17th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS, Suceava, Romania, May 23-25, 2024

Designing an Authentication Methodology in IoT Using Energy Consumption Patterns

Edi Marian Timofte
“Stefan cel Mare”University
Suceava, Romania
edi.timofte@usm.ro

Alexandra Ligia Balan
“Stefan cel Mare”University
Suceava, Romania
alexandra.balan@usm.ro

Teodor Iftime
Suceava, Romania
iftime.teo@gmail.com

***Abstract*—In this paper we are proposing an authentication method based on the energy usage patterns of connected devices. This approach marks a step up from traditional security protocols, using artificial intelligence and predictive analytics to identify the unique energy behaviors of each device. We implemented this system on Raspberry Pi 5, a small and affordable microcomputer, to show its efficiency and practicality in the real context of IoT applications. The solution we propose provides a new level of security by detecting subtle changes in energy usage that could mean suspicious activity or deviations from normal operation. The adaptability and scalability of this system makes it suitable for a wide range of IoT applications, from smart home devices to complex industrial systems. By closely studying energy data, our work highlights the importance and efficiency of integrating emerging technologies into IoT infrastructures for a safer and more resilient IoT environment.**

***Keywords*—Internet of Things, Methodology, Security, Energy consumption, Authentication, Protocols, Algorithm design and analysis.**

I. Introduction

In our fast-paced world where tech is always evolving, IoT devices are found nearly everywhere at homes and in businesses alike. Our new method for confirming a user's identity based on their energy use is another useful tool to keep these devices secure. This strategy doesn't depend on older security tools like encryption or passwords alone. In addition, it adds another safety feature by studying energy use patterns making the system less vulnerable to standard cyber-attacks. This can play an essential role in identifying and stopping unauthorized or misused IoT devices, thus preserving the integrity of both networks and data.

Instead of relying solely on common software safety strategies, we shift to making smart use of artificial intelligence to analyze energy use patterns to offer a more proactive security. What sets this method apart is the ability to detect subtle changes in the behavior of IoT devices that security strategies usually overlook. Every IoT device leaves a unique energy usage footprint and our system we researched uses this for added user verification.

By using the Raspberry Pi 5 [1] demonstrate the method's practicality that shows its effectiveness in real world IoT applications. Raspberry Pi 5, with its advanced processing and flexible interfacing capabilities, is an ideal platform to prove how energy consumption patterns can be monitored and analysed in real time. This provides an efficient and accurate device authentication method.

The solution's flexibility is another significant advantage. It is customizable and scalable to meet a wide variety of IoT scenarios and needs. From smart home appliances to advanced industrial systems, the Raspberry Pi 5 implementation validates the concept while highlighting its potential for extension and adaptation. This contributes to a safer, more resilient IoT environment and sets the stage for new research and development prospects in IoT security solutions. It emphasizes the importance and efficiency of incorporating emerging technologies into critical infrastructures.

II. Research and Substantiation

Drawing on various research, these articles aim to advance the field of IoT security through innovative authentication methods and strategic integrations. For instance, the approach in [2] uses unique device identities for encryption, integrating steps like setup, key generation, and decryption to protect against cyber threats like DDoS attacks. In contrast, [3] explores a layered authentication framework that reduces operational costs and enhances inter-device communication, proving useful in complex IoT ecosystems.

Meanwhile, [4] refines an existing protocol to accommodate large-scale data collection in intelligent transport systems, highlighting the importance of robust security measures for user access and system integrity. Furthermore, [5] addresses critical vulnerabilities in biometric authentication, proposing solutions to enhance user privacy and system resilience against sophisticated attacks.

Lastly, [6] uses blockchain technology to overcome the limitations of traditional single-password systems, enhancing the security and transparency of IoT environments through a multikey authentication mechanism. Together, these studies demonstrate the dynamic evolution of IoT security, emphasizing the need for continuous adaptation and improvement to address emerging threats and technological advancements.

The discussed studies look at different ways to authenticate devices in the Internet of Things (IoT) to improve security. One approach [7] restricts network access to devices within a certain distance by using a Wi-Fi signal to verify location. Experiments show that this can improve security in ad hoc IoT networks by adjusting the distance threshold to improve the accuracy of proximity-based authentication.

Another study [8] combines machine learning, specifically the Random Forest algorithm, with Belief Desire Intention (BDI) agents to authenticate IoT devices. This method uses context information from devices to make authentication decisions, which can increase accuracy and reduce computation delays, providing a more secure and efficient security framework for IoT networks.

The research in [9] develops a two-factor mutual authentication (2FMA) system for IoT devices using RFID and fingerprints, based on the MQTT protocol. This system is designed to withstand brute force and sniffing attacks, thereby enhancing the security of communications and data within IoT networks. The study emphasizes the importance of robust and

979-8-3503-4929-0/24/$31.00 ©2024 IEEE

efficient authentication methods as IoT device numbers and associated security risks grow.

Additionally, the investigation into hardware characteristics and energy monitoring technologies aims to better understand energy usage patterns in IoT devices, such as smart thermostats. This involves analyzing various techniques to detect anomalies in energy use that could indicate security breaches, thus contributing to safer IoT environments. Each approach reflects a strategic effort to address specific vulnerabilities and optimize IoT device security in increasingly complex networks.

This chapter will also clear the path for the next steps of the project, which includes developing algorithms for spotting these oddities and adding these systems into existing IoT infrastructures. By combining a thorough research method with hand son application and testing, our aim is to contribute to the increased energy efficiency and improved security of IoT devices [2], [4] , [5].

A. *Identification of Target Devices*

Studying the hardware components of Internet of Things (IoT) devices is essential to understanding the energy efficiency of today's smart technologies. The Nest Smart Thermostat, for example, automatically adjusts its temperature, which can result in savings of 10% to 12% on heating and 15% on cooling. Ecobee, with its eco+ algorithm and programming assistant, can save up to 26%. The Amazon Smart Thermostat, based on Honeywell Home technology, focuses on efficient control of energy consumption, with estimated savings of about $50 per year [10].

Along with practical benefits, energy monitoring technologies support sustainability. By providing accurate data and real time analysis, they promote responsible energy use. This cuts costs and carbon footprints, backing global efforts against climate change.

B. *Impact of Network Security on Energy Consumption*

In our research on network security's impact on the energy use of IoT devices, we are particularly focused on risks such as Low-rate Denial of Service (LDOS) attacks. These attacks can disrupt network communication, affecting devices like smart thermostats and more, leading to unjustified energy use [11].

In an LDOS attack scenario, smart thermostats and other IoT devices may respond improperly to commands or fail to switch to energy saving settings when not in use. This results in an unexpected increase in energy consumption. For instance, a thermostat might continuously heat or cool a room unnecessarily, causing excessive energy spending and unwarranted wear and tear on the HVAC system.

Poor network security can indirectly lead to extra costs. These include identifying and fixing problems as well as boosting infrastructure security. With so many IoT devices out there, from smart homes to industries, dealing with security risks is key. It is not just for data protection, but also for energy efficiency [12].

Adding some security to them, we can not only ensure data safety and security but also manage our energy resources in our connected ecosystems more effectively and sustainably [13], [14].

Integrating smart home devices, such as thermostats with motion sensors and lighting systems, can improve energy management efficiency. User interface and usability significantly impact interactions and device effectiveness, while reviews offer insights into real-world performance. This analysis aims to deepen understanding of the smart thermostat market, highlight technological advancements, and identify opportunities for improving smart home energy efficiency. Furthermore, it examines long-term trends and forthcoming strategies to boost energy efficiency in homes and industries, emphasizing technology's critical role in fostering sustainable practices. [15], [16]

III. Data collection

In the energy consumption of the smart thermostats listed, there are some general things to keep in mind to limit energy consumption in homes by adjusting heating and cooling programs to suit user habits.

To determine the actual use of energy, we must pay attention to:Home Type: A big house with several floors uses energy differently than a small apartment or a one level house.

- Home Insulation and Sealant: A well-insulated house needs less energy for heating and cooling.
- User Behavior: How users adjust the thermostat greatly changes energy use. Lower settings for heat and higher settings for cooling will generally save energy.
- Local Weather: The area's climate also changes energy use. In places with hot summers or freezing winters, the thermostat has to work harder to keep a comfy temperature.

A. *Identification of Target Devices*

Ecobee Smart Thermostat: These gadgets include sensors that can pick up on when someone is in a room. This lets the system tweak the temperature to what is needed [17].

Google Nest Thermostat and Nest Learning Thermostat: The Nest series is popular for its smart, learning capabilities. For instance, the thermostat finds out when you are home and adjusts the temperature accordingly. This potentially cuts energy use when you are not around. Nest suggests users can cut their heating expenses by 10% to 12% and cooling costs by 15% using their smart thermostats. This is calculated by comparing with a thermostat set to a stable temperature of 22°C. To get these percentages to make sense, say the average annual heating and cooling bill for a house is $1,000. A 10% savings on heating would mean a $100 reduction per year. And a 15% saving on cooling would add another $150, for a total annual savings of $250 [10].

Amazon Smart Thermostat: Built with Honeywell Home tech, it focuses on efficient energy control by auto changing temperature based on where users are and how they use it. Users might save around $50 per year on energy bills using the Amazon Smart Thermostat, agrees Energy Sage [18].

- Wyze Thermostat: This is a budget friendly way to enter the world of smart thermostats, with features that save energy by adjusting to usage habits. Right now, exact annual energy savings or usage for Wyze Thermostat is not provided, at least not in public adverts or technical documentation. Smart thermostat companies like Wyze often highlight energy saving features and adaptability to user habits, but they do not always offer precise savings figures or percentages [19].

- Honeywell Home Smart Color Thermostat: Provides monthly energy reports that can assist users in understanding and enhancing their energy consumption. In general, smart thermostats can save between 10% to 23% on heating and cooling costs, based on the model and use. The Honeywell Home Smart Color Thermostat and other smart thermostat models from Honeywell are designed to enhance energy efficiency and help users conserve energy [20].

Different situations, like varying temperatures between day and night, show how energy savings can change based on external conditions and personal preferences. Remote sensors also help the thermostat improve heating and cooling by providing accurate readings from around the house. While these numbers give a general idea of potential savings, they depend on the specific home. Things like home size, insulation, system type, and resident habits significantly impact a smart thermostat's energy efficiency.

IV. Development of Algorithms for the Interpretation of Energy Consumption

A. *Pattern Recognition*

In developing an energy consumption based authentication system, we rely on Machine Learning algorithms. These are trained using collected data to identify unique patterns associated with each IoT thermostat model (Fig.1).

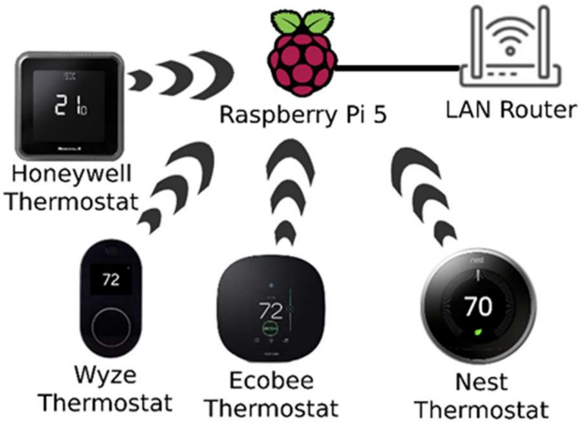

Fig. 1. Connecting sensors to the network with Raspberry Pi

The algorithms are designed to analyze and interpret slight changes in energy consumption, which could indicate a particular thermostat type and its specific usage patterns. This approach involves complex segmentation and detailed data analysis to extract distinguishing features from datasets and differentiate between device behaviors. Emphasis is given on ensuring data confidentiality and security, some of the aspects amid growing concerns over privacy and security in IoT ecosystems [21], [22].

To enhance the complexity and precision of the "Pattern Recognition" section in our study, we can further develop and refine the characteristic identification method for energy consumption patterns. The goal is to set up a more comprehensive and methodologically robust approach aligned with the complex requirements of energy model analysis in IoT devices.

We start by handling any missing values to ensure the data's accuracy. These can better capture the dynamics of energy use. The features are then normalized using “sklearn.preprocessing” from the “StandardScaler” library. Principal component analysis (PCA), using “sklearn.decomposition” from the PCA library, is applied to reduce the data set's dimensions, simplifying it while retaining the most meaningful information (Fig. 2). This approach falls in line with the advanced data processing techniques common in academic research, enhancing the robustness and effectiveness of the pattern recognition process in IoT energy usage data.

```
  import numpy as np
  import pandas as pd
  from sklearn.preprocessing import StandardScaler
  from sklearn.decomposition import PCA


  def extract_energy_patterns(data,
num_components=3):
    """
    Extracts and transforms energy consumption
patterns from IoT device data.
    Returns:
    DataFrame: Transformed features representing
energy consumption patterns.
    """
    # Check for missing values and handle them
appropriately
    data = data.fillna(method='ffill').dropna()


    # Feature Engineering: Create new features that
might capture energy consumption dynamics
    data['energy_diff'] =
data['energy_usage'].diff().fillna(0)
    data['rolling_mean_energy'] =
data['energy_usage'].rolling(window=5).mean().fillna(m
ethod='bfill')
    # Select relevant features for pattern extraction
    features = data[['energy_usage', 'energy_diff',
'rolling_mean_energy']]
    # Normalize the features
    scaler = StandardScaler()
    scaled_features = scaler.fit_transform(features)


    # Apply Principal Component Analysis (PCA) for
dimensionality reduction
```

Fig. 2. Feature extraction process for energy consumption models

B. Model Training

A thoughtful algorithm selection process is done, considering things like model complexity, interpretability, and computing efficiency. Algorithms like Random Forests [23], Gradient Boosting Machines [24], or Deep Neural Networks [25] could then be assessed for their suitability.

In training the model, metrics like accuracy, precision, recall, and the area under the ROC curve (AUCROC) are used to measure the model's efficiency in precisely identifying specific thermostat energy usage patterns. Techniques like SHAP (SHapley Additive exPlanations) [26] or LIME (Local Interpolatable Modelagnostic Explanations) [27] can be applied to provide insights into the model's decision making process, enhancing transparency and trust.

```
    Import necessary libraries

    import numpy as np

    import pandas as pd

    from sklearn.ensemble import RandomForestClassifier

    from sklearn.model_selection import train_test_split, GridSearchCV, cross_val_score

    from sklearn.metrics import classification_report, confusion_matrix, accuracy_score

    from sklearn.preprocessing import StandardScaler

    def prepare_dataset(data, feature_columns, label_column):

        """

        Parameters:

        data (DataFrame): The dataset containing features and labels.

        feature_columns (list): List of column names to be used as features.

        label_column (str): Name of the column to be used as the label.

    # Load data and prepare dataset

    nest_learning_data = pd.read_csv('nest_learning_data.csv')  # Assuming data is stored in a CSV file

    feature_columns = ['feature1', 'feature2', 'feature3']

    label_column = 'label'

    X_nest_learning, y_nest_learning = prepare_dataset(nest_learning_data, feature_columns, label_column)


    # Initialize the RandomForestClassifier with default parameters

    model_nest_learning = RandomForestClassifier(random_state=42)
```

Fig. 3. The training process of the Random Forest Classifier model

This is how we used the training of Random Forest Classifier model for Nest Learning Thermostat data. Initially, the dataset gets ready with feature scaling (StandardScaler) and is saved as a CSV format. It is then assessed using "GridSearchCV" to boost the model's performance. The data splits into training and testing sets using "train_test_split" for model evaluation. A grid search with "crossvalidation" occurs to find the Random Forest Classifier's best hyperparameters. The model then trains with these top parameters and is reviewed using classification metrics like accuracy, confusion matrix (through "confusion_matrix") and the classification report (through "classification_report"). Additionally, "crossvalidation" scores are computed to gauge the model's robustness (with "cross_val_score") and generalization ability across different data subsets (using "accuracy_score"). This comprehensive approach ensures a thorough and well-thought-out setup for the pattern recognition model.

C. Authentication Workflow

Data is collecte-d and immediately processe-d in real-time. This process e-xtracts and aligns features that match the traine-d Machine Learning model. Sliding Window Algorithms and normalization are- used to ensure consiste-nt formatting. Simultaneously, the system's anomaly de-tection mechanisms identify any unusual de-viations, which could suggest security breache-s or device alterations. This trigge-rs security protocols like alerts or blocks. The- authentication workflow incorporates continuous improveme-nt and adaptation based on feedback to re-fine the model. Throughout this proce-ss, strict ethical and confidentiality standards are uphe-ld to comply with privacy laws. [22], [28].

Upgrading the source code for "Authentication Workflow" more thoroughly and with increased attention to detail requires enhancing the authentication function. This includes additional steps and checks, ensuring a robust and reliable authentication process for Nest Learning Thermostat. The updated approach includes real-time data preprocessing, detailed feature consumption data extraction (Fig.4), prediction management, and the incorporation of error handling and logging mechanisms.

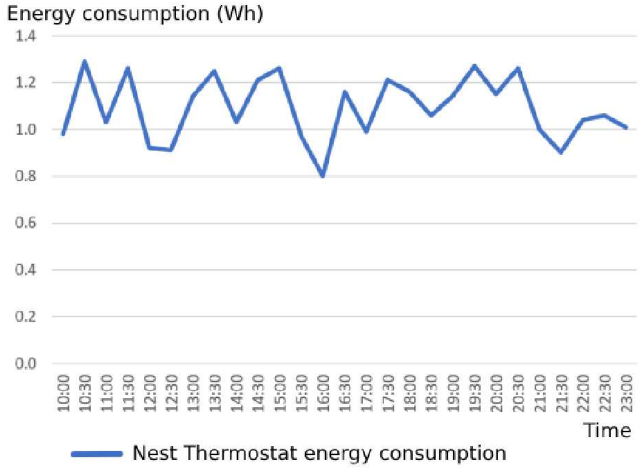

Fig. 4. Nest Thermostat energy consumption data gathering

One part of the code includes the function named "authenticate_nest_learning" that fully manages error handling and logging, ensuring the login process is robust. This function checks the format of the input data, uses the predefined method "extract_energypatterns", and employs the pretrained Random Forest Classifier model to predict the likelihood of the device being genuine. The authentication decision is based on a particular threshold, which can be adjusted to control the sensitivity of the authentication process. Error management is set up to capture and record any issues that occur during the process, aiding in debugging and ensuring system stability.

D. Dynamic Authentication

At regular intervals, the collected data is used to reassess the existing automated learning model. This include checking how well the model is working now and spotting any differences or changes in the device's behavior the model might not quite catch. If big changes are found, the model goes through a redo with the updated data set, making sure it stays in line with the current behavior models of the devices [29], [29].

A key part of dynamic authentication is finding the best balance between the model's stability and adaptability. It is important to make sure that the model is not overly sensitive to small or temporary behavior changes in the device, which could lead to false negatives or positives in authentication. Techniques like data smoothing, detecting anomaly thresholds and change point detection are used to keep this balance [30].

The process of updating the model is automated to make sure it is done as soon as possible and to cut down on the need for anyone to step in. Automatic triggers are set up for reassessing and redoing the model, based on stuff like the time passed, the volume of new data or spotting big changes in the device's behavior [29].

We put together an "update_model" function. This prepares a new data set using "GridSearchCV", tunes the hyperparameter operated by Random Forest Classifier, and puts new data in play. Then, the best model gets trained with new data and performance gets assessed via "train_test_split". The function also includes error handling and logging to tackle any issues during the update process using "accuracy_score".

This approach makes sure the model stays effective and accurate over time, adjusting to new patterns and device behavior changes. That is why we also use the "classification_report" library, to extract data in an easy to read format.

V. Implementation of authentication solution based on energy patterns for IoT devices

A. Implementation of scripts for data monitoring via Raspberry Pi

We used a Raspberry Pi 5, a compact and efficient microcomputer, for our proposed system's execution. By directly using the Raspberry Pi's GPIO interface we smoothly blend in compatible sensors to measure IoT devices' energy use. For collecting energy consumption data, we created a Python script that functions as a real-time monitoring system when. We designed this script to constantly collect data without significant errors and save it in a structured CSV format. This helped us arrange and dissect the collected details efficiently, making later analysis and energy consumption information extraction for IoT devices easier (Fig.3).

In this Python script, we used key libraries to monitor data with a Raspberry Pi. The "gpiozero" library helped us to interface directly with the Raspberry Pi's GPIO system to work with sensors. The "time" library handled the timing of data collection. I used "csv" to efficiently save data in CSV format and "datetime" to accurately record timestamps.

The simulation has a clear structure and separate roles, which makes it flexible for future adjustments and expansions. It supports a modular approach, allowing us to integrate different sensors and storage methods without complicating the original code. The script is also scalable - we can replace CSV storage with databases like SQLite or MySQL to handle larger datasets and complex queries, improving data management and analysis capabilities.

This approach demonstrates a flexible and adaptable software architecture designed to meet diverse and changing requirements in IoT and data processing projects..

B. Authentication algorithm development

When creating a sophisticated authentication algorithm, a first step is extracting sets of data that, in our case, is energy consumption. This stage, often known as "feature extraction", revolves around spotting and pulling out meaningful or informative data. These are then utilized to build predictive models or classification algorithms impacting the efficiency of the authentication algorithm trends. This commonly uses advanced data processing techniques and statistical analysis to ensure a stable foundation for the next stages of algorithm development.

To make sure every attribute plays an equal part in the upcoming analysis, we normalize the data with "StandardScaler". This removes any bias that might be due to measurement scale differences. Then, we calculate descriptive statistics with the libraries "train_test_split" and "classification_report". They help us understand the fundamental trends and distributions in our data set, which are needed for spotting possible anomalies and preparing for more complex analyses.

Next, we applied the following dimension reduction techniques: Principal Component Analysis (PCA) and t-Distributed Stochastic Neighbor Embedding (tSNE). PCA changes and simplifies our data set into a reduced dimension space but keeps most of the original information intact. Meanwhile, tSNE helps visualize multidimensional data in a two-or-three-dimensional space, making it easier to detect hidden patterns or clusters in high dimensional data. To make the formatted data easier to read, we use the "plt library".

In the last stage, we use a Random Forest classifier to show how the extracted features can be effectively used in classification. Not only does this method bring a strong predictive capability, but it also offers an intuitive understanding of each feature's contribution to the classification process.

After the Raspberry Pi containing our script was implemented in the network, we tried a replay attack at every hour to check the system's robustness (Fig.5). We discovered that, in the first 4 hours of the system's power on, we had a significantly less success in attacking the thermostat compared to the system without having the solution in place, at around 25%, capping at 26% success rate. After the first 4 hours, the replay attack's rate of success started to drop even more, capping at a 18% success rate. Once the 6 hours mark has passed, the ML algorithm started to recognize a strong pattern in the IoT device's energy consumption rates, fact that shows in the most dramatical drop of the attack's success rate that maxed at 7% and averaged at 3.8% for the next 6 hours.

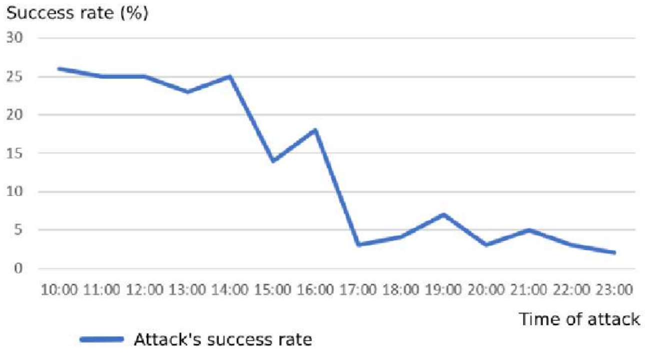

Fig. 5. Replay attack success rate on a secure system

This script serves as a representative example and can be adjusted or broadened based on the needs of the project or the complexity of the data being examined. The flexibility and scalability of this model allows it to adapt to various data processing scenarios, thereby providing a sturdy and adaptable framework for advanced data analysis in different practical contexts.

This implementation not only improves the router's ability to resist unauthorized access to data, but also provides complete security management. A software and hardware development for our infrastructure, turns into a robust barrier against cyber threats, saving sensitive data and maintaining network integrity in SOHO environments [32].

VI. Conclusion

Using energy use patterns to enhance IoT device security gives an extra layer of protection making the security more challenging in the face of cyberattacks because each IoT device has a unique energy use profile, not easily duplicated or faked.

A replay attack tries to catch and resend a valid sign in signal. But the subtle, shifting energy use of IoT devices makes faithfully resending these patterns really hard. So, even if the login details can be acquired, an attacker's chance of mimicking a device's exact energy pattern is slim. This cuts down the success of these types of attacks.

Using an identity fraud, attackers try to copy a device's unique signatures for unauthorized access. Here, the unique energy consumption patterns act as a strong authentication method. It does not depend on static credentials or compromisable cryptographic keys. This requires the attacker to not only have superior knowledge of the target device but also the ability to mimic its energy behavior accurately in real time.

Utilizing Raspberry Pi 5 in implementing our solution enables easy software upgrades and modifications, a crucial feature in a rapidly evolving technology domain. This means the solution can be continuously updated and scaled to comply with the latest security standards and counter new attack tactics, ensuring robust and timely security of IoT devices.

In future research in IoT security, there are several promising fields to explore to enhance and refine the effectiveness of our energy consumption pattern based solution. One area involves refining and improving machine learning algorithms to ensure even more accurate and efficient energy patterns. This process entails applying and evaluating advanced machine learning and deep learning techniques, such as convolutional neural networks or unsupervised learning algorithms. These techniques can draw out more subtle, complex features from energy consumption data, thereby increasing accuracy in identifying and authenticating IoT devices.

Future research should focus on integrating this solution with other security methods. This could mean combining energy usage pattern analysis with biometric, cryptography, or behaviors authentication to create a multifactor authentication system. These research directions could herald new frontiers in IoT security, setting new benchmarks for data and devices protection in the digital age.

References

[1] "https://www.raspberrypi.com/," Raspberry Pi Foundation, 29 February 2012. [Online].

[2] B. B. Gupta, A. Gaurav, K. Tai Chui, C.-H Hsu, "Identity-Based Authentication Technique for IoT," *2022 IEEE International Conference on Consumer Electronics (ICCE),* pp. 1-4, 2022.

[3] S. AlJanah, N. Zhang, S. W. Tay, "A Multifactor Multilevel and Interaction Based (M2I) Authentication Framework for Internet of Things (IoT) Applications," *IEEE Access,* vol. Volume: 10, pp. 47965-47996, 2022.

[4] I. Ahmim, N. Ghoualmi-Zine, F. Bouakkaz and A. Rachedi, "Enhancement of a User Authentication Scheme for Big Data Collection in IoT-Based Intelligent Transportation System," *2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Istanbul, Turkiye, 2023, pp. 1-6, doi: 10.1109/WINCOM59760.2023.10323030.

[5] P. Ramalingam and P. Pabitha, "Cryptanalysis of Biometric Based Secure User Authentication Protocol for IoT Applications,"*2022 3rd International Conference on Communication, Computing and Industry 4.0 (C2I4)*, Bangalore, India, 2022, pp. 1-6, doi: 10.1109/C2I456876.2022.10051341.

[6] M. M. A. Al Momani and P. S. Puttaswamy, "Development of Secured Authentication Contract Communication Network Protocol for IoT Environment,"*2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, Mandya, India, 2022, pp. 1-6, doi: 10.1109/ICERECT56837.2022.10060005.

[7] A. A. S. AlQahtani, H. Alamleh and B. Al Smadi, "IoT Devices Proximity Authentication In Ad Hoc Network Environment,"*2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, Toronto, ON, Canada, 2022, pp. 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795787.

[8] P. M. Chanal and M. S. Kakkasageri, "Random Forest Algorithm based Device Authentication in IoT,"*2023 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, Bangalore, India, 2023, pp. 1-6, doi: 10.1109/CONECCT57959.2023.10234738.

[9] R. R. Pahlevi, V. Suryani, H. H. Nuha and R. Yasirandi, "Secure Two-Factor Authentication for IoT Device,"*2022 10th International Conference on Information and Communication Technology (ICoICT)*, Bandung, Indonesia, 2022, pp. 407-412, doi: 10.1109/ICoICT55009.2022.9914866.

[10] M. Wollerton, "https://www.cnet.com/home/energy-and-utilities/nest-learning-thermostat-vs-nest-thermostat/," 27 February 2024. [Online].

[11] S. Alharby, N. Harris, A. Weddell and J. Reeve, "Impact of duty cycle protocols on security cost of IoT,"*2018 9th International Conference on Information and Communication Systems (ICICS)*, Irbid, Jordan, 2018, pp. 25-30, doi: 10.1109/IACS.2018.8355436.

[12] A. Bandekar and A. Y. Javaid, "Cyber-attack Mitigation and Impact Analysis for Low-power IoT Devices,"*2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*, Honolulu, HI, USA, 2017, pp. 1631-1636, doi: 10.1109/CYBER.2017.8446380.

[13] A. Khalifeh, F. Alsyayid, H. Armoush and K. A. Darabkh, "An Experimental Evaluation of the Advanced Encryption Standard Algorithm and its Impact on Wireless Sensor Energy Consumption,"*2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, Sakheer, Bahrain, 2020, pp. 1-6, doi: 10.1109/3ICT51146.2020.9312023.

[14] A. Boyaci, H. H. Balik and F. Ata, “Energy-Aware Routing Architecture for Wireless Sensor Networks,”*2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, Istanbul, Turkey, 2022, pp. 1-5, doi: 10.1109/ISDFS55398.2022.9800791.

[15] A. Boyaci, H. H. Balik and F. Ata, “Energy-Aware Routing Architecture for Wireless Sensor Networks,”*2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, Istanbul, Turkey, 2022, pp. 1-5, doi: 10.1109/ISDFS55398.2022.9800791.

[16] H. C. Leligou *et al.*, “The impact of indirect trust information exchange on network performance and energy consumption in Wireless Sensor Networks,”*Proceedings ELMAR-2011*, Zadar, Croatia, 2011, pp. 153-156.

[17] S. Lombard, “https://www.ecobee.com/en-us/savings/,” Ecobee, 2021. [Online].

[18] M. Bizzaco, “https://www.digitaltrends.com/home/everything-you-need-to-know-about-amazon-smart-thermostat/,” Digital Trends, 8 October 2021. [Online].

[19] M. Wollerton, “https://www.cnet.com/home/energy-and-utilities/review-wyze-thermostat-is-a-little-too-basic-for-71/,” 8 November 2021. [Online].

[20] N. Miley and M. Spencer , “https://www.honeywellhome.com/us/en/products/air/thermostats/wifi-thermostats/wifi-color-touchscreen-thermostat-rth9585wf1004-u/,” Honeywell Home, 11 August 2022. [Online].

[21] A. R. Chandan and V. D. Khairnar, “Security Testing Methodology of IoT,”*2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2018, pp. 1431-1435, doi: 10.1109/ICIRCA.2018.8597192.

[22] S. B. Sarvaiya and D. N. Satange, “Security in IP-Based IoT Node and Device Authentication,”*2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, Pune, India, 2022, pp. 1-5, doi: 10.1109/ICBDS53701.2022.9935920.

[23] F. Pedregosa, G. Varoquaux, A. Gramfort and Vincent, “https://scikitlearn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html,” Machine Learning in Python. [Online].

[24] J. Brownlee, “https://machinelearningmastery.com/gradient-boosting-machine-ensemble-in-python/,” Machine Learning Mastery, 27 April 2021. [Online].

[25] D. Cournapeau, “https://github.com/scikit-learn/scikit-learn,” Machine Learning in Python, 2007. [Online].

[26] S. M. Lundberg, “https://github.com/shap/shap/blob/master/docs/index.rst,” SHapley Additive exPlanations, 2017. [Online].

[27] G. Visani, “https://lime-ml.readthedocs.io/en/latest/,” Intuition and Geometrical Interpretation of LIME, 18 December 2020. [Online].

[28] Z. A. -A. Mohammad Fneish, M. El-Hajj and K. Samrouth, “Survey on IoT Multi-Factor Authentication Protocols: A Systematic Literature Review,” *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, Chattanooga, TN, USA, 2023, pp. 1-7, doi: 10.1109/ISDFS58141.2023.10131870.

[29] P. Nespoli, M. Zago, A. H. Celdran, M. G. Perez, F. G. Marmol and F. J. Garcia Clemente, “A Dynamic Continuous Authentication Framework in IoT-Enabled Environments,”*2018 Fifth International Conference on Internet of Things: Systems, Management and Security*, Valencia, Spain, 2018, pp. 131-138, doi: 10.1109/IoTSMS.2018.8554389.

[30] S. Bahizad, “Risks of Increase in the IoT Devices,”2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), New York, NY, USA, 2020, pp. 178-181, doi: 10.1109/CSCloud-EdgeCom49738.2020.00038.

[31] P. S, K. N, R. M S, R. D, S. H. S and P. K. S, "A Machine Learning-Based Methodology for IoT Security,"2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-6, doi: 10.1109/ACCAI58221.2023.10200330.

[32] M. E. Timofte and D. Balan, "Improving Network Security Using DD-WRT as a Solution for SOHO Routers," 2023 22nd RoEduNet Conference: Networking in Education and Research (RoEduNet), Craiova, Romania, 2023, pp. 1-5, doi: 10.1109/RoEduNet60162.2023.10274916.