

Research Paper

FEDERATED LEARNING FOR DECENTRALIZED DDOS ATTACK DETECTION IN IOT NETWORKS

PRIYA RANJAN RAJ¹, SAMA AKSHITHA², SHAIK SIRAJ³, LODI PAVANI⁴, KARNE JAGADEESH KUMAR⁵

¹Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

^{2, 3, 4, 5}B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— In the ever-expanding domain of Internet of Things (IoT) networks, Distributed Denial of Service (DDoS) attacks represent a significant challenge, compromising the reliability of these systems. Traditional centralized detection methods struggle to cope effectively in the widespread and diverse environment of IoT, leading to the exploration of decentralized approaches. This study introduces a Federated Learning-based approach, named Federated Learning for Decentralized DDoS Attack Detection (FL-DAD), which utilizes Convolutional Neural Networks (CNN) to efficiently identify DDoS attacks at the source. Our approach prioritizes data privacy by processing data locally, thereby avoiding the need for central data collection, while

enhancing detection efficiency. Evaluated using the comprehensive CICIDS2017 dataset and compared with conventional centralized detection methods, FL-DAD achieves superior performance, illustrating the potential of federated learning to enhance intrusion detection systems in large-scale IoT networks by balancing data security with analytical effectiveness.

Index Terms – Federated Learning, DDoS Detection, IoT Security, Intrusion Detection, Network Security, Decentralized Learning, Deep Learning, Anomaly Detection, Edge Computing, Cybersecurity.

I. INTRODUCTION

The Internet of Things (IoT) epitomizes the transformation of the digital landscape, moving beyond traditional devices like computers and smartphones to create an interconnected web of everyday objects. These objects, embedded with sensors, software, and other technologies, seamlessly communicate and exchange data with other devices and systems over the Internet. IoT has emerged as a cornerstone of the 21st-century digital revolution. From smart thermostats and wearable health monitors to intelligent traffic systems and advanced manufacturing tools, the integration of IoT has seen an upsurge across various sectors. According to Gartner, by 2025, the number of connected things worldwide is expected to surpass 30 billion. This burgeoning network promises unparalleled opportunities for personal, industrial, and societal applications. Enhanced data collection, real-time communication, and a vastly improved user experience are just some of the many advantages IoT brings.

However, the proliferation of IoT devices also introduces an array of vulnerabilities. The very attributes that make IoT devices versatile, their connectivity, ease of access, and ubiquity, also render them susceptible to threats. Of these threats, Distributed Denial of Service (DDoS) attacks

are particularly ominous. These attacks involve overwhelming a targeted system, such as a website or an IoT device, with a flood of Internet traffic, rendering it inoperative. 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. The inherent characteristics of IoT devices further exacerbate their vulnerability. These devices, often manufactured with cost-effectiveness in mind, may lack sophisticated security features. Moreover, their widespread deployment across various environments, each with its unique security posture, makes establishing a unified protective framework challenging.

Traditional security measures, especially centralized intrusion detection systems, are ill-equipped to handle the intricacies of IoT. These centralized systems often suffer from scalability issues, struggling to monitor the massive data flows generated by the plethora of IoT devices. Moreover, centralized systems also introduce a single point of failure, making them attractive targets for adversaries. Furthermore, the transmission of data to a central location for analysis compromises

user privacy, as sensitive information may be exposed during transit or storage. To address these shortcomings, there's a growing interest in decentralized learning methodologies, specifically Federated Learning. In federated frameworks, devices, or nodes, are trained locally on their data. Only the model updates, not the raw data, are shared with a central server for aggregation. This approach has the dual advantage of mitigating data privacy concerns and reducing the data transmission overhead. Given the decentralized nature of IoT networks, federated learning seems to be an ideal fit. By processing data locally on IoT devices, federated learning can offer real-time insights, vital for timely detection and mitigation of threats like DDoS attacks.

To this end, in this study, we introduce the Federated Learning for Decentralized DDoS Attack Detection (FL-DAD) approach in IoT Networks. In the proposed approach, we utilize Convolutional Neural Networks (CNNs), leveraging their adeptness in feature extraction and pattern recognition. This makes them particularly effective for identifying complex patterns in network traffic, which is crucial for detecting DDoS attacks in IoT environments. By training the model at the edge, close to where the data originates, our approach aims to adeptly

detect DDoS attacks while upholding the principles of data privacy and operational efficiency. Using the CICIDS2017 dataset, a comprehensive benchmark for intrusion detection, we present the performance of the FL-DAD approach against traditional centralized methods, showcasing the merits of our decentralized approach.

II. RELATED WORK

A. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for Internet of Things

Decentralized paradigm in the field of cybersecurity and machine learning (ML) for the emerging Internet of Things (IoT) has gained a lot of attention from the government, academia, and industries in recent years. Federated cybersecurity (FC) is regarded as a revolutionary concept to make the IoT safer and more efficient in the future. This emerging concept has the potential of detecting security threats, taking countermeasures, and limiting the spreading of threats over the IoT network system efficiently. An objective of cybersecurity is achieved by forming the federation of the learned and shared model on top of various participants. Federated learning (FL), which is regarded as a privacy-aware ML model, is

particularly useful to secure the vulnerable IoT environment. In this article, we start with background and comparison of centralized learning, distributed on-site learning, and FL, which is then followed by a survey of the application of FL to cybersecurity for IoT. This survey primarily focuses on the security aspect but it also discusses several approaches that address the performance issues (e.g., accuracy, latency, resource constraint, and others) associated with FL, which may influence the security and overall performance of the IoT. To anticipate the future evolution of this new paradigm, we discuss the main ongoing research efforts, challenges, and research trends in this area. With this article, readers can have a more thorough understanding of FL for cybersecurity as well as cybersecurity for FL, different security attacks, and countermeasures.

B. Future mining based on Internet of Things (IoT) and sustainability challenges

Sustainable Development (SD) has played an important role in all industries and mining activities. The Internet of Things (IoT), interacting with industrial machines or home appliances through an interconnected network, can assist in developing real-time platforms for monitoring and operating a

complex production system with minimal intervention of humans, which made it possible to benefit from the data obtained to increase production rate, Net Present Value optimization, workforce and machine safety, and decreasing pollution. Ideal automated mining can be achieved by designing an IoT based framework and suitable SD assessment. This research aims to achieve a holistic understanding of the current IoT scenario by conducting a comparative analysis of the prevailing literature regarding IoT applications in the mining and SD area. The results showed that, in the economic index of sustainability, mining activity based on IoT can increase productivity, wealth, income, and GDP and decrease operating expenses, depreciation costs, and total cost. From environmental point of view, a significant reduction in emission and pollution can be obtained. In addition, the increase in workforce safety and positive impact on culture and knowledge are the components of the social index of sustainability. These activities are followed by some significant challenges such as developing infrastructures, modern machinery, adequate security for data transmission, increase business in the area, creating new jobs for individuals, especially those who have lost their jobs. It's essential

to devise new rules to protect local people, properly distribute the wealth gained from this development to improve the infrastructure of the mining area.

C. Threat analysis and distributed denial of service (DDoS) attack recognition in the Internet of Things (IoT)

The Internet of Things (IoT) plays a crucial role in various sectors such as automobiles and the logistic tracking medical field because it consists of distributed nodes, servers, and software for effective communication. Although this IoT paradigm has suffered from intrusion threats and attacks that cause security and privacy issues, existing intrusion detection techniques fail to maintain reliability against the attacks. Therefore, the IoT intrusion threat has been analyzed using the sparse convolute network to contest the threats and attacks. The web is trained using sets of intrusion data, characteristics, and suspicious activities, which helps identify and track the attacks, mainly, Distributed Denial of Service (DDoS) attacks. Along with this, the network is optimized using evolutionary techniques that identify and detect the regular, error, and intrusion attempts under different conditions. The sparse network forms the complex hypotheses evaluated using neurons, and the obtained event stream outputs are propagated

to further hidden layer processes. This process minimizes the intrusion involvement in IoT data transmission. Effective utilization of training patterns in the network successfully classifies the standard and threat patterns. Then, the effectiveness of the system is evaluated using experimental results and discussion. Network intrusion detection systems are superior to other types of traditional network defense in providing network security. The research applied an IGA-BP network to combat the growing challenge of Internet security in the big data era, using an auto encoder network model and an improved genetic algorithm to detect intrusions. MATLAB built it, which ensures a 98.98% detection rate and 99.29% accuracy with minimal processing complexity, and the performance ratio is 90.26%. A meta-heuristic optimizer was used in the future to increase the system's ability to forecast attacks.

III. PROPOSED METHODOLOGY

Our approach prioritizes data privacy by processing data locally, thereby avoiding the need for central data collection, while enhancing detection efficiency.

Evaluated using the comprehensive compared with conventional centralized detection methods, FL-DAD achieves

superior performance, illustrating the potential of federated learning to enhance intrusion detection systems in large-scale IoT networks by balancing data security with analytical effectiveness.

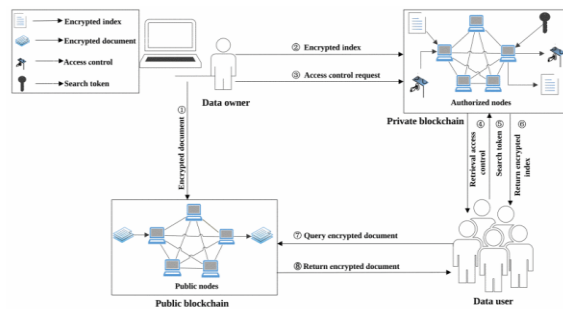
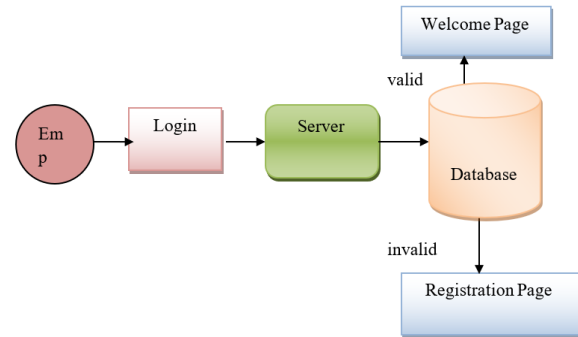


Fig. 1: System Overview

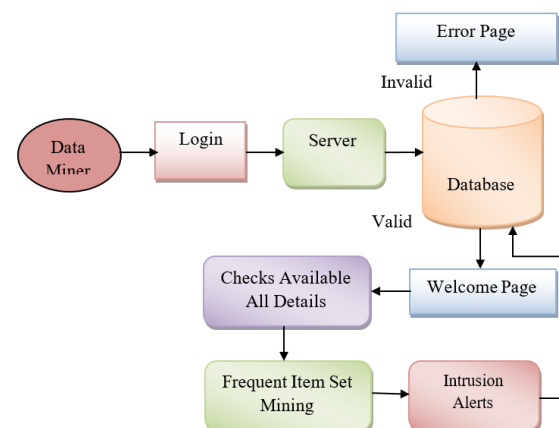
1. User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exists directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.



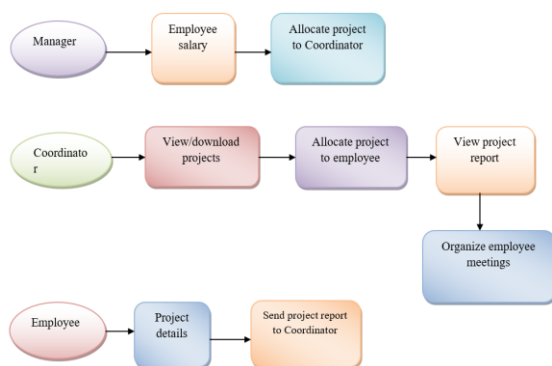
2. Cloud Service Provider (Data Miner):

This module will represent as a database in our project, We are assuming that the data which we are uploading in the project is supposed to store in the CSP which we are taking as a database. Whenever the user uploads the data that will be stored in an encrypted format in the real path of the project work space. The CSP along with the help of Evaluator collects encrypted transactions and maintains an encrypted database in the real path, to carry mining on encrypted data.



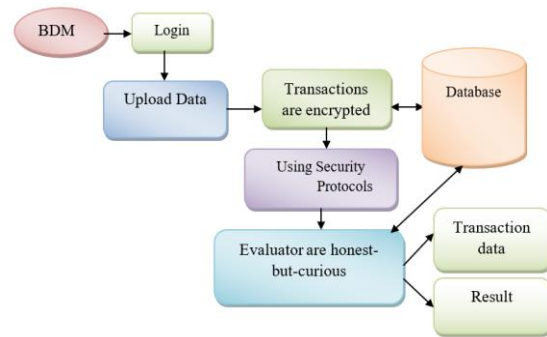
3. User

This is the third module in our project, where Coordinator, BDM, and Employee acts as a user for our project. In which we are considering the BDM data as crucial data and applying our encryption protocols on the data uploaded by him. BDM can upload 'n' number of files.

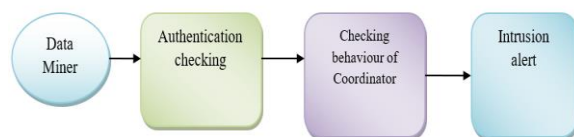


4. Encryption & Decryption Phase:

In this module all the files which are uploaded by the BDM will be encrypted and stored in the CSP which maintains transaction database. Users do not fully trust the CSP with the privacy of their transactions. Therefore, all their transactions are encrypted before contributing to the CSP. we assume both the CSP and the Evaluator are honest-but-curious, which indicates both of them can compute data correctly by following protocols but are curious about data in the transaction database and results of frequent itemset mining.

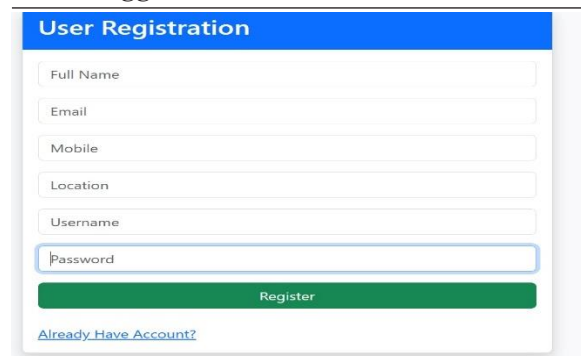


5. Frequent Itemset mining:



IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the integration of Federated Learning enabled collaborative model training across multiple IoT devices without sharing raw network traffic data, thereby preserving privacy and reducing communication overhead. The model effectively detected distributed denial-of-service attacks with high detection accuracy and low false alarm rates. The analysis showed that the decentralized learning framework maintained robust performance even as the number of participating IoT devices increased.



User Registration

Full Name

Email

Mobile

Location

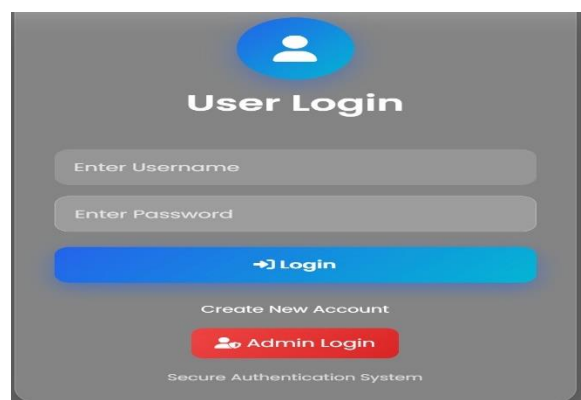
Username

Password

Register

[Already Have Account?](#)

Fig. 2: Registrtaion



User Login

Enter Username

Enter Password

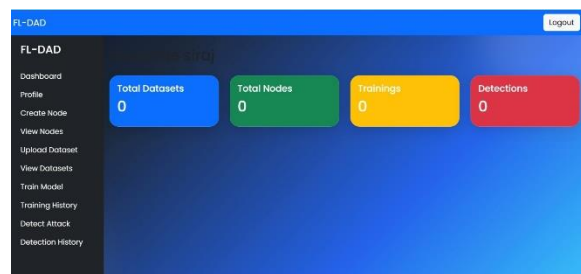
Login

Create New Account

Admin Login

Secure Authentication System

Fig. 3: Login



FL-DAD

Dashboard

Profile

Create Node

View Nodes

Upload Dataset

View Datasets

Train Model

Training History

Detect Attack

Detection History

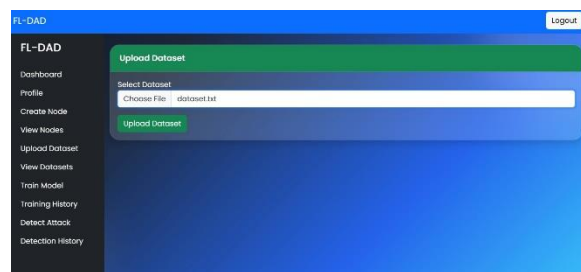
Total Datasets: 0

Total Nodes: 0

Trainings: 0

Detections: 0

Fig. 4: Dashboard



FL-DAD

Dashboard

Profile

Create Node

View Nodes

Upload Dataset

View Datasets

Train Model

Training History

Detect Attack

Detection History

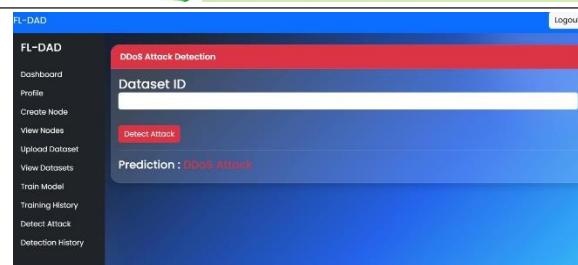
Upload Dataset

Select Dataset

Choose File: dataset.txt

Upload Dataset

Fig. 5: Upload



FL-DAD

Dashboard

Profile

Create Node

View Nodes

Upload Dataset

View Datasets

Train Model

Training History

Detect Attack

Detection History

DDoS Attack Detection

Dataset ID

Detect Attack

Prediction: DDoS attack

Fig. 6: Detect Attack

V. CONCLUSION

In this research, we embarked on an exploration of the potential of Federated Learning (FL) in bolstering the security landscape of Internet of Things (IoT) networks, particularly focusing on the detection of Distributed Denial of Service (DDoS) attacks. Our proposed FL-DAD methodology underscored the efficacy of decentralizing the learning process, ensuring data privacy while not compromising on detection accuracy. The numerical results demonstrated that our FL-DAD approach achieved an accuracy rate consistently above 98% across various DDoS attack classes, significantly outperforming traditional centralized models. Noteworthy findings included the system's resilience in terms of accuracy even when exposed to varied data attributes across nodes and its competitive edge over centralized counterparts.

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. Damaševičius, 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.

AUTHORS Profile



Mr. PRIYA RANJAN RAJ completed his Bachelor of Technology (B.Tech) in Computer Science and Engineering (CSE) in 2019 from MIT University of Meghalaya, India. He earned his Master of Technology (M.Tech) in Computer Science and Engineering (CSE) in 2021 from Chandigarh University, Mohali, Punjab, India. He is currently pursuing his Ph.D. in Computer Science and Engineering (CSE) at Chandigarh University, Mohali, Punjab, which is expected to be completed in 2027. With 4 years of teaching experience, he is currently serving as an Assistant Professor in the Department of Computer Science and Engineering (CSE) at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India. His research interests include Networking, Edge Computing, and the Internet of Things (IoT),

and he is actively engaged in research and academic activities in these domains.



Ms. SAMA AKSHITHA
pursuing B.Tech degree in
Computer Science and
Engineering at Guru Nanak
Institutions Technical

Campus affiliated to JNTUH in 2022-2026.



Mr. SHAIK SIRAJ
pursuing B.Tech degree in
Computer Science and
Engineering at Guru Nanak
Institutions Technical

Campus affiliated to JNTUH in 2022-2026.



Ms. LODI PAVANI
pursuing B.Tech degree in
Computer Science and
Engineering at Guru Nanak
Institutions Technical

Campus affiliated to JNTUH in 2022-2026.



**Mr. KARNE
JAGADEESH KUMAR**
pursuing B.Tech degree in
Computer Science and
Engineering at Guru

Nanak Institutions Technical Campus
affiliated to JNTUH in 2022-2026.