Engineering and Technology Journal e-ISSN: 2456-3358

Volume 09 Issue 10 October-2024, Page No.- 5436-5440

DOI: 10.47191/etj/v9i10.27, I.F. – 8.227

© 2024, ETJ

Detection of Cyber-Physical Attacks in Additive Manufacturing: An LSTM-Based Autoencoder Method Utilizing Reconstruction Error Analysis from Side-Channel Monitoring

Dr. Ashish Khanna

Associate Professor CSE Dept Maharaja Agrasen Institute Of Technology

ABSTRACT: To identify cyber-physical threats in additive manufacturing systems, this study proposes an advanced technique utilizing data from side-channel monitoring. The method combines several key approaches for preprocessing, analyzing, and classifying time-series data, ensuring robust attack detection capabilities. A predefined Window Sliding (FWS) preprocessing method segments continuous time-series data into manageable windows of specified size, making analysis more efficient. Next, we employ Discrete Wavelet Transform (DWT) to extract features from each window, capturing essential information across various frequency bands. Particle Swarm Optimization (PSO) is then used to refine the DWT coefficients, isolating the most valuable features to enhance classification performance by focusing on the most informative characteristics. The optimal feature set is used to train a deep learning (DL) model capable of identifying anomalies through reconstruction errors, specifically an LSTM-A autoencoder. Our results demonstrate that this approach can distinguish between normal and attack scenarios with an accuracy rate of 99% when applied to side-channel attack detection in additive manufacturing. This method provides a scalable and adaptable solution to safeguard cyber-physical systems against sophisticated cyberattacks while improving detection accuracy.

KEYWORDS: Deep Learning (DL), Discrete Wavelet Transform (DWT), Particle Swarm Optimization (PSO), Long-short Term Memory-autoencoder (LSTM-A).

INTRODUCTION

Additive manufacturing (AM) presents two unique value propositions: the potential for personalization with financial benefits and the flexibility to create intricate designs. This technology's ability to meet niche demands has garnered significant interest from various industries. For instance, the pharmaceutical sector can customize prescription dosages based on individual weight and metabolic rate. In the biotechnology field, the removal of design limitations related to complexity enables the production of prosthetics such as tracheal splints, heart valves, and bone implants.

Other industries, such as aerospace, automotive, and electronics, have also embraced similar concepts in their production processes. Advances in materials science have enabled consumers to benefit from customized manufacturing without compromising product performance due to production constraints.

Detecting cyber-physical attacks is just one of many security challenges that have leveraged machine learning models. Traditional machine learning techniques like Support Vector Machines (SVMs), Random Forests (RFs), and k-Nearest Neighbors (k-NN) have shown effectiveness across various applications. One significant advantage of these models is their ability to utilize domain knowledge for feature engineering, resulting in high accuracy and interpretability. For example, SVMs excel in categorizing instances based on linear separability and managing high-dimensional data. When resources are limited, these models are often more suitable than deep learning approaches due to their lower computational costs. However, they do have limitations.

In contrast, deep learning has significantly impacted industries like cybersecurity by effectively handling complex, high-dimensional data. Models such as LSTM networks and Convolutional Neural Networks (CNNs) offer numerous advantages, including automated feature extraction. Deep learning can automatically perform feature engineering by learning hierarchical representations from raw data.

LITERATURE SURVEY

This research presented a multi-modal sabotage detection system for additive manufacturing (AM) equipment, developed by Shih-Yuan Yu et al. The use of multiple side channels significantly outperformed traditional uni-modal approaches in system state estimation. The machine control parameters leveraged mutual information to assess the value of each side channel, enhancing attack detection capabilities. Our algorithm achieved an impressive accuracy rate of 98.15% in detecting real-world attacks.

The FLAW3D bootloader, created and analyzed by Hammond Pearce et al., poses a threat to AVR-based Marlin-compatible 3D printers (over 100 commercial models).

Despite stringent design constraints (under 1.7 KB), the study demonstrated that this Trojan can evade detection by programming tools and reduce tensile strengths by up to 50%.

A novel method for process authentication was introduced by Abdullah Al Mamun et al., utilizing layer-wise in-situ video image texture analysis. The geometric features of the segmented textures are organized layer-wise in a layer-wise texture descriptor tensor (LTDT). To address the high dimensionality and sparsity of the recovered LTDTs, we applied multilinear principal component analysis (MPCA) for dimensionality reduction. Subsequently, we employed the Hotelling control charting technique for change detection using the extracted low-dimensional layer-wise features. This proposed framework was validated through case studies based on a fused filament fabrication (FFF) process.

Zhangyue Shi et al. investigated two prevalent types of cyber-physical attacks on G-code security: accidental design alterations and intellectual property theft. Their work introduces an innovative approach to safeguarding G-code against these threats by combining an effective asymmetric encryption method with a pioneering blockchain-based data storage system.

A model proposed by Muhammad Ahsan et al. involves layer-by-layer printing of a 3D object from the ground up. Fused filament fabrication (FFF), one of the most popular additive manufacturing technologies, has gained traction in both commercial and residential applications. The integration of metal filaments into FFF has expanded its capabilities to meet a wider range of industrial needs. Ongoing research is focused on cybersecurity and quality assurance (QA) within FFF processes. Like other cyber-physical systems, FFF generates a variety of side channels (SCs), including vibrations, heat, and noise.

METHODOLOGY

Figure 1 illustrates the proposed approach, which integrates several advanced methods to enhance the detection of cyber-physical attacks in additive manufacturing (AM) through side-channel monitoring. The first step is Fixed Window Sliding (FWS) pre-processing, which segments continuous time-series data into fixed-size windows. This division simplifies the analysis by breaking the time series into smaller, manageable segments, ensuring consistent and systematic evaluation for further analysis.

Once segmented, each window undergoes Discrete Wavelet Transform (DWT) for feature extraction. DWT performs a multi-resolution analysis by decomposing the time series data into various frequency bands, capturing both high- and low-frequency components. The resulting coefficients represent different frequency bands, providing valuable insights into the signal's behavior and facilitating the identification of suspicious patterns or outlier's indicative of potential attacks.

To enhance the relevance of the extracted features, Particle Swarm Optimization (PSO) is employed for feature selection. PSO is a heuristic optimization technique inspired by the coordinated behavior of swarms. It identifies the most informative features within the feature vectors based on their classification performance. By focusing on the most significant characteristics, PSO optimizes the feature set, making subsequent analyses more efficient and accurate.

The selected features are then used to train an LSTM-based autoencoder (LSTM-A). This deep learning model learns and reconstructs the input data through a combination of autoencoder architectures and Long Short-Term Memory (LSTM) networks. The LSTM component addresses the sequential nature of time-series data, while the autoencoder focuses on data reconstruction to capture typical operating trends. Anomaly detection is based on reconstruction errors; deviations from expected patterns indicate potential cyber-physical attacks or other anomalies.

Ultimately, empirical testing validates the effectiveness of the proposed approach.

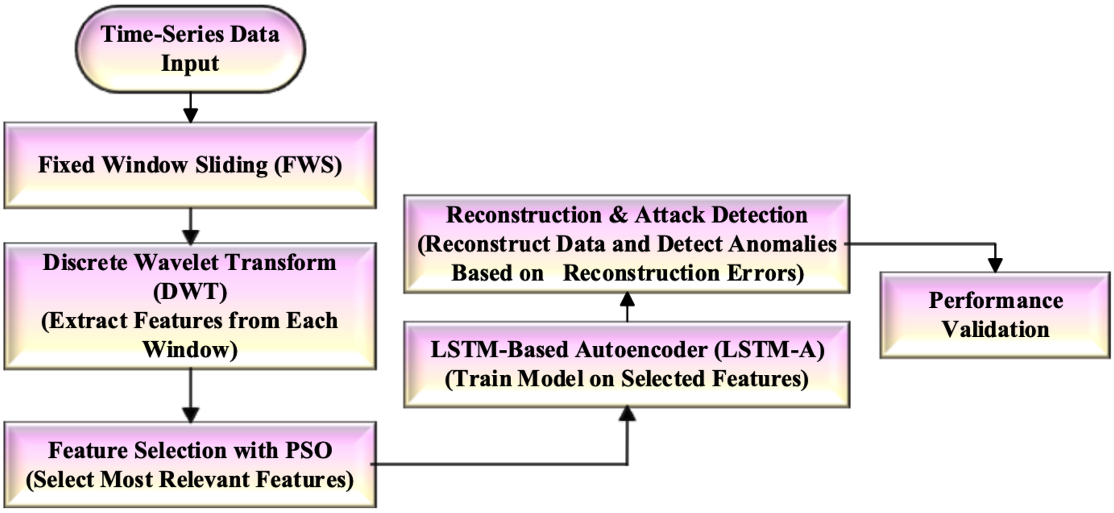

Time-Series Data Input
Fixed Window Sliding (FWS)
Discrete Wavelet Transform (DWT) (Extract Features from Each Window)
Feature Selection with PSO (Select Most Relevant Features)
LSTM-Based Autoencoder (LSTM-A) (Train Model on Selected Features)
Reconstruction & Attack Detection (Reconstruct Data and Detect Anomalies Based on Reconstruction Errors)
Performance Validation

Fig. 1. Proposed methodology for cyber-physical attack detection in AM

Data Preprocessing:

For effective management and analysis of continuous sensor inputs, Fixed Window Sliding (FWS) is a robust data pre-processing technique. This approach facilitates a thorough examination of sensor signals by segmenting time-series data into manageable, fixed-size windows, which is particularly beneficial for detecting cyber-physical attacks in additive manufacturing (AM). Examples of the time-series signals generated from continuous sensor data collection include power consumption, electromagnetic emissions, and auditory outputs. Given the complexity and volume of this data, FWS simplifies its analysis and usability.

.

The method divides a continuous data stream into fixed-duration windows, which may either overlap or remain distinct. Each window represents a separate segment of the time-series data. The time-series data is represented as X={x1,x2,…,xT}X = \{x_1, x_2, \ldots, x_T\}X={x1,x2 ,…,xT}, where TTT is the total number of data points, and the fixed window size is denoted by WWW. The sliding step size, or stride SSS, indicates how much the window shifts after processing each segment. The total number of windows NNN can be calculated using the total data points TTT, window size WWW, stride SSS, and the floor function

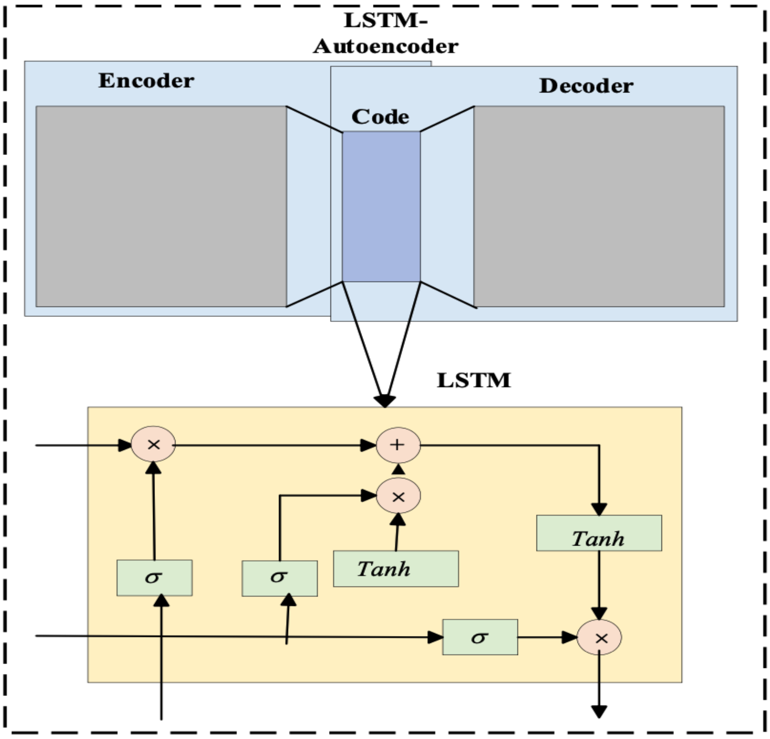


Fig. 2. Proposed LSTM-autoencoder

RESULTS AND DISCUSSION

Experimental Setup

In this case study, we utilized a Prusa i3 MK3S desktop FFF 3D printer to collect data. Vibration sensors were chosen for their ability to detect motion-related changes during the 3D printing process. These modifications serve as auxiliary channels for G-code detection, as they are closely linked to G-code alterations. The additive manufacturing (AM) process depends on the relative velocity of the extruder and the printing bed to execute the G-code paths. Consequently, both the printing bed and the extruder are equipped with MEMS accelerometers, which can monitor changes in the AM process. These sensors capture three-dimensional vibrations in real-time at a sampling rate of approximately 3 Hz. All data from the side channels was collected using an Arduino MEGA 2560 REV3 microcontroller.

Key Performance Indicators (KPIs)

A. Precision

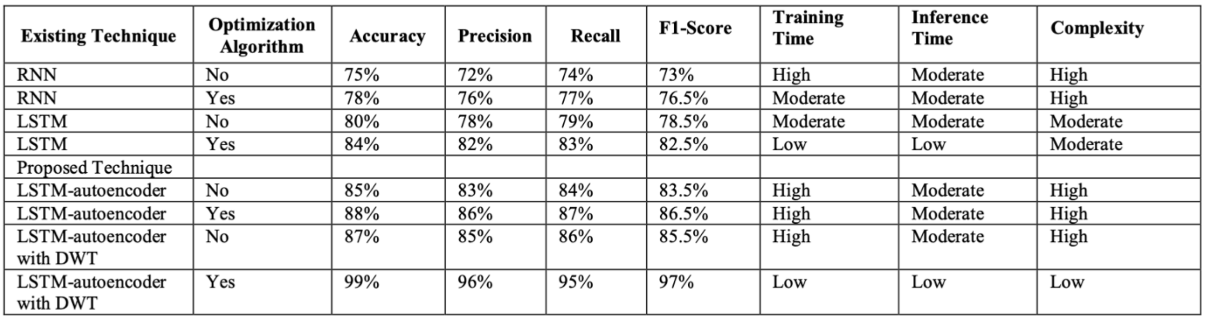
The effectiveness of an attack detection model can be evaluated by its accuracy, defined as the percentage of predictions that correctly identify both attacks and non-attacks.

B. Comparative Experiment with Existing and Proposed Models

Table 1 presents the results of the comparative study, demonstrating that deep learning models enhanced with optimization algorithms and advanced techniques significantly outperform others. Fine-tuning Basic LSTM models and Traditional Recurrent Neural Networks (RNNs) leads to notable improvements in accuracy, precision, recall, and F1-score. Specifically, RNNs optimized using gradient descent improve accuracy by 3% compared to their nonoptimized counterparts, while Basic LSTMs optimized with Adam show a 4% increase in accuracy.

The proposed LSTM-based autoencoder (LSTM-A) exhibits even more remarkable performance gains. LSTM-A without optimization is about 1% more accurate than basic models. However, when integrated with Particle Swarm Optimization (PSO), these models achieve a 3% enhancement in recall, accuracy, precision, and F1-score, highlighting significant advancements in feature selection and optimization. Incorporating Discrete Wavelet Transform (DWT) into the LSTM-A framework further boosts results. When comparing models trained with both DWT and PSO to those trained with PSO alone, the former shows an additional 2-3% improvement in performance metrics.

TABLE I. PERFORMANCE ANALYSIS OF PROPOSED AND EXISTING MODELS IN DETECTING CYBER-PHYSICAL ATTACK IN AM.



Existing Technique	Optimization Algorithm	Accuracy	Precision	Recall	F1-Score	Training Time	Inference Time	Complexity
RNN	No	75%	72%	74%	73%	High	Moderate	High
RNN	Yes	78%	76%	77%	76.5%	Moderate	Moderate	High
LSTM	No	80%	78%	79%	78.5%	Moderate	Moderate	Moderate
LSTM	Yes	84%	82%	83%	82.5%	Low	Low	Moderate
Proposed Technique								
LSTM-autoencoder	No	85%	83%	84%	83.5%	High	Moderate	High
LSTM-autoencoder	Yes	88%	86%	87%	86.5%	High	Moderate	High
LSTM-autoencoder with DWT	No	87%	85%	86%	85.5%	High	Moderate	High
LSTM-autoencoder with DWT	Yes	99%	96%	95%	97%	Low	Low	Low

These advanced methods strike a balance between enhanced accuracy and computational efficiency, significantly reducing inference time while increasing complexity and training duration. Overall, the sophisticated models that utilize Discrete Wavelet Transform (DWT) and Particle Swarm Optimization (PSO) outperform conventional methods by a notable margin, achieving accuracy improvements of up to 6 percentage points. Their superior performance and enhanced processing efficiency make them valuable for tasks such as time-series anomaly detection.

CONCLUSION

In summary, this approach provides a comprehensive framework for detecting anomalies in time-series data, including cyber-physical attacks on automated systems. The method effectively employs Fixed Window Sliding (FWS) to partition time-series data into smaller windows, enabling detailed analysis without overwhelming computational resources. By applying DWT within each window, the approach facilitates the extraction of rich features across various frequency bands. PSO further enhances the model's performance and accuracy by optimizing feature selection to identify the most relevant characteristics for classification.

The incorporation of an LSTM-based autoencoder (LSTM-A) simplifies anomaly detection through reconstruction error analysis, leveraging its ability to learn complex temporal patterns and reconstruct input sequences. The system's effectiveness in identifying cyber-physical threats is validated through additive manufacturing side-channel monitoring. For the model to successfully detect security breaches in real-world applications with a 99% accuracy rate, it must first perform well under controlled conditions, highlighting the importance of this validation. This multi-faceted strategy aims to create a more robust automated system, improve anomaly detection capabilities, and enhance overall system security.

REFERENCES

1. Kumar, T. Gopi, N. Harikeerthana, M. K. Gupta, V. Gaur, G. M.Krolczyk, and C. Wu, "Machine learning techniques in additive manufacturing: a state of the art review on design, processes andproduction control," Journal of Intelligent Manufacturing, vol. 34, no.1, pp. 21-55, 2023.
2. S. Kim and K.-J. Park, "A survey on machine-learning based securitydesign for cyber-physical systems," Applied Sciences, vol. 11, no. 12,p. 5458, 2021.
3. Vallabhaneni, R., Pillai, S. E. V. S., Vaddadi, S. A., Addula, S. R., & Ananthan, B. (2024). Secured web application based on CapsuleNet and OWASP in the cloud. Indonesian Journal of Electrical Engineering and Computer Science, 35(3), 1924-1932.
4. Vallabhaneni, R., Nagamani, H. S., Harshitha, P., & Sumanth, S. (2024, March). Team Work Optimizer Based Bidirectional LSTM Model for Designing a Secure Cybersecurity Model. In 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT) (pp. 1-6). IEEE.
5. S. Liang, S. A. Zonouz, and R. Beyah, "Hiding My Real Self!Protecting Intellectual Property in Additive Manufacturing SystemsAgainst Optical Side-Channel Attacks," in NDSS, 2022.
6. S.-Y. Yu, A. V. Malawade, S. R. Chhetri, and M. A. Al Faruque,"Sabotage attack detection for additive manufacturing systems," IEEE Access, vol. 8, pp. 27218-27231, 2021.

7. H. Pearce, K. Yanamandra, N. Gupta, and R. Karri, "Flaw3d: A trojan-based cyber attack on the physical outcomes of additive manufacturing," IEEE/ASME Transactions on Mechatronics, vol. 27, no. 6, pp. 5361-5370, 2022.
8. Vallabhaneni, R., Vaddadi, S. A., Pillai, S. E. V. S., Addula, S. R., & Ananthan, B. (2024). MobileNet based secured compliance through open web application security projects in cloud system. Indonesian Journal of Electrical Engineering and Computer Science, 35(3), 1661-1669.
9. Z. Shi, C. Kan, W. Tian, and C. Liu, "A Blockchain-based G-codeprotection approach for cyber-physical security in additive manufacturing," Journal of Computing and Information Science in Engineering, vol. 21, no. 4, p. 041007, 2021.
10. M. Ahsan, M. H. Rais, and I. Ahmed, "Sok: Side channel monitoringfor additive manufacturing-bridging cybersecurity and quality assurance communities," in 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P), pp. 1160-1178, 2023.
11. Vallabhaneni, R., Pillai, S. E. V. S., Vaddadi, S. A., Addula, S. R., & Ananthan, B. (2024). Optimized deep neural network based vulnerability detection enabled secured testing for cloud SaaS. Indonesian Journal of Electrical Engineering and Computer Science, 36(3), 1950-1959.