iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

POISONED DATA DETECTION USING FOR DISTRIBUTED MACHINE LEARNING TECHNIQUES

Mr. S. SATHISH KUMAR[1]
Assistant Professor, J.B. Institute of Engineering and Technology,
Hyderabad, Telangana, India,
S. Karthikeya[2] **, G. Venugopal**[3] **,S. Pradhyumna**[4]**, G. Vivek**[5]
UG Students, Department of Artificial Intelligence and Machine Learning,
J.B. Institute of Engineering and Technology, Hyderabad, Telangana, India,

ABSTRACT

Distributed Machine Learning (DML) facilitates large-scale model training across multiple nodes, improving efficiency and scalability. However, it is highly susceptible to data poisoning attacks, where adversaries inject manipulated data to degrade model performance. Detecting poisoned data in DML is essential for ensuring model reliability and security. This paper explores detection techniques such as anomaly detection, trust-based evaluation, and statistical analysis to identify malicious contributions. We implement and evaluate these methods in various DML environments to assess their effectiveness in mitigating adversarial threats. Experimental results demonstrate that our approach significantly improves model robustness while maintaining computational efficiency.

Keywords:
Distributed Machine Learning, Data Poisoning, Anomaly Detection, Model Security, Trust-Based Evaluation, Adversarial Attacks, Secure Learning.

INTRODUCTION

In distributed systems, when there is too much data for one computer to handle quickly, we use something called distributed ML. This means that we split up the data and give it to different computers to work on. These computers then share their results with a main computer, which puts everything together to make a final model. However, it is getting harder to keep all the computers safe as more and more of them are used. If there is a mistake in the security, bad people might change the information that is used to teach computers. One way they can do this is by adding bad information to the data. This is more likely to happen because of the mistake. It was a big problem, especially when the people who are working on the computer are in different places and need to use new information often to make decisions. Scholars are paying close attention to this ML risk. Initially, Dalvi et al. showed that if an attacker had all the knowledge, they could modify the data to make the data miner fail. Subsequently, Lowd et al. shown that attackers may create assaults using partial knowledge, proving the impracticality of the perfect information assumption. Following then, a number of studies were carried out with an emphasis on the setting of non-distributed ML. There have been several recent initiatives focused on stopping data manipulation in DML. For instance, game theory was applied by Zhang et al. and Esposito et al. to develop safe algorithms for collaborative deep learning and distributed support vector machine (DSVM), respectively

OBJECTIVES

1. **Identify Data Poisoning Attacks**
   - Detect adversarial manipulations in distributed machine learning models.
   - Classify different poisoning techniques (e.g., label flipping, data injection, backdoor attacks).
2. **Develop Robust Detection Mechanisms**
   - Implement anomaly detection methods to identify poisoned data.

   - Use statistical and machine learning techniques to recognize unusual patterns.
3. **Enhance Model Security & Accuracy**
   - Maintain high accuracy while filtering out malicious contributions.
4. **Efficient Distributed Processing**
   - Optimize detection algorithms for decentralized and federated learning environments.
   - Minimize computational overhead while ensuring real-time detection.
5. **Evaluate Performance Metrics**
   - Measure false positive and false negative rates of the detection system.
   - Ensure minimal impact on overall model efficiency.
6. **Scalability & Generalization**
   - Ensure the detection system adapts to different datasets and ML architectures.
   - Develop a scalable framework for large-scale distributed learning.

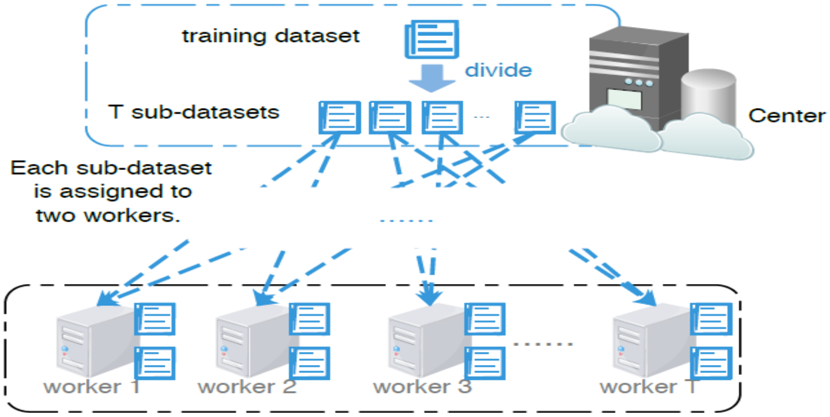
METHODOLOGY

Distributed machine learning, often known as DML, may generate massive dataset training in scenarios where a single node is unable to generate accurate results within an acceptable time frame. Contrary to the non-distributed system, this will inevitably expose more potential targets to attackers.

Using this method, unusual values will be found in the training dataset and removed. The Data Poison approach allows us to increase the accuracy of ML systems

We have evaluated performance of existing SVM and DML where existing SVM will not apply Data Poison Detection technique and DML approach will employ Data Poison technique.

Data Poison Detection is a technique used by authors to identify and eliminate altered data in distributed environments where attackers may alter training data and cause ML to anticipate incorrect results. Using this method, unusual values will be found in the training dataset and removed. The Data Poison approach may be used to increase the accuracy of ML systems The two distributed methodologies used in this research are Basic DML and Semi DML.



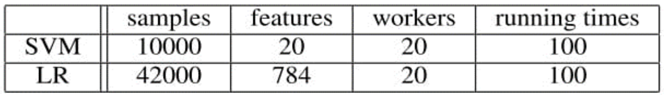
The working flow of the proposed method is as follows.

- Upload Dataset
- Divide Dataset
- Model Generation
- Distribute Dataset & Run Basic-DML
- Run Semi-DML
- Accuracy Comparison Graph

1. Upload Dataset:

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Gathering the pertinent dataset for the issue area should come first. Make that the dataset is suitably big, representative, and diversified.
2. Divide Dataset:
Divide the dataset into subsets that are suitable for testing, validation, and training. Typical ratios for training, validation, and testing sets are 70-15-15 or 80-10-10, respectively.
3. Model Generation:
A ML model appropriate for the given job (e.g., regression, classification).
B. Create the architecture, set up the hyperparameters, and use the training dataset to train the model.
4. Distribute Dataset & Run Basic-DML:
a. In a decentralized system, distribute the training dataset among several participants or nodes.
b. To safeguard individual data privacy during model training, use Basic Differential Privacy Machine Learning (Basic-DML) approaches.
5. Run Semi-DML:
i. Use semi-supervised or semi-differential privacy ML approaches to improve the privacy protection and resilience of your model.
ii. Optimize the model's generalization on the training dataset while respecting privacy.
6. Accuracy Comparison Graph:
I. Assess the model's effectiveness using the test and validation datasets.
II. Create measures for accuracy and use a comparison graph to highlight the model's performance in different settings.



	samples	features	workers	running times
SVM	10000	20	20	100
LR	42000	784	20	100

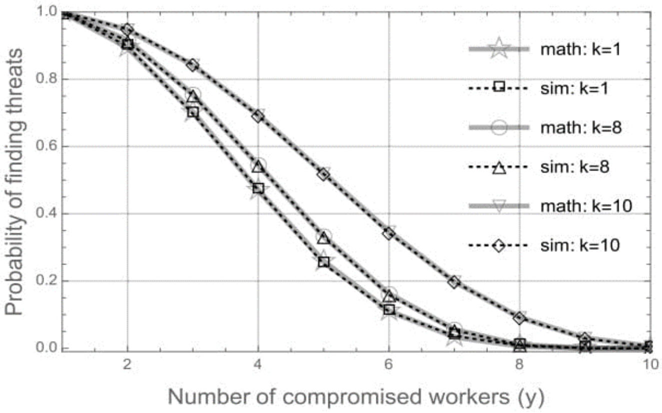


Fig 1: Overall results comarision

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

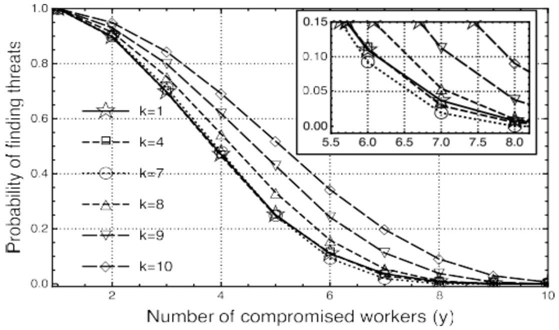


Fig 2: Comparison between compromised workers with finding threats.

In the basic-DML scenario, the PFT is shown in figure 3 for k = 1, 4, 7, 8, 9, and 10. There is a clear trend between the three lines representing k = 1, 4, and 7 in the figure; as y increases from 1 to 6, the trend slows down to zero, and as y increases from 6 to 10, the trend slows down even more. Starting at k=7, the PFT clearly increases as it moves to k=8, and it continues to do so until k=10, when it reaches its maximum value.

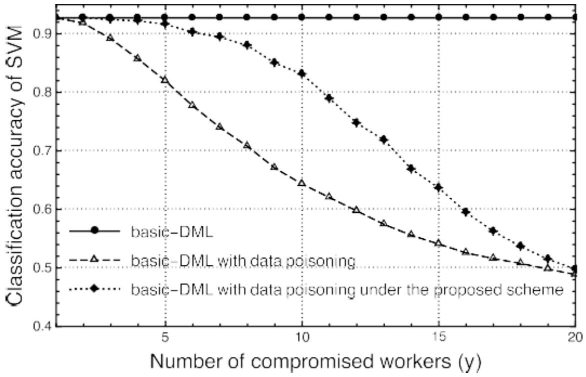


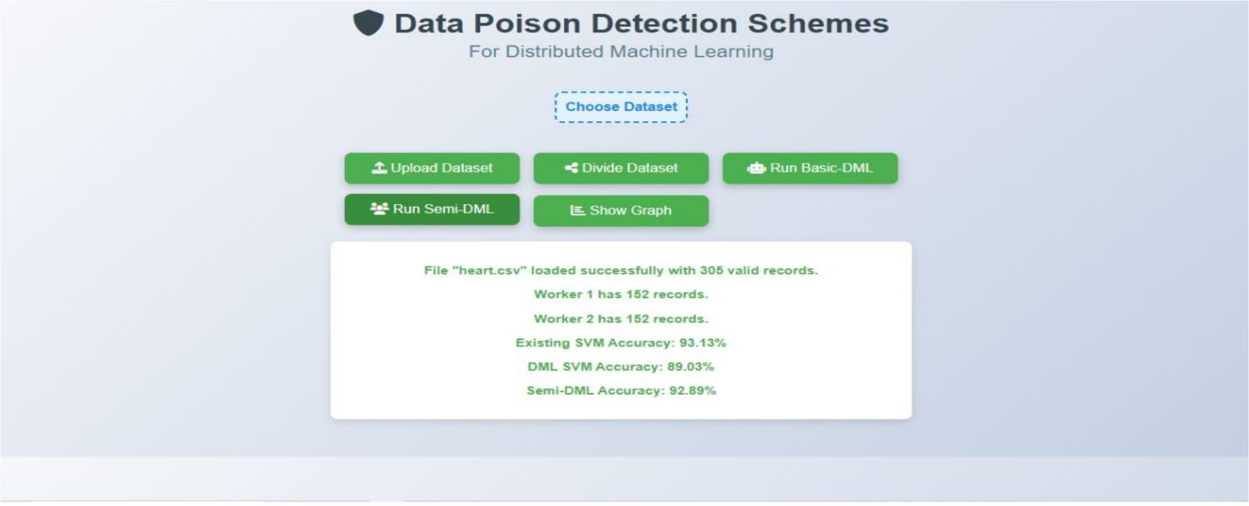
***Fig 3: Comparison between compromised workers with Accuracy*.**

Figure 2.3 shows the standard-DML with SVM classification accuracy in three cases: no data poisoning, data poisoning without the suggested scheme, and data poisoning with the suggested scheme. The classification accuracy is close to 93% in the basic-DML scenario where data poisoning is not present. As the number of impacted workers increases, the classification accuracy would progressively decline from 93% to almost 50% if data poisoning were to impact the basic-DML system.

RESULTS AND DISCUSSIONS

In this research, we introduced a refined data poison detection technique that, with the help of the central resource, offers enhanced learning protection. One way to make the most of the system's resources is to find the best way to distribute them. In the basic-DML situation, the indicated approach can enhance the final model's accuracy by 60% for logistic regression and up to 20% for support vector machine, according to the simulation findings.

Based on the results shown in figure 2, it is clear that the mathematical model can accurately derive the PFT in the suggested scheme, as the results match the simulation results well. In addition, it is evident from both sets of data that the simulation's maximum value of k, which is 10, represents the ideal number of training cycles.



File "heart.csv" loaded successfully with 305 valid records.
Worker 1 has 152 records.
Worker 2 has 152 records.
Existing SVM Accuracy: 93.13%
DML SVM Accuracy: 89.03%
Semi-DML Accuracy: 92.89%

Fig 1: Data Poison Detection Schemes For Distributed Machine Learning

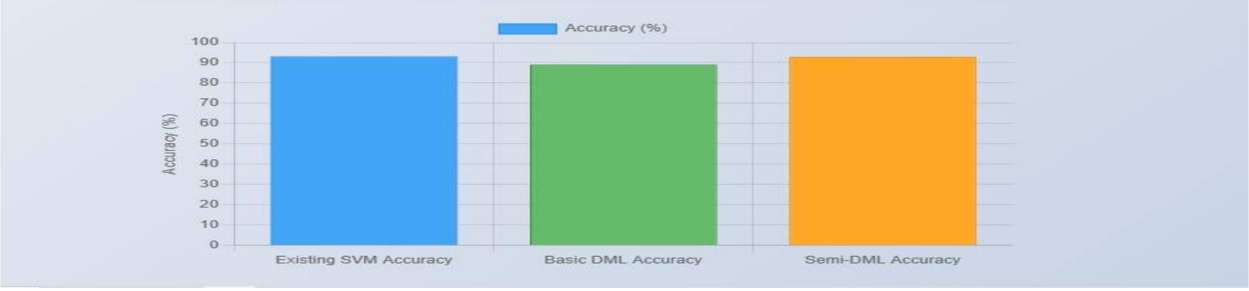


Fig 2: Accuracy (%) Of DML

ACKNOWLEDGMENT

We would like to express our sincere gratitude to all those who contributed to the successful completion of this research on **Poisoned Data Detection Using Distributed Machine Learning Techniques**. First and foremost, We extend our sincere gratitude to Dr. Mr. S. SATHISH KUMAR (Assistant Professor) for his invaluable guidance and support throughout this research. We also thank the faculty members of the Department of ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING, J.B. Institute of Engineering & Technology, for their insights and encouragement.

CONCLUSION AND FUTURE SCOPE

In this work, we learned about ways to find bad data in different situations. We use certain rules to figure out which parts of the data are bad in one situation, and we also made a math model to help us know how likely it is to find bad things as we keep looking at the data more and more times. Additionally, we demonstrated the best resource allocation in the semi-DML situation as well as an enhanced data poisoning detection technique. The suggested plan can make the models more accurate by up to 20% for support vector machines and 60% for logistic regression in a basic situation. Compared to other plans that don't use resources efficiently, this improved technique can reduce wasted resources by 20-100% in a more advanced situation.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

REFERENCES

[1] G. Qiao, S. Leng, K. Zhang, and Y. He, “Collaborative task offloading in vehicular edge multi-access networks,” IEEE Communications Magazine, vol. 56, no. 8, pp. 48–54, 2018.

[2] K. Zhang, S. Leng, X. Peng, L. Pan, S. Maharjan, and Y. Zhang, “Artificial intelligence inspired transmission scheduling in cognitive vehicular communications and networks,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1987–1997, 2019.

[3] V. N. Thatha, B. VeerasekharReddy, G. VenuGopal, K. Ashok, S. Maddu and S. V, "An Enhanced Support Vector Machine Based Pattern Classification Method for Text Classification in English Texts," 2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, India, 2023, pp. 1-6, doi: 10.1109/CSITSS60515.2023.10334170.

[4] S, Phalguna &Thatha, Venkata&Mamidisetti, Gowtham&Mantena, Srihari &Chintamaneni, Phanikanth&Vatambeti, Ramesh. (2023). Hybrid deep learning model with enhanced sunflower optimization for flood and earthquake detection. Heliyon. 9. e21172. 10.1016/j.heliyon.2023.e21172.

[5] L. Zhou, S. Pan, J. Wang, and A. V. Vasilakos, “Machine learning on big data: Opportunities and challenges,” Neurocomputing, vol. 237, pp. 350– 361, 2017.

[6] S. Yu, M. Liu, W. Dou, X. Liu, and S. Zhou, “Networking for big data: A survey,” IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 531–549, 2017.

[7] M. Li, D. G. Andersen, J. W. Park, A. J. Smola, A. Ahmed, V. Josifovski, J. Long, E. J. Shekita, and B.-Y. Su, “Scaling distributed machine learning with the parameter server.” in 11th USENIX Symposium on Operating Systems Design and Implementation (OSDI), vol. 14. USENIX Association, 2014, pp. 583–598.

[8] D. Sandeep, G. Bhuvana, T. Aishwarya, C. Vivek and K. Manikanta, "Securable Personal Healthcare Record in Cloud Storage," 2023 3rd Asian Conference on Innovation in Technology (ASIANCON), Ravet IN, India, 2023, pp. 1-6, doi: 10.1109/ASIANCON58793.2023.10270484.