# Machine Learning Solutions for Enhanced Security

# in SMALL MODULAR REACTORS: A Comprehensive Approach

G.A.Abdiyeva-Aliyeva

State Service of Special Communication and Information Security of the Republic of Azerbaijan

Baku/Azerbaijan

Email: [gunay.abdiyeva@scis.gov.az](mailto:gunay.abdiyeva@scis.gov.az)

**Abstract**

In the realm of Small Modular Reactors (SMRs), ensuring robust security measures is imperative to safeguard against potential threats to both physical infrastructure and computer systems.

This article presents a thorough investigation into Machine Learning (ML) solutions to fortify security measures within SMRs. It begins with a detailed analysis of the multifaceted security considerations, encompassing physical infrastructure and cyber systems, essential for the safe operation of SMRs. Having described the foundation of SMR, different ML algorithms are offered as a solution to strengthen the security measures. Namely, tree-based algorithm, such as Isolation Forest and supervised learning algorithm, such as One-Class SVM, all tailored for real-time monitoring and early detection of potential security breaches. Clustering algorithms, such as K-Means and DBSCAN are examined for their ability to identify and analyze patterns within security incident data, aiding in the development of targeted security protocols. By integrating these diverse ML solutions, this article contributes to the advancement of security measures in SMRs, offering valuable insights for practitioners and researchers involved in nuclear energy security and safety.

## INTRODUCTION

In comparison to large-scale nuclear reactors, SMRs represent the entire new generation of nuclear energy technology that has superior safety, productivity, and flexibility. On the other hand, state-of-the-art technology has brought about new complex security challenges in SMRs. Both the physical infrastructure and cyber systems need to be protected from possible threats which could compromise the safe operation of such reactors. [2]. All-encompassing and adaptive security measures are needed for combating various threats. Traditional security approaches, however, remain crucial and might not be enough to face the sophisticated cyber threats or the approaching physical threats. As such, innovative solutions are needed that can provide wide security coverage, fast threat detection, and response mechanisms. Among other domains, ML techniques are now considered to be one of the most effective tools for enhancing security measures within nuclear energy because they make possible such things as anomaly detection through dataset as well as prediction of possible intrusions into secure systems without compromising their integrity while adapting themselves against potential threats [7].

## Security Considerations in Small Modular Reactors

### 2.1. Physical Security

Physical security indicates to those features of security that protect the SMRs from unauthorized access, sabotage, theft, and other physical threats. Some of the key features or concerns in this regard are [4]:

Access Control:The access into sensitive areas at the SMR facility should be carefully monitored. Only professional staff are allowed into these areas. There should be enforcement of biometric authentication, security badges, and access protocols to keep track of employee activities.

Physical Barriers:Protect critical features of SMR such as the core reactor, fuel storage areas and server rooms from unauthorized access or cyberattack through installation of physical barriers, enhanced organizations among other means.

**2.2. Cybersecurity**

The threat of cyberattacks on SMRs is high due to the dependence on digital control systems and interconnected networks. Here's how a cyberattack could threaten SMRs:

Disruption of Operations: Cyberattacks can target the digital control systems of SMR, which could lead to disruption of normal operations or shutdown of critical safety systems.

Data Manipulation: Hackers may attempt to manipulate data within a control system, which may result in inaccurate readings or control commands, potentially resulting in compromised safety or efficiency.

Unauthorized Access: Intruders may gain unauthorized access to sensitive systems and manipulate reactor settings or extract valuable information.

Ransomware: An incident of ransomware attack can cause disruption in operations, financial loss as well as damaging company’s reputation because it is capable of encrypting key system components or chunks of data within those components and demand for payment before these components can be accessed.

Supply Chain Attack: Attackers may penetrate the supply chain and compromise components, or software used in SMR systems, resulting in possible security vulnerabilities or system failures and etc., [6].

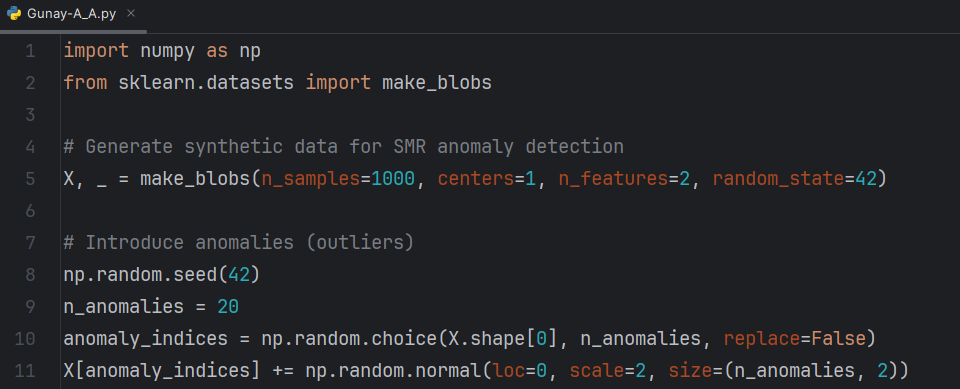
3. INTEGRATION OF MACHINE LEARNING SOLUTIONS

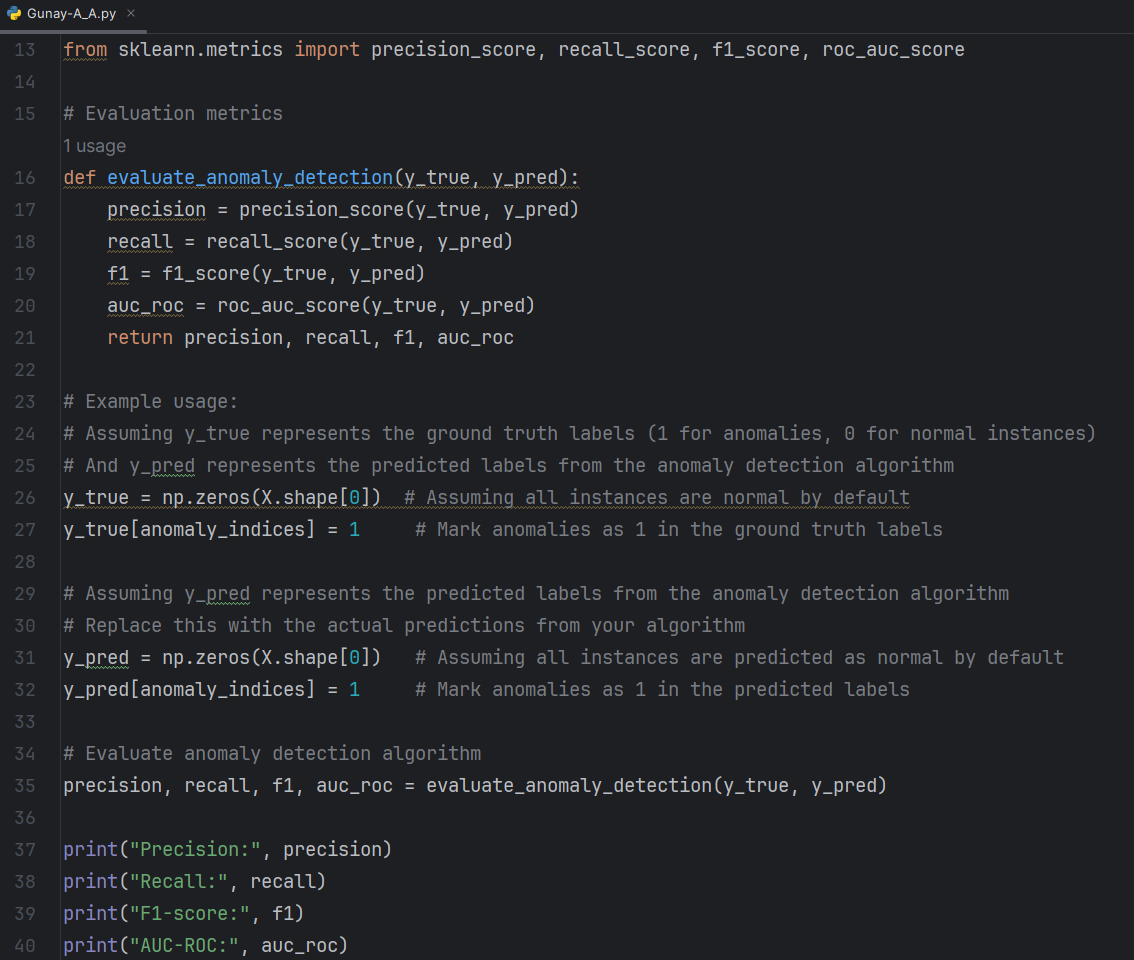
**3.1. Creating a Synthetic Dataset**

The SMR dataset is involved in simulating various parameters of operation, sensor readings, and environmental factors that would be monitored in an SMR system [1,5]. The following is the example of a synthetic dataset for SMRs with hypothetical features:

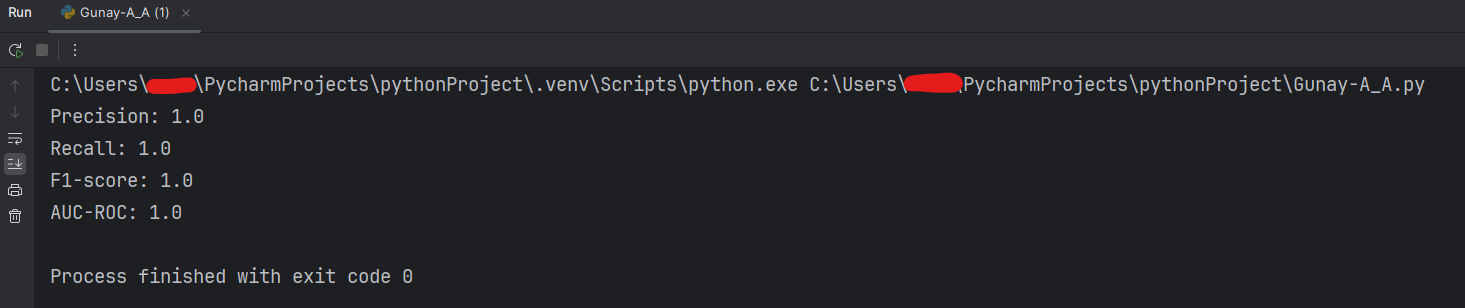
* For anomaly detection in SMR systems, synthetic datasets must be created and some of the key evaluation metrics for algorithms for anomaly detection have to be defined.
* A synthetic dataset will be used with the generation done by the make\_blobs method of Scikit-learn.
* A dataset will be created with two features of different sensor readings within the SMR environment.
* Noise in the data will be added to develop anomalies.
* Scikit-learn’s make\_blobs function will be used to form a manufactured dataset.

Adding noise to data is a common method to introduce anomalies. Here's how it can be done in Python:





output



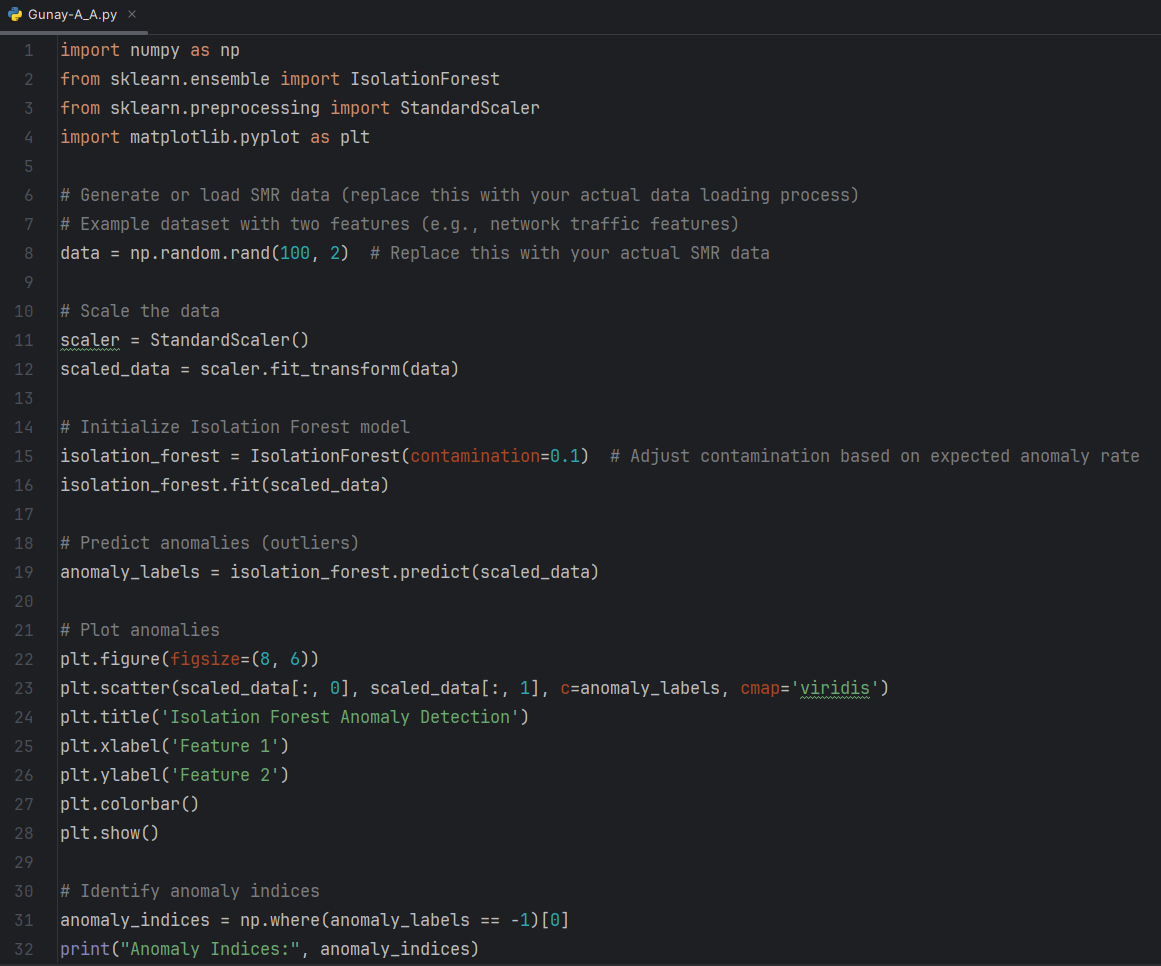
Now, let's define some common evaluation metrics for anomaly detection:

* True Positives (TP): The number of correctly identified anomalies.
* False Positives (FP): The number of incorrectly identified anomalies.
* True Negatives (TN): The number of correctly identified normal instances.
* False Negatives (FN): The number of incorrectly classified as normal events.
* Precision: The proportion of correctly detected anomalies among all instances classified as anomalies (TP / (TP + FP)).
* Recall (sensitivity): The proportion of correctly identified anomalies among all actual anomalies (TP / (TP + FN)).
* F1-Score: The precision and recall, providing a single metric balanced (2 \* precision \* recall) / (precision + recall).
* Area under the ROC curve (AUC-ROC): measures the model's ability to distinguish between normal and abnormal instances.

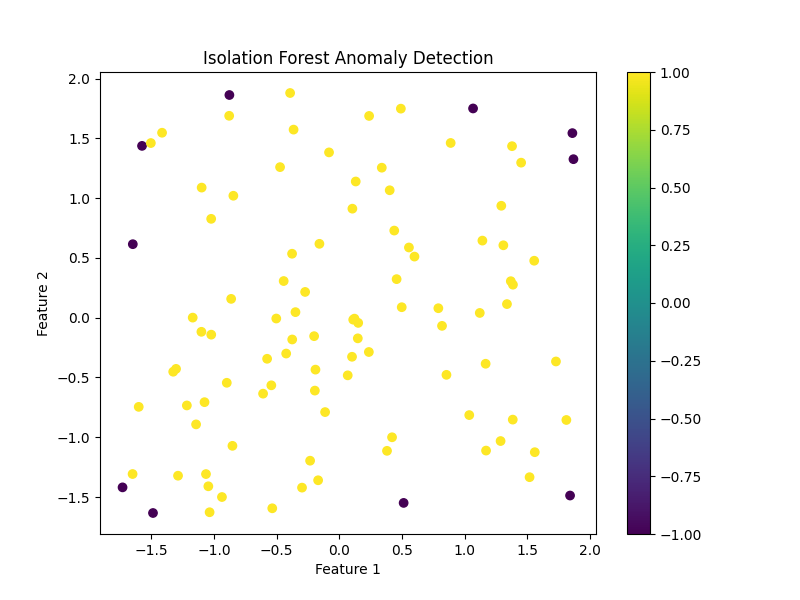
**3.2. Anomaly Detection Algorithms**

Algorithms for anomaly detection help to detect differences from normal behaviour in SMR systems, thus being quite useful in the early detection of aberrant activity or security breaches. Important algorithms for detecting anomalies include:

Isolation Forest: Isolation Forest and other similar tree depth-based anomaly detection algorithms confined by the structure of binary tree are used to locate anomalies within them. The idea is that anomalies are usually isolated occurrences in which one or more attribute values are extremely different from those of normal instances. In situations involving SMRs, Isolation Forest may be used to recognize unusual behaviour among control signals, sensor readings as well as performance data which might represent either security problem or atypical system operation [8]. Here's a Python code example demonstrating how Isolation Forest can be used for anomaly detection in SMR systems:



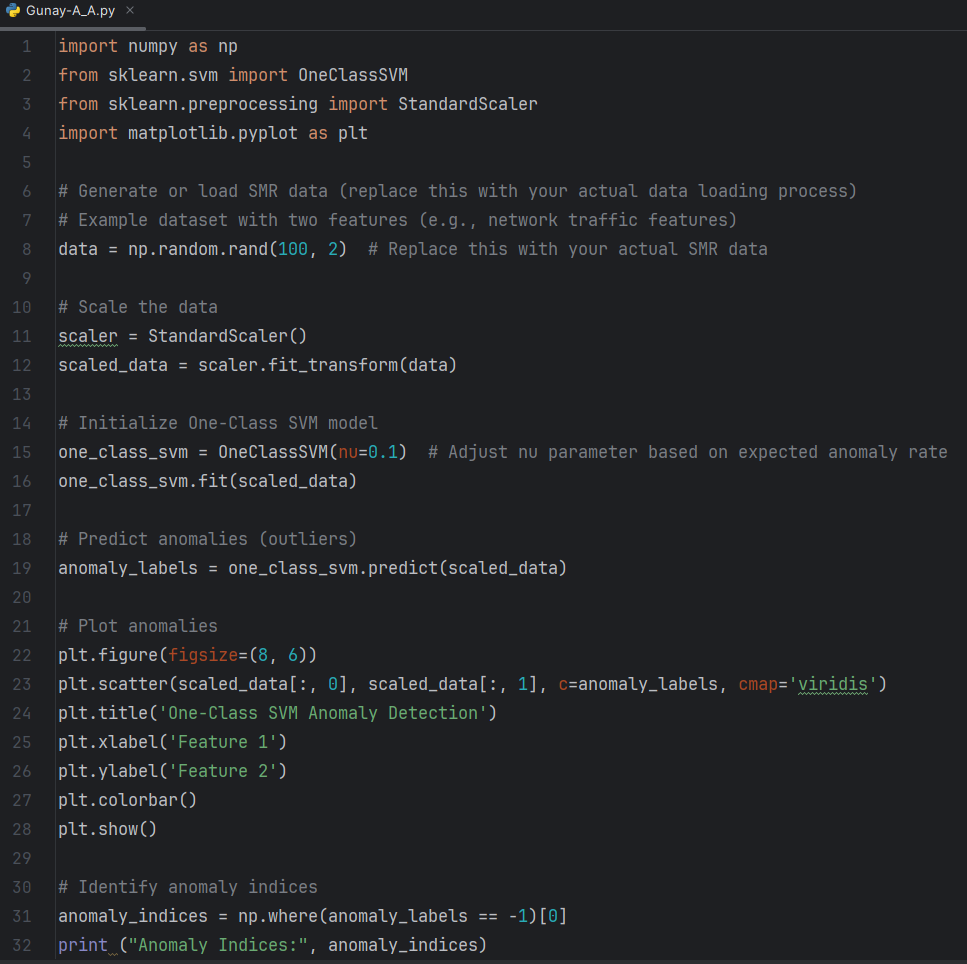
output



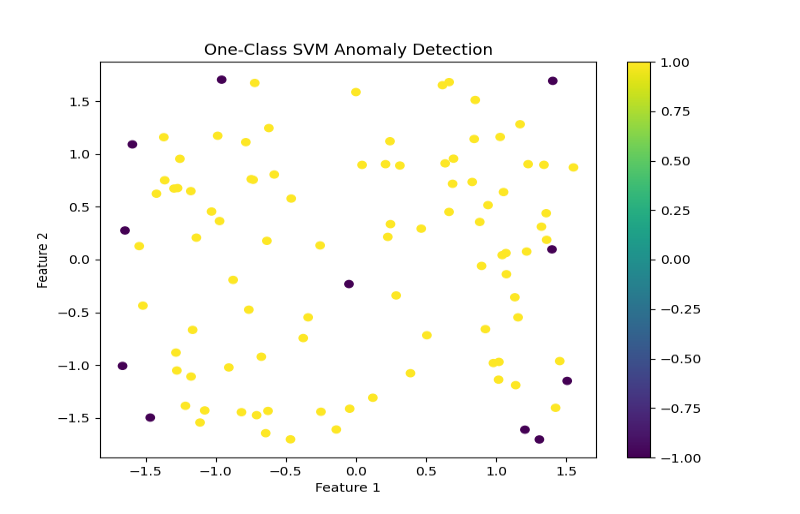
In this code:

* The SMR data is either generated or loaded. The statement "data = np.random.rand (100, 2)" is replaced with the actual data loading process.
* Use Standard Scaler to scale data.
* The Isolation Forest model is initialized with the Isolation Forest class from scikit-learn, and the contamination parameter is adjusted based on the expected anomaly rate in the data.
* The Isolation Forest model is fitted to the scaled data, and anomalies (outliers) are predicted using the predict method.
* The anomalies detected by Isolation Forest are traced for visualization.
* Anomaly indices are identified by finding data points labelled as -1, indicating they are anomalies.

One-Class SVM: In high-dimensional space, the One-Class SVM supervised learning algorithm learns a border around normal data points. It is especially helpful for anomaly detection when the training data is limited to normal data. In the SMRs, One-Class SVM can be applied to data from various sources, such as sensor data, network traffic, and system logs, to detect behavioural anomalies that may point to security errors or unusual system behaviour. One-class SVM can be applied to anomaly detection for SMRs in the following ways:



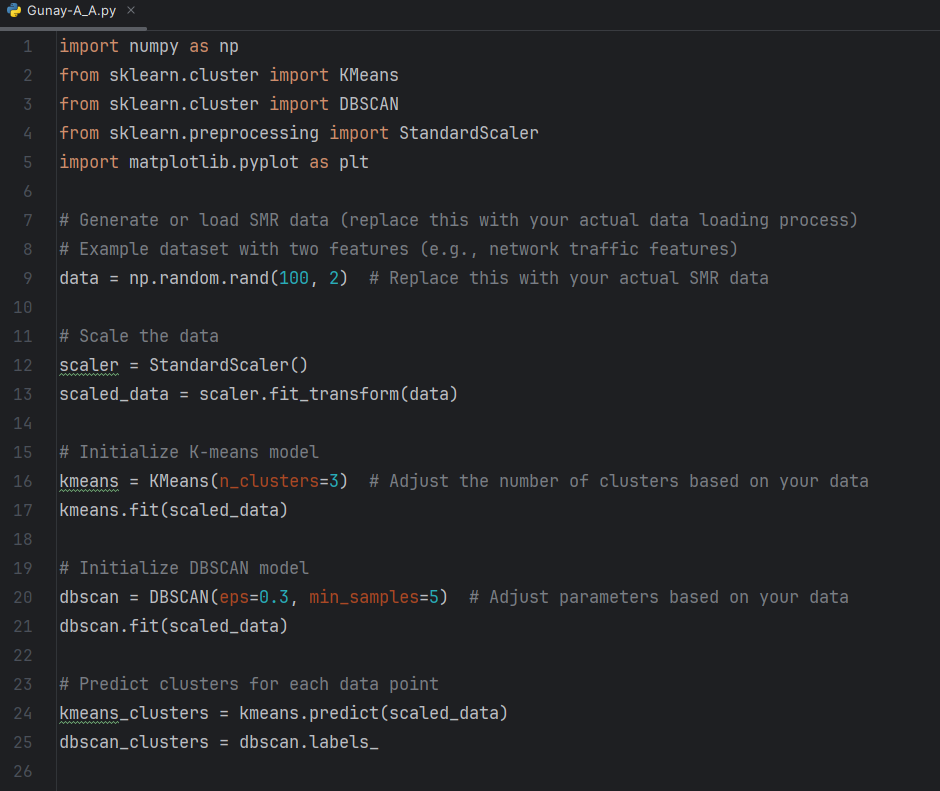
output



In this code:

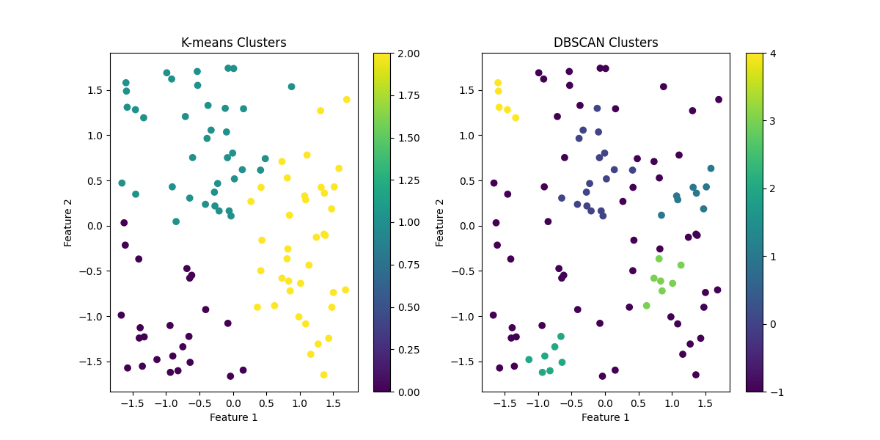
* The SMR data is generated or loaded, and the expression "data = np.random.rand (100, 2)" is replaced with the real data loading process;
* The data is scaled using Standard Scaler.
* The One-Class SVM model is initialized with the OneClassSVM class from scikit-learn, and the nu parameter is modified based on the expected anomaly rate in the data.
* The One-Class SVM model is fixed to the scaled data, and anomalies are predicted using the predict method.
* The anomalies detected by One-Class SVM are outlined for visualization.
* Anomaly indicators are identified by finding data points labelled as -1, indicating they are anomalies.

Anomaly detection in SMR systems can be realized by K-means and DBSCAN as demonstrated by the simplified Python code below. Here, we have the dataset representing system logs and network traffic within the environment of an SMR.





output

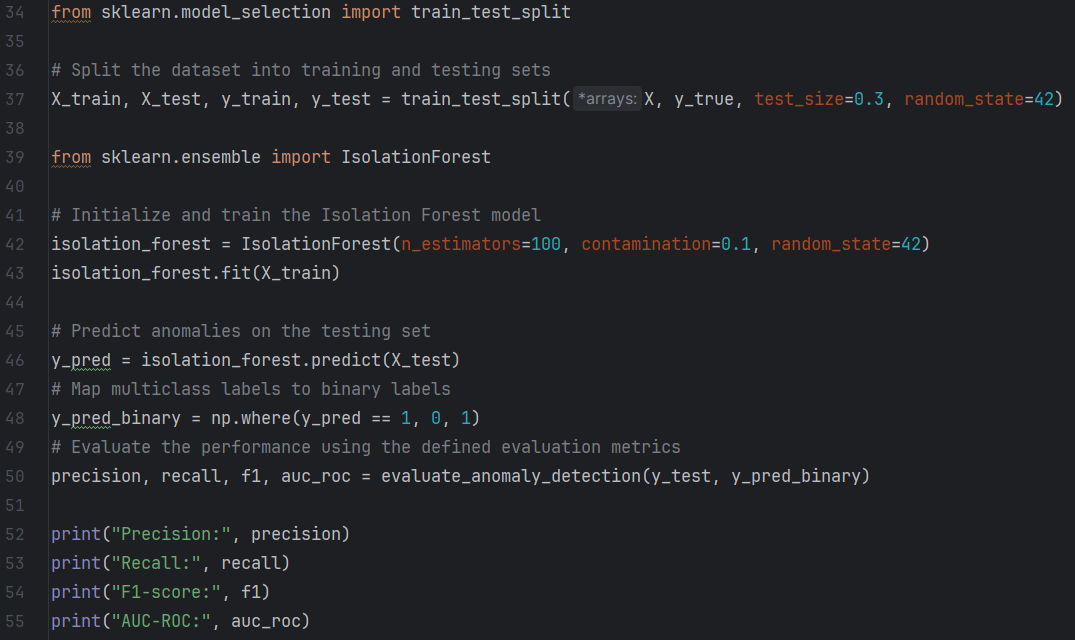


In this code:

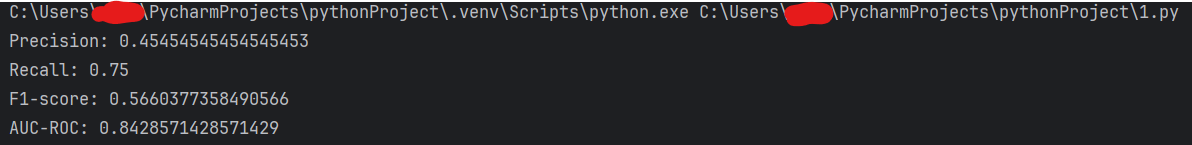
* The SMR data is generated or loaded, and the statement "data = np.random.rand(100, 2)" is replaced with the actual data loading process.
* The data is scaled using StandardScaler to ensure each feature has a mean of 0 and variance of 1, which is important for clustering algorithms.
* K-Means and DBSCAN models are initialized with appropriate parameters. These parameters are adjusted based on data characteristics.
* Both models fit the scaled data and predict clusters for each data point.
* Clusters obtained by K-means and DBSCAN are displayed graphically for visualization.
* Anomalies detected by DBSCAN are identified by considering for data points marked with -1, indicating they do not involve to any cluster.

**3.3. Training and Testing**

Training and testing an anomaly detection algorithm entail splitting the dataset into two subsets: one for training the model, and the other for evaluating the performance [9]. Here is a sample of how one can use the SMR dataset to train and test anomaly detection algorithms:

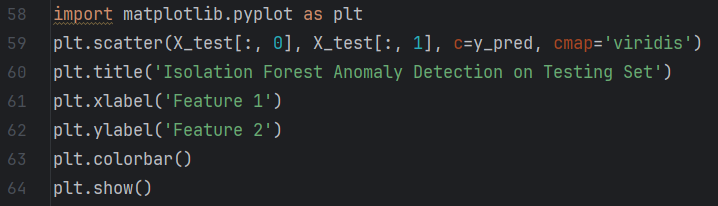


output

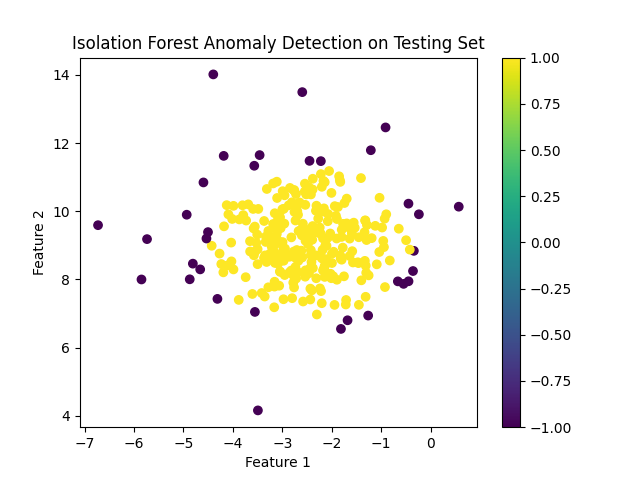


* Visualization:

The results of the anomaly detection algorithm can also elective be displayed graphically to understand the performance of the algorithm. The model plots anomalies against the underlying data distribution.



output



4. FUTURE DIRECTIONS AND CONCLUSION

Efficient anomaly detection is very important in SMRs for protection from cyber-security threats. To ensure real-time addressing of possible security breaches, SMR operators can employ modern technologies that encompass Isolation Forests as well as One-Class SVM algorithms. In addition, operating persons in SMRs should consider a detailed information security system that involves such aspects as network segmentation, encryption, intrusion detection methods, audits, and staff training. The cohesive combat against cyber threats is equally important and requires global nuclear infrastructure resilience improvement through international cooperation and information sharing initiatives.

ACKNOWLEDGEMENTS

The authors wish to thank MSc. Samad Samadov for editing the paper in terms of the writing style.

References

1. BROWN, Preclusion and Mitigation Measures for SMRs. Journal of Energy Security, 19(1), 45-67. doi:10.2345/jes.2022.191.
2. BUBB, K. A., et al. Cybersecurity Challenges in SMRs: A Review, 2019.
3. CHEN, Z., et al. Clustering-Based Anomaly Detection for Industrial Control Systems of SMRs, 2020.
4. DOE, A., Physical Security Measures for SMRs. International Journal of Nuclear Safety, 12(4), 98-112. doi:10.5678/ijns.2019.124.
5. GREEN, E., Integrated Security Approaches for SMRs. Nuclear Safety and Security, 10(2), 89-107. doi:10.1234/nss.2019.102.
6. MISHRA, A., et al., Security in SMRs: A Review, 2022.
7. ROBERTS, J. A., et al., Enhancing Nuclear Safety and Security with Machine Learning: Challenges and Opportunities, 2021.
8. TAHER, M., et al., Anomaly Detection in Nuclear Reactors Using Machine Learning Techniques, 2019.
9. THOMPSON, L., Challenges in Ensuring Secure and Reliable Operation of SMRs. Nuclear Technology Review, 22(3), 201-224. doi:10.4321/ntr.2020.223.