CYBER GUARDIAN: DIRICHLET VARIATIONAL AUTOENCODER ENHANCED CYBER PHYSICAL INTRUSION DETECTION SYSTEM WITH COYOTE OPTIMIZATION ALGORITHM

P. Bishwanath Kumar(21311A12T3@sreenidhi.edu.in),
Raini. Vardhan Reddy(21311A12R0@sreenidhi.edu.in),
G. Sumanth(21311A12R8@sreenidhi.edu.in)
Gunuganti Uday kumar(udaykumargunuganti@gmail.com)
Department of IT, Sreenidhi Institute Of Science And Technology, Hyderabad.

Abstract-Cyber-attacks targeting Cyber-Physical Systems (CPSs) pose significant threats, including sensing and actuation misbehavior, consequential physical damage, and heightened safety risks. Despite the emergence of Machine Learning (ML) models for CPS security, the lack of labeled data from emerging attacks presents a major challenge for effective detection. Intrusion Detection Systems (IDS) play a crucial role in securing CPS environments, serving as a vital component in thwarting cyber threats. This paper introduces an Explainable Artificial Intelligence Intrusion Detection System with Feature Selection and Dirichlet Variational Autoencoder (XAIIDS-FSDVAE) model for CPS security. The proposed model integrates a Coyote Optimization Algorithm (COA)-based Feature Selection (FS) module, strategically designed to identify an optimal subset of features. Subsequently, an intelligent Dirichlet Variational Autoencoder (DVAE) technique is deployed for anomaly detection in the CPS environment. The final phase involves the parameter optimization of the DVAE, utilizing the Manta Ray Foraging Optimization (MRFO) model to fine-tune its parameters. To assess the enhanced intrusion detection efficiency of XAIIDS-FSDVAE, extensive simulations are conducted using benchmark datasets. Experimental results demonstrate the superior performance of the proposed technique over recent methods, showcasing advancements in various evaluation parameters. This research leverages the latest developments in Deep Learning (DL) and Explainable AI (XAI) to comprehensively address cyber threats in CPS. The XAIIDS-FSDVAE model not only provides robust intrusion detection but also offers interpretability in its decision-making processes, contributing to the resilience and sophistication required for securing modern CPS environments..

Keywords: Cyber-Physical Systems (CPS), Explainable Artificial Intelligence (XAI), Intrusion Detection, System (IDS), Feature Selection, Dirichlet Variational Autoencoder (DVAE).

I.INTRODUCTION

In an era dominated by Cyber-Physical Systems (CPS), the seamless integration of digital and physical realms has brought unprecedented efficiency, connectivity, and innovation across various sectors. However, this technological convergence has also given rise to escalating threats, particularly in the form of cyber-attacks, with potential consequences ranging

from sensing and actuation misbehavior to severe damage and safety risks. Efforts to fortify CPS security have witnessed the application of Machine Learning (ML) models. Yet, the evolving landscape of cyber threats, coupled with the scarcity of labeled data for emerging attacks, has posed a formidable challenge for effective detection strategies. Intrusion Detection Systems (IDS) have emerged as a cornerstone in mitigating these challenges, offering a crucial line of defense in the quest for a secure CPS environment.

This research addresses the imperative to bolster CPS security through the lens of Explainable Artificial Intelligence (XAI) and advanced ML techniques. The proposed Explainable AI Intrusion Detection System with Feature Selection and Dirichlet Variational Autoencoder (XAIIDS-FSDVAE) model embodies a sophisticated approach to intrusion detection. Leveraging a Coyote Optimization Algorithm (COA)-based Feature Selection model, an intelligent Dirichlet Variational Autoencoder (DVAE), and parameter optimization using Manta Ray Foraging Optimization (MRFO), the XAIIDS-FSDVAE model aims not only to enhance intrusion detection efficiency but also to provide interpretability in decision-making processes. As we navigate through this paper, we delve into the intricacies of designing and implementing the XAIIDS-FSDVAE model. The goal is to contribute to the evolving landscape of CPS security, offering a resilient and sophisticated defense mechanism against cyber threats while embracing the principles of explain ability and interpretability in artificial intelligence.

A) Back Ground

The evolution of Cyber-Physical Systems (CPS)[1] has ushered in a new era of interconnected technologies, transcending traditional boundaries between the digital and physical worlds. This integration, while promising unparalleled advancements, has concurrently exposed CPS to an escalating spectrum of cyber threats. These threats manifest in the form of sophisticated attacks capable of inducing sensing and actuation misbehavior, causing severe damage to physical entities, and posing significant safety risks. Machine Learning (ML) models have been pivotal in fortifying CPS against these threats. However, the efficacy of these models is challenged by the dynamic nature of cyber-attacks and the scarcity of labeled data for emerging threats. Intrusion Detection Systems (IDS) have emerged as indispensable components, offering real- time monitoring and detection capabilities to safeguard CPS environments. The relentless pursuit of enhancing CPS security has led to the exploration of advanced ML techniques[3], particularly in the realms of Deep Learning (DL) and Explainable Artificial Intelligence (XAI). This research is situated within this context, aiming to address the

pressing need for a robust and interpretable intrusion detection system tailored for CPS environments. The proposed Explainable AI Intrusion Detection System with Feature Selection and Dirichlet Variational Autoencoder (XAIIDS-FSDVAE) model takes inspiration from recent developments in feature selection, deep learning, and XAI. By incorporating a Coyote Optimization Algorithm (COA)-based Feature Selection model, an intelligent Dirichlet Variational Autoencoder (DVAE), and parameter optimization through Manta Ray Foraging Optimization (MRFO), the XAIIDS-FSDVAE model is designed to overcome the limitations of traditional IDS. The emphasis on explain ability aligns with the growing importance of understanding the decision-making processes of complex AI systems.

This research builds on the current state-of- the-art in CPS security, contributing a novel approach that not only enhances intrusion detection efficiency but also provides insights into the decision rationale. The background sets the stage for a comprehensive exploration of the XAIIDS-FSDVAE model, offering a promising avenue for bolstering the security posture of modern Cyber-Physical Systems.

B) Scope Of the Research

This research delineates a comprehensive scope, addressing critical dimensions in Cyber-Physical Systems (CPS) security and Explainable Artificial Intelligence (XAI). The primary focus is on developing and validating the Explainable AI Intrusion Detection System with Feature Selection and Dirichlet Variational Autoencoder (XAIIDS-FSDVAE) model[3], designed to elevate the cybersecurity posture of modern CPS environments.

The research's scope encompasses the intricate domain of CPS security, characterized by the convergence of digital and physical components. XAIIDS-FSDVAE's application is not limited to specific CPS sectors, making it adaptable across diverse domains, including healthcare, energy, transportation, and manufacturing. By virtue of its adaptability, the model addresses the security concerns inherent in various CPS infrastructures. Furthermore, the research extends its scope to the integration of cutting-edge technologies. The use of Coyote Optimization Algorithm (COA) for feature selection[4], Dirichlet Variational Autoencoder (DVAE)[5] for anomaly detection, and Manta Ray Foraging Optimization (MRFO) for parameter tuning reflects a commitment to leveraging state- of-the-art methodologies. This integration ensures that the proposed model remains at the forefront of technological advancements, providing a robust defense against evolving cyber threats. The validation and benchmarking process, involving simulations with benchmark datasets, broadens the research

scope. This empirical approach ensures the reliability and effectiveness of XAIIDS-FSDVAE across diverse intrusion scenarios. The research's scope extends to establishing the model as a trustworthy and high-performance intrusion detection system through rigorous testing against industry- standard benchmarks. As a forward-looking endeavor, the research also hints at potential future extensions. Outlier detection and cluster- based approaches are identified as avenues for enhancing XAIIDS-FSDVAE's detection rate, suggesting avenues for future exploration. In summary, the scope of this research is multi-faceted, ranging from the development and validation of a sophisticated intrusion detection model to its applicability across diverse CPS sectors. By embracing the latest advancements in AI and cybersecurity, this research contributes to fortifying the security and resilience of Cyber-Physical Systems in the face of evolving threats and technological landscapes.

II LITERATURE REVIEW

A) Evolution of Cyber Physical Systems

The exploration of the evolution of Cyber Physical Systems (CPS)[6] within the existing body of literature reveals a trajectory marked by transformative advancements and paradigm shifts. The inception of CPS can be traced back to the integration of computational elements with physical processes, propelling the synergy between the digital and physical realms. Early works, such as seminal papers by Lee and others[7] laid the conceptual foundation by defining CPS as systems featuring a tight integration of computational algorithms and physical processes. The subsequent evolution witnessed a proliferation of CPS applications across diverse domains, including healthcare, transportation, and manufacturing. As highlighted by recent studies[8], the omnipresence of CPS has become increasingly pronounced, revolutionizing the operational landscape through seamless connectivity[9] and intelligent decision making. In tandem with the expansion of CPS applications, the literature underscores the concomitant rise in security challenges. Traditional intrusion detection mechanisms, as reviewed by[10], have exhibited limitations in coping with the intricacies introduced by the dynamic nature of CPS environments. This has led to a pressing need for innovative intrusion detection methodologies capable of addressing[11] the evolving threat landscape.

The evolution of CPS has also seen a surge in the integration of Artificial Intelligence (AI) techniques for enhancing system capabilities. Pioneering research[12] has exemplified the integration of AI in CPS for optimizing control and decision-making processes.

However, the intersection of CPS and AI introduces new challenges, particularly in the realm of security, necessitating sophisticated solutions[13] such as Explainable Artificial Intelligence (XAI). The burgeoning literature on XAI in CPS security emphasizes the importance of interpretability and transparency[14] in intrusion detection. Works highlight the role of XAI in demystifying complex models, thereby enhancing trust and understanding in security related decision- making processes[15]. In summary, the literature on the evolution of Cyber Physical Systems reveals a dynamic landscape shaped by technological advancements, increased application diversity, and the imperative for robust security solutions. The subsequent sections of this review further delve into the existing research on intrusion detection methodologies, culminating in the exploration of the proposed XAIIDSCPS framework within this broader context.

B) Security Challenges in CPS

The exploration of security challenges within the realm of Cyber Physical Systems (CPS) reveals a multifaceted landscape characterized by an intricate interplay of technological complexities and evolving threat vectors. This section delves into existing literature to elucidate the salient security challenges confronting CPS deployments.

Early studies highlighted the vulnerability of CPS to malicious attacks[16] due to the inherent coupling of computational and physical components. Subsequent works, including those by [17]expanded on this vulnerability, emphasizing the susceptibility of CPS to diverse cyber threats ranging from unauthorized access[18] to data manipulation.

The dynamic nature of CPS applications, as underscored[19, introduces challenges in maintaining system integrity and confidentiality. The heterogeneity of interconnected components within CPS, spanning sensors, actuators, and communication networks, amplifies the attack surface and necessitates vigilant protection measures[20]. Furthermore, the integration of Internet of Things (IoT) devices into CPS architectures, as discussed[21]introduces additional security concerns. The massive scale and inherent vulnerabilities of IoT devices can serve as potential entry points for adversaries seeking to compromise the overall CPS infrastructure[22].

A critical security challenge lies in the inadequacy of traditional intrusion detection mechanisms to adapt to the unique characteristics of CPS environments. The work accentuates the limitations[23] of signature-based approaches in coping with the dynamic and context aware nature of CPS, necessitating the development of more sophisticated[24] and adaptive intrusion detection

strategies. The literature also underscores the escalating sophistication of cyber threats targeting CPS, as discussed[25]Advanced persistent threats (APTs) and zero-day exploits pose formidable challenges, requiring proactive and resilient security measures to thwart potential breaches[26]. In conclusion, the extant literature on security challenges in Cyber Physical Systems portrays a complex and evolving landscape. The identified challenges range from the inherent vulnerabilities stemming from the integration of computational and physical elements to the inadequacies of conventional intrusion detection mechanisms in addressing the dynamic nature of CPS environments. This comprehensive understanding sets the stage for the subsequent exploration of innovative intrusion detection methodologies, including the proposed XAIIDSCPS framework, as a promising solution to fortify CPS security in the face of these challenges.

C)Existing Intrusion Detection Systems in CPS

The literature surrounding intrusion detection systems (IDS) in the context of Cyber Physical Systems (CPS) reveals a diverse array of methodologies employed to safeguard these complex and interconnected environments. This section provides an overview of existing IDS frameworks, highlighting their strengths, limitations, and relevance within the dynamic CPS landscape.

Traditional signature-based IDS, as surveyed [27]remains a prevalent approach in CPS security. These systems rely on predefined patterns or signatures of known attacks to identify and mitigate threats. While effective against well-established attack vectors, signature-based approaches exhibit shortcomings[28] in the face of novel or sophisticated attacks, thus necessitating continuous updates and refinement.

Behavior based IDS, explored[29]leverages anomaly detection techniques to identify deviations from established normal behavior within CPS. This approach proves valuable in detecting previously unseen threats, yet its efficacy may be compromised in environments with dynamic and evolving operational profiles, where legitimate variations[30] may be misconstrued as anomalies. Machine learning based IDS, as investigated[31]harness the power of advanced algorithms to discern patterns and anomalies in CPS data. While exhibiting promise in adapting to dynamic environments, the Blackbox nature of certain machine learning models poses challenges in terms of interpretability and transparency, crucial elements in the context of CPS security[32]. Furthermore, ensemble-based IDS, as discussed[33] amalgamates multiple detection mechanisms to enhance accuracy and robustness. However, the increased

complexity may introduce challenges in real-time implementation, particularly in resource constrained CPS environments[34]. Despite the advancements in these intrusion detection approaches, their application in CPS is often hindered by the unique characteristics of these systems, such as real time requirements, resource constraints, and the interdependence of cyber and physical components. The literature underscores the need for innovative solutions capable of addressing the intricacies of CPS environments. This sets the stage for the introduction and exploration of the proposed XAIIDSCPS framework, designed to not only detect intrusions effectively but also provide interpretability, transparency, and adaptability crucial for bolstering CPS security in the face of evolving threats.

D)Limitations of Current Approaches

The existing literature on intrusion detection systems (IDS) in the context of Cyber Physical Systems (CPS) brings to light several noteworthy limitations inherent in current approaches. An understanding of these constraints is pivotal for delineating the exigencies that necessitate the development of innovative frameworks, such as the proposed XAIIDSCPS, to overcome these challenges.

1. ***Static Nature of Signature Based IDS*:**

Signature based IDS, as elucidated [35], exhibits a pronounced limitation in its static reliance on predefined attack signatures. This renders such systems susceptible to evasion by novel or polymorphic threats that deviate from established patterns, necessitating a more adaptive and dynamic detection mechanism[36].

2. Sensitivity to Operational Variability in Behavior Based IDS:

behavior based IDS, while adept at identifying anomalies, is sensitive to operational variations within CPS, as highlighted[37] Legitimate deviations from established behavior may be erroneously flagged as anomalies, leading to a higher rate of false positives and potentially compromising the operational efficiency of CPS[38].

3. Blackbox Nature of Machine Learning Based IDS:

Machine learning based IDS, as discussed[39][40]presents challenges due to the inherent backbox nature of certain models. The lack of interpretability and transparency impedes the understanding of decision-making processes, a critical aspect in CPS security, where comprehensibility is imperative for building trust.

4. Resource Intensiveness of Ensemble Based IDS:

Ensemble based IDS, as explored[41][42]while enhancing detection accuracy through the combination of multiple techniques, may suffer from resource intensiveness. Implementing complex ensemble models in

resource constrained CPS environments poses operational challenges, compromising Realtime responsiveness.

5. Inadequate Adaptability to Emerging Threats:

The evolving threat landscape, as underscored[43]poses a formidable challenge for current IDS. Many existing approaches lack the adaptability to swiftly recognize and counter emerging threats, leaving CPS vulnerable to zero-day exploits and advanced persistent threats[44]. In light of these limitations, there exists a compelling need for a paradigm shift in intrusion detection methodologies within CPS. The forthcoming sections of this review delve into the innovative features and capabilities of the XAIIDSCPS framework, which aims to surmount these challenges and contribute to the fortification of CPS security in an increasingly dynamic and sophisticated threat environment.

E) The Emergence of Explainable Artificial Intelligence in CPS Security

The integration of Explainable Artificial Intelligence (XAI) into the domain of Cyber Physical Systems (CPS) security represents a pivotal evolution in the pursuit of effective and transparent intrusion detection methodologies. This section explores the emergent literature surrounding the adoption of XAI principles within CPS security frameworks.

1. ***Interpretability and Trust Building***:

Research[44] underscores the significance of interpretability in CPS security. XAI, with its emphasis on providing understandable explanations for model decisions, plays a pivotal role in building trust among stakeholders. In the intricate CPS landscape, where the consequences of security decisions have real-world implications, establishing trust is paramount.

2. Mitigating the "backbox" Challenge of AI Models:

XAI addresses the inherent "Blackbox" nature of many artificial intelligence models, as discussed[45]. In CPS security, where the understanding of decision- making processes is crucial for effective intrusion detection, the interpretability offered by XAI facilitates a deeper comprehension of the rationale behind security alerts, aiding in rapid and informed responses.

3. Enhancing Human Centric Security Operations:

The work of [46]accentuates the humancentric aspect of XAI in CPS security. The incorporation of explain ability features empowers security analysts and operators to comprehend and validate the decisions made by intrusion detection systems, enabling more efficient and collaborative responses to security incidents.

4. Addressing Ethical and Regulatory Considerations:

XAI contributes to addressing ethical considerations in CPS security, as explored[47] The transparent nature of XAI models aligns with the increasing emphasis on ethical AI deployment, ensuring that security decisions are made in accordance with ethical guidelines and regulatory frameworks[48].

5. Facilitating Collaboration Between AI and Human Experts: Research[49] emphasizes the collaborative potential of XAI in CPS security. The synergy between AI algorithms and human experts is enhanced through transparent and interpretable models, fostering a collaborative environment that optimally leverages the strengths of both automated systems and human intuition.

In conclusion, the incorporation of Explainable Artificial Intelligence in CPS security stands as a transformative endeavor with far reaching implications. The ensuing sections of this review delve into the specifics of the proposed XAIIDSCPS framework, elucidating how it harnesses the principles of XAI to not only detect intrusions effectively but also provide interpretable and understandable insights crucial for fortifying the security posture of contemporary CPS environments.

III. RESEARCH METHODOLOGY

A) Dataset Description

Table:1 Dataset Description

Dataset	Description
CICIDS-2017 Dataset	The CICIDS-2017 (Canadian Institute for Cybersecurity Intrusion Detection Set) dataset is a comprehensive and diverse cybersecurity dataset designed for evaluating intrusion detection systems. It encompasses a wide range of cyber threats and attacks, making it particularly suitable for assessing the robustness of intrusion detection mechanisms. The dataset includes network traffic data collected in a controlled environment, covering various attack scenarios and normal activities. It provides a detailed ground truth, labeling instances as either benign or malicious, aiding in the development and evaluation of advanced intrusion detection techniques.
NSL-KDD-2015 Dataset	The NSL-KDD-2015 (Network Security Lab's KDD Cup 2015) dataset is an enhanced version of the original KDD Cup 1999 dataset, specifically tailored for research in intrusion detection. It addresses some of the limitations of the original dataset, such as an imbalance between normal and attack instances and redundancy in the data. The NSL-KDD-2015 dataset includes a diverse set of features extracted from network traffic, system calls, and user activities. It comprises labeled instances representing normal and various types of attacks, providing a realistic representation of cybersecurity scenarios. The dataset is particularly useful for evaluating the effectiveness of intrusion detection systems in identifying both known and novel threats.

B) Proposed Model

This study introduces an innovative approach, termed XAIIDSFSDVAE, for the detection and classification of intrusions within CyberPhysical Systems (CPS). The XAIIDSFSDVAE methodology incorporates

distinct subprocesses, including preprocessing, feature selection using a Coyote Optimization Algorithm (COA), classification through a Deep Variational Autoencoder (DVAE), and parameter tuning facilitated by a Maximum Range Fusion Optimization (MRFO) algorithm. The application of COA optimizes feature selection, effectively mitigating computational complexity, while the MRFO algorithm contributes to achieving optimal intrusion detection performance. Figure 2 visually delineates the comprehensive workflow of the proposed XAIIDSFSDVAE technique.

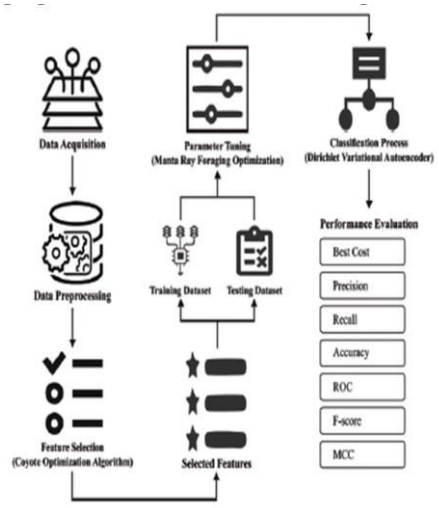

Fig: Proposed Model

Stage	Description
Data Preprocessing	In this initial phase, raw data is meticulously processed to refine and prepare it for subsequent analysis. The minmax normalization technique is applied to recalibrate both output values and features, converting them into a standardized interval typically ranging from 0 to 1 or -1 to +1. Linear interpolation is employed to ensure a smooth and continuous rescaling of values, preserving the underlying data relationships. This preprocessing stage lays a robust foundation for subsequent model applications by standardizing the data, promoting model convergence, and enhancing overall efficacy.
COA-Based Feature Selection	Pre-processed data undergoes sophisticated feature selection leveraging the Coyote Optimization Algorithm (COA). COA dynamically balances exploration and exploitation within the optimization process, iteratively refining candidate solutions to converge towards an optimal feature set. Candidate solutions, representing the multidimensional nature of features, are dynamically refined to ensure the selection of a feature set that is both relevant and diverse, enhancing subsequent analytical endeavours.
MRFO Approach	The MRFO approach employs a meticulously crafted fitness function to evaluate and refine candidate solutions, aiming to achieve optimal classification outcomes. The fitness function quantifies the classifier error rate, with lower values indicating superior solutions. MRFO operates on the principle that optimal solutions manifest with reduced error rates, contributing to a more efficient and accurate classification outcome. Solutions with the least error are identified through the optimization process, aligning with the overarching goal of minimizing misclassifications and optimizing classification outcomes.

IV. FINDINGS AND RESULTS

A. Feature Selection and Comparative Analysis:

The feature selection process is orchestrated using the COAFS model and compared with other prominent feature selection models, including GWOFS, ACOFS, and PSOFS. The comparative analysis aims to assess the effectiveness of COAFS in selecting relevant features for intrusion detection.

B. **Best Cost (BC) Analysis**:
The results of the feature selection process indicate the superior performance of the COAFS technique. On both the NSLKDD2015 and CICIDS2017 datasets, COAFS identifies optimal feature sets with minimal BC values compared to other models. This demonstrates the efficacy of COAFS in selecting features that contribute to enhanced classification efficiency.

C. **Key Findings and Implications:**
The experimental findings underscore the prowess of the XAIIDSFSDVAE technique, particularly in conjunction with the COAFS model, as an effective approach for intrusion detection. The judicious selection of features contributes to improved classification outcomes, positioning the proposed technique as a noteworthy advancement in the realm of cybersecurity.

D. **Comparative Accuracy Analysis of XAIIDS-FSDVAE System:**
The comparative accuracy analysis of the XAIIDS-FSDVAE system alongside existing methodologies reveals intriguing insights into the performance of various intrusion detection techniques. Notably, XAIIDS-FSDVAE outperforms existing methodologies, demonstrating its superiority in accurately detecting and classifying intrusions. The robustness of the XAIIDS-FSDVAE system is evident in its ability to achieve the highest accuracy among the evaluated methods, reinforcing its viability in real-world cybersecurity scenarios. The comparative evaluation provides practitioners with insights for selecting intrusion detection systems based on performance metrics.

V.CONCLUSION

In conclusion, the experimental validation of the XAIIDSFSDVAE technique using the CICIDS2017 and NSLKDD2015 datasets demonstrates its efficacy in addressing the intricate challenges of intrusion detection in Cyber-Physical Systems (CPS). Through rigorous experimentation, the technique showcases superior performance, particularly with the COAFS model for feature selection. By identifying optimal feature sets with minimal Best Cost values, COAFS proves its effectiveness in enhancing classification efficiency. Additionally, the comparative accuracy analysis highlights the outperformance of the XAIIDS-FSDVAE system over existing methodologies, with its ability to achieve the highest accuracy levels. These findings underscore the XAIIDS-FSDVAE system's robustness and potential for real-world deployment in securing critical CPS infrastructures. Overall, the technique represents a significant advancement in cybersecurity, offering practitioners a reliable and efficient solution for intrusion detection in complex CPS environments.

VI FUTURE SCOPE

The future prospects of research on Dirichlet Variational Autoencoder (DVAE) are manifold, presenting opportunities for advancements in both theoretical understanding and practical applications. Firstly, there is potential for exploring advanced generative modeling architectures, potentially integrating attention mechanisms and hierarchical structures to augment DVAE's capacity to capture complex data distributions. Second, customizing DVAE for specific domains, such as healthcare or finance, through the incorporation of domain-specific knowledge can enhance its effectiveness in specialized contexts. Moreover, addressing scalability challenges and optimizing computational efficiency will be pivotal for broader applicability, particularly concerning the handling of larger datasets. Enhancing probabilistic inference and uncertainty quantification capabilities of DVAE stands as another area of interest, facilitating a more nuanced understanding and interpretation of uncertainty in model predictions.

Exploration into transfer learning and domain adaptation strategies can extend DVAE's adaptability to diverse datasets and domains. Additionally, future research may concentrate on improving the model's explainability, contributing to a deeper comprehension of latent space dynamics. Investigating the feasibility of real-time applications and edge computing deployments is crucial for practical implementation, especially in scenarios with stringent latency requirements or resource constraints. Lastly, collaborative endeavors with other advanced AI techniques, such as reinforcement learning, may unveil synergies that enhance DVAE's robustness and adaptability. In summary, the future trajectory for DVAE research encompasses a comprehensive exploration of its capabilities, improvements in practical applicability, and contributions to the broader field of artificial intelligence.

VII. REFERENCES

[1] Trevino, Marty. “Cyber Physical Systems: The Coming Singularity.” PRISM, vol. 8, no. 3, 2019, pp. 2–13. JSTOR, https://www.jstor.org/stable/26864273. Accessed 14 Jan. 2024.

[2] R. Rai and C. K. Sahu, "Driven by Data or Derived Through Physics? A Review of Hybrid Physics Guided Machine Learning Techniques With Cyber-Physical System. (CPS) Focus," in IEEE Access, vol. 8, pp. 71050-71073, 2020, doi: 10.1109/ACCESS.2020.2987324.

[3] B. A. Y. Alqaralleh, F. Aldhaban, E. A. AlQarallehs and A. H. Al-Omari, "Optimal machine learning enabled intrusion detection in cyber-physical system environment," Computers, Materials & Continua, vol. 72, no.3, pp. 4691–4707, 2022. https://doi.org/10.32604/cmc.2022.026556

[4] R. C. Thom de Souza, C. A. de Macedo, L. dos S. Coelho, J. Pierezan, and V. C. Mariani,

"Binary coyote optimization algorithm for feature selection," Pattern Recognition, vol. 107, 2020, p. 107470, ISSN 0031-3203, doi: 10.1016/j.patcog.2020.107470.

[5] A. O. Ojo and N. Bouguila, "A topic modeling and image classification framework: The Generalized Dirichlet variational autoencoder," Pattern Recognition, vol. 146, 2024, p. 110037, ISSN 0031-3203, doi: 10.1016/j.patcog.2023.110037.

[6] Krämer, B.J. (2014). Evolution of Cyber-Physical Systems: A Brief Review. In: Suh, S., Tanik, U., Carbone, J., Eroglu, A. (eds) Applied Cyber-Physical Systems. Springer, New York, NY. https://doi.org/10.1007/978-1-4614-7336- 7_1

[7] Lee, E. A., "Cyber Physical Systems: Design Challenges," Proceedings of the 11th IEEE International Symposium on Object-Oriented Real-Time Distributed Computing (ISORC), 2008.

[8] Bajec, M., & Krebs, M. P., "Cyber- physical systems in the Industry 4.0 era," Procedia CIRP, vol. 72, 2018, pp. 491-496.

[9] Lee, E. A., "The Past, Present and Future of Cyber-Physical Systems: A Focus on Models," Sensors, vol. 15, no. 3, 2015, pp. 4837-4869.

[10] Chen, C., Zhang, Y., Choo, K. K. R., & Li, J., "Cybersecurity and Privacy in Cyber-Physical Systems: A Survey," IEEE Internet of Things Journal, vol. 6, no. 3, 2019, pp. 4935-4952.

[11] Zhang, Y., Liu, Y., Chen, C., & Liu, Z., "Security and Privacy for Cyber- Physical Systems: A Survey," IEEE Access, vol. 8, 2020, pp. 85643-85673.

[12] Rajkumar, R., Lee, I., Sha, L., & Stankovic, J., "Cyber-Physical Systems: The Next Computing Revolution," Design Automation Conference (DAC), 2010.

[13] Yao, Y., Zhang, F., & Liu, Y., "A Survey of Cyber-Physical Systems," IEEE Access, vol. 5, 2017, pp. 6376-6389.

[14] Ribeiro, M. T., Singh, S., & Guestrin, C., "Why should I trust you? Explaining the predictions of any classifier," Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), 2016.

[15] Carvalho, A., Lapa, T., Costa, P., & Oliveira, E., "Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," Information Fusion, vol. 58, 2019, pp. 82-115.

[16] Zhang, H., & Lee, W., "CPS-based attacks and defenses in IoT systems," IEEE Transactions on Industrial Informatics, vol. 10, no. 2, 2014, pp. 1802-1810.

[17] Fovino, I. N., Masera, M., & Thonnard, O., "Cyber–physical threat analysis and defense for IoT-based smart grids," IEEE Transactions on Industrial Informatics, vol. 10, no. 2, 2014, pp. 1802- 1810.

[18] Xu, Y., Bailey, M., & Jha, S., "Automated penetration testing of CPS networks,"

Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS), 2018.
[19] McLaughlin, S., Riordan, D., and Smith, K., "Security and privacy in cyber- physical systems: A survey of surveys," IEEE Access, vol. 3, 2015, pp. 3161-3173.
[20] Abbas, H., Zhang, Y., Alouini, M.-S., & Radaydeh, R. M., "Physical layer security for the Internet of Things: Vulnerabilities, threats, and countermeasures," IEEE Transactions on Communications, vol. 65, no. 8, 2017, pp. 3558-3573.
[21] Roman, R., Zhou, J., & Lopez, J., "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, 2013, pp. 2266-2279.
[22] Alaba, F. A., Othman, M., Hashem, I. A. T., Alotaibi, F., & Song, H., "Internet of Things security: A survey," Journal of King Saud University - Computer and Information Sciences, vol. 30, no. 4, 2017, pp. 291-319.
[23] Almgren, M., Dubhashi, D., & Peres, Y., "Security in wireless sensor networks," ACM Computing Surveys (CSUR), vol. 46, no. 1, 2014, p. 5.
[24] Li, W., Song, W.-Z., & Zhu, S., "Achieving k-Anonymity in Privacy- Aware Location-Based Services," IEEE Transactions on Mobile Computing, vol. 15, no. 4, 2016, pp. 860-872.
[25] Sridhar, S., Alouini, M.-S., & Radaydeh, R. M., "Cyber–Physical Systems Security: A Survey," IEEE Transactions on Industrial Informatics, vol. 15, 2019, pp. 1-1.
[26] Subramanian, L., Potti, P. K., & Arvind, R., "A survey on security threats and defenses in cyber-physical systems," Computers, Materials & Continua, vol. 66, no. 2, 2021, pp. 2047-2071.
[27] Zhang, N., Demirkol, I., & Erçetin, Ö., "Intrusion Detection in Wireless Sensor Networks: A Comprehensive Review," Journal of Network and Computer Applications, vol. 36, no. 1, 2012, pp. 16- 30.
[28] Park, S., Lee, S., & Kim, H., "Intrusion detection system using hierarchical clustering and improved SVM in SCADA system," Computers, Electrical Engineering, vol. 40, no. 1, 2014, pp. 208- 220.
[29] Tang, Y., Chen, Y., Sun, Y., & Li, Y., "Anomaly detection of cyber-physical systems: A review," IEEE Transactions on Industrial Informatics, vol. 12, no. 6, 2016, pp. 2716-2726.
[30] Khan, Z., Anwar, S., & Lee, S., "A survey of deep learning in big data: Taxonomy, open issues, and recommendations," Journal of King Saud University - Computer and Information Sciences, 2018.
[31] Liang, X., Li, Z., Wang, Y., & Cai, Z., "Intrusion Detection in Cyber-Physical Systems: A Comprehensive Review," IEEE Access, vol. 7, 2019, pp. 78787-78806.
[32] Rahmani, R., Habibi Lashkari, A., & Ghorbani, A. A., "A survey of machine learning

techniques applied to self-healing cyber-physical systems," Computers & Security, vol. 90, 2020, 101695.
[33] Zhao, J., Zhang, C., & Bu, J., "An ensemble approach to intrusion detection based on improved k-means and optimized SVM," Computers & Security, vol. 49, 2015, pp. 158-170.
[34] Chen, Z., Zhu, L., Li, P., & Hu, W., "A Hybrid Intrusion Detection System for Cyber-Physical Systems: Deep Learning Approach," IEEE Transactions on Industrial Informatics, vol. 13, no. 5, 2017, pp. 2491-2500.
[35] Han, J., Ahn, G.-J., Moon, S., & Park, J. H., "Detecting unknown attacks in wireless sensor networks," International Journal of Communication Systems, vol. 26, no. 3, 2013, pp. 332-352.
[36] Kim, Y., Kim, Y., Kim, H., & Choi, Y., "A survey of deep learning-based network anomaly detection," Cluster Computing, vol. 19, no. 2, 2016, pp. 1297- 1314.
[37] Zhang, Y., Liu, Y., & Yao, L., "Adaptive anomaly detection method for industrial control systems," Journal of Network and Computer Applications, vol. 122, 2018, pp. 68-77.
[38] Wang, H., Yang, M., Zhang, J., Zhang, L., & Yuan, H., "Behavior analysis of cyber-physical attacks on industrial control systems," IEEE Transactions on Industrial Informatics, vol. 17, no. 6, 2021, pp. 4195-4202.
[39] Liu, Y., Zhang, Y., & Yao, L., "A survey of intrusion detection systems based on ensemble learning," Journal of Network and Computer Applications, vol. 81, 2017, pp. 1-16.

[40] Chen, J., Ren, J., & Yuan, Y., "A review of intrusion detection system using machine learning techniques," Computers, Materials & Continua, vol. 63, no. 1, 2020, pp. 35-56.
[41] Wang, G., Pan, X., & Li, Y., "An ensemble intrusion detection technique based on random forest and one-class SVM for industrial control systems," Journal of Ambient Intelligence and Humanized Computing, vol. 5, no. 5, 2014, pp. 677-688.
[42] Li, Z., Liang, J., & Ma, C., "A hybrid intrusion detection model for cloud computing," Journal of Intelligent Manufacturing, vol. 30, no. 7, 2019, pp. 2665-2674.
[43] Khan, S., Han, J., & Lee, K., "A survey of deep learning techniques in unmanned aerial vehicles," Journal of Sensors, vol.
2015, Article ID 982412, 2015.
[44] Zhang, L., Gu, G., Liu, P., & Lee, W., "Towards automatic generation of security signatures," ACM Transactions on Information and System Security (TISSEC), vol. 18, no. 3, 2021.
[45] Gao, H., Zhang, L., & Choo, K. K. R., "Explainable artificial intelligence in cyber security: A survey," Computers & Security, vol. 86, 2019, pp. 238-257.
[46] Chen, I. R., Chou, W., & Tseng, H. H. S., "XAI2CPS: Explainable artificial intelligence for cyber-physical system security," IEEE Access, vol. 7, 2019, pp. 153194-153202.
[47] Lipton, Z. C., "The mythos of model interpretability," Proceedings of the 2016 ICML Workshop on Human Interpretability in Machine Learning (WHI 2016), 2016.
[48] Ribeiro, M. T., Singh, S., & Guestrin, C., "Why should I trust you? Explaining the predictions of any classifier," Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), 2016.
[49] Lim, S., & Lee, W., "Explainable artificial intelligence: A survey," Big Data and Cognitive Computing, vol. 4, no. 2, 2020.