments: Machine Learning, Deep Learning, and FL Perspectives. *Electronics*, *14*(21), 4222.

16. Jia, Y., Gu, Z., Du, L., Long, Y., Wang, Y., Li, J., & Zhang, Y. (2023). Artificial intelligence enabled cyber security defense for smart cities: A novel attack detection framework based on the MDATA model. *Knowledge-Based Systems*, *276*, 110781.

17. Aborokbah, M. M. (2024). A novel intrusion detection model for enhancing security in smart city. *IEEE Access*, *12*, 107431-107444.

18. Haque, A. B., Bhushan, B., & Dhiman, G. (2022). Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends. *Expert Systems*, *39*(5), e12753.

19. Al-Begain, K., Khan, M., Alothman, B., Joumaa, C., & Alrashed, E. (2022). A DDoS detection and prevention system for IoT devices and its application to smart home environment. *Applied Sciences*, *12*(22), 11853.

20. Rehman, T., Tariq, N., Khan, F. A., & Rehman, S. U. (2024). FFL-IDS: a FOG-Enabled FL-Based Intrusion Detection System to counter jamming and spoofing attacks for the industrial internet of things. *Sensors*, *25*(1), 10.

21. Bhavsar, M. H., Bekele, Y. B., Roy, K., Kelly, J. C., & Limbrick, D. (2024). Fl-ids: FL-based intrusion detection system using edge devices for transportation iot. *IEEe Access*, *12*, 52215-52226.

22. Ahmim, A., Maazouzi, F., Ahmim, M., Namane, S., & Dhaou, I. B. (2023). Distributed denial of service attack detection for the Internet of Things using hybrid deep learning model. *IEEE Access*, *11*, 119862-119875.

23. Reis, M. J. (2025). AI-Driven Anomaly Detection for Securing IoT Devices in 5G-Enabled Smart Cities. *Electronics*, *14*(12), 2492.

24. Rashid, M. M., Khan, S. U., Eusufzai, F., Redwan, M. A., Sabuj, S. R., & Elsharief, M. (2023). A FL-based approach for improving intrusion detection in industrial internet of things networks. *Network*, *3*(1), 158-179.

25. Ali, M. N., Imran, M., din, M. S. U., & Kim, B. S. (2023). Low rate DDoS detection using weighted FL in SDN control plane in IoT network. *Applied Sciences*, *13*(3), 1431.

26. Neto, H. N. C., Hribar, J., Dusparic, I., Mattos, D. M. F., & Fernandes, N. C. (2023). A survey on securing FL: Analysis of applications, attacks, challenges, and trends. *IEEE Access*, *11*, 41928-41953. Lakshmi, V., & Rajkumar, S. (2025).

27. Zhang, T., Gao, L., He, C., Zhang, M., Krishnamachari, B., & Avestimehr, A. S. (2022). FL for the internet of things: Applications, challenges, and opportunities. *IEEE Internet of Things Magazine*, *5*(1), 24-29.

28. Baig, Z., Syed, N., & Mohammad, N. (2022). Securing the smart city airspace: Drone cyber-attack detection through machine learning. *Future Internet*, *14*(7), 205.

29. Isma'ila, U. A., Danyaro, K. U., Muazu, A. A., & Maiwada, U. D. (2024). Review on approaches of federated modeling in anomaly-based intrusion detection for IoT devices. *IEEE Access*, *12*, 30941-30961.

30. Ghimire, B., & Rawat, D. B. (2022). Recent advances on FL for cybersecurity and cybersecurity for FL for internet of things. *IEEE Internet of Things Journal*, *9*(11), 8229-8249.

31. Alhasawi, Y., & Alghamdi, S. (2024). FL for decentralized DDoS attack detection in IoT networks. *IEEE Access*, *12*, 42357-42368.

32. Alamir, R. H., Noor, A., Almukhalfi, H., Almukhlifi, R., & Noor, T. H. (2025). SecFedDNN: A Secure Federated Deep Learning Framework for Edge–Cloud Environments. *Systems*, *13*(6), 463.

33. Javeed, D., Saeed, M. S., Adil, M., Kumar, P., & Jolfaei, A. (2024). A FL-based zero trust intrusion detection system for Internet of Things. *Ad Hoc Networks*, *162*, 103540.

34. Prazeres, N., Costa, R. L. D. C., Santos, L., & Rabadão, C. (2023). Engineering the application of machine learning in an IDS based on IoT traffic flow. *Intelligent Systems with Applications*, *17*, 200189.

35. Elsayed, R. A., Hamada, R. A., Abdalla, M. I., & Elsaid, S. A. (2023). Securing IoT and SDN systems using deep-learning based automatic intrusion detection. *Ain Shams Engineering Journal*, *14*(10), 102211.

36. Cui, J., Sun, H., Zhong, H., Zhang, J., Wei, L., Bolodurina, I., & He, D. (2023). Collaborative intrusion detection system for SDVN: A fairness federated deep learning approach. *IEEE transactions on parallel and distributed systems*, *34*(9), 2512-2528.

37. Abbas, S., Al Hejaili, A., Sampedro, G. A., Abisado, M., Almadhor, A. S., Shahzad, T., & Ouahada, K. (2023). A novel federated edge learning approach for detecting cyberattacks in IoT infrastructures. *IEEE Access*, *11*, 112189-112198.

38. Gaber, T., El-Ghamry, A., & Hassanien, A. E. (2022). Injection attack detection using machine learning for smart IoT applications. *Physical Communication*, *52*, 101685.

39. Alsamiri, J., & Alsubhi, K. (2023). FL for intrusion detection systems in internet of vehicles: A general taxonomy, applications, and future directions. *Future Internet*, *15*(12), 403.

40. Pourahmadi, V., Alameddine, H. A., Salahuddin, M. A., & Boutaba, R. (2022). Spotting anomalies at the edge: Outlier exposure-based cross-silo FL for ddos detection. *IEEE Transactions on Dependable and Secure Computing*, *20*(5), 4002-4015.

41. Islam, U., Muhammad, A., Mansoor, R., Hossain, M. S., Ahmad, I., Eldin, E. T., ... & Shafiq, M. (2022). Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. *Sustainability*, *14*(14), 8374.

42. Cao, Z., Liu, B., Gao, D., Zhou, D., Han, X., & Cao, J. (2025). A Dynamic Spatiotemporal Deep Learning Solution for Cloud–Edge Collaborative Industrial Control System Distributed Denial of Service Attack Detection. *Electronics*, *14*(9), 1843.

43. de Caldas Filho, F. L., Soares, S. C. M., Oroski, E., de Oliveira Albuquerque, R., Da Mata, R. Z. A., De Mendonça, F. L. L., & de Sousa Júnior, R. T. (2023). Botnet detection and mitigation model for IoT networks using FL. *Sensors*, *23*(14), 6305.

44. Liu, Z., Guo, C., Liu, D., & Yin, X. (2023). An asynchronous FL arbitration model for low-rate ddos attack detection. *IEEe Access*, *11*, 18448-18460.

45. Hsu, M. H., & Liu, C. C. (2025). A Decentralized Framework for the Detection and Prevention of Distributed Denial of Service Attacks Using FL and Blockchain Technology. *Engineering Proceedings*, *92*(1), 48.

46. Ntizikira, E., Lei, W., Alblehai, F., Saleem, K., & Lodhi, M. A. (2023). Secure and privacy-preserving intrusion detection and prevention in the internet of unmanned aerial vehicles. *Sensors*, *23*(19), 8077.

47. Dwivedi, A. K., & Prasad, S. K. (2024). Security Enhancement Scheduling Model for IoT-Based Smart Cities Through Machine Learning Method. *Advanced Control for Applications: Engineering and Industrial Systems*, *6*(4), e235.

48. Kumar, A., & Singh, D. (2024). Detection and prevention of DDoS attacks on edge computing of IoT devices through reinforcement learning. *International Journal of Information Technology*, *16*(3), 1365-1376.

49. Almuqren, L., Aljameel, S. S., Alqahtani, H., Alotaibi, S. S., Hamza, M. A., & Salama, A. S. (2023). A White Shark Equilibrium Optimizer with a hybrid deep-learning-based cybersecurity solution for a smart city environment. *Sensors*, *23*(17), 7370.

50. Ain, N. U., Sardaraz, M., Tahir, M., Abo Elsoud, M. W., & Alourani, A. (2025). Securing IoT networks against DDoS attacks: a hybrid deep learning approach. *Sensors*, *25*(5), 1346.

51. Kianpisheh, S., & Taleb, T. (2024). Collaborative FL for 6G with a deep reinforcement learning-based controlling mechanism: A DDoS attack detection scenario. *IEEE Transactions on Network and Service Management*, *21*(4), 4731-4749.

52. Alshdadi, A. A., Almazroi, A. A., Ayub, N., Lytras, M. D., Alsolami, E., Alsubaei, F. S., & Alharbey, R. (2025). Federated Deep Learning for Scalable and Privacy-Preserving Distributed Denial-of-Service Attack Detection in Internet of Things Networks. *Future Internet*, *17*(2), 88.

53. Saba, T., Khan, A. R., Sadad, T., & Hong, S. P. (2022). Securing the IoT system of smart city against cyber threats using deep learning. *Discrete Dynamics in Nature and Society*, *2022*(1), 1241122.

54. Escolar, A. M., Wang, Q., & Calero, J. M. A. (2024). Enhancing honeynet-based protection with network slicing for massive Pre-6G IoT Smart Cities deployments. *Journal of Network and Computer Applications*, *229*, 103918.

55. Doriguzzi-Corin, R., & Siracusa, D. (2024). FLAD: Adaptive FL for DDoS attack detection. *Computers & Security*, *137*, 103597.

56. Al Razib, M., Javeed, D., Khan, M. T., Alkanhel, R., & Muthanna, M. S. A. (2022). Cyber threats detection in smart environments using SDN-enabled DNN-LSTM hybrid framework. *IEEe Access*, *10*, 53015-53026.

57. Fotse, Y. S. N., Tchendji, V. K., & Velempini, M. (2024). FL based DDoS attacks detection in large scale software-defined network. *IEEE Transactions on Computers*.

58. Hazman, C., Guezzaz, A., Benkirane, S., & Azrour, M. (2024). Enhanced IDS with deep learning for IoT-based smart cities security. *Tsinghua Science and Technology*, *29*(4), 929-947.

59. Dilshad, M., Syed, M. H., & Rehman, S. (2025). Efficient distributed denial of service attack detection in internet of vehicles using Gini index feature selection and FL. *Future Internet*, *17*(1), 9.

60. Escolar, A. M., Wang, Q., & Calero, J. M. A. (2024). Enhancing honeynet-based protection with network slicing for massive Pre-6G IoT Smart Cities deployments. *Journal of Network and Computer Applications*, *229*, 103918.