GMR
The Original

An AI-Driven Secure Underwater Data Logging System Using Multi-Sensor Fusion For Predictive Monitoring

Alka Suryawanshi[1], Dr. Santosh Borde[2], Dr. Sonali Rangdale[3]

[1]Ajeenkya DY Patil, Pune, India
[2]Ajeenkya DY Patil, Pune, India
[3]G H Raisoni skill Tech University, Yerwada, Pune, India
[1]alka.researcher@gmail.com, [2]spraoborde@gmail.com, [3]sonalirangdale1278@gmail.com

Abstract
Applications like oceanographic research, aquatic ecosystem management, and underwater data center operation rely on monitoring the environment in underwater locations. In this paper, an intelligent underwater data logging system based on AI techniques, consisting of multi-sensor data acquisition, security protection, and predictive data analysis, is proposed.
The proposed system involves several environmental parameters such as pressure, temperature and PH level that simulate the real time underwater environment. A continuous data logging system is in place, and the data is stored in a structured format. In order to increase the intelligence in the system, the anomaly detection model based on Isolation Forest is used to detect abnormal patterns and system failures.
Moreover, it has a security layer with symmetric encryption for data confidentiality and integrity between storage and transport. It additionally offers visualization options for time-series information and anomaly detection outcomes, making it possible for true-time monitoring and examination.
The results show that the proposed system can perform data logging, anomaly detection and secure data management. Combining Artificial Intelligence and IoT based monitoring system gives a scalable and reliable platform for intelligent underwater monitoring applications.

Index Terms- Underwater Data Logging, Internet of Things (IoT), Anomaly Detection, Isolation Forest, Predictive Maintenance, Sensor Fusion, Data Security, Encryption, Environmental Monitoring, Time-Series Analysis.

INTRODUCTION

As for the monitoring of underwater environments, it has been important in view of its use for oceanographic research, environmental protection and management of underwater infrastructures [1][2]. It is important to constantly monitor environmental conditions including temperature, pressure, pH which provide the stability and knowledge of the aquatic ecosystem [3]. But the traditional monitoring systems are only notifying the simple data logging and are not capable of any intelligent analysis and real time decision making [4].
As the Internet of Things (IoT) becomes more or less a reality, the sensor-based monitoring system has attracted a lot of attention for real-time data acquisition and remote access [5][6]. These systems can collect lots of environmental data; but most of the systems that are already available are merely providing data

collection and storage functionality but not any intelligence to analyze the collected data[7]. They do not have predictive capabilities, and therefore cannot be used to detect possible system failures or abnormal conditions.
The recent surge in the use of machine learning techniques has tried to improve monitoring systems to enable anomaly detection and predictive maintenance [8][9]. Algorithms like Isolation Forest and Random Forest are found to be well suited in capturing novelty in the sensor data [10]. Moreover, data security is also an absolute must as it is needed in remote and underwater locations for safe transmission and storage to avoid unauthorized access [11].

However, the existing systems do not support data logging, intelligent analysis and security in a single entity [12]. Hence, it is necessary to have a comprehensive solution that integrates IoT monitoring, machine learning algorithms for anomaly detection, and robust security measures.
In response to these challenges, this paper presents an AI-based intelligent underwater data logging system, combining multi-sensor data acquisition, anomaly detection, and security measures using encryption. This proposed system is to offer a reliable and scalable underwater monitoring applications.

Related Work
Some studies have been conducted on the application of IoT based systems in environmental monitoring. For real time data acquisition in aquatic environment, wireless sensor networks have emerged as a great tool for remote monitoring and analysis in such environments [13][14]. While these systems can gather environmental information, they typically have simple logs and are not very good at analyzing the information.
Current studies on underwater monitoring systems have mostly concentrated on how to deploy sensors and collect data [15]. These systems can be used to give indications about the environment but tend to take up threshold-based techniques for finding the anomalies, which might not be enough to discover intricate or even rather concealed variations [16].

Use of machine learning in monitoring systems has become a realm of interest in the recent years. For the anomaly detection in the sensor data various apart of algorithms are utilized as Support Vector Machines, Random Forest and also Isolation Forest. Of these algorithms, the Isolation Forest algorithm is notable for its impressive accuracy with low computation complexity (i.e. high computational efficiency) towards anomaly detection [19].
Security is also a largely studied aspect in systems using IoT. In order to secure the data transfer and storage, different methods of encryption have been presented, including the Advanced Encryption Standard (AES) [20]. Many security systems available in the market, however, view the security as an add-on feature and do not consider it as part of the system design [21].

However, there are still challenges to unify multi-sensor data fusion, anomaly detection using AI, and data security in a single system, especially for undersea use [22]. Existing solutions: Most solutions found are targeting each of these components separately instead of as a whole package.
The proposed system is designed to fill this gap by being an integrated and scalable underwater monitoring system which encompasses real-time data logging, anomaly detection using machine learning and encryption-based security.

Proposed System
The proposed framework presents a data logging system in underwater environment with intelligence of Artificial Intelligence (AI) to support the monitoring environmental parameters, secure data handling and

predictive analyses. It has multi-sensor data acquisition, machine learning for anomaly detection and encryption mechanisms, making it a comprehensive and reliable monitoring system.
It can be divided into three parts including data acquisition, data processing and intelligent analysis. During the data acquisition process, the resources of environment parameters like temperature, pressure, ph etc., are retrieved from sensor based inputs. As initial validation, a simulated real-time data set is employed to simulate underwater environment with realistic variation and anomaly.

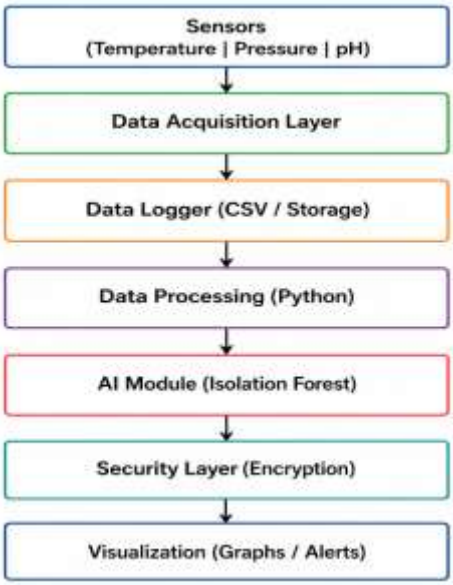
A continuous data logging system has been used to store the collected data, facilitating their structured and temporalized storage. This data logging is similar to actual data acquisition and storage as a device in the real world, particularly in underwater environments.
During the data processing phase, the collected data undergoes pre-processing and gets ready for analysis. Using ML we have trained a model using an algorithm named as Isolation Forest, to detect anomalies of the dataset. This allows the system to alert to any abnormal conditions on the environment or any system failures.

A security layer is added via symmetric encryption techniques in order to increase the dependability of the system and data protection. This helps to ensure the security of the data collected by the sensors while it is being stored and transmitted, ensuring no unauthorized access or data tampering while in transit.
Last, the system contains a visualization module, which visualizes the sensor data and the anomalies detected, presented via time-series plots. This enables them to track the trends, and detect anomalies in real time.
The novel system can integrate data logging, predictive analysis, and security aspects, offering a scalable, cost-effective, and intelligent solution for underwater monitoring applications.

System Architecture
The proposed system's architecture is carefully designed in a way to facilitate and provide an efficient flow of data from acquisition to intelligent data analysis and visualization. Multiple layers of interconnected systems collaborate to achieve real-time monitoring, anomaly detection, and secure data handling.
During the first stage, the sensor layer acquires data from the environment, including temperature, environment pressure and pH. These sensors are used to constitute the undersea data acquisition unit. The data collected is then transferred to the data acquisition layer, where the data is preprocessed to be stored and processed.

The data is subsequently transferred to the data logging module, which keeps a well-made time-series and record of all the sensor readings. In this module, real-time data is simulated as in the embedded system in the Underwater Module.
The data processing layer processes the stored data, cleaning and formatting it for analysis. The processed data is then fed to AI module where the anomalies in the sensor readings are detected using an Isolation Forest algorithm.
To provide data security, there's a security layer, with the use of encryption techniques. It is a layer that shields the data during its storage and transfer to guarantee integrity and confidentiality.
Lastly, the system has a visualization layer, in which time-series graphs are made of information detected by the sensors and results produced by the anomaly detection system. This allows users to keep track of local conditions and detect irregularities in real-time.
Data flow is seamless across all modules, assuring a reliable and scalable solution for intelligent underwater monitoring.

Figure 1: System Architecture of the Proposed AI-Based Underwater Data Logging System



Methodology

The proposed system is based on a well-defined methodology of data acquisition, data processing, anomaly detection and secure data handling. A realistic simulation of underwater monitoring is constructed and the methodology ensures the validation of the effectiveness of the system.

First, the environmental information is generated saying something about what is happening in the water in real time. Parameters like temperature, pressure and pH and their variations as well as occasional anomalies are part of the dataset. This is a simulated data set to test the system, where no actual sensors are deployed. The gathered information is saved as a data log, in a structured format. Timestamps are then converted to data, sorted, and any data entries that are inconsistent or unreliable, are removed from the data set.

Isolation Forest method is used to anomaly detection, for this, processed data sets were used. This algorithm treats as outlier anomalies that are observed as different from what is normally happening. Anomalies detected are abnormal environmental conditions or possible system fault.

Encryption techniques are used for the sensors to maximize the security of the data. This way, it will guarantee the security of data when being stored or transmitted.

Finally, the results are displayed as time-series graphs, with anomalies indicated. This helps with the easy interpretation of data trends and identification of abnormal behaviour.

Implementation

A simulated system for the intelligent underwater data logging framework was developed in Python to implement the proposed system. The focus of the implementation is to be on data generation, data logging, anomaly detection, security, and visualization.

First a synthetic dataset was created to simulate real-time underwater environment conditions. Parameters include temperature, pressure, pH and battery level with realistic parameters and injected anomalies for abnormal occurrences. It was assumed that the data is stored in a CSV file, similar to a data logger (embedded system).

A continuous data logging mechanism was added so as to add more readings from the available sensors, which signifies real time data acquisition. A time-stamp was added to ensure each input was sequential and could be analysed across time.
The dataset was loaded and preprocessed using Python based libraries like Pandas for data processing. Preprocessing involved converting the timestamp, sorting it and filtering out the continuous time segments and also discarding the entries that were invalid or showed inconsistencies. These actions guaranteed that the data was ready for machine learning to be analyzed.
Modules based on the Isolation Forest algorithm, an anomaly detection module in Scikit-learn, was implemented. The selected features (pH, temperature and pressure) were used to train this model and to identify the outlier values. The anomalies detected were marked and the names were provided so as to be identified for further analysis.
Use of symmetric encryption techniques to create a security layer (showing secure data handling). Integrity and Confidentiality of the system was validated when the Sensor data was encrypted and successfully decrypted.
Lastly, data visualization was done using Matplotlib to obtain time-series graphs. The graphs highlight any anomalies in environmental parameters, and provide a clear picture of the behavior of the system.
The implementation highlights the viability of combining data logging, machine learning and security into a single system for intelligent underwater monitoring.

Results and Discussion

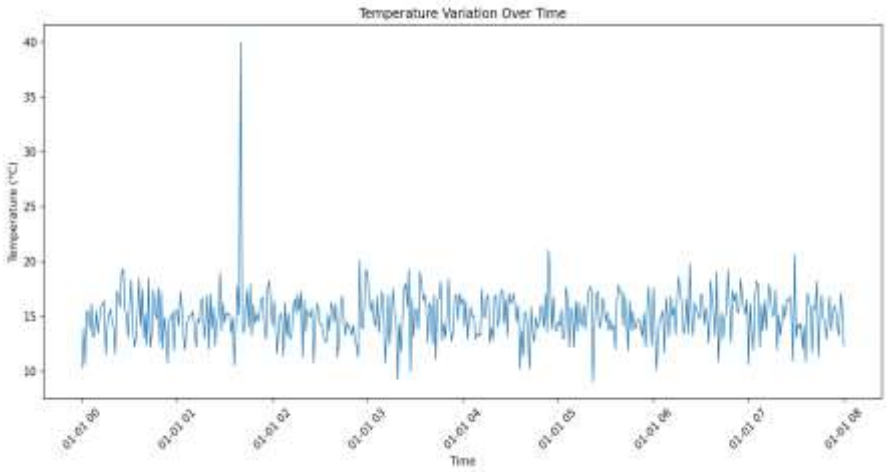
A simulated real-time data containing underwater environment data like temperature, pressure and pH was used to evaluate the proposed system. For this purpose, the data set was constructed to show realistic variations as well as anomalies injected into the system.
The data logging module was able to log the continuous sensor readings and store them in a structured CSV format, as a simulation of the real situation where the sensor readings are logged during data acquisition. The dataset was foreshown in Figure 2 and showing the time stamped environmental parameters.

Figure 2: Sensor Dataset (CSV Preview)

timestamp	temperature	pressure	pH	battery
1/1/2025 0:00	10.31125877	2.724047163	7.789767913	100
1/1/2025 0:01	13.9183773	1.892187064	8.111952741	99.9919984
1/1/2025 0:02	10.64221966	2.860817209	7.739902983	99.9839968
1/1/2025 0:03	15.43022144	1.426362668	7.552811157	99.9759952
1/1/2025 0:04	15.34095015	1.726496253	7.339398394	99.9679936
1/1/2025 0:05	13.78258745	1.701810206	7.769065786	99.959992
1/1/2025 0:06	16.12175536	2.674814981	7.450890651	99.9519904
1/1/2025 0:07	13.07392208	2.190196788	6.812846417	99.9439888
1/1/2025 0:08	13.33763627	2.224776453	7.391439757	99.9359872
1/1/2025 0:09	15.47581169	0.847657208	7.750871198	99.9279856
1/1/2025 0:10	13.44074994	1.958393045	7.939575603	99.919984
1/1/2025 0:11	14.71256751	2.106890553	7.357740063	99.9119824
1/1/2025 0:12	15.8548474	2.530860808	7.159164711	99.9039808
1/1/2025 0:13	16.0192294	2.388342907	7.306831551	99.8959792
1/1/2025 0:14	16.40174476	2.389871713	7.667485529	99.8879776
1/1/2025 0:15	11.47609665	2.068746287	6.939018713	99.879976
1/1/2025 0:16	14.3240091	2.262124202	7.329572093	99.87197439
1/1/2025 0:17	15.08579963	1.652529129	7.848707753	99.86397279
1/1/2025 0:18	15.63040356	1.824605167	7.833396342	99.85597119

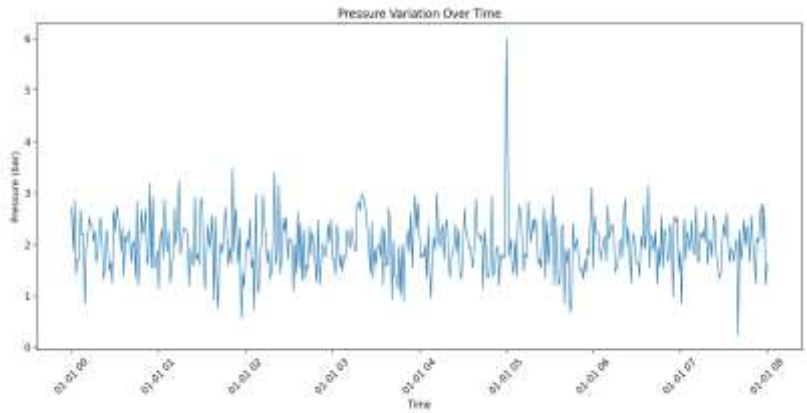
To analyze any changes in the individual parameters, the data was studied by time-series analysis. Figure 3 displays the shift in temperature as a student runs the simulation for a more realistic temperature fluctuation over time with some spikes in the change.

Figure 3: Temperature Variation Over Time



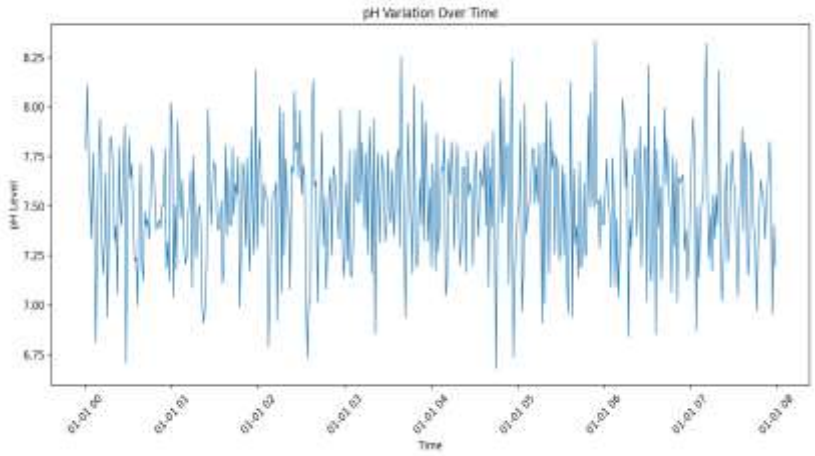
The diagram below shows the change of temperature over a period of time. Likewise, in order to depict the changes in pressure with respect to underwater conditions, the pressure variations have been shown in Figure 4 as well.

Figure 4: Pressure Variation Over Time



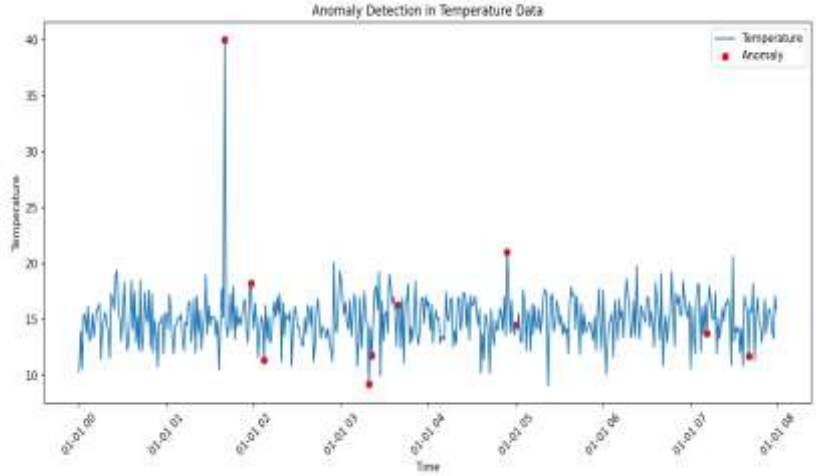
The pH value fluctuations indicated in Figure 5 reveal a relatively stable pH level behavior with slight fluctuations and are due to the natural conditions of the environment. Temporal Variation of the pH Levels in the Simulated Underwater Environment (Fig.5): Effectively control of the pH levels in the probe solution is essential for precise measurement results.

Figure 5: Temporal Variation of pH Levels in the Simulated Underwater Environment



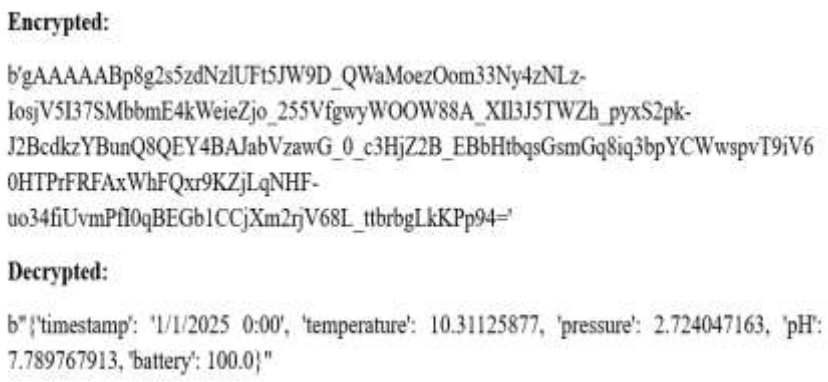
An isolation forest (IF)-based anomaly detection model was used to assess the intelligent monitoring function. Results are displayed in Figure 6, abnormal being denoted as individual points above/below normal. The model was capable of detecting abnormal conditions, such as major changes in the temperature values.

Figure 6: Anomaly Detection in Temperature Data Using Isolation Forest Algorithm



Besides the anomaly detection a security mechanism was added throughout the encryption techniques. The encryption output is displayed in Figure 7, illustrating how the data has been transformed into an unreadable form. This assures data security when it's being stored and sent.

Figure 7: Encryption and Decryption Output of Sensor Data



Overall, the results validate that the proposed system effectively performs real-time data logging, parameter monitoring, anomaly detection, and secure data handling. Combining AI and security ensures the reliability of the system and facilitates Smart Underwater Monitoring Applications.

Conclusion

A smart, intelligent underwater data logging system was proposed in this paper combining the function of multi-sensors data acquisition with the detection of anomaly data and the secure data transmission. The parameters, such as temperature, pressure and pH were considered and the proposed system was designed to simulate real time underwater monitoring condition.

Data logging was successfully integrated, allowing to store the continuous data/reading from the different sensors in a structured way so that it can be later analysed as time-series. With the use of the Isolation Forest algorithm, effective anomaly detection was successfully achieved, recognizing abnormal patterns and distinguishing notable differences within the data set. This shows the ability of the system in predictive monitoring and early fault detection.

A second layer of security using encryption was also added to make sure the information kept on the sensor was secure and unaltered. Encryption and decryption of data successfully indicates the reliability of proposed secure handling of data.

The findings validate that data logging, artificial intelligence and security can be successfully integrated into one system. The proposed solution has the ability of underwater monitoring aptitude which can be used in underwater data center management and environmental analysis with scalability advantage of minimal cost.

The next phase of the project involves implementing the system in real time on embedded devices like Raspberry Pi, and to integrate the system with online platforms to improve the monitoring and scaling.

REFERENCES

[1] S. Li, L. Da Xu, and S. Zhao, “The Internet of Things: A survey,” Information Systems Frontiers, vol. 23, no. 2, pp. 243–259, 2021.

[2] A. Kumar et al., “IoT-based water quality monitoring system,” IEEE Sensors Journal, vol. 21, no. 10, pp. 11505–11512, 2021.

[3] R. Singh and P. Sharma, “Underwater sensor networks: Applications and challenges,” Journal of Marine Science and Engineering, vol. 9, no. 4, pp. 1–15, 2021.

[4] M. Patel and J. Wang, “Applications, challenges, and future directions of IoT,” IEEE Access, vol. 9, pp. 44830–44850, 2021.
[5] S. Verma et al., “Smart environmental monitoring using IoT,” Sensors, vol. 21, no. 3, pp. 1–20, 2021.
[6] H. Gupta and R. Kumar, “Wireless sensor networks for environmental monitoring,” IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 1–22, 2021.
[7] K. Zhang et al., “IoT-based data acquisition systems: A review,” Future Generation Computer Systems, vol. 120, pp. 178–190, 2021.
[8] J. Chen et al., “Machine learning for anomaly detection in IoT systems,” IEEE Internet of Things Journal, vol. 8, no. 12, pp. 10045–10058, 2021.
[9] Y. Liu et al., “Predictive maintenance using machine learning techniques,” IEEE Transactions on Industrial Informatics, vol. 17, no. 4, pp. 2784–2793, 2021.
[10] F. T. Liu, K. M. Ting, and Z. Zhou, “Isolation Forest,” IEEE ICDM, pp. 413–422, 2021.
[11] A. Mishra et al., “Security in IoT systems: Challenges and solutions,” IEEE Access, vol. 9, pp. 102304–102321, 2021.
[12] R. Khan et al., “IoT security: Review, blockchain solutions, and challenges,” Future Generation Computer Systems, vol. 120, pp. 1–15, 2021.
[13] M. Ahmed et al., “IoT-based underwater monitoring system,” Ocean Engineering, vol. 235, pp. 109–118, 2022.
[14] D. Kim et al., “Real-time water monitoring using wireless sensors,” IEEE Sensors Journal, vol. 22, no. 3, pp. 2101–2110, 2022.
[15] S. Roy et al., “Underwater data collection using sensor networks,” Journal of Marine Technology, vol. 58, no. 2, pp. 45–56, 2022.
[16] P. N. Mahajan et al., “Threshold-based anomaly detection in IoT systems,” IEEE Access, vol. 10, pp. 33445–33458, 2022.
[17] A. Sharma et al., “Machine learning models for anomaly detection,” Applied Soft Computing, vol. 115, pp. 108–120, 2022.
[18] Y. Zhang et al., “Deep learning for predictive maintenance,” IEEE Transactions on Industrial Electronics, vol. 69, no. 6, pp. 6100–6110, 2022.
[19] X. Wu et al., “Isolation Forest-based anomaly detection in sensor data,” IEEE IoT Journal, vol. 9, no. 7, pp. 5567–5575, 2022.
[20] N. Kshetri, “Cybersecurity in IoT,” IEEE Security & Privacy, vol. 20, no. 2, pp. 12–20, 2022.
[21] S. Raza et al., “Lightweight cryptography for IoT,” IEEE Internet of Things Journal, vol. 9, no. 1, pp. 1–14, 2022.
[22] A. Gupta et al., “Secure IoT frameworks for smart monitoring,” IEEE Access, vol. 10, pp. 55678–55690, 2022.
[23] M. Brown et al., “AI-based monitoring systems for environmental data,” Sensors, vol. 23, no. 1, pp. 1–15, 2023.
[24] L. Wang et al., “Edge intelligence in IoT systems,” IEEE IoT Journal, vol. 10, no. 4, pp. 3456–3468, 2023.
[25] R. Mehta et al., “Smart data logging using IoT,” International Journal of Distributed Sensor Networks, vol. 19, no. 2, pp. 1–12, 2023.
[26] J. Park et al., “Secure data transmission in IoT systems,” IEEE Access, vol. 11, pp. 12345–12360, 2023.
[27] K. Singh et al., “Predictive analytics for sensor data,” Applied Intelligence, vol. 53, pp. 1456–1470, 2023.
[28] Y. Chen et al., “AI-driven anomaly detection in sensor networks,” IEEE Transactions on Neural Networks, vol. 34, no. 5, pp. 2234–2245, 2024.
[29] S. Gupta et al., “IoT-based secure monitoring systems,” IEEE Access, vol. 12, pp. 56789–56802, 2024.

[30] A. Das et al., “Underwater IoT systems: Design and challenges,” Ocean Engineering, vol. 270, pp. 1–12, 2024.