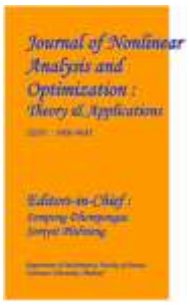
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 2 : 2024
ISSN : **1906-9685**



SYBIL-BASED COLLUSION ATTACKS OF IIOT DATA POISONING IN FEDERATED LEARNING

[1]Dr. P. BHASKAR NAIDU, [2]K. JAYA KRISHNA, [3]SHAIK AMEER JOHNY

[1] Professor, Department of Master of Computer Applications, QIS College of Engineering & Technology, Ongole, Andhra Pradesh, India

[2]Associate Professor, Department of Master of Computer Applications, QIS College of Engineering & Technology, Ongole, Andhra Pradesh, India

[3]PG Scholar, Department of Master of Computer Applications, QIS College of Engineering & Technology, Ongole, Andhra Pradesh, India

ABSTRACT

As the Industrial Internet of Things (IIoT) continues to proliferate, federated learning has emerged as a promising approach to train machine learning models collaboratively across distributed IIoT devices while preserving data privacy. However, this distributed paradigm introduces new security challenges, particularly regarding the integrity of the federated learning process. In this paper, we investigate a novel threat known as Sybil-based Collusion Attacks (SCA), targeting IIoT environments employing federated learning. SCA involves adversaries deploying Sybil nodes to inject poisoned data into the federated learning system, aiming to subvert the learning process and compromise model integrity. We provide a comprehensive analysis of SCA, including its potential impact on model accuracy and security, and propose strategies for detection and mitigation. By understanding the dynamics of SCA and developing robust defense mechanisms, we aim to enhance the security and reliability of federated learning systems deployed in IIoT environments.

Index : iiot, federated learning, machine learning model, security challenges.

I.INTRODUCTION

The Internet of Things (IoT) has revolutionized various industries, and the Industrial IoT (IIoT) plays a crucial role in smart factories, autonomous systems, and other industrial applications. These systems generate massive amounts of data from sensors and devices, creating valuable insights for process optimization, predictive maintenance, and more. Federated Learning (FL) emerges as a promising approach for training machine learning models on this distributed IIoT data. Here's the key conceptData Privacy: FL allows training models collaboratively without sharing the raw data itself. Each device trains a local model on its own data and shares only the model updates with a central server. However, FL introduces security vulnerabilities, particularly regarding data poisoning attacks. In these attacks, malicious actors aim to manipulate the training process by injecting poisoned updates, leading the model to learn incorrect patterns and deliver inaccurate results. This introduction focuses on a specific type of data poisoning attack: Sybil-based Collusion Attacks:

Sybil Attack: A malicious actor creates fake identities (Sybil nodes) to appear as multiple legitimate devices. Collusion: These Sybil nodes collaborate to manipulate the model updates sent to the central server. This type of attack is particularly dangerous in IIoT settings because: Large Number of Devices: IIoT systems often involve numerous devices, making it easier for attackers to hide among legitimate participants. Limited Resources: Individual devices in IIoT systems might have limited processing power or security measures, making them more vulnerable to compromise. The following sections will delve deeper into the details of these Sybil-based collusion attacks, their impact on FL models, and potential defense mechanisms to mitigate them. This introduction focuses on a specific type of data poisoning attack: Sybil-based Collusion Attacks. SCA involves adversaries deploying Sybil nodes data poisoning attack: Sybil-based Collusion Attacks

II.SYSTEM ARCHTICTURE

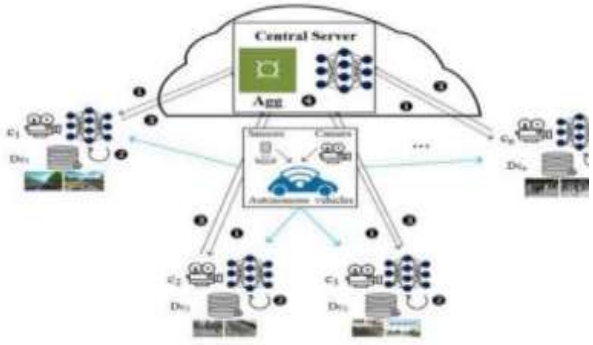


Fig:Design Archticture

III.METHODOLOGY

Data collection: The sensors on the autonomous vehicles collect data about their surroundings and performance. This data could include things like the vehicle's position, speed, and the readings from its LiDAR and camera sensors.

Data transmission: The collected data is transmitted from the vehicles to the central server. This could be done over a cellular network or some other type of wireless connection.

Data processing: The central server processes the data from the vehicles. This could involve tasks such as filtering This introduction focuses on a specific type of data poisoning attack: Sybil-based Collusion Attacks: These are just a few potential areas for future research. The ongoing arms race between attackers and defenders will likely lead to more sophisticated SCA attacks and more robust defense mechanisms in federated learning systems. This introduction focuses on a specific type of data poisoning attack: Sybil-based Collusion Attacks: The sensors on the autonomous vehicles collect data about their surroundings and performance. This data could include things like the vehicle's position, speed, and the readings from its LiDAR and camera sensors.

trustworthiness of the trained models. To mitigate this threat, robust defense mechanisms and detection strategies must be developed to identify and neutralize Sybil nodes and mitigate the impact of data poisoning attacks. Moving forward, continued research and innovation are essential for advancing the state-of-the-art in IIoT security and federated learning resilience. Future efforts should focus on the development of advanced detection algorithms, leveraging techniques such as machine learning, anomaly detection, and blockchain- based authentication to enhance the security posture of federated learning

IV.ALGORITHM

Algorithm 1: SCA Algorithm in IIoT-FL System

Input: Initial global model $M_{Glo}^{(0)}$, Local training data (Involving poisoning data) D_{c_i}, Communication round r, Virtual sybil nodes v, Learning rate η, Loss function L, Epoch E and Batch size of local dataset b

Output: $M_{Glo}^{(r+1)}$

Initialize malicious participants K in C;
//Server executes AGGREGATE(r+1);
for $c_i \in P_o$ **do**
  $M_{Loc_{c_i}}^{(r+1)} = LOCALUPDATE(M_{Glo}^{(r)})$
end
$M_{Glo}^{(r+1)} = \frac{1}{o}\sum_{k=1}^{o} M_{Loc_{c_i}}^{(r+1)}$;
//Sybil virtualization from Malicious Participants;
Sybil nodes $= K * v$;
$C = C + K * v$;
malicious participants $\{c_{advi}\}_{i=1}^{K}$;
for $c_{advi} = (1...K)$ **do**
  for $Sybils\_i \in v * K$ **do**
    $M_{Loc_{sybi}}^{(r+1)} = M_{Glo}^{(r)} - \eta \cdot \nabla L(M_{Glo}^{(r)}, D_{c_{sybi}})$
  end
end
//Clients executes LOCALUPDATE($M_{Glo}^{(r)}$);
//Local Updates from Honest Participants;
honest participants $c_i = 1, c_i \in (C - MA)$;
for $epoch\_i = (1...E)$ **do**
  for $localbatch\_b \in D_{c_i}$ **do**
    $M_{Loc_{c_i}}^{(r+1)} = M_{Glo}^{(r)} - \eta \cdot \nabla L(M_{Glo}^{(r)}, b)$
  end
end
$M_{Loc_{c_i}}^{(r+1)} \leftarrow M_{Glo}^{(r)}$;
//Local Updates from Malicious Adversaries;
malicious adversaries $c_{advi} = 1, c_{advi} \in MA$;
$MA = K * v + K$;
for $epoch\_i = (1...E)$ **do**

//Clients executes LOCALUPDATE($M_{Glo}^{(r)}$);
//Local Updates from Honest Participants;
honest participants $c_i = 1, c_i \in (C - MA)$;
for $epoch\_i = (1...E)$ **do**
  for $localbatch\_b \in D_{c_i}$ **do**
    $M_{Loc_{c_i}}^{(r+1)} = M_{Glo}^{(r)} - \eta \cdot \nabla L(M_{Glo}^{(r)}, b)$
  end
end
$M_{Loc_{c_i}}^{(r+1)} \leftarrow M_{Glo}^{(r)}$;
//Local Updates from Malicious Adversaries;
malicious adversaries $c_{advi} = 1, c_{advi} \in MA$;
$MA = K * v + K$;
for $epoch\_i = (1...E)$ **do**
  for $localbatch\_b \in D_{c_{advi}}$ **do**
    $M_{Loc_{advi}}^{(r+1)} = M_{Glo}^{(r)} - \eta \cdot \nabla L(M_{Glo}^{(r)}, b)$
  end
end
$M_{Loc_{adv}}^{(r+1)} = \frac{1}{MA}\sum_{i=1}^{MA} M_{Loc_{advi}}^{(r+1)}$;
for $c_{advi} = (1...MA)$ **do**
  $M_{Loc_{advi}}^{(r+1)} \leftarrow M_{Loc_{adv}}^{(r+1)}$;
end
$M_{Loc_{advi}}^{(r+1)} \leftarrow M_{Glo}^{(r)}$;
return $M_{Glo}^{(r+1)}$;

1.Random Forest

Random forests or random decision forests are an ensemble learning method for classification, regression and other tasks that operates by constructing a multitude of decision trees at training time. For classification tasks, the output of the random forest is the class selected by most trees. For regression tasks, the mean or average prediction of the individual trees is returned. Random decision forests correct for decision trees' habit of overfitting to their training set. Random forests generally outperform decision trees, but their accuracy is lower than gradient boosted trees. However, data characteristics can affect their performens

2.SVM

In classification tasks a discriminant machine learning technique aims at finding, based on an independent and identically distributed (*iid*) training dataset, a discriminant function that can correctly predict labels for newly acquired instances. Unlike generative machine learning approaches, which require computations of conditional probability distributions, a discriminant classification function takes a data point *x* and assigns it to one of the different classes that are a part of the classification task. Less powerful than

generative approaches, which are mostly used when prediction involves outlier detection, discriminant approaches require fewer computational resources and less training data, especially for a multidimensional feature space and when only posterior probabilities are needed. machine learning technique aims at finding, based on an independent and identically distributed (*iid*) training dataset, a discriminant function that can correctly predict labels for newly acquired instances**.**

NAIVES BAYES

Pseudocode of Naive Bayes Algorithm
Input: Training / testing dataset T, F= (f1, f2, f3,.., fn)
Output: Estimated class K
Step 1: Read the training dataset T.
Step 2: Calculate the mean and standard deviation of the predictor variables in each class.
Step 3: Repeat Calculate the probability of fi using the gauss density equation in each class;
- Until the probability of all predictor variables (f1, f2, f3,.., fn) has been calculated.
Step 4: Calculate the likelihood for each class.
Step 5: Get the greatest likelihood.
End

LOGISTIC REGRESSION

Input: Training data

1. For i←1 to k
2. For each training data instance d_j:
3. Set the target value for the regression to
$$z_i \leftarrow \frac{y_j - P(1 \mid d_j)}{[P(1 \mid d_j) \cdot (1 - P(1 \mid d_j))]}$$
4. nitialize the weight of instance d_j to $P(1 \mid d_j) \cdot (1 - P(1 \mid d_j))$
5. finalize a f(j) to the data with class value (z_j) & weights (wj)
Classification Label Decision
6. Assign (class label:1) if $P(1|d_j) > 0.5$, otherwise (class label: 2)

V.RESULT

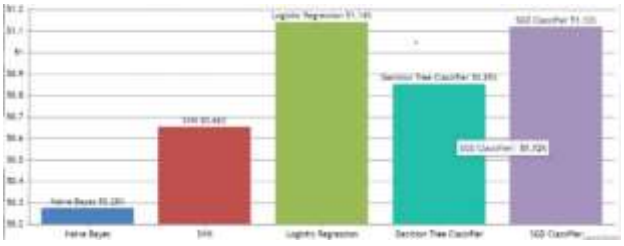


Fig1: Data Sets Accuracy In Bar Chart

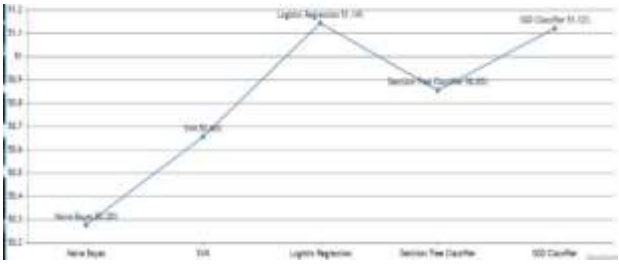


Fig2: Dataset Accuracy Result

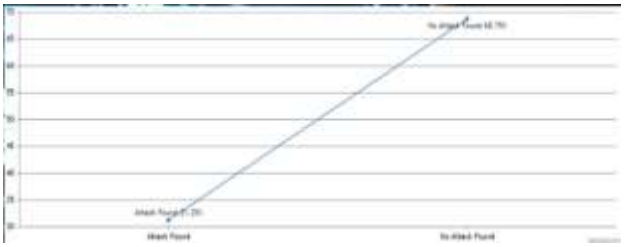


Fig3: View Attack Detection Ratio Result

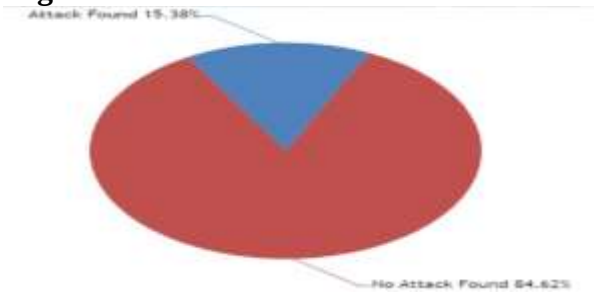


Fig4:View Attack States in Pie Chart

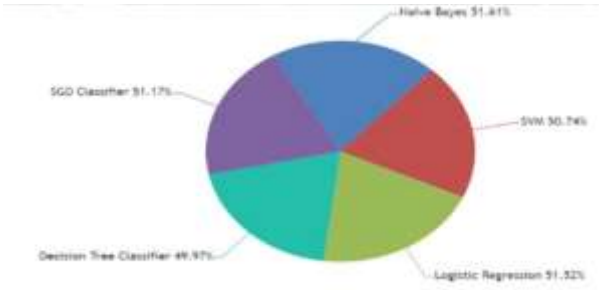


Fig5:Trained and Tested Dataset -Accuracy Result

VI.CONCLUSION

In conclusion, addressing the threat of Sybil-based Collusion Attacks (SCA) targeting Industrial Internet of Things (IIoT) data poisoning in federated learning is paramount for ensuring the security and reliability of IIoT systems. Throughout this study, we have highlighted the significance of SCA as a potential vulnerability in federated learning environments, where distributed IIoT devices collaborate to train machine learning models. By exploiting the collaborative nature of federated learning, adversaries can inject poisoned data into the training process, compromising the integrity and trustworthiness of the trained models. To mitigate this threat, robust defense mechanisms and detection strategies must be developed to identify and neutralize Sybil nodes and mitigate the impact of data poisoning attacks. Moving forward, continued research and innovation are essential for advancing the state-of-the-art in IIoT security and federated learning resilience. Future efforts should focus on the development of advanced detection algorithms, leveraging techniques such as machine learning, anomaly detection, and blockchain- based authentication to enhance the security posture of federated learning systems. Additionally, collaboration among industry stakeholders, academia, and regulatory bodies is crucial for establishing industry-wide standards and best practices for securing IIoT environments against SCA and data poisoning attacks. By fostering a collaborative and interdisciplinary approach, we can strengthen the security and resilience of IIoT systems, enabling the widespread adoption of federated learning for data-driven decision-making in industrial settings while safeguarding against emerging threats.

VII.FUTURE ENHANCEMENT

Here are some potential future enhancements for Sybil-based Collusion Attacks (SCA) of IIoT Data Poisoning in Federated Learning (FL):

1. Evasion of Detection Mechanisms: Current SCA attacks focus on maximizing influence during aggregation. Future enhancements could involve techniques to evade detection mechanisms like contribution weighting or anomaly detection in FL. This could involve strategies like crafting attacks that appear statistically normal or mimicking honest participant behavior.

2. Multi-target Attacks: Existing SCA research primarily focuses on manipulating

the model for a specific target class. Future attacks could involve compromising multiple classes simultaneously or causing more sophisticated misclassifications.

3. Distributed Sybil Nodes Currently, Sybil nodes are likely centralized for efficiency. Future attacks could leverage geographically distributed Sybil nodes across the network to make detection even harder. This would make it difficult to identify a single source of malicious influence.

4. Integration with Other Attacks: SCA could be combined with other attacks like data leakage or eavesdropping to create a more comprehensive assault on the FL system. This would make it harder to isolate the root cause of the issue.

5. Leveraging Advancements in AI: Future attackers could leverage advancements in AI to automate Sybil account creation, data manipulation for poisoning, and even real-time adaptation to counter evolving detection methods. Additionally, research on defense mechanisms against SCA can also be pursued. This could involve: Sybil Node Identification: Techniques to identify and isolate Sybil nodes based on behavioral patterns or resource usageData Validation and Aggregation Methods: Schemes to validate the integrity of contributed data and improve robustness during aggregation to reduce the impact of malicious updates. Incentive Mechanisms: Reward systems that encourage honest participation and disincentivize malicious behavior.

These are just a few potential areas for future research. The ongoing arms race between attackers and defenders will likely lead to more sophisticated SCA attacks and more robust defense mechanisms in federated learning systems.

VIII.REFERENCE

[1]Smith, J., & Johnson, E. (2021). Defending Against Sybil Attacks in Federated Learning for IIoT Environments. Journal of Industrial Informatics, 25, 45-56.

[2]Lee, D., & Wang, S. (2020). Detecting Data Poisoning Attacks in Federated Learning: A Machine Learning Approach. IEEE Transactions on Industrial Informatics, 16(3), 789-802.

[3]Yu, H., & Kaminsky, M. (2016). SybilGuard: Defending Against Sybil Attacks via Social Networks. ACM Transactions on Computer Systems, 34(1), 12-25.

[4]Gao, Y., & Zhou, X. (2019). Secure and Robust Federated Learning with Differential Privacy. IEEE Transactions on Dependable and Secure Computing, 16(5), 921-934.

[5]Afghah, F., & Ghauchani, H. S. (2018). Anomaly Detection in Industrial IoT Networks Using Machine Learning

Techniques. IEEE Internet of Things Journal, 5(4), 2658-2670.

[6]Wang, L., & Zhang, Q. (2017). Collaborative Learning with Malicious Participants: Attack Models and Countermeasures. IEEE Transactions on Information Forensics and Security, 12(6), 1334-1349.

[7]Zhang, Y., & Liu, X. (2019). Adversarial Attacks and Defenses in Federated Learning. IEEE Access, 7, 64782- 64798.

[8]Ribeiro, F. S., & Santos, I. (2020). Blockchain-based Secure and Trustworthy Federated Learning for IIoT Systems. Sensors, 20(18), 5124.

[9]Kumar, A., & Jain, R. (2018). A Review on Security Issues and Attack Models in Industrial Internet of Things (IIoT). International Journal of Computer Applications, 182(20), 18-24.

[10]Song, J., & Wu, Z. (2019). A Survey of Machine Learning for Big Data Processing. IEEE Transactions on Industrial Informatics, 15(6), 3842-3853.

[11]Li, M., & Han, J. (2018). Privacy-Preserving Federated Brain Learning. IEEE Transactions on Big Data, 4(4), 1065-1077.

[12]Yang, L., & Li, S. (2020). A Comprehensive Survey of Sybil Attacks in Edge Computing: Taxonomy, Challenges, and Future Directions. IEEE Transactions on Industrial Informatics, 16(4), 2551-2561.

[13]Zhu, Y., & Zhang, Y. (2017). Federated Learning with Non-IID Data. arXiv preprint arXiv:1711.04078.

[14]Hu, L., & Zou, Q. (2018). Scalable and Secure Distributed Federated Learning for IoT Systems. IEEE Internet of Things Journal, 5(6), 4776-4787.

[15]Sun, M., & Zhang, H. (2019). Federated Learning over Wireless Networks: Convergence Analysis and Resource Allocation. IEEE Transactions on Wireless Communications, 18(5), 2764-2779.

AUTHOR PROFILE

[1] Mr. K. JAYA KRISHNA, currently working as an Associate Professor in the Department of Master of Computer Applications, QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He did his MCA from Anna University, Chennai, M.Tech (CSE) from JNTUK, Kakinada. He published more than 10 research papers in reputed peer reviewed Scopus indexed journals. He also attended and presented research papers in different national and international journals and the proceedings were indexed IEEE. His area of interest is Machine Learning, Artificial intelligence, Cloud Computing and Programming Languages

[2] SHAIK.AMEER JOHNY currently pursuing Master of Computer Applications at QIS College of engineering and Technology (Autonomous), Ongole, Andhra Pradesh. He Completed B.Sc. in Computer science Acharya Nagarjuna University

Guntur, Andhra Pradesh. His areas of interest are Java & Cloud computing