A Machine Learning-Based Temperature Control and Security Protection for Smart Buildings

Mostafa Zaman[1], Maher Al Islam[1], Nasibeh Zohrabi[2], Sherif Abdelwahed[1]
[1]Department of Electrical and Computer Engineering, Virginia Commonwealth University, Richmond, VA
[2]Department of Engineering, Pennsylvania State University Brandywine, Media, PA, USA
zamanm@vcu.edu, alislamm@vcu.edu, nmz5171@psu.edu, sabdelwahed@vcu.edu

***Abstract*—With the advent of IoT technology, smart building management has been transformed, leading to significant improvements in energy efficiency and occupant comfort. Indoor room temperature control is crucial as it affects both building performance and occupant quality of life. Nevertheless, stringent cybersecurity measures are required due to the increasing susceptibility to cyber attacks with more IoT links in smart buildings. Identifying and managing unusual temperature readings is essential to keep the system running smoothly, efficiently, and safely. By integrating classical control methods such as PID with anomaly detection and LSTM modeling, this approach enables proactive anomaly identification and accurate temperature forecasts, rendering sustainable and resilient living conditions. This integration optimizes resource usage and mitigates cyber risks. This paper presents a holistic method that combines PID control, LSTM forecasting, and anomaly detection for smart building applications. The proposed integrated approach successfully addresses aberrant temperature variations and enhances building performance, as shown through experimental validation.**

***Index Terms*—Smart Building, Anomaly Detection, Machine Learning, PID Controller, Random Forest Classifier, FDI.**

I. Introduction

In the European Union, buildings contribute to around 30-40% of overall energy consumption, with approximately half of this usage allocated to indoor climate regulation [1]. Globally, buildings now surpass industry and transportation combined in terms of environmental impact. Despite this, many buildings continue to utilize outdated technologies for climate control, resulting in significant energy inefficiencies compared to newer approaches [2].

With the onset of Industry 4.0 [3], the concepts of smart cities and smart buildings are quickly gaining traction in the market and are becoming commonplace terms among researchers. Smart cities, with their interconnected and intelligent infrastructure, have shown promise in improving the standard of living in cities as well as addressing a range of urban issues. In recent years, smart buildings have emerged as a promising solution for optimizing energy consumption and improving occupant comfort [4].

In a recent incident, smart thermostats in Finland fell victim to a security breach, leading to severe cold conditions for residents during the winter [5]. The infamous Mirai malware, which gained widespread attention in 2016, orchestrated large-scale distributed denial-of-service attacks targeting multiple high-profile entities [6]. These incidents underscore the vulnerabilities of Internet of Things (IoT) devices and the potential risks associated with their exploitation. Due to the widespread adoption of smart meters, security attacks like False Data Injection (FDI) [7] have become more common, targeting sensor networks in smart buildings by inserting false readings. Machine learning plays an important role in IoT security by analyzing data for irregular patterns, allowing it to discover and fix vulnerabilities proactively. However, challenges remain in combating cyber-attacks, specifically the absence of specialized intrusion detection systems for IoT devices and cloud data centers capable of identifying zero-day attacks [8].

Modifications are often necessary to increase user comfort and energy efficiency in buildings since they lack sustainability features. However, budget restraints and the slow replacement of components make significant improvements almost impossible. Developing building energy management systems (BEMS) using software-based IoT technology solutions is a well-known sought-after option [9]. BEMS operates in real-time to optimize energy use by monitoring and controlling HVAC systems, either reactively or proactively. Effective HVAC systems need a lot of computing power, but there is a growing need for more straightforward, energy-efficient economical options specifically designed for residential buildings [10]. This paper aims to use machine learning-based anomaly detection and temperature regulation to decrease energy consumption, improve building efficiency, and enhance predictive maintenance and user comfort in smart buildings.

Inefficient and uncomfortable indoor climate control is a common problem with reactive HVAC systems in smart buildings. Proactive measures similar to predictive maintenance are essential to maximize efficiency and comfort. Identifying early anomalies in indoor climatic parameters and intervening promptly to improve occupant well-being and decrease energy consumption is crucial [11]. Following the detection of attacks, implementing control strategies such as PID (Proportional-Integral-Derivative), Fuzzy Logic, and Model Predictive Control (MPC) can facilitate the system in taking appropriate actions to mitigate the impact of the attacks. PID controllers [12] provide a well-established method for regulating system parameters by continuously adjusting control inputs based on error signals, integral of errors, and their derivatives.

A. Related Work

In this subsection, we discuss relevant studies on anomaly detection and LSTM prediction for smart buildings.

Various approaches are employed to identify and diagnose abnormalities, establishing a foundation for robust anomaly detection systems in smart buildings. The authors in [13] proposed a semi-supervised clustering technique using Self-Organizing Maps neural networks to detect unusual patterns in smart-home user behavior based on presence sensor data. In [14], researchers utilized a model to identify security breaches based on user behavior, considering differences caused by time and temperature. The authors in [15] designed an ensemble model to identify anomalies in smart buildings. In [16], One-Class Support Vector Machines were used to determine unusual occurrences. Lastly, the study in [17] utilized Hidden Markov Models to analyze user behaviors and detect abnormal operations.

Neural networks outperform conventional approaches in predicting the indoor temperature of buildings using historical data. Their growing popularity in building energy management applications is due to their ability to solve complex problems [18], [19]. Several studies have compared conventional machine learning models, such as Autoregressive and Multiple Linear Regression, with neural network models, including MLP-NARX, Extreme Learning Machine, and Long Short Term Memory (LSTM), in predicting indoor temperature [20]. The results indicate that both Neural Architecture Representation (NAR) architecture and LSTM models perform well, with LSTM particularly effective at identifying key inputs for accurate predictions [21]. Prediction accuracy can further be improved by considering factors such as weekends and holidays [22]. Previous work has shown that neural networks can create accurate models for predicting indoor temperature, although they often require large datasets for effective training and improved accuracy [23].

Recent innovations in anomaly detection are significantly improving the management of building systems. In [24], researchers developed an anomaly detection system using a two-stacked LSTM model to monitor internal environment variables and identify outliers. The study in [25] utilizes IoT sensors to collect data from various home appliances, showing significant patterns in each appliance's energy usage to improve power system maintenance and management. Additionally, [26] introduces an unsupervised method for detecting anomalies in temperature time series data using dynamic thresholds. Another study proposes a framework for detecting abnormal electrical loads in homes, which combines a rule-engine-based load anomaly detector with a hybrid one-step-ahead load predictor [27]. To the best of our knowledge, the smart building temperature control management framework has not yet integrated three essential modules: anomaly detection, LSTM prediction, and control approaches.

B. Contributions of This Study

In this paper, we aim to integrate anomaly detection technologies with classifiers and machine learning-based controllers to efficiently handle discovered anomalies and ensure the system's resilient functioning. This approach facilitates proactive anomaly management and precise temperature forecasts, thereby improving the quality of life for occupants. Using PID controllers, smart buildings can optimize temperature set points, which improves energy efficiency, and occupant well-being, and increases resistance against cyber attacks.

The primary contributions of this paper are outlined below:

- Presented a new approach integrating false data injection, machine learning-based anomaly detection, and control techniques within a smart home environment, using a real-world dataset to simulate an attacker's scenario.
- Employed an LSTM model to predict future temperature data as a threshold for detected temperature anomalies.
- Assessed the effectiveness of the anomaly detection and classification and LSTM modules using various performance indicators.
- To handle falsified temperature fluctuations, a PID controller is used to dynamically adjust temperature values to predetermined thresholds based on LSTM predictions.
- To ensure the validity and applicability of our findings, real-time datasets are used for anomaly detection and threshold prediction. Experiments will be conducted on our smart city testbed [28] to validate the effectiveness and real-world applicability of our proposed approach.

The structure of the paper is as follows: Section II delves into the theoretical foundations of the methods used, while Section III presents the proposed integrated approach and its different modules. Section IV illustrates the experimental data and simulation analysis. The paper concludes with Section V.

II. Theoretical Background

A. Random Forest Classifier

Random forests algorithm is an ensemble of decision trees first introduced in [29], which comprises decision trees, each contributing a vote towards a specific class. According to [29], random forests are more resistant to noise and produce more accurate tree classifiers than Adaboost. A learning set $L = \{(M_1, N_1), \ldots, (M_n, N_n)\}$ made of n vectors, $M \in X$ where X is a set of numerical or symbolic observations, and $N \in Y$ where Y is a set of classes [30] can be considered. In classification tasks, a classifier, which is represented as a mapping $X \rightarrow Y$, assigns class labels to input vectors. Each tree independently classifies a new input vector in a forest of decision trees, producing a specific classification result. The final decision is determined by aggregating the decisions of all trees in the forest, resulting in a majority vote for classification or averaging for regression. This aggregation process constitutes the ensemble's prediction mechanism.

B. Long Short Term Memory (LSTM)

Since the introduction of LSTM networks [31], they have become a valuable tool due to their ability to capture long-term dependencies and mitigate the vanishing gradient issue. An LSTM unit comprises a memory cell, an input gate, an output gate, and a forget gate. Memory cell c_t saves the input x_t at time t, defined by the input gate. Forget gate forgets the state of the last moment cell, c_{t-1}. The output

gate h_t added a part of the cell c_t. The input and output gate equations are illustrated in the following Equations (1).

$$i_t = \sigma(W_i \times [h_{t-1,x_t}] + b_i)$$
$$f_t = \sigma(W_f \times [h_{t-1,x_t}] + b_f) \quad (1)$$

W_i and W_f represent the weights linked to the input and forget gates, respectively. h_{t-1} denotes the last memory cell output, whereas x_t represents the current input. Similarly, b_i and b_f represent the bias vectors. Equation (2) is used to assist in updating the memory cell state.

$$c_t = f_t \times c_{t-1} + i_t \times (\tanh(W_c \times [h_{t-1,x_t}] + b_c)) \quad (2)$$

W_c represents memory cell weight, c_{t-1} signifies the preceding memory cell state, and b_c denotes the bias vector. The output h_t is calculated using Equation (3).

$$o_t = \sigma(W_o \times [h_{t-1,x_t}] + b_o)$$
$$h_t = \sigma_t \times \tanh(c_t) \quad (3)$$

C. PID (Proportional – Integral – Derivative) Controller

Over 90% of control loops utilize the PID controller, making it a crucial component of current feedback control systems [32]. Effectively regulating system behavior across varied applications, PID control integrates proportional (P), integral (I), and derivative (D) input. A PID controller uses adjustable parameters (K_p, K_I, K_D) to balance accuracy, stability, and responsiveness by modifying system inputs according to the difference between desired and actual outputs. In response to the amount of the present error, the P adjusts output proportionately; in contrast, the I collects errors over time to reduce steady-state errors. Overshoot, nevertheless, is possible, especially with shorter integral periods. In contrast, the D is stable-contributing yet noise-prone since it predicts error changes by looking at its velocity of change. Together, these parts enhance the system's performance, making it more resistant to disruptions and manageable to regulate [33].

III. Proposed Methodology

The proposed architecture aims to safeguard smart home environments against temperature manipulation attacks, as depicted in Fig. 1. Firstly, real-world temperature data is obtained from the IoT Dataset block, detailed in III-D. The attacker manipulates the dataset using False Data Injectionapproach III-A. Then, we employ a Random Forest Classifier to detect anomalies caused by the attackers. This classifier is trained on the dataset to identify deviations from normal temperature patterns. The ensemble learning capabilities of the Random Forest Classifier allow our system to detect anomalies faster and more effectively, strengthening the security of smart home environments.

Subsequently, upon anomaly detection, our system leverages an LSTM model within the Prediction Module, referenced as III-B, to forecast temperatures during instances of attack. During the training phase, the LSTM model is trained to learn temporal patterns from the data. Then, during the testing phase, this trained LSTM model is employed to predict temperature values at the time indices corresponding to detected anomalies calculated from the anomaly detection block. These predicted values serve as estimations of future threshold values, aiding in anticipating temperature variations induced by the attack.

Finally, to maintain the desired temperature and ensure user comfort, a PID controller (Controller Module - III-C) utilizes the predictions generated by the LSTM model as a threshold temperature. By regulating the HVAC system based on these values, the PID controller effectively counteracts the effects of the FDI attack on the temperature sensor data.

A. Anomaly Injection and Classification Module

We train a Random Forest Classifier to detect the anomaly in the temperature dataset consisting of 1000 instances. These temperature setpoints, which the system will regulate, reflect user preferences. However, attackers can maliciously add, delete, manipulate, or delay the data. In this work, we consider FDI attacks, a concept first introduced in [7], which compromise data integrity by exploiting sensor vulnerabilities. For any FDI attack vector, we have equation 4:

$$z_a = z + a \quad \text{where } z \text{ is the clean data and } a \in \mathbb{R} \quad (4)$$

Fig. 2 shows a modified dataset using FDI attacks. We injected 1000 synthetic points and set the value a to the range $16 \leq a \leq 45$. This range was selected based on the clean data distribution shown in Fig 3. We then derive the anomaly instances index for use in the prediction module to find the relative threshold for the controller. Fig. 4 illustrates the confusion matrix derived from the anomaly detection classifier. Out of 8112 data points in the testing dataset, we found 7734 were true positive, 10 to be genuine negative, 2 to be false positive, and 392 to be false negative. The classification accuracy of the anomaly detection and classification module is 0.998, demonstrating the efficacy of the classifier in precisely categorizing anomalies.

B. Prediction Module

We develop a custom normalization function for our dataset to preprocess the input temperature data. We then employ an LSTM module to forecast the temperature for each setpoint in abnormal cases. Utilizing sequence learning, the LSTM model analyzes historical patterns to predict future temperatures. The model is configured with a timestep of 25 recent data points. We experiment with different layers and varying neuron counts to achieve optimal performance. Next to the sequence learning block is a dense layer that facilitates dimensionality modifications by linking the output to subsequent layers. The output layer's neuron number changes depending on the predicted horizon. We train our model over 100 epochs with a batch size of 64 using Adam optimizer. To evaluate performance, we divided our dataset into two parts: 60% for training and 40% for testing. Table I details the network setup for the proposed LSTM model.

C. Control Module

We employ a PID controller to model temperature feedback loops in a smart building. We first define proportional, integral,

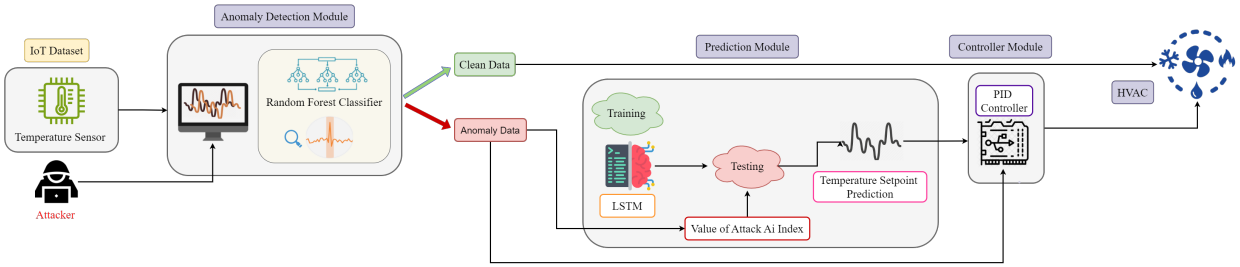

Fig. 1. Proposed Architecture of Machine Learning-Based Anomaly Detection for Temperature Setpoint Control

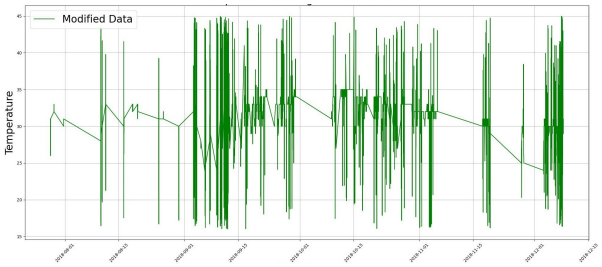

Fig. 2. Portion of Modified Dataset

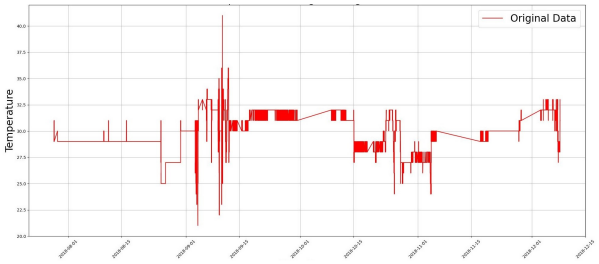

Fig. 3. Portion of Original Dataset

and derivative gains as the standard PID constants. After detecting aberrant temperature sensors in the initial stage of the experiment, we randomly assigned indices to represent each one. These indices allow for the calculation of setpoint temperatures and the appropriate initialization of PID controllers for each sensor. The temperature feedback loop is replicated across multiple iterations, capturing temperature data and control signals for every sensor. Using PID control to regulate a smart building's temperature dynamically allows for exact tracking and control. It also shows how the PID controller can be adjusted and used in many situations by employing random sampling to mimic different sensor circumstances.

D. Dataset Description

The dataset [34] includes temperature readings from IoT sensors, both indoors and outdoors, collected from July 28, 2018, to December 08, 2018. During the recording period, the devices encountered intermittent instances of being uninstalled or shut down, which led to the collection of readings occurring at irregular intervals. The dataset consists of 97,605 recorded values. Our research primarily focuses on 20,345 interior temperature data. Each reading has a unique ID and additional details such as room number, time of measurement, temperature value, and whether it was taken indoors or outdoors.

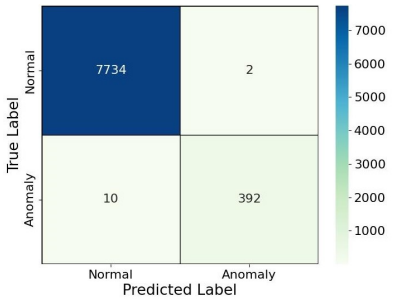

Fig. 4. Confusion Matrix for Anomaly detection

TABLE I
PROPOSED LSTM NETWORK ARCHITECTURE

Layer	Output Shape	Parameter
lstm (LSTM)	(None, 25, 100)	40800
lstm_1 (LSTM)	(None, 25, 100)	80400
lstm_2 (LSTM)	(None, 100)	80400
dense (Dense)	(None, 1)	101

Fig. 3 and Fig. 2 show a portion of the original dataset and modified dataset (false data injection), respectively.

IV. Simulation Results

A. Performance Metrics

In this section, we assess the model's effectiveness using various performance criteria. Confusion Matrix is a popular method for assessing the performance of a classification model on test data with known actual values [35]. A classification system's accuracy is the percentage of true positives relative to the total number of categories, shown in Equation (5). The variables TP, TN, FP, and FN in the equation represent true positive, true negative, false positive, and false negative detections, respectively [36]. We use three standard metrics, mean square error (MSE), mean absolute error (MAE), and root mean square error (RMSE), to evaluate our proposed method's performance. The MSE metric calculates the average of the squares of errors between predicted values and actual values, as shown in equation (7) [37]. The MAE metric calculates the average of the absolute differences between predicted and target values, using equation (6) [37]. The RMSE metric, presented in equation (8), measures the standard deviation of prediction errors [37].

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \tag{5}$$

$$MAE = \frac{1}{n}\sum_{1}^{n} \mid y - \hat{y} \mid \tag{6}$$

$$MSE = \frac{1}{n}\sum_{1}^{n} (y - \hat{y})^2 \tag{7}$$

$$RMSE = \sqrt{\frac{1}{n}\sum_{1}^{n} (y - \hat{y})} \tag{8}$$

where y and $\hat{y}$ represent the true and predicted values of the indoor temperature, respectively. In Table III, we can see several performance metrics that show how our suggested LSTM model works to determine the threshold temperature for aberrant sensors that are randomly identified.

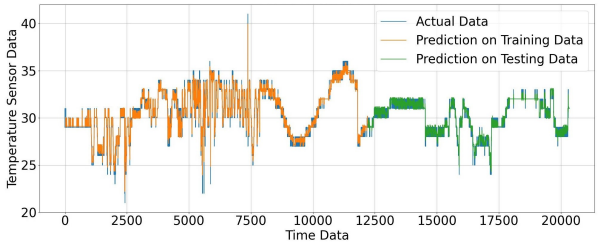

Fig. 5. Prediction results of Temperature Prediction

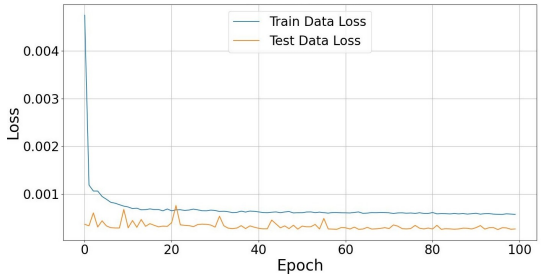

Fig. 6. Training and Testing Loss

B. Result Analysis

Table II presents various performance metrics for five sensors in a smart building. Sensors 1-3 experience fewer overshoots compared to Sensors 4-5, highlighting how much each sensor's temperature surpasses the target setpoint. The Rise Time indicates the rate at which the temperature reaches a certain percentage of the setpoint, while the Settling Time measures the rate at which the temperature stabilizes around the setpoint. A negative value for the Steady-State Error indicates that the temperature falls below the setpoint. The precision of each sensor's temperature control system over time is shown by the Integral of Absolute Error (IAE).

The LSTM model's accuracy in predicting future temperatures for accessing the anomaly temperature data indices is evaluated using three metrics: Mean Squared Error (MSE), Mean Absolute Error (MAE), and Root Mean Squared Error (RMSE). During the training phase, the model records an MSE of 0.383, an MAE of 0.364, and an RMSE of 0.619. During the testing phase, the model shows an improved performance with an MSE of 0.184, an MAE of 0.302, and an RMSE of 0.429. These results indicate that the LSTM model effectively

TABLE II
PERFORMANCE METRICS FOR DIFFERENT SENSORS IN A BUILDING

Sensor Info	PID		
	Overshoot	Steady-State Error	IAE
Sensor #328	0.923	0.00018	36.344
Sensor #58	1.106	-7.788e-05	15.0491
Sensor #13	0.057	-4.018e-06	0.776
Sensor #380	0.423	-2.978e-05	5.755
Sensor #141	2.919	-0.0002	39.695

TABLE III
PERFORMANCE METRICS FOR LSTM MODEL

MSE		MAE		RMSE	
Train	Test	Train	Test	Train	Test
0.383	0.184	0.364	0.302	0.619	0.429

learns temporal patterns in the temperature data, aiding in the detection of abnormal temperature indices. This ability to generalize to new data during testing is reflected in lower error metrics, which signify enhanced predictive accuracy. The performance metrics for the LSTM model are illustrated in Table II. Fig. 5 further demonstrates the model's ability to accurately represent real-world temperature dynamics by comparing predicted values with actual temperatures. Fig. 6 shows the loss in both the training and the testing periods, consistently approaching zero. This pattern indicates that our model demonstrates remarkable performance by closely matching its temperature predictions with actual data. Fig. 7 illustrates the temperature monitoring behavior of randomly selected anomalous sensors on a floor. The set threshold values serve as benchmarks for these abnormalities, demonstrating their increasing alignment with the projected thresholds generated by the LSTM module. This diagram illustrates the automatic adjustment process activated when unusual sensor data is detected, highlighting the effectiveness of our technique. Furthermore, Fig. 8 emphasizes the efficiency and resilience of the system, showing that reducing control input levels enhances stability around the defined threshold values, thereby improving overall system performance.

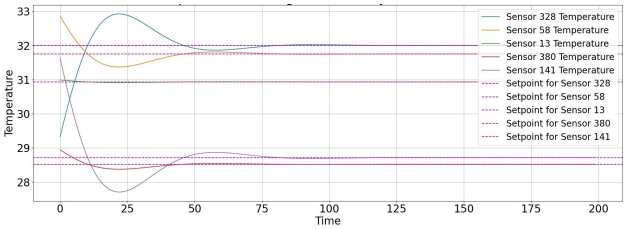

Fig. 7. Temperature Tracking for Randomly Selected Sensors

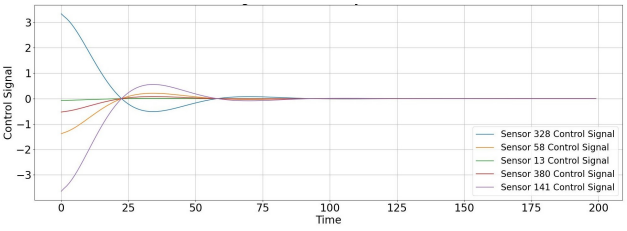

Fig. 8. Control Signal for Randomly Selected Sensors

V. Conclusion

Smart buildings usher in a new age of livability, energy efficiency, and sustainability with the ubiquitous integration of IoT sensors, which optimize energy usage and enhance occupant comfort. Accurate forecasting of temperature and humidity are essential for maintaining indoor thermal comfort and optimizing HVAC system operations. Predictive indoor temperature control strategies utilize historical and real-time environmental data to predict fluctuations, enabling proactive interventions for efficient climate management. This paper represents an initial step towards incorporating machine learning-driven anomaly detection into control systems for optimal indoor climate regulation. It presents a comprehensive anomaly detector-based framework for smart building applications that combine PID control and LSTM forecasting. Experimental validation confirms its efficacy in minimizing temperature fluctuations and enhancing building performance. By integrating anomaly detection with machine learning and control approaches, smart buildings can maximize resource use, mitigate cyber threats, and foster resilient ecosystems.

Acknowledgment

This work is supported by the Commonwealth Cyber Initiative (CCI), an investment in the advancement of cyber R&D, innovation, and workforce development in Virginia. For more information about CCI, visit cyberinitiative.org.

References

[1] P. Ferreira, A. Ruano, S. Silva, and E. Conceicao, "Neural networks based predictive control for thermal comfort and energy savings in public buildings," *Energy and buildings*, vol. 55, pp. 238–251, 2012.

[2] E. Dahlberg, M. Mineur, L. Shoravi, and H. Swartling, "Replacing setpoint control with machine learning: Model predictive control using artificial neural networks," 2020.

[3] K. Schwab, *The fourth industrial revolution*. Crown Currency, 2017.

[4] M. Zaman, M. Al Islam, A. Tantawy, C. J. Fung, and S. Abdelwahed, "Adaptive control for smart water distribution systems," in *2021 IEEE International Smart Cities Conference (ISC2)*, pp. 1–6, IEEE, 2021.

[5] S. Robinson, "Smart home attacks are a reality, even as the smart home market soars," *Last accessed*, vol. 27, 2019.

[6] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, *et al.*, "Understanding the mirai botnet," in *26th USENIX security symposium (USENIX Security 17)*, pp. 1093–1110, 2017.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[8] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, "Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning," in *IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0305–0310, IEEE, 2019.

[9] J. Novacic and K. Tokhi, "Implementation of anomaly detection on a time-series temperature data set," 2019.

[10] P. Danassis, K. Siozios, C. Korkas, D. Soudris, and E. Kosmatopoulos, "A low-complexity control mechanism targeting smart thermostats," *Energy and Buildings*, vol. 139, pp. 340–350, 2017.

[11] Y. Liu, Z. Pang, M. Karlsson, and S. Gong, "Anomaly detection based on machine learning in iot-based vertical plant wall for indoor climate control," *Building and Environment*, vol. 183, p. 107212, 2020.

[12] M. A. Johnson and M. H. Moradi, *PID control*. Springer, 2005.

[13] M. Novák, F. Jakab, and L. Lain, "Anomaly detection in user daily patterns in smart-home environment," *J. Sel. Areas Health Inform*, vol. 3, no. 6, pp. 1–11, 2013.

[14] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, and Y. Kato, "Anomaly detection for smart home based on user behavior," in *IEEE international conference on consumer electronics (ICCE)*, pp. 1–6, IEEE, 2019.

[15] S. Tang, Z. Gu, Q. Yang, and S. Fu, "Smart home iot anomaly detection based on ensemble model learning from heterogeneous data," in *IEEE International Conference on Big Data*, pp. 4185–4190, IEEE, 2019.

[16] V. Jakkula and D. Cook, "Detecting anomalous sensor events in smart home data for enhancing the living experience," in *Workshops at the twenty-fifth AAAI conference on artificial intelligence*, 2011.

[17] S. Ramapatruni, S. N. Narayanan, S. Mittal, A. Joshi, and K. Joshi, "Anomaly detection models for smart home security," in *IEEE 5th Intl Conference on Big Data Security on Cloud*, pp. 19–24, IEEE, 2019.

[18] A. E. Ruano, E. M. Crispim, E. Z. Conceiçao, and M. M. J. Lúcio, "Prediction of building's temperature using neural networks models," *Energy and Buildings*, vol. 38, no. 6, pp. 682–694, 2006.

[19] A. Bellagarda, S. Cesari, A. Aliberti, F. Ugliotti, L. Bottaccioli, E. Macii, and E. Patti, "Effectiveness of neural networks and transfer learning for indoor air-temperature forecasting," *Automation in Construction*, vol. 140, p. 104314, 2022.

[20] F. Mateo, J. J. Carrasco, A. Sellami, M. Millán-Giraldo, M. Domínguez, and E. Soria-Olivas, "Machine learning methods to forecast temperature in buildings," *Expert Systems with Applications*, vol. 40, no. 4, pp. 1061–1068, 2013.

[21] A. Aliberti, F. M. Ugliotti, L. Bottaccioli, G. Cirrincione, A. Osello, E. Macii, E. Patti, and A. Acquaviva, "Indoor air-temperature forecast for energy-efficient management in smart buildings," in *2018 IEEE International Conference on Environment and Electrical Engineering*, pp. 1–6, IEEE, 2018.

[22] C. Xu, H. Chen, J. Wang, Y. Guo, and Y. Yuan, "Improving prediction performance for indoor temperature in public buildings based on a novel deep learning method," *Building and Environment*, vol. 148, pp. 128–135, 2019.

[23] A. Aliberti, L. Bottaccioli, E. Macii, S. Di Cataldo, A. Acquaviva, and E. Patti, "A non-linear autoregressive model for indoor air-temperature predictions in smart buildings," *Electronics*, vol. 8, no. 9, p. 979, 2019.

[24] S.-H. Noh and H. J. Moon, "Anomaly detection based on lstm learning in iot-based dormitory for indoor environment control," *Buildings*, vol. 13, no. 11, p. 2886, 2023.

[25] A. Malki, E.-S. Atlam, and I. Gad, "Machine learning approach of detecting anomalies and forecasting time-series of iot devices," *Alexandria Engineering Journal*, vol. 61, no. 11, pp. 8973–8986, 2022.

[26] W. Liu, H. Jiang, D. Che, and L. Chen, "A real-time temperature anomaly detection method for iot data," in *IoTBDS*, pp. 112–118, 2020.

[27] X. Wang and S.-H. Ahn, "Real-time prediction and anomaly detection of electrical load in a residential community," *Applied Energy*, vol. 259, p. 114145, 2020.

[28] N. Zohrabi, P. J. Martin, M. Kuzlu, L. Linkous, R. Eini, A. Morrissett, M. Zaman, A. Tantawy, O. Gueler, M. Al Islam, *et al.*, "Opencity: An open architecture testbed for smart cities," in *2021 IEEE International Smart Cities Conference (ISC2)*, pp. 1–7, IEEE, 2021.

[29] L. Breiman, "Random forests," *Machine learning*, vol. 45, pp. 5–32, 2001.

[30] A. T. Azar, H. I. Elshazly, A. E. Hassanien, and A. M. Elkorany, "A random forest classifier for lymph diseases," *Computer methods and programs in biomedicine*, vol. 113, no. 2, pp. 465–473, 2014.

[31] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[32] K. J. Åström and T. Hägglund, "The future of pid control," *Control engineering practice*, vol. 9, no. 11, pp. 1163–1175, 2001.

[33] S. Ahmed and O. Ugur, "Pid in smart buildings," 2017.

[34] A. A. Jha, "Temperature readings from iot devices." https://www.kaggle.com/datasets/atulanandjha/temperature-readings-iot-devices/data, 2020. Accessed: March 4, 2024.

[35] N. Elmrabit, F. Zhou, F. Li, and H. Zhou, "Evaluation of machine learning algorithms for anomaly detection," in *International conference on cyber security and protection of digital services*, pp. 1–8, IEEE, 2020.

[36] M. Zaman, S. Saha, N. Puryear, N. Zohrabi, and S. Abdelwahed, "Incorporation of physiological features in drowsiness detection using deep neural network approach," in *2022 IEEE Transportation Electrification Conference & Expo (ITEC)*, pp. 219–224, IEEE, 2022.

[37] M. Zaman, S. Saha, R. Eini, and S. Abdelwahed, "A deep learning model for forecasting photovoltaic energy with uncertainties," in *IEEE Green Energy and Smart Systems Conference (IGESSC)*, pp. 1–6, IEEE, 2021.