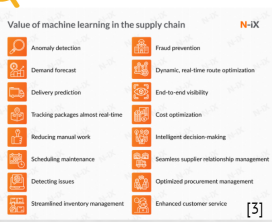
Machine Learning, Privacy & Supply Chains

Research Question:

How can privacy be preserved for machine learning based applications in supply chains?

01: Introduction

- Supply chains are vital in the modern age
- Machine Learning applications exist in several aspects of supply chains
- Vulnerabilities exist, and privacy concerns arise, especially related to sensitive data



[3]

02: Objective

The case for privacy-preservation for ML applications in supply chains:

- Adoption of ML solutions in supply chains is increasing [6]
- ML solutions offer increased efficiency for supply chain management [8]
- Organizations are reluctant to implement ML solutions due to privacy concerns

Advantageous Machine Learning Applications:

- Demand Forecasting and Forecasting Accuracy
  - Significant advantages in accuracy over traditional methods
  - Models may be susceptible to attacks
- Customer/Supplier Relations Using Chat-bots
  - Improved performance of chat-bots, large reductions in expenses [1]
  - Several privacy issues concerning training data exist

03: Method

Literature reviews of existing sources will be conducted, with the use of Google Scholars, WorldCat, IEEExplore, and other similar tools from the TULib resources.

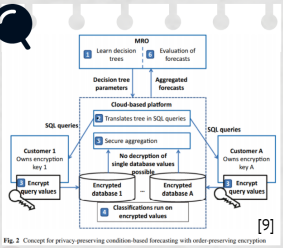
Research Method Steps:

1. Identify privacy concerns in Supply Chains
2. Identify threats to privacy in Machine Learning applications
3. Discover privacy-preserving techniques for machine learning applications
4. Determine connections between uses of machine learning and supply chains
5. Determine privacy-preserving techniques to address issues

04: Results - Threats

Related mostly to sensitive data. Following attacks pose risks [2]:

- Model Inversion Attacks
- Reconstruction Attacks
- Membership Inference Attacks
- Re-Identification



[9]

Fig. 2 Concept for privacy-preserving condition-based forecasting with order-preserving encryption

05: Results - Potential Solutions

Cryptographic Approaches

- Cryptographic Protocols
  - Good for custom solutions
  - Can be slow and remain susceptible to some attacks [9]
- Homomorphic Encryption
  - High level of privacy preservation and safeguards against various attacks
  - Can be costly or lack functionality depending on situation [2]
- Garbled Circuits
  - Significantly fast operations compared to other approaches [7]
  - More than two parties cannot collaborate

Differential Privacy With Perturbation Approaches

- Input and Output Perturbation
- Algorithmic Perturbation
  - Useful for safeguarding against re-identification, reconstruction, and inference attacks [5]
  - Lossy encryption reduces accuracy

06: Conclusion

- Significant benefits are possible by using machine learning in supply chains
- Organizations are reluctant to implement efficient solutions due to privacy concerns
- Some existing implementations of ML do not take special care for privacy
- Cryptographic approaches and differential privacy can be used for different applications, especially in demand forecasting and chat-bot development and training.

Potential Area for Future Work

- Demand forecasting in Fast Fashion industry's supply chains

07: References

[1] Martin Adam, Michael Wessel, and Alexander Benlian. Ai-based chatbots in customer service and their effects on user compliance. Electronic Markets, Mar 2020.

[2] Mohammad Al-Rubaie and J. Morris Chang. Privacy preserving machine learning: Threats and solutions. CoRR, abs/1804.11238, 2018.

[3] Kostiantyn Bokhan. Machine learning in supply chain: 8 use cases that will impress you, Nov 2020.

[4] Real Carbonneau, Kevin Laframboise, and Rustam M. ˙ Vahidov. Application of machine learning techniques for supply chain demand forecasting. Eur. J. Oper. Res., 184(5):1140–1154, 2008.

[5] Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. Found. Trends Theor. Comput. Sci., 9(3-4):211–407, 2014

[6] Vikas Hassija, Vinay Chamola, Vatsal Gupta, Sarthak Jain, and Nadra Guizani. IEEE Internet Things J., 8(8):6222–6246, 2021.

[7] Yan Huang, David Evans, Jonathan Katz, and Lior Malka. Faster secure two-party computation using garbled circuits. In 20th USENIX Security Symposium, San Francisco, CA, USA, August 8-12, 2011, Proceedings. USENIX Association, 2011.

[8] Ashvin Kochak and Suman K Sharma. Demand forecasting using neural network for supply chain management. 2014.

[9] Fabian Taigel, Anselme K. Tueno, and Richard Pibernik. Privacy-preserving condition-based forecasting using machine learning. Journal of Business Economics, 88(5):563–592, Jul 2018.

By: Ayush K. Joshi
a.k.joshi@student.tudelft.nl
CSE3000 - Research Project
Group 49

Department of Intelligent Systems
Cyber Security Group
Delft University of Technology

Supervisors: Tianyu Li, Zekiriya Erkin

TU Delft