Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7765928

SGDA: PERFORMANCE ANALYSIS OF LESS ENERGY CONSUMPTION IN SMART IOT USING STOCHASTIC GRADIENT DESCENT ALGORITHM

Mrs.I.Varalakshmi1, S.Harisankaran2, S.Kishor3, Surya Kumar N4
[1]Assistant Professor(SG), Department of Computer Science & Engineering,
Manakula Vinayagar Institute of Technology, Puducherry, India.
[2,3,4]B.Tech, Department of Computer Science & Engineering,
Manakula Vinayagar Institute of Technology, Puducherry, India.

ABSTRACT: Many subsystems, including those for lighting, security, weather management, entertainment etc., are managed and coordinated by a central control system in smart homes. By gathering information from multiple sensors, the proposed method improves the automation system remotely using a WiFi-enabled environment. Contours are used to categorize objects and people in the surroundings. Performance is measured by analyzing the IDI datasets (IoT Device identification) and controlled. The main objective of this system is to behave system intelligently. This system can achieve low energy consumption and excellent computational performance, when the devices are increased. The challenges faced in the existing system : high energy consumption, large installation footprint, and subpar effectiveness. It provides the accuracy of 75% to 94% based on the parameters :Pattern, light, Temp, Humidity, Motion etc., using machine learning techniques. Our proposed system, training a model to recognise the power consumption of the devices, categorize and acquire data from the environment using SGDClassifier algorithm. The major objective of this system is to classify the devices and control them based on the high and low power consumption. Performance analysis of algorithms and epochs are discussed and experimental results show the system accuracy from 95.89%- 96.75% based on Human Recognition Percentage(HRP), Watt, Epoch and learning rate parameter and achieves less consumption time with low computational energy.
Keywords: IoT, IDI dataset, SGDClassifier, Accuracy.

I.INTRODUCTION

The suggested solution uses computer vision to identify people in a certain region and adjust the location's Internet of Things (IoT) devices. The system captures and processes real-time video streams using Python's OpenCV and MediaPipe libraries, and it uses a machine learning algorithm that was trained on two datasets to determine if an image contains humans or not. The system will use Python's subprocess module to transmit orders to nearby IoT devices, turning them on or off as needed, if people are found. The suggested system is an Internet of Things (IoT) human detection and control system that makes use of computer vision and machine learning techniques to identify the human presence in a specific region and adjust the IoT devices inside[50]. To offer a seamless and automated user experience, the system is created to be deployed in a range of situations, such as smart homes or office buildings. Using a mix of the OpenCV and MediaPipe libraries, the system employs two datasets that are trained using the stochastic gradient descent machine learning technique to successfully recognise humans in real time [47]. To save energy and cut expenses, the system leverages Python's

subprocess module to automatically turn off any nearby IoT devices when it detects a person nearby. The proposed system is created with scalability and collaboration in mind in addition to its useful applications. It is easily adaptable to various hardware setups and can be released open-source to encourage wider developer community adoption and participation. To ensure that sensitive data is handled in a secure and morally sound manner, the system was also developed with privacy and security in mind. The system is made to be reliable and precise, able to recognize people in a variety of lighting situations and camera stances [41]. The system is appropriate for a variety of applications, from home automation to security and surveillance, thanks to the use of machine learning, which enables the system to learn from examples and improve over time. The suggested system is made up of several crucial parts, such as picture pre-processing, model training, model evaluation, real time video stream processing, and IoT device control. Each of these parts is essential to the system's overall performance and helps to make sure that it can reliably detect human presence and effectively operate IoT devices. Smart lights, thermostats, and power outlets are just a few examples of IoT devices that can be integrated into the suggested system. Additionally, the system may be altered to fit different user preferences, such as choosing which IoT devices should be turned off when humans are detected or modifying the sensitivity of human detection [49]. It is possible to assess the system's accuracy and dependability using a variety of performance indicators, including precision, recall, and F1 score. These indicators can be used to assess the system's effectiveness and pinpoint areas that need improvement. Users will be able to watch live video feeds of the area in issue if the system is built with real-time video processing capabilities [31]. This can be especially helpful for keeping an eye on places where safety or security are issues, such as public spaces or business buildings. To make it simpler for users to control their IoT devices, the proposed solution can be integrated with popular home automation systems like Amazon Alexa or Google Home. Users can accomplish this by giving their voice assistants orders. Hardware requirements: The suggested system may require specific hardware components, such as a camera or Internet of Things (IoT) devices that use Python's subprocess module [27]. You might also include a description of the system's essential technical needs as well as a list of the required hardware components. Dataset selection and preparation: Given that the system entails training a machine learning algorithm on two datasets, you might need to go into further detail about the dataset selection and preparation process. This could contain specifics like the size of the datasets, the method used to gather the data, and any pre-processing measures that were done to clean and normalize the data. Model choice and optimization: Stochastic gradient descent is a well-liked optimization approach for developing machine learning models, but there are other alternative possibilities to take into account. You could investigate several machine learning techniques and evaluate how well they perform on the datasets. To improve the performance of the selected algorithm, you might also look at hyperparameter tuning methods. Integration with other systems: The suggested system may require integration with other hardware or software platforms, such as a home automation platform or a security system [7]. You could elaborate on the difficulties or restrictions that might develop as a result of how the proposed system would interact with these other systems. Testing and evaluating the system's performance after it has been developed will be crucial to ensure that it operates as intended in a range of circumstances. You could talk about the testing procedures and

evaluation criteria that will be employed to rate the system's precision, quickness, and dependability. Considerations regarding privacy and security: If the suggested system involves gathering and processing video data, it may have an impact on both privacy and security [17]. You might go over any ethical issues that might come up, as well as how the system will handle sensitive data, such as by putting access control or encryption mechanisms in place. Design of the user interface: In order for users to engage with the proposed system, such as to configure Internet of Things (IoT) devices or view real-time video streams, it may be necessary to design the user interface [35]. You might talk about how the user interface was created and any usability tests that were done to make sure it was simple to use. Scalability: Depending on the application, it may be necessary for the proposed system to scale in order to support numerous users or a high number of IoT devices. You might talk about the scalability of the system and how it will be constructed, e.g., by utilizing distributed computing or cloud-based services. Open-source and collaboration: You may want to think about making the suggested system's code open-source so that other programmers can contribute to and improve it [29]. This will promote more widespread adoption and collaboration. You could also look at possibilities for working together with organizations or research groups working on related subjects. Deployment and upkeep: As a final point, you might talk about the deployment and upkeep of the suggested system, including how it will be set up and configured on various hardware platforms and how it will be updated and maintained over time [23]. Versioning of software, reporting of errors, and logging are a few examples of possible factors here. Fig. Previous System Algorithms with their Parameters and their Accuracy Stochastic gradient descent (SGD) improves generalization performance by acting as implicit regularization for deep learning. Additionally, empirical studies have shown that SGD with momentum significantly improves generalization performance. The stability and generalization of stochastic gradient-based methods provide valuable insights into understanding the algorithmic performance of machine learning models. Multi-pass stochastic gradient descent can further improve learning performance by taking a systemion.

II. LITERATURE REVIEW

In [2], a thorough analysis of some of the popular styles connected to energy-efficient, optimized recognition with several Machine Learning methods and a large amount of datasets is done. Intelligent buildings can now account for every minute of energy use because of the advancement of smart grid technology in [1]. As a result, in addition to providing a comfortable environment, scientists and experimenters are working to optimize energy operation, particularly in smart metropolises. In terms of smart system use, energy use, and comfort indicator functionality, the system's overall performance has improved according to the predicted stoner parameters. The club method converges extremely quickly in the beginning, but as it progresses, the rate of convergence diminishes. If the number of function evaluations is low, accuracy may be limited. As various residential equipment, including air conditioners, heaters, and refrigerators, were targets of cyberattacks in [9], major issues arose, including safety concerns and even harm to drug users. When our system detected event sequences associated with the operation, we were able to achieve discovery rates for anomalous operations above 90 with less than 10 false positives. Due to the erratic behavior of drug users

and networks, anomaly finding techniques typically result in a large number of false warnings. The various methods and algorithms for human detection in video surveillance systems are given a thorough discussion in this paper. The writers contrast and compare different strategies, both established computer vision approaches as well as more current deep learning-based ones. The article offers insightful analysis of the benefits and drawbacks of various methodologies and might be a helpful design guide for the system's human detection component. The use of IoT and machine learning techniques in automated smart homes is covered in this review paper. The authors give a summary of the state of the subject at the moment while highlighting recent developments in disciplines like human detection, activity recognition, and energy management. In addition to suggesting potential directions for future research, the paper offers insights into how our suggested system might fit into the broader framework of smart home automation. Using MediaPipe for real-time object detection is explained in detail in this lesson. Key ideas like creating the detection graph, importing the model, and integrating with OpenCV are covered in the tutorial. The tutorial can be a useful tool for putting our suggested system's human detection component into practice. The performance of healthcare monitoring and demand-control operations for the elderly and those with special needs is greatly improved by in-home monitoring [3]. Automated reflection procedures have appeared to understand resident gestures in terms of conditioning, thanks to the rapid expansion of Internet-of-effects operations. The suggested methodology simulates conditioning based on spatially respected behavior, with each effort expected to have a direct association with a particular set of locations. The Manual contains reflection techniques that are time-consuming (and valuable), delicate, personal, and inconsistent. It reflects less accurately and with more error in automatic. It takes less time than handcrafted reflection in Semi-Automatic and less time than automatic reflection. The typical Laplacian medium cannot be utilized in [5] to resolve data sequestration firms utilizing discriminational sequestration, and the conventional coin-flipping procedure has a high possibility of producing wasted energy calculation errors. The sequestration and usability of the proposed processes have been compared with the traditional approaches 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, all of which are based on a 30-day sample period of factual BEMS. These proposed techniques are suggested for further extension to use at BEMS data gateways in real-time based on their readily available efficacy. (BEMS) uses eye-catching detectors and clever techniques to reveal power usage and marijuana use within buildings. Both tackle-grounded styles, which include protrusive cargo monitoring, and software-grounded styles, which concern non-intrusive cargo monitoring, can be used to manage processes that are similar. The suggested IoT armature comprises the appliances subcaste, perception subcaste, communication network subcaste, middleware subcaste, and operation subcaste. ILM findings can be rather valuable, but they also provide advanced effectiveness and trustability. The appliance recognition module's primary job is to label detector data and permit the execution of various home functions. including software-grounded designs for protruding cargo monitoring (ILM) (NILM). Several experimenters are investigating the smart home environment in [4] conjunction with the continuous development of Internet of effects technology. Home drug users have access to and control over a wide range of home gadgets, including speakers, lights, and smart curtains that are installed throughout the

house. Smart homes offer accessible features like home monitoring, temperature control, and nocturnal work support, but because all dispatches are sent through insecure channels, they are susceptible to severe attacks. In the below mentioned table 1 the existing system algorithms, dataset, parameters and their accuracy are shown.

Table 1:Analysis of various algorithm and its results

Algorithm	Dataset	Parameter	Accuracy
CNN, BLSTM, QL	MAC00050	Time, Daytime, Label class, Shift and Window(FSTW)	75.03%
Naive Bayesian classifier	Amazon Alexa Reviews (Positive and Negative reviews)	Statistics, Rating, Feedback	93% - 94%
Long Short Term Memory (LSTM)	WISDM (Wireless Sensor Data Mining) dataset	Pre-processing data, dimension	92.67%
Random Forest	OWN	Pattern, light, Temp, Humidity, Motion, Predicted Result, Actual Result	85.40%
Radon recognition	education dataset	high quality image	89.33%
GRNN(general regression neural network)	Continuous target variable, Large dataset	Learning rate, Spread parameter, Momentum	93.90%
GRM(gradient Boosting Machine)	MNIST dataset, House Prices dataset	subsample, learning_rate, max_depth	89.80%

Also, because they are located in easily accessible areas, home bias can be a target for device prisoner attacks. However, to address related security issues, secure authentication and a crucial agreement method are required. Perpetrator remains a crucial component of the Internet of affects in [7] smart home technology. There aren't many SLR studies available on smart home monitoring technology. As a result, the current study evaluates the literature to gather evidence for studies on the implementation of smart home monitoring technologies. In the below Fig.1, the existing systems use machine learning algorithms where the algorithms, their accuracy and their parameters are compared on this graph.

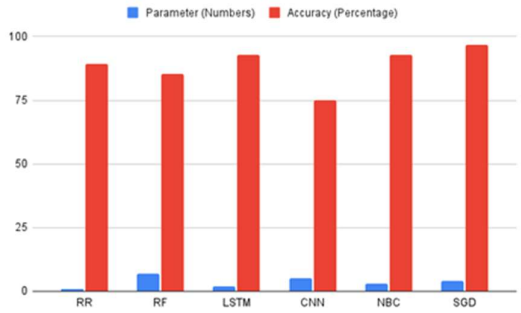

Fig.1 Comparison of existing accuracy

As a result, the current study evaluates the literature to gather evidence for studies on the implementation of smart home monitoring technologies. There is not enough perpetration of (SLR) on smart home technology. There aren't many SLR studies available on smart home monitoring technology.

III. PROPOSED METHODOLOGY

In this study, we developed a general model to handle the issues in the references mentioned before, together with energy efficiency, optimal recognition, and machine learning techniques. Here, we present three crucial procedures: an IoT device controller, image recognition, and machine learning. Applications for the powerful tool for computer vision and image processing tasks are numerous. With this, cv2 records the video. The parameter for the VideoCapture() function, which in this example is 0 to signal that we are only utilizing one camera, depends on your system. And we are utilizing cvzone to detect the pose, or body detection. After detecting the body motion, we set a line on the screen using the cv2.line() method (Syntax: cv2.line(image, start point, end point, color, thickness), which takes a parameter of image start point: Here, we are taking shoulder body points, i.e. 11 and 12. These are the points to detect the full human body and fix it in a box. The starting point for the line should be at these coordinates. The coordinates are displayed as tuples, which are pairings of two values (X coordinate value, Y coordinate value). endpoint: These are the final coordinates of the line. The coordinates are displayed as tuples, which are pairings of two values (X coordinate value, Y coordinate value). This color indicates the intended color of the line. For RGB, we pass a tuple. as in the blue color (255, 0, 0). Thickness: This word describes the px thickness of the line. We must decide whether or not the body crosses the line inside the border after securing the lines as boundaries on the screen. To accomplish this, we must switch the color of the line from blue to red (0, 0, 255). The hue shifts from blue to red when an object—in this case, the human body—crosses the line. This enables us to decide whether the object crosses or not.To make sure the object stays within the region that the camera is watching, we will draw some cross lines inside the boundary area. These lines will demonstrate if the object remains inside the perimeter or not. When an object crosses the line and stays inside the barrier, the IoT devices inside the barrier need to turn on automatically. We are using a subprocess module for this automation step, where we must fix the time in seconds, in order to automatically turn on or off the wifi-connected devices. This works just fine if we are using similar-wattage devices (for example, a 9-watt bulb), but if we are using different-wattage bulbs in various locations, we must first turn off the high-wattage light before turning off the others in order to save energy, for this we are using a protocol called Varak where it is trained simultaneously in the SGDClassifier trained model. To automate the process, estimate which devices it should turn on or off, and train the algorithm to make more accurate forecasts, we are using machine learning.

Fig.2 Comparison Datasets size and Accuracy

In the above graph Fig.2 shows the Datasets size on the existing systems and their accuracy varies based on the data present inside the Datasets.

The Stochastic Gradient Descent Algorithm is a machine learning approach that we are employing to forecast the results more correctly. Math forms the basis of practically all machine learning algorithms. Similar to this, the machine learning technique known as gradient descent draws its inspiration from mathematics and can be applied to first-order optimization. It can be used to find the local minima of any differential function, in essence. We show that the gradient descent method generates steps by repeatedly moving away from any location where the gradient is greatest. When the same operation is performed in the opposite direction, we get a gradient ascent, which leads us to a local maximum. We can assert that machine learning has the potential to be employed for improvement that improves learning. Stochastic gradient descent is another optimization method.

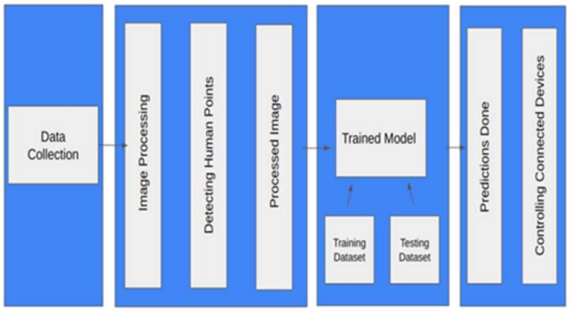

Fig.3 Proposed Architecture

In Fig.3, the Data collection part gathers data, i.e., video data, from input devices like CCTV. The data is then sent to the image processing part, which uses opencv2 to convert the image to a frame and process it. It then uses a mediapipe to detect human motion. The processed image is then displayed and given to the trained model (trained using SGDClassifier Algorithm with datasets). This trained model predicts the output with the help of the datasets. Using these predictions, the data collection part can With this, a subprocess is used to control wifi-connected devices, connecting and disconnecting them based on expected outputs.A model is created and trained using testing and training datasets using Scikit-Learn (which has the SGDClassifier), and it predicts the output, which results in the final output. The programme receives video as an input, pre-processes the input, and then pulls the feature out of the input. Stochastic gradient descent differs from gradient descent in that it uses smoothness properties that are appropriate for the objective function that needs to be optimized. It is possible to consider gradient descent's stochastic approximation as maximizing a smooth objective function. This concept also has mathematical roots, and it may be used in machine learning to minimize the objective function by finding the local minima of the objective function with the proper level of smoothness. The smoothness characteristics might be sub- or otherwise differentiable. Let's assume that an optimization function looks like this:

$$\theta(j) = \theta(j) - \alpha(\partial/\partial(\theta j))\, J(\theta) \qquad -(1)$$

where,

$$J(\theta) = 1/m\ m \wedge \sum_{(y-\hat{y})}^{i=1} i \wedge X \vee j \qquad -(2)$$

In equation 1 equation is substituted. The parameter J(θ) in this function has to be computed because it minimizes the function. The steps for calculating the J(θ) will be the subject of stochastic gradient descent organizing the arbitrary J(θ) terms:

1. The θ-term algorithm will be used to calculate the forecasts.
2. Using the previous value of the parameter and the mean square error, obtaining the updated value of the parameter requires computing the mean square error between actual values and systemions (θ).
3. Continue forecasting and updating the parameter's value up to convergence.

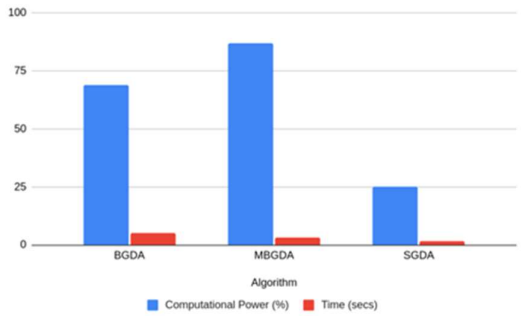

Fig.4 Computational Power of Gradient Descent

The above Fig.4 shows a comparison of time and computational power of 3 different algorithms in the Gradient Descent.

Update linear classifiers and regressors using convex loss functions, such as those used by (linear) Support Vector Machines and Logistic Regression, using the simple but effective stochastic gradient descent (SGD) algorithm. Although SGD has been around for a while in the machine learning field, large-scale learning has just recently begun to show a lot of interest in it. SGD, strictly speaking, does not belong to any particular family of machine learning models and is just an optimization technique. In essence, it is a model-training method. There is normally a sci-kit-learn API similar estimator for each SGDClassifier or SGDRegressor instance, maybe employing a different optimization method. Use SGDClassifier(loss='log loss') to create a model equivalent to LogisticRegression that is fitted by SGD rather than one of the other solvers in LogisticRegression, for example. Ridge finds different approaches to the same optimization issue, and SGDRegressor(loss='squared error', penalty='l2') does the same. Stochastic gradient descent offers the advantages of being efficient and easy to implement (lots of opportunities for code tuning). This is being done with the help of SGDClassifier, which carries out a simple stochastic gradient descent learning technique and supports different classification loss functions and penalties. Algorithm parameters for the Modified Stochastic Gradient Descent include X, y_ true, epochs, and learning rate. The datasets' characteristics, specifically Watt, Human Recognition Percentage (HRP), and w1 and w2 bias (here, two features). The Modified Stochastic Gradient Descent method examines random dataframe items and lowers the error rate until it discovers that the expected and actual outputs are almost equal. The values for w1, w2, and bias are initially set to 1, and features obtained from the dataframe are then applied to the formula of

SGD = w1 * feature1 + w2 * feature2 + bias - (1)

The formula is used to generate the w1 value here.

w1 = w1-learning rate*(∂(MSE)/∂w1) - (2)

MSE stands for Mean Squared Error.

By dividing the total error by the number of data in the dataframe, the Mean Squared Error is obtained.

MSE is calculated as Total Error / Data in Dataframes.

Where Total Error = E1+E2+.....+En

w2 is calculated by the formula,

w2 = w2 - learning rate*(∂(MSE)/∂w2) - (3)

The formula is used to determine the bias value,

bias = bias - learning rate * (∂(MSE) / ∂b) - (4)

The equations (2), (3), (4) are substituted in the equation (1). The formula is amended using the updated values for w1, w2, and bias until the error rate is decreased.
Although 0 is also a valid value for bias, we are using 1 in the formula.
The decision boundary of an SGDclassifier that is similar to a linear SVM that was trained using the hinge loss is displayed below.

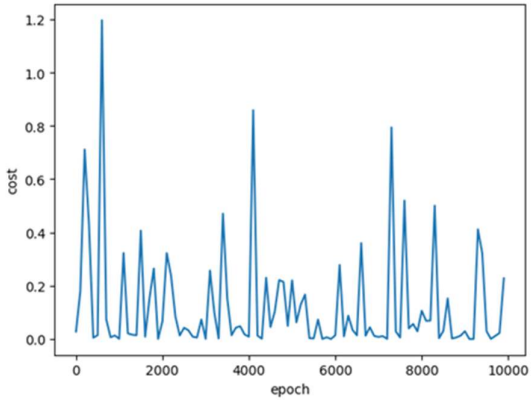

Fig.5 Predictions made by modified SGDClassifier

In the above Fig.5, the epoch and their cost is compared which gives the predicted value to the actual value. As we discussed before, when learning rate is set to high value then epoch is decreased, where the cost i.e, the predicted value is depends on the learning rate and epoch rate. SGD requires the same two arrays to be fitted as prior classifiers: an array X of the form (n samples, n features) storing the training samples and an array Y of the shape (n samples) storing the target values (class labels) for the training samples. He sklearn.linear model import syntax The SGDClassifier is imported using SGDClassifier. We must use the fit() function to fit the data after importing this. Once the model has been fitted, it can be used to predict new values.

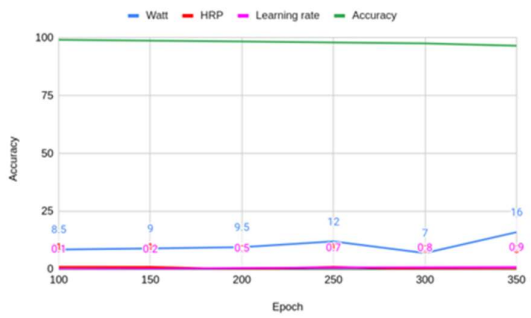

Fig.6 Comparison of Epoch size and Accuracy

In Fig.6, the parameters used in our system (watt, HRP, Learning rate) and accuracies are compared and shown in this graph. The epoch size is the size of epoch and accuracy differs depending on given epoch size. When the size of epoch is low then accuracy is very high, if the size of epoch is high then the accuracy is low. The IoT devices that are located inside the bounds that the CCTV camera captures are managed after the values are more precisely predicted.

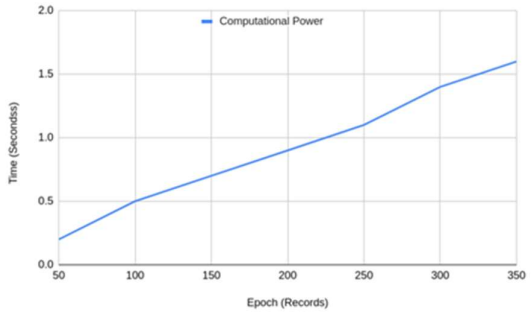

Fig.7 Computational power of Modified SGD System

In Fig.7, It shows the computational power of the modified SGDClassifier system i.e. when the data increases the computational time of the system also increases. The maximum computational power of our system is 2.5 seconds to the given 450 records. We need to download and run the programme in order to use this as a more efficient means of controlling IoT devices. The application should automatically turn on the IoT (Smart Devices) devices that are connected through the same WiFi if any human motions are detected inside the set border. But the process should be done in a secure manner, without any encryption algorithm to secure the internet connection between the devices so we are using AES (Advanced Encryption Standard) to offer secure connection with the cloud or other devices. The performance and security of the encryption process can be enhanced by combining machine learning and AES. Using an adaptive key generation technique is one method of using machine learning with AES in IoT devices. This entails utilizing a machine learning algorithm to discover the IoT device's usage patterns and generating encryption keys on the fly based on those patterns. By creating distinct keys for each communication session, the goal is to make it more challenging for attackers to deduce the encryption secret. Making the most of the device's resources to optimize the encryption process is another technique to employ machine learning with AES in IoT devices. Since IoT devices frequently have limited resources, it's critical to reduce the computational burden of the encryption procedure. Algorithms for machine learning can be

used to examine the device's resources and modify the encryption process as necessary. For instance, depending on the computing capability of the device, the algorithm might change the amount of rounds used in the AES encryption process. After Encrypting the connection by AES we have to control the devices based on the given condition. Until the user closes the programme, this procedure runs in a loop to detect human movements and continuously control the devices.

IV. CONCLUSION

The Internet of Things (IoT) is used in a wide range of fields and enterprises. It has experienced tremendous developments across many different fields. This paper discusses an IoT innovation that facilitates human work while simultaneously posing security questions. Predictions' value is also increased by the use of machine learning algorithms, which improve prediction accuracy. This essay describes challenges and problems that can be overcome using this strategy in a number of different industries. To solve those issues, we don't need to spend a lot of money on expensive equipment; all we need is a simple programme.

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] 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.
[16] 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.
[17] 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.
[18] 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.
[19] Olutosin Taiwo and Absalom E. Ezugwu. Internet of Things-Based Intelligent Smart Home Control System. South Africa, published on 24 September 2021, IEEE.
[20] 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.
[21] Eirini Anthi, Lowri Williams, Amir Javed, Pete Burnap. Hardening machine learning denial of service (DoS) defenses against adversarial attacks in IoT smart home networks. Cardiff, United Kingdom Published on May 24, 2021, Elsevier.
[22] Marijana Zekić-Sušac , Saša Mitrović, Adela Has. Machine learning based system for managing energy efficiency of public sector as an approach towards smart cities. Osijek, Croatia Published on 2021, Elsevier.
[23] Miia Lillstrang, Markus Harju, Guillermo del Campo, Gonzalo Calderon, Juha Röning, Satu Tamminen. Implications of properties and quality of indoor sensor data for building

machine learning applications: Two case studies in smart campuses. Madrid, Spain, published on October 28, 2021, Elsevier.
[24] Seppo Sierla, Mahdi Pourakbari-Kasmaei, Valeriy Vyatkin. A taxonomy of machine learning applications for virtual power plants and home/building energy management systems. Espoo, Finland, published on February 12, 2021, Elsevier.
[25] Amer Malki, El-Sayed Atlam, Ibrahim Gad. Machine learning approach of detecting anomalies and forecasting time-series of IoT devices. Yanbu, Saudi Arabia published on February 13, 2022, Elsevier.
[26] Arek Gaber, Amir El-Ghamry, Aboul Ella Hassanien. Injection attack detection using machine learning for smart IoT applications. United Kingdom, published on March 16, 2022, Elsevier.
[27] Alex Roberge, Bruno Bouchard, Julien Maître, Sébastien Gaboury. Hand Gestures Identification for Fine-Grained Human Activity Recognition in Smart Homes. Porto, Portugal, published on March 25, 2022, Elsevier.
[28] Kari Alanne, Seppo Sierla. An overview of machine learning applications for smart buildings. Aalto, Finland, published on October 12, 2021, Elsevier.
[29] Nikolaos Koltsaklis, Ioannis Panapakidisc, Georgios Christoforidisb, Jaroslav Knápe. Smart home energy management processes support through machine learning algorithms. Volos, Greece, published on February 2, 2022, Elsevier.
[30] Rachneet Kaur, Clara Schaye, Kevin Thompson, Daniel C. Yee, Rachel Zilz, R.S. Sreenivas, Richard B. Sowers. Machine learning and price-based load scheduling for an optimal IoT control in the smart and frugal home. Urbana, USA, published on December 23, 2020, Elsevier.
[31] Rizwan Majeed, Nurul Azma Abdullah, Imran Ashraf, Yousaf Bin Zikria, Muhammad Faheem Mushtaq, and Muhammad Umer. An Intelligent, Secure, and Smart Home Automation System. Rahim Yar Khan, Pakistan, published on October 29, 2020, Hindawi.
[32] Basman M. Hasan Alhafidh1, Amar I. Daood2, Mudhar A. Design and Implementation of Home Autonomous System Based on Machine Learning Algorithms. Mosul, Iraq, published on November 9, 2020, IJERA.
[33] George Vardakis, George Tsamis, Eleftheria Koutsak, Kondylakis Haridimos and Nikos Papadakis. Smart Home: Deep Learning as a Method for Machine Learning in Recognition of Face, Silhouette and Human Activity in the Service of a Safe Home. Heraklion, Greece, published on May 19, 2022, MDPI.
[34] Rishabh Dev Manu, Sourav Kumar, Sanchit Snehashish, K.S. Rekha. Smart Home Automation using IoT and Deep Learning. Mysuru, Karnataka, India, published on April 4, 2019, IRJET.
[35] Murad Khan, Junho Seo and Dongkyun Kim. Towards Energy Efficient Home Automation: A Deep Learning Approach. Daegu, Korea, published on December 15, 2020, MDPI.
[36] Keshav Kaushik, Akashdeep Bhardwaj, Susheela Dahiya, Mashael S. Maashi, Moteeb Al Moteri, Mohammed Aljebreen and Salil Bharany. Multinomial Naive Bayesian Classifier Framework for Systematic Analysis of Smart IoT Devices. Riyadh, Saudi Arabia, published on September 27, 2022, MDPI.

[37] Seppo Sierla, Mahdi Pourakbari-Kasmaei, Valeriy Vyatkin. A taxonomy of machine learning applications for virtual power plants and home/building energy management systems. Petersburg, Russia, published on February 22, 2022, Elsevier.
[38] Anthi E, Williams L, Malgortzata G, Theodorakopoulos G, Burnap P. A supervised intrusion detection system for smart home IoT. IEEE Internet Things J. 2018;78:477–90.
[39] Baracaldo N, Chen B, Ludwig H, Safavi A, Zhang R. Detecting poisoning attacks on machine learning in IoT environments. In: 2018 IEEE International Congress on Internet of Things (ICIOT). IEEE; 2018. p. 57–64.
[40] Dhanjani N. Hacking lightbulbs: Security evaluation of the Philips hue personal wireless lighting system. Internet Things Secur. Eval. Series 2013.
[41] Doshi, R., Apthorpe, N., Feamster, N., 2018. Machine learning DDoS detection for consumer internet of things devices. arXiv preprint arXiv:1804.04159.
[42] Erba, A., Taormina, R., Galelli, S., Pogliani, M., Carminati, M., Zanero, S., Tippenhauer, N. O., 2019. Real-time evasion attacks with physical constraints on deep learning-based anomaly detectors in industrial control systems. arXiv preprint arXiv:1907.07487.
[43] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. 2013;29(7):1645–60.
[44] McDermott CD, Majdani F, Petrovski AV. Botnet detection in the internet of things using deep learning approaches. In: 2018 International Joint Conference on Neural Networks (IJCNN). IEEE; 2018. p. 1–8.
[45] Abusnaina A, Khormali A, Alasmary H, Park J, Anwar A, Mohaisen A. Adversarial learning attacks on graph-based IoT malware detection systems. In: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). IEEE; 2019. p. 1296–305.
[46] Amouri A, Alaparthy VT, Morgera SD. Cross layer-based intrusion detection based on network behavior for IoT. In: Wireless and Microwave Technology Conference (WAMICON), 2018 IEEE 19th. IEEE; 2018. p. 1–4.
[47] OConnor T, Enck W, Reaves B. Blinded and confused: uncovering systemic flaws in device telemetry for smart-home internet of things. In: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks; 2019. p. 140–50.
[48] Ronen E, Shamir A. Extended functionality attacks on IoT devices: the case of smart lights. In: 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE; 2016. p. 3–12.
[49] Q. Li, H. Tan, Y. Wu, L. Ye, F. Ding, Traffic flow prediction with missing data imputed by tensor completion methods, Published on 21 March 2020, IEEE.
[50] Palanivel, N., et al. "IoT Health Care Devices for Patient Monitoring." Cyber Security and Operations Management for Industry 4.0. CRC Press, 2022. 109-123.