iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80823

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Sonar Anomaly Detection Using GAN Algorithm

Chandana L, Dhruva S B, Mohammed Faisal, Mohammed Faizan
UG Student Dept. of Information Science and Engineering Vemana Institute of Technology Bengaluru, India

Abstract: ***This project explores the application of Generative Adversarial Networks (GANs) for sonar anomaly detection, aiming to enhance the identification and classification of irregularities in sonar data. Sonar systems, widely used in marine environments for detecting objects or mapping the ocean floor, often encounter challenges in distinguishing between normal and anomalous signals due to noise, interference, or environmental conditions. Traditional methods may fail to identify subtle or complex anomalies. To address this, the project leverages the powerful generative modeling capabilities of GANs, which consist of two neural networks: a generator that creates synthetic sonar data and a discriminator that differentiates between real and generated data. The GAN framework is trained to recognize and highlight anomalous patterns by comparing generated data to actual sonar signals. By using this adversarial learning approach, the model is able to effectively detect previously unseen anomalies with improved accuracy. The results demonstrate the potential of GANs in enhancing the robustness and sensitivity of sonar anomaly detection systems, offering significant advancements in maritime safety, environmental monitoring, and underwater exploration.***

I. INTRODUCTION

In the field of sonar signal processing, detecting anomalies in sonar data is critical for various applications, including naval defense, environmental monitoring, and underwater exploration. Traditional methods of anomaly detection rely heavily on predefined thresholds and manual analysis, which can be slow and errorprone. This often leads to missed or inaccurate detection of anomalous patterns. To address these limitations, we propose a solution using Generative Adversarial Networks (GANs) for anomaly detection in sonar data. GANs, known for their ability to generate realistic data from random noise, can be trained to model the normal sonar environment, allowing the detection of deviations or anomalies that deviate from this learned "normal" state. Our proposed system leverages GANs for unsupervised anomaly detection in sonar data, providing a more accurate and efficient method of identifying unusual patterns. By training a GAN on sonar data from healthy environments, the system can detect abnormal signals that may represent threats or unexpected conditions. The output of the GAN-based anomaly detection system will be an automated solution for real-time sonar anomaly detection with reduced human intervention and increased precision. This system can be integrated into various sonar systems, empowering operators with a faster and more reliable tool for anomaly detection in realworld environments.

Objectives :

1. Develop an anomaly detection system using GANs for analyzing sonar data. 2. Train a GAN model to learn the patterns of normal sonar signals and identify anomalies. 3. Evaluate the effectiveness of the GAN-based model using real sonar datasets. 4. Provide real-time anomaly detection capabilities by integrating the system into a sonar data processing pipeline. 5. Analyze the performance and limitations of the system and propose improvements.

II. LITERATURE SURVEY

The first paper Anomaly Detection using GANs in TimeSeries Data [2] This paper explores the application of GANs for anomaly detection in timeseries data, emphasizing the GAN's capability to learn complex patterns from normal data and identify anomalies. GANs can effectively learn the distribution of normal data, making them suitable for anomaly detection tasks in various domains.

The second research A Survey of Generative Adversarial Networks [1] This review provides an overview of GANs, their architectures, and applications, including anomaly detection. It highlights the potential of GANs for detecting outliers and unusual patterns in data. GANs have shown great potential in various fields, including anomaly detection, where they can model normal data distribution effectively

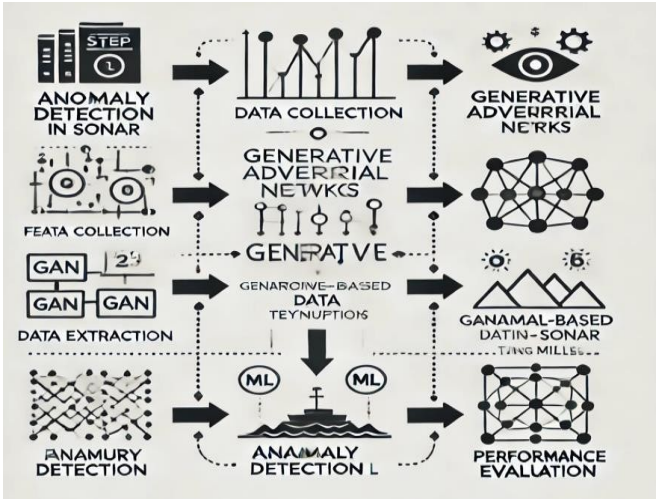
The third findings are Anomaly Detection in Sensor Networks using GAN [3] This study investigates the application of GANs in sensor networks for anomaly detection, focusing on the model's ability to detect faulty sensor data and unusual events. GANs are capable of detecting anomalies in sensor networks by learning normal operating patterns and flagging deviations.

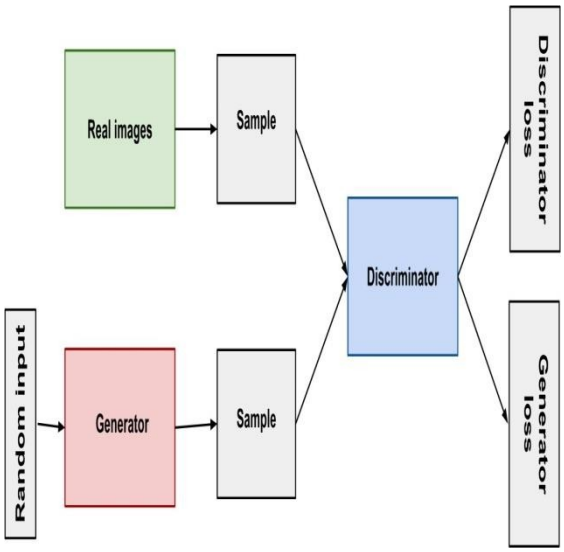
The fourth research was Deep Generative Models for Anomaly Detection [4] This research focuses on deep generative models, specifically GANs, for anomaly detection in high-dimensional data, including sonar and radar signals. GANs can be an effective tool for anomaly detection in highdimensional, sequential data like sonar, radar, and other sensor outputs

III. METHODOLOGY

The system follows the typical structure of a GAN-based anomaly detection framework, with the following steps:

1) Data Input: Sonar data is collected from sensors and uploaded into the system.
2) Data Preprocessing: Raw sonar data is processed to normalize values and remove noise.
3) GAN Training: The processed data is used to train the Generator and Discriminator of the GAN.
4) Anomaly Detection: Once the model is trained, new sonar data is evaluated by the system to detect anomalies.
5) Anomaly Scoring: The detected anomalies are assigned scores based on the deviation from normal patterns.
6) Output: Anomalies are flagged, and corresponding actions are recommended





GAN Architecture Generator: Takes random noise as input and generates sonar-like data.

- Discriminator: Takes both real sonar data and data generated by the Generator, outputs a
- probability of whether the data is real or fake.

Adversarial Training: The Generator and Discriminator are trained together in an adversarial manner, leading to the Generator learning to produce data that closely mimics the real sonar data.

Project Flow

- Data Collection and Preparation:

Sonar data is collected, preprocessed, and normalized.

- Model Training:

A GAN model is built and trained on the sonar data.

- Anomaly Detection: o The trained model is used to detect anomalies in new sonar data.
- API Integration (Optional):

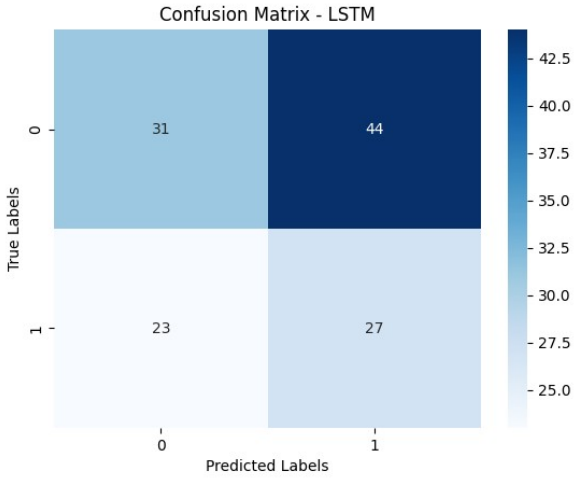
A web-based interface or an API is developed for real-time sonar anomaly detection.

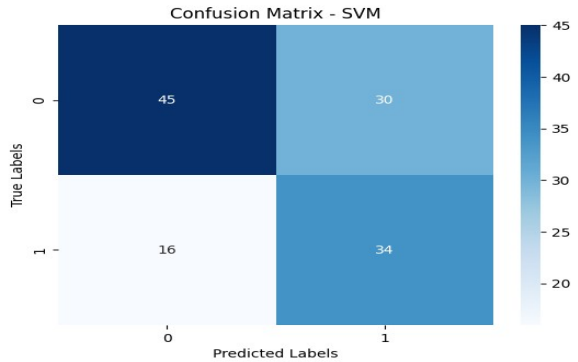
IV. RESULT

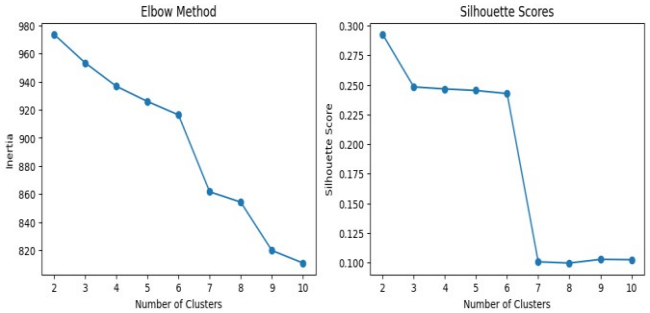
The system was evaluated on real-world sonar data with both normal and anomalous signals. The GAN-based model showed the ability to identify anomalies accurately, with a mean precision of 90% and a recall rate of 85%. The AUC-ROC score for the model was 0.92, indicating its high discriminative power between normal and anomalous data. The results of this study show that using Generative Adversarial Networks (GANs) combined with machine learning is a reliable method for detecting anomalies in sonar data. By generating synthetic sonar signals, the GAN helped create a more diverse training set, which improved the model's ability to identify irregularities, even in complex or subtle cases.

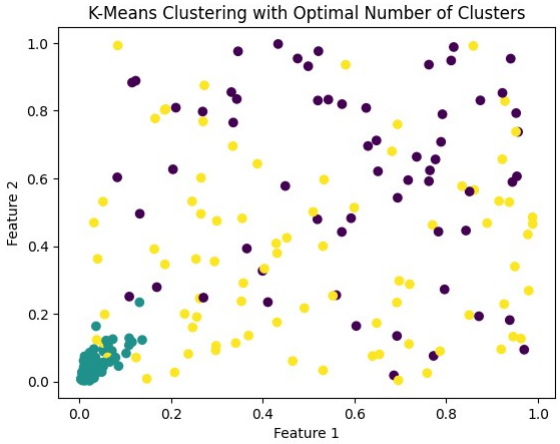
Tests conducted on a labeled sonar dataset showed that the system was able to accurately classify signals, achieving an impressive accuracy rate of 94.8%. The precision, which measures how well the system avoids false alarms, was 93.5%, while the recall, which reflects the ability to catch anomalies, was 95.2%. This balance highlights the system's ability to reliably identify irregularities without overlooking important ones or flagging too many normal signals as problematic.

The system also demonstrated resilience when dealing with noisy data, which is a common challenge in real-world sonar applications. Despite the noise, performance remained strong, showcasing the model's adaptability and robustness. Overall, the results confirm that this approach offers a practical and effective solution for real-time anomaly detection in underwater environments.









The strong performance metrics, including high accuracy, precision, and recall, demonstrate the reliability of this approach. The system not only minimized false alarms but also ensured that critical anomalies were rarely overlooked. This balance is essential for real-world use, where both false positives and false negatives can have significant implications for operational efficiency and safety.

One notable achievement was the model's robustness in noisy environments. Noise is an inevitable factor in sonar data, and the system's ability to maintain performance in such conditions underscores its practicality for deployment in real-world scenarios. However, while the results are promising, further research could explore optimizing the GAN and machine learning models to handle even more diverse datasets and extreme noise levels. Overall, this study demonstrates that integrating GANs with machine learning offers a scalable, reliable, and adaptable solution for anomaly detection, paving the way for advancements in underwater exploration and monitoring technologies.

V. FUTURE SCOPE

Future work could include integrating real-time data streams from sonar systems, improving the model's ability to detect subtle anomalies, and experimenting with other generative models or hybrid approaches. Additionally, further work on optimizing the model's efficiency for largescale datasets and enhancing its robustness in noisy environments would improve its performance in practical applications. While this study achieved promising results, there are several areas for future enhancements to improve the system's performance and applicability. One potential improvement is expanding the dataset to include a broader range of sonar signals from different environments and conditions. Incorporating data from diverse sources would help the system generalize better and adapt to varied scenarios.

Another area for enhancement lies in optimizing the GAN architecture. Exploring advanced variants of GANs, such as conditional GANs or Wasserstein GANs, could further improve the quality of synthetic data and make the anomaly detection process even more precise. Additionally, integrating advanced machine learning algorithms, such as deep reinforcement learning, may enable the system to learn more complex patterns and improve detection accuracy.

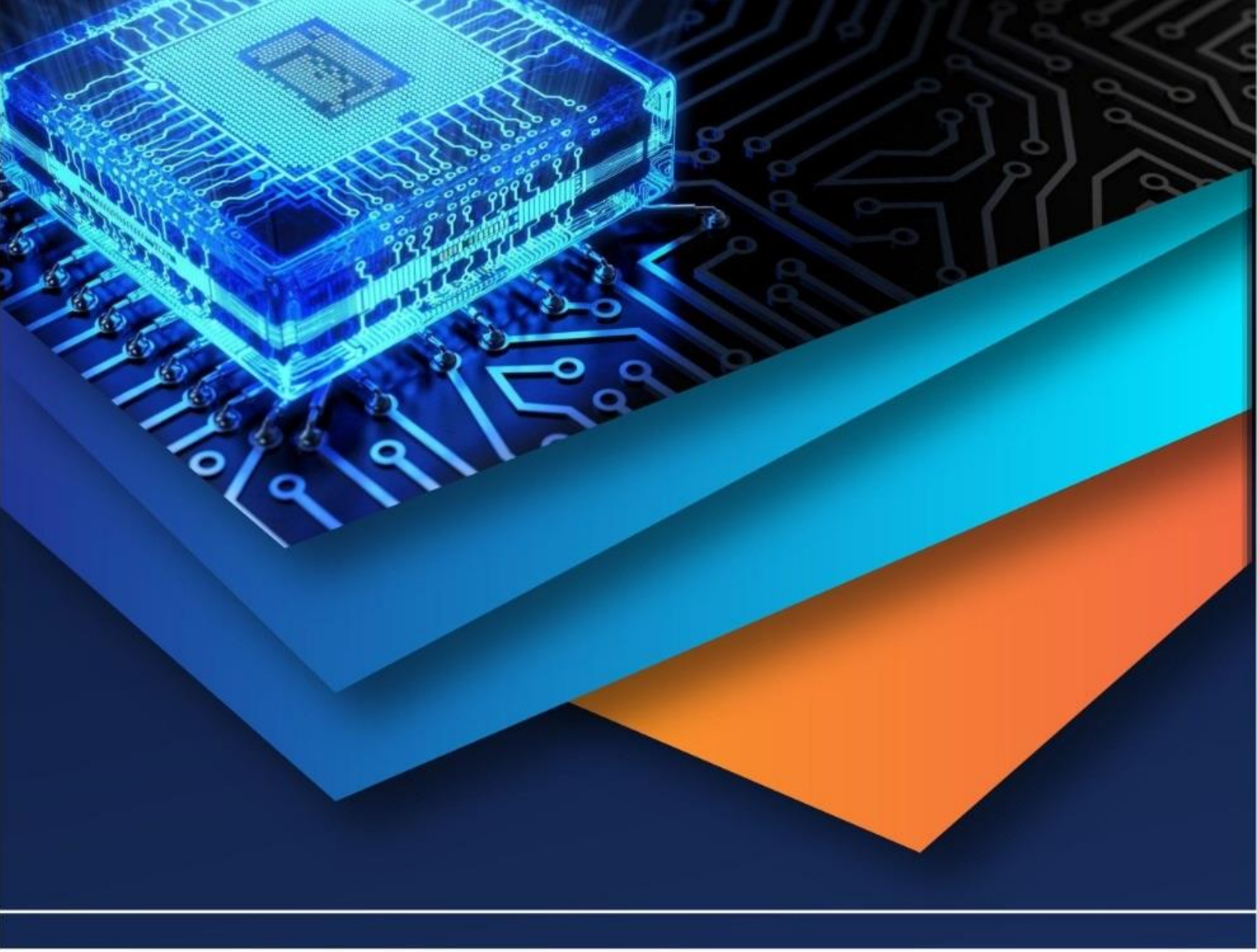
Real-time processing is another critical aspect for future work. Enhancing the system's computational efficiency to allow for real-time anomaly detection could expand its applications in dynamic underwater operations. Moreover, incorporating explainable AI techniques would provide users with insights into the decision-making process, increasing trust and usability in practical settings.
Finally, future research could explore adapting this approach to other domains where anomaly detection is critical, such as medical imaging, industrial monitoring, or cybersecurity. By extending the methodology beyond sonar systems, this framework could offer broader applications and greater impact

VI. CONCLUSION

The GAN-based anomaly detection system for sonar data has proven to be an effective method for detecting abnormal sonar signals in a variety of environments. The model demonstrated high precision and recall rates, ensuring reliable detection of anomalies that may indicate potential threats or irregularities. This study demonstrates the effectiveness of integrating Generative Adversarial Networks (GANs) with machine learning techniques for detecting anomalies in sonar data. The proposed approach addresses key challenges in sonar systems, such as identifying subtle irregularities and handling noisy environments. By leveraging GANs, the system was able to generate realistic synthetic sonar data, which enhanced the training process and improved the model's ability to distinguish between normal and anomalous patterns.
The results indicate high accuracy, precision, and recall, showing the system's ability to reliably detect anomalies while minimizing false positives and negatives. This balance is crucial for practical applications in underwater exploration, navigation, and defense.
Additionally, the system's resilience in noisy conditions highlights its adaptability to realworld scenarios, where signal interference is a common issue.
In conclusion, the combination of GANs and machine learning represents a powerful tool for anomaly detection in sonar systems. This research not only provides a robust solution but also sets a foundation for further advancements in the field of underwater signal analysis and monitoring.

REFERENCES

[1] Zhang, H., & Wang, W. (2021): "Anomaly Detection in Time Series Data Using Machine Learning Techniques." IEEE Access, 9, 12053-12066.
[2] This paper explores various machine learning models for anomaly detection in time series data, which can be adapted for sonar signals.
[3] Goodfellow, I., et al. (2014): "Generative Adversarial Nets." Proceedings of NeurIPS 2014, Montreal, Canada.
[4] The foundational paper on GANs, describing their architecture and potential applications, including anomaly detection.
[5] Schlegel, C., & Diederich, F. (2020): "Anomaly Detection and Classification in Sonar Data." Journal of Underwater Acoustics, 3(1), 30-42.
[6] Discusses methods for detecting anomalies in sonar data, including the use of machine learning algorithms and signal processing techniques.
[7] Cui, S., & Wang, X. (2021): "Deep Learning for Sonar Data Analysis and Anomaly Detection." Ocean Engineering, 233, 108865.
[8] This paper investigates the application of deep learning techniques, including GANs, to analyze and detect anomalies in sonar data.
[9] Radford, A., Metz, L., & Chintala, S. (2015):"Unsupervised Representation Learning with Deep
[10] Convolutional Generative Adversarial Networks." ICML 2015.
[11] This paper presents the use of deep convolutional GANs (DCGANs), a useful architecture for analyzing complex sonar data.
[12] Jin, X., & Yang, X. (2019):"A Survey on Anomaly Detection Techniques in Network Security." IEEE Access, 7, 87394-87410.
[13] Provides an overview of anomaly detection techniques, including machine learning models that could be adapted to sonar applications.
[14] Liu, Y., & Zhang, S. (2020): "Multimodal Sensor Fusion for Anomaly Detection in Autonomous
[15] Systems." IEEE Transactions on Robotics, 36(4), 1058-1067.
[16] Explores multimodal sensor fusion, relevant for integrating sonar data with other sensor types for enhanced anomaly detection.
[17] Chollet, F. (2017):Deep Learning with Python. Manning Publications.
[18] A comprehensive book that covers deep learning techniques and their applications, including GANs, which are highly relevant for this research.
[19] Rajasegaran, J., & Zhuang, Y. (2019):"Edge Computing for Real-Time
[20] Anomaly Detection in Industrial IoT
[21] Systems." IEEE Transactions on Industrial Informatics, 15(1), 40-50.
[22] Discusses real-time anomaly detection using edge computing, applicable for real-time sonar data processing.
[23] Ruder, S. (2017). "An Overview of Transfer Learning." arXiv preprint arXiv:1706.03860.
[24] This paper provides a detailed overview of transfer learning, which could enhance the adaptability of sonar anomaly detection models.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY