ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN: 2454-9940 www.ijsem.org

Vol 19, Issuse.3 July 2025

COLLABORATIVE LEARNING FOR DECENTRALIZED NETWORK SECURITY: DETECTING DDOS ATTACKS

Mohammed Ibrahim Masood[1], Mohammed Waheeduddin Hussain[2], Imtiyaz Khan[3]

[1]Research Scholar, Department of CNIS, SCET, Hyderabad, Telangana
masoodibrahim4@gmail.com

[2]Professor, Department of Information Technology, SCET, Hyderabad, Telangana.
mdwaheeduddinhussain@gmail.com

[3]Professor, Department of Information Technology, SCET, Hyderabad, Telangana.
Imtiyaz.khan.7@gmail.com

ABSTRACT

Distributed Denial of Service (DDoS) assaults pose a substantial threat to the stability of Internet of Things (IoT) networks, which are rapidly developing. Traditional centralized detection methods struggle to cope adequately in the vast and heterogeneous IoT environment, prompting the investigation of decentralized options. This article describes a Federated Learning-based approach called Federated Learning for Decentralized DDoS Attack Detection (FL-DAD), which uses Convolutional Neural Networks (CNN) to efficiently detect DDoS attacks at their source. Our solution prioritizes data privacy by processing data locally, eliminating the need for central data collecting and increasing detection efficiency. FL-DAD outperforms conventional centralized detection methods when tested on the comprehensive CICIDS2017 dataset, demonstrating the potential of federated learning to improve intrusion detection systems in large-scale IoT networks by balancing data security and analytical effectiveness.

1. INTRODUCTION

The Internet of Things (IoT) represents the digital landscape's evolution, expanding beyond traditional devices such as computers and smartphones to create a linked web of ordinary things [1]. These items, equipped with sensors, software, and other technologies, communicate and exchange data with other devices and systems via the Internet. The Internet of Things (IoT) has evolved as a cornerstone of the twenty-first century digital revolution. From smart thermostats and wearable health monitors to intelligent traffic systems and enhanced production equipment, IoT integration has grown across a variety of industries [2]. Gartner predicts that by 2025, the world's connected things will exceed 30 billion [3]. This rapidly expanding network presents unprecedented prospects for personal, industrial, and societal applications. Enhanced data collecting, real-time communication, and a greatly better user experience are just a few of the many benefits IoT provides.

However, the growth of IoT devices creates a variety of dangers. The very characteristics that make IoT devices versatile—their connectivity, ease of access, and ubiquity—also make them vulnerable to threats. Of these dangers, Distributed Denial of Service (DDoS) assaults are especially dangerous [4]. These attacks include flooding a certain system, such as a website or an IoT device, with Internet traffic, rendering it inoperable. Given the decentralized nature of IoT networks, a successful DDoS attack can have catastrophic ramifications, disrupting service delivery, compromising user experience, and potentially causing significant economic losses [5], [6]. The inherent characteristics of IoT devices further exacerbate their vulnerability. These devices, often manufactured with cost-effectiveness in mind, may lack sophisticated security features [7]. Moreover, their widespread deployment across various environments, each with its unique security posture, makes establishing a unified protective framework challenging.

Traditional security techniques, particularly centralized intrusion detection systems, are well-equipped to tackle the complexities of IoT. These centralized systems frequently experience scalability challenges, failing to manage the huge data flows generated by the profusion of IoT devices. Furthermore, centralized systems create a single point of failure, making them prime targets for enemies [8]. Furthermore, sending data to a central place for analysis violates user privacy because sensitive information may be exposed during transit or storage. To solve these problems, there is an increasing interest in dispersed learning approaches, particularly Federated Learning [9]. In federated frameworks, devices, or nodes, are taught on their own data. Only the model updates, not the raw data, are transmitted to a central server for aggregation. This technique has the twin advantage of decreasing data transmission overhead while also addressing data privacy concerns. Given the decentralization of IoT networks, federated learning appears to be an excellent fit [10], [11]. Federated learning can provide real-time insights by processing

ISSN: 2454-9940 www.ijsem.org

Vol 19, Issuse.3 July 2025

data locally on IoT devices, which is critical for rapid threat identification and mitigation, such as DDoS attacks [12].

To this purpose, we present the Federated Learning for Decentralized DDoS Attack Detection (FL-DAD) technique in IoT Networks. In the suggested technique, we use Convolutional Neural Networks (CNNs) to take advantage of their ability to extract features and recognize patterns. This makes them very adept in identifying complicated patterns in network traffic, which is critical for detecting DDoS attacks in IoT contexts. Our technique attempts to detect DDoS attacks effectively by training the model at the edge, near to where the data originates, while adhering to data privacy and operational efficiency considerations. Using the CICIDS2017 dataset, a comprehensive intrusion detection benchmark, we compare the performance of the FL-DAD technique to standard centralized methods, demonstrating the benefits of our decentralized approach. The paper's key contributions include the following:

- We present a federated learning-based technique to detect decentralized DDoS attacks in IoT networks using CNN.
- Our evaluation of the FL-DAD approach on the CICIDS2017 dataset compares it to classic centralized detection methods, confirming its effectiveness and efficiency.

2. RELATED WORK

In today's digital age, IoT networks have emerged as a cornerstone, driving innovation across a wide range of industries. As these networks grow, so do the challenges of protecting them. A critical challenge to overcome is the rise of DDoS attacks, which undermine the entire foundation of IoT networks. The quest for sophisticated and adaptive DDoS detection strategies is at the heart of this part, which begins with an examination of classic techniques and concludes with the promise of federated learning to revolutionize detection. Figure 1 depicts a danger to the traditional centralized and distributed approaches as opposed to the federated learning approach.

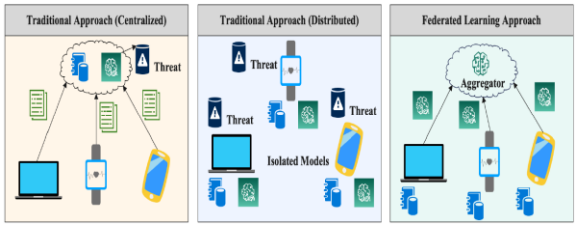

FIGURE 1. Comparison between threats in traditional and federated learning approaches.

A. Traditional DDoS Attack Detection Methods

Distributed Denial of Service (DDoS) assaults, which overwhelm targeted systems with traffic from various sources, remain one of the most serious cyber dangers. Several methodologies for countering these risks have been developed over time [13].

Signature-based Detection: Signature-based detection, one of the earliest and most straightforward ways, works by keeping a database of previously detected attack patterns, or'signatures'. As traffic enters a system, it is continuously inspected for these signatures. If a match is found, the system marks it as a possible assault. While this strategy provides rapid identification of known threats, it is fundamentally reactive. Its effectiveness is reduced against novel attack tactics that are not included in the existing database [14].

Anomaly-based Detection: Moving beyond the signature-based strategy, anomaly-based detection does not require prior knowledge of assaults. Instead, it creates a baseline for 'typical' network behavior. Network traffic is continuously monitored, and any variation from the baseline is considered suspicious. While this strategy is adaptable, it is not without limitations [15]. The dynamic nature of network behavior can occasionally cause genuine traffic to be misclassified as an attack, resulting in a greater number of false positives.

Rate-based Detection: Recognizing that many DDoS attacks overwhelm systems with an unusually large number of requests, rate-based detection was proposed [16]. This technique detects when incoming traffic exceeds a predetermined threshold. While it is adept at detecting volumetric attacks, it may miss subtler, low-volume threats.

Table 1 presents a complete description of the key focus and approaches from existing literature relevant to our research area.

B. EVOLUTION AND PRINCIPLES OF FEDERATED LEARNING

In the field of machine learning, a revolutionary technique gained traction, proposing a major shift from traditional centralized federated learning models.

- **Historical Context:** The emergence of federated learning was largely motivated by growing

concerns about data privacy and the inefficiencies of transmitting huge datasets to centralized servers[28]. It proposed an alternative: why not bring the model to the data, rather than the other way around?

- **Operational Dynamics**: In federated learning, local devices (or 'nodes') are given the power to train machine-learning models on their data. These local models are then combined into a global model, which contains insights from all participating nodes without exposing their raw data [29]. This protects data privacy and reduces the need for data transportation, which saves bandwidth [30].
- **Advantages Over Centralized Models:** Aside from the obvious advantages in data privacy and bandwidth savings, federated learning provides resilience to network faults [31], [32]. In a centralized setup, if the central server fails, the entire system fails.
- Federated learning's distributed nature makes it less vulnerable to single points of failure.

C. IOT SECURITY AND MACHINE LEARNING CONVERGENCE

The combination of IoT with machine learning is not new, but the perspective from which it is approached has shifted.

- Earlier paradigms: Historically, projects typically used centralized machine learning models. Although they partially improved IoT security, they created worries. Centralized approaches required that data from several IoT devices be transmitted to a single place for processing [33]. This raised worries about both data privacy and scalability in IoT networks (34).
- The IoT ecosystem generates massive amounts of data from billions of devices, leading to a trend towards decentralization. Processing this centrally proved increasingly unsustainable [35]. This forced a shift toward decentralized techniques, prompting academics to investigate federated learning's potential for improving IoT security.

Consider the confluence of IoT and machine learning as a journey rather than an endpoint. As attacks evolve, so must defenses, ensuring that IoT networks stay secure and robust in the face of a constantly evolving cybersecurity landscape.

3. METHODOLOGIES

Federated Learning: Concepts and Principles

A. Workings of Federated Learning:

Federated Learning (FL) is a collaborative machine learning technique in which several devices (or nodes) train on local data but only model changes, not raw data, are exchanged centrally [39]. This represents a paradigm shift away from traditional centralized learning.

The formal process can be described as follows:
Let N be the number of nodes participating in FL, each node i having a dataset Di with ni samples. Each node computes an update from its local dataset:

$$\Delta w_i = \text{Train}(D_i, w) \qquad (1)$$

where w represents the global model parameters and Δw_i represents the update from node i.

The global model is then updated by aggregating local updates:

$$w_{new} = w + \eta \sum_{i=1}^{N} \frac{n_i}{n} \Delta w_i \qquad (2)$$

where η is a learning rate and $n = \sum_{i=1}^{N} n_i$ is the total number of samples across nodes. The whole process of federated learning is depicted in Figure 2.

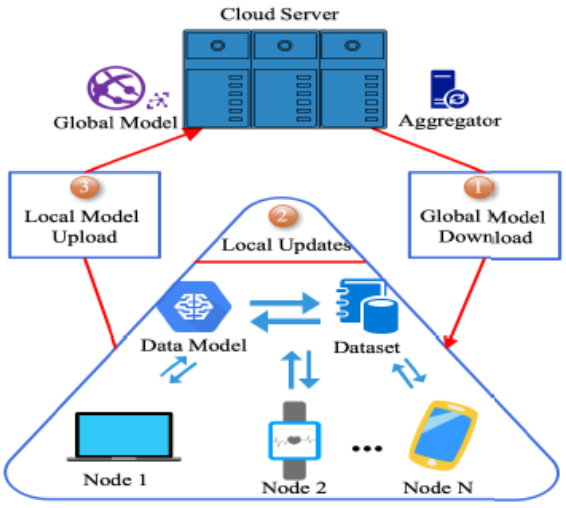

FIGURE 2. The federated learning process in IoT networks.

B. Advantages Over Centralized Models

In the context of IoT, FL brings several advantages [40]:

- **Data Privacy:** Raw data remains on the local device, reducing exposure risks.

- **Bandwidth Efficiency:** Transmitting only model updates rather than vast amounts of raw data optimizes bandwidth usage.
- **Real-time Adaptation:** Local updates allow for real-time model improvement.

Moreover, the global model is refined with diverse data, enhancing its generalization capabilities:

Generalizationerror ≤ Averagelocalerror + Divergenceterm (3)

C. Challenges in Implementing Federated Learning

Despite its benefits, implementing FL, especially in the complex IoT landscape, is not devoid of hallenges [41]:

Heterogeneity: Devices might have non-IID (Independent and Identically Distributed) data, leading to a skewed learning process. This skewness can be quantified as:

$$\text{Skewness} = \frac{\sum_{i=1}^{N}(\mu_i - \mu)^2}{N} \quad (4)$$

where μi is the local mean and μ is the global mean.

- Communication Overheads: Frequent model updates can strain limited IoT communication capabilities.
- Security Concerns: External threats might try to compromise the model's integrity through malicious updates.

4. OUR PROPOSED MODEL

A. Design of the Federated Learning-Based DDOS Detection System

Our overarching design incorporates a federated learning architecture that allows multiple IoT nodes to train localized models without centralizing data. This not only ensures data privacy but also leverages local data peculiarities to enhance detection performance.

where L(w) is the global loss, $F_i(w)$ is the local loss at node i, and $f_i(w; x_{ij}; y_{ij})$ is the training example at node i.

B. Data Collection, Preprocessing, and Distribution

Data plays a pivotal role in training robust models. In a federated environment, data remains local to each node. For our IoT-based DDoS detection:

- Data Collection: Data generated from network traffic at each IoT node is collected locally.
- Preprocessing: Data is normalized, outliers are identified and removed, and relevant features are selected to feed into the model.
- Distribution: While data remains at each node, the model updates will be communicated across the network.

C. Model Architecture and Training Strategies

We propose using a CNN model due to its proficiency in identifying patterns, which is essential for DDoS detection.

$$z^{[l]} = W^{[l]}a^{[l-1]} + b^{[l]} \quad (6)$$

$$a^{[l]} = g^{[l]}(z^{[l]}) \quad (7)$$

where $a^{[l]}$ is the activation at layer l, $W^{[l]}$ and $b^{[l]}$ are the weights and biases, and $g^{[l]}$ is the activation function. The training process in the federated environment is given in Algorithm 1:

D. MODEL AGGREGATION MECHANISMS

Post-training, model aggregation is vital to consolidate knowledge from all nodes. We use weighted averaging based on the number of samples at each node.

$$w_{global} = \frac{\sum_{i=1}^{n} n_i w_i}{\sum_{i=1}^{n} n_i} \quad (8)$$

where n_i is the number of samples at node i and w_i is the local model weight.

Algorithm 1 Federated Learning Training Procedure

Require: Initial global model weights w_0
Ensure: Updated global model weights w
Input: Initial global model weights w_0
Output: Updated global model weights w
Initialize global model weights $w \leftarrow w_0$
for each training round $t = 1, 2, \ldots, T$ **do**
  for each node i in parallel **do**
    Compute model update Δw_i using local data D_i
  end for
  Aggregate updates: $w \leftarrow w + \eta \sum_i \Delta w_i$
end for

E. COMMUNICATION PROTOCOLS FOR MODEL UPDATES

Ensuring efficient and fault-tolerant communication is paramount. Model updates are packaged and transmitted to a central server which then broadcasts the global model to all nodes [42]. During this, nodes utilize a protocol ensuring that if updates aren't received within a specified window, they'll request them again.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN: 2454-9940 www.ijsem.org

Vol 19, Issuse.3 July 2025

Algorithm 2 Model Update Communication Protocol

Require: Local model updates Δw_i from each node i
Ensure: Successful transmission of updates to central server

```
Input: Model updates Δw_i for each node i
Output: Acknowledgement of successful update transmission
for each node n do
    Transmit model updates Δw_n to the central server
    if Acknowledgement not received within timeout then
        Re-transmit model updates Δw_n
    end if
end for
```

F. EXECUTION OF FL-DAD

The intricate FL-DAD execution process is meticulously designed to integrate seamlessly with existing IoT infrastructures, thus bolstering their resilience against DDoS assaults whilst ensuring the sanctity of data privacy. The sequential stages of this methodical approach encompass:

1) Initialization: Let M_{global} be the global model. We initialize:

$$M_{global}^{(0)} \leftarrow \text{InitModel}() \quad (9)$$

where InitModel() represents the initialization function.

2) Local Model Training: For each node i, using its local dataset D_i, the node updates its local model M_i. The model is trained by optimizing a loss function L:

$$M_i^{(t)} \leftarrow \text{Train}(M_i^{(t-1)}, D_i) \quad (10)$$

where t is the current iteration. This step enables each node to independently detect potential DDoS threats based on its local data, prior to participating in the global model aggregation. However, during this phase, privacy risks emerge from the potential for sensitive information inference from model updates, necessitating the implementation of techniques such as differential privacy or homomorphic encryption to safeguard data.

3) Model Update Communication: The model update from node i can be computed as:

$$\Delta M_i^{(t)} = M_i^{(t)} - M_i^{(t-1)} \quad (11)$$

Nodes transmit $\Delta M_i^{(t)}$ to the centralized server. The pseudocode of the model update communication process is mentioned in Algorithm 2.

4) Global Model Aggregation: Aggregation at the central server is performed using the weighted sum of local model updates:

$$M_{global}^{(t)} \leftarrow M_{global}^{(t-1)} + \sum_i w_i \Delta M_i^{(t)} \quad (12)$$

where w_i is the weight assigned to node i, reflecting its reliability or the size of its local dataset. During aggregation, privacy risks are accentuated as aggregated data might inadvertently reveal information about individual nodes' data. To mitigate this, secure multi-party computation (SMPC) or federated averaging with secure aggregation protocols can be employed to ensure that the aggregated model does not expose any node's data.

5) Global Model Broadcast: Post-aggregation, $M^{(t)}_{global}$ is broadcasted to all nodes:

$$M_i^{(t)} \leftarrow M_{global}^{(t)} \quad (13)$$

for all nodes i.

6) Evaluation: Every node i evaluates $M^{(t)}_{global}$ against potential DDoS patterns using the evaluation metric E:

$$\text{Score}_i = \mathcal{E}(M_{global}^{(t)}, D_{i_{\text{test}}}) \quad (14)$$

where Ditest is the testing dataset at node i.

7) Iteration: Based on the evaluations, the process is iteratively continued:

$$t \leftarrow t + 1 \quad (15)$$

until a stopping criterion, such as a predetermined number of rounds or a desired accuracy level, is reached.

The Algorithm 3 elegantly encapsulates the FL-DAD execution process. By meticulously adhering to its procedures, IoT networks can not only fortify their defenses against DDoS threats but also ensure an unwavering commitment to data privacy.

5. RESULT

FIGURE 3 – Co-Ordinator Home Page

ISSN: 2454-9940 www.ijsem.org

Vol 19, Issuse.3 July 2025

FIGURE 4 – Behavior of network users

FIGURE 5 – Attackers Information

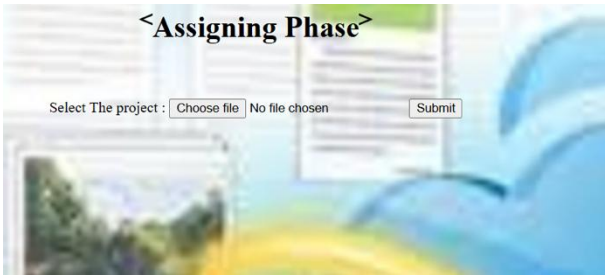

FIGURE 6 – Assigning network work to employees

FIGURE 7 – Attacker Identifier Data

Fig 3. Home Page

6. CONCLUSION AND FUTURE ENHANCEMENT

In this study, we investigated the potential of Federated Learning (FL) in improving the security landscape of Internet of Things (IoT) networks, with a specific focus on the detection of Distributed Denial of Service (DDoS) assaults. Our suggested FL-DAD methodology demonstrated the effectiveness of decentralizing the learning process, which ensures data privacy while maintaining detection accuracy. The numerical results showed that our FL-DAD approach consistently achieved an accuracy rate of more than 98% across multiple DDoS attack classes, exceeding previous centralized models. Notable findings included the system's durability in terms of accuracy even when exposed to diverse data properties among nodes, as well as its competitive advantage over centralized versions.

Furthermore, the difficulties and complexities faced, ranging from synchronization with older systems to dealing with abnormal data intricacy, cleared the path for future study possibilities. The exhibited outstanding performance, notably in terms of precision and recall, supports FL-DAD's practical application in real-world IoT security scenarios. These directions, which range from extending convergence algorithms to developing efficient aggregation protocols, will serve as the foundation for further refinement of FL-DAD.

REFERENCES

1. B. Ghimire and D. B. Rawat, "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for Internet of Things", IEEE Internet Things J., vol. 9, no. 11, pp. 8229-8249, Jun. 2022.
2. M. Pouresmaieli, M. Ataei and A. Taran, "Future mining based on Internet of Things (IoT) and sustainability challenges", Int. J. Sustain. Develop. World Ecol., vol. 30, no. 2, pp. 211-228, Feb. 2023.
3. J. Rivera and L. Goasduff, "Gartner says a thirty-fold increase in Internet-connected physical devices by 2020 will significantly alter how the supply chain operates", 2020.
4. M. H. Ali, M. M. Jaber, S. K. Abd, A. Rehman, M. J. Awan, R. Damasevicius, et al., "Threat analysis and distributed denial of service (DDoS) attack recognition in the Internet of Things (IoT)", Electronics, vol. 11, no. 3, pp. 494, Feb. 2022.
5. M. Aslam, D. Ye, A. Tariq, M. Asad, M. Hanif, D. Ndzi, et al., "Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT", Sensors, vol. 22, no. 7, pp. 2697, Mar. 2022.
6. S. A. Yousiff, R. A. Muhajjar and M. H. Al-Zubaidie, "Designing a blockchain approach to secure firefighting stations based Internet of Things", Informatica, vol. 47, no. 10, Dec. 2023.

7. L. Gerrits, "Comparative study of EOS and IOTA blockchains in the context of smart IoT for mobility", 2020.
8. M. Aslam, D. Ye, M. Hanif and M. Asad, "Machine learning based SDN-enabled distributed denial-of-services attacks detection and mitigation system for Internet of Things", Proc. 3rd Int. Conf. Mach. Learn. Cyber Secur., pp. 180-194, 2020.
9. C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li and Y. Gao, "A survey on federated learning", Knowl.-Based Syst., vol. 216, Mar. 2021.
10. M. Asad, S. Shaukat, E. Javanmardi, J. Nakazato, N. Bao and M. Tsukada, "Secure and efficient blockchain-based federated learning approach for VANETs", IEEE Internet Things J., vol. 11, no. 5, pp. 9047-9055, 2023.
11. C.-D. Lee, J.-H. Li and T.-H. Chen, "A blockchain-enabled authentication and conserved data aggregation scheme for secure smart grids", IEEE Access, vol. 11, pp. 85202-85213, 2023.
12. Q. Tian, C. Guang, C. Wenchao and W. Si, "A lightweight residual networks framework for DDoS attack classification based on federated learning", Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), pp. 1-6, May 2021.
13. P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures", Comput. Secur., vol. 127, Apr. 2023.
14. P. Szynkiewicz, "Signature-based detection of botnet DDoS attacks" in Cybersecurity of Digital Service Chains: Challenges Methodologies and Tools, Springer, pp. 120-135, 2022.
15. P. K. Kishore, S. Ramamoorthy and V. N. Rajavarman, "ARTP: Anomaly based real time prevention of distributed denial of service attacks on the web using machine learning approach", Int. J. Intell. Netw., vol. 4, pp. 38-45, Nov. 2023.
16. L. Liu, H. Wang, Z. Wu and M. Yue, "The detection method of low-rate DoS attack based on multi-feature fusion", Digit. Commun. Netw., vol. 6, no. 4, pp. 504-513, Nov. 2020.
17. V. Gaur and R. Kumar, "Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices", Arabian J. Sci. Eng., vol. 47, no. 2, pp. 1353-1374, Feb. 2022.
18. J. Li, L. Lyu, X. Liu, X. Zhang and X. Lyu, "FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT", IEEE Trans. Ind. Informat., vol. 18, no. 6, pp. 4059-4068, Jun. 2022.
19. M. Paricherla, S. Babu, K. Phasinam, H. Pallathadka, A. S. Zamani, V. Narayan, et al., "Towards development of machine learning framework for enhancing security in Internet of Things", Secur. Commun. Netw., vol. 2022, pp. 1-5, May 2022.
20. Q. Li, H. Huang, R. Li, J. Lv, Z. Yuan, L. Ma, et al., "A comprehensive survey on DDoS defense systems: New trends and challenges", Comput. Netw., vol. 233, Sep. 2023.
21. X. Feng, X. Zhu, Q.-L. Han, W. Zhou, S. Wen and Y. Xiang, "Detecting vulnerability on IoT device firmware: A survey", IEEE/CAA J. Autom. Sinica, vol. 10, no. 1, pp. 25-41, Jan. 2023.
22. M. A. Al-Shareeda, S. Manickam and M. A. Saare, "DDoS attacks detection using machine learning and deep learning techniques: Analysis and comparison", Bull. Electr. Eng. Informat., vol. 12, no. 2, pp. 930-939, Apr. 2023.
23. P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti and T.-H. Kim, "Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey", IEEE Access, vol. 10, pp. 121173-121192, 2022.
24. A. Singh, H. Kaur and N. Kaur, "A novel DDoS detection and mitigation technique using hybrid machine learning model and redirect illegitimate traffic in SDN network", Cluster Comput., pp. 1-21, Oct. 2023.
25. Y. Zhong, L. Chen, C. Dan and A. Rezaeipanah, "A systematic survey of data mining and big data analysis in Internet of Things", J. Supercomput., vol. 78, no. 17, pp. 18405-18453, Nov. 2022.
26. Z. Alarnaout, N. Mostafa, S. Alabed, W. H. F. Aly and A. Shdefat, "RAPT: A robust attack path tracing algorithm to mitigate SYN-flood DDoS cyberattacks", Sensors, vol. 23, no. 1, pp. 102, Dec. 2022.
27. A. Alotaibi and M. A. Rassam, "Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense", Future Internet, vol. 15, no. 2, pp. 62, Jan. 2023.
28. M. Aledhari, R. Razzak, R. M. Parizi and F. Saeed, "Federated learning: A survey on enabling technologies protocols and applications", IEEE Access, vol. 8, pp. 140699-140725, 2020.
29. J. Zheng, K. Li, N. Mhaisen, W. Ni, E. Tovar and M. Guizani, "Exploring deep-reinforcement-learning-assisted federated learning for online resource allocation in privacy-preserving EdgeIoT", IEEE Internet Things J., vol. 9, no. 21, pp. 21099-21110, Nov. 2022.
30. M. Asad, A. Moustafa and T. Ito, "FedOpt: Towards communication efficiency and privacy preservation in federated learning", Appl. Sci., vol. 10, no. 8, pp. 2864, Apr. 2020.
31. M. Asad, A. Moustafa, F. A. Rabhi and M. Aslam, "THF: 3-Way hierarchical framework for efficient

client selection and resource management in federated learning", IEEE Internet Things J., vol. 9, no. 13, pp. 11085-11097, Jul. 2022.
32. Q. Pan, J. Wu, A. K. Bashir, J. Li, W. Yang and Y. D. Al-Otaibi, "Joint protection of energy security and information privacy for energy harvesting: An incentive federated learning approach", IEEE Trans. Ind. Informat., vol. 18, no. 5, pp. 3473-3483, May 2022.
33. F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges", IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 1686-1721, 3rd Quart. 2020.
34. M. Asad and S. Otoum, "Towards privacy-aware federated learning for user-sensitive data", Proc. 5th Int. Conf. Blockchain Comput. Appl. (BCCA), pp. 343-350, Oct. 2023.
35. M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke and L. Shu, "Federated deep learning for cyber security in the Internet of Things: Concepts applications and experimental analysis", IEEE Access, vol. 9, pp. 138509-138542, 2021.
36. M. Aljanabi, "Navigating the void: Uncovering research gaps in the detection of data poisoning attacks in federated learning-based big data processing: A systematic literature review", Mesopotamian J. Big Data, vol. 2023, pp. 149-158, Dec. 2023.
37. S. Dange and M. Chatterjee, "IoT botnet: The largest threat to the IoT network" in Data Communication and Networks, Springer, pp. 137-157, 2019.
38. N.-N. Dao, T. V. Phan, U. Sa'ad, J. Kim, T. Bauschert, D.-T. Do, et al., "Securing heterogeneous IoT with intelligent DDoS attack behavior learning", IEEE Syst. J., vol. 16, no. 2, pp. 1974-1983, Jun. 2022.
39. M. Asad, A. Moustafa, T. Ito and M. Aslam, "Evaluating the communication efficiency in federated learning algorithms", Proc. IEEE 24th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD), pp. 552-557, May 2021.
40. M. Asad, A. Moustafa and T. Ito, "Federated learning versus classical machine learning: A convergence comparison", arXiv:2107.10976, 2021.
41. S. Abdulrahman, H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi and M. Guizani, "A survey on federated learning: The journey from centralized to distributed on-site learning and beyond", IEEE Internet Things J., vol. 8, no. 7, pp. 5476-5497, Apr. 2021.
42. M. Asad, S. Shaukat, D. Hu, Z. Wang, E. Javanmardi, J. Nakazato, et al., "Limitations and future aspects of communication costs in federated learning: A survey", Sensors, vol. 23, no. 17, pp. 7358, Aug. 2023.
43. T. Solanki, B. K. Rai and S. Sharma, "Federated learning using tensor flow" in Federated Learning for IoT Applications, Springer, pp. 157-167, 2022.
44. R. Panigrahi and S. Borah, "A detailed analysis of CICIDS2017 dataset for designing intrusion detection systems", Int. J. Eng. Technol., vol. 7, no. 3, pp. 479-482, 2018.
45. J.-H. Lee, J.-W. Kim and M.-J. Choi, "SSAE—DeepCNN model for network intrusion detection", Proc. 22nd Asia–Pacific Netw. Operations Manage. Symp. (APNOMS), pp. 78-83, Sep. 2021.
46. E. A. Shams and A. Rizaner, "A novel support vector machine based intrusion detection system for mobile ad hoc networks", Wireless Netw., vol. 24, no. 5, pp. 1821-1829, Jul. 2018.
47. C. Liu, Z. Gu and J. Wang, "A hybrid intrusion detection system based on scalable K-means+ random forest and deep learning", IEEE Access, vol. 9, pp. 75729-75740, 2021.
48. A. Meryem and B. E. Ouahidi, "Hybrid intrusion detection system using machine learning", Netw. Secur., vol. 2020, no. 5, pp. 8-19, May 2020.