JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

INTELLIGENT ENERGY EFFICIENCY SYSTEM USING GRADIENT DESCENT ALGORITHM IN IOT

Mrs.VARALAKSHMI[1], HARISANKARAN S[2], SURYA KUMAR N[3], KISHOR S[4]

[1]Assistant Professor, Department of Computer Science & Engineering,

[2,3,4]B.Tech, Department of Computer Science & Engineering,

[1,2,3,4]Manakula Vinayagar Institute of Technology, Puducherry, India.

ABSTRACT: Many household items, including fans, air conditioners, lights, and other gadgets, are now connected to the Internet to communicate with one another and allow the environment to function more intelligently with fewer human interventions. The smart house features a central management system that manages multiple gadgets to improve communication, security, and energy efficiency, among other things. The main issues with the current approach are high energy costs, a large installation footprint, and low-efficiency levels (accuracy is 75%). By gathering information from multiple sensors, the proposed work improves the security of the automation system using the AES algorithm in a WiFi-enabled milieu. When training a model to identify, categorize, and gather data from the milieu, the SGDClassifier algorithm is used. This methodology's primary goal is to prioritize devices depending on their power efficiency, limit CPU usage using the Varak protocol and use a separate network for security. This study increases the accuracy of the model to 85 percent while using less energy and having great computational power.

Keywords: IoT, AES algorithm, SGDClassifier, protocol.

I. INTRODUCTION

The term "Internet of Things" (IoT) describes a network of actual machines, automobiles, and other physical objects that have sensors, software, and network connectivity built into them so they can gather and share data. [10] Smart home technology is one area where IoT devices have become increasingly popular, allowing homeowners to automate and control various aspects of their homes through a central hub or a smartphone app. One of the main benefits of using IoT devices in a smart home is convenience. [23] With the ability to control and monitor various systems and appliances remotely, homeowners can save time and effort by not having to physically adjust settings or check on their homes. For example, a smart thermostat can automatically adjust the temperature of a home based on the time of day and the homeowner's schedule, while an intelligent security system can alert homeowners of any unusual activity while they are away. One of the main benefits of using IoT devices in an intelligent home is convenience. With the ability to control and monitor various systems and appliances remotely, homeowners can save time and effort by not having to physically adjust settings or check on their homes. [13] Some smart home systems even offer integration with professional monitoring services, providing homeowners with an additional layer of protection. Smart home technology can also improve the accessibility of a home for people with disabilities or mobility issues. [22] IoT devices such as smart door locks, smart thermostats, and smart lighting systems can be controlled remotely, making it easier for people with mobility issues to access and control different aspects of their homes. In addition to the benefits for homeowners, smart home technology can also have a positive impact on the wider community. For example, the use of smart thermostats and smart lighting systems can help to reduce energy consumption and carbon emissions, contributing to a more sustainable and environmentally-friendly society. [10] Smart home technology can also play a role in improving public safety, through the use of smart security systems and emergency response systems. Overall, the potential benefits of IoT devices in a smart home are numerous and varied, offering convenience, energy efficiency, security, customization, accessibility, and a range of other benefits to homeowners and the wider community. As technology continues to evolve and improve,

the adoption of smart home technology will likely continue to increase in the coming years. [15] One important aspect to consider when using IoT devices in a smart home is security. As these devices are connected to the internet and often transmit and store sensitive data, it is important to ensure that they are secure and protected from potential cyber threats. Use a secure network: Make sure to use a secure and encrypted network, such as a virtual private network (VPN), to protect your smart home system from external threats. [19] Research the security of different devices: Before purchasing any smart home devices, research their security features and consider the security track record of the manufacturer. Choose devices from reputable companies with a history of good security practices. [9] Use a smart home hub or platform: Many smart home systems offer a central hub or platform that allows you to manage and control all of your devices from one place. This can help to improve security by providing a single point of access and control. By following these steps, homeowners can help to ensure the security of their smart home system and protect their personal data. It is also important to be aware of potential cyber threats and to regularly review the security of your system to ensure it remains secure. Considering all the things in mind and we are giving a slightly different and more efficient way to make those intelligent systems even more intelligent by using CCTV cameras to capture the video lively and if any motion (i.e Human Motion) is detected in the area that camera is capturing and if any IoT devices in the captured area are controlled more efficiently.

II. LITERATURE REVIEW

A detailed review of some of the prominent styles related to energy effective, optimized recognition with some Machine Learning algorithms with a lot of datasets is carried out in [2]. The development of smart grid technology in [1] has made it possible to account for every minute of energy use in intelligent constructions. Due to that, scientists and experimenters are working on optimizing energy operation, especially in smart metropolises, besides furnishing a comfortable terrain. The prognosticated stoner parameters have bettered the system's overall performance in terms of ease of use of smart systems, energy consumption, and comfort indicator operation. The club algorithm converges veritably snappily at the early stage and also the confluence rate slows down, Accuracy may be limited if the number of function evaluations isn't high. In [2] several home appliances, similar as air conditioners, heaters, and refrigerators were connected to the Internet, and they came targets of cyberattacks, which beget serious problems similar as compromising safety and indeed harming druggies. We attained discovery rates exceeding 90 for anomalous operations with lower than 10 of misdetections when our system- observed event sequences related to the operation. Anomaly discovery approaches generally produce a large number of false admonitions due to the changeable actions of druggies and networks. In- home monitoring [3] exertion recognition significantly enhances the performance of healthcare monitoring and exigency- control operations for the senior and people with special requirements. With the accelerated development of Internet-of-effects operations, automated reflection processes have surfaced to understand resident gestures that like for in terms of conditioning. The proposed methodology models conditioning grounded on spatial honored conduct, with every exertion anticipated to have a direct relationship with a specific set of locales. Reflection ways have time-consuming (precious), delicate, private, and inconsistent in the Manual. It has Error-prone and less accurate reflection in Automatic. It has lower time than automatic reflection and lesser time than homemade reflection in Semi-Automatic. In [5] to resolve data sequestration enterprises using discrimination sequestration, the traditional Laplacian medium cannot be used to descry overloads and the standard coin-flipping algorithm gives a high chance error of wasted energy computation. Grounded on a 30- day sample period of factual BEMS, both the sequestration and usability of the proposed processes have been compared with the traditional styles in terms of the sequestration loss parameters, the reported error of energy consumption, the correctness of load discovery, and the error of the wasted energy computation. Grounded on the accessible effectiveness, these proposed processes are recommended for further extension to apply at BEMS data gateways in real-time. (BEMS) uses colorful detectors and smart measures to descry power consumption and stoner movement within structures. In [6] the styles to manage similar processes can be classified into tackle-grounded styles, including protrusive cargo monitoring, and software-grounded styles pertaining to non-intrusive cargo monitoring. Although ILM results can be fairly precious, they give advanced effectiveness and trustability, the proposed IoT armature consists of the appliances subcaste, perception subcaste, communication network subcaste, middleware subcaste, and operation sub caste. The main function of the appliance recognition module is to label detector data and allow the perpetration of different home operations. Including protrusive cargo monitoring (ILM) and software-grounded styles pertaining to (NILM). In [4] with the nonstop development of Internet of effects technology, exploration of smart home surroundings is being conducted by numerous experimenters. In smart home surroundings, home druggies can ever pierce and control a variety of home biases similar to smart curtains, lights, and speakers placed throughout the house. Despite furnishing accessible services, including home monitoring, temperature operation, and diurnal work backing, smart homes can be vulnerable to vicious attacks because all dispatches are transmitted over insecure channels. also, home bias can be a target for device prisoner attacks since they're placed in physically accessible locales. But secure authentication and crucial agreement scheme are needed to help similar security problems. In [7] smart home technology perpetration remains an essential aspect of the Internet of effects. There's a limited number of SLR studies on smart home monitoring technology. thus, the current study assesses the literature to collect substantiation regarding studies on smart home monitoring technology implantation. (SLR) on smart home technology, perpetration is lacking. There's a limited number of SLR studies on smart home monitoring technology.

III. PROPOSED METHODOLOGY

We proposed a general model in this study to address the problems in the previously cited references, along with energy efficiency, optimal recognition, and machine learning methods. Here, we put forth three key procedures including image recognition, machine learning, and an IoT device controller. The potent tool for computer vision and image processing jobs is utilized in a wide range of applications. Using this, the video is captured by cv2.VideoCapture() function takes the parameter that indicates the camera we are using a single camera, in this case, the parameter is 0, it differs based on your system. And detecting the pose i.e body detection we are using cvzone.PoseModule which is used to detect body motion, here we are taking shoulder body points i.e. 11 and 12 these are the points to detect the full human body and fix in a box, after detecting the body motion we are setting a line on screen using cv2.line() method (Syntax: cv2.line(image, start_point, end_point, color, thickness)in which takes a parameter of image start point: These are the coordinates at which the line should begin to be drawn. The coordinates are shown as pairs of two values, or tuples (X coordinate value, Y coordinate value). endpoint: These are the line's final coordinates. The coordinates are shown as pairs of two values, or tuples (X coordinate value, Y coordinate value). The line's intended color is indicated by this color. We pass a tuple for RGB. as in (255, 0, 0) for the color blue. thickness: This term refers to the line's px thickness. After securing the lines as boundaries on the screen, we must determine whether or not the body crosses the line inside the boundary. To do this, we must change the line's color from blue to red (0, 0, 255). When an object—in this case, the human body crosses the line, the color changes from blue to red. This allows us to determine whether or not the object crosses. We are going to create some cross lines inside the boundary area to verify whether the object stays inside the area that the camera watches. These lines will show whether the thing stays inside the boundary or not. The IoT devices inside the barrier must be turned on automatically when the object crosses the line and remains inside it. In order to automatically turn on or off the devices linked to the wifi, we are utilizing a subprocess module for this automation phase, where we must fix the time in seconds. If the devices we are using have the same wattage (let's say a 9-watt bulb), then this works just fine, but if we are using different wattage bulbs in various locations, then we must first turn off the high-wattage bulb before turning off the others in order to conserve energy. We are utilizing machine learning to automate the process, forecast the devices it wants to turn on or off, and train the algorithm to generate more accurate predictions. We are using a Machine Learning algorithm to predict the output more accurately called the Stochastic Gradient Descent Algorithm. The foundation of almost all machine learning algorithms is mathematics. Similar to this, the gradient descent method used in machine learning is inspired by mathematics and can be used to first-order optimization. Essentially, it may be used to locate the local minima of any differential function. When discussing how the gradient descent algorithm generates steps, we see that it does so by repeatedly moving away from any place where the gradient is steepest. A gradient ascent, which brings us to a local maximum, is what happens when the identical action is carried out in the opposite direction. We can claim that machine learning has the potential to be used for optimization that enhances the learning process. Another optimization technique is stochastic gradient descent. The objective function that needs to be optimized has the right smoothness characteristics, which sets stochastic gradient descent apart from gradient descent. It is possible to think about optimizing a smooth objective function as the stochastic approximation of gradient descent. This idea comes from mathematics as well, and it may be applied to machine learning to minimize the objective function, which entails locating the objective function's local minima with the appropriate degree of smoothness. It is possible for the smoothness qualities to be sub- or differently differentiable. Let's say there is an optimization function as the following:

$$\Theta j = \Theta j - \alpha\, (\partial/\partial \Theta j)\, J(\Theta)$$

here, $J(\Theta) = 1/m\ m^{\wedge}\sum i=1\ (y - \hat{y})\ i^{\wedge}X\_ j$

In this function, the parameter J(Θ) must be calculated because it minimizes the function. Stochastic gradient descent will focus on the following steps for estimating the J(Θ):

setting up the random J(Θ) words

1. The predictions will be calculated using the O-term algorithm.
2. The mean square error between actual values and projections should be calculated, utilizing the previous value of the parameter and the mean square error, determining the updated value of the parameter (O).
3. Until convergence, keep calculating the parameter's updated value and forecast.

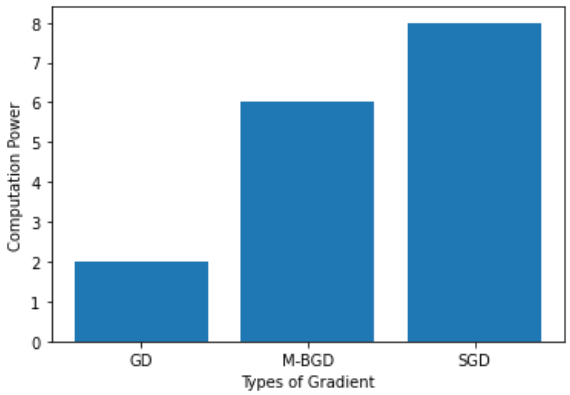

Fig.1 SGD algorithm graph

The stochastic gradient descent (SGD) technique is a simple but very powerful approach to updating linear classifiers and regressors under convex loss functions, such as those employed by (linear) Support Vector Machines and Logistic Regression. Although SGD has been around for some time in the machine learning community, it has only lately started to get a lot of interest in the context of large-scale learning. SGD is only an optimization method and does not, strictly speaking, belong to any one family of machine learning models. It is essentially a model-training technique. For each SGDClassifier or SGDRegressor instance, there is typically a sci-kit-learn API comparable estimator, perhaps using a different optimization technique. A model equivalent to Logistic Regression that is fitted by SGD rather than one of the other solvers in Logistic Regression is

produced, for instance, by using SGDClassifier (loss='log loss'). Similar to Ridge, SGDRegressor (loss='squared error', penalty='l2') finds alternative solutions to the same optimization problem. The effectiveness and simplicity of implementation are two benefits of stochastic gradient descent (lots of opportunities for code tuning). We are doing this using SGDClassifier, which implements a straightforward stochastic gradient descent learning procedure and supports various classification loss functions and penalties. The decision boundary of an SGDClassifier that was trained with the hinge loss and is comparable to a linear SVM is shown below.

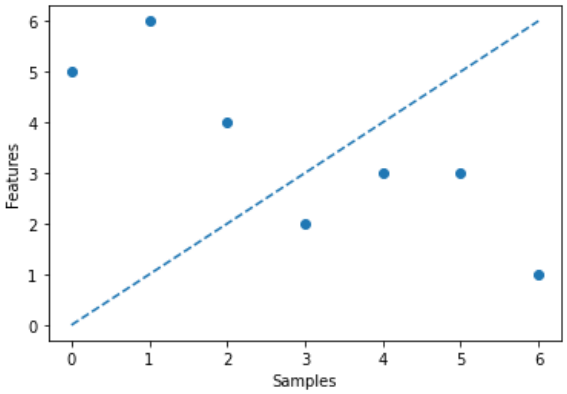

Fig 2 SGDClassifier

As with previous classifiers, SGD requires two arrays to be fitted: an array X of the form (n samples, n features) storing the training samples and an array Y of shape (n samples,) holding the target values (class labels) for the training samples. The syntax from sklearn.linear model import SGDClassifier is used to import the SGDClassifier. After importing this, we must use the fit() function to fit the data. The model can then be used to forecast new values after being fitted. The IoT devices inside the boundaries that the CCTV camera records are controlled after the values are predicted more accurately. To use this as a more effective method of controlling IoT devices, we must download and run the application.

IV. CONCLUSION

The Internet of Things (IoT) has numerous uses in numerous industries. It has undergone numerous developments in a variety of fields. This paper discusses an IoT breakthrough that makes human tasks increasingly easier while also raising security concerns. Additionally, machine learning algorithms are applied to make predictions more accurate, which increases their usefulness. This essay outlines obstacles and issues that can be resolved utilizing this approach across a variety of industries. We don't need to spend a lot of money on expensive gear to tackle those problems; just use a quick program.

REFERENCES

[1] Abdul Salam Shah, Haidawati Nasir, Muhammad Fayaz, Adidah Lajis, Israr Ullah and Asadullah Shah “Dynamic User Preference Parameters Selection and Energy Consumption Optimization for Smart Homes Using Deep Extreme Learning Machine and Bat Algorithm”.Malaysia published on 10 November 2020, IEEE.

[2] Masaaki Yamauchi, Yuichi Ohsita, Masayuki Murata, Kensuke Ueda, Yoshiaki Kato “Anomaly Detection in Smart Home operation From User Behaviors and Home Conditions “, published on 2 May, 2020, IEEE.

[3] Mohammed Gh. Al Zamil, Majdi Rawashdeh, Samer Samarah, Ml Shamim Hossain, Awny Alnusair, Sk Md Mizanur Rahman “An Annotation Technique for In-Home Smart Monitoring Environments”.Saudi Arabia, published on 4 December 2017, IEEE.

[4] Yeongjae Cho, Jihyeon Oh, Deokkyu Kwon, Seunghwan Son, Joonyoung Lee, Youngho Park “A Secure and Anonymous User Authentication Scheme for IoT Enabled Smart Home Environments Using PUF”.South Korea, published on 21 September 2022, IEEE.

[5] Siravit Kwankajornkeat and Chaodit Aswakul “Differential Private Motion Sensor and Wasted Energy in Building Energy Management System”.Thailand, published on 24 December 2021, IEEE.

[6] Patrica Franco, Jose Manuel Martinez, Young-chon Kim, Mohamed A. Ahmed “IoT Based Approach for Load Monitoring and Activity Recognition in Smart Homes”.South Korea, published on 18 March 2021, IEEE.

[7] Kholoud Maswadi, Norjihan Binti Abdul Ghani, Suraya Binti Hamid “Systematic Literature Review of Smart Home Monitoring Technologies Based on IoT for the Elderly”.Saudi Arabia, published on 6 May 2020, IEEE.

[8] Debnath, B.; Dey, R.; Roy, S. Smart switching system using Bluetooth technology. In Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, published on 4–6 February 2019, IEEE.

[9] Anandhavalli, D.; Mubina, N.S.; Bharath, P. Smart Home Automation Control Using Bluetooth and GSM. Int. J. Inf. Futur. Res. 2015,2,2547-2552, IEEE.

[10] Froiz-Mergiz, Fernández-Caramés, T.M.; Fraga-Lamas, P.; Castedo, L. Design, Implementation and Practical Evaluation of an IoT Home Automation System for Fog Computing Applications Based on MQTT and ZigBee-WiFi Sensor Nodes, 2018, IEEE.

[11] Murthy, A.; Irshad, M.; Noman, S.M.; Tang, X.; Hu, B.; Chen, S.; Khader, G. Internet of Things, a vision of digital twins

and casestudies. In IoT and Spacecraft Informatics; Elsevier: Amsterdam, The Netherlands 2022, IEEE.

[12] A. Singaravelan 1 Gunapriya B. 1, Kowsalya M. 2, (Senior Member, IEEE), J. Prasanth Ram 3, (Member, IEEE), and Young-jin Kim 3, (Senior Member, IEEE). Application of Two-Phase Simplex Method (TPSM) for an Efficient Home Energy Management System to Reduce Peak Demand and Consumer Consumption Cost. India, published on 12 April 2021, IEEE.

[13] Leo Willyanto Santoso, Resmana Lim, and Kevin Trisnajaya, Member, KIICE. Smart Home System Using Internet of Things. Indonesia, published on March 2018, IEEE.

[14] Patricia Franco, Jose Manuel Martinez, (Member, IEEE), Young-Chon Kim, and Mohamed A. Ahmed, (Member, IEEE). Framework for IoT-Based Appliance Recognition in Smart Homes. South Korea, published on 29 September 2021, IEEE.

[15] Mrs I Varalakshmi, M Thenmozhi. Mitigation of DDoS attack using Machine Learning Algorithms in SDN_IoT environment. India, published on 14 October 2021, IEEE.

[16] Jungyoon Kim, Songhee Chon, and Jihye Lim. IoT-Based Unobtrusive Physical Activity Monitoring System for Predicting Dementia. United States of America, published on 3 March 2022, IEEE.

[17] Sergio H.M.S. Andrade, Gustavo O. Contente, Lucas B. Rodrigues, Luiguy X. Lima, Nandamudi L. VijayKumar, and Carlos Renato L. Frances. A Smart Home Architecture for Smart Energy Consumption in a Residence with Multiple Users. Brazil, published on 18 January 2021, IEEE.

[18] Paola Pierleoni , Alberto Belli , Omid Bazgir, Lorenzo Maurizi, Michele Paniccia, and Lorenzo Palma. A Smart Inertial System for 24h Monitoring and Classification of Tremor and Freezing of Gait in Parkinson's Disease. Published on 1 December 2019, IEEE.

[19] Mrs I Varalakshmi, S Kumarakrishnan. Navigation system for the visually challenged using Internet of Things. India, published on 29 March 2019, IEEE.

[20] Zhiqing Zhou, Heng Yu, and Hesheng Shi. Optimization of Wireless Video Surveillance System for Smart Campus Based on Internet of Things. China, published on 27 July 2020, IEEE.

[21] Olutosin Taiwo and Absalom E. Ezugwu. Internet of Things-Based Intelligent Smart Home Control System. South Africa, published on 24 September 2021, IEEE.

[22] Mrs I Varalakshmi, M Thenmozhi, R Sasi. Detection of Distributed Denial of Service Attack in an Internet of Things Environment-A Review. India published on 30 July 2021, IEEE

[23] Mrs. Jyotsna P. Gabhane, Ms. Shradha Thakare, Ms. Monika Craig. Smart Homes System Using Internet-of-Things: Issues, Solutions, and Recent Research Directions. India, published on May 2017, IEEE.