AI-Based Cloud-Edge Collaboration for Enhanced Cybersecurity in Industrial IoT

M. Ranjini[1*]

[1]Research Analyst, National Institute of STEM Research, Coimbatore, Tamil Nadu, India.

ranjinimanickam27@gmail.com

Abstract: The rapid proliferation of Industrial Internet of Things (IIoT) systems has posed significant cybersecurity challenges, as these devices are interconnected and distributed. Conventional security controls, which tend to be fixed and centralized, do not suffice to meet the dynamic, real-time needs of IIoT environments. The proposed paper presents a novel AI-assisted Cloud-Edge Collaboration Model to improve the cybersecurity of IIoT systems by leveraging edge computing to detect threats with low latency and cloud computing to scale and perform advanced analytics and threat intelligence aggregation. The proposed model is evaluated on the TON-IoT Network Intrusion Dataset, and the key performance metrics include Detection Accuracy, False Positive Rate (FPR), False Negative Rate (FNR), Response Time, and Scalability. The Proposed Model demonstrates significant improvements, with 98.6% detection accuracy, dramatically outperforming the Existing Model, with 90.5%. Also, the FPR decreases to 3.2 (instead of 7.5), and the FNR decreases to 2.4 (instead of 6.8), indicating improved performance in identifying true threats and reducing false alarms. The Proposed Model also shows that it has significantly shortened response time, which was 10-15 seconds in the Existing Model, to 3-5 seconds and is thus able to mitigate security threats faster. In addition to that, the number of devices supported by the Proposed Model is 500 while the Existing Model only supports 50 devices. These findings show the efficiency of combining AI, cloud, and edge computing in offering scalable, accurate, and efficient cybersecurity solutions for IIoT systems.

Keywords: Industrial internet of things (IIoT); cybersecurity; artificial intelligence (AI); cloud-edge collaboration; intrusion detection; edge computing.

I. Introduction

The application of the Industrial Internet of Things (IIoT) has brought about great changes in the efficiency and productivity in industries since it brings about connectivity, analysis, and automation. However, this advancement in technology has increased the vulnerability of industries to various cyber-attacks, such as data breach and unauthorized access as well as attacks to infrastructure. The nature of IIoT is highly distributed and real-time in nature, thus making it difficult for the traditional cybersecurity methods such as firewalls and intrusion detection to work. This is because the traditional cybersecurity techniques are static, centralized, and inefficient in scaling. This makes it hard for them to deal with the complex needs of cybersecurity in IIoT environment. The innovative approach of AI-based cloud-edge collaboration framework in the current paper is aimed at increasing

ISBN: 978-81-687498-3-2

cybersecurity in IIoT environment (Santhoshkumar et al., 2025). The framework takes advantage of edge computing, cloud computing, and artificial intelligence (AI) to come up with an effective and real-time solution. The framework shall be efficient in threat management and operations due to the integration of edge AI threat detection, scalability, and cloud computing power (Hawage & Madireddy, 2025; Mani, 2024).

It is possible to ensure the distributed control of security through such cloud-edge cooperation because one can mitigate threats in real-time at the edge and then use the cloud to share this information and analyze threat data. The paper describes the potential of using the AI-based cloud-edge cooperation for increasing the level of cybersecurity in Industrial IoT. Moreover, it considers the incorporation of blockchain for increasing the level of accountability and transparency of industrial IoT systems Sengupta & Deshmukh, (2024). The suggested model is experimentally verified, and its effectiveness and efficiency are shown.

Key Contributions

1. Proposed AI-driven cloud and edge computing framework to assist real-time cybersecurity in the IIoT environment by incorporating edge computing for detecting threats in a low-latency way and cloud computing for scalability.
2. Performance measurement of the framework using performance indicators like detection accuracy, latency, and scalability to assess how efficiently the framework is working in IIoT environment.
3. AI-driven real-time threat detection and mitigation capability with the help of AI algorithms that increase the efficiency of the system compared to traditional cybersecurity systems.

In Section I, the IIoT cybersecurity threats are stated and the objectives of the proposed model are described. In Section II, the existing approaches and need for the application of AI in the process are discussed. In Section III, an explanation of the proposed architecture for the use of AI in cloud-edge collaboration is provided. In Section IV, a comparison of the performance of the proposed model and the existing approach is made. Finally, a conclusion section (Section V) is included.

II. Literature Survey

This rapid advancement of the Industrial Internet of Things (IIoT) has contributed to increased automation, efficiency, and data analysis in industry. But the increased connectivity brings about vulnerabilities to security, including the potential for hackers to gain unauthorized access and attack critical systems. The article highlights the susceptibility of IIoT systems because it is highly connected and because of their dependence on resource-constrained and inexpensive devices with little robust security protections (Zhukabayeva et al., 2025). Such difficulties are enhanced by the fact that there are no standardized security measures in the heterogeneity of devices and that the devices in IIoT networks are not uniform. Moreover, the large amount of real-time data and the necessity of constant surveillance require complex cybersecurity solutions that could not be met by traditional

ISBN: 978-81-687498-3-2

security measures that are not real-time. With the development of IoT systems, the risks of data integrity, confidentiality, and system availability are growing, and it is necessary to implement new security frameworks. AI is becoming one of the facilitators of effective cybersecurity measures to IIoT systems (Alamir et al., 2026). The use of AI-based methods enables the real-time processing of data by IIoT devices, detecting anomalies and possible threats very precisely. Machine learning (ML) and deep learning (DL) are AI methods that are increasingly used to improve threat detection and automate response activities. AI-based systems in industrial security. According to AI-driven systems in industrial security, which leverage edge AI to execute real-time anomaly detection, intrusion detection, and predictive maintenance, hence enhancing system resilience to cyber threats (Joel, 2024). Through the analysis of large datasets, the AI models can evolve over time and continuously adjust to new attack vectors and enhance their capacity to detect new threats that were previously unknown. The ability of AI to integrate with edge and cloud computing facilitates threat detection that is scalable and efficient in terms of latency, and is very advantageous as opposed to traditional security methods.

Edge and cloud computing integration are important in tackling the cybersecurity challenges in IIoT systems. Since edge computing enables real-time processing of data at the device level, it makes the processing much faster and less latency in applications where rapid decision-making is necessary (Pal, 2024). This is especially vital in industries where delays may cause operational inconveniences or accidents. Nevertheless, edge devices possess limited processing capabilities and storage, thus limiting their capability to perform complex cybersecurity functions. Cloud computing, however, presents enormous computing capabilities and scalability, which can be used to perform sophisticated data analytics, share threat intelligence, and store large volumes of data to be analyzed over time. IIoT systems can find a balanced approach between real-time threat detection and the extensive and resource-intensive security processing by integrating the benefits of edge and cloud computing. This partnership makes sure that security capabilities, including AI-based anomaly detection and incident response, can be carried out at the edge and in the cloud, which offers a unified, adaptive solution to IIoT cybersecurity (Haseeb et al., 2026). A number of solutions have been suggested to improve IIoT cybersecurity, but most of them have serious drawbacks. The conventional security mechanisms such as firewalls, intrusion detection systems (IDS) cannot be effective in identifying new cyber threats and need regular updates to be relevant. These traditional systems, as mentioned, are unable to detect in real-time and have difficulties with the sheer amount of data produced by IIoT devices (Kondori & Peashdad, 2015). The limitations have been overcome with the introduction of AI-based solutions. Nevertheless, the incorporation of AI into IIoT systems is not without its issues (Lakhan & Groenli, 2025). Training can often demand large datasets to be trained on, and sometimes it is not readily available or needs considerable computational resources, especially at the edge (Goswami, 2025). In addition, the current cloud-based solutions are usually characterized by high latency of real-time data processing which is a critical consideration in industrial settings (Zhukabayeva et al., 2025). The proposed AI-based cloud-edge collaboration suggests that these limitations can be addressed by using real-time threat detection at the edge with

ISBN: 978-81-687498-3-2

scalable analytics, which are resource-intensive, in the cloud to offer a more efficient and adaptive security solution to IIoT systems (Jonnalagadda, 2025; Ravi, 2024).

Although there has been progress on IIoT security, conventional models are still struggling to cope with the dynamism of real-time business and large-scale environments. The majority of currently existing systems are not scalable or do not offer low-latency threat detection. Moreover, the use of AI in combination with cloud and edge computing in the IIoT cybersecurity has not been thoroughly researched. This paper will fill these gaps by suggesting a single framework of real-time threat detection and scalable cybersecurity solutions through AI, edge, and cloud computing.

III. Methodology

Overall Architecture

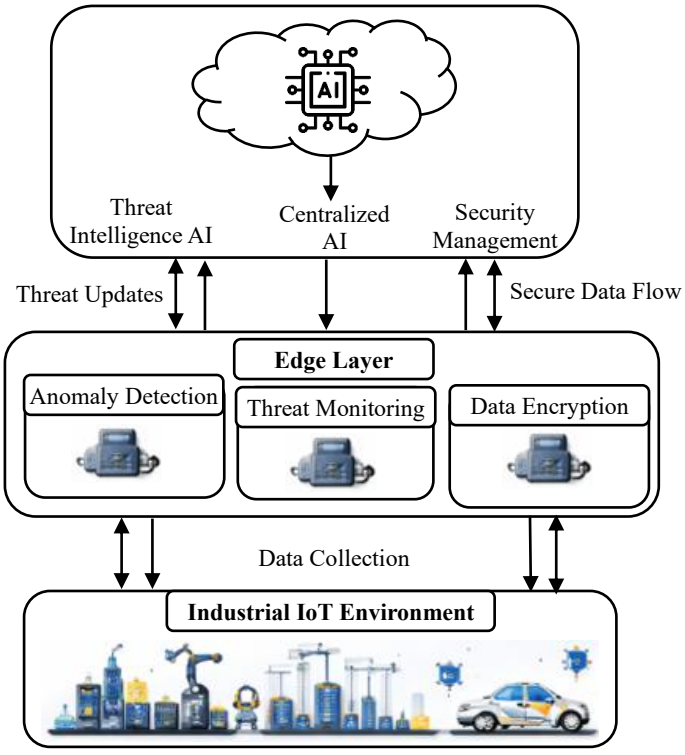

Fig. 1. AI-based Cloud-Edge IIoT Cybersecurity Architecture.

Fig. 1 is a cloud-edge collaboration framework based on AI and aimed at improving the level of cybersecurity in the context of Industrial IoT (IIoT) systems. The Cloud Layer at the top contains the centralized AI models that offer threat intelligence, security management, and processing of large amounts of data, and regularly updates the threat intelligence to offer real-time protection. The Edge Layer processes data nearer to the IIoT devices, performing essential tasks such as anomaly detection, real-time threat tracking, and data encryption, and provides low-latency detection and mitigates device-level security threats. The origin of data is the Industrial IoT Environment, where the information is generated through connected devices, machinery, and sensors and must be safeguarded. The industrial environment sends data through the edge layer to be immediately analyzed and to

ISBN: 978-81-687498-3-2

the cloud to be further processed and updated on the intelligence, merging the scalability and processing capabilities of the cloud with the low-latency of the edge to integrate to offer an all-encompassing, real-time cybersecurity solution.

An IIoT system calculates the security risk by summing the anomaly detection, threat intelligence, and response time. The contribution of each component is weighted with λ 1, λ 2, and λ 3, and it is possible to prioritize the components according to the requirements of the system. The model gives a holistic measure of security risk to be used in decision-making and mitigation. Equation (1) makes sure that the system accommodates the detected anomalies as well as timely responses to threats.

$$R_t = \lambda_1 \cdot A_t + \lambda_2 \cdot \mathcal{T}_t + \lambda_3 \cdot T_{\text{response}} \quad (1)$$

Where:

- R_t is the security risk at time t.
- A_t is the anomaly score at time t(representing threat detection at the edge).
- $\mathcal{T}_t$is the threat intelligence score at time t(aggregated in the cloud).
- T_{response} is the response time to detected threats.
- $\lambda_1, \lambda_2, and\ \lambda_3$ are weighting factors that prioritize anomaly detection, threat intelligence, and response time, respectively.

The equation is a generalized calculation of the security risk based on the detected anomalies, threat intelligence and response time of the system.

IV. Results and Discussion

4.1. Dataset Description

The TON-IoT Network Intrusion Dataset is a dataset that is used to test intrusion detection systems (IDS) within IoT networks (Programmer3, 2025). It includes network traffic data of IoT devices, of both benign (normal) and malicious traffic of all types of attacks such as DoS, DDoS, and botnet attacks such as Mirai and Gafgyt. The features of the dataset include a timestamp, a type of protocol, source and destination IP addresses, size of the payload, and size of the packet. It works well to train and test anomaly detection models and IDS on IIoT systems, which assists in the evaluation of the real-time threat detection at the edge and threat intelligence aggregation in the cloud. The data can be used in cybersecurity studies and applications in IIoT systems since it is in CSV format and with specified classes that identify the normal and attack traffic.

ISBN: 978-81-687498-3-2

4.2. Hardware and Software Configuration

The hardware architecture of the AI-based cloud-edge collaboration system consists of edge devices such as ARM Cortex-A53 processors with 2GB to 4GB RAM and 16GB to 64GB storage of the IoT devices, as well as Intel Core i5/i7 edge nodes with 8GB to 16GB RAM and 256GB SSD to process real-time data. It is supported by multi-core processors (Intel Xeon or AMD EPYC), 64GB-128GB RAM, 1TB SSD storage, and fast networking (Gigabit or 10Gbps). On the software side, the edge layer is powered by a Linux-based OS and AI software such as TensorFlow Lite or PyTorch, and MQTT/HTTP to communicate. The edge nodes provide Linux and AI operations based on either TensorFlow, Keras, or PyTorch, with data streaming capabilities by Apache Kafka and encryption with OpenSSL. Scalable services are deployed in the cloud, such as AWS, Azure, or Google Cloud, with analytics of big data running on Apache Hadoop or Spark, AI on TensorFlow or PyTorch, and cloud-native security services such as AWS Guard Duty to monitor threats.

4.3. Evaluation Metrics

1. Detection Accuracy

Equation (2) is used to determine the percentage of threats (true positives and true negatives) in the sample of the total number of samples tested. It is one of the important metrics to assess the quality of threat detection models.

$$\text{Detection Accuracy } = \frac{TP + TN}{TP + TN + FP + FN} \qquad (2)$$

Where:

- TP: True Positives (correctly identified threats)
- TN: True Negatives (correctly identified normal traffic)
- FP: False Positives (incorrectly identified as threats)
- FN: False Negatives (missed threats)

2. False Positive Rate (FPR)

Equation (3) is used to measure the ratio of normal data that is falsely detected as a threat. This measurement is significant to make sure that the system is not producing too many false alarms.

$$\text{False Positive Rate} = \frac{FP}{FP + TN} \qquad (3)$$

Where:

- FP: False Positives
- TN: True Negatives

3. False Negative Rate (FNR)

ISBN: 978-81-687498-3-2

Equation (4) measures the proportion of actual threats that are incorrectly identified as normal (i.e., missed threats). Reduced FNR is significant to ensure that the system does not miss out on the possible risks.

$$\text{False Negative Rate} = \frac{FN}{FN + TP} \quad (4)$$

Where:

- FN: False Negatives
- TP: True Positives

4. Response Time

Equation (5) is used to quantify the time it requires the system to react to the threats detected by it once the latter have been identified. This is an imperative parameter in real-time systems, whereby speed in mitigation of threats is required.

$$\text{Response Time} = \frac{\text{Time of Response} - \text{Time of Detection}}{\text{Total Number of Detected Threats}} \quad (5)$$

Where:

- Time of Response: Time when the threat is mitigated, or action is taken.
- Time of Detection: Time when the threat was first detected.

5. Scalability

The capability of the system to sustain performance with increase in number of devices or data points is measured by equation (6). It is vital in determining the capability of the model to cope with the expanding IIoT networks.

$$\text{Scalability Efficiency} = \frac{\text{Performance with Increased Devices}}{\text{Performance with Initial Devices}} \times 100 \quad (6)$$

Where:

- Performance with Increased Devices: Metrics like detection accuracy or response time when the number of devices is scaled up.
- Performance with Initial Devices: Metrics with a baseline number of devices (e.g., 50 devices in the Existing Model).

Table 1 presents the analysis of the Existing Model and the Proposed AI-based Cloud-Edge Collaboration Model, demonstrating that there are significant improvements in many important metrics. Detection accuracy of The Proposed Model is 98.6% as against 90.5% of the Existing Model, which shows that there is a marked improvement in the capability to detect threats. It also decreases False Positive Rate (FPR) to 3.2% instead of 7.5% to decrease false alarms, and False Negative Rate (FNR) is decreased to 2.4% rather than 6.8% of the Existing Model,

ISBN: 978-81-687498-3-2

which is more efficient in detecting actual threats. The Proposed Model also has a faster response rate (3-5 seconds) compared with the Existing Model (10-15 seconds), which allows for mitigating the identified threats faster.

Table 1. Model Performance Comparison.

Metric	Existing Model	Proposed Model (AI-based Cloud-Edge Collaboration)
Detection Accuracy	90.5%	98.6%
False Positive Rate (FPR)	7.5%	3.2%
False Negative Rate (FNR)	6.8%	2.4%
Response Time	10-15 seconds	3-5 seconds
Scalability	Supports up to 50 devices (100%)	Supports up to 500 devices (1000%) more, with no degradation in performance

In addition, the Proposed Model has 1000% better scalability with the capability of supporting up to 500 devices without decreasing performance, as compared to the existing Model, which supports 50 devices. Generally, the Proposed Model demonstrates undoubted strengths in the detection accuracy, efficiency, and scalability, which make it a more powerful and scalable offering to cybersecurity in IIoT settings. Offering to cybersecurity in IIoT settings.

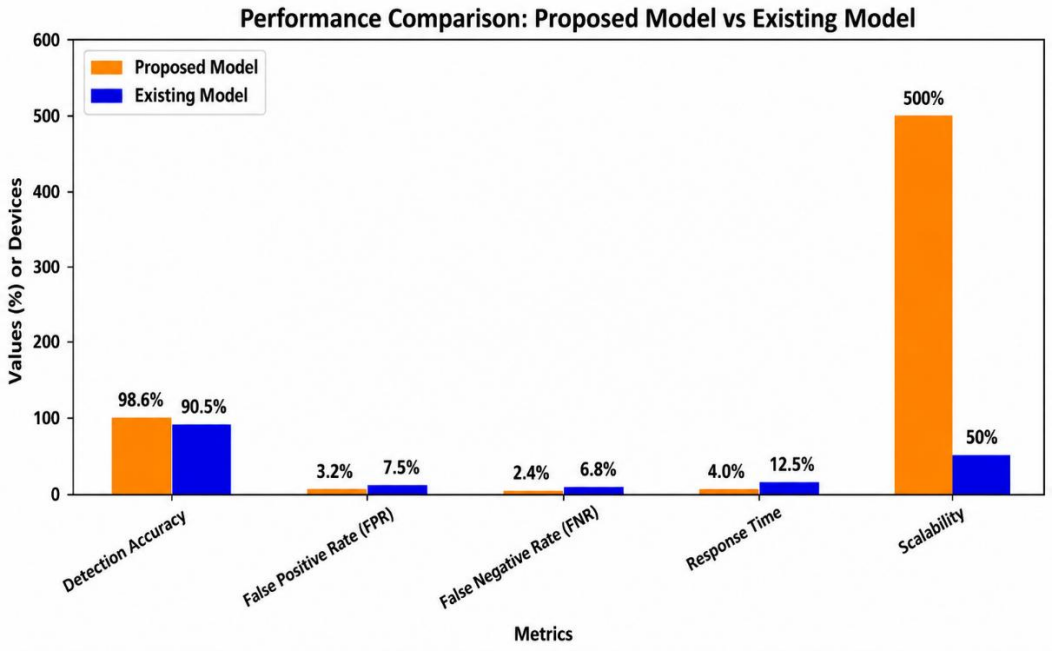

Fig. 2. Model Comparison: Existing vs Proposed AI-Edge Collaboration.

Fig. 2 compares the most important measures of performance between the Existing Model and the Proposed AI-based Cloud-Edge Collaboration Model. It indicates that the Proposed Model is much better in the Detection Accuracy than the Existing Model, 98.6% vs. 90.5%. Both False Positive Rate (FPR) and False Negative Rate (FNR) are significantly lower with the Proposed Model, 3.2% and 2.4, respectively, than the Existing Model, which is 7.5% and 6.8, respectively. Response Time in the Proposed Model is also significantly lower (3-5 seconds on average)

ISBN: 978-81-687498-3-2

than the Response Time of 10-15 seconds in the Existing Model. Scalability-wise, the Proposed Model would support up to 500 devices, which is 1000% more than the 50 devices that the Existing Model would support, and still manages to perform as well as the Existing Model. This shows that the Proposed Model has a more efficient, scalable, and precise solution to IIoT cybersecurity.

V. Discussion

The Proposed AI-based Cloud-Edge Collaboration Model performs much better than the Existing Model in various critical areas of IIoT cybersecurity. The proposed system has a higher detection accuracy (98.6), as compared to the current model (90.5), which can further be used to identify a threat more accurately in real time because of the AI-based edge and cloud-based anomaly detection. This strategy resulted in lowering the False Positive Rate (FPR) and False Negative Rate (FNR) to 3.2% and 2.4%, respectively, as opposed to 7.5% and 6.8% in the present model. This will reduce false alarms and reduce the number of threats that are not detected. The proposed model also has a much lower response time of 3-5 seconds compared to the existing model, which needs 10-15 seconds to process the data, due to the capability to handle it at the edge. This allows quicker response to the emergent threats, which is essential in IIoT settings where real-time security is essential. Scalability-wise, the proposed model can support up to 500 devices, increasing 1000 % compared to the 50 devices of the current model, without compromising the performance. The model offers scalability, which is achieved by means of cloud-edge collaboration, to make it compatible with large IIoT networks. On the whole, the Proposed Model offers a more efficient, precise, and scalable cybersecurity protection of IIoT systems that are more efficient in detection, better in threat mitigation, and smoother management of large-scale deployments, overcoming the limitations of more traditional cybersecurity systems.

VI. Conclusion

The Proposed AI-based Cloud-Edge Collaboration Model to IIoT cybersecurity can be seen as having significantly better results on several crucial performance indicators than the current systems. The proposed model will outperform the Existing Model with 98.6% detection accuracy as compared to the 90.5%. This enhancement will be critical in detecting possible cyber threats in real-time so that the system can be able to protect IIoT environments against emerging threats. Moreover, the False Positive Rate (FPR) and False Negative Rate (FNR) are also significantly lower in the proposed system, as compared to the current system of 7.5% and 6.8%, respectively. Such a decrease in the FPR and FNR means that the detection system is more accurate, with fewer false alarms and fewer threats missed, which helps to improve the efficiency of the operations. The other notable improvement is in the response time, which reduces to 3-5 seconds in the proposed model as compared to the 10-15 seconds in the current model. This enhancement allows a quicker mitigation of threats and aids in preserving the operational integrity of IIoT systems in real-time. In addition, the Proposed Model can serve up to 500 devices, and this is 1000% better than the Existing Model, which serves only 50 devices. The scalability guarantees that the

ISBN: 978-81-687498-3-2

suggested system can support large industrial networks without a decline in performance. On the whole, these findings highlight the importance of AI with cloud-edge cooperation, not only enhancing the quality and efficiency of IIoT cybersecurity, but also its scalability and flexibility in securing large-scale industrial systems. This solution is more reliable and flexible in countering the emerging cyber threats.

References

1. Alamir, R., Noor, A., Almukhalfi, H., Almukhlifi, R., & Noor, T. H. (2026). AI-Enhanced Cybersecurity in Edge Computing: Threats, Solutions, and Future Directions. *ACM Computing Surveys*, *58*(11), 1-48. https://doi.org/10.1145/3801741
2. Goswami, A. (2025). *Privacy-preserving AI models in cloud-based cybersecurity*. SGSH Publications.
3. Haseeb, S., Javed, S., Mokayed, H., Martin-del-Campo, S., Sandin, F., Liwicki, M., & Delsing, J. (2026). Local cloud-based collaborative learning vs other IIoT decentralized AI solutions: A systematic literature review. *Journal of Network and Systems Management*, *34*(2), 49. https://doi.org/10.1007/s10922-025-10029-y
4. Hawage, R., & Madireddy, L. (2025, October). AI-Enabled Cloud Computing for Scalable and Adaptive Digital Ecosystems. In *2025 2nd International Conference on Electronic Circuits and Signaling Technologies (ICECST)* (pp. 636-641). IEEE. https://doi.org/10.1109/ICECST66106.2025.11307198
5. Joel, M. R. (2024). Industrial security and its advancement through the use of edge artificial intelligence: Edge AI. In *Deep Learning Model Optimization, Deployment and Improvement Techniques for Edge-Native Applications* (p. 367). Cambridge Scholars Publishing.
6. Jonnalagadda, A. M. C. (2025). Integrating AI and Cloud Technologies for Scalable, Low-Latency Edge Computing in Enterprise Workloads. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, *8*(3), 12110-12120. https://doi.org/10.15662/IJRPETM.2025.0803007
7. Kondori, M. A., & Peashdad, O. H. (2015). Analysis of challenges and solutions in cloud computing security. *International Academic Journal of Innovative Research, 2*(1), 20–30.
8. Lakhan, A., & Groenli, T. M. (2025). Sustainable AI-assisted energy-efficient edge cloud system for industrial Internet of Things applications. In *Intelligent Urban Mobility* (pp. 315-326). Academic Press. https://doi.org/10.1016/B978-0-443-34160-1.00005-5
9. Mani, R. (2024). AI enabled cloud architectures for intelligent secure and resilient enterprise systems with autonomous decision intelligence. *International Journal of Computer Technology and Electronics Communication*, *7*(6), 9923-9931. https://doi.org/10.15680/IJCTECE.2024.0706026
10. Pal, S. (2024). Artificial intelligence-based IoT-edge environment for industry 5.0. In *IoT Edge Intelligence* (pp. 111-148). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-58388-9_4
11. Programmer3. (2025). *TON-IoT network intrusion dataset* [Data set]. Kaggle. https://www.kaggle.com/datasets/programmer3/ton-iot-network-intrusion-dataset

ISBN: 978-81-687498-3-2

12. Ravi, C. T. (2024). Optimizing edge computing and AI for low-latency cloud workloads. *International Journal*, *13*(1), 3484-3500. https://doi.org/10.30574/ijsra.2024.13.1.1761
13. Santhoshkumar, K. S., Vanitha, V., Jasim, L. H., Abdul Latheef, M. M., Subburam, S., & Arthanarieswaran, V. P. (2025). Ultra-reliable low latency wireless systems for industrial IoT. *Journal of Internet Services and Information Security, 15*(3), 160–173. https://doi.org/10.58346/JISIS.2025.I3.011
14. Sengupta, S., & Deshmukh, A. (2024). Blockchain for transparent supply chains: enhancing accountability in SDG-aligned trade. *International Journal of SDG's Prospects and Breakthroughs*, *2*(1), 7-9.
15. Zhukabayeva, T., Ahmad, Z., Adamova, A., Karabayev, N., & Abdildayeva, A. (2025). An edge-computing-based integrated framework for network traffic analysis and intrusion detection to enhance cyber–physical system security in industrial IoT. *Sensors*, *25*(8), 2395. https://doi.org/10.3390/s25082395
16. Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions. *Sensors*, *25*(1), 213. https://doi.org/10.3390/s25010213

ISBN: 978-81-687498-3-2