The Role of Federated Learning in Protecting Market Intelligence Against Data Poisoning

Aji Jayaloka[1], Teddy Mantoro[2]
[1]Department of Information Technology, Pradita University, Jakarta, Indonesia
[2]School of Computer Science, Nusa Putra University, West Java, Indonesia

Abstract— The proliferation of data resulting from these as-a-services and the adoption of 5g technology is overwhelmingly high in fact many companies today are trying to figure out how they can better utilize their data in order to create actionable market intelligence this new revolution allows corporations to address opportunities and deliver results as this inscribes to be the scalable advantage in modern business unfortunately data poisoning attacks can be a huge problem for achieving market intelligence and persistence through the hallmarks of data driven decision making process. With this research attempt we aim to explore and understand how federated learning can be applied as an effective and practical counter mechanism against such attacks in future. In this fiducial blearing model, there is further no direct sharing of datasets so even the likelihood of relevant data being tampered with is appreciably lowered. This type of model not only improves data security but also helps to maintain privacy which in turn makes the model fit for sensitive business scenarios. In this instance, federated learning applied techniques may empower global users to cooperatively train predictive systems that are reliable and acceptable by minimizing the adverse effect of powerfully polluted samples on statistical accuracy weighting. In this regard this proposal touches on the advantage of federated learning as it comes in to enhance the security of business intelligence systems as well as the security of data of analytics insights.

Keywords- Market Intelligence, Data Poisoning, Federated Learning, Artificial Intelligence

I.INTRODUCTION

The exponential growth of data, has been driven by the rise of "as-a-service" models and 5G technology, presents both an opportunity and a challenge for businesses. While this data explosion enables the extraction of valuable insights for informed decision-making, it also exposes organizations to new threats, particularly data poisoning. As machine learning becomes increasingly integrated into business intelligence systems, ensuring the integrity of these models is paramount.

Data poisoning attacks involve the subtle injection of malicious or misleading data into training datasets, aiming to manipulate model behavior and compromise the accuracy of BI outputs. This poses a significant risk to organizations, as compromised insights can lead to flawed decision-making and financial losses. Traditional security measures, focused on infrastructure protection, often prove inadequate against this insidious form of attack.

Federated learning (FL) emerges as a promising solution by enabling collaborative model training on decentralized datasets without requiring direct data sharing. This approach inherently reduces vulnerabilities to manipulation and enhances privacy, making it particularly suitable for sensitive business environments. By decentralizing the learning process and incorporating robust aggregation techniques, FL can effectively mitigate the impact of poisoned data on overall model accuracy and reliability.

II.RELATED WORK

Mitigating Image Data Poisoning Attacks in Federated Machine

Federated machine learning cannot escape the challenges of data pollution, which will jeopardize the core premises of cooperative learning. The punishment is correlated to offense and several studies in the recent past have shown the possibility of data poisoning where attackers deploy false data into the training datasets of the devices taking part in the federated learning. Such attacks are bound to distort the precision of the global model leaving it with abnormal predictions which might be detrimental when applied to highly sensitive fields like health care and financial matters. [1].

The existing literature on attack mechanisms in federated learning presents a number of data poisoning strategies which have an equal number of adversary subtypes. Some of these are attacks which aim for the mislabeling of a specific input while others focus on more sweeping measures against the model and its learning process or development. Users are able to abuse the characteristics of federated learning to contaminate local training datasets for individual users thus caressing the learning processes of the global model or updates. [2].

Various approaches have been developed to handle data poisoning attacks in the domain of Federated Learning. These include aggregation techniques which are robust enough to prevent the impact of the poisoned dataset from affecting the global model, anomaly detection methods to allow malicious participants to be excluded and ashamed, and cryptographic methods to ascertain local model integrity. But still for many of these defense strategies, there exist challenges such as overheads, actual dependency on assumptions about specific attack strategies and the requirement for the central authority's trust. [3].

This proposed research aims at overcoming these challenges by analyzing the effectiveness of federated learning in protecting business intelligence from data poisoning. As two strategies, pushing back the attack points and making it hard to successfully compromise most federated learning models, this research enhances the impact of the decentralized network against poisoned data. The research will also study the impact of business intelligence systems on data poisoning and help in formulating practice

work and suitable guidelines on the use of federated learning to protect these systems from new threats. [4]. [5].

The Poisoning Attack and Defense of a Personalized Intrusion Detection System based on Federated Learning.[6].

Federated learning (FL) has gained traction in training collaborative intrusion detection systems (IDS) with IoT data volumes while maintaining data privacy. FL-based IDS also has its share of challenges including attacks where a small [number of malicious clients active participating in the training try to poison the model.

Data Heterogeneity is the result of the non-independently and identically distributed (non-IID) structure of non-similar and distinct IoT traffic where a network comprises of several IoT devices having various traffic volumes and types. This might lead to client drift, where local model optima converge separately and affect the performance of the target global model. To solve this, the use of personalized federated learning (pFL) has been suggested to train unique models to each client based on their data distribution. [7].

Meanwhile, in the case of poisoning attacks, bad clients attempt to disrupt and compromise the performance of the global model by injecting bad data or model updates. Attacks of this kind can degrade the performance of an FL based IDS significantly, resulting in a wrong classification of network traffic leading to a breach in security. Several means of defense have been suggested, including a novel, robust in-built aggregation mechanism at the server and detection of chicken participants who are poisoned. [8].

A few works have recently addressed the problem of data heterogeneity and the task of poisoning attacks in the context of pFL approaches within the FL based IDS models. They do involve techniques such as model decoupling, in which a neural network is cut into its feature extractor and classifier portions, and personal loss functions directed at tuning the local models to a specific client data distribution. Furthermore, server-side detection systems have also been proposed which determine poisoned clients according to the cosine similarity of the [9]. [10].

III. METHODOLOGY

This research will employ a mixed-methods approach, combining as in Figure 1.

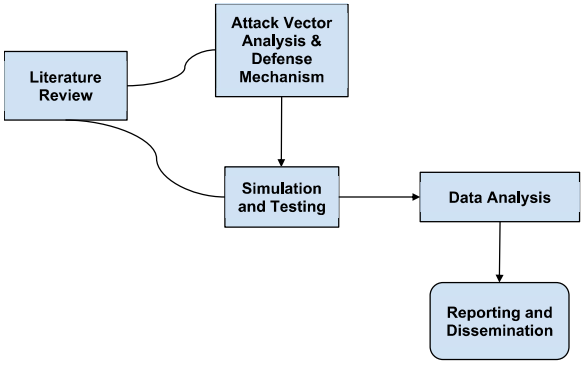


Figure 1. Research Methodology Flow Chart

- Literature Review: Detailed survey of the rich body of work available in Federated Learning domain including but not limited to data poisoning attacks and their corresponding defense mechanisms will also be carried out. This would aid in holding self within the existing scholarship and drawing upon weaknesses in them.
- **Attack Vector Analysis:** Identify and categorize the specific forms of data poisoning attacks that observe the factual approach targeting the FL systems. This also entails looking back on history and specific cases in order to understand how attacks take place and the consequences as in Figure 2.

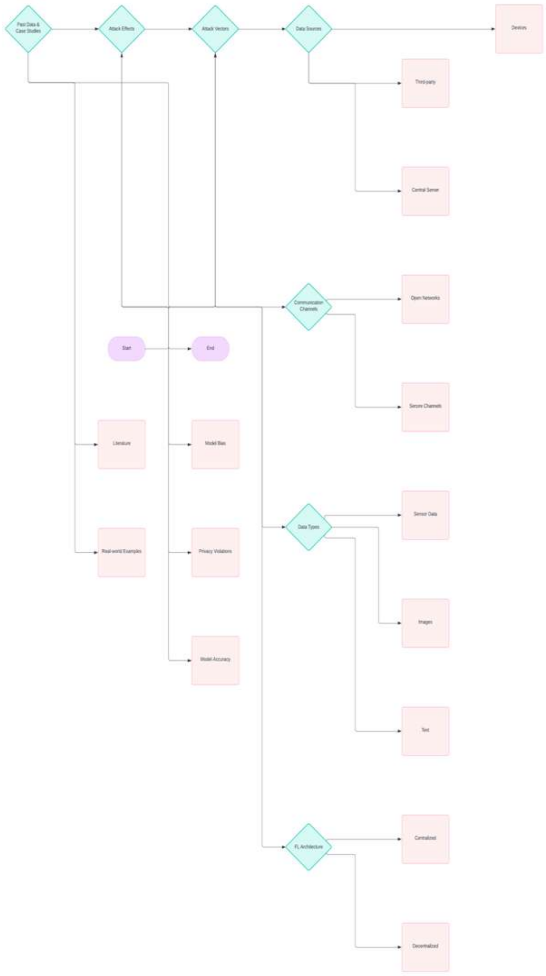


Figure 2. Attack Vector Flow Chart

- Defense Mechanism Evaluation: Evaluate the existing countermeasures to data poisoning in FL that have been incorporated into systems in practice today both in terms of their technical and practical realizations. These could either be models or strategies that will be applied in practice, and their effectiveness and drawbacks will be assessed., as in Figure 3.

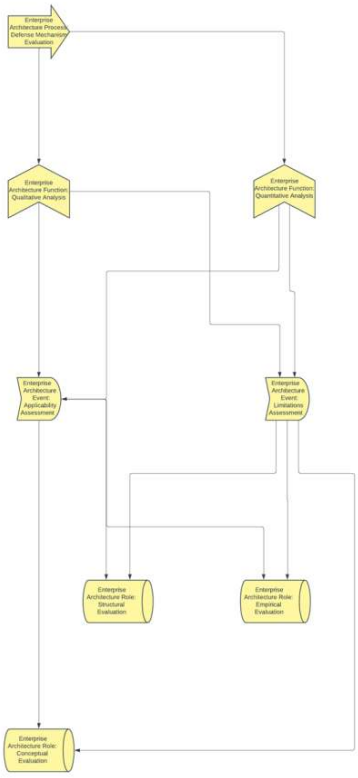


Figure 3. Defence Mechanism Evaluation

- Simulation and Testing: Implement the proposed methodologies in the simulated environment of a FL domain. Such measures should be tested to the level possible in order to determine how effective they can be in combating and eliminating data poisoning attacks on market information.

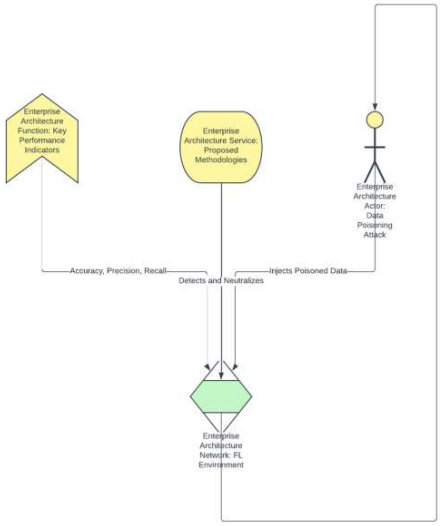


Figure 4. Simulation and testing

- Data Assessment: Examine the effects of the simulations concerning the achievement of the prescribed recommended actions. Conclusion will be made and statistical analysis presented in order to test the bent conclusions
- Reporting and Dissemination: Write the research results in one suitable report. Disperse the results in scientific publications and conferences as well as in the industry workshops in order to contribute to the existing knowledge as well as to the practitioners

IV. Result and Discussion

This research explores the advantages of using a Federated Learning (FL) approach to mitigate data poisoning attacks in Market Intelligence applications compared to traditional machine learning.

1. *Enhanced Data Security*

- Data Assessment: Evaluate how the simulations have impacted the end state with respect to the set target actions. A conclusion will be drawn, and relevant statistical methods employed, to evaluate the bent conclusions drawn within.
- Reporting and Dissemination: Document It will be necessary to write the research results in only one appropriate report. – Disseminate the results through scientific articles and conferences, and through the workshops in the industry aiming at enhancing the body of knowledge, and the practitioners.

2. *Preserved Data Privacy*

Data Minimization: FL only shares model updates, not raw market data, with the central server. This principle of data minimization reduces the risk of privacy breaches and helps comply with data protection regulations.

Differential Privacy Integration: FL readily accommodates differential privacy techniques. By adding noise to local model updates, differential privacy further protects individual client data and hinders attackers' ability to infer sensitive information or introduce targeted biases.

3. *Improved Model Robustness*

Diverse Data Sources: FL leverages diverse data sources, making the global model more robust to data poisoning from a small number of malicious clients. The aggregation process in FL can effectively dilute the impact of poisoned updates, especially when combined with robust aggregation techniques.

Adaptive Defenses: FL allows for the implementation of adaptive defense mechanisms. These defenses can dynamically adjust to the presence of attacks by analyzing the distribution of client updates, identifying outliers, and weighting contributions accordingly.

4. Increased Trust and Collaboration

Data Ownership and Control: FL empowers data owners (e.g., individual consumers, businesses) to retain control over their market information. This fosters trust and

encourages participation in collaborative market intelligence initiatives.

Auditable Updates: The decentralized nature of FL enables more transparent and auditable model updates. This facilitates the detection of anomalies and increases accountability, further strengthening trust in the system.

5. Real-time Market Insights

- On-device Processing: FL enables on-device processing of market information, allowing for real-time insights and faster response to market dynamics. This is particularly valuable in time-sensitive applications like fraud detection, risk assessment, and personalized marketing.

Table 1.

Comparison to Traditional Machine Learning

Feature	Federated Learning	Traditional Machine Learning
Data Storage	Decentralized	Centralized
Data Sharing	Model updates only	Raw data
Attack Surface	Reduced	Larger
Privacy	Enhanced	Vulnerable
Robustness	Higher	Lower
Trust	Increased	Limited
Real-time Insights	Enabled	Challenging

A. Conclusion

Federated learning offers significant advantages over traditional machine learning in mitigating data poisoning attacks in Market Intelligence applications. Its decentralized nature, privacy-preserving capabilities, and robust aggregation mechanisms enhance data security, model robustness, and trust among participants.

By enabling real-time insights while protecting sensitive market information, FL paves the way for more secure and collaborative market intelligence initiatives.

This research provides a good basis for further studies on the potential uses of Federated Learning (FL) in Market Intelligence. Based on the findings, here are some future research directions:

- Exploring the Dimensions of Robust Aggregation Techniques:

  Exploration of Advanced Methods: Explore and analyze the applicability of various robust aggregation techniques (for example, Median Aggregation, trimmed mean, Krum, Byzantine-resilient aggregation) in the context of data poisoning attacks of model aggregation matrices in Market Intelligence.

  Modification of Aggregation Measures: Create and modify aggregate measures so that they are responsive to the nature and degree of the data poisoning effort, including possible use of trust or reputation scores of data providers.

- An In-Depth Understanding of Fine-grained Privacy-Preserving Mechanisms:

  Personalized Differential Privacy: Evaluate the deploy ability of personalized differential privacy in FL for market intelligence whereby privacy protection is client sensitivity-level specific.

  Secure Multi-party Computation (MPC): Examine the possibilities of embedding MPC techniques into the FL architecture to further improve privacy by allowing model training with encrypted data.

- Some Implementation Challenges of FL in Market Intelligence. Scalability and Efficiency:

  Identify ways of implementing FL in Market Intelligence with a larger number of clients and large amounts of data in a short span of time with optimal communication costs.

  Heterogeneity: Tackle the issue of heterogeneity of client data and devices in Market Intelligence perspectives. Investigate methods such as federated transfer learning to enhance the model's performance over a multitude of data distributions.

- Increasing the Possibilities of FL Applications in Market Intelligence: Particular Use Cases:

  Evaluate the relevance of FL in performing specific Market Intelligence tasks including customer segmentation, demand forecasting, competitor analysis, and sentiment analysis.

  Fusion with Other Technologies: Investigate how FL can be integrated with emerging technologies such as blockchain for improved data security, tracking data provenance and incentivization mechanisms and applications in Market Intelligence.

- Ethical and Societal Considerations:

  Fairness and Bias: Identify the key sources of bias for FL models when applied to Market Intelligence modeling and develop mechanisms that enhance fairness and reduce the probability of discrimination.

  Transparency and Explainability: Develop measures to increase the transparency of FL models in Market Intelligence to enhance explainability and restore trust and accountability.

As far as these research directions are concerned, there is a great potential for improvement of secure, privacy-preserving and solid Market Intelligence applications utilizing Federated Learning.

REFERENCES

[1] Jodayree, M. He, W. Dr. Janicki, R. Preventing Image Data Poisoning Attacks in Federated Machine Learning by an Encrypted Verification Key, Procedia Computer Science, Volume 225, 2023.

[2] Thein, T. Shiraishi, Y. Morii, M. Personalized federated learning-based intrusion detection system: Poisoning attack and defense, Future Generation Computer Systems, Volume 153, 2024.

[3] Qi, P. Chiaro, D. Guzzo, A. Ianni, M. Fortino, G. Piccialli, F. Model aggregation techniques in federated learning: A comprehensive survey, Future Generation Computer Systems, Volume 150,2024.

[4] Fahd S. Alharithi, Ahmad A. Alzahrani, Enhancing environmental sustainability with federated LSTM models for AI-driven optimization, Alexandria Engineering Journal,Volume 108, 2024.

[5] Kumar, Abdul R. Ashraf, Waqar Nadeem, AI-powered marketing: What, where, and how?, International Journal of Information Management, Volume77, 2024.

[6] Terziyan,V. Malyk, D. Golovianko, M Branytskyi, V. Encryption and Generation of Images for Privacy-Preserving Machine Learning in Smart Manufacturing, Procedia Computer Science, Volume 217, 2023

[7] Thiyam, B. Dey, S. Efficient Feature Evaluation Approach for a class-imbalanced dataset using Machine learning, Procedia Computer Science, Volume 218, 2023

[8] Bach, M. Werner, A. Palt, M The Proposal of Undersampling Method for Learning from Imbalanced Datasets, Procedia Computer Science, Volume 159, 2019

[9] Zhou, T. Yan, H. Han, B. Liu, L. Zhang, J. Learning a robust foundation model against clean-label data poisoning attacks at downstream tasks, Neural Networks, Volume 169, 2024

[10] Karmakar, S. Mukherjee, A. Papamarkou, T Depth-2 neural networks under a data-poisoning attack, Neurocomputing, Volume 532, 2023