SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

Scalable Deep Learning Frameworks for Distributed Computing Environments

Snehal Kamble[1], Veerendra Yadav[2], Keerthika K[3], Sagar Gulati[4], Sathya Arthi R[5], Rahul Bhatt[6], M. Sangeetha[7], Sachin S. Pund[8]

[1] Assistant Professor, Department of Civil Engineering, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India. Email: snehalkamble444@gmail.com, ORCID: 0000-0002-4745-6422
[2] Assistant Professor, Department of Computer Science & Engineering, Noida International University, Greater Noida, Uttar Pradesh, India. Email: veerendra.yadav@niu.edu.in
[3] Assistant Professor, Computer Science, Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research, India. Email: keerthikak@maher.ac.in
[4] Director, Department of CS & IT, JAIN (Deemed-to-be University), Bengaluru, Karnataka, India. Email: sagar.gulati@jainuniversity.ac.in, ORCID: 0000-0001-5498-7347
[5] Assistant Professor, Department of Management Studies, Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research, India. Email: sathyaarmba@maher.ac.in
[6] Assistant Professor, Department of Computer Science & Engineering, Dev Bhoomi Uttarakhand University, Dehradun, Uttarakhand, India. Email: socse.rahul@dbuu.ac.in, ORCID: 0009-0004-0486-9413
[7] Associate Professor, Department of Computer Science and Engineering, Panimalar Engineering College, India. Email: Sangeethameckanzi2224@gmail.com, ORCID: 0000-0002-1973-6339
[8] Assistant Professor, Department of Mechanical Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra, India. Email: pundss@rknec.edu, ORCID: 0000-0002-5616-2469

Abstract
The rapid growth of large-scale visual data generated from intelligent surveillance systems, Internet of Things (IoT) enabled cameras, and smart monitoring environments has created significant challenges for efficient Deep Learning (DL) model training in distributed computing infrastructures. These environments require scalable frameworks capable of handling continuous high-volume image streams while ensuring fast training, optimal resource utilization, and minimal communication overhead across Multi-GPU Systems. To address these challenges, this research proposes a scalable distributed DL framework designed specifically for large-scale image-based analytics in IoT and intelligent monitoring applications. The proposed framework integrates data-parallel training with an optimized communication mechanism based on the Seven-Spot Ladybird Optimized Intelligent VariationalAutoencoder (SSLO-IntVAE), enabling efficient synchronization across distributed GPUs while reducing inter-node communication costs. In addition, an optimized data pipeline is incorporated to minimize input/output bottlenecks and improve throughput during large-scale training processes. A publicly available large-scale image dataset is utilized as a representative benchmark of visual data generated in IoT-based surveillance and monitoring systems. The framework is implemented and tested on a multi-GPU cluster using DL models trained in a distributed environment. Experimental results demonstrate significant improvements in 93.18% of precision, 92.53% of recall, and 96.10% of F1-score. The proposed framework provides a robust solution for large-scale visual data processing, supporting intelligent decision-making in distributed IoT and surveillance systems.

Keywords: Scalable Deep Learning, Distributed Computing, Data Parallelism, Model Parallelism, GPU Clusters, Mixed Precision Training.

1. Introduction

The development of Internet of Things (IoT)enabled surveillance systems resulted from the need for intelligent and connected security systems. These systems involve the use of sensors, cameras, and the Internet to facilitate monitoring. The conventional method of surveillance was very manual, as it required physical presence at the site to observe and record information [1]. The IoT surveillance network is efficient through the introduction of wireless technologies. Cloud computing is an important element in IoT surveillance technology because it allows for the storage and processing of data anywhere in the world [2]. Edge computing enhances the efficiency of IoT-based surveillance by reducing decision-making delays and enabling data to be processed closer to its source. MachineLearning (ML) is also being adopted in IoT surveillance technology for the purposes of intelligent object and anomaly detection [3]. Monitoring with the help of IoT technology is extensively used in areas such as smart homes, smart cities, industry, health care, and environmental research for increasing safety and operational efficiency. In spite of the benefits that come with this technique, there are certain problems associated with it, like data security issues [4]. Early warning technologies that incorporate intelligence are receiving considerable attention in research on safety management, but remain limited in some ways. Statistical threshold methods require specific thresholds, which can lead to problems such as low adaptability and incorrect predictions [5-7]. The cameras are used for visual inspection and Artificial Intelligence (AI) processing, but also pose security concerns. The usage of energy increases when using several cameras, and the instantaneous processing experiences some delay due to loading issues. Furthermore, hardware-dependent Vision Processor Units (VPUs) pose an inflexibility issue, which causes high costs for scaling [8].

1.1 Research Aim: This research develops a scalable distributed Deep Learning (DL) framework for IoT-based visual analytics using Seven-Spot Ladybird Optimized Intelligent VariationalAutoencoder (SSLO-IntVAE), aiming to predict GPU training performance (Excellent, Good, Moderate, Poor) while reducing communication overhead and improving efficiency and resource utilization across multi-GPU systems.

Section 1 provides the background of the research. Section 2 focuses on reviewing existing research. Section 3 discusses the methodology of data collection, preprocessing, and future extraction, as well as the proposed model SSLO-IntVAE. Section 4 includes results obtained from experimental analysis. Section 5 presents the conclusion with the performance, limitations, and future work.

2. Related Work

The Abnormal human action in videos with the custom dataset was developed in [9]. The technique includes training the Convolutional Long Short-Term Memory (ConvLSTM) algorithm for tasks such as theft and harassment. The system managed to achieve an accuracy of 96.19%, and short time periods limit its effectiveness. Automating Closed Circuit Television (CCTV) video screening to detect anomalies and lessen the need for manual monitoring was explored [10]. An edge-based surveillance system processes video data on edge nodes. Thirteen categories of anomalous events are proposed to be classified using a customized Bidirectional Long Short-Term Memory (Bi-LSTM) model. With increased efficiency, the system attains a greater accuracy of 91.62%, limitations in reliance on labeled data, and difficulties with instantaneous scaling across many cameras and surroundings. The Multi-Sensor Node Integration and Performance Evaluation in various situations was conducted [11]. Install Wi-Fi LoRa 32 boards with temperature, gas, and smoke sensors to send data over great distances using Long Range Wide Area Network (LoRaWAN) technology. Attain increased efficiency (over 90%) and dependable data transport with quicker response times. Signal interference, interior range restrictions, and reliance on precise hardware calibration are some of the limitations. The system intended to guarantee a reliable water supply in rural areas through long-distance transmission via Long Range (LoRa) technology was examined [12]. This system minimized energy wastage and instances of theft, as well as automated pump operations. The findings indicated that energy consumption was decreased by 41.2%. Some of the weaknesses associated with the system include distance limitations and message delays. Cyber-physical security using human activity recognition enhancement was analyzed [13]. This solution uses a combination of GoogleNet-BiLSTM with IoT edge computing. The system can recognize suspicious activities with 73.15% accuracy. Drawbacks of this solution are its limited accuracy, sensitivity to video quality, and difficulty in complex settings.

The research into utilizing a secure IoT network through an anomaly-based intrusion detection system was explored [14]. This technique suggests using a combination of CNN-Gated Recurrent Unit (GRU) for performing binary and multi-class classifications. The performance result shows exceeded 98%. The limitations are

associated with high computing costs, dataset dependency, and efficiency on IoT resources. Improvement in safety for smart buildings through IoT sensor data was explored [15]. A light-weight unsupervised sparse U-Net proposed method for detecting anomalies at edge nodes that works on instantaneous data without requiring any labeled datasets and achieves an accuracy of around 90%-95%. However, the noise-sensitive nature and low performance in highly dynamic environments are limitations. Traffic accidents detected in surveillance videos are examined [16]. The methodology applies CNN to detect Video Traffic Surveillance Cameras (VTSS) footage anomaly detection. The accuracy obtained was 82%. There are restrictions in the data set, accuracy limitations, and difficulties in generalizing different instantaneousinstances. Developing adaptive Quality of Service (QoS) for IoT multimedia using Software-Defined Network (SDN) and DL was investigated [17]. For instantaneous weapon detection, train several models and choose the top one, You Only Look Once version 5 nano(YOLOv5n). Use edge AI to decrease traffic and send important frames. The results demonstrate a 75.0% increase, and an improvement in packet loss of 32.5%. Model generalization issues and edge resource limitations are examples of limitations.

The IoT surveillance dependability creation, including the identification of critical elements and metrics, was developed [18]. To maximize availability and dependability, the model system makes use of camera Mean Time To Failure (MTTF). The findings indicate that while reliability rises by about 20% with increased MTTF, availability improves significantly with more LTE stations. Modeling assumptions and a lack of instantaneous validation are the limitations. An IoT-based anomaly detection system for surveillance of smart cities using massive amounts of video data was examined [19]. Use an autoencoder for refinement, an edge-deployable Echo State Network (ESN) for temporal learning and detection. The model improves detection efficiency with an accuracy of roughly 94%. Limitations include reliance on data quality and sensitivity to extremely complicated abnormalities. The use of a Lightweight CNN for resource-constrained devices to enable instantaneous gun and knife detection in Multiview Surveillance was investigated [20]. The proposed method classifies, and identifies anomalous items using a Multiclass Subclass Detection CNN. Precision is up to 90.50% on Olmos, and 90.7% on Multiview Cameras. Reduced performance in extremely complex scenarios and reliance on dataset quality are the limitations.

3. Methodology

Figure 1 illustrates the methodology developed specifically to evaluate the scalability of DL frameworks in distributed GPU environments. The primary purpose of this methodology is to enable efficient analysis of images at scale in IoT-based surveillance systems and intelligent monitoring systems. The proposed methodology comprises data collection, bilateral filter–based preprocessing, Local Binary Pattern (LBP) feature extraction, communication optimization using SSLO-IntVAE, and comprehensive performance evaluation.

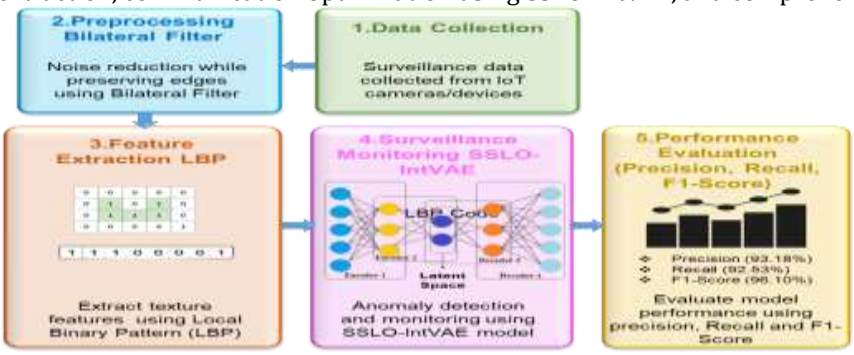

Figure 1: Methodology Workflow for the IoT-Based Surveillance and Monitoring

3.1 Data Collection

Data Collection is carried out using the Kaggle Dataset (https://www.kaggle.com/datasets/colabsss/distributed-gpu-training-performance-data). It contains 8,120 data entries in one CSV file with 11 columns of distributed GPU training performance data. The dataset is created to test scalable DL frameworks in distributed GPU-based architectures that serve IoT and surveillance purposes. Evaluating scalability, efficiency of communication, GPU usage, and distributed DL performance. For large-scale visual analytics applications, research is being done on intelligent monitoring, resource optimization, and performance evaluation in multi-GPU settings.An 80% data training and 20% data testing split was applied for model evaluation.

3.2. Data Preprocessing Using Bilateral Filter

Following the data gathering process, the data preprocessing phase is carried out by employing a Bilateral Filter to improve image quality without compromising the significant structural features, including the edges that are necessary for deep feature extraction through a distributed DL model. This is especially crucial in scenarios where IoT-based surveillance and smart monitoring systems are being utilized, since the input data in such instances suffers from various forms of distortion due to noise resulting from different factors. The Bilateral Filter process is expressed in Equation (1).

$$h'(o) = \frac{1}{X(o)} \times \sum_{r \in M(o)} L_d(\|o - r\|) L_t(\|h(r) - h(o)\|)\, h(r) \quad (1)$$

$h'(o)$ represents enhancing the clarity while preserving edges in surveillance images, $x(o)$ represents the normalization factor to maintain the brightness of camera-based monitoring systems, and $\in$ indicates that an surveillance object is a member of a set Σ_r represents surveillance data. $M(o)$represents filtering noisy camera image data, $L_d(\|o - r\|)$ represents the ensuring of pixels in surveillance frames, and $L_t(\|h(r) - h(o)\|)$ represents preserving the edges in surveillance images. $h(r)$represents local information of image capture by surveillance data. The kernel functions are defined using a Gaussian distribution expressed in Equation (2).

$$L_{j(w)} = f^{-w^2/2\sigma_j^2} \quad (2)$$

$L_{j(w)}$ represents the smoothing of important structure in surveillance data, f represents consistency of GPU Pipelines, and w represents intensity variation between pixels in surveillance images. $\sigma_j$represents smoothing noise in monitoring environments.

3.3. Feature Extraction Using Local Binary Pattern (LBP)

After the preprocessing by Bilateral Filtering, the LBP method is used for feature extraction to extract robust texture information from large-scale visual information. This technique is crucial for a distributed DL framework based on the IoT, which needs discriminative and efficient features for its operation in intelligent surveillance applications involving multiple GPUs. The LBP of each pixel of the image is expressed in Equation (3).

$$LBP_{o,q} = \sum_{o=0}^{o-1} t\,(h_o - h_d) * 2^0, t(w) = \begin{Bmatrix} 1 & \times \geq 0 \\ 0 & \times < 0 \end{Bmatrix} \quad (3)$$

$LBP_{o,q}$ represent the local texture patterns captured by the camera in surveillance Multi-GPU Systems, Σ represents the summation, which encodes the patterns, and o represents the extraction of texture details in IoT monitoring. t represents the encoding of a texture pattern into binary format (0 or 1), h_o represents the recognition of texture patterns, and h_d represents the detection of changes in local texture. $t(w)$represents the local pixel variations, which are converted into a compact binary code.

3.4. IoT-based surveillance and monitoring using Seven-Spot Ladybird Optimized Intelligent VariationalAutoencoder (SSLO-IntVAE)

The Seven-Spot Ladybird Optimized Intelligent VariationalAutoencoder (SSLO-IntVAE) is designed for IoT-based surveillance and monitoring systems to efficiently analyze large-scale visual data from distributed camera networks. It improves model training efficiency and communication effectiveness across IoT-enabled multi-GPU systems for scalable performance. In addition, the overall scalability performance is categorized as Excellent, Good, Moderate, and Poor, enabling systematic evaluation of distributed training behavior in complex surveillance scenarios. This classification supports adaptive optimization, improved resource allocation, and reliable decision-making in large-scale IoT surveillance deployments using the SSLO-IntVAE architecture, ensuring robustness and scalability in an instantaneous applications framework performance-enhanced.

Hybrid SSLO–IntVAE Framework for IoT Surveillance Optimization: To improve IoT surveillance performance, the hybrid SSLO–IntVAE system combines IntVAE-based latent feature learning with SSLO-driven communication optimization. IntVAE extracts robust probabilistic representations after SSLO adjusts multi-GPU parameters for effective data transfer. In dispersed environments, this sequential combination guarantees scalable, low-latency, and precise intelligent monitoring.

3.4.1Intelligent VariationalAutoencoder (IntVAE) for Latent Representation in Distributed GPU-Based Deep Learning Frameworks

After the Hybrid SSLO–IntVAE Framework for IoT Surveillance Optimization, the IntVAE model is used to learn a concise probability distribution representation of the high-dimensional features. As such, in the distributed DL algorithm architecture, while traditional autoencoders rely on deterministic functions, IntVAE adopts a new technique by using the latent space as a distribution. Consequently, this method enables the IntVAE to capture the variations that exist in the surveillance data better than other techniques, as expressed in Equations (4- 7).

$$r^*(y) = \underset{r(y)}{\text{minimize}}\, KL(r(y)\|o(y|w)) \quad (4)$$

$r^*(y)$represent the optimal latent distribution of surveillance data, r(y) represent the true latent large-scale IoT surveillance image data in the encoder, and KL represents the Kullback–Leibler divergence, which ensures the IntVAE learns accurate uncertainty modeling for IoT data. o(y|w)represents surveillance input data to generate latent representations.

$$\mathbb{E}_{r(y)}[\log r(y)] - \mathbb{E}_{r(y)}[\log o(y, w)] + \log o(w) \quad (5)$$

$\mathbb{E}_{r(y)}[.]$ represents the estimation of properties in surveillance data, $o(y, w)$ represents the relationship between surveillance images and their hidden representations, and o(w) represents input image streams in monitoring systems.

$$\mathbb{E}_{r\phi(y|w)}[\log(o_\theta(w|y)o_\theta(y)) - \log r_\phi(y|w)] \quad (6)$$

$\mathbb{E}_{r\phi(y|w)}$represents the map of surveillance inputs into latent feature space, $o_\theta(w|y)$ represents reconstructing the surveillance images from latent representations, and $o_\theta(y)$ represents decoder parameters. $\log r_\phi(y|w)$represents the improvement in consistency of surveillance data.

$$\mathcal{L}(\phi, \theta, w) = \mathbb{E}_{r\phi(y|w)}[\log(o_\theta(w|y)] - KL(r\phi(y|w)\|o_\theta(y)) \quad (7)$$

$\mathcal{L}(\phi, \theta, w)$represent the optimization of reconstructing surveillance data, and $(r\phi(y|w)\|o_\theta(y))$ represent the smooth latent space of IoT monitoring.

3.4.2. Seven-Spot Ladybird Optimization (SSLO) for Communication Efficiency in Surveillance Monitoring

The SSLO is used for the optimization process of the proposed DL system to improve its efficiency and robustness. The optimization process is done by applying the SSLO algorithm on various system parameters.An optimization process is highly relevant in the context of IoT-based surveillance and intelligent monitoring systems. The SSLO algorithm models the search process conducted by SSL in multi-dimensional search spaces. The search space is divided into different patches, while each ladybug is considered to be a potential solution in the optimization problem space process is expressed in Equation (8).

$$n = \Pi n_i \quad (8)$$

nrepresents the overall search space optimization of surveillance, Π represents the segmented optimization of surveillance, and n_i represents parameter groups across distributed monitoring nodes. Updating Position procedure expressed in Equations (9 and 10).

$$U_j(s) = d * q_1 * \left(T_j(s) - W_j(s)\right) + \varepsilon_1 \quad (9)$$

$U_j(s)$ represent the improvement of communication efficiency in IoT Monitoring, d represent balanced exploration of surveillance optimization, and q_1 represent fine-tune parameters for efficient monitoring performance. $T_j(s)$represent the surveillance of optimal configuration for communication efficiency, and $W_j(s)$ represent system parameter setting before optimization for monitoring, and ε_1 represents surveillance optimization to improve robustness of data variations.

$$W_j(s+1) = W_j(s) + U_j(s), \quad |U_j(s)| \le U_{max} \quad (10)$$

$(s+1)$represents the next optimization round for surveillance, and U_{max} represents ensuring the Multi-GPU optimization for surveillance. In case of intensive searching, a ladybird starts extensive searching. The position update takes the form as stated in Equation (11).

$$U_j(s) = d * q_2 * \left(K_j(s) - W_j(s)\right) + \varepsilon_2 \quad (11)$$

$q_2$represents the enhancement of fine-tuning for high-density surveillance environments, $K_j(s)$ represent the refinement of model accuracy or communication efficiency for monitoring, and ε_2 represents the stagnation prevention to improve the dynamic environment of surveillance. Convergence Multi-GPU optimization is expressed in Equation (12).

$$U_{max} = 0.2(u_b - l_b) \quad (12)$$

U_{max}represents the stable of convergence for Multi-GPU Optimization in surveillance, u_b represents the upper bound allowing for the highest configuration value to the communication setting, and l_b represents the lower bound to ensure the parameter remains within feasibility in surveillance optimization.

Hyperparameter: The Hyperparameters are adjusted to achieve maximum efficiency for SSLO-IntVAE in a distributed GPU environment. The Neural Network consists of 256 Input Neurons, Three Layers (512, 256, and 128), 64 Latent Variables, and ReLU Activation Function. The training procedure is done by the Adam Optimization Technique at a learning rate of 0.001, 64 Samples per Batch, 200 epochs, 80-20 Training-Test Ratio, and the SSLO method using 30 Agents.

4. Results

Using distributed GPU settings, the suggested SSLO-IntVAEmethod shows excellent performance, reducing computation time while maintaining accuracy and scalable performance consistency in IoT-based surveillance systems. It demonstrates its efficacy in dependable detection and monitoring with precision, recall, and the F1-Score. Additionally, the framework guarantees faster convergence and lowers communication overhead, which makes it appropriate for large-scale DL applications in resource-intensive and dynamic IoT surveillance and monitoring settings.

4.1. Experimental Setup

The experiment is performed on a configuration to analyze the effectiveness of the proposed SSLO-IntVAE method through its application in distributed GPUs in the context of DL. The hardware used in this model includes an Intel i7/i9 12th Gen CPU, 32 GB RAM, 1TB SSD, and NVIDIA RTX 3080/4070 GPU with CUDA 12.1. The software includes Python 3.10, TensorFlow 2.13, Keras, and SSLO packages.

4.2 Exploratory Data Analysis

Figure 2(a) shows that the key objective is to discover "sweet spots" within the parameter setting space, where throughput is optimized with minimum resource wastage. Another dimension is added to the plot through the color scale representing GPU Utilization ranges between 50% range to 90%. Figure 2(b) depicts the aggregated makeup of system resources through 200 Sample Indices. The stacked area region is constant, that the model is compute-limited instead of memory-limited. Figure 2(c) displays the detection of anomalies and pattern recognition within high-dimensional datasets. Through visual inspection of whether the different performance groups and their distinct features overlap. Figure 2(d) displays each horizontal line as the difference between two different metrics. This allows for the identification of particular samples that indicate poor system performance relative to its capabilities.

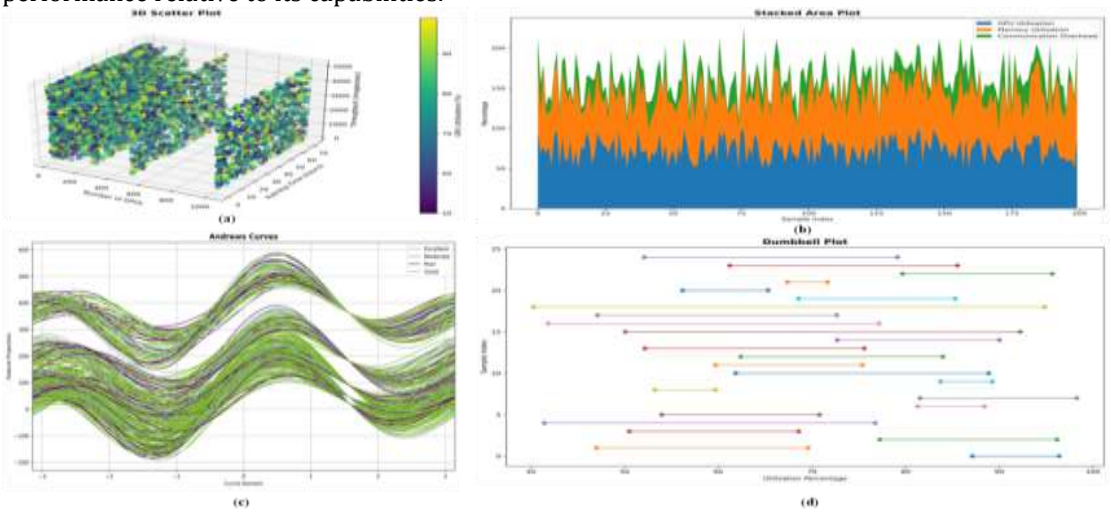

Figure 2: Scalable Framework ofDistributed DL GPU System(a) Multivariate Data Distribution, (b) Resource Utilization, (c) Multidimensional Data Patterns, and (d) Utilization Performance Variance Analysis

4.3 Evaluation Metrics

This research assesses the effectiveness of the proposed SSLO-IntVAEmethod usingPrecision, Recall, and F1-Score for IoT-based surveillance and monitoring by utilizing a large-scale image dataset in a distributed GPU environment. Precision denotes the percentage of true positive samples out of all predictions made as positives, showing the correctness of the surveillance predictions made by the system, where accurate identification of suspicious or relevant objects/events is critical for reliable monitoring. Recall shows the extent to which the model can identify all the necessary images in the data set, denoting the completeness of the detection process in monitoring systems, ensuring that any important surveillance is not missed. F1 score is the harmonic mean of precision and recall, providing a balanced evaluation metric for overall performance in IoT-based surveillance and Monitoring for effective decision-making.

4.4 Performance Evaluation

Table 1 and Figure 3 present the proposed SSLO-IntVAE with MSD-CNN [20] in the IoT Surveillance and monitoring. The MSD-CNN attains a precision value of 90.7%, a recall value of 86.33%, and an F1 score of 95.7%.

In contrast, the proposed model SSLO-IntVAE performs well on all parameters, having a precision of 93.18%, which means fewer incorrect predictions, and a higher recall of 92.53%. The F1 score is 96.10%, which shows that the model achieves well-balanced performance.

Table 1: Comparison analyses of Existing and Proposed Method

Methods	Precision	Recall	F1-Score
MSD-CNN [20]	90.7%	86.33%	95.7%
SSLO-IntVAE [Proposed]	93.18%	92.53%	96.10%

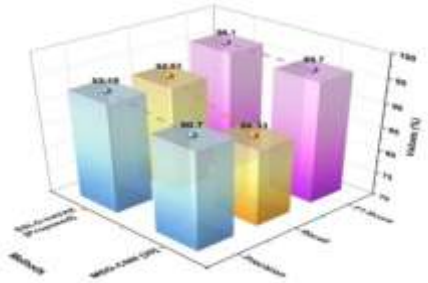

Figure 3: Performance comparison of MSD-CNN [20] and proposed SSLO-IntVAE

4.5 Discussion

An emphasis on enhancing training effectiveness, scalability, and communication optimization in large-scale visual analytics systems, the research attempts to assess the performance of scalable DL frameworks in distributed GPU contexts for IoT-based surveillance and monitoring datasets. To provide weapon identification in multiview scenarios, a Lightweight Convolutional Neural Network was introduced [20] for resource-constrained surveillance equipment. Although, its limited feature representation and reliance on high-quality training data caused performance problems in challenging instantaneous circumstances. It ignores problems with distributed training, like inter-GPU communication and synchronization delays. To overcome these limitations, the proposed research presents a scalable distributed DL framework that optimizes inter-node communication across GPU clusters while improving feature learning. This framework is built on the SSLO-IntVAE mechanism. To assure robustness, scalability, and consistent performance on large-scale IoT surveillance datasets, the suggested SSLO-IntVAE-based scalable distributed framework makes use of multi-GPU data-parallel training, enhanced data pipelines, and optimized communication.

5. Conclusion

The research proposes a framework based on DL for a surveillance and monitoring system based on the Internet of Things, using a distributed environment with GPUs. Collecting the data for image preprocessing, the data is processed using the Bilateral Filter, whereas the feature extraction uses the LBP algorithm. In terms of effective communication, using SSLO, while IntVAE provided the latent representations of high dimensions. The proposed framework based on SSLO-IntVAE proved to be highly efficient, with results like 93.18% of precision, 92.53% of recall, and 96.10% of F1-score, as well as the GPU utilization. Nevertheless, despite the expensive gear and excellent scalability, several issues are still unresolved. Future work focuses on edge-GPU integration and adaptive instantaneous learning for dynamic IoT environments.

REFERENCES

1. Diaz-Gorrin, J. and Caballero-Gil, C., 2026. Enhancing Vehicle IoT Security with PQC: A Lightweight Approach for Encrypted Sensor Data Transmission. Electronics, 15(3), p.684. https://doi.org/10.3390/electronics15030684
2. Aljami, H.M., Alrowais, N.A., AlAwajy, A.M., Alhrgan, S.O., Aldwaani, R.A., Alsawadi, M.S., Saqib, N.U., Alam, S.S. and Alsubaie, R., 2026. Benchmarking YOLOv8 Variants for Object Detection Efficiency on Jetson Orin NX for Edge Computing Applications. Computers, 15(2), p.74. https://doi.org/10.3390/computers15020074

3. Liao, T., Zeng, X., Li, X., Li, Z., Zhang, J., Liu, C. and Wu, W., 2026. Research and Application of Intelligent Control System for Uniform Pellet Distribution. Processes, 14(3), p.490. https://doi.org/10.3390/pr14030490
4. Liu, Z., Wang, B., Hu, F., Wan, R. and Zhou, C., 2026. Development of a novel intelligent control system for an autonomous multiple codend opening/closing mechanism in sampling nets. Applied Ocean Research, 166, p.104906. https://doi.org/10.1016/j.apor.2025.104906
5. Li, J., Huang, J., Bao, X., Shen, J., Chen, X. and Cui, H., 2026. Tunnel intelligent monitoring and early warning system integrating multi-source data: Methods, architecture, and engineering practices. Tunnelling and Underground Space Technology, 168, p.107142.https://doi.org/10.1016/j.tust.2025.107142
6. Pardo-Pina, S., Germer, J., Suay-Cortés, R., Platero-Horcajadas, M. and Ferrández-Pastor, F.J., 2026. An Agent-Based Service Architecture for Smart Greenhouses: Telemetry Analytics and Decision Support with RAG-grounded LLM Agents. Smart Agricultural Technology, p.101872. https://doi.org/10.1016/j.atech.2026.101872
7. Bicamumakuba, E., Reza, M.N., Jin, H., Samuzzaman, Choi, H. and Chung, S.O., 2026. Real-Time Remote Monitoring of Environmental Conditions and Actuator Status in Smart Greenhouses Using a Smartphone Application. Sensors, 26(5), p.1548. https://doi.org/10.3390/s26051548
8. Cob-Parro, A.C., Losada-Gutiérrez, C., Marrón-Romera, M., Gardel-Vicente, A. and Bravo-Muñoz, I., 2021. Smart video surveillance system based on edge computing. Sensors, 21(9), p.2958. https://doi.org/10.3390/s21092958
9. Vrskova, R., Hudec, R., Kamencay, P. and Sykora, P., 2022. A new approach for abnormal human activities recognition based on ConvLSTM architecture. Sensors, 22(8), p.2946. https://doi.org/10.3390/s22082946
10. Ali, M., Goyal, L., Sharma, C.M. and Kumar, S., 2024. Edge-computing-enabled abnormal activity recognition for visual surveillance. Electronics, 13(2), p.251. https://doi.org/10.3390/electronics13020251
11. Safi, A., Ahmad, Z., Jehangiri, A.I., Latip, R., Zaman, S.K.U., Khan, M.A. and Ghoniem, R.M., 2022. A fault tolerant surveillance system for fire detection and prevention using LoRaWAN in smart buildings. Sensors, 22(21), p.8411. https://doi.org/10.3390/s22218411
12. Balderrama-Rey, U., Verdugo-Miranda, R., Martínez-Gil, M., Carvajal-Soto, J., Romo-García, F., Medina-Zazueta, L., Espinoza-Zallas, E. and Flores-Ochoa, R., 2026. Design and Implementation of a Remote Water Level Control and Monitoring System in Rural Community Tanks Using LoRa and SMS Technology. Applied System Innovation, 9(4), p.76. https://doi.org/10.3390/asi9040076
13. Achar, S., Faruqui, N., Whaiduzzaman, M., Awajan, A. and Alazab, M., 2023. Cyber-physical system security based on human activity recognition through IoT cloud computing. Electronics, 12(8), p.1892. https://doi.org/10.3390/electronics12081892
14. Ullah, I., Ullah, A. and Sajjad, M., 2021. Towards a hybrid deep learning model for anomalous activities detection in internet of things networks. IoT, 2(3), pp.428-448. https://doi.org/10.3390/iot2030022
15. Cicero, S., Guarascio, M., Guerrieri, A. and Mungari, S., 2023. A deep anomaly detection system for iot-based smart buildings. Sensors, 23(23), p.9331. https://doi.org/10.3390/s23239331
16. Khan, S.W., Hafeez, Q., Khalid, M.I., Alroobaea, R., Hussain, S., Iqbal, J., Almotiri, J. and Ullah, S.S., 2022. Anomaly detection in traffic surveillance videos using deep learning. Sensors, 22(17), p.6563. https://doi.org/10.3390/s22176563
17. Fathy, C. and Saleh, S.N., 2022. Integrating deep learning-based iot and fog computing with software-defined networking for detecting weapons in video surveillance systems. Sensors, 22(14), p.5075. https://doi.org/10.3390/s22145075
18. Gonçalves, I., Rodrigues, L., Silva, F.A., Nguyen, T.A., Min, D. and Lee, J.W., 2021. Surveillance system in smart cities: a dependability evaluation based on stochastic models. Electronics, 10(8), p.876. https://doi.org/10.3390/electronics10080876
19. Islam, M., Dukyil, A.S., Alyahya, S. and Habib, S., 2023. An IoT enable anomaly detection system for smart city surveillance. Sensors, 23(4), p.2358. https://doi.org/10.3390/s23042358
20. Ingle, P.Y. and Kim, Y.G., 2022. Real-time abnormal object detection for video surveillance in smart cities. Sensors, 22(10), p.3862. https://doi.org/10.3390/s22103862