ASME Journal of Computing and Information Science in Engineering
Online journal at:
https://asmedigitalcollection.asme.org/computingengineering

Journal of Computing and Information Science in Engineering

Guest Editorial

Special Issue: Cybersecurity in Manufacturing

The landscape of cybersecurity in manufacturing exhibits a dynamic interplay between evolving threats and vulnerabilities against innovative defense mechanisms. With the increasing adoption of smart and cloud-controlled technologies, there is a growing emphasis on securing manufacturing systems from cyberattacks. Future trends indicate a shift toward implementing more advanced technologies such as artificial intelligence and machine learning for threat identification, attack detection, and response. In addition, the adoption of secure-by-design principles in product development and the integration of blockchain technology for ensuring the integrity of supply chain data are expected to become more prevalent. As manufacturers continue to digitize and connect their operations, collaboration between industry stakeholders, government agencies, and cybersecurity experts will be crucial in developing robust defense strategies against evolving security threats. This Special Issue provided a platform for the research advancing understanding of and addressing these threats.

The article by Rahman et al., "Taxonomy-Driven Graph-Theoretic Framework for Manufacturing Cybersecurity Risk Modeling and Assessment," presents a taxonomy-driven graph-theoretic model and framework to represent the threat landscape of cybersecurity and identify vulnerable manufacturing assets. The model and framework contain three techniques to address identified research challenges. First, the proposed framework characterizes threat actors' techniques, tactics, and procedures using taxonomical classifications of manufacturing-specific threat attributes and integrates these attributes into cybersecurity risk modeling. Second, using the attack graph formalism, the proposed framework enables concurrent modeling and analysis of a wide variety of cybersecurity threats comprising varying attack vectors, locations, vulnerabilities, and consequences. Third, a quantitative risk assessment approach is presented to evaluate the cybersecurity risk associated with potential attack paths. It also identifies the attack path with the maximum likelihood of success, pointing out critical manufacturing assets requiring prioritized control. Finally, the proposed risk modeling and assessment framework is demonstrated using an example of a connected smart manufacturing system, wherein various attack paths and their associated risks are computed.

The article by Kokhahi and Li, "GLHAD: A Group Lasso-Based Hybrid Attack Detection and Localization Framework for Multistage Manufacturing Systems," proposes a framework utilizing the group lasso technique for the detection and localization of attacks in a multistage manufacturing system (MMS). The detection of cyberattacks in MMS is crucial due to the increasing sophistication of attacks and the complexity of MMS. As the attacks propagate, they affect subsequent stages, and formulating detection and localization is difficult. The article presents the algorithm through a case study of simple linear MMS and outperforms traditional hypothesis testing-based methods in expected detection delay and localization accuracy.

The article by Milaat and Lubell, "Layered Security Guidance for Data Asset Management in Additive Manufacturing," puts forth a structured layering approach utilizing the National Institute of Standards and Technology's cybersecurity framework (CSF) to develop risk-based guidance for fulfilling specific security outcomes for additive manufacturing technology. The CSF asset identification and management security outcomes are used as bases for providing AM-specific guidance. AM geometry and process definitions are identified in standardized and system-neutral data representations to aid manufacturers in mapping data flows and documenting processes. The Open Security Controls Assessment Language (OSCAL) is then utilized to integrate the AM-specific guidance with existing IT and OT security guidance in a rigorous and traceable manner.

The article by Lee et al., "Privacy-Preserving Neural Networks for Smart Manufacturing," presents a novel technique—Mosaic Neuron Perturbation (MNP)—to preserve latent information in the framework of the AI model, ensuring differential privacy requirements while mitigating the risk of model inversion attacks. MNP is flexible to implement into AI models, enabling a trade-off between model performance and robustness against cyberattacks while being highly scalable for large-scale computing. The MNP technique is then demonstrated in an experiment where real-world manufacturing data are collected from a computer numerical control turning process, showing a significant improvement in the prevention of inversion attacks while maintaining high prediction performance.

The article by Shi et al., "Sensor Data Protection through Integration of Blockchain and Camouflaged Encryption in Cyber-Physical Manufacturing Systems," proposes an integrative blockchain-enabled data protection method by leveraging camouflaged asymmetry encryption. The goal is to develop an effective approach to protecting data from cyberattacks so that the cyber-physical security of the manufacturing systems could be assured in the cyber-enabled environment. A real-world case study that protects the cyber-physical security of collected sensor data in additive manufacturing is presented to demonstrate the effectiveness of the proposed method. The results demonstrate that malicious tampering could be detected in a relatively short time (less than 0.05 ms), and the risk of unauthorized data access is significantly reduced as well.

The article by ElSayed and Panchal, "Information Embedding in Additively Manufactured Parts through Printing Speed

Control," demonstrates an approach to embed and retrieve information in AM parts by controlling the printing process parameters. The approach leverages variations in printing speed to encode information on the surface of AM parts. The retrieved data (via optical imaging techniques) are processed using computer vision techniques such as morphological segmentation and binary classification. A characterization is conducted to understand the impact of variations in the encoding parameters on the information retrieval accuracy. The advantages are demonstrated via experiments showcasing high accuracy in classifying bits, and retrieval of complete encoded messages, while successfully distinguishing subtle surface features resulting from varying printing speeds.

The article by Kuo and Yang, "Federated Learning on Distributed and Encrypted Data for Smart Manufacturing," introduces a privacy-preserving framework for enabling federated learning on encrypted data in smart manufacturing. The framework utilizes fully homomorphic encryption (FHE) to produce encrypted results from ciphertexts, preserving the mathematical operations' characteristics on plaintexts upon decryption. This approach maintains machine learning model performance while mitigating data breaches. The article showcases FHE's potential in smart manufacturing, reducing data breach risks and facilitating data sharing among parties to enhance machine learning modeling using shared data.

Gaurav Ameta
Siemens Corporate Research,
Princeton, NJ 08540
e-mail: gaurav.ameta@siemens.com

Satish Bukkapatnam
Department of Industrial and Systems Engineering,
Texas A&M University,
College Station, TX 77843
e-mail: satish@tamu.edu

Dan Li
Department of Industrial Engineering,
Clemson University,
Clemson, SC 29634
e-mail: dli4@clemson.edu

Wenmeng Tian
Department of Industrial and Systems Engineering,
Mississippi State University,
Mississippi State, MS 39762
e-mail: tian@ise.msstate.edu

Mark Yampolskiy
Department of Computer Science and Software Engineering,
Auburn University,
Auburn, AL 36849
e-mail: mark.yampolskiy@auburn.edu

Fan Zhang
School of Mechanical Engineering,
Georgia Institute of Technology,
Atlanta, GA 30318
e-mail: fan.zhang@me.gatech.edu