www.editada.org

International Journal of Combinatorial Optimization Problems and Informatics, 16(4), Sep-Dec 2025, 375-380. ISSN: 2007-1558. https://doi.org/10.61467/2007.1558.2025.v16i4.1023

Systematic Review of Evolutionary Algorithm-Based Techniques for Cyberattack Detection in IoT and IIoT Environments

Jesús Enrique Soto-Soto[1], José Isidro Hernández-Vega[1], Alejandra Guadalupe Silva-Trujillo[2], Luis Alejandro Reynoso-Guajardo[1], Carlos Hernández-Santos[1], Mario Carlos Gallardo-Morales[1]
[1] TecNM Instituto Tecnológico de Nuevo León, México.
[2] Universidad Autónoma de San Luis Potosí, México
jesussoto171996@gmail.com, {jose.hv, luis.rg, mario.gm}@nuevoleon.tecnm.mx, asilva@uaslp.mx, carlos.hernandez@itnl.edu.mx

Abstract. The rapid growth of the Internet of Things (IoT) in industrial environments has increased efficiency but also heightened vulnerability to sophisticated cyber-attacks. Traditional cyber security approaches are insufficient to protect critical infrastructure, creating a need for dynamic, adaptive solutions. Evolutionary algorithms (EAs), owing to their ability to explore large search spaces and optimise parameters, offer a promising route to enhancing IoT security. This review highlights the integration of EAs with deep-learning techniques to improve intrusion detection and system resilience. Building on this background, we propose an adaptive cyber-security framework that leverages evolutionary optimisation and continual learning to detect, prevent and mitigate attacks in real time. The study emphasises the importance of validating hybrid models in real-world settings and of optimising computational efficiency. Future work should investigate autonomous response mechanisms and the scalability of solutions for large-scale Industrial IoT (IIoT) deployments, ensuring robust protection against emerging threats and aligning academic advances with industry needs.
Keywords: cybersecurity, internet of things, industrial internet of things, optimization, evolutionary algorithms

Article Info
Received February 25, 2025
Accepted July 6, 2025

1 Introduction

The integration of the Internet of Things (IoT) into industrial environments has significantly transformed the way operations are managed and optimized. This convergence, known as the Industrial Internet of Things (IIoT), has enabled greater efficiency, real-time monitoring, and process automation. However, this interconnectivity has also expanded the attack surface, exposing critical infrastructures to a wide range of cyber threats.

Recent studies highlight that the adoption of advanced digital technologies in industrial settings has introduced new vulnerabilities to cyberattacks, giving rise to the concept of cyber-resilience as a key strategy to mitigate these risks (Alshahrani et al., 2023; Lezzy et al., 2025). Traditional intrusion detection systems (IDSs), which rely on signatures or predefined rules, are often inadequate for detecting sophisticated and previously unknown attacks in IIoT environments. To address this limitation, more adaptive and intelligent techniques, such as evolutionary algorithms (EAs), have been explored. These algorithms, inspired by natural processes such as selection and evolution, have proven effective in optimizing solutions to complex and dynamic problems, including anomaly detection in IoT networks (Thakkar et al., 2020).

Several studies have proposed hybrid approaches that combine EAs with machine learning and deep learning techniques to enhance detection accuracy and reduce false positive rates. For instance, the integration of genetic algorithms with deep neural networks has demonstrated significant improvements in identifying attack patterns within IIoT environments (Zhang et al., 2021). Additionally, systems employing Particle Swarm Optimization and Grey Wolf Optimization have been developed for relevant feature selection and parameter tuning in detection models (Fang et al., 2024; Gueriani et al., 2024). Despite these advancements, multiple challenges remain, including the lack of validation in real-world environments, the scarcity of standardized datasets, and the high computational costs associated with deploying such systems on resource-constrained

devices. Moreover, the rapid evolution of cyber threats demands solutions that are not only accurate but also adaptable and scalable (Bankó et al., 2025).
The objective of this study is to analyze and classify evolutionary algorithm–based techniques, both pure and hybrid, applied to cyberattack detection in IoT and IIoT environments between 2020 and 2025. The aim is to identify emerging trends, strengths, limitations, and improvement opportunities with respect to accuracy, scalability, and adaptability in cybersecurity systems.

2 Methodology

This review focused on studies published between 2020 and 2025 that apply evolutionary algorithms (EAs) to the detection and mitigation of cyberattacks in IoT and IIoT environments. The literature was collected from high-impact academic databases such as IEEE Xplore, MDPI, ScienceDirect, and SpringerLink, selecting only peer-reviewed articles that included experimental validation.

The inclusion criteria were as follows: (i) explicit implementation of evolutionary algorithms or nature-inspired metaheuristic techniques (such as Genetic Algorithms, Particle Swarm Optimization, Differential Evolution, among others); (ii) applications focused on cybersecurity in IoT/IIoT networks; (iii) quantitative reporting of performance metrics such as accuracy, recall, F1-score, detection rate, or false positive rate; and (iv) publication date between 2020 and 2025, with keywords including cybersecurity, evolutionary algorithm, IoT, IIoT, and metrics. Exclusion criteria comprised narrative reviews without comparative results, studies lacking numerical validation, conceptual works, or implementations outside the IoT/IIoT domain.

As a result, 17 studies meeting the inclusion criteria were selected and are summarized in Table 1. This table organizes key information from each article, including the authors, the proposed technical approach, the algorithms or techniques applied, and the reported evaluation metrics. The synthesis of these works enabled the analysis to be structured around three main axes: the type of evolutionary algorithm employed (classical or hybrid), the methodological approach and system architecture, and the experimental results obtained.

A consistent finding across literature is the superiority of hybrid approaches that combine evolutionary algorithms with deep learning techniques, particularly in conventional performance metrics such as accuracy, recall, and F1-score. For instance, studies such as (Alkhafaji et al., 2024) and (Prasad et al., 2024) report accuracy values exceeding 98%, in contrast to models based solely on classical evolutionary algorithms, such as (Dwivedi et al., 2020), where accuracy remains below 93%. This discrepancy can be attributed to the ability of deep neural networks to capture complex nonlinear patterns in the data, while evolutionary algorithms simultaneously optimize model configurations—resulting in greater overall effectiveness in threat detection.

Similar trends are observed when comparing recall or detection rate: hybrid models consistently achieve values above 95%, as reported by (Saheed et al., 2024) and (Bajpai et al., 2024), indicating a high capacity to correctly identify actual attacks. In contrast, studies relying exclusively on traditional evolutionary techniques or without integration of supervised learning methods, such as (Kareem et al., 2022), report lower recall values, typically ranging between 88% and 90%, which may compromise the detection of advanced or stealthy threats. This difference is particularly critical in industrial applications, where undetected attacks can result in significant operational and economic damage. Furthermore, some studies—such as (Francis et al., 2024)—demonstrate the possibility of achieving a balance between high accuracy and an acceptable false positive rate by employing classifiers like Random Forest, optimized via evolutionary algorithms.

Regarding the F1-score, which reflects the harmonic balance between precision and recall, the most effective models reach nearly or above 96%, especially those integrating autoencoder mechanisms or deep classifiers fine-tuned with algorithms such as Grey Wolf Optimization (GWO) or Particle Swarm Optimization (PSO). The effective combination of evolutionary feature selection with structured learning allows these models to maintain such balance even when working with highly imbalanced datasets, as demonstrated by (Dey et al., 2023) and (Huang et al., 2022).

Nevertheless, it should be noted that some studies fail to report essential metrics such as the Area Under the Curve (AUC) or false positive rate, limiting full comparability across models. Still, the overall evidence indicates that the strategic incorporation of evolutionary algorithms within hybrid architecture provides a substantial and consistent improvement in evaluation metrics when compared to conventional or monolithic methods.

The qualitative and quantitative analysis of these studies serves as the foundation for identifying emerging trends, strengths, recurring limitations, and future research opportunities in the development of more adaptive and efficient cybersecurity systems for interconnected industrial environments.

Table 1. Related work on IIoT infrastructures with evolutionary algorithms

Reference	Paper	Algorithm/Technique	Metrics
Talpur et al. (2025)	ML-Based Detection of DDoS Attacks Using Evolutionary Algorithms Optimization	Genetic Algorithm, XGBoost, Random Forest	Accuracy, Precision, Recall, F1-score
Maazalahi et al. (2025)	A Novel Hybrid Method Using Grey Wolf Algorithm and Genetic Algorithm for IoT Botnet DDoS Attacks Detection	Hybrid Method of Grey Wolf Algorithm and Genetic Algorithm	Accuracy, Precision, Recall, F1-measure
Bajpai et al. (2024)	Anomaly Detection in IoT Networks Using Differential Evolution and XGBoost	Differential Evolution and XGBoost Model	Accuracy, Detection rate, Precision, F1-score, False alarm rate
Alkhafaji et al. (2024)	Integrated Genetic Algorithm and Deep Learning Approach for Effective Cyber-Attack Detection and Classification in IIoT Environments	Genetic Algorithm, Deep Neural Network	Accuracy, Loss, Precision, Recall
Saheed et al. (2024)	Modified genetic algorithm and fine-tuned long short-term memory network for intrusion detection on the internet of things networks with edge capabilities	Hybrid model of Genetic Algorithm with Long Short-Term Memory Network	Accuracy, Precision, Sensitivity, Detection Rate
Francis et al. (2024)	A hybrid intrusion detection approach based on message queuing telemetry transport (MQTT) protocol in industrial internet of things.	Hybrid model of Genetic Algorithm with Random Forest	Accuracy, Precision, Recall, F1-score, Mean absolute error
Prasad et al. (2024)	Augmenting cybersecurity through attention based stacked autoencoder with optimization algorithm for detection and mitigation of attacks on IoT assisted networks	Attention-based Stacked Autoencoder with Pelican Optimization Algorithm, Greylag Goose Optimization	Accuracy, Precision, Recall, F1-score, AUC score, Processing time
Dey et al. (2023)	Hybrid Meta-Heuristic based Feature Selection Mechanism for Cyber-Attack Detection in IoT-enabled Networks	Hybrid Meta-heuristic of the Grey Wolf Optimization algorithm and the Gravitational Search Algorithm, Decision Tree, AdaBoost, Random Forest	Accuracy, F1-score, Precision, False Positive Rate, Detection Rate
Kareem et al. (2022)	An Effective Feature Selection Model Using Hybrid Metaheuristic Algorithms for IoT Intrusion Detection	Hybrid model of Gorilla Troops Optimizer with Bird Swarm Algorithm	Average accuracy, Sensitivity, Specificity, Average Fitness, Average number of features, Average computation time Standard deviation
Leon et al. (2022)	Feature encoding with autoencoder and differential evolution for network intrusion detection using machine learning	Differential evolution	Mean Squared Error, Accuracy
Alterazi et al. (2022)	Prevention of Cyber Security with the Internet of Things Using Particle Swarm Optimization	Genetic Algorithm, Ant Colony Optimization, Particle Swarm Optimization	Accuracy, Precision, Recall, F-Measure
Huang et al. (2022)	SOPA-GA-CNN: Synchronous optimization of parameters and architectures by genetic algorithms with convolutional neural network blocks for securing Industrial Internet-of-Things.	Synchronously optimisation of parameters and architectures by genetic algorithms with convolutional neural networks	Accuracy, Precision, Recall, F1-score, Number of paramters
Kasongo et al. (2021)	An Advanced Intrusion Detection System for IIoT Based on GA and Tree-Based Algorithms	Genetic Algorithm with Random Forest and to classify with Decision Tree, Random Forest, Extra Trees, Logistic Regression, Naïve Bayes, Extreme Gradient Boosting	Accuracy, Precision, Recall, F1-score, ROC curve True Positive vs False Positive rates, AUC
Lu et al. (2021)	Evolutionary Deep Belief Network for Cyber-Attack Detection in Industrial Automation and Control System	Population extremal optimization - based deep belief network detection method	Accuracy, False positive rate, Friedman test, Quade test
Faber et al. (2021)	Ensemble Neuroevolution-Based Approach for Multivariate Time Series Anomaly Detection	Neuroevolution techniques with deep learning models	Precision, Recall, F1-score
Davahli et al. (2020)	Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight	Hybrid model of Genetic algorithm and Gery wolf	Accuracy, Detection rate, False Positive rate, Precision, F1- score

	intrusion detection system for IoT wireless networks	optimizer	
Dwivedi et al. (2020)	Defense against distributed DoS attack detection by using intelligent evolutionary algorithm	Grasshopper optimization algorithm with Support vector machine, Multi-layer perceptron, Naïve Bayes, Decision Tree	Accuracy, Recall, Precision, F-measure, False positive rate, Specificity, AUC

3 Discussion

The systematic review on the use of evolutionary algorithms in intrusion detection systems within IoT and IIoT environments reveals a series of trends, strengths, limitations, and research opportunities that provide a comprehensive perspective on the current state of the art.

One of the most notable findings is the prevalence of Genetic Algorithm (GA) as the foundational evolutionary technique in numerous studies. This predominance can be attributed to its versatility, ease of implementation, and proven effectiveness in parameter optimization and feature selection tasks. (Alkhafaji et al., 2024) and (Kasongo et al., 2021), for example, demonstrated that combining GA with robust classifiers such as deep neural networks or decision trees significantly improves metrics like accuracy, recall, and detection rate.

However, there is a clear shift toward hybrid models that integrate evolutionary algorithms with deep learning, traditional machine learning, and other metaheuristic methods. Studies such as those by (Prasad et al., 2024) and (Dey et al., 2023) propose models where evolutionary algorithms not only tune parameters but also serve as feature selection mechanisms for deep neural networks, autoencoders, and ensemble models. This hybrid approach not only enhances the overall performance of intrusion detection systems but also contributes to reducing false positives—one of the persistent challenges in IoT cybersecurity.

Another important trend is the increasing use of alternative evolutionary algorithms, including Differential Evolution (DE), Particle Swarm Optimization (PSO), Grey Wolf Optimizer (GWO), and, more recently, nature-inspired optimizers such as the Pelican Optimization Algorithm and Gorilla Troops Optimizer. These methods have been applied to mitigate issues such as premature convergence and to improve exploration of the search space, showing promising results, particularly when embedded in multilayered or adaptive architectures.

Among the main strengths identified, the adaptive capacity of evolutionary algorithms stands out, as it allows flexible responses to dynamic scenarios and changing environments—an essential characteristic of IoT networks. Their effectiveness in feature selection is equally relevant, reducing the dimensionality of complex datasets and facilitating the identification of relevant variables for anomaly detection. This optimization capability translates into measurable improvements in accuracy, recall, and F1-score, demonstrating a direct impact on detection capabilities. Furthermore, their modularity is advantageous, since they can be integrated as standalone components within broader architectures, improving existing models without requiring complete restructuring.

Nevertheless, several limitations remain. A recurring issue is the limited validation of models in simulated or controlled environments, which restricts the generalizability of results to real-world scenarios, where network conditions, noise levels, and attack types are more diverse. Additionally, only a minority of studies report the computational costs of training and inference, raising concerns about feasibility on resource-constrained devices such as gateways or microcontrollers.

Another critical limitation is the lack of standardization in evaluation metrics, which hinders objective comparison across studies—particularly when essential indicators such as false positive rate, energy consumption, or response time are omitted. Reproducibility also remains a challenge, as many authors do not provide comprehensive technical details, preprocessed datasets, or source code, limiting the ability of the research community to replicate or benchmark results against new techniques.

Despite these challenges, the research landscape offers clear opportunities to move toward more robust and practical solutions. A priority direction is the validation of models in real industrial infrastructures or laboratory testbeds, to evaluate their performance under heterogeneous traffic and novel attack scenarios. There is also a pressing need for lightweight models tailored to edge computing environments, capable of running efficiently on devices with limited resources while maintaining high accuracy.

Another promising avenue is the incorporation of adaptive and continuous learning mechanisms, enabling systems to evolve in response to emerging threats without requiring manual retraining. Similarly, collaborative intelligence across distributed nodes

could provide an effective strategy for event correlation and distributed detection. Finally, advancing toward standardized evaluation frameworks, including public datasets, common testing conditions, and unified metrics, will be essential for enabling rigorous comparisons, fostering transparency, and ensuring reproducibility in future research.

4 Conclusions

The findings of this systematic review reaffirm that evolutionary algorithms (EAs) constitute a highly promising approach for addressing the current challenges in the detection and mitigation of cyberattacks in IoT and IIoT environments. Their capacity to explore complex search spaces and dynamically adapt to changing conditions makes them well-suited for industrial cybersecurity systems. In particular, the integration of EAs with machine learning and deep learning techniques has led to the development of hybrid models capable of overcoming the limitations of traditional approaches, particularly in identifying sophisticated attacks, reducing false positives, and improving key metrics such as accuracy, recall, and F1-score.

Furthermore, there is a clear trend toward the design of modular and scalable architectures, where EAs are employed not only as parameter optimizers or feature selectors but also as central components within adaptive decision-making systems. This versatility allows models to be tailored to diverse industrial contexts, ranging from distributed sensor networks to SCADA systems, thereby broadening their applicability. However, the review also highlights significant gaps in literature, including the lack of experimental validation in real-world production environments, the absence of models optimized for deployment on resource-constrained devices, and the limited standardization of evaluation procedures.

Therefore, it can be concluded that although the use of evolutionary algorithms has demonstrated clear advantages in simulated and controlled environments, their transition to real industrial scenarios requires greater emphasis on computational efficiency, interoperability with existing infrastructures, and the incorporation of continuous learning mechanisms to respond to emerging threats. In this regard, collaboration between academia and industry becomes essential to bridge this gap—through the development of experimental frameworks that enable model evaluation under real operating conditions, using authentic network traffic and evolving threat landscapes.

5 Future work

Based on the analysis of the 18 reviewed studies, future research should prioritize the design and experimental validation of adaptive cybersecurity architectures that leverage evolutionary algorithms within industrial IoT environments. The findings of this review suggest that hybrid models combining evolutionary optimization with deep learning classifiers offer notable improvements in detection accuracy and in reducing false positives.

A promising research direction involves the development of modular intrusion detection systems capable of self-optimization through algorithms such as Genetic Algorithm (GA), Differential Evolution (DE), Grey Wolf Optimizer (GWO), and Particle Swarm Optimization (PSO), integrated with deep learning frameworks. These systems should incorporate continuous monitoring capabilities for industrial protocols (e.g., Modbus, OPC UA, MQTT), along with dynamic feature selection mechanisms that adapt to environmental changes and evolving threat patterns.

To assess their feasibility, future studies should implement these models in laboratory-scale industrial testbeds, using real sensor data combined with simulated attack traffic. Special emphasis should be placed on evaluating performance under operational constraints such as limited computational resources, high-volume data streams, and latency requirements typical of edge computing platforms.

Additionally, researchers are encouraged to investigate the integration of autonomous response mechanisms, enabling real-time mitigation actions based on anomaly detection. These perspectives highlight the importance of bridging the gap between theoretical optimization and practical implementation through sustained collaboration between academia and industry.

Such advancements could significantly enhance cyber-resilience in critical sectors such as manufacturing, energy, and smart logistics, ultimately providing scalable, efficient, and context-aware solutions tailored to the specific challenges of IIoT environments.

References

Alkhafaji, N., Viana, T., & Al-Sherbaz, A. (2024). Integrated Genetic Algorithm and Deep Learning Approach for Effective Cyber-Attack Detection and Classification in Industrial Internet of Things (IIoT) Environments. Arab. J. Sci. Eng., 1–25. https://doi.org/10.1007/s13369-024-09663-6

Alshahrani, H., Khan, A., Rizwan, M., Reshan, M. S. A., Sulaiman, A., & Shaikh, A. (2023). Intrusion Detection Framework for Industrial Internet of Things Using Software Defined Network. Sustainability, 15(11), 9001. https://doi.org/10.3390/su15119001

Alterazi, H. A., Kshirsagar, P. R., Manoharan, H., Selvarajan, S., Alhebaishi, N., Srivastava, G., & Lin, J. C.-W. (2022). Prevention of Cyber Security with the Internet of Things Using Particle Swarm Optimization. Sensors, 22(16), 6117. https://doi.org/10.3390/s22166117

Bankó, M. B., Dyszewski, S., Králová, M., Limpek, M. B., Papaioannou, M., Choudhary, G., & Dragoni, N. (2025). Advancements in Machine Learning-Based Intrusion Detection in IoT: Research Trends and Challenges. Algorithms, 18(4), 209. https://doi.org/10.3390/a18040209

Dey, A. K., Gupta, G. P., & Sahu, S. P. (2023). Hybrid Meta-Heuristic based Feature Selection Mechanism for Cyber-Attack Detection in IoT-enabled Networks. Procedia Comput. Sci., 218, 318–327. https://doi.org/10.1016/j.procs.2023.01.014

Dwivedi, S., Vardhan, M., & Tripathi, S. (2020). Defense against distributed DoS attack detection by using intelligent evolutionary algorithm. Int. J. Comput. Appl. Retrieved from https://www.tandfonline.com/doi/full/10.1080/1206212X.2020.1720951

Faber, K., Pietron, M., & Zurek, D. (2021). Ensemble Neuroevolution-Based Approach for Multivariate Time Series Anomaly Detection. Entropy, 23(11), 1466. https://doi.org/10.3390/e23111466

Fang, Y., Yao, Y., Lin, X., Wang, J., & Zhai, H. (2024). A feature selection based on genetic algorithm for intrusion detection of industrial control systems. Computers & Security, 139, 103675. https://doi.org/10.1016/j.cose.2023.103675

Francis, G. T., Souri, A., & İnanç, N. (2024). A hybrid intrusion detection approach based on message queuing telemetry transport (MQTT) protocol in industrial internet of things. Trans. Emerging Telecommun. Technol., 35(9). https://doi.org/10.1002/ett.5030

Gueriani, A., Kheddar, H., & Mazari, A. C. (2024). Deep Reinforcement Learning for Intrusion Detection in IoT: A Survey. arXiv, 2405.20038. Retrieved from https://arxiv.org/abs/2405.20038v1

Huang, J.-C., Zeng, G.-Q., Geng, G.-G., Weng, J., & Lu, K.-D. (2023). SOPA-GA-CNN: Synchronous optimisation of parameters and architectures by genetic algorithms with convolutional neural network blocks for securing Industrial Internet-of-Things. IET Cyber-Syst. Robot., 5(1), e12085. https://doi.org/10.1049/csy2.12085

Kasongo, S. M. (2021). An Advanced Intrusion Detection System for IIoT Based on GA and Tree Based Algorithms. IEEE Access, 9, 113199–113212. https://doi.org/10.1109/ACCESS.2021.3104113

Leon, M., Markovic, T., & Punnekkat, S. (2022). Feature encoding with autoencoder and differential evolution for network intrusion detection using machine learning. ACM Conferences. Association for Computing Machinery. https://doi.org/10.1145/3520304.3534009

Lezzi, M., Corallo, A., Lazoi, M., & Nimis, A. (2025). Measuring cyber resilience in industrial IoT: a systematic literature review. Manag. Rev. Q., 1–55. https://doi.org/10.1007/s11301-025-00495-8

Lu, K.-D., Zeng, G.-Q., Luo, X., Weng, J., Luo, W., & Wu, Y. (2021). Evolutionary Deep Belief Network for Cyber-Attack Detection in Industrial Automation and Control System. IEEE Trans. Ind. Inf., 17(11), 7618–7627. https://doi.org/10.1109/TII.2021.3053304

Martínez, A. (2023). Diseño de una solución basada en SDN para la microsegmentación de servicios IoT. Universitat Politècnica de València. http://hdl.handle.net/10251/196462

Prasad, K. S., Lydia, E. L., Rajesh, M. V., Radhika, K., Ramesh, J. V. N., Neelima, N., & Pokuri, S. R. (2024). Augmenting cybersecurity through attention based stacked autoencoder with optimization algorithm for detection and mitigation of attacks on IoT assisted networks. Sci. Rep., 14(1), 1–23. https://doi.org/10.1038/s41598-024-81162-y

Saheed, Y. K., Abdulganiyu, O. H., & Tchakoucht, T. A. (2024). Modified genetic algorithm and fine-tuned long short-term memory network for intrusion detection in the internet of things networks with edge capabilities. Appl. Soft Comput., 155, 111434. https://doi.org/10.1016/j.asoc.2024.111434

Thakkar, A., & Lohiya, R. (2020). Role of swarm and evolutionary algorithms for intrusion detection system: A survey. Swarm Evol. Comput., 53, 100631. https://doi.org/10.1016/j.swevo.2019.100631

Talpur, F., Korejo, I. A., Chandio, A. A., Ghulam, A., & Talpur, Mir. S. H. (2024). ML-Based Detection of DDoS Attacks Using Evolutionary Algorithms Optimization. Sensors, 24(5), 1672. https://doi.org/10.3390/s24051672

Zhang, L., Jiang, S., Shen, X., Gupta, B. B., & Tian, Z. (2021). PWG-IDS: An Intrusion Detection Model for Solving Class Imbalance in IIoT Networks Using Generative Adversarial Networks. arXiv, 2110.03445. Retrieved from https://arxiv.org/abs/2110.03445v1