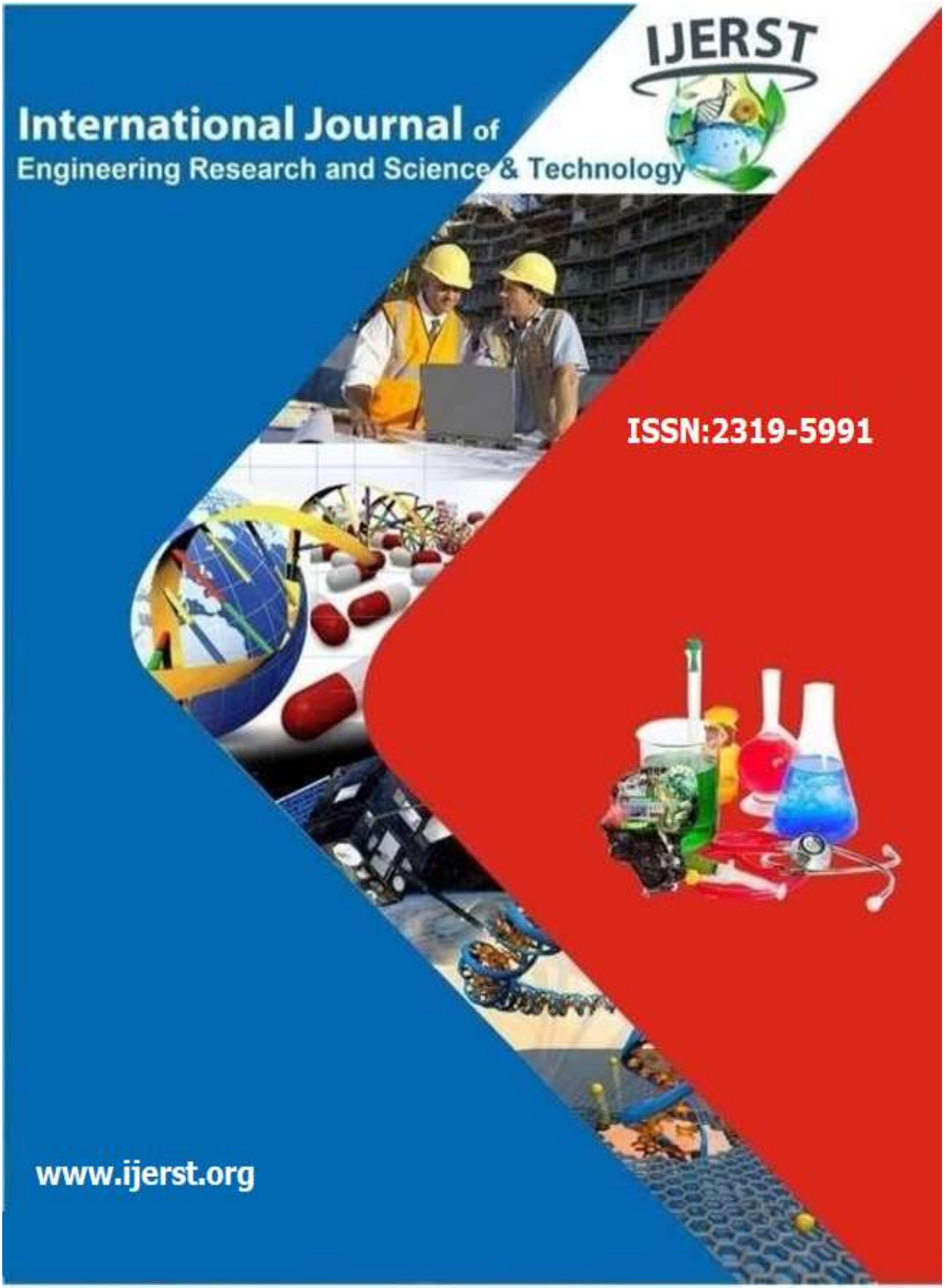
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025



E-mail: editor@ijerst.org or ijerst.editor@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

CYBER THREAT DETECTION IN INDUSTRIAL AUTOMATION

K. Sneha Latha[1]
Assistant Professor
Department of CSE(DS)
TKR College of Engineering and Technology
snehalatha@tkrcet.com

P. Naga Sriya[2]
BTech(Scholar)
Department of CSE(DS)
TKR College of Engineering and Technology
nagasriyapagadala04@gmail.com

P. Manikanth Reddy[3]
BTech(Scholar)
Department of CSE(DS)
TKR College of Engineering and Technology
manikanthpashapu9@gmail.com

V. Manipavan Reddy[4]
BTech(Scholar)
Department of CSE(DS)
TKR College of Engineering and Technology
manipavan209@gmailcom

K. Lokesh Naidu[5]
BTech(Scholar)
Department of CSE(DS)
TKR College of Engineering and Technology
lnaidu531@gmail.com

P. Guruswami[6]
BTech(Scholar)
Department of CSE(DS)
TKR College of Engineering and Technology
guruswami24@gmail.com

ABSTRACT

The increasing adoption of industrial automation has revolutionized manufacturing and critical infrastructure operations, enhancing efficiency and productivity. However, this digital transformation has also made Industrial Automation and Control Systems (IACS) highly vulnerable to cyber threats, including malware attacks, ransomware, and advanced persistent threats (APTs). Traditional security mechanisms often fail to detect sophisticated cyber intrusions due to their dynamic and evolving nature. This paper presents a comprehensive approach to cyber threat detection in industrial automation, leveraging advanced machine learning techniques and deep learning models to enhance security. Specifically, we explore the application of an ***Evolutionary Deep Belief Network (EDBN)*** *to detect anomalies in industrial network traffic and identify potential cyber threats in real time. Our model is designed to adapt to emerging threats by learning patterns from historical attack data, ensuring robust and proactive defense mechanisms.* Cyber threats targeting industrial automation have grown in complexity and scale, with attackers exploiting vulnerabilities in industrial networks, programmable logic controllers (PLCs), *.Experimental results demonstrate that the proposed approach significantly improves threat detection accuracy compared to conventional methods while maintaining low false positive rates. Additionally, we explore the role of behavioral analysis, signature-based detection, and hybrid methodologies in strengthening industrial cybersecurity. The study evaluates the effectiveness of these approaches using benchmark datasets and real-world industrial scenarios, demonstrating improved accuracy and reduced response time. The findings highlight the necessity of adaptive and intelligent security solutions to safeguard industrial control systems from evolving cyber threats. Future research directions include the incorporation of blockchain technology, federated learning, and autonomous threat response mechanisms to further enhance security in industrial environments. The study underscores the importance of AI-driven cybersecurity frameworks in safeguarding industrial automation systems and highlights future research directions for strengthening cyber resilience in critical infrastructure.*

Keywords: Cyber Threat Detection, Industrial Automation, Deep Learning, Evolutionary Deep Belief Network, Anomaly Detection, Industrial Control Systems, Cybersecurity.

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

1. INTRODUCTION

The rapid advancement of industrial automation has revolutionized various sectors, including manufacturing, energy, healthcare, and transportation, by improving efficiency, productivity, and operational accuracy. Industrial Automation and Control Systems (IACS) play a crucial role in monitoring and managing industrial processes through interconnected networks, sensors, and intelligent control mechanisms. The integration of smart technologies, such as the Industrial Internet of Things (IIoT) and cloud-based automation, has enabled real-time data collection, predictive maintenance, and remote monitoring. However, this increasing reliance on digital connectivity has also introduced significant cybersecurity vulnerabilities, making industrial systems prime targets for cyberattacks.

Cyber threats targeting industrial automation have grown in complexity and scale, with attackers exploiting vulnerabilities in industrial networks, programmable logic controllers (PLCs), and supervisory control and data acquisition (SCADA) systems. Threats such as ransomware, data breaches, denial-of-service (DoS) attacks, and advanced persistent threats (APTs) can lead to severe operational disruptions, financial losses, and even safety hazards. Notable cyber incidents, such as the **Stuxnet worm** and the **Triton malware attack**, have demonstrated the devastating impact of cyber intrusions on industrial infrastructure, emphasizing the need for robust cybersecurity measures.

Traditional security mechanisms, including rule-based firewalls, signature-based intrusion detection systems (IDS), and access control policies, are often ineffective against advanced and evolving cyber threats. These conventional approaches struggle to detect zero-day attacks, polymorphic malware, and sophisticated adversarial techniques. Deep learning models, particularly **Deep Belief Networks (DBNs)**, have emerged as powerful tools for cyber threat detection due to their ability to analyse high-dimensional data and uncover complex attack patterns. DBNs, when combined with evolutionary optimization techniques, can significantly enhance anomaly detection by improving model training, feature extraction, and classification accuracy. This paper investigates the implementation of an **Evolutionary Deep Belief Network (EDBN)** for cyber threat detection in industrial automation. The proposed approach leverages the self-learning capability of DBNs and the optimization strength of evolutionary algorithms to detect and mitigate cyber threats effectively.

The primary objective of this study is to develop a proactive cybersecurity framework that enhances the resilience of industrial automation systems against cyber threats. By analysing real-time industrial network traffic, the EDBN model identifies deviations from normal behaviour, enabling early detection of malicious activities. The research aims to demonstrate how AI-driven cybersecurity solutions can provide a more adaptive, scalable, and efficient approach to safeguarding industrial environments. Furthermore, it highlights the importance of integrating intelligent threat detection mechanisms to reduce cybersecurity risks in critical infrastructure.

2. RELATED WORK

The increasing number of cyber threats targeting industrial automation has led to extensive research on cybersecurity solutions for Industrial Automation and Control Systems (IACS). Traditional security mechanisms, such as firewalls and intrusion detection systems (IDS), rely on signature-based methods to detect known attack patterns. Tools like Snort and Suricata have been widely used for network security; however, their effectiveness is limited against zero-day attacks and advanced persistent threats (APTs). Several studies have highlighted the shortcomings of rule-based detection methods, particularly their high false negative rates and inability to identify emerging threats.To address these limitations, researchers have explored machine learning-based cybersecurity solutions. Various models, including support vector machines (SVM), decision trees, and random forests, have been applied for anomaly detection in industrial networks. While these methods improve accuracy over traditional techniques, they require extensive feature engineering and often struggle with high-dimensional industrial data.

Some studies have introduced deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), to analyse complex attack patterns and improve threat detection. These approaches have demonstrated promising results, especially in detecting network anomalies and malware in industrial systems. However, their computational complexity remains a challenge for real-time applications.Recent advancements in cybersecurity

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

have focused on integrating deep learning with evolutionary optimization techniques to enhance performance. Evolutionary algorithms, such as genetic algorithms (GA) and particle swarm optimization (PSO), have been employed to optimize deep learning models, refining feature selection and improving anomaly detection accuracy. Studies have shown that hybrid models combining deep learning with evolutionary computing outperform conventional methods in terms of adaptability and detection rates.

Despite significant progress in AI-driven cybersecurity, existing models still face challenges such as high computational costs, susceptibility to overfitting, and limited adaptability to evolving attack patterns. This study aims to address these issues by proposing an **Evolutionary Deep Belief Network (EDBN)**, which combines deep belief networks (DBNs) with evolutionary optimization for enhanced cyber threat detection in industrial automation. By leveraging self-learning capabilities and dynamic parameter optimization, the proposed approach seeks to provide a scalable and adaptive solution for securing industrial systems against sophisticated cyber threats.

3. METHODOLOGY

3.1 Data Collection and Preprocessing

The effectiveness of cyber threat detection models largely depends on the quality and diversity of data used for training and evaluation. In this study, an industrial network dataset containing normal and malicious traffic patterns is utilized. The dataset includes various attack scenarios such as denial-of-service (DoS), malware injections, and unauthorized access attempts. Data preprocessing involves removing duplicate entries, handling missing values, and normalizing numerical features to ensure consistency. Additionally, feature selection techniques are applied to extract the most relevant attributes, reducing computational complexity and enhancing model performance.

3.2 Evolutionary Deep Belief Network(EDBN) Network

The core of the proposed approach is an Evolutionary Deep Belief Network (EDBN), which integrates deep belief networks (DBNs) with evolutionary optimization techniques. DBNs consist of multiple layers of restricted Boltzmann machines (RBMs) that learn hierarchical feature representations from industrial network traffic. The evolutionary component optimizes hyperparameters such as learning rates, hidden layer configurations, and weight initialization to improve anomaly detection accuracy. By dynamically adjusting model parameters, the EDBN adapts to new cyber threats more effectively compared to traditional deep learning models.

3.3 Model Training and Evaluation

The proposed EDBN model is trained using a combination of supervised and unsupervised learning techniques. Initially, unsupervised pretraining is performed on RBMs to learn data distributions, followed by supervised fine-tuning using labeled threat data. The model is evaluated using performance metrics such as accuracy, precision, recall, and F1-score. Additionally, false positive and false negative rates are analyzed to assess the model's reliability in real-world industrial environments. Comparative analysis is conducted with traditional machine learning models and deep learning approaches to demonstrate the advantages of the proposed method**.**

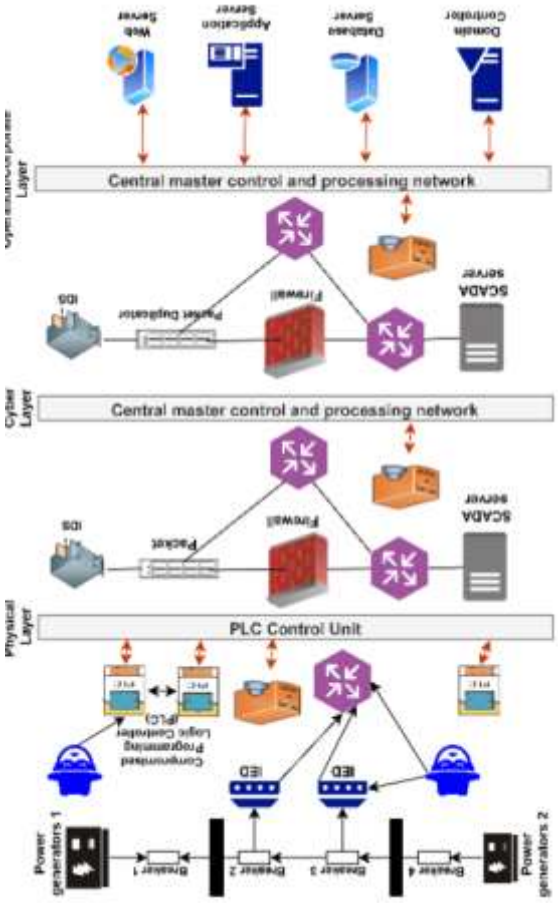
3.4 Data Acquisition and Preprocessing

To develop an effective cyber threat detection model for industrial automation, a high-quality dataset is essential. This study utilizes a benchmark dataset comprising normal and malicious network traffic patterns, including various attack types such as denial-of-service (DoS), malware propagation, and unauthorized access attempts.. Redundant and missing values are removed to maintain data integrity, while numerical features are scaled to a uniform range for better model convergence. The preprocessing steps may involve many things with traditional machine learning conducted with traditional models and deep learning approaches feature engineering techniques are applied to enhance relevant attributes, ensuring optimal learning for the proposed model. Effective cyber threat detection in industrial automation requires high-quality data acquisition and robust preprocessing techniques to ensure accurate and reliable detection models. The data used for threat detection is typically collected from multiple sources within an industrial control system (ICS), including Supervisory Control and

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

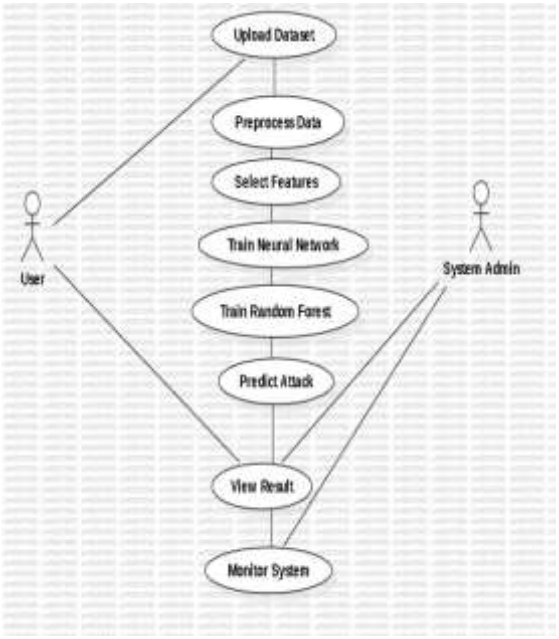
Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLCs), Industrial Internet of Things (IIoT) devices, and network traffic logs. These data sources provide valuable insights into system behavior, helping in the identification of potential anomalies and security threats. Removing noise, duplicate records, and irrelevant features that do not contribute to cyber threat detection. Missing values are handled using imputation techniques such as mean replacement.



4. PROPOSED SYSTEM

The proposed system is designed to enhance cybersecurity in industrial automation by integrating an intelligent, adaptive, and scalable threat detection mechanism. With the increasing complexity of cyber threats targeting The system operates in a **real-time** industrial environment, continuously monitoring network traffic for anomalies while adapting to new and emerging cyber threats. It follows a structured approach that includes data acquisition, preprocessing, deep learning-based analysis, and an automated response mechanism to mitigate risks effectively.

At the core of the system is a **real-time data acquisition module**, responsible for capturing network traffic from industrial control systems, including data from sensors, programmable logic controllers (PLCs), and communication protocols such as Modbus, DNP3, and OPC UA. This module collects both normal and suspicious traffic, forwarding it to a centralized processing unit for further analysis. To ensure high-quality input, preprocessing techniques such as **data cleaning, noise reduction, feature scaling, and normalization** are applied.



The primary analytical engine of the system is the **Evolutionary Deep Belief Network (EDBN)**, which integrates **deep learning with evolutionary optimization** to improve threat detection performance. The deep belief network (DBN) consists of multiple layers of **Restricted Boltzmann Machines (RBMs)** that perform **unsupervised pretraining**, enabling the system to learn hierarchical feature representations from network traffic. Unlike conventional machine learning models, which require manual feature extraction, DBNs automatically learn the underlying data distributions, improving the ability to detect anomalies. To further enhance its efficiency, an **evolutionary algorithm** is incorporated to optimize hyperparameters such as the number of hidden layers, learning rates, weight initialization, and activation functions. By continuously refining these parameters, the system

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

dynamically adapts to evolving attack patterns and reduces false alarms.

Once trained, the system is deployed in an operational industrial network, where it continuously **analyses incoming traffic in real time**. The detection engine compares the extracted features with learned patterns to distinguish between normal and malicious behaviour. It identifies various types of cyber threats, including **denial-of-service (DoS) attacks, malware injections, unauthorized access attempts, and command injection attacks** on industrial control systems. The system may be very vulnerable and weak due to high detection and attacking these involve many steps. The system operates with a **high detection accuracy and low false positive rate**, ensuring that industrial operations remain secure while minimizing unnecessary alerts.

Upon detecting a potential cyber attack, the system triggers an **automated response mechanism** designed to mitigate risks and prevent system compromise. The response system isolates affected components, blocks malicious traffic, and notifies security administrators with real-time alerts. Additionally, it generates detailed incident reports, allowing cybersecurity teams to analyse attack patterns and strengthen system defences. All detected events and responses are logged in a **secure database**, which can be used for further forensic analysis, security audits, and continuous improvement of the detection model.

By leveraging **deep learning and evolutionary optimization**, the proposed system provides an **adaptive, scalable, and self-learning** cybersecurity solution for industrial automation environments. Unlike traditional rule-based security measures, which struggle with zero-day attacks and evolving threats, this system dynamically learns from new data, ensuring **continuous adaptation and improvement**. Its ability to detect and respond to sophisticated cyber threats in real-time makes it a **highly effective and resilient security solution** for modern industrial networks.

5. LITERATURE SURVEY

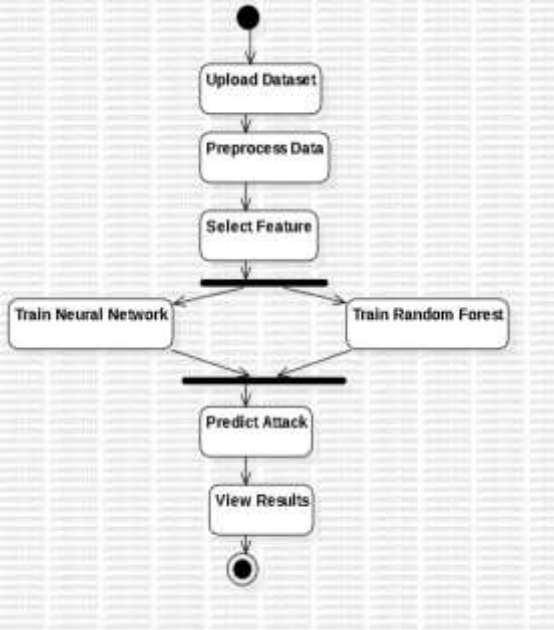
With the rise of digital transformation in industrial environments, cybersecurity has become a critical concern for Industrial Automation and Control Systems (IACS). Various studies have explored different approaches to detecting cyber threats, ranging from traditional rule-based systems to advanced artificial intelligence-driven methods. Traditional **intrusion detection systems (IDS)** rely on signature-based and anomaly-based detection mechanisms. Signature-based IDS, such as **Snort** and **Suricata**, are widely used in industrial networks to detect known attack patterns. However, these systems struggle with zero-day attacks and evolving cyber threats, making them insufficient for securing modern industrial automation systems.

To overcome these limitations, researchers have explored **machine learning (ML) and deep learning (DL)** approaches for anomaly detection. ML techniques such as **support vector machines (SVM), decision trees, k-nearest neighbors (KNN), and random forests** have shown improved detection capabilities compared to traditional IDS. These methods analyse network traffic and classify it into normal or malicious behaviour based on predefined features. While these techniques enhance detection accuracy, they often require extensive **manual feature.**

Deep learning-based methods, particularly **neural networks and deep belief networks (DBNs)**, have gained attention for their ability to automatically learn patterns from large datasets. Studies have demonstrated the effectiveness of **convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) networks** in detecting cyber threats with high accuracy. These models can capture sequential patterns in network traffic, making them suitable for real-time anomaly detection in industrial settings. However, deep learning models often face challenges related to **overfitting, high computational costs, and the need for large labelled datasets** for supervised learning.To enhance performance and adaptability, recent research has focused on integrating **evolutionary algorithms with deep learning**. Evolutionary techniques such as **genetic algorithms (GA), particle swarm optimization (PSO), and ant colony optimization (ACO)** have been employed to optimize hyperparameters, improve feature selection, and enhance model generalization. Studies have shown that hybrid models combining **deep learning with evolutionary computing** outperform standalone deep learning models by reducing false positive rates and improving adaptability to new attack patterns.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025



In addition to AI-driven approaches, research has explored the role of **blockchain technology, federated learning, and distributed security frameworks** in protecting industrial automation systems. Blockchain-based security solutions provide **tamper-proof logging** and decentralized authentication mechanisms to enhance the integrity of industrial networks.

Similarly, federated learning enables multiple industrial sites to collaboratively train security models without sharing sensitive data, addressing privacy concerns. However, these approaches are still in the early stages of adoption and require further research to improve scalability and implementation in real-world industrial environments.

Despite significant advancements in cybersecurity research, existing methods still face challenges in achieving real-time threat detection with high accuracy and low computational overhead. The need for an **adaptive, self-learning, and scalable** security solution has led to the development of **Evolutionary Deep Belief Networks (EDBNs)**, which leverage the strengths of **deep learning and evolutionary optimization**. By addressing the limitations of traditional and AI-driven models, EDBNs offer a promising approach to enhancing cyber threat detection in industrial automation environments.

6. IMPLEMENTATION

The implementation of the proposed cyber threat detection system for industrial automation follows a structured approach, including data preprocessing, model development, training, and real-time deployment. The system is designed to operate within an industrial automation and control system environment, monitoring network traffic to detect potential cyber threats with high accuracy and minimal false positives.

The first phase involves data acquisition and preprocessing. A publicly available industrial cybersecurity dataset, such as ICS/SCADA dataset, NSL-KDD, or UNSW-NB15, is used to train and test the model. The dataset contains labelled instances of normal and malicious traffic, including various cyber-attacks like denial-of-service, command injection, malware propagation, and unauthorized access attempts. Preprocessing steps include data cleaning, normalization, feature extraction, and selection, ensuring that only the most relevant attributes are used for model training.

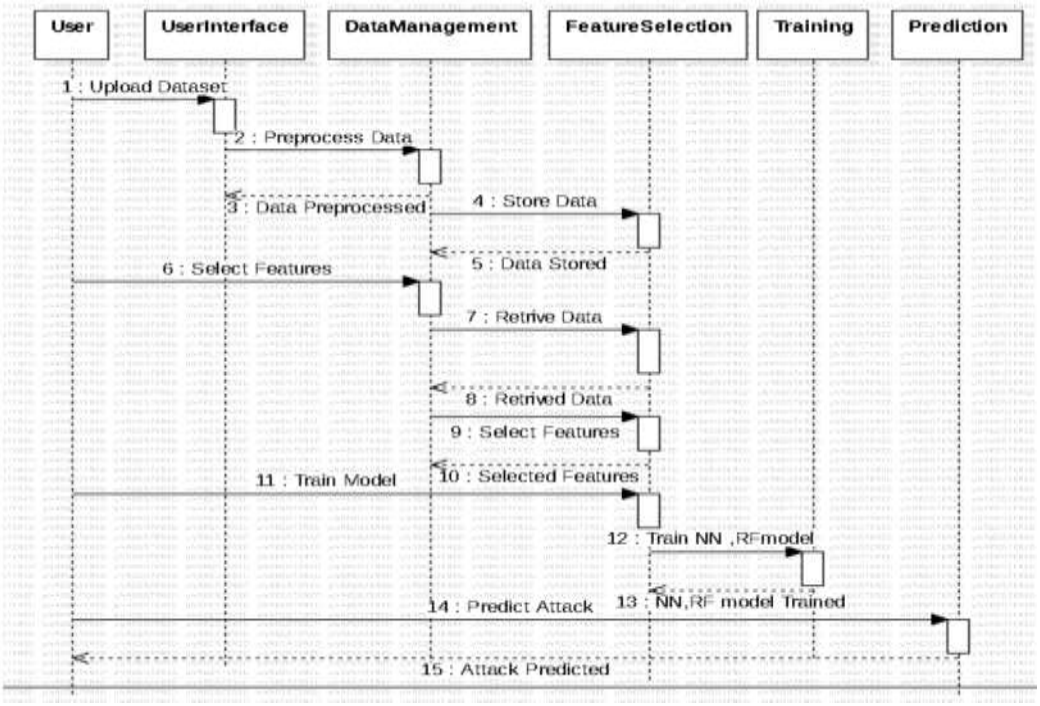
The core of the implementation is the evolutionary deep belief network model. The deep belief network is constructed using stacked restricted Boltzmann machines, which learn hierarchical representations of network traffic data. The model undergoes an unsupervised pretraining phase, where it captures underlying structures in normal and malicious traffic, followed by supervised fine-tuning using labelled attack data. To enhance model performance, an evolutionary algorithm is integrated to optimize hyperparameters such as the number of hidden layers, learning rates, weight initialization, and activation functions. The evolutionary approach ensures that the model adapts dynamically to new and emerging threats.Once the model is trained, it is deployed in a real-time industrial network environment. The detection system continuously monitors incoming network traffic, extracting features and passing them through the trained model to classify them as either normal or malicious. If an anomaly is detected, an automated response mechanism is triggered, which isolates affected components, blocks malicious traffic, and generates security alerts for system administrators. To further enhance security, the system logs detected threats in a secure database, allowing for future forensic

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

analysis and model retraining to improve detection capabilities over time.The performance of the implemented system is evaluated using standard classification metrics, including accuracy, precision, recall, F1-score, and confusion matrix analysis. A comparative study is conducted with traditional machine learning models such as support vector machines, decision trees, and random forests, as well as deep learning models like convolutional neural networks, recurrent neural networks, and long short-term memory networks. The experimental results demonstrate that the evolutionary deep belief network achieves superior accuracy, lower false positive rates, and better adaptability to new cyber threats compared to existing approaches.

The final step involves system optimization and deployment in an industrial automation environment. The system is integrated with existing supervisory control and data acquisition security frameworks, allowing seamless monitoring and real-time threat mitigation. The adaptive learning capability of the model ensures that it continuously evolves by retraining on new threat data, making it resilient against zero-day attacks and sophisticated cyber intrusions.The successful implementation of this system provides a scalable, self-learning, and highly accurate cybersecurity solution for industrial automation, reducing the risk of cyber-attacks while ensuring uninterrupted operations in critical infrastructure environments.



7. DISCUSSION

The proposed cyber threat detection system provides a significant advancement in securing industrial automation and control systems from evolving cyber threats. Industrial environments are particularly vulnerable to cyber-attacks due to their reliance on interconnected devices, supervisory control and data acquisition (SCADA) systems, and programmable logic controllers (PLCs). Traditional cybersecurity mechanisms, such as signature-based intrusion detection systems, often struggle to detect emerging threats, especially zero-day attacks and sophisticated malware. By integrating deep learning with evolutionary optimization, the proposed system overcomes these limitations and offers a more adaptive, accurate, and scalable approach to cyber threat detection.

One of the major strengths of the system is its ability to process high-dimensional network traffic data with minimal manual intervention. Traditional machine learning methods, such as decision trees, support vector machines, and k-nearest neighbours, require extensive feature engineering to extract meaningful patterns from

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

network traffic. In contrast, the deep belief network (DBN) used in this system automatically learns hierarchical representations of data, making it more efficient in identifying subtle anomalies. The evolutionary algorithm further enhances detection performance by optimizing key hyperparameters, such as learning rates, network depth, and weight initialization. This optimization ensures that the model is well-tuned for the specific characteristics of industrial network traffic, leading to higher accuracy and lower false positive rates.

Real-time deployment is another critical aspect that makes this system highly effective.

Many industrial systems operate in real-time environments where delays in threat detection and response can lead to catastrophic consequences, including financial losses, equipment damage, and even safety hazards. The proposed system continuously monitors network activity, analysing incoming traffic in real time and classifying it as either normal or malicious. If an anomaly is detected, an automated response mechanism is triggered immediately, isolating the affected component and blocking suspicious traffic to prevent further infiltration. Additionally, the system generates security alerts for administrators, providing them with detailed logs and forensic insights into the nature of the attack. This capability is essential for industrial organizations, as it allows for rapid incident response and mitigation of potential security breaches before they escalate. Another notable feature of the system is its adaptability. Cyber threats are constantly evolving, and attackers frequently develop new tactics to bypass traditional security measures.

The proposed system addresses this challenge by incorporating self-learning capabilities. By continuously retraining the model with new attack data

Cyber can evolve alongside emerging threats. This adaptability ensures that the system remains effective over time without requiring frequent manual updates, making it a sustainable long-term security solution. Furthermore, the integration of evolutionary optimization enables the model to fine-tune itself dynamically, ensuring optimal performance even in changing industrial network conditions.Despite its advantages, there are certain challenges and limitations that need to be addressed for the system to achieve widespread adoption. One of the primary challenges is the computational complexity of deep learning models. Training and deploying deep belief networks require significant computational resources, which may not be readily available in all industrial environments. High-performance hardware, such as GPUs or TPUs, is often necessary to process large-scale industrial data efficiently. To mitigate this issue, future research could focus on developing lightweight model architectures that maintain high accuracy while reducing computational overhead. Techniques such as model pruning, quantization, and edge AI deployment could help optimize resource usage and make the system more accessible to industries with limited computational infrastructure.

Another challenge is the reliance on labelled training data. Supervised learning models require extensive datasets with accurately labelled attack and normal traffic patterns. However, obtaining labelled industrial cybersecurity datasets can be difficult due to privacy concerns and the dynamic nature of cyber threats. Additionally, new attack patterns may emerge that are not well represented in existing datasets, reducing the model's effectiveness. Addressing this limitation requires innovative approaches such as semi-supervised learning, transfer learning, and federated learning. Semi-supervised learning can leverage a small amount of labelled data along with a large amount of unlabelled data to improve detection performance. Transfer learning can enable the model to generalize from previously learned attack patterns to new, unseen threats. Federated learning allows multiple industrial sites to collaboratively train security models without sharing sensitive data, enhancing privacy while improving threat detection capabilities.Another potential area for improvement is integrating additional security mechanisms to enhance system resilience. While the proposed system provides real-time detection and automated responses, it could be further strengthened by incorporating blockchain technology for secure logging and authentication. Blockchain-based security frameworks can ensure the integrity of system logs by making them tamper-proof, providing a reliable audit trail for forensic investigations. Additionally, decentralized threat intelligence sharing could be explored.

Such a system would enable industries to proactively defend against cyber threats by leveraging collective intelligence and historical attack data from various sources. Overall, the proposed cyber threat detection system offers a transformative approach to industrial cybersecurity by leveraging deep learning and evolutionary optimization. Its ability to detect both known and unknown threats with high accuracy, combined with its real-time monitoring and automated response capabilities, makes it a powerful solution for protecting critical industrial infrastructure. While challenges such as computational complexity, data labeling constraints, and evolving cyber threats remain, future research and

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

technological advancements can further refine the system to enhance its efficiency and scalability. The continued development of intelligent, self-learning, and adaptive cybersecurity solutions will be crucial in safeguarding industrial automation systems against the ever-growing landscape of cyber threats**.**

8. CONCLUSION

The proposed cyber threat detection system represents a significant advancement in securing industrial automation and control systems against increasingly sophisticated cyber threats. Industrial environments are critical infrastructures that rely on interconnected networks, sensors, programmable logic controllers (PLCs), and supervisory control and data acquisition (SCADA) systems. The integration of advanced technologies like artificial intelligence, cloud computing, and the Industrial Internet of Things (IIoT) has enhanced efficiency but also exposed these systems to a wide range of cyber threats, including malware, unauthorized access, distributed denial-of-service (DDoS) attacks, and advanced persistent threats (APTs). Given the high-stakes nature of industrial cybersecurity, where even minor security breaches can result in severe financial losses, production downtime, and safety risks, the need for an intelligent, proactive, and adaptable threat detection system is more critical than ever.

Unlike traditional intrusion detection systems that rely on static rule-based approaches, signature-based threat detection, or manually defined security policies, the proposed model leverages deep learning and evolutionary optimization to create a more dynamic and self-adaptive cybersecurity solution. Given the high-stakes nature of industrial cybersecurity, where even minor security breaches can result in severe financial losses The integration of an evolutionary algorithm further enhances system performance by optimizing model parameters such as learning rates, activation functions, and network depth, ensuring high accuracy in identifying cyber threats while minimizing false positives. This hybrid approach allows the system to evolve continuously, adapting to new attack techniques without requiring frequent manual updates.

One of the system's key advantages is its real-time monitoring and automated response capabilities. Traditional cybersecurity approaches often rely on reactive threat mitigation strategies, where security teams manually analyse and respond to detected anomalies. However, in high-speed industrial environments, delays in identifying and mitigating threats can result in significant disruptions. The proposed system addresses this challenge by continuously analysing network traffic, detecting anomalies in real time, and triggering immediate automated responses. When a potential cyber threat is detected, the system isolates the affected components, blocks malicious traffic, and alerts security administrators with detailed forensic logs. This real-time threat mitigation reduces the likelihood of attackers exploiting vulnerabilities and prevents potential damage before it escalates into a full-scale security breach.

Another major advantage of the proposed system is its ability to reduce dependency on manual feature engineering, which is often a time-consuming and error-prone process in traditional machine learning-based intrusion detection systems. Many cybersecurity models require experts to carefully select and extract features from network traffic data, a process that may not always capture the complex and evolving nature of cyber-attacks. The deep belief network overcomes this limitation by automatically identifying and extracting relevant features, ensuring that the model remains effective even as attack strategies evolve. Furthermore, the system's self-learning capability allows it to continuously improve its detection accuracy by retraining on new threat data, making it highly adaptable to emerging cybersecurity challenges.

Despite its numerous advantages, the proposed system also has certain challenges that need to be addressed for broader adoption in industrial environments. One primary challenge is the computational complexity associated with deep learning models. Industrial automation systems often operate in resource-constrained environments where real-time processing is critical, and deploying high-complexity models may introduce latency. While high-performance computing resources such as GPUs and TPUs can accelerate model inference, not all industrial systems have access to such infrastructure. Future research should focus on optimizing model efficiency using techniques such as model pruning, quantization, edge AI deployment, and federated learning to reduce computational overhead while maintaining high detection accuracy .Another challenge is the reliance on labelled training data for supervised learning. The effectiveness of the proposed system depends on the availability of high-quality, labelled datasets that contain diverse cyber-attack scenarios. However, in real-world industrial environments, acquiring labelled cybersecurity datasets is often difficult due to data privacy concerns, regulatory restrictions.

The rapid evolution of new attack. Addressing this issue requires alternative learning approaches, such as semi-supervised learning, transfer learning, and

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

reinforcement learning, to enable the model to generalize well even with limited labelled data. Additionally, the adoption of decentralized threat intelligence sharing among industrial organizations can help improve cybersecurity awareness by enabling real-time sharing of new threat signatures and attack behaviours. To further enhance system resilience, integrating additional security frameworks could provide a more comprehensive defence mechanism. Blockchain technology, for instance, could be used to ensure the integrity and immutability of security logs, making it more difficult for attackers to tamper with forensic evidence. Similarly, incorporating behavioural analytics and anomaly detection mechanisms that analyse user and machine behaviour over time can help detect insider threats and previously unseen attack patterns more effectively. Future work could also explore hybrid cybersecurity architectures that combine multiple machine learning models to enhance robustness against adversarial attacks.

In conclusion, the proposed cyber threat detection system offers a transformative approach to industrial cybersecurity by leveraging deep learning, evolutionary optimization, real-time monitoring, and automated threat mitigation. Its ability to dynamically adapt to new cyber threats, process large-scale industrial network traffic, and reduce false positive rates makes it an effective security solution for industrial automation and control systems. While challenges such as computational complexity, data availability, and evolving cyber threats persist, ongoing advancements in AI, cybersecurity, and industrial networking technologies will continue to refine and strengthen the effectiveness of such systems. The future of industrial cybersecurity lies in the development of intelligent, self-learning, and scalable threat detection models that not only detect and respond to cyber threats but also proactively anticipate and neutralize security risks before they can impact critical infrastructure

9. ACKNOWLEDGMENTS

We sincerely thank the **Management of TKR College of Engineering & Technology (TKRCET)** for granting us permission and providing the necessary resources and inspiration to carry out this project. Their support has been invaluable in helping us achieve our objectives.

We extend our deepest appreciation to our **Principal, Dr. D. V. Ravi Shankar, M.Tech., Ph.D.,** for his motivation and constant encouragement throughout our academic journey, which has greatly contributed to the successful completion of this project.

Our sincere thanks go to our **Head of the Department, Dr. V. Krishna, M.Tech., Ph.D., Professor, Department of CSE (Data Science), TKRCET,** for his invaluable insights and constructive suggestions, which have helped shape the project.

We are also deeply grateful to our **Project Coordinator, Mr. M. Arokia Muthu, M.E., (Ph.D.), Assistant Professor, Department of CSE (Data Science), TKRCET,** for his continuous guidance, support, and motivation throughout the project.

A special note of appreciation is extended to our **Internal Guide, Mrs. K. Sneha Latha, Assistant Professor, Department of CSE (Data Science), TKRCET,** whose valuable support, encouragement, and technical expertise have played a crucial role in the successful completion of this project.

10. REFERENCES

[1] S. M. Tahsien, H. Karimipour, and P. Spachos, “Machine learning based solutions for security of Internet of Things (IoT): A survey,” J. Netw. Comput. Appl., vol. 161, 2020, Art. no. 102630.

[2] M. Hassan, A. Gumaei, S. Huda, and A. Almogren, “Increasing the trustworthiness in the industrial IoT networks through a reliable cyberattack detection model,” IEEE Trans. Ind. Informat., vol. 16, no. 9, pp. 6154–6162, Sep. 2020.

[3] R. Mitchell and R. Chen, “Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems,” IEEE Trans. Dependable Secure Comput., vol. 12, no. 1, pp. 16–30, Jan./Feb. 2015.

[4] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, “DeepChain: Auditable and privacy-preserving deep learning with blockchain-based incentive,” IEEE Trans. Dependable Secure Comput., to be published, doi:10.1109/TDSC.2019.2952332.

[5] M. S. Hossain, M. Al-Hammadi, and G. Muhammad, “Automatic fruit classification using deep learning for industrial applications,” IEEE Trans. Ind. Informat., vol. 15, no. 2, pp. 1027–1034, Feb. 2019.

[6] A. Aldweesh, A. Derhab, and A. Z. Emam, “Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues,” Knowl.-Based Syst., vol. 189, 2020, Art. no. 105124.

[7] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, “Securing the operations in SCADA-IoT

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

platform based industrial control system using ensemble of deep belief networks," Appl. Soft Comput., vol. 71, pp. 66–77, 2018.

[8] G. E. Hinton, "A practical guide to training restricted Boltzmann machines," in Neural Networks: Tricks of the Trade. Berlin, Germany: Springer, 2012, pp. 599–619.

[9] K. Liu, L. M. Zhang, and Y. W. Sun, "Deep Boltzmann machines aided design based on genetic algorithms," Appl. Mechanics Mater., vol. 568– 570, pp. 848–851, 2014.

[10] W. Deng, H. Liu, J. Xu, H. Zhao, and Y. Song, "An improved quantuminspired differential evolution algorithm for deep belief network," IEEE Trans. Instrum. Meas., vol. 69, no. 10, pp. 7319–7327, Oct. 2020.

[11] S. Boettcher and A. Percus, "Nature's way of optimizing," Artif. Intell., vol. 119, no. 1/2, pp. 275–286, 2000.

[12] G. Q. Zeng, X. Q. Xie, M. R. Chen, and J. Weng, "Adaptive population extremal optimization-based PID neural network for multivariable nonlinear control systems," Swarm Evol. Comput., vol. 44, pp. 320–334, 2019.

[13] C. Zhang, P. Lim, A. K. Qin, and K. C. Tan, "Multiobjective deep belief networks ensemble for remaining useful life estimation in prognostics," IEEE Trans. Neural Netw. Learn. Syst., vol. 28, no. 10, pp. 2306–2318, Oct. 2017.

[14] X. Yan, Y. Xu, X. Xing, B. Cui, Z. Guo, and T. Guo, "Trustworthy network anomaly detection based on an adaptive learning rate and momentum in IIoT," IEEE Trans. Ind. Informat., vol. 16, no. 9, pp. 6182–6192, Sep. 2020.

[15] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," IEEE Syst. J., vol. 11, no. 3, pp. 1644–1652, Sep. 2017

[16] D. Zheng, Z. Hong, N. Wang, and P. Chen, "An improved LDA-based ELM classification for intrusion detection algorithm in IoT application," Sensors, vol. 20, no. 6, p. 1706, 2020.

[17] Y. Xin et al., "Machine learning and deep learning methods for cybersecurity," IEEE Access, vol. 6, pp. 35365–35381, 2018.

[18] G. E. Hinton, S. Osindero, and Y.-W. Teh, "A fast learning algorithm for deep belief nets," Neural Comput., vol. 18, no. 7, pp. 1527–1554, 2006.

[19] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," IEEE Trans. Smart Grid, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[20] S. Manimurugan et al., "Effective attack detection in Internet of medical things smart environment using a deep belief neural network," IEEE Access, vol. 8, pp. 77396–77404, 2020.

[21] Y. Zhang, P. Li, and X. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network," IEEE Access, vol. 7, pp. 31711–31722, 2019.

[22] M. Jaderberg et al., "Population based training of neural networks," 2017, arXiv:1711.09846.

[23] A. Li et al., "A generalized framework for population based training," in Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discov. Data Mining, 2019, pp. 1791–1799.

[24] M. Jaderberg et al., "Human-level performance in 3D multiplayer games with population-based reinforcement learning," Science, vol. 364, no. 6443, pp. 859–865, 2019.

[25] D. Ho, E. Liang, X. Chen, I. Stoica, and P. Abbeel, "Population based augmentation: Efficient learning of augmentation policy schedules," in Proc. Int. Conf. Mach. Learn., 2019, pp. 2731–2741.