A Unified Data Security Framework for Federated Prognostics and Health Management in Smart Manufacturing

Behrad Bagheri[1*], Maryam Rezapoor[2], Jay Lee[1]

[1]*NSF Industry/University Cooperative Research Center on Intelligent Maintenance Systems (IMS), University of Cincinnati, Cincinnati, OH, United States*

[2]*Haas School of Business, University of California Berkeley, Berkeley, CA, United States*

** Corresponding author: bagherbd@mail.uc.edu*

Abstract

Data security is one of the most important concerns of manufacturing entities. Therefore, enterprises hesitate to share data with third parties for building predictive and prognostic models. In such scenario, building comprehensive models for predicting asset failures is challenging given data from a single enterprise would not include required variety of operation regimes and failure modes. In this article, we present an encrypted and federated framework for training diagnosis and prognosis models that would not require sharing data. The proposed framework guarantees the privacy of the data while generates comprehensive models that leverage the variety of multiple enterprises operations.

1 Introduction

The advent of the Internet of Things (IoT) and initiatives such as Industry 4.0 and Cyber-physical systems have directed enterprises to gather and process more data. Moreover, the increasing availability of computing power and advancement of data analysis techniques lead into development and implementation of advanced predictive and prognostics models in manufacturing settings [1].

Data-driven Prognostics and Health Management (PHM) models require a variety of asset and fleet-level data to generate reliable outputs [2]. Despite the ever growing availability of sensory data from machines, the volume of “event” data per asset that represents failures is low due to the not-to-fail tendency of machines; moreover, due to operational variation, machines do not present all degradation and failure patterns in their lifetime (Figure 1). Therefore, training a comprehensive PHM model that is capable of detecting all failure patterns require high volume and variety datasets. Preparing such dataset from only one enterprise is difficult given the number of assets and operational condition per enterprise is limited.

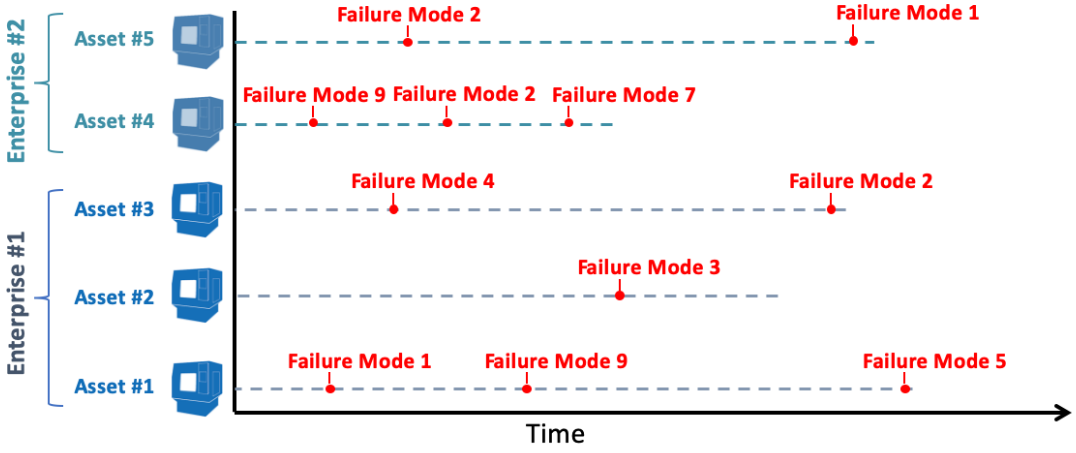

Figure 1 - Similar instances of a machine experience various failure patterns during their operation life. A comprehensive PHM model requires knowledge sharing between assets and organizations to perform properly.

One plausible solution for building comprehensive PHM models is aggregating operational data from multiple enterprises. While this approach increases the probability of accessing a wider range of failure modes and degradation patterns, it has two major flaws: First, enterprises consider their operational data as trade secret. McKinsey & Company reports cyber-security and data ownership are two major barriers for manufacturing companies toward working with third-party providers such as scientists [3]. This data privacy concern has created significant limitations in the possibility of gathering inter-organizational datasets for training PHM models.

Second, the data is currently being stored in silos around the world. Transferring or physically shipping these datasets to a central processing hub (e.g. a cloud server) is not an efficient solution. Even recent advancements in cloud computing and the use of cloud-based solutions has merely addressed the concern of centralized data storage, and has led to the emergence of fog[4] and edge computing [5] solutions. In this article, we present a novel approach for decentralizing PHM by introducing Encrypted Federated PHM framework.

2 Encrypted Federated PHM (EF-PHM) Framework

The primary objective of this article is to address the data privacy and security concerns in Industry4.0 environments by proposing a framework that enables training PHM models without sharing and directly accessing the data. We propose a homomorphically encrypted[6] federated [7] PHM (EF-PHM) framework that enables enterprises to leverage a comprehensive PHM model without sharing their data. In this section we introduce the underlying technologies for EF-PHM and then describe the framework.

2.1 Underlying Technologies

The EF-PHM framework leverages the following state of the art technologies:

2.1.1 Federated Learning

Federated learning enables training machine learning models on distributed clients without requiring the nodes to share data [7]–[9]. In such an environment, instead of gathering data from clients, we distribute the model among clients. In this manner, the client, which in the context of manufacturing is an enterprise, would receive and train the model with their local data. After training, the updated model properties such as weights and biases, is sent to the server for aggregation. After several iterations of this process, a global master model can be generated without directly accessing their data.

2.1.2 Homomorphic Encryption

Homomorphic encryption (HE) is a form of data encryption that preserves the structure of the message space to make arithmetic operations possible over the ciphertext [10], [11]. HE enables aggregation of encrypted values with basic math operations without knowing actual values. Although reverse engineering operational data from model parameters on complex models is nearly impractical, the use of homomorphic encryption in EF-PHM acts as additional privacy preserving measure for the model updates that are shared outside the enterprise network.

2.1.3 Block Chain

Using blockchain is not a necessity for EF-PHM framework but it provides an extended security to the inter-organization communications. A blockchain is an immutable public ledger that consist of series of data blocks that are connected to each other via a hash value. The hash value is a function of the current block contents and previous block, therefore any modification of the current or previous blocks of data would result in break of the chain. In 2017, Marfia and Esposti, introduced the use of blockchain to bring transparency in manufacturing and discussed the use sensory data along with blockchain for reputation tracking and as proof of local production [18].

2.2 EF-PHM Components and Operational Process

We define three main components of the EF-PHM framework as Master Agent, Federated Agent, and EF-PHM Network.

The Master Agent is a software program that independently manages the federated agents. It initiates model update rounds where it requests encrypted updates from a randomly ordered set of federated agents. Then the Master Agent, aggregates the encrypted updates and pushes the new model to agents.

Federated Agents are software programs that are deployed to the enterprises. They act as the only bridge between the enterprise secure network and the public EF-PHM network on solely transfer encrypted model updates. Federated agents have the liberty of deciding if they want to participate in an update round initiated by the Master Agent. During each update round, federated agent receives an encrypted update and applies it to the local PHM model. Then it performs several training iterations using the local data and calculates changes to the local model as a result of the training. Finally, it homomorphically encrypts this update and securely sends it to the Master Agent for aggregation

The EF-PHM network is the communication infrastructure for the framework which could be over the Internet or a public Blockchain. These components and their roles are visualized in Figure 2.

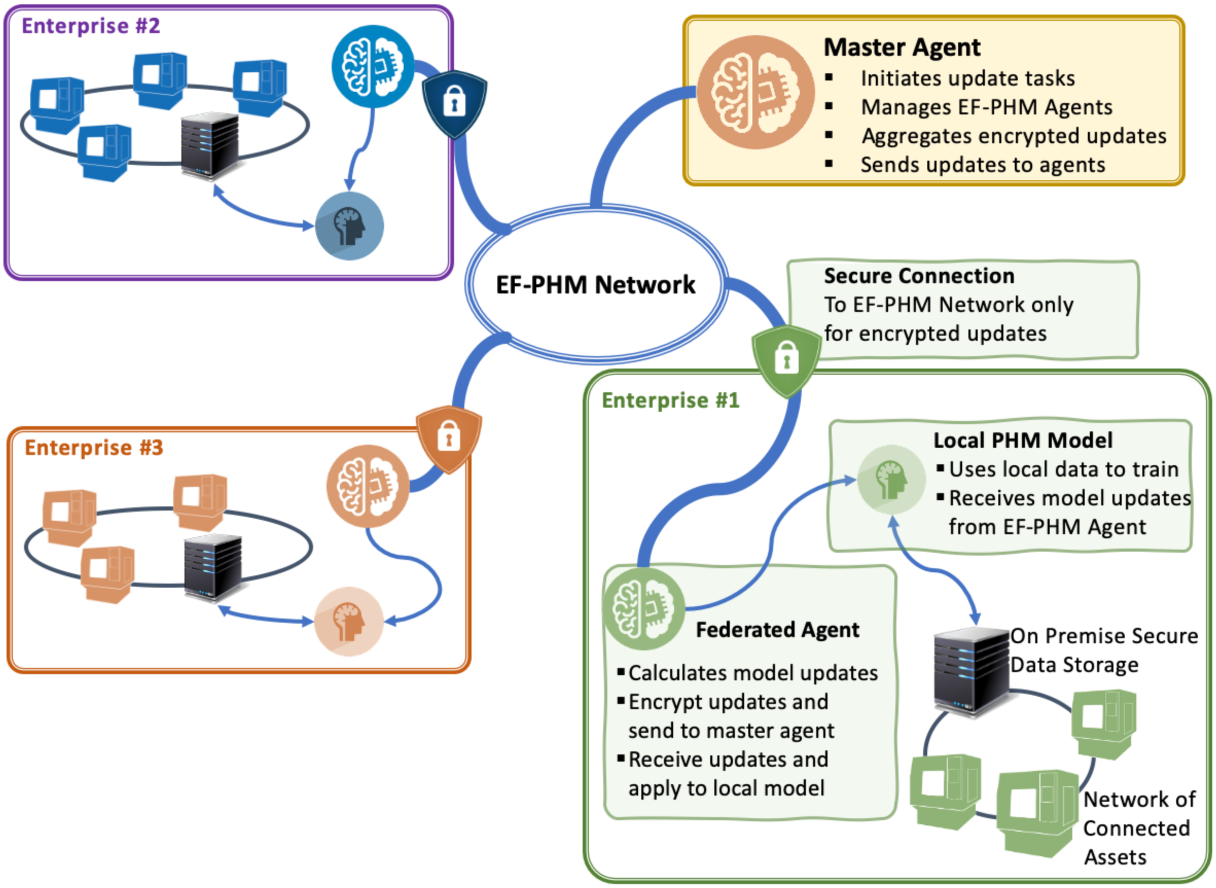

Figure 2 Overall design of the federated learning PHM

3 EF-PHM in 5C CPS Architecture

In 2015, we introduced a five level (5C) architecture for Cyber-Physical Systems [12]. EF-PHM complements 5C and provides infrastructure for implementing it in practice. In this section we briefly discuss how EF-PHM impacts each level of the 5C architecture:

- *Connection*: The proposed framework promotes Edge Computing enhances the network communication by significantly reducing the payload size.
- *Conversion*: with the decentralized nature of the proposed framework, data to information conversion would occur at the edge. It requires on premise computation which enables enterprises to keep their data within their secure network.
- *Cyber:* EF-PHM carries out the secure knowledge sharing, and aggregation required for cyber-agents at the cyber level of the 5C architecture in a decentralized manner. With the proposed encrypted differential updates, these inter-organization communications are secure against cyber-attacks.
- *Cognition:* EF-PHM enable digital twins [12] to improve their self-awareness given the extended shared knowledge between enterprises.

- *Configuration:* the proposed framework has potential to be used for configuration sharing amongst the participants. In the same fashion of learning the failure modes through differential model updates, optimal configuration realization is also possible using this framework.

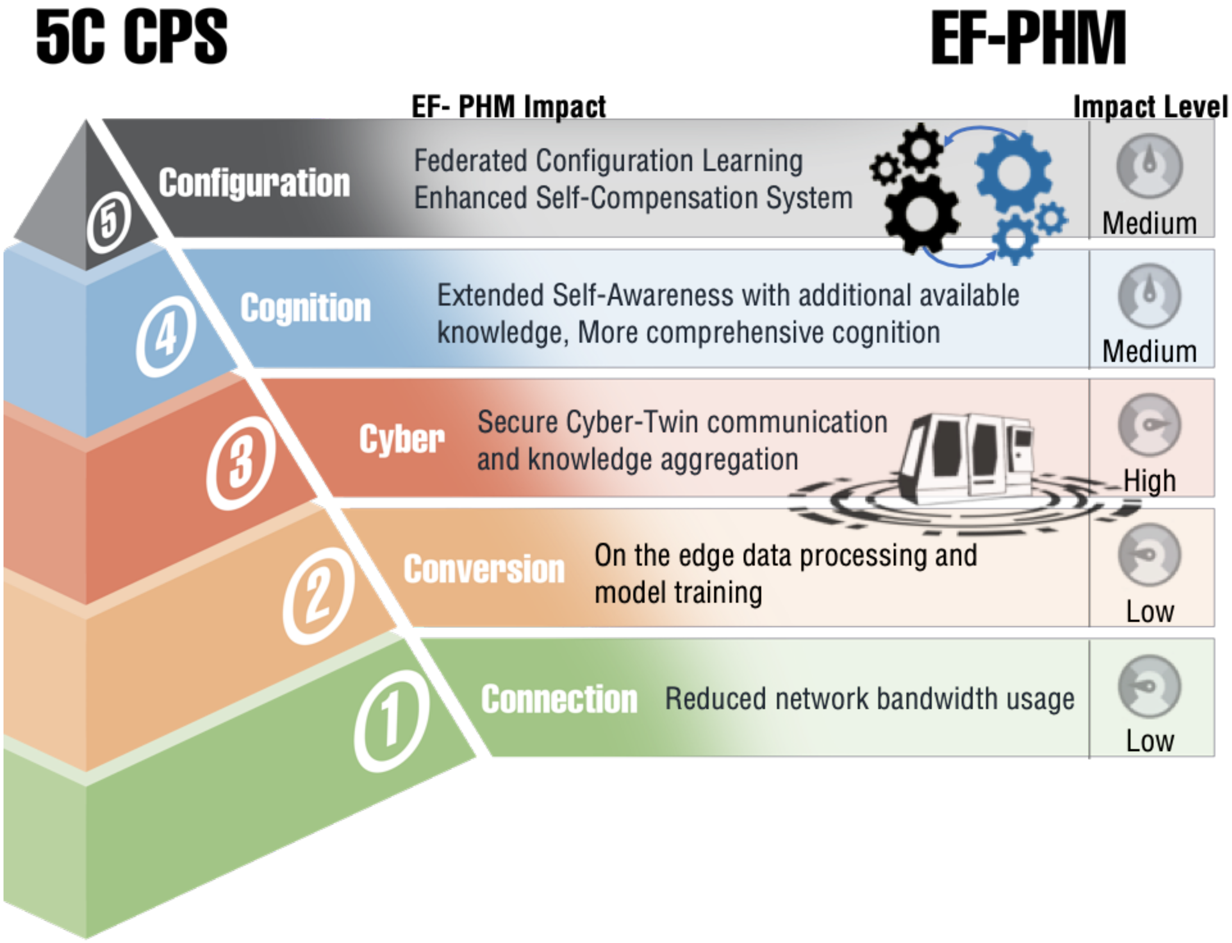
5C CPS
EF-PHM
EF- PHM Impact
Impact Level
5
Configuration
Federated Configuration Learning
Enhanced Self-Compensation System
Medium
4
Cognition
Extended Self-Awareness with additional available knowledge, More comprehensive cognition
Medium
3
Cyber
Secure Cyber-Twin communication and knowledge aggregation
High
2
Conversion
On the edge data processing and model training
Low
1
Connection
Reduced network bandwidth usage
Low

Figure 3 EF-PHM Framework in 5C CPS Architecture

4 Discussion and Integration Challenges

Although the EF-PHM framework enables implementation of cross-enterprise PHM solutions, its real-world application imposes challenges. First, for the framework to be viable, multiple enterprises should participate, which requires convincing of leadership of enterprises as discussed in section 5. Second, participation of multiple enterprises does not necessarily result in high performing framework; in the cases that one or more faults are dominant across all participating enterprises and/or the dataset lacks one or more failure modes, the resulted PHM model would not perform as expected. Third is addressing variation in working regimes; in traditional PHM separate models can handle various working regimes. In the proposed setting, identifying working regimes is more challenging given it requires sharing the data among enterprises. In this case, usage of more complex models (such as deep neural networks) is a potential solution.

5 Business Strategy - Game Theory Analysis

We acknowledge that the EF-PHM is a new framework and its practicality requires enterprise managers to make an unprecedented decision to implement. To give informed support to this decision, we model the situation using game theory and introduce a 2-player game in which players have two options: participating in EF-PHM (P) or not participating (NP). In the NP case, we assume that the enterprise is engaged in the conventional data analysis practice and therefore we omitted the fixed implementation costs of data acquisition, handling, and processing from both P and NP cases. For simplicity, we assume the new knowledge each enterprise provides (x) is equal and mutually exclusive from what others offer, therefore, the total extent of shared knowledge has linear relationship with number of participating enterprises (n). By this definition, the participating players earn the value of $y = n \times x$. For the non-participating player, we define C as the cost of sharing data with third parties for building PHM models, therefore, their final earned value is $y'_{NP} = x - C$. We also introduce Switching Cost (S) accounting for resistance to change. Therefore, the final earned value for participating parties is $y'_P = (n \times x) - S$.

This game theory analysis suggests that the dominant strategy is dependent on number of participants (n) and their switching costs (S). With very low participation (very small n) and high switching cost due to uncertainty, the dominant strategy falls on NP-NP. As the number of participants grows, the total payoff increases, and the switching cost reduces, therefore participating in EF-PHM will become the dominant strategy for all players and the (P-P) is the equilibrium. This model can yield valuable competitive insights, improves internal alignment around the decision and maximizes strategic utility of the EF-PHM framework.

Table 1 EF-PHM Payoff matrix

	P	NP
P	$(n \times x) - S\,, (n \times x) - S$	$\big((n-1) \times x\big) - S, x - C$
NP	$x - C, \big((n-1) \times x\big) - S$	$x - C, x - C$

6 Conclusions

In this article we introduced EF-PHM framework that facilitates cross-enterprise PHM model training, enables development of comprehensive PHM models, and improves the practicality of the 5C CPS architecture that we previously published in 2015. We discussed its integration challenges and used game theory analysis to further review business implications. The future work will include designing a solution for automatically determining the working regime and sharing it among the network agents without violating privacy;

Declaration of Competing Interest

None.

References

[1] J. Lee, B. Bagheri, and C. Jin, "Introduction to cyber manufacturing," *Manuf. Lett.*, vol. 8, pp. 11–15, 2016.

[2] J. Lee, F. Wu, W. Zhao, M. Ghaffari, L. Liao, and D. Siegel, "Prognostics and health management design for rotary machinery systems—Reviews, methodology and applications," *Mech. Syst. Signal Process.*, vol. 42, no. 1–2, pp. 314–334, Jan. 2014.

[3] McKinsey Digital, "Industry 4.0 after the initial hype Where manufacturers are finding value and how they can best capture it," 2016.

[4] S. Yi, C. Li, and Q. Li, "A Survey of Fog Computing: Concepts, Applications and Issues," *Proc. 2015 Work. Mob. Big Data - Mobidata '15*, pp. 37–42, 2015.

[5] G. I. Klas, "Fog Computing and Mobile Edge Cloud Gain Momentum Open Fog Consortium , ETSI MEC and Cloudlets," pp. 1–14, 2015.

[6] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," *Proc. 3rd ACM Work. Cloud Comput. Secur. Work. - CCSW '11*, p. 113, 2011.

[7] J. Konečný, H. B. McMahan, D. Ramage, and P. Richtárik, "Federated Optimization: Distributed Machine Learning for On-Device Intelligence," pp. 1–38, 2016.

[8] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated Learning: Strategies for Improving Communication Efficiency," pp. 1–10, 2016.

[9] B. McMahan and D. Ramage, "Federated Learning: Collaborative Machine Learning without Centralized Training Data," 2017. [Online]. Available: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html.

[10] E. Hesamifard, H. Takabi, and M. Ghasemi, "CryptoDL: Deep Neural Networks over Encrypted Data," pp. 1–21, 2017.

[11] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A Survey on Homomorphic Encryption Schemes: Theory and Implementation," pp. 1–35, 2017.

[12] J. Lee, B. Bagheri, and H.-A. Kao, "A Cyber Physical Systems Architecture for Industry 4.0-based Manufacturing Systems," *Manuf. Lett.*, vol. 3, pp. 18–23, Dec. 2015.