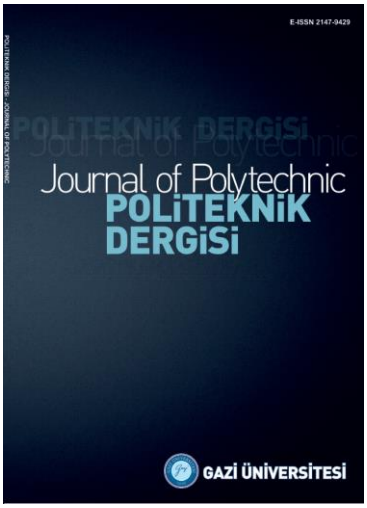

POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)
URL: http://dergipark.org.tr/politeknik

Anomaly detection with gradient boosting regressor on HVAC systems

HVAC sistemlerinde gradyan arttırma regresyonu ile anomali tespiti

***Authors**: M. Fatih ADAK[1], Refik KİBAR[2], Kevser OVAZ AKPINAR[3]*

ORCID[1]: 0000-0003-4279-0648

ORCID[2]: 0000-0002-3228-7494

ORCID[3]: 0000-0002-9859-6855

To cite to this article: Adak M.F., Kibar R. and Akpinar Ovaz K., "Anomaly Detection with Gradient Boosting Regressor on HVAC Systems", ***Journal of Polytechnic***, 27(6): 2117-2125, (2024).

Bu makaleye şu şekilde atıfta bulunabilirsiniz: Bulut S., "Anomaly Detection with Gradient Boosting Regressor on HVAC Systems", ***Politeknik Dergisi***, 27(6): 2117-2125, (2024).

Erişim linki (To link to this article): http://dergipark.org.tr/politeknik/archive

DOI: 10.2339/politeknik.1379049

Anomaly Detection with Gradient Boosting Regressor on HVAC Systems

Highlights

- *Analyzing a HVAC dataset from an Office building*
- *Preprocessing data and reducing dimension*
- *Preparing five different regression models*
- *Detecting anomalies and cyber-attacks with GBR*

Graphical Abstract

Gradient Boosting Regressor, a powerful machine learning technique is used to improve the anomaly detection capabilities of HVAC systems

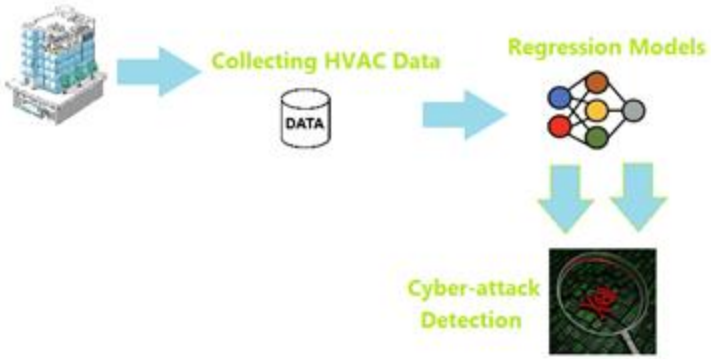

Figure. The structure of developd model

Aim

The aim of the study is optimizing energy consumption, improve thermal comfort and indoor air quality, detect and isolate sensor faults, and, more importantly, detect cyber-attacks.

Design & Methodology

we propose the application of Gradient Boosting Regressor, a powerful machine learning technique, to enhance anomaly detection accuracy and reliability. We evaluate the model's performance using real-world HVAC data, comparing it with existing anomaly detection methods.

Originality

Traditional anomaly detection methods often struggle to adapt to the dynamic nature of HVAC systems and may generate false alarms or miss critical issues. To address these challenges, Gradient Boosting Regressor based model proposed.

Findings

The findings of the study are significant improvements in the system's ability to identify anomalies accurately while minimizing false alarms. The true positive rate is 100% and false positive rate is 0%.

Conclusion

This research advances HVAC system security by providing a more robust and adaptive anomaly detection solution. Integrating Gradient Boosting Regressor into the cybersecurity framework of HVAC systems offers improved protection against cyber threats.

Declaration of Ethical Standards

The authors of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

Anomaly Detection with Gradient Boosting Regressor on HVAC Systems

Araştırma Makalesi / Research Article

M. Fatih ADAK[1*], Refik KİBAR[2], Kevser OVAZ AKPINAR[3]

[1,2]Faculty of Computer and Information Sciences, Department of Computer Engineering, Sakarya University, Turkey
[3]Department of Electrical Engineering & Computing, Rochester Institute of Technology of Dubai, UAE

(Geliş/Received : 20.10.2023 ; Kabul/Accepted : 12.12.2023 ; Erken Görünüm/Early View : 05.03.2024)

ABSTRACT

HVAC systems are important in buildings due to their significant energy consumption, impact on indoor air quality, and role in occupant comfort. Optimizing the operation and control of these systems is crucial for improving energy efficiency and reducing costs. Anomaly detection in HVAC systems aims to optimize energy consumption, improve thermal comfort and indoor air quality, detect and isolate sensor faults, and, more importantly, detect cyber-attacks. By analyzing system data for unusual patterns or unauthorized access attempts, anomaly detection can play a vital role in safeguarding HVAC systems against cyber threats. Detecting and isolating potential cyber-attacks can prevent disruptions in building operations, protect sensitive data, and ensure the continued functionality of HVAC systems securely and reliably. In this study, Gradient Boosting Regressor is used to improve the anomaly detection capabilities of HVAC systems. HVAC dataset used in this study was collected from an office building was gathered data between 6 AM and 6 PM. Traditional anomaly detection methods often struggle to adapt to the dynamic nature of HVAC systems and may generate false alarms or miss critical issues. To address these challenges, we propose the application of Gradient Boosting Regressor, a powerful machine learning technique, to enhance anomaly detection accuracy and reliability. We evaluate the model's performance using real-world HVAC data, comparing it with existing anomaly detection methods. The results demonstrate significant improvements in the system's ability to identify anomalies accurately while minimizing false alarms. This research advances HVAC system security by providing a more robust and adaptive anomaly detection solution. Integrating Gradient Boosting Regressor into the cybersecurity framework of HVAC systems offers improved protection against cyber threats, thereby enhancing the resilience and reliability of critical infrastructures.

Keywords: HVAC, Gradient Boosting Regressor, cyber-attack, anomaly detection, time series.

HVAC Sistemlerinde Gradyan Arttırma Regresyonu ile Anomali Tespiti

ÖZ

HVAC sistemleri, önemli enerji tüketimleri, iç mekan hava kalitesi üzerindeki etkileri ve bina sakinlerinin konforundaki rolleri nedeniyle binalarda büyük önem taşımaktadır. Bu sistemlerin çalışmasını ve kontrolünü optimize etmek, enerji verimliliğini artırmak ve maliyetleri düşürmek için çok önemlidir. HVAC sistemlerinde anomali tespiti, enerji tüketimini optimize etmeyi, termal konforu ve iç mekan hava kalitesini iyileştirmeyi ve sensör hatalarını tespit edip izole etmeyi, ancak daha da önemlisi siber saldırıları tespit etmeyi amaçlamaktadır. Anomali tespiti, olağandışı modeller veya yetkisiz erişim girişimleri için sistem verilerini analiz ederek, HVAC sistemlerinin siber tehditlere karşı korunmasında hayati bir rol oynayabilir. Potansiyel siber saldırıların tespit edilmesi ve izole edilmesi, bina operasyonlarındaki kesintileri önleyebilir, hassas verileri koruyabilir ve HVAC sistemlerinin güvenilir bir şekilde işlevselliğini sürdürmesini sağlayabilir. Bu çalışmada, HVAC sistemlerinin anomali tespit yeteneklerini geliştirmek için Gradyan Arttırma Regresyonu kullanılmıştır. Bu çalışmada kullanılan HVAC veri seti bir ofis binasından toplanmıştır ve veriler sabah 6 ile akşam 6 arasını kapsamaktadır. Geleneksel anomali tespit yöntemleri genellikle HVAC sistemlerinin dinamik yapısına uyum sağlamakta zorlanır ve yanlış alarmlar üretebilir veya kritik sorunları gözden kaçırabilir. Bu zorlukların üstesinden gelmek için, anomali tespit doğruluğunu ve güvenilirliğini artırmak üzere güçlü bir makine öğrenimi tekniği olan Gradyan Arttırma Regresyonu bu çalışmada kullanılmıştır. Modelin performansını ölçmek adına gerçek HVAC verileri kullanılarak anomali tespit yöntemleriyle karşılaştırılmıştır. Sonuçlar, yanlış alarmları en aza indirirken sistemin anormallikleri doğru bir şekilde tanımlama becerisinde önemli gelişmeler olduğunu göstermektedir. Genel olarak, bu araştırma daha sağlam ve uyarlanabilir bir anomali tespit çözümü sağlayarak HVAC sistem güvenliğinin ilerlemesine katkıda bulunmaktadır. Bu çalışma, Gradyan Arttırma Regresyonu'nun HVAC sistemlerinin siber güvenlik çerçevesine entegrasyonu ile siber tehditlere karşı gelişmiş koruma sağlayacağı ve böylece kritik altyapıların esnekliğini ve güvenilirliğini arttıracağını göstermiştir.

Anahtar Kelimeler: HVAC, Gradyan Arttırma Regresyonu, siber saldırı, anomali tespiti, zaman serisi.

**Corresponding Author*
e-posta : fatihadak@sakarya.edu.tr

1. INTRODUCTION

Modern living and working environments rely on intricate climate control solutions to ensure comfort and efficiency. Directly related to this field, Heating, Ventilation, and Air Conditioning systems play a crucial role in buildings due to their impact on energy conservation, air quality, and user satisfaction. The main energy consumers in buildings are these systems, accounting for 40-60% of energy usage [1], [2]. The sustainability of HVAC systems is an important consideration. These systems account for much of the world's energy consumption [3]. In addition to this importance, anomaly detection in HVAC systems is crucial for optimizing energy use, reducing operational costs, ensuring occupant comfort, and minimizing environmental impact. It helps facility managers make data-driven decisions and maintain efficient, reliable, compliant HVAC systems.

Moreover, one of the critical aspects of anomaly detection in HVAC systems is its role in cybersecurity. With the increasing connectivity of HVAC systems through the Internet of Things (IoT) and building automation systems, they have become potential targets for cyber-attacks. By analyzing system data for unusual patterns or unauthorized access attempts, anomaly detection can play a vital role in safeguarding HVAC systems against cyber threats. Detecting and isolating potential cyber-attacks can prevent disruptions in building operations, protect sensitive data, and ensure the continued functionality of HVAC systems securely and reliably.

Anomaly detection in HVAC systems is an important area of research and has been the focus of several studies. One approach to anomaly detection in HVAC systems is the application of computational intelligence (CI) techniques, followed by optimizing climate satisfaction and environmental well-being [4]. Another approach to anomaly detection in HVAC systems is using fault detection and isolation (FDI) techniques to detect and isolate sensor faults in HVAC systems [5]. Anomaly detection techniques, such as outlier detection, have also been applied to HVAC systems. These techniques monitor HVAC systems to identify faults and anomalies [6]. Visualization-driven approaches have also been proposed for anomaly detection in HVAC systems. These approaches use visualization techniques to explore and analyze HVAC data [7]. Artificial intelligence methods, like deep neural networks, have additionally found utility in identifying anomalies within HVAC systems. These techniques use confidence sampling to quantify anomaly detection confidence [8]. Anomaly detection in HVAC systems for cyber-attacks is a multidisciplinary field that combines machine learning, visualization, and cybersecurity. By leveraging machine learning algorithms, visualization models, and datasets, researchers can develop effective methods for detecting anomalies in HVAC system operation and mitigating cyber-attack risks.

HVAC systems and the Internet of Things (IoT) have become closely intertwined in recent years, leading to significant advancements in energy efficiency, comfort control, and maintenance of HVAC systems. Integrating IoT technology with HVAC systems offers numerous benefits, including energy savings, improved comfort, predictive maintenance, and enhanced control. As IoT advances, it will likely play an even more significant role in the evolution of HVAC systems and building automation. However, it also introduces challenges related to data security and system integration. The progress of IoT has made the precautions that need to be taken by using the vulnerabilities and increasing the attacks important. Attackers initially use vulnerable IoT technologies as a first step toward compromising a critical system. Since IoT technologies are part of critical infrastructures, such attacks are significant for industry, smart buildings and grids, transportation, and medical services. HVAC systems face these attacks when all possible attack paths are not examined for systems where the Internet of Things is the end user, such as smart buildings and houses. Consequently, attacks aimed at the HVAC infrastructure can lead to substantial damage and expenses. Several studies have been conducted to address this issue and improve the anomaly detection capabilities of HVAC systems. An alternative method involves utilizing machine learning methods to improve the HVAC systems' ability to detect anomalies [9]. Likewise, Nixon et al. examined the real-world implementation of online intrusion detection using machine learning in IoT networks, encompassing HVAC systems [10]. Another approach is to utilize Bayesian networks for scalable anomaly detection, where anomalies can arise from malicious cyber-attacks and operational faults [11]. Rashid et al. discussed the concept of anomaly detection as identifying data patterns that deviate from expected behavior [12].

Jadidi et al. proposed a comprehensive system-wide anomaly detection approach that utilized deep neural networks to identify anomalies and correlation analysis to investigate cyber-attacks impact interconnected devices in industrial control systems [13]. In addition to machine learning and deep learning approaches, Wang et al. discussed using outlier detection techniques, such as anomaly detection, in building and HVAC system operations [14].

The rising incorporation of various elements within buildings leads to Building Management Systems becoming increasingly accessible via the internet [15]. This latest development in connecting Supervisory Control and Data Acquisition (SCADA) to the network has led to integrating a new model with the old one. It has exposed the environment more to cyberattacks. As a result of the literature review, it can be said that it is challenging to detect the attack on the system and during the attack. In this age of vital infrastructure, the primary worry revolves around distinguishing a power failure from a cyberattack.

One time, the distinction between an attack and an error is clarified, the primary objective is to identify the category of cyberattack. Different control policies should be triggered when a cyber-attack is detected to maintain system resilience. For example, Khan et al. suggested a study explainable forecasting model using machine learning algorithms to detect different types of attacks in HVAC systems, and they got approximately %99 accuracy [16]. For security attack detection studies, Mariam et al. published a dataset gathered from HVAC systems [17]. In another similar study, Principal Component Analysis, Neural Network, and feature extraction approaches are investigated, assessing the cybersecurity aspect of HVAC systems [18]. Many critical message time series such as energy savings, healthcare, and automation have an important place. Input parameters to time series with dependent outcome variables should be processed by paying attention to the sampling of the current system. Analysis of outliers in time series data examines anomaly behavior over time [19]. A similar approach is used in tracking employee computer use behavior and detecting anomalous behavior by Support Vector Machines [20]. In general, the related literature on anomaly detection for HVAC systems within the framework of cyber-attacks emphasize the importance of robust anomaly detection techniques, including machine learning, deep neural networks, and statistical methods. The objective of these methods is to bolster the safety and reliability of HVAC systems when confronted with cybersecurity risks.

With the increasing connectivity of HVAC systems through IoT, these systems have become potential targets for cyber-attacks. Anomaly detection serves as a crucial defense mechanism against unauthorized access, ensuring system integrity, and safeguarding sensitive data. This and efficient anomaly detection ensures a comfortable environment while minimizing operational expenses are the motivation of this study. Given these motivations, the study aims to achieve the following objectives:

- Identifying anomalies within HVAC systems, addressing both operational faults and potential cyber-attacks.
- Categorizing attack types, and implementing appropriate control policies to ensure system resilience.
- Develop explainable forecasting models and utilize datasets specifically gathered from HVAC systems to improve anomaly detection accuracy.

2. MATERIAL AND METHOD

In an increasingly interconnected world, the importance of data analysis and anomaly detection cannot be overstated. Whether it's monitoring complex systems like HVAC systems or safeguarding critical information in cyber-security, the ability to identify unusual patterns and deviations from the norm is paramount. This article delves into the fascinating realm of anomaly detection in time series datasets, focusing on its applications in HVAC datasets and cyber-security.

Time series data refers to sequential data points collected over time. It is prevalent in various domains, including finance, healthcare, manufacturing, and more. Analyzing time series data can offer valuable insights into trends, seasonality, and anomalies. Anomalies, alternatively labeled as outliers or novelties, signify data points that exhibit notable deviations from the expected patterns.

In cyber-security, anomalies can indicate suspicious activities. Detecting unusual login patterns or network traffic can help identify security breaches or intrusions.

In the pursuit of safeguarding critical infrastructure against potential cyber threats, detecting anomalies within HVAC datasets has emerged as a paramount concern.

This methodological section delineates the comprehensive approach employed to tackle this imperative challenge. Leveraging a suite of regression algorithms, including Gradient Boosting Regressor (GBR), Random Forest Regression (RFR), K-Neighbor Regression (KNR), Linear Regression (LR), and Decision Tree Regression (DTR), our study seeks to establish a robust framework for anomaly detection in HVAC datasets, thus fortifying the cyber-security defenses of these vital systems.

2.1. Linear Regression

Linear regression is a widely used modeling method for examining the connection between a dependent variable and independent variables. It accomplishes this by creating a linear equation that best represents the provided dataset [21]. It presupposes a linear correlation among the factors and strives to discover the optimal-fitting line that reduces the total of the squared variances between the observed and predicted values. Linear regression proves to be a valuable method for identifying anomalies, particularly in the analysis of time series data. It can be used to represent the relationship between variables and identify anomalies by comparing observed and predicted values.

2.2. Decision Tree Regression

Decision tree regression is a supervised machine learning algorithm used for solving regression problems. While decision trees are commonly associated with classification tasks, decision tree regression is specifically designed to predict a continuous target variable [22]. It works by recursively partitioning the dataset into smaller subsets based on the input features and fitting a regression model to predict the target variable within each subset. At each step, the algorithm selects the feature and the corresponding threshold that best splits the data, aiming to minimize the variance of the target variable within each partition [23]. The recursive division process persists until it satisfies a termination condition, which can include reaching a

maximum tree depth or achieving a minimum number of data points in each leaf node [24].

Nonetheless, decision trees may be susceptible to overfitting, particularly as the tree deepens and becomes more complex. Overfitting arises when the model faces extraneous details and inconsequential trends within the training dataset, resulting in poor adaptability to novel data [25].

2.3. K-Neighbor Regression

K-Neighbor Regression (KNR) is a non-parametric algorithm for classification and regression tasks [26]. It was developed by Fix and Hodges in the 1950s and is regarded as one of the most straightforward variations of supervised machine learning algorithms [27]. In KNR, the algorithm uses a distance metric (e.g., Euclidean distance, Manhattan distance, or others) to calculate the similarity between data points in the feature space. It selects the nearest points from the training data to predict a new center. The neighbors are chosen based on the distance algorithms mentioned above [28].

2.4. Random Forest Regression

Random Forest Regression (RFR) is a machine-learning algorithm proposed by Breiman [29]. It is an ensemble learning method that can be used for classification and regression case studies. The algorithm follows the steps by building one or more decision trees through the training phase and then outputting the mode of the classes for classification or the mean prediction for regression [30].

2.5. Gradient Boosting Regressor

A machine learning model that builds an ensemble of decision trees to sequentially minimize the error between predictions and actual target values called Gradient Boosting Regressor (GBR). GBR is resulting in a powerful regression model. It is a tree-based implementation of gradient boosting machines (GBM) and is widely used in various domains such as computer science, medicine, and materials science [31]. The learning procedure in Gradient Boost Regressor (GBR) repeatedly tries new models to estimate the response variable better. The fundamental concept underlying the algorithm is to create new core learners that exhibit the highest possible correlation with the negative gradient of the loss function connected to the entire ensemble [32]. The identification of the optimal loss function can be ascertained through a systematic empirical approach, owing to the considerable latitude in the model's design. Boosting algorithms are straightforward to execute, enabling users to explore diverse model configurations. The selection of the loss function may involve the selection of the foundational learner function given in Eq. 1.

$$g_t(x) = E_y\left[\frac{\partial \Psi\big(y, f(x)\big)}{\partial f(x)} | x\right]_{f(x)=f^{t-1}(x)} \quad (1)$$

GBR is a robust machine learning algorithm widely used in various domains for regression tasks. Its ability to sequentially build subsequent trees and reduce errors effectively improves prediction accuracy. However, careful hyperparameter tuning and consideration of the depth of each regression tree are important for optimizing its performance.

2.3. Anomaly Types

Anomaly detection is important in various fields, including industrial scenarios, physics, computer science, and healthcare. Different forms of anomalies may be observed as point, conditional, and group anomalies. Point anomalies refer to individual data points exhibit substantial deviations from the anticipated behavior or pattern [33]. These anomalies are characterized by their dissimilarity to other data points in the dataset.

For example, in the context of time series data, a point anomaly could be manifest as an individual data point that diverges markedly from the remainder of the time series. Conditional anomalies, on the other hand, are anomalies that occur under specific conditions or contexts. These anomalies are not necessarily outliers in the entire dataset but exhibit abnormal behavior within certain conditions or contexts [34]. Group anomalies occur collectively within a group or subset of data points. These anomalies are characterized by their abnormal behavior when considered a group rather than individual data points. In the context of time series data, a group anomaly could be a set of consecutive data points that exhibit abnormal behavior when analyzed together [35], [36].

3. OVERVIEW OF THE STUDY AREA AND DATASET

The dataset used in this study is derived from the study [17]. The purpose of the dataset is to provide a collection of data that can be used to detect attacks on HVAC systems. The dataset was collected from an office building was gathered data between 6 AM and 6 PM. The building has labeled floors A, B, and C, each consisting of multiple zones. Zones from one to three are office rooms, while remaining zone is a hall. The dataset includes data from these zones (Table 1), which can be used to analyze the behavior of the HVAC system and detect any abnormal or malicious activities. By analyzing the data in this dataset, researchers can develop and test algorithms and techniques for detecting attacks on HVAC systems. This approach is important because HVAC systems play a vital role in preserving the comfort and safety of buildings, and any attacks on these systems can have serious consequences.

Table 1. Details of HVAC dataset [17]

Data	Type	Spec.	# Samples
Dataset1	Normal	51	194301
Dataset2	Normal	65	32161
Dataset3	Normal&Attack	65	8840

The data attributes in the dataset are shown in Table 2. These parameters are crucial for monitoring and controlling the environmental conditions within the building. The first two parameters, ty and td, represent time-related variables, indicating the yearly hour and the daily hour, respectively. Tanb stands for the ambient temperature, essential for understanding the outdoor climate. The subsequent parameters (from 4 to 15) are denoted as the temperatures within different zones in the building. Parameters 16 to 18 describe the temperature of the Air Handling Unit's supply air. Parameters 19 to 21 represent the temp. of the cooling coil's return water. Tt denotes the temp. of the chilled water tank, and Tchiller denotes the temp. of the chiller's outgoing water.

Table 2. Data attributes used in the dataset [17]

Index	Attribute
1	t_y
2	t_d
3	T_{amb}
4-15	T_{ZA1}-T_{ZA4}, T_{ZB1}-T_{ZB4}, T_{ZC1}-T_{ZC4}
16-18	T_{aoA}, T_{aoB}, T_{aoC}
19-21	T_{woA}, T_{woB}, T_{woC}
22	T_t
23	$T_{chiller}$
24-36	$U_1 - U_{13}$
37-51	-
52-63	PMV_1 - PMV_{12}
64	P_{total}
65	label

Parameters 24 to 36 represent control signals, likely used for regulating the HVAC system. Parameters 37 to 51 denote temperature setpoints for different zones. Parameters 52 to 63 pertain to the thermal comfort indices of the zones, indicating occupants' comfort levels. Finally, parameter 64, Ptotal, signifies the expected power usage of the entire HVAC system, while parameter 65 is the system status label. These parameters collectively enable a comprehensive analysis of the HVAC system's performance, energy consumption, and the thermal comfort of the building's occupants.

The attack methods used in this study are as follows.

Attack 1: Manipulating the control system's target values.

Attack 2: Tampering with sensor data through freezing or introducing bias.

Attack 3: Corrupting control signals via freezing or introducing a bias.

Attack 4: Altering command signals sent to various components.

In this study, the list of attacks injected into the dataset is given in Table 3 in detail. The steps of the algorithm performed with Python are listed below.

- Dependent and independent variable definitions are made on the application's data set.
- Algorithms to be used are defined on the project.
- Algorithms are trained by dividing the data set for training and testing purposes. Algorithm performances are compared according to error parameters.
- The trained algorithms are tested on the data set with cyber-attacks, and the data is labeled as an anomaly according to a certain threshold.
- The data labeled as an anomaly by the algorithms are compared with the actual results and evaluated according to the confusion matrix results.
- Correlational: the data set is reduced on the input parameters, the models are recreated, and their performances are reported.
- The change in model performance will be proven after applying the correlational relationship model on multivariate time series with the study carried out.

Table 3. List of attacks injected into the dataset

Index	Definition	Time
1.1	Change chiller set point to 14 °C	1st Day 12:00
1.2	Change water tank set point to 16 °C	2nd Day 06:00
1.3	Change AHU set point to 20 °C	2nd Day 10:00
1.4	Change A1 zone set point to 26 °C	2nd Day 11:00
1.5	Change C4 Zone set point to 18 °C	1st Day 03:00
2.1	Freeze B1 zone reading	5th Day 16:00
2.2	Freeze Zone C4 reading	7th Day 6:00
2.3	Freeze Zone A2 reading	9th Day 04:00
2.4	Freeze Zone C3 reading	1st Day 06:00
2.5	Introduce B3 zone deviation of 3 °C	3rd Day 06:00
3.1	Freeze C2 zone control signal	1st Day 15:00
3.2	Freeze B3 zone control signal	13th Day 18:00
3.4	Freeze B1 zone control signal	15th Day 06:00

Table 3. (cont.) List of attacks injected into the dataset

3.5	Setting B2 zone control signal to 0	19th Day 14:00
3.6	Setting A3 zone control signal to 1	19th Day 20:00
4.1	Reduce AHU-B water speed of the pump to 1/3	18th Day 12:00

In the context of Dataset 1, comprising a total of 194,301 samples, a data partitioning scheme has been implemented, wherein 80% of the data are allocated for training, with the remaining 20% reserved for testing. Within this dataset, 64 dataset parameters have been designated as the input feature. In contrast, the parameter denoted as "Total Power Using" is the dependent variable, thereby representing the output value under consideration within the system. This allocation and parameter specification are integral components of the experimental design and data preprocessing procedures employed for the ensuing analysis.

4. RESULTS

In this section, we present the results of our analysis for the HVAC Datasets 1 and 3, employing a comprehensive array of machine learning methods, including LR, DTR, KNR, RFR, and GBR. These methods were systematically applied to predict system performance in anomaly detection, and we unveil the highest accuracy test results, which notably stem from the Gradient Boosting Regression (GBR) approach. The outcomes of our analysis give valuable perspectives on the efficiency of these methods for identifying anomalies in HVAC systems, with GBR emerging as the standout performer in terms of predictive accuracy in test datasets. Table 4 presents the performance results on test dataset 1 for various regression methods, including GBR, LR, DTR, KNR, and RFR. Among these methods, GBR demonstrates the highest coefficient of determination R2 with a remarkable score of 0.99, indicating its superior ability to capture the variance in the dataset. Additionally, GBR achieves the lowest mean squared error (MSE) with a value of 2E+06, suggesting its efficacy in minimizing prediction errors. Regarding Mean Absolute Percentage Error (MAPE), GBR also outperforms the other methods with a score of 18.41, indicating its capability to make accurate predictions while keeping errors relatively low. Table 5 presents the error measurement results for various regression methods applied to test dataset 3.

Table 4. The performance results on test dataset 1

Method	R^2	MSE	MAPE
GBR	**0.99**	**2E+06**	**18.41**
LR	0.86	3E+08	54.17
DTR	0.90	1E+08	41.03
KNR	0.92	8E+07	32.17
RFR	0.95	7E+07	36.72

The methods assessed include GBR, LR, DTR, KNR, and RFR. Among these methods, GBR exhibited the highest coefficient of determination R2 at 0.425, suggesting the best overall fit to the data. Conversely, DTR performed the least favorably, with an R2 of only 0.012. When considering mean squared error (MSE), GBR again outperformed the other methods with a considerably lower value of 3E+10, while LR showed the highest MSE at 6E+11. As for Mean Absolute Percentage Error (MAPE), LR yielded the highest error percentage at 62.77%, while GBR again exhibited the lowest MAPE at 16.39%.

Table 5. Error measurement results on test dataset 3

Method	R^2	MSE	MAPE
GBR	**0.425**	**3E+10**	**16.02**
LR	0.281	6E+11	62.77
DTR	0.012	6E+10	19.39
KNR	0.261	7E+10	17.22
RFR	0.288	4E+10	17.61

GBR demonstrates relatively better predictive performance on test dataset 3. The test performance results of models employed in our study are given in Fig. 1. We evaluate these models based on their predictive performance, focusing on their ability to make accurate predictions and handle anomalies. The best-fit prediction model among the ones we explored in this study is the GBR. GBR exhibited the highest predictive accuracy and robustness across various test scenarios.

It consistently demonstrated the ability to make accurate predictions and handle a variety of data points. On the opposite end of the spectrum, the LR model always exhibited the lowest test performance among all models tested. Its inability to capture complex relationships in the data led to subpar predictive accuracy. The KNN and DT models performed relatively close to each other, but they faced challenges when making predictions at critical data points. When accurate predictions at crucial data junctures were required, KNN and DT models struggled and exhibited suboptimal performance. Our analysis reveals that the GBR model excels as the best-fit prediction model in this study, demonstrating superior predictive capabilities and effective anomaly detection. The RF model closely follows GBR in terms of predictive performance. Conversely, LR consistently delivered the lowest test performance, while KNN and DT models exhibited relatively comparable performance but struggled in making accurate predictions at critical anomaly points. These findings highlight the importance of selecting the appropriate model for specific predictive tasks and underline the utility of the GBR model in HVAC applications, especially in cyber-attack detection. Fig 2. shows data that compares actual and predicted anomaly data in detecting cybersecurity attacks in an HVAC system dataset. True positives represent the instances in which the GBR model correctly identified anomalies in the HVAC system as actual anomalies. In

this case, the model correctly detected 238 anomalies. False positives represent the instances where the GBR model incorrectly identified normal system behavior as an anomaly. Remarkably, in this evaluation, there were zero false alarms, indicating a high level of precision in the model's predictions. True negatives represent the instances in which the GBR model accurately identified normal system behavior as not being an anomaly. In this scenario, the model correctly classified 351 normal instances as such.

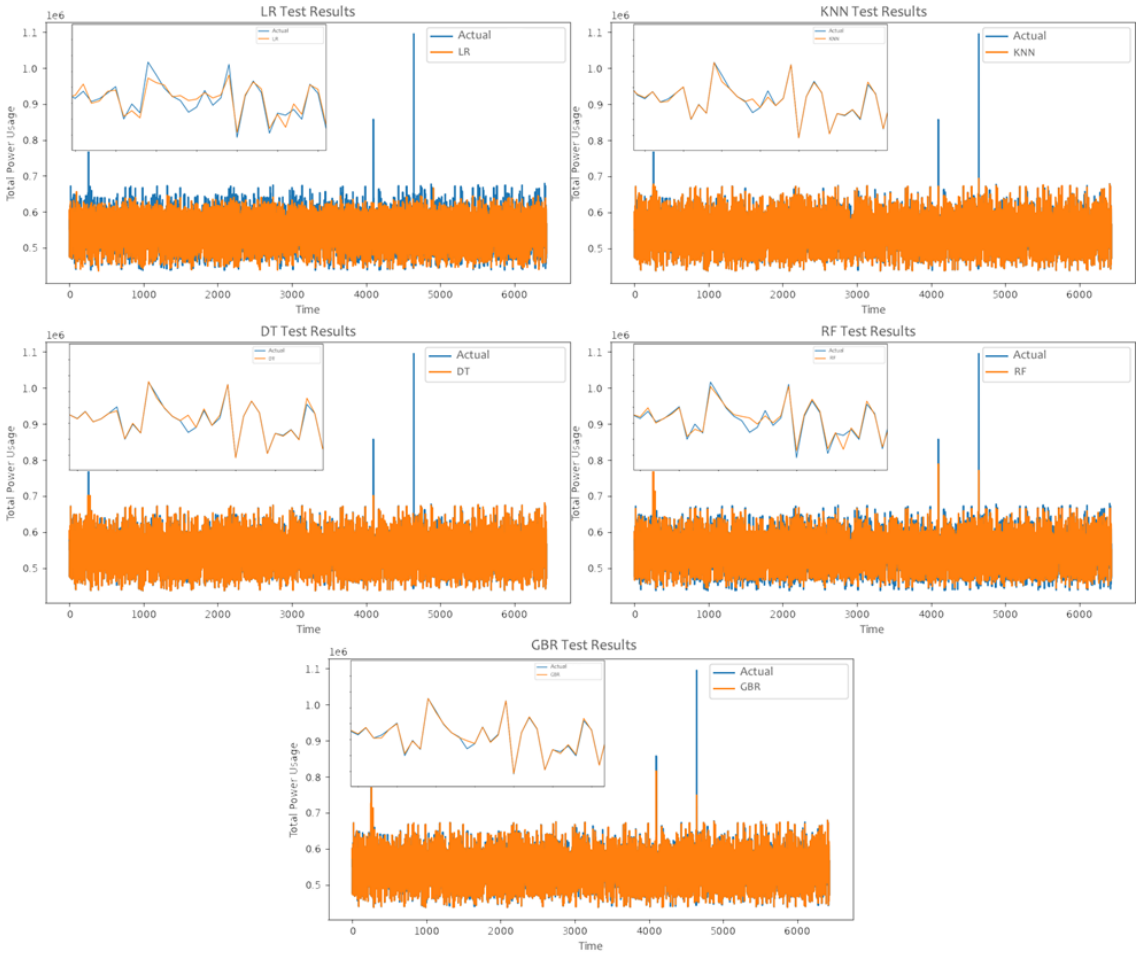

Figure 1. Test results of regression models

False negatives represent the instances where the GBR model failed to identify actual anomalies in the HVAC system. In this evaluation, the model missed two anomalies. The ROC curve which stands for Receiver Operating Characteristic is a visual depiction of the effectiveness of a binary categorization model. It illustrates the Sensitivity as True Positive Rate versus the Specificity as False Positive Rate at different threshold values. An "ideal" ROC curve is a curve that represents a perfect classification model, which can distinguish between the two classes (anomaly and normal) without making any mistakes. In this ideal scenario, the ROC curve would follow the plot's top-left corner, meaning that the True Positive Rate is 1 (100% sensitivity) and the False Positive Rate is 0 (0% specificity) for all possible threshold settings. In other words, the model correctly identifies all positive instances and makes no false positive errors. Relatively high. Fig. 3 shows that the GBR model is close to the Ideal ROC.

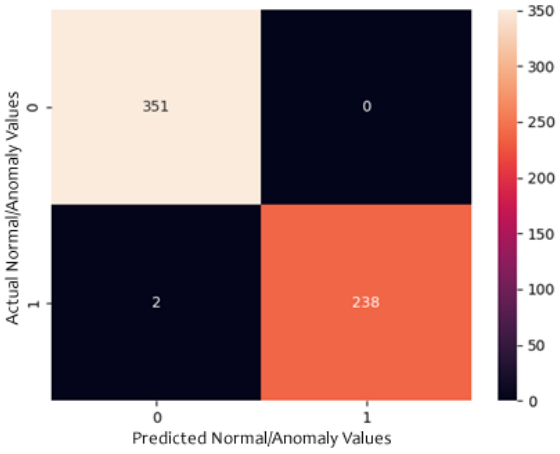

Figure 2. GBR accuracy performance

This indicates that GBR can detect cyber-attacks with a performance close to 100%.

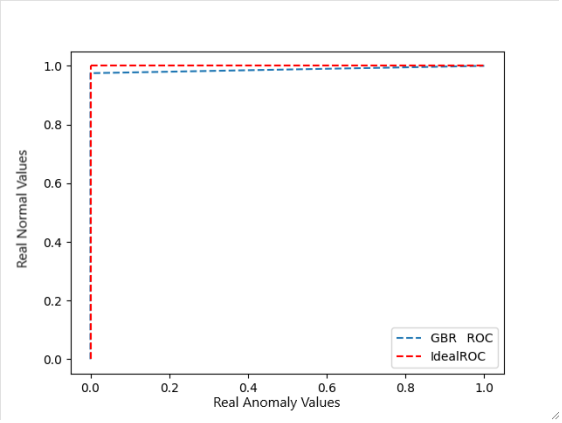

Figure 3. GBR and Ideal ROC curve

5. CONCLUSION

Consequently, HVAC systems are critical to modern building design, providing comfortable indoor environments by regulating temperature, humidity, and air quality. Cyber-attacks on HVAC systems pose a significant threat to building infrastructure and the safety and security of its occupants. HVAC systems become increasingly vulnerable to cyber-attacks as they become more interconnected and reliant on networked technologies. These attacks range from simple data breaches to sophisticated ransomware attacks, causing significant disruption, financial loss, and even endangering human lives. It is, therefore, essential for building owners and managers to take proactive measures to secure their HVAC systems against cyber-attacks, including implementing robust cybersecurity protocols, regularly updating software and firmware, and training staff on best practices for cybersecurity. By taking these steps, we can help safeguard our built environment and ensure the continued comfort and safety of building occupants.

As a general conclusion of this study, it can be stated that among the five different regression models, Gradient Boosting Regressor has a high success rate in detecting cyber-attacks and anomaly behavior in HVAC datasets.

In summary, the Gradient Boosting Regressor is the most effective choice for identifying cyber-attacks and anomalous behavior in HVAC datasets, highlighting its potential for enhancing system security. By prioritizing cybersecurity in HVAC systems, we can create resilient and secure buildings that protect the physical infrastructure and the well-being of those who occupy them. Road map for future studies would be ensemble methods or hybrid models incorporating GBR with other techniques for improved accuracy. Protocols would be developed for automated responses or alerts triggered by the model's detections to mitigate potential cyber threats promptly.

ACKNOWLEDGEMENT

This research received funding from the Sakarya University Scientific Research Projects Commission (BAPK) with project number 2023-19-43-16.

DECLARATION OF ETHICAL STANDARDS

The authors of this article declare that the materials and methods used in their study do not require ethics committee approval and/or legal-specific permission.

AUTHORS' CONTRIBUTIONS

M. Fatih Adak: Leading the dimensionality reduction efforts and contributing to the preparation of regression models.

Refik KIBAR: Analyzing the HVAC dataset and preparing regression models.

Kevser OVAZ AKPINAR: Taking charge of the cybersecurity aspect by detecting anomalies and cyber-attacks using GBR, and actively participating in data preprocessing.

CONFLICT OF INTEREST

There is no conflict of interest in this study.

REFERENCES

[1] Asim, N., Badiei, M., Mohammad, M., Razali, H., Rajabi, A., Chin Haw, L., & Jameelah Ghazali, M. "Sustainability of heating, ventilation and air-conditioning (HVAC) systems in buildings—An overview". ***International journal of environmental research and public health***, 19(2): (2022).

[2] Pérez-Lombard, L., Ortiz, J., & Pout, C. "A review on buildings energy consumption information." ***Energy and buildings***, 40(3): 394-398, (2008).

[3] Xiao, F., & Wang, S. "Progress and methodologies of lifecycle commissioning of HVAC systems to enhance building sustainability." ***Renewable and sustainable energy reviews***, 13(5): 1144-1149, (2009).

[4] Ahmad, M. W., Mourshed, M., Yuce, B., & Rezgui, Y. "Computational intelligence techniques for HVAC systems: A review In Building Simulation" 9: 359-398. ***Tsinghua University Press***, (2016).

[5] Reppa, V., Papadopoulos, P., Polycarpou, M. M., & Panayiotou, C. G. "A distributed architecture for HVAC sensor fault detection and isolation." ***IEEE Transactions on Control Systems Technology***, 23(4): 1323-1337, (2014).

[6] Wang, Z., Parkinson, T., Li, P., Lin, B., & Hong, T. "The Squeaky wheel: Machine learning for anomaly detection in subjective thermal comfort votes." ***Building and Environment***, 151: 219-22, (2019).

[7] Novikova, E., Belimova, P., Dzhumagulova, A., Bestuzhev, M., Bezbakh, Y., Volosiuk, A.& Lavrov, A. Usability assessment of the visualization-driven approaches to the HVAC data exploration. In Proceedings of the 30th International Conference on Computer Graphics and Machine Vision 1-12, (2020).

[8] Tasfi, N. L., Higashino, W. A., Grolinger, K., & Capretz, M. A. "Deep neural networks with confidence sampling for electrical anomaly detection." In 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) 1038-1045, (2017).

[9] Hindy, H., Brosset, D., Bayne, E., Seeam, A., & Bellekens, X. "Improving SIEM for critical SCADA water infrastructures using machine learning." In International Workshop on Security and Privacy Requirements Engineering, 3-19. Cham: Springer International Publishing, (2018).

[10] Nixon, C., Sedky, M., & Hassan, M. "Practical application of machine learning based online intrusion detection to internet of things networks." In 2019 IEEE Global Conference on Internet of Things (GCIoT) 1-5, (2019).

[11] Krishnamurthy, S., Sarkar, S., & Tewari, A. Scalable anomaly detection and isolation in cyber-physical systems using bayesian networks. In Dynamic Systems and Control Conference 46193, V002T26A006. American Society of Mechanical Engineers, (2014).

[12] Bazlur Rashid, A. N. M., Ahmed, M., & Pathan, A. S. K. "Infrequent pattern detection for reliable network traffic analysis using robust evolutionary computation", ***Sensors***, 21(9), (2021).

[13] Jadidi, Z., Pal, S., Hussain, M., & Nguyen Thanh, K. "Correlation-Based Anomaly Detection in Industrial Control Systems". ***Sensors***, 23(3): 1561, (2023).

[14] Wang, Z., Parkinson, T., Li, P., Lin, B., & Hong, T. "The Squeaky wheel: Machine learning for anomaly detection in subjective thermal comfort votes." ***Building and Environment***, 151: 219-227, (2019).

[15] J. Vijayan, "With the Internet of Things, smart buildings pose big risk," ***Computer World***, (2014).

[16] Khan, I. U., Aslam, N., AlShedayed, R., AlFrayan, D., AlEssa, R., AlShuail, N. A., & Al Safwan, A. "A proactive attack detection for heating, ventilation, and air conditioning (HVAC) system using explainable extreme gradient boosting model (XGBoost)". ***Sensors***, 22(23): 9235, (2022).

[17] Elnour, M., Meskin, N., Khan, K., & Jain, R. "HVAC system attack detection dataset." ***Data in Brief***, 37: 107166, (2021).

[18] Elnour, M., Meskin, N., Khan, K., & Jain, R. "Application of data-driven attack detection framework for secure operation in smart buildings". ***Sustainable Cities and Society***, 69: 102816, (2021).

[19] A. Blázquez-García, A. Conde, U. Mori, and J. A. Lozano, "A review on outlier/anomaly detection in time series data", ***ACM Computing Surveys***, 54(3): 1-33, (2020).

[20] Akpinar, M., Adak, M. F., & Guvenc, G. "SVM-based anomaly detection in remote working: Intelligent software SmartRadar." ***Applied Soft Computing***, 109: 107457, (2021).

[21] Neter, J., Wasserman, W., & Kutner, M. H. "Applied linear regression models." Richard D. Irwin (1983).

[22] Komarasamy G and Ravishankar T.N., "The Application of Decision Tree Method for Data Mining" ***Technoarete Transactions on Intelligent Data Mining and Knowledge Discovery***, 2(3), (2022).

[23] Sapri, F. E., Nordin, N. S., Hasan, S. M., Yaacob, W. F. W., & Nasir, S. A. M. "Decision tree model for non-fatal road accident injury." ***International Journal on Advanced Science, Engineering and Information Technology***, 7(1): 63-70, (2017).

[24] Zhang, M., Rong, J., Liu, S., Zhang, B., Zhao, Y., Wang, H., & Ding, H. "Factors related to self-rated health of older adults in rural China: A study based on decision tree and logistic regression model." ***Frontiers in Public Health***, 10: 952714, (2022).

[25] Chen, D., Hu, F., Nian, G., & Yang, T. Deep residual learning for nonlinear regression. ***Entropy***, 22(2): 193, (2020).

[26] Cover, T. "Estimation by the nearest neighbor rule." ***IEEE Transactions on Information Theory***, 14(1), 50-55 (1968).

[27] Han, J., Pei, J., & Tong, H. "Data mining: concepts and techniques. Morgan kaufmann", ***MK Press***, (2022).

[28] Fazakas-Anca, I. S., Modrea, A., & Vlase, S. "Determination of Reactivity Ratios from Binary Copolymerization Using the k-Nearest Neighbor Non-Parametric Regression." ***Polymers***, 13(21): 3811, (2021).

[29] Breiman L., "Random Forests," ***Mach Learn***, 45(1), 5–32, (2001).

[30] Xing, F., Luo, R., Liu, M., Zhou, Z., Xiang, Z., & Duan, X. "A new random forest algorithm-based prediction model of post-operative mortality in geriatric patients with hip fractures." ***Frontiers in Medicine***, 9: 829977, (2022).

[31] Freund Y. and Schapire R. E., "A Short Introduction to Boosting," ***Journal of Japanese Society for Artificial Intelligence***, 14(5): 771–780, (1999).

[32] Schapire R. E., "The boosting approach to machine learning: An overview", ***Nonlinear estimation and classification***, 149–171, (2003).

[33] Chandola, V., Banerjee, A., & Kumar, V. "Anomaly detection: A survey." ***ACM computing surveys (CSUR)***, 41(3): 1-58, (2009).

[34] Canizo, M., Triguero, I., Conde, A., & Onieva, E. "Multi-head CNN–RNN for multi-time series anomaly detection: An industrial case study", ***Neurocomputing***, 363: 246-260, (2019).

[35] Ahmed, M., & Pathan, A. S. K. "Deep learning for collective anomaly detection", ***International Journal of Computational Science and Engineering***, 21(1): 137-145, (2020).

[36] Ahmed, M., & Mahmood, A. N. "Network traffic pattern analysis using improved information theoretic co-clustering based collective anomaly detection", In International Conference on Security and Privacy in Communication Networks: 10th International ICST Conference, SecureComm Beijing, China, Revised Selected Papers, Part II 10 204-219. ***Springer International Publishing***, (2015).