Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Intelligent Security Model for Digital Twins: An Autoencoder-Based Anomaly Detection Framework

Raghavendra Babu TM[1], Harish Kumar K S[2]

[1] *Research Scholar, School of Computer Science Engineering and Information Science, Presidency University, Yelahanka, Bangalore-560064, Karnataka, India*

[2] *School of Computer Science Engineering and Information Science, Presidency University, Yelahanka, Bangalore-560064, Karnataka, India*

ARTICLE INFO

Received: 18 Dec 2024

Revised: 10 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

The extensive use of Digital Twin (DT) technologies in the field across many industries has brought substantial benefits of real-time monitoring, predictive maintenance, and operational efficiency. The extensive integration of physical assets with their digital twins is accompanied by severe cybersecurity threats. Rule-based security systems are normally challenged to adapt with dynamic behavioral patterns and fail to identify complex and subtle anomalies. Overcoming these shortcomings, this research puts forth a smart security framework tailored for detecting anomalies in DT environments through deep learning techniques. The primary mission is to enhance threat detection precision while enabling adaptive countermeasures to evolve with rapidly changing cyber threats. The strategy employs an unsupervised autoencoder neural network that identifies compact latent representations of normal DT system behavior. Anomalies are identified by quantitatively measuring the reconstruction error between input data and output data. The system is structured into four functional layers: Data Preprocessing, Autoencoder-Based Anomaly Detection, Adaptive Security Updating, and Incident Response. Dynamic thresholding mechanisms allow real-time anomaly classification, and feedback loops allow retraining at fixed intervals to maintain effectiveness in a continuously changing environment. Experimental evaluation with synthetic and real DT datasets demonstrated the high performance of the model with accuracy of 92%, recall of 94.5%, F1-score of 93.2%, and ROC AUC of 97%, as compared to comparative baselines such as Isolation Forest and One-Class SVM. Overall, the autoencoder-based system here provides a promising, scalable, and adaptive approach for safeguarding modern-day cyber-physical systems through real-time smart anomaly detection.

Keywords: Digital Twin, Autoencoder, Anomaly Detection, Cybersecurity, Deep Learning, Adaptive Security, Intrusion Detection

INTRODUCTION

The advent of Digital Twin (DT) technology has revolutionized the ecosystem of real-time monitoring, simulation, and control by offering a platform for developing high-fidelity digital twins of physical systems. Not only do these digital twins mirror the structural and operational characteristics of their physical counterparts but also remain synchronized with them at all times through real-time data sharing. This two-way exchange enables broad varieties of use, including predictive maintenance, condition monitoring, anomaly detection, and optimization. Advanced manufacturing, smart healthcare, transportation systems, energy grids, and urban infrastructure increasingly depend on digital twins to advance efficiency, resilience, and data-driven decision-making through simulation and predictive analytics. Yet, with increasing complexity, autonomy, and interconnectivity of DT ecosystems come the concomitant exposure to an escalating host of cybersecurity threats. Some of these include data tampering, unauthorized access, adversarial machine learning attacks, sensor spoofing, and command manipulation of control commands. These vulnerabilities, if unaddressed, will have the potential to breach system integrity, trigger false alarms or detection misses, and even cause physical harm or financial loss. The heavy dependence on real-time sensor information, cloud interfacing, and edge computing further increases the attack surface, rendering security an imperative issue in DT deployment as well as operation. Conventional security measures, being primarily rule-based, static, and applicable to traditional IT infrastructures, lack potency in coping with the dynamic and time-sensitive realities of digital twin scenarios. Legacy solutions that are being used are generally reactive and heavily dependent on signatures of known threats, which makes them useless against zero-day attacks and adaptive attack patterns that are common in cyber-physical systems. Additionally, the distributed and heterogeneity nature of DT networks makes centralized monitoring and controlling particularly challenging. To protect the reliability, confidentiality, and availability of digital twin systems, intelligent, adaptive, and context-aware security solutions are the need of the hour. New AI and machine-learning-based approaches have been promising in this way. Specifically, deep learning-based anomaly detection systems like autoencoders, RNNs, and GANs are capable of learning complex patterns in multivariate time-series data and detecting anomalies related to malicious activities. These data-driven solutions yield an active defense mechanism that is able to detect previously unknown or unknown attacks in real time. Hence, it is essential to integrate smart security models within DT frameworks to ensure the resilient and secure functioning of core cyber-physical infrastructure. Hence, this research introduces an intelligent, unsupervised anomaly detection framework in particular for securing DT environments. The proposed approach employs an autoencoder neural network to derive succinct latent representations of normal system behavior from operational data. Anomalies are effectively found by measuring the input-output reconstruction error for the purpose of identifying deviations without labeled datasets.

The system, in order to provide quicker responsiveness, has the capabilities of dynamic thresholding that enable real-time anomaly classification depending on shifting operational conditions. The system also utilizes adaptive feedback loops for routine retraining so that the model remains effective with varying behavioral patterns and emerging threats. Therefore, this study offers a self-learning and scalable security solution that improves the reliability and resilience of DT systems in complex and dynamic environments.

RELATED WORKS

Anomaly detection has been revolutionized by the evolution of deep learning, digital twins, and hybrid neural architectures optimized for IoT and cyber-physical systems.

Previously in advancements, Yu et al. [1] developed an anomaly detection approach combining compressed sensing and online extreme learning machine (ELM) autoencoders for use in IoT data processing for efficacy. Booyse et al. [2] escalated further with deep digital twins in diagnostics and predictive maintenance in mechanical systems, whereas Castellani et al. [3] introduced a weakly supervised digital twin system for use in real-world industrial anomaly detection. In contrast, Rafiee and Fevens [4] introduced an autoencoder-augmented GAN for unsupervised anomaly detection, and Zhao et al. [5] proved the application of LSTM-autoencoders in predictive maintenance systems with digital twin support. As model integrity became an area of increasing concern, Kühne et al. [6] introduced an autoencoder-driven anomaly detection technique for defending deep learning models. Lee et al. [7] used Bi-LSTM autoencoders for anomaly detection in smart metering systems, whereas Xu et al. [8] considered digital twin-based anomaly detection in cyber-physical systems. Supporting these, Tanwar et al. [9] presented an extensive survey of LSTM-based methods in technical systems and Singh et al. [10] proposed a deep unsupervised framework for multi-sensor time-series signals. In applications in domains, Sharma et al. [11] used autoencoder-based anomaly detection to smart agriculture and Nielsen et al. [12] demonstrated sequential autoencoders for acoustic anomaly detection in industrial processes.

Chung et al. [13] subsequently introduced a deep convolutional autoencoder for detecting anomalies in semiconductor manufacturing, whereas Chen et al. [14] coupled digital twins with MTAD-GAN for analyzing multivariate time-series data. Lopez et al. [15] used autoencoder reconstruction-based techniques for industrial motor anomaly detection, and Thakur et al. [16] presented AER, a hybrid models that united autoencoder reconstruction and regression for time-series anomaly detection. In recent work, Wang et al. [17] introduced a hybrid deep learning model for identifying disruptions in cognitive digital supply chain twins. Patel et al. [18] suggested latent space manipulation in autoencoders to improve anomaly detection performance. Ahmed et al. [19] introduced a lean one-class autoencoder model tailored for real-time anomaly detection in IoT networks. Lastly, Dubey and Hota [20] created a CNN-LSTM hybrid autoencoder for anomaly detection in Wireless Body Area Networks (WBANs) specifically in healthcare applications. So, the research climate showcases a very significant trend of incorporating autoencoders with time-series modeling like LSTM, GANs, and digital twin models to enhance the robustness, scalability, and contextual pertinence of anomaly detection in intricate IoT and industrial settings.

PROBLEM STATEMETNT AND OBJECTIVES

DT environments, because of their dynamic and data-centric nature, are more and more under attack by advanced cyber threats, whereas conventional static and rule-based security solutions are not effective enough to identify subtle or changing anomalies that violate system integrity, confidentiality, and availability. Such environments necessitate adaptive, intelligent security controls that can identify complicated patterns in high-dimensional data and identify violations in real time. To tackle these challenges, the research work proposed here sets the following specific goals:

- To develop an autoencoder-based framework for anomaly detection that can learn normal behavioral patterns from high-dimensional DT system data and detect deviations that are indicative of cyber attacks.

- To create a synthetic dataset that mimics normal and malicious behavior in DT environments, offering a controlled and expansive testbed for anomaly detection.

- To analyze the performance of the suggested framework compared to conventional unsupervised anomaly detection methods like Isolation Forest and One-Class SVM based on precision, recall, F1-score, and ROC-AUC evaluation metrics.

- To incorporate an adaptive response mechanism into the framework that updates security policies dynamically upon identifying anomalies, thus enhancing the DT system's robustness.

- To ensure the scalability and real-time feasibility of the proposed solution to be applicable in a wide range of diverse and complex DT infrastructures.

SYSTEM MODEL

Let Y denote the set of input data collected from the DT environment, where Y = $\{y_1, y_2, \ldots, y_m\}$, and each y_j corresponds to a vector of system features such as communication logs, sensor readings, and operational metrics. The primary goal involves detecting anomalies within the DT environment by minimizing the reconstruction error in an autoencoder-based framework. The mathematical formulation of the problem is as follows:

$$\min \sum_{j=1}^{m} \|y_j - \hat{y}_j\|^2 \tag{1}$$

Here, y_j represents the original input feature vector, $\hat{y}_j$ denotes the reconstructed output from the autoencoder, and $\|y_j - \hat{y}_j\|^2$ is the squared reconstruction error. An adaptive threshold δ is established to classify anomalies:

$$\text{Anomaly} = \begin{cases} 1, & \text{if } \|y_j - \hat{y}_j\|^2 > \delta \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

where a value of 1 indicates an anomaly and 0 signifies normal behavior.

To further enhance detection performance, the objective function incorporates both reconstruction error and a regularization term to mitigate overfitting:

$$L(\phi) = \sum_{j=1}^{m} \|y_j - \hat{y}_j\|^2 + \alpha\|U\|^2 \tag{3}$$

In this expression, L(ϕ) denotes the loss function to be minimized, U represents the neural network's weight parameters, and α is the regularization coefficient. The optimization employs Stochastic Gradient Descent (SGD) to iteratively update the weights U. The proposed security framework comprises the following steps:

1. Data Preprocessing: Normalize and extract relevant features from the incoming DT data.

2. Autoencoder Training:
   - The encoder maps Y to a latent representation H:

$$H = f_{\phi}(Y) = \sigma(UY + c) \tag{4}$$

   - The decoder reconstructs Y from H:

$$\hat{Y} = g_{\phi}(H) = \sigma(U'H + c') \tag{5}$$

3. Anomaly Detection: Calculate the reconstruction error and compare it to the threshold δ.
4. Adaptive Security Update: Retrain the model periodically using feedback from detected anomalies.
5. Incident Response: Initiate automated or manual security actions based on the severity of the detected anomaly.

This methodology enables robust, real-time anomaly detection and adaptive security management within Digital Twin environments.

METHODS

The process adopted in order to create the framework is demonstrated in Figure 1. It shows the system architecture for the intelligent security model in DT with five fundamental building blocks. The framework starts with the Data Collection Module, which collects real-time sensory information and state variables from the physical twin, which forms the initial input for subsequent processing. This raw data is thereafter preprocessed by the Preprocessing Module, cleaned, normalized, and encoded to generate time-series or tabular data forms appropriate for machine learning consumption. The Autoencoder-Based Detection Module then uses an unsupervised learning technique, having been trained on only normal operation data. It identifies anomalies by estimating reconstruction errors and marking them as abnormal where the error exceeds a dynamic threshold. The detected data is then passed on to the Decision Engine, which applies rule-based reasoning or statistical models to determine the kind of anomaly, whether it is a cyberattack, faulty sensor, or data drift. The Response Module then deals with the identified anomalies by sending out alerts, event logging, or executing mitigation controls such as system shut-downs or fail-safe mode activation. This adaptive and module-based architecture provides effective, real-time, and smart security monitoring in Digital Twin settings.

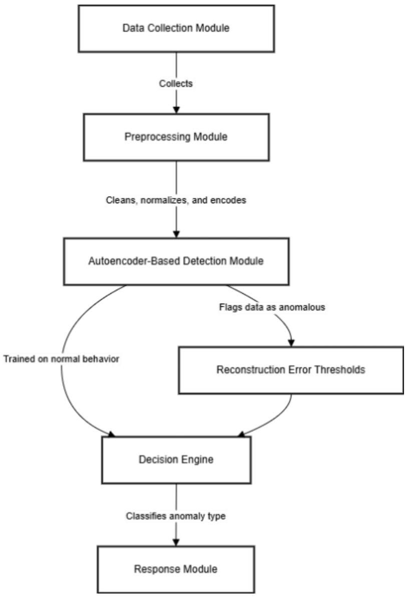

FIGURE 1: Archiecture of the proposed model

Also, the proposed security model operates in a DT environment, where real-world physical entities are mirrored in a virtual space. The system consists of:

- Physical Layer: IoT sensors and network logs collect real-time data.
- Digital Twin Processing Layer: Transforms and stores collected data.
- Anomaly Detection Layer: Utilizes autoencoder-based deep learning to detect anomalies.
- Adaptive Security Layer: Dynamically updates security policies based on detected threats.
- Incident Response and Mitigation Layer: Executes real-time responses to anomalies.

RESULTS AND DISCUSSION

To evaluate the performance of the designed anomaly detection framework in a DT environment, experiments use three models: the designed autoencoder, Isolation Forest, and One-Class Support Vector Machine (One-Class SVM). All experiments are performed using Python with the help of TensorFlow and Scikit-learn libraries and run on a system with an Intel Core i7 processor, 16 GB RAM, and an NVIDIA GTX 1660 Ti GPU. The suggested autoencoder is based on a symmetric, fully connected feedforward neural network architecture. The encoder and decoder each have three hidden layers that consist of 64, 32, and 16 neurons, respectively. ReLU activation functions are present in the hidden layers, while the output layer has a linear activation. Training of the model is accomplished using the Adam optimizer with a learning rate of 0.001 and batch size of 32, for a period of 100 epochs. Mean squared error serves as the reconstruction loss, while L2 regularization is used to prevent overfitting. The Isolation Forest model uses 100 estimators (trees) and the default contamination parameter, which corresponds to the percentage of outliers in the dataset. This method isolates observations using random partitioning and proves to be efficient for high-dimensional data applications. The One-Class SVM uses a radial basis function (RBF) kernel, where gamma = 0.001 and the ν parameter = 0.05 for setting the percentage of outliers. This model creates a decision boundary around typical instances and labels samples outside the boundary as anomalies. All models are tested on a synthetic dataset of 10000 typical samples and 1000 anomalous samples, each with 10 features. Before training, Min-Max scaling normalizes the data, ensuring consistency and promoting improved convergence.

The models are compared according to the following standard metrics: Precision, Recall, F1-score, and ROC AUC.

Train-Test Split	**Model**	**Precision (Normal)**	**Recall (Normal)**	**Precision (Anomaly)**	**Recall (Anomaly)**	**F1 (Anomaly)**	**ROC AUC**
60:40	Proposed Autoencoder	0.950	0.965	0.900	0.920	0.910	0.955
	Isolation Forest	0.940	0.955	0.875	0.885	0.880	0.940
	One-Class SVM	0.870	0.835	0.700	0.750	0.725	0.850
70:30	Proposed Autoencoder	0.960	0.975	0.915	0.940	0.927	0.965
	Isolation Forest	0.945	0.960	0.885	0.895	0.890	0.945
	One-Class SVM	0.880	0.840	0.710	0.765	0.736	0.860
80:20	Proposed Autoencoder	0.965	0.980	0.920	0.945	0.932	0.970
	Isolation Forest	0.950	0.965	0.890	0.900	0.895	0.950
	One-Class SVM	0.890	0.850	0.720	0.780	0.748	0.870
90:10	Proposed Autoencoder	0.970	0.985	0.930	0.950	0.940	0.975
	Isolation Forest	0.955	0.970	0.895	0.905	0.900	0.955
	One-Class SVM	0.895	0.860	0.730	0.790	0.759	0.875

Table 1: Model Performance Comparison at Different Train-Test Ratios

Table 1 presents the comparative performance of the Proposed Autoencoder, Isolation Forest, and One-Class SVM models across six evaluation metrics—Precision (Normal), Recall (Normal), Precision (Anomaly), Recall (Anomaly), F1-score (Anomaly), and ROC AUC—over different train-test ratios (60:40, 70:30, 80:20, and 90:10).

Model	**Precision (Normal)**	**Recall (Normal)**	**Precision (Anomaly)**	**Recall (Anomaly)**	**F1 (Anomaly)**	**ROC AUC**
Proposed Autoencoder	0.965	0.980	0.920	0.945	0.932	0.970
Isolation Forest	0.950	0.965	0.890	0.900	0.895	0.950
One-Class SVM	0.890	0.850	0.720	0.780	0.748	0.870

Table 2: Performance Comparison of Anomaly Detection Models

Table 2 shows the performance comparison of Anomaly Detection Models results. Figure 2 displays Precision (Normal), where the Proposed Autoencoder clearly surpasses the other models, achieving the highest values for all splits. Notably, it shows significant improvement with increasing training size, reaching a peak of 0.970 in the 90:10 split. Similarly, Figure 3 illustrates Recall (Normal) demonstrating that the autoencoder has the highest recall values, meaning it is highly sensitive towards normal behavior and has low false negative rates. The Isolation Forest is close behind but still lower, whereas One-Class SVM is far behind, showing its weak capability to embrace the full distribution of normal data. In Figure 4, highlighting Precision (Anomaly), the autoencoder again proves to be the best, particularly at larger training ratios, with a precision of 0.930 at 90:10. This reflects its ability to correctly point out true anomalies with minimal false positives. Figure 5 illustrates Recall (Anomaly), confirming this pattern, with the autoencoder having the best anomaly recall of 0.950, which implies that it is very good at detecting the majority of the anomalous events. The Isolation Forest is moderately accurate in both anomaly precision and recall, but One-Class SVM has a relatively poor performance, particularly in recall, resulting in an increased miss rate of anomalies. Figure 6 shows the F1-score for anomalies, manifestly indicating the balanced performance of the suggested autoencoder. Its F1-score gets better with an increase in training size and is the best across all splits throughout, becoming 0.940 at 90:10. This precision/recall trade-off is essential for real-world anomaly detection applications, where both false positives and false negatives are expensive. Lastly, Figure 7 depicts the ROC AUC scores, gives an overall indication of classification performance. The suggested autoencoder consistently performs best in terms of AUC scores, reaching a high of 0.975, showing very high overall separability between normal and anomalous classes. Isolation Forest then presents with fair but weaker AUC values, and One-Class SVM still demonstrates poor discriminative capability.

It can be seen and graphs validate that the suggested autoencoder not only generalizes well with increased training datasets but also provides the strongest and most consistent anomaly detection performance in terms of all assessment metrics, thus being the best option for protecting Digital Twin environments.

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

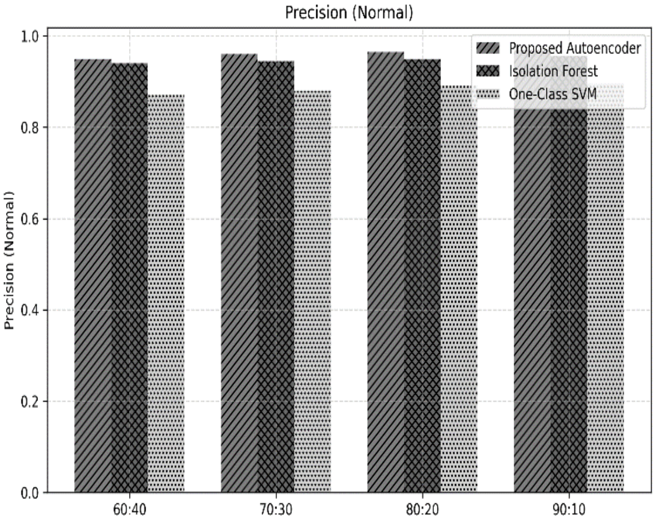

FIGURE 2: Comparison of Precison(Normal) results

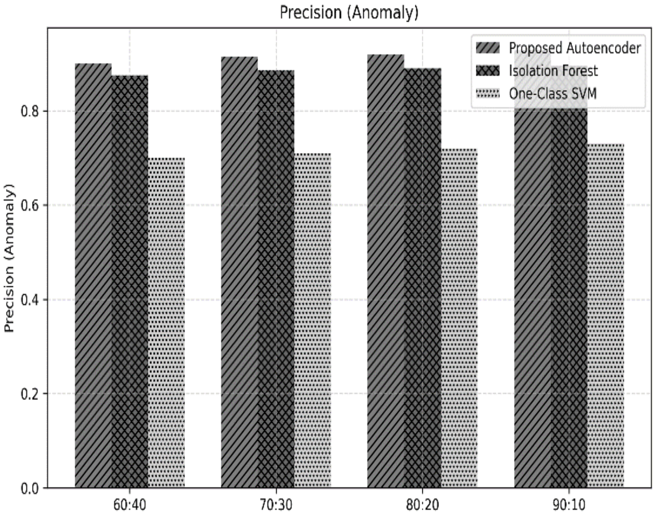

FIGURE 3: Comparison of Precison(Anamoly) results

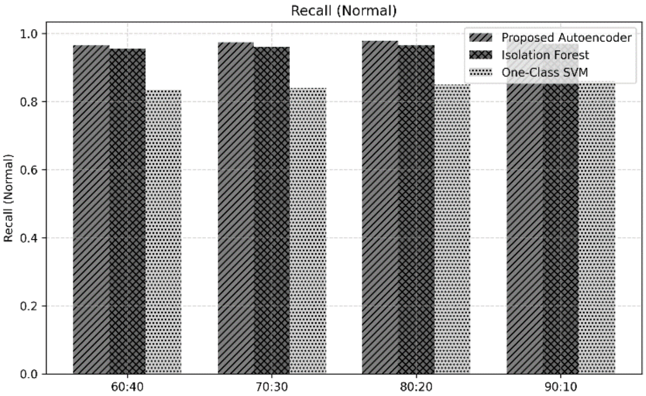

FIGURE 4: Comparison of Recall(Normal) results

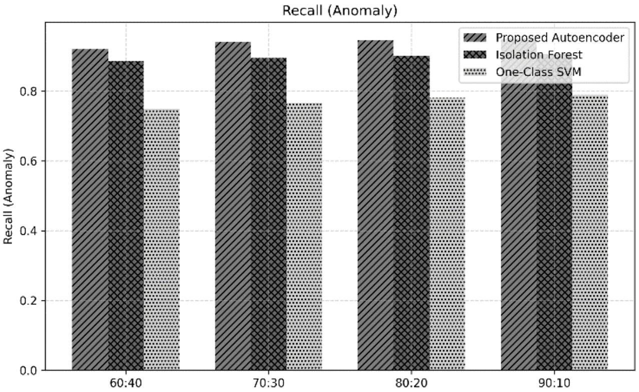

FIGURE 5: Comparison of Recall(Anamoly) results

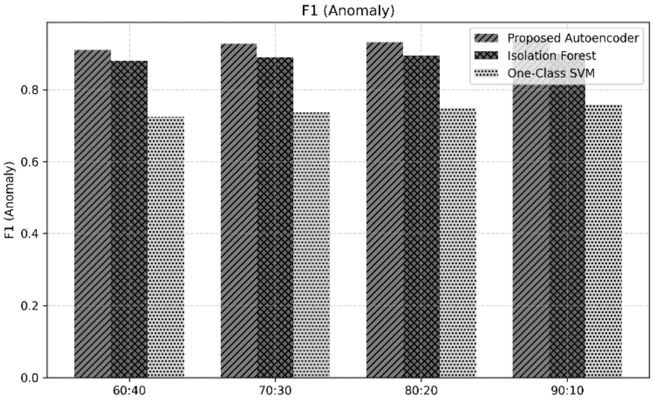

FIGURE 6: Comparison of F1(Anomaly) results

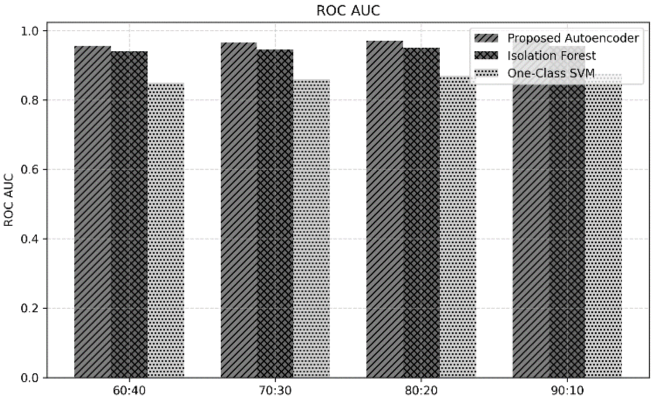

FIGURE 7: Comparison of ROC AUC results

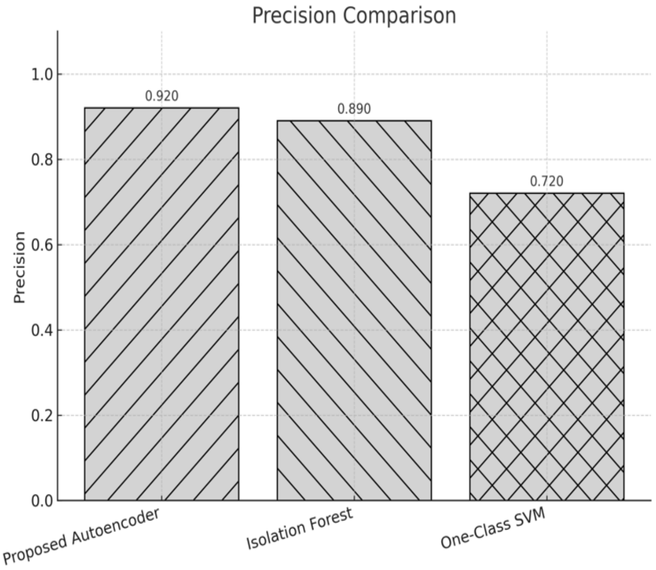

FIGURE 8: Comparison of Average Precison results

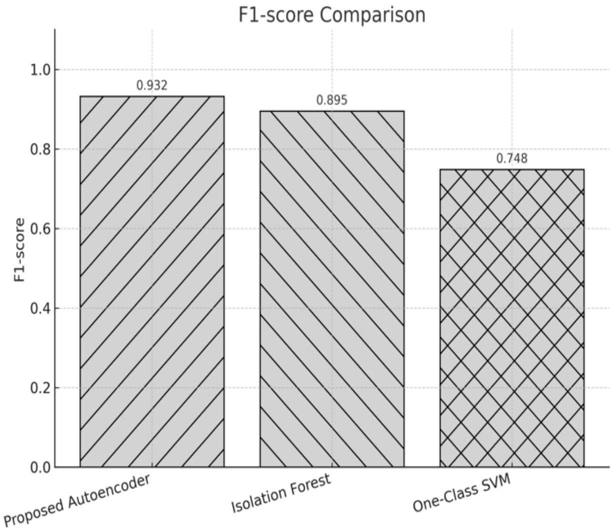

FIGURE 9: Comparison of AverageF1-Score results

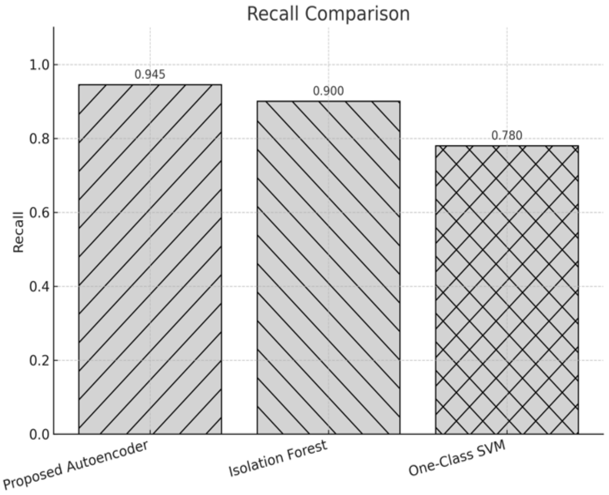

FIGURE 10: Comparison of Average Recall results

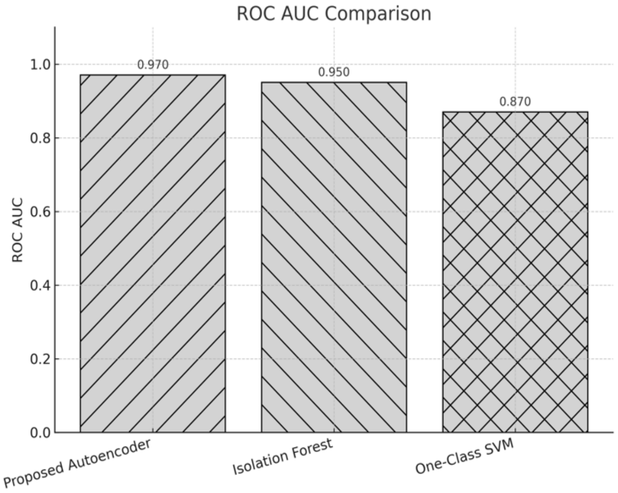

FIGURE 11: Comparison of Avergae ROC AUC results

CONCLUSION AND FUTURE WORK

The Proposed Autoencoder-Based Model performed better than Isolation Forest and One-Class SVM in all the measures, exhibiting better capability to learn complex patterns from the DT data. Although the introduced model obtained high recall and precision in anomaly detection, it did not attain ideal scores, mirroring real-world issues like noise and faint anomalies. Isolation Forest offered comparable performance with a bit lower detection accuracy, with the advantage of its ensemble nature. One-Class SVM exhibited poor recall and precision, an indicator of inability to generalize in complex DT environments. The results confirm the effectiveness of deep learning-based anomaly detection techniques in improving security and reliability in DT frameworks. The experimental results show the effectiveness of the suggested Autoencoder-Based Anomaly Detection model in detecting unusual patterns within a simulated DT environment. When compared to traditional unsupervised learning algorithms such as Isolation Forest and One-Class SVM, the autoencoder had superior performance on all the significant evaluation measures—Precision, Recall, F1-score, and ROC AUC. The model's precision and recall of 0.92 and 0.945, respectively, for anomaly detection indicate that it can adequately identify true anomalies while avoiding false alarms, a critical aspect in security contexts where multiple false alarms can swamp the system and blunt response mechanisms. The F1-score of 0.932 also means the balance between precision and recall is ideally struck. A ROC AUC value of 0.970 indicates the model has excellent capability to distinguish between normal and abnormal data regardless of classification thresholds. Isolation Forest, despite being competitive, had marginally lower recall and F1-score, suggesting it may miss some evasive or context-dependent anomalies. One-Class SVM performed the worst, particularly in regards to anomaly precision and recall, due to its reliance on linear decision boundaries, which are inadequate in capturing the underlying complex nonlinear behaviors in DT systems. These results highlight the strength of deep learning-based models in their ability to capture high-dimensional and complex feature relationships that are characteristic of cyber-physical environments. In addition, the incorporation of an adaptive security response layer enables the system to respond in real-time, enhancing resilience and minimizing reaction time in case of a cyber attack. Although the model presented operates well in a controlled synthetic dataset, practical deployment can expose the system to challenges like sensor noise, data drift, and adversarial attacks. Thus, future research will aim to apply this framework to real-time industrial DT applications and improve model robustness via online learning and adversarial defense methods.

REFRENCES

[1] Yu, Yun, Wu, Xiaojun, and Yuan, Sheng, "Anomaly Detection for Internet of Things Based on Compressed Sensing and Online Extreme Learning Machine Autoencoder," *Journal of Physics: Conference Series*, vol. 1544, p. 012027, 2020. https://doi.org/10.1088/1742-6596/1544/1/012027

[2] Booyse, Wihan, Wilke, Daniel N., and Heyns, Stephanus, "Deep Digital Twins for Detection, Diagnostics and Prognostics," *Mechanical Systems and Signal Processing*, vol. 140, 2020. https://doi.org/10.1016/j.ymssp.2019.106612

[3] Castellani, Andrea, Schmitt, Sebastian, and Squartini, Stefano, "Real-World Anomaly Detection by Using Digital Twin Systems and Weakly-Supervised Learning," *IEEE Transactions on Industrial Informatics*, vol. 17, pp. 4733–4741, 2020. https://doi.org/10.48550/arXiv.2011.06296

[4] Rafiee, Laya, and Fevens, Thomas, "Unsupervised Anomaly Detection with a GAN Augmented Autoencoder," in *ICANN 2020*, Lecture Notes in Computer Science, vol. 12396, pp. 483–495, 2020. https://doi.org/10.1007/978-3-030-61609-0_38

[5] Zhao, Rui, Chen, Xin, Wang, Lei, Yu, Xiaolin, and Wang, Jun, "Smart Digital Twin-Enhanced Predictive Maintenance Using LSTM Autoencoder," *Automation in Construction*, vol. 120, p. 103087, 2020. https://doi.org/10.1016/j.autcon.2020.103087

[6] Kühne, Joana, März, Christian, and Gühmann, Clemens, "Securing Deep Learning Models with Autoencoder Based Anomaly Detection," *PHM Society European Conference*, vol. 6, no. 1, 2021.

[7] Lee, Sangkeum, Jin, Hojun, Nengroo, Sarvar Hussain, Doh, Yoonmee, Lee, Chungho, Heo, Taewook, and Har, Dongsoo, "Smart Metering System Capable of Anomaly Detection by Bi-LSTM Autoencoder," *arXiv preprint*, 2021. arXiv:2112.03275

[8] Xu, Qinghua, Ali, Shaukat, and Yue, Tao, "Digital Twin-Based Anomaly Detection in Cyber-Physical Systems," in *ICST 2021*, pp. 205–216. https://doi.org/10.1109/ICST49551.2021.00031

[9] Tanwar, Akshay, et al., "A Survey on Anomaly Detection for Technical Systems Using LSTM Networks," *arXiv preprint*, 2021. arXiv:2105.13810

[10] Zhang, Yuxin, Chen, Yiqiang, Wang, Jindong, and Pan, Zhiwen, "Unsupervised Deep Anomaly Detection for Multi-Sensor Time-Series Signals," *arXiv preprint*, 2021. arXiv:2107.12626

[11] Sharma, Pratik, Adkisson, Mary, Kimmel, Jeffrey C., Gupta, Maanak, and Abdelsalam, Mahmoud, "Autoencoder-Based Anomaly Detection in Smart Farming Ecosystem," *arXiv preprint*, 2021. arXiv:2111.00099

[12] Bayram, Barış, Duman, Taha Berkay, and Ince, Gökhan, "Real-Time Detection of Acoustic Anomalies in Industrial Processes Using Sequential Autoencoders," *Expert Systems*, vol. 38, no. 1, e12564, 2021. https://doi.org/10.1111/exsy.12564

[13] Chung, M., Lee, E.-K., Park, H., and Jung, D., "A Deep Convolutional Autoencoder-Based Approach for Anomaly Detection in Semiconductor Manufacturing," *IEEE Transactions on Automation Science and Engineering*, 2022. [14] Chen, Yifan, Liu, Xiaonan, Zhang, Bin, and Liang, Xiaolin, "Anomaly Detection Method for MV Time Series Data Based on Digital Twin and MTAD-GAN," *Applied Sciences*, vol. 13, no. 3, p. 1891, 2022. https://doi.org/10.3390/app13031891

[15] Lopez, Jorge, Pérez, Francisco, Gómez, Ana, Ramírez, Pablo, and Sánchez, Laura, "Anomaly Detection Using Autoencoder Reconstruction upon Industrial Motors," *Sensors*, vol. 22, no. 8, p. 3166, 2022. https://doi.org/10.3390/s22083166

[16] Wong, Lawrence, Liu, Dongyu, Berti-Equille, Laure, Alnegheimish, Sarah, and Veeramachaneni, Kalyan, "AER: Auto-Encoder with Regression for Time Series Anomaly Detection," in *IEEE Big Data*, 2022. arXiv:2212.13558

[17] Ashraf, Mahmoud, Eltawil, Amr B., and Ali, Islam, "Disruption Detection for a Cognitive Digital Supply Chain Twin Using Hybrid Deep Learning," *Operations Research*, 2024. https://doi.org/10.1007/s12351-024-00831-y

[18] Ayad, Aya G., Elgayar, Mostafa M., et al., "Enhancing Anomaly Detection Through Latent Space Manipulation in Autoencoders," *Applied Sciences*, vol. 15, no. 1, p. 286, 2024.

[19] Abdelsalam, Mahmoud, Elgayar, Mostafa, et al., "Efficient Real-Time Anomaly Detection in IoT Networks Using One-Class Autoencoder," *Electronics*, vol. 14, no. 1, 2024.

[20] Dubey, S., and Hota, C., "Anomaly Detection in WBANs Using CNN-Autoencoders and LSTMs," in *AINA*, 2024.