Fortifying Multi-Agent Architectures in Smart Manufacturing: Leveraging Federated Learning and Blockchain for Security and Resilience

Petro M. Tshakwanda*, Henok B. Tsegaye†, Raddad Almaayn‡, Michael Devetsikiotis§
*‡§Department of Electrical and Computer Engineering, University of New Mexico, USA
†Department of Information Engineering and Computer Science, University of Trento, Italy
{*pmushidi, ‡raddadalmaayn, §mdevets}@unm.edu, †henokberhanu.tsegaye@unitn.it

2025 IEEE 22nd Consumer Communications & Networking Conference (CCNC) | 979-8-3315-0805-0/25/$31.00 ©2025 IEEE | DOI: 10.1109/CCNC54725.2025.10975963

***Abstract*—This work presents a blockchain-based communication architecture for multi-agent smart manufacturing systems, enhanced with federated learning to improve security, data privacy, and scalability. Comparative evaluation with traditional centralized systems across various configurations reveals that our approach achieves up to 12% higher model accuracy and 15% greater security, particularly in large-scale deployments, with scalability scores surpassing those of centralized systems by 18% as agent numbers increase. Although initial latency and energy consumption are higher, these factors improve significantly as the system scales, indicating suitability for complex manufacturing networks. This research underscores the potential of combining federated learning and blockchain to enhance resilience, security, and efficiency in Industry 4.0 smart manufacturing systems.**

***Index Terms*—Blockchain, Federated Learning, Security, Scalability, Smart Manufacturing, Industry 4.0.**

I. Introduction

Centralized smart manufacturing systems face challenges such as single points of failure, scalability issues, and data privacy concerns. Traditional architectures often lack transparency and struggle to adapt to real-time dynamic conditions. This work proposes a decentralized architecture combining federated learning and blockchain to address these limitations. Federated learning ensures secure, decentralized model training, preserving data privacy [1], [2], while blockchain enhances data integrity and transaction traceability [3]. By merging intelligent agents, federated learning, and blockchain, we optimize manufacturing processes through decentralized decision-making and enhanced responsiveness. This approach addresses transparency and accountability issues, enabling research in cooperative intrusion detection and explainable AI (XAI), thereby enhancing cybersecurity and fostering trust in the ecosystem trust [4]. Key challenges include designing secure multi-agent architectures, developing intrusion detection mechanisms, exploring XAI, and addressing scalability and interoperability [2], [4]. Our work aims to enhance data privacy, system optimization, and secure model aggregation in multi-agent systems, advancing trustworthy AI in smart manufacturing for more efficient, secure, and adaptive Industry 4.0 processes.

II. Proposed Architecture

This section presents a secure, resilient multi-agent architecture for smart manufacturing using federated learning and blockchain, aligned with NIST's Smart Manufacturing Ecosystem framework [5]. It integrates product lifecycle, production systems, and business operations.

As shown in Figure 1, the architecture comprises four layers:

- **Integration Layer**: Integrates data, processes, and systems across SME dimensions.
- **Smart Manufacturing Environment**: The core layer for manufacturing processes and decision-making.
- **Federated Trust Layer**: Leverages blockchain and federated learning (FL) to ensure security and privacy. FL enables collaborative model training while preserving data privacy, formalized as:

$$w_{t+1} = w_t + \eta \sum_{k=1}^{K} \frac{n_k}{n} (w_t^k - w_t) \tag{1}$$

  where w_t is the global model, w_t^k is the local model, η is the learning rate, and n_k is the number of data points at agent k. A private Ethereum network (Ganache) ensures secure data management with a custom consensus algorithm and smart contracts.
- **Edge Layer**: Hosts intelligent agents for process control, predictive maintenance, quality control, and resource allocation.

The architecture includes security and resilience features such as encrypted communication, blockchain-based verification, privacy-preserving training, continuous monitoring, adaptive threat response, and distributed consensus.

Algorithm 1 details the federated learning process in our manufacturing network, corresponding to Equation (1).

III. Methodology and Evaluation Metrics

The experimental setup includes up to 100 intelligent agents, a federated learning server, a private Ethereum blockchain with 10 validator nodes, and a simulated smart manufacturing environment. Experiments with 20, 50, and 100 agents compare a baseline (centralized ML without blockchain) to the proposed federated learning with blockchain approach using Adaboost, repeated 10 times for statistical significance. Data is collected from sensors, processes, and supply chains. Evaluation metrics include model accuracy, security, scalability, latency, and energy efficiency.

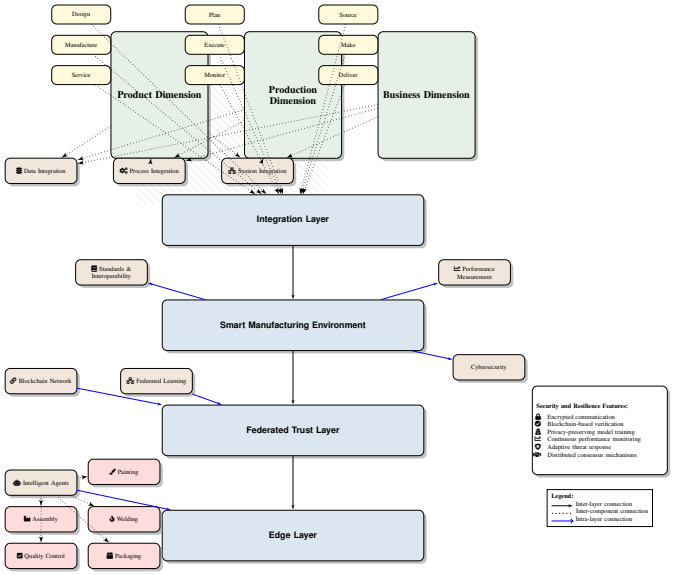

Fig. 1: Secure and Resilient Multi-Agent Smart Manufacturing Architecture

Algorithm 1 Federated Learning in Manufacturing Network

Require: Agents $A = a_1, \ldots, a_K$, learning rate η, rounds T
Ensure: Final global model w_T

Initialize w_0
for $t = 1$ to T **do**
  $wt^k \leftarrow \texttt{LocalTrain}(A, wt - 1)$ ▷ Train local model
  $\Delta w, n \leftarrow 0$ ▷ Initialize model update and total data points
  for each a_k in A **do**
    $n_k \leftarrow \texttt{GetDataPoints}(a_k)$
    $\Delta w \leftarrow \Delta w + (nk/n) \cdot (w_t^k - wt - 1)$
    $n \leftarrow n + n_k$
  end for
  $wt \leftarrow wt - 1 + \eta \cdot \Delta w$ ▷ Update global model
  $\texttt{DistributeModel}(A, w_t)$ ▷ Distribute updated global model
end for
return w_T

The multi-step process tests system capabilities, resilience, and advantages over traditional methods, offering insights into this new manufacturing paradigm.

IV. Results and Discussion

In Figure 2, approach 2, integrating federated learning and blockchain, outperforms Approach 1 in model accuracy, security, and scalability, especially for larger systems. While Approach 2 initially shows higher latency and lower energy efficiency, it becomes more efficient as the system scales, making it ideal for large-scale, secure manufacturing networks.

V. Conclusion

This paper presents a Multi-Agent Architecture integrating blockchain and federated learning for Smart Manufacturing

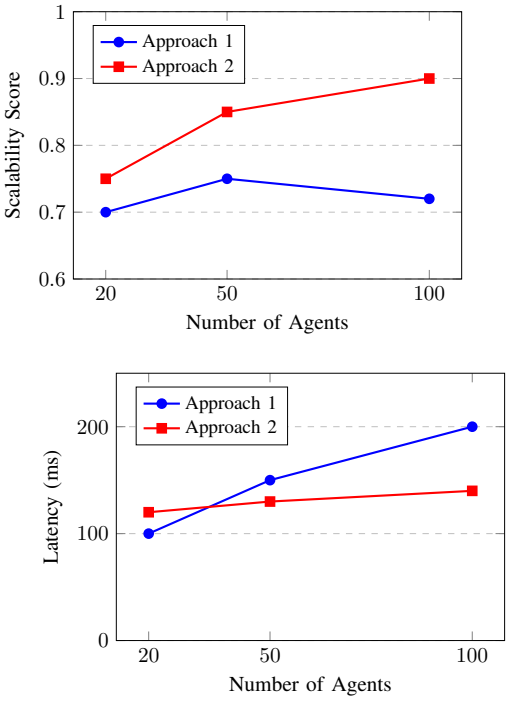

Fig. 2: Performance Comparison of Approach 1 and Approach 2

systems. It outperforms traditional centralized systems, especially in large deployments, with key findings including improved model accuracy, security, and scalability. While smaller systems experience initial overhead, larger systems benefit from better performance. Future research should focus on optimizing smaller systems and exploring real-world implementation challenges, advancing secure, efficient, and scalable solutions for Industry 4.0.

VI. Acknowledgements

This research was funded by the US National Science Foundation under the New Mexico ERISE DREAM project (EPSCoR cooperative agreement, Grant 271856).

References

[1] F. Islam, A. S. Raihan, and I. Ahmed, "Applications of federated learning in manufacturing: Identifying the challenges and exploring the future directions with industry 4.0 and 5.0 visions," *Proceedings of the International Conference on Industrial Engineering and Operations Management*, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:258715339

[2] X. Zuo, M. Wang, T. Zhu, L. Zhang, S. Yu, and W. Zhou, "Federated learning with blockchain-enhanced machine unlearning: A trustworthy approach," *ArXiv*, vol. abs/2405.20776, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:270199869

[3] J. Leng, S. Ye, M. Zhou, J. L. Zhao, Q. Liu, W. Guo, W. Cao, and L. Fu, "Blockchain-secured smart manufacturing in industry 4.0: A survey," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 237–252, 2021.

[4] G. Sofianidis, J. M. Rožanec, D. Mladenić, and D. Kyriazis, "A review of explainable artificial intelligence in manufacturing," *ArXiv*, vol. abs/2107.02295, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:235742844

[5] Q. Li, Q. Tang, I. Chan, H. Wei, Y. Pu, H. Jiang, J. Li, and J. Zhou, "Smart manufacturing standardization: Architectures, reference models and standards framework," *Computers in Industry*, vol. 101, pp. 91–106, 2018.