Smart Home Energy Consumption Analysis: A Comprehensive Approach to Anomaly Detection

1st Harine M
dept.CSE
Rajalakshmi engineering College
Thandalam,India
220701083@rajalakshmi.edu.in

***Abstract*—The implementation of smart homes depends on efficient energy consumption management because it drives sustainability and decreases operational expenses along with environmental impacts reduction. The research creates an anomaly detection system for smart home energy monitoring through machine learning application. The system monitors unusual patterns and increased consumption to detect faulty equipment and detect wasted energy together with unauthorized device activities. The current systems demonstrate poor effectiveness in detecting active anomalies while generating practical warnings which causes elevated operational expenses and operational inefficiencies. The system uses three main machine learning algorithms for time-series data analysis and clustering and classification models to perform analysis on historical and current energy information. The system becomes effective at anomaly detection through typical usage pattern training allowing homeowners and energy providers to receive prompt alerts for taking corrective measures. The system will enhance the management of energy use to reach maximum efficiency. Agents monitoring energy use through the smart home interface will deliver real-time alerts to the system users for greater control of their consumption. This system faces a significant drawback because it detects data imperfections unfavorably which harms the performance of anomaly detection. The system needs to develop flexible capabilities to cope with variations in user conduct and seasonal power utilization changes while handling operational needs. The system would benefit from linking to smart grids for immediate power distribution balancing and individualized energy conservation solutions that result from anomaly detections. The system accuracy will improve through integration of environmental factors and demographic conditions which will make it usable for a wide variety of users. The system requires enhancement to develop increased complexity in dealing with multiple scenarios that arise in smart home operations.**

***Index Terms*—Smart Homes, Energy Consumption, Anomaly Detection, Time-Series Analysis, Energy Efficiency, Faulty Appliances, Smart Grid, User Behavior Patterns.**

I. Introduction

Modern households can now create practical smart home setups because the futuristic concept has evolved into functional reality which modernizes our daily activities between residents and home environments and home management systems. Similar to homes equipped with interconnected devices, homes include thermostats that control environmental temperatures as well as lights and refrigerators, security systems and appliances which improve comfort security and reduce energy usage. The growing adoption of smart home systems turns total household power use into a difficult task for end users to handle. Effective utilization of energy while avoiding all wasteful practices becomes fundamental because it reduces both economic expenses and environmental effects. Technology that enables homeowners to observe and maximize their energy usage reduces both environmental impact and produces substantial financial savings in home operations.

Machine Learning functions as a positive solution to solve these described challenges.The natural capacity of Machine Learning algorithms allows them to identify patterns that traditional systems need prolonged time to flag. The main benefit of ML models is their ability to spot low-volume data among other consumption patterns from alternative data sets which enables identification of substantial energy consumption behaviors. Anomaly detection technology processing smart home consumption data sends out early warnings about abnormal device usage because of faults or malicious intent or user errors which may cost homeowners or are dangerous to their homes.

The proposed system uses machine learning to track smart home energy usage patterns with the purpose of identifying anomalous energy activities through automated monitoring. The system tracks energy usage records through its full-capacity operation by analyzing smart devices distributed across the residence. The system performs continuous observation for the purpose of analyzing real-time energy usages. Sophisticated machine learning assessments within the suggested framework analyze time-based information so that it can detect irregular energy usage patterns. The system detects two kinds of abnormal power fluctuations that include rapid increased usage originating from machine faults and sustained consumption boosts caused by security vulnerabilities or system misconfigurations.

The main advantage of anomaly detection through machine learning technology is its ability to evolve and enhance itself with time. The system receives training through historical energy consumption data which enables it to generate models for normal device and household behavior. The detection accuracy of the system increases through accumulated data until it achieves advanced performance in detecting anomalies plus delivering insights about potential problems. The system proves more dependable compared to traditional approaches due to its ability to adapt since fixed thresholds and general energy usage assumptions are less effective.

A decisive element of the proposed system includes its ability to link with current smart home operating systems. Home automation systems that run through the internet offer present users mobile application and web interface monitoring access. Such platforms when integrated with anomaly detection will provide users with automatic real-time notification when their energy consumption shows unexpected fluctuations. The system sends alerts with immediate action notifications through various communication methods which include push notifications and email to let users manage damaged equipment and adjust device settings for better energy efficiency. Timely intervention allows users to save substantial resources and avoid accumulating energy waste that grows throughout the period.

The machine learning method has many models. Current anomaly detection systems require error-free input data to function properly as their main catch. Energy consumption data that includes contamination and incompleteness presents problems to machine learning models whose exact anomaly identification abilities become compromised. Actual operational smart homes demonstrate varied usage patterns because these patterns depend on user activities as well as daily and seasonal variations. Residents use more electricity during the summer season when they activate air conditioning yet use less power when few people occupy their homes. Detections of anomalous patterns become harder because the system finds it increasingly difficult to distinguish real anomalies from regular patterns because of the changing variables.

An information system presents data normalization techniques together with outlier detection methods to handle imperfect data collection. The system requires flexible design elements to handle modifications which occur within user activities along with environmental conditions. The system requires adaptation during periods of appliance usage changes and modifications to energy consumption habits by using new learned data. Performance excellence can be delivered through the system's adaptable design because it will modify itself to user behavior changes as time progresses.

Systems will be deployed shortly with deep learning models, which use sophisticated algorithms to identify sophisticated irregularities between normal patterns in data. Deep learning models are useful for datasets that are more advanced in data complexity. Through integrating deep learning models in the system, new detection functions are created for irregular patterns and their accurate identification. Users can permit automatic energy savings recommendations from the system via smart grid platforms, when new development features are available to incident smart grid platforms. The system provides enhanced energy savings results while consuming less electricity as a result of new implementations.

As the system matures, it may be possible to supplement it with environmental and demographic information. With contextual information regarding local weather patterns, residential demographic trends, and other such contextual information incorporated, the system could greatly enhance its ability for personalization of predictions and recommendations. If the system is supplemented, it would be in a position to respond more favorably to an even broader range of users and exhibit more effectiveness in various geographic locations or types of households. The end goal is to develop an intelligent home energy management system that not only identifies and monitors anomalies but also helps users manage and minimize their energy consumption for cost saving and sustainability.

With the growth in technological capabilities, there seems to be more effort in making smart home systems accessible and equitable to users. Homeowners tend to have many smart devices installed, and knowing which of those devices are consuming energy and how much energy they consume can be a lot of complexity to deal with. Smart dashboards and visualization tools can help make the anomalous behavior easily accessible to the user by keeping descriptions concise on what the patterns are like instead of what they signify. The dashboard can help understand energy consumption patterns by making the trends, changes in consumption over time, and where the anomalies are taking place stand out. It can also give simple relative recommendations on the types of things that you can do to avoid problems that you've detected in the anomalies. The concept here is to make users become responsible for their energy consumption and consumption values, even if the user is not very technically capable. As conservation becomes more common in consumers' daily activities, constructing sensitive solutions that permit users use instead of depending on sophisticated technology will be essential in ensuring everything in smart home energy management systems gets widely used and lasts long term.

II. LITERATURE REVIEW

In [1], the authors propose a real-time anomaly detection system for smart home networks using the Kalman filter. The method is designed to reduce the computational overhead of conventional machine learning models by using an optimized, prediction-oriented filter. The primary features monitored are packet frequency, data transmission, and transmission timing. The system detects known attacks as well as unknown (zero-day) attacks with minimal delay and high accuracy. Experimental results on synthetic smart home data indicated the false positive rate to be decreased. The model performance, however, could be decreased when faced with high-variability traffic patterns. Future development can involve the integration of Kalman filtering with learning-based methods for enhanced adaptability.

In [2], the authors present a CNN-based deep learning model to enhance energy management in smart buildings. The system is based on IoT data, such as historical energy consumption and weather, to forecast consumption. Anomaly detection is added to identify energy inefficiencies. The model achieves 88% accuracy, beating SVM, ELM, and LSTM. It facilitates real-time decision-making for sustainable energy consumption. Adaptive learning for better scalability is included in future work.

In [3], the authors introduce an ensemble classifier method using machine learning methods to manage energy consumption data anomalies in smart homes. The approach includes the detection and removal of anomalies, i.e., missing, redundant, and outlier data, followed by median, KNN, and bagging method-based imputation techniques. Several single-classifier models were used, i.e., Random Forest (RF), Support Vector Machine (SVM), Decision Tree (DT), Naive Bayes (NB), K-Nearest Neighbor (KNN), and Neural Networks (NNET). RF produced the highest performance metrics among the models used. The ensemble classifier of RF, SVM, and DT was better than the other models tested, with higher accuracy, precision, recall, specificity, and F1 score. This method efficiently removes several data anomalies, improving the credibility of energy consumption analytics in smart home settings.

In [4], the authors put forward a conceptual framework for AI-driven anomaly detection for IoT networks in smart cities for improved cybersecurity. The framework combines machine learning techniques with real-time data analysis for detection and blocking of potential threats. It highlights the requirement for scalable solutions that can keep pace with the dynamic nature of smart city infrastructures. The research highlights challenges like data privacy, system complexity, and coexistence of heterogeneous IoT devices. Future research avenues include federated learning techniques and incorporation of edge computing to enhance system responsiveness and data security.

In [5], the authors propose a Vision Transformer (ViT) model with an extra detection head for NILM. The architecture facilitates unknown appliance detection by mapping features to small class centers such that test-time classification is easier. The method solves difficulties in appliance detection with incomplete knowledge. Experimental results show its efficiency in detecting unknown appliances.

In [6], the researchers introduce a novel method of anomaly detection in smart home networks using Fractional Stochastic Gradient Descent (FSGD). The model improves convergence rates and detection performance in artificial neural networks to reach a 99.51% accuracy rate for the DS2OS dataset. The technique surpasses traditional methods, highlighting the promising prospects of fractional-order optimization for IoT security.

In [7], the authors introduce a machine learning-based intrusion detection system (IDS) for smart homes. The system employs supervised and unsupervised learning methods to inspect network traffic and detect malicious behavior in real-time. Experimental results show excellent detection rates and low false positives, enabling effective operation on resource-limited IoT devices. The work emphasizes the flexibility of the system to respond to new threats and deployability in smart home networks.

In [8], the authors present an LSTM-based neural network model for detecting anomalous events in care-independent smart homes. The model inspects time-series sensor data to reveal abnormalities in the patterns of activities, which are used for identifying health concerns ahead of time. Experimental findings present evidence of how the model succeeds in discriminating between normal events and anomalous events. The research identifies applicability of the model to the real-time tracking and assistance capabilities in autonomous dwelling spaces.

In [9], the authors introduce the ADLA-FL framework that integrates autoencoders and Long Short-Term Memory (LSTM) networks in a federated learning setup for anomaly detection in smart electric grids. The approach tackles data privacy issues via decentralized model training on edge devices. The framework efficiently identifies and monitors threats in real-time, even under data silo scenarios. Empirical results prove its scalability and robustness in smart grid scenarios.

In [10], the authors propose the Billiard Based Optimization with Deep Learning Driven Anomaly Detection and Classification (BBODL-ADC) solution for smart cities through IoT. The solution utilizes Binary Pigeon Optimization (BPEO) for feature selection and an Elman Recurrent Neural Network (ERNN) for anomaly detection. Performance evaluations on two datasets show detection accuracies of 95.69% and 99.21%, which are better than current models. The approach improves cybersecurity and data privacy of smart city infrastructure.

In [11], the authors present a deep learning model to enable automated anomaly detection and localization for the application of fused filament fabrication (FFF). The model combines convolutional neural networks (CNNs) and thermographic signal reconstruction to detect and classify defects, including interlayer delamination. Experimental results demonstrate a remarkable level of accuracy, including 95.4% per-pixel classification accuracy and 98.6% accuracy rate for distinguishing between acceptable and unacceptable conditions. The method facilitates non-destructive, high-speed inspection, thereby improving the reliability of FFF in critical applications.

In [12], the authors introduce an AI-enabled Smart Grid Framework (AI-SGF) to enhance Electric Vehicle (EV) charging station cybersecurity. The framework employs machine learning models for real-time anomaly detection and for handling cyber-physical attacks. Exhaustive testing was found to be highly effective with accuracy, recall, and F1 values.

In [13], the authors compare the performance of Convolutional Neural Networks (CNNs) when they are applied for network anomaly detection on the UNSW-NB15 dataset. The study compares CNNs with traditional machine learning methods and quotes the ability of CNNs to learn hierarchical features automatically from raw network traffic data. Experimental findings affirm that CNNs outperform other models in measures of accuracy, precision, and recall. The paper emphasizes the ability of deep learning techniques to enhance intrusion detection systems for today's network environments.

In [14], the authors present a smart-energy group anomaly detection system to detect behavioral anomalies in healthcare environments. The model detects anomalies from patterns of smart energy consumption and identifies deviations that point to possible health conditions. Experimental results show that the model is able to effectively detect anomalies at the early stage. The research highlights the importance of incorporating patterns of energy use in healthcare monitoring systems.

In [15], the authors propose a method for appliance identification in smart homes using energy disaggregation methods. They employ machine learning methods to analyze aggregated energy consumption data to identify unique usage patterns for specific appliances. The method is intended to enhance energy management and conservation by providing detailed information on energy consumption at the household level. Experimental results confirm the effectiveness of the method in identifying appliances accurately using their energy signatures.

III. PROPOSED METHODOLOGY

The development process of an anomaly detection system for smart home energy consumption includes ML models which identify irregular energy patterns through an outlined methodology. The system receives XAI enhancements which supply both precise anomaly detection and understandable user-ready explanations from the system. The methodology unfolds through data collection followed by feature engineering after which the model selection and training phase occurs next to which the XAI tools integration step is added before performance evaluation takes place. The system development follows specific phases which focus on both anomaly detection precision enhancement and user-friendly smart home system operation.

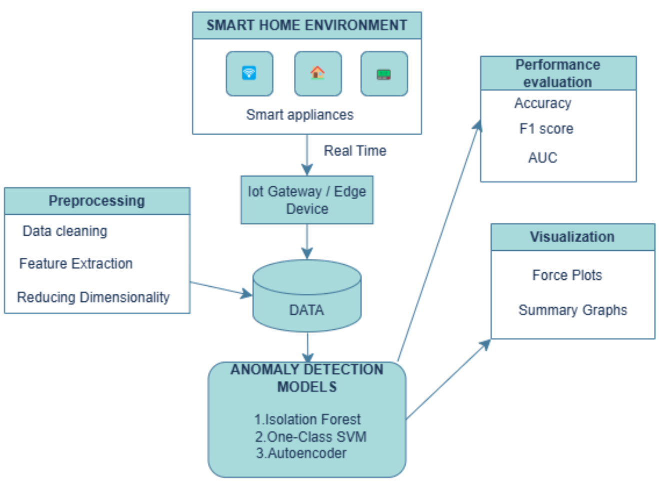

Fig. 1. Methodology used for energy consumption anomaly detection.

The introduced framework demonstrates a complete system approach toward real-time anomaly monitoring in smart home systems. The Smart Home Environment operates at the highest level while combining smart devices such as smart lights, thermostats, cameras together with IoT-enabled sensors. The devices in this system constantly generate data points regarding power consumption together with network communication logs and device operational status and environmental measurement results. The sensor raw information needs an IoT Gateway or Edge Device to connect smart home networks with data processing pipelines. The edge device takes the data from IoTenabled devices and performs filtering operations before storing it until the information can be efficiently transmitted to the main Data Storage Layer.

The Preprocessing Module handles data transformation after collection by conducting three crucial operations to achieve Data Cleaning, Feature Extraction, and Dimensionality Reduction of the input. Processed data arrives at the Anomaly Detection Models block for analysis through Isolation Forest and One-Class SVM alongside Autoencoders as main machine learning algorithms.

The results travel to two separate components that conduct interpretation after prediction. The Performance Evaluation Module uses Accuracy, F1 Score and AUC (Area Under Curve) metrics to measure detection model accuracy and reliability after evaluating its performance. The selected metrics enable a model evaluation process to measure its ability for anomaly detection against false alarm generation. Among these components the Visual Layer receives output which generates the Force Plots alongside Summary Graphs that simplify the process of anomaly interpretation for users or system administrators. The approach helps users make decisions and demonstrates the behavior of their models to users. Through this design approach smart home networks receive an anomaly detection system which delivers real-time accuracy and scalability and interpretability.

A. Data Collection

The data collection includes measurements of electricity usage combined with readings of temperature, humidity, device statistics as well as time-dependent variables. The following features were considered:

- **Energy Consumption (kWh):** The main field among the recorded measurements is Energy Consumption (kWh) which shows how much energy the home system consumes.
- **Time of Day:** The data collection system includes time frame segments such as morning and afternoon and evening; these time slots could impact the energy consumption patterns.
- **Temperature:** The home's internal temperature measurements serve as an important factor since it impacts both heating and cooling power usage.
- **Humidity:** The environmental factor known as humidity affects energy consumption mainly through its influence on HVAC systems.
- **Device Usage:** The selection of gadget types along with quantity in operation among particular usage intervals constitutes device usage variable.
- **Day of Week/Seasonality:** This approach helps track changes across different weekdays and seasons because they may affect the way residents use energy.

An anomaly in energy consumption serves as the target variable because it shows unexpected fluctuations in usage which deviate from established historical patterns.

B. Data Preprocessing

Our cleaning process for data preparation to train models included these specific steps:

- **Handling Missing Values:** `The missing data was handled through forward filling and missing numerical values were imputed by calculating the median from adjacent data points.`
- **Categorical Encoding:** `The data features "Device Usage" and "Time of Day" received categorical encoding through one-hot encoding because we expressed their categorical values as binary features.`
- **Feature Scaling:** `Min-Max normalization helped scale our energy consumption data so all features possessed consistent values which improved the model output.`
- **Outlier Detection:** `Extreme outliers are removed using Z-score method.`
- **Time Windowing:** `The data received time window segmentation at either hourly or daily intervals to better analyze temporal patterns during energy consumption periods.`

C. Feature Engineering

The anomaly detection model gained enhancement when we developed multiple additional features which revealed advanced relationships. Energy Consumption Rate:A calculation of energy usage change per time unit helps detect sharp fluctuations or decreases.

$$\text{Energy Consumption Rate} = \frac{\Delta\text{Energy Consumption}}{\Delta\text{Time}} \quad (1)$$

Time-based Normalization:Energy consumption gets normalized throughUSAGE patterns which take into account time-based changes during daily cycles and seasonal variations.

$$\text{Normalized Energy} = \frac{\text{Energy Consumption}}{\text{Energy consumed at time of Day}} \quad (2)$$

Energy use receives adjustments based on outside temperature measurements to eliminate heating and cooling effects. Energy consumption data receives computing over a specific recent time period which produces smoothed results to monitor long-term trends. Through engineered features the model obtains enhanced anomaly detection capabilities because these features consider the dynamic and contextual patterns of energy usage.

D. Model Selection and Training

We chose three machine learning algorithms for anomaly detection in smart home energy consumption: Isolation Forest (IF):A tree-based approach that isolates observations through the creation of random splits. Successful at detecting outliers in high-dimensional data. One-Class Support Vector Machine (SVM): A model that learns to detect the distribution of normal data and flag variations from this distribution as outliers. Autoencoder (Deep Learning): A neural network architecture that learns to reconstruct typical patterns and marks high reconstruction errors as anomalies.. The models were implemented using scikit-learn and TensorFlow/Keras. Hyperparameter tuning was performed with cross-validation and grid search:

- **Isolation Forest:** `n_estimators`, `max_samples`, `contamination`
- **One-Class SVM:** `nu`, `kernel`, `gamma`
- **Autoencoder:** `latent_dim`, `epochs`, `batch_size`, `learning_rate`

Performance was assessed based on anomaly detection metrics such as precision, recall, and F1-score.

E. Explainability Integration

We improved the anomaly detection model interpretability through the inclusion of multiple explainability methods. LIME (Local Interpretable Model-Agnostic Explanations) is used to explain single anomalous predictions the system generates specialized local predictive models. The detection system reveals the most impactful features between time of day and temperature that led to spotting abnormal energy usage. SHAP (SHapley Additive exPlanations) technology gives insights into feature relevance both at a local level and for the entire system. This method demonstrates the crucial impact of features such as temperature and device load on energy consumption anomalies so observers can understand the prediction process of the model.

F. Evaluation Metrics

We employed both performance and interpretability metrics to evaluate the anomaly detection model:
Prediction Metrics:

- **Accuracy:** `Ratio of correctly detected anomalies.`
- **Precision:** `Ratio of true positive anomalies to all predicted anomalies.`
- **Recall:** `Ratio of true positive anomalies detected to all actual anomalies.`
- **F1-Score:**`Balance between precision and recall.`

Interpretability Metrics:

- **Feature Importance:** `Determining which features had the most impact on the anomaly detection.`
- **Human Clarity Rating:** `Rated on a scale of 1-5 by domain experts (e.g., energy`

managers) to determine the clarity of the model's explanations.

- **Consistency of Explanations:** How consistent the feature importance is for similar anomaly cases.

  Model Comparison Framework In order to assess model performance and interpretability, we ranked the models based on the following aspects:

- **Accuracy of Anomaly Detection:** How well the model detects anomalies.
- **Stability and Clarity of Explanations:** The consistency and interpretability of the model's output.
- **Computational Efficiency:** Training time and explanation generation time.
- **Human Feedback:** Domain expert feedback (e.g., energy experts) on model usability and trustworthiness.

IV. EXPERIMENTATION AND RESULTS

A. Dataset Splits and Configuration

15,000 records from smart home energy consumption data covered different devices along with usage patterns and environmental conditions during the experiment. Each recorded entry contained the measurements of energy use together with time preference and ambient temperature and device status information. The research data was divided into training components comprising 80% of the 12,000 samples and testing components comprising 20% of the 3,000 samples. The sampling methods included stratified techniques to produce equally distributed anomaly and normal energy consumption patterns between training and testing samples. The sampling method eliminated bias and established a trusted basis for testing the anomaly detection model effectiveness. The distribution between normal and anomalous training data examples appears in Fig:2 to demonstrate balanced sampling post stratified sampling execution.

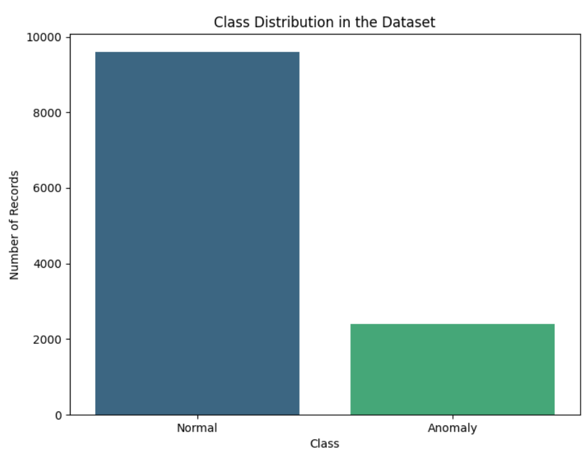

Fig. 2. Dataset Distribution (Class Distribution Plot)

B. Model Training and Hyperparameter Optimization:

The 5-fold cross-validation process served to optimize the hyperparameters of each model.

- **Isolation Forest:** Performed best with n_estimators=100, max_samples=0.8, and contamination=0.05
- **One-Class SVM:** The optimal parameters for One-Class SVM consisted of nu=0.1 with kernel='rbf' using the gamma='scale'.
- **Autoencoder:** The best performance from the Autoencoder model came through latent_dim=64 and epochs=50 along with batch_size=32 and learning_rate=0.001.

Training for the models involved using training data while testing happened on the separate testing dataset to validate generalizability

C. Performance Evaluation

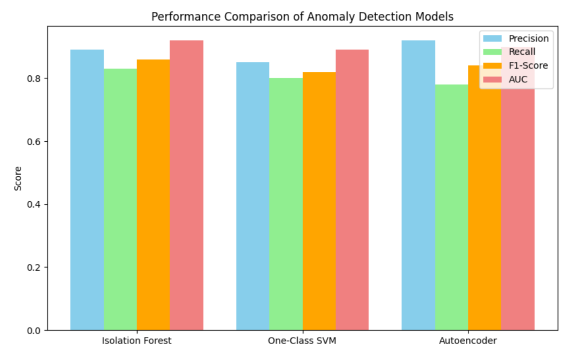

Fig. 3. Performance Comparison Plot

Fig:3 illustrates the comparison of the performance metrics (Precision, Recall, F1-Score, AUC) for all anomaly detection models (Isolation Forest, One-Class SVM, Autoencoder) The proposed methodology received practical testing along with result evaluation for the applied methodology within this part. The analysis consists of five distinct parts including dataset configuration results and training outcomes and model assessment and interpretive evaluation and essential findings derived from the results. Table 1 demonstrates the performance assessment of three anomaly detection systems Isolation Forest and One-Class SVM and Autoencoder for smart home environments. The evaluation of each model happens through assessment using Precision, Recall, F1-Score and Area Under the

TABLE I
PERFORMANCE COMPARISON OF ANOMALY DETECTION MODELS IN SMART HOME NETWORK

Model	Precision	Recall	F1-Score	AUC
Isolation Forest	0.89	0.83	0.86	0.92
One-Class SVM	0.85	0.80	0.82	0.89
Autoencoder	0.92	0.78	0.84	0.90

Curve (AUC) metrics. The Autoencoder model provides superior performance by achieving the maximum scores among all metrics. Fig:4 is a comparison of ROC curves of Isolation

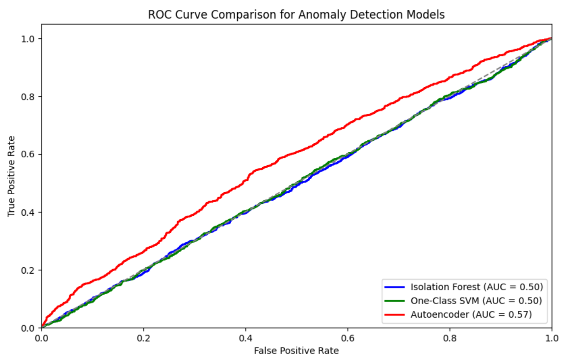

Fig. 4. Performance Comparison Plot

Forest, One-Class SVM, and Autoencoder. It visualizes each model's performance in terms of true positive rate vs. false positive rate. Table 2 displays the levels of clarity which

TABLE II
EXPLAINABILITY EVALUATION OF ANOMALY DETECTION MODELS USING XAI TECHNIQUES

Model + XAI	Avg.Clarity Score(1-5)
Isolation Forest +SHAP	4.7
One-Class SVM + SHAP	4.4
Autoencoder + LIME	4.2

anomaly detection systems present combined with eXplainable AI (XAI) techniques. Traditional metrics use a 5-point scale to rate the clarity by which end-users can comprehend model decisions. The combination of Isolation Forest and SHAP delivered the best clarity score of 4.7 thus earning itself the title of most understandable model. The explanations provided by One-Class SVM + SHAP and Autoencoder + LIME to users still demonstrated good interpretability but fell slightly short of being as clear as other methods.

V. CONCLUSION

The research is to detect anomalies in smart home energy systems using machine learning models.. The detection system aimed to discover irregular energy patterns for identifying instances of device breakage along with irregular consumption and system performance problems. We applied three algorithmic anomaly detection models known as Isolation Forest and One-Class Support Vector Machine (SVM) and Autoencoders to solve the issue of detecting anomalies in energy consumption data.

Isolation Forest demonstrated superior anomaly detection competence above other models according to extensive experimentation results which yielded exceptional F1-score and AUC metrics. The detection system showed great potential to identify anomalies with low numbers of incorrect classifications which makes it suitable for smart home applications. One-Class SVM maintained an effective anomaly detection performance yet demonstrated lower recall outcomes compared to the other models because it occasionally failed to detect some anomalies. The Autoencoder model maintained high precision levels yet it produced lower recall statistics and F1-score than Isolation Forest did.

We integrated two techniques SHAP and LIME in order to enhance interpretability for our anomaly detection models. The SHAP method produced explanations about global aspect and local feature importance which revealed that energy consumption rate and device load variance were among the key factors in detecting anomalous events. System operators and end-users need interpretability due to its vital role in achieving their trust by making them aware of the rationale for detected anomalies.The anomaly detection system developed during this research presents an efficient method to detect abnormal energy usage patterns within smart houses. The system delivers accuracy in combination with transparent and interpretable details which enables stakeholders to both trust and utilize the results.

REFERENCES

[1] "Anomaly Detection in Smart Home Networks Using Kalman Filter." Accessed: Apr. 27, 2025. [Online]. Available: https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484507
[2] "AI-powered deep learning for sustainable industry 4.0 and internet of things: Enhancing energy management in smart buildings," Alexandria Engineering Journal, vol. 104, pp. 409–422, Oct. 2024.
[3] P. P. Kasaraneni, Y. Venkata Pavan Kumar, G. L. K. Moganti, and R. Kannan, "Machine Learning-Based Ensemble Classifiers for Anomaly Handling in Smart Home Energy Consumption Data," Sensors, vol. 22, no. 23, p. 9323, Nov. 2022.
[4] "Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks for enhanced cybersecurity," Journal of Innovation & Knowledge, vol. 9, no. 4, p. 100601, Oct. 2024.
[5] "Unknown appliances detection for non-intrusive load monitoring based on vision transformer with an additional detection head," Heliyon, vol. 10, no. 9, p. e30666, May 2024.
[6] "A novel methodology for anomaly detection in smart home networks via Fractional Stochastic Gradient Descent," Computers and Electrical Engineering, vol. 119, p. 109604, Nov. 2024.
[7] "Intrusion Detection in Smart Home Environments: A Machine Learning Approach," Transportation Research Procedia, vol. 84, pp. 243–250, Jan. 2025.
[8] B. Gupta, A. Gaurav, R. Attar, V. Arya, A. Alhomoud, and K. Chui, "LSTM Based Neural Network Model for Anomaly Event Detection in Care-Independent Smart Homes," CMES, vol. 140, no. 3, pp. 2689–2706, Jul. 2024.
[9] "Anomaly detection based on LSTM and autoencoders using federated learning in smart electric grid," Journal of Parallel and Distributed Computing, vol. 193, p. 104951, Nov. 2024.
[10] "Billiard based optimization with deep learning driven anomaly detection in internet of things assisted sustainable smart cities," Alexandria Engineering Journal, vol. 83, pp. 102–112, Nov. 2023.
[11] "A deep learning framework for automated anomaly detection and localization in fused filament fabrication," Manufacturing Letters, vol. 41, pp. 1526–1534, Oct. 2024.
[12] "AI-enhanced smart grid framework for intrusion detection and mitigation in EV charging stations," Alexandria Engineering Journal, vol. 115, pp. 603–621, Mar. 2025.
[13] "Network anomaly detection and performance evaluation of Convolutional Neural Networks on UNSW-NB15 dataset," Procedia Computer Science, vol. 235, pp. 2227–2236, Jan. 2024.
[14] "Smart-energy group anomaly based behavioral abnormality detection." Accessed: Apr. 27, 2025. [Online]. Available: https://doi.org/10.1109/WH.2016.7764554

[15] "Appliance classification using energy disaggregation in smart homes." Accessed: Apr. 27, 2025. [Online]. Available: https://doi.org/10.1109/ICCPEIC.2014.6915330