Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1 : 2024
ISSN : **1906-9685**

A SMART AND SECURE INTERNET OF THINGS USING MACHINE LEARNING ALGORTHIM

Kamatala .Vinnusri, Department of Electronics and Communication Engineering, DVR & Dr.HS MIC College of Technology, Kanchikacherla , Andhra Pradesh.

[1] vinnusri9948@gmail.com

Kota.Srinivasa Rao, Assistant Professor, Department of Electronics and Communication Engineering, DVR & Dr.HS MIC College of Technology, Kanchikacherla , Andhra Pradesh.

[2] Srinuk.449@gmail.com

Ravula.Vamsi, Yarra.Pavani and Bandareddy.Venkata Sai Varun, Department of Electronics and Communication Engineering, DVR & Dr.HS MIC College of Technology, Kanchikacherla , Andhra Pradesh.

[3] rvn7801@gmail.com, [4]pavaniyarra@gmail.com, [5]varunbvns@gmail.com

ABSTRACT

IOT devices are various types of hardware such as appliances, sensors, machines, or actuators that are programmed for specific applications such as data transmission over a network or the Internet. They are embedded in other industrial devices, biological sensors, mobile devices, and medical devices. There are approximately 7.62 billion people in our world, with a growing graph of IOT devices. So, the amount of data released from these IOT devices also increases, and there may be a chance of leakage of data from these devices. These IOT devices used in our home is exposed to different types of attacks like eavesdropping, brute force attack, leakage of information, cyber attacks etc. In detecting these types of attacks the machine learning algorithms play an important role and If we improve the security of these IoT devices it helps in making these IOT devices more secure; that is the primary goal of this project. Machine learning models can help in finding the spam in the data. To cope with different security challenges, Machine Learning Techniques are able to provide intelligence for IOTdevices and networks. This idea presents the security problems and the existing ML solutions to manage security aspects related to the IOT domain. This paper proposes a classification model to detect attack on the dataset and implements the following algorithms namely, Decision Tree, Random Forest, Linear Regression and k-Nearest Neighbors. The best results were achieved by the Random Forest algorithm, with a higher accuracy.

Keywords: Decision Tree, Random Forest, Linear Regression and k-Nearest Neighbors

INTRODUCTION

In recent years, the proliferation of Internet of Things (IoT) devices has revolutionized various industries, enabling connectivity and automation in homes, businesses, healthcare, transportation, and more. However, as the number of IoT devices grows exponentially, so do the challenges related to security, efficiency, and intelligence Rajendrakumar, et al. (2017) This has led to the integration of machine learning algorithms into IoT systems to enhance their capabilities and address these challenges effectively Ukil et al. (2016). This paper explores the intersection of IoT and machine learning, focusing on how machine learning algorithms can be leveraged to create smart and secure IoT systems. Machine learning algorithms are a core component of the field of machine learning, enabling computers to learn from and make decisions based on data. These algorithms can be broadly classified into several categories based on their learning style and function. Here's an overview of some of the primary types of machine learning algorithms and a few notable examples within each category.

Supervised Learning: In supervised learning, the algorithm learns from a labeled dataset, providing an answer key that the algorithm can use to evaluate its accuracy on training data. The goal is to learn a mapping from inputs to outputs Doan et al. (2015)

Linear Regression: Predicts a continuous output based on one or more input features. Logistic Regression: Used for binary classification tasks (e.g., spam or not spam). Support Vector Machines Han, Guangjie, et al. (2018)

Decision Trees: A tree-like model of decisions and their possible consequences; it's simple to understand and interpret. Random Forests: An ensemble of decision trees, typically used for classification and regression tasks. Gradient Boosting Machines (GBMs) Gai et al. (2018). An ensemble technique that builds models sequentially, each new model correcting errors made by previous ones.

Unsupervised Learning: Unsupervised learning algorithms infer patterns from untagged data. The system tries to learn without a teacher. K-means Clustering: Partitions the data into k distinct clusters based on feature similarity. Principal Component Analysis (PCA): A dimensionality reduction technique used to reduce the dimensionality of large datasets. Ng, Jin Ren, et al (2019)

Auto encoders: Neural networks used for dimensionality reduction or feature learning by learning to compress and then reconstruct the input data. HTTP (Hypertext Transfer Protocol) is the foundation of data communication on the World Wide Web. It's a protocol used by web browsers and servers to communicate and exchange data. HTTP works as a request-response protocol, Li, Wenjuan, et al. (2019) where a client (typically a web browser) sends a request to a server for a resource (such as a web page), and the server responds with the requested resource along with an HTTP status code indicating the success or failure of the request. HTTP operates over TCP/IP, typically on port 80 for unencrypted connections and port 443 for encrypted connections (HTTPS).

2.Related Work

In this section, when discuss related work in the context of smart homes, especially focusing on the integration of machine learning algorithms, HTTP protocol, and specific devices like door locks and fans, we delve into a realm where technology meets daily living. This intersection aims to enhance security, comfort, and energy efficiency. Below, we explore various studies, projects, and innovations that have contributed to this field, highlighting how these components come together to push the boundaries of what's possible in smart home.

2.1 Machine Learning for Predictive and Adaptive control

Energy Efficient Smart Home control: A notable study involves the use of machine learning algorithmsto predict a household's energy needs and manage devices accordingly. By analyzing historical data, thesystem can control heating, ventilation, air conditioning (HVAC) systems, and fans to optimize energy usage without compromising comfort. This is often done using predictive models that adjust settings based on anticipated occupancy and temperature fluctuations.

Security Enhancements with Anomaly Detection: Machine learning algorithms are employed to enhance security by learning typical user behaviors. Anomalous actions, such as an unexpected attempt to unlocka door, trigger alerts or preventive actions. The integration of facial recognition or unusual activity patterns helps in distinguishing between legitimate users and potential security threats, significantly improving the efficacy of smart locks.

2.2 HTTP Protocol for Device Communication and Control

Remote Control and Automation: Various projects utilize the HTTP protocol to facilitate communicationbetween smart devices and servers, allowing users to control smart home devices remotely. For instance,a user can lock or unlock doors, turn fans on or off, and adjust settings via a smartphone app. This remote control extends to scheduling routines, where devices like smart locks and fans operate based on preset schedules, enhancing convenience and energy efficiency.

Integration with IoT Platforms: The HTTP protocol is fundamental in integrating smart home deviceswith broader Internet of Things (IoT) platforms. These platforms aggregate data from various sources,enabling centralized control and advanced locked if no one is home.

.Materials and Methods

Designing a smart home system that leverages Machine Learning (ML) algorithms and HTTP protocol to control devices such as door locks and fans involves a detailed approach. Below, I outline a general framework for the materials and methods required to implement such a system, emphasizing the technological components, software architecture, and the role of ML and HTTP in device control.

3.1 Materials Required

Smart Devices

Smart Door Lock: A door lock with connectivity features (Wi-Fi, Bluetooth) that can be controlled remotely. Smart Fan: An IOT-enabled fan that supports remote control over the internet. Additional sensors might be needed for enhanced functionality, such as temperature sensors, motion sensors, and cameras for security and environmental monitoring. Central Hub or Controller: A device or server that acts as the central processing unit of the smart home system. It can be a dedicated smart home hub, a personal computer, or a cloud-based server. Networking Equipment: Wi-Fi router and possibly additional networking tools to ensure full home coverage. Smartphone or Tablet: For user interaction with the smart home system, including setup, monitoring, and manual control.

3.2 Methods

Setup and Integration

Device Configuration: Install and configure all smart devices according to the manufacturer's instructions. Ensure each device is connected to the home network.

Central Hub Setup: Establish the central hub that will communicate with all smart devices. This could involve setting up software on a personal computer or configuring a cloud-based service.

HTTP Protocol Implementation: Implement HTTP endpoints for each device to allow for RESTful communication. This can often be facilitated by the device manufacturer's APIs.

Machine Learning Implementation

Data Collection: Gather data from smart devices and sensors. This data can include door lock activity logs, fan usage patterns, environmental conditions, and user interactions.

Data Processing and Analysis: Clean and preprocess the collected data. Perform exploratory dataanalysis to understand patterns and correlations.

Feature Engineering: Identify and engineer features from the dataset that are predictive of user behavioror necessary conditions for device operation.

Model Training: Use the processed data to train ML models. Models can be trained to predict user preferences, detect anomalies, or automate device control based on learned patterns.

Model Deployment: Deploy the trained models to the central hub or cloud-based server, integrating them with the device control mechanisms.

Device Control and Automation

Automated Device Control: Implement control algorithms that use the outputs of ML models to automate device actions. For example, automatically adjusting fan speed based on temperature or turningon the fan when the room is occupied.

User Defined Rules: Allow users to define custom rules and schedules via a smartphone app or web interface. These rules can complement the ML-driven automation.

Monitoring and Adjustment: Continuously monitor system performance and user satisfaction. AdjustML models and control algorithms based on feedback and new data.

This framework outlines a comprehensive approach to creating a smart home system that uses machine learning and HTTP protocol to enhance the functionality and automation of door locks and fans, among other devices. The continuous cycle of testing, feedback, and improvement is essential to refining the system and ensuring it meets user needs and expectations.

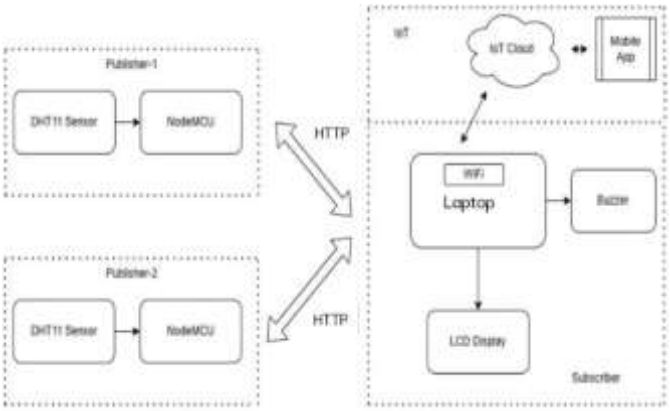

Fig 3.1 Block Diagram

Result And Analysis

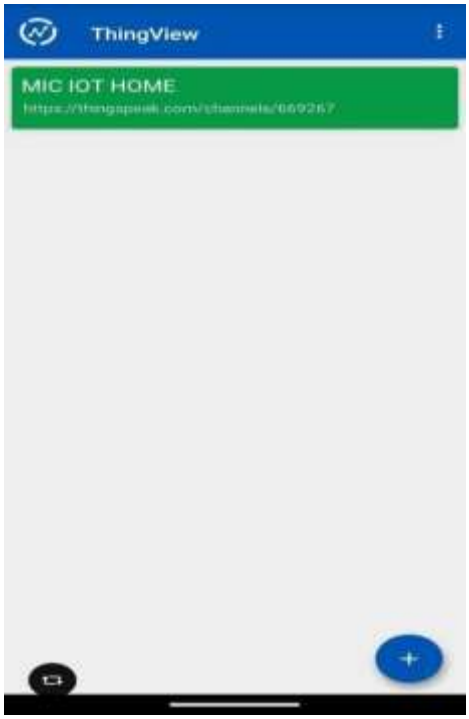

Fig 3.2 ThingView app

ThingView app serves as an invaluable tool for transforming a regular home into a smart home, offering users seamless control and management over various IoT devices and systems. Here's how the Thing View app can be used for smart home applications.

4. OUTPUTS

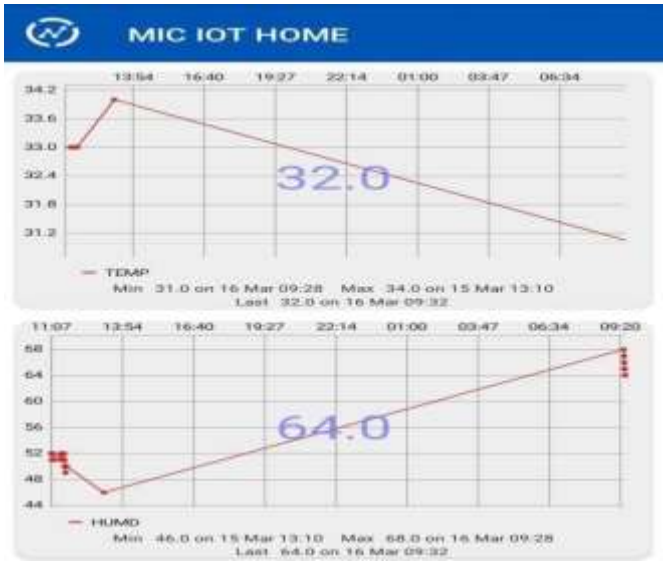

Fig 4.1 TEMPERATURE AND HUMIDITY

The output of the Thing View app provides users with a seamless and intuitive interface to monitor,manage, and control their IoT devices, particularly in smart home applications. Users can access real-time data streams, receive timely alerts and notifications, and remotely interact with their connected devices with ease. With its centralized control and automation features, Thing View simplifies the management of smart home ecosystems, promoting convenience, energy efficiency,and enhanced security. Additionally, its integration with voice assistants further enhance accessibility, offering users a comprehensive solution for transforming their homes into smart,connected environments.

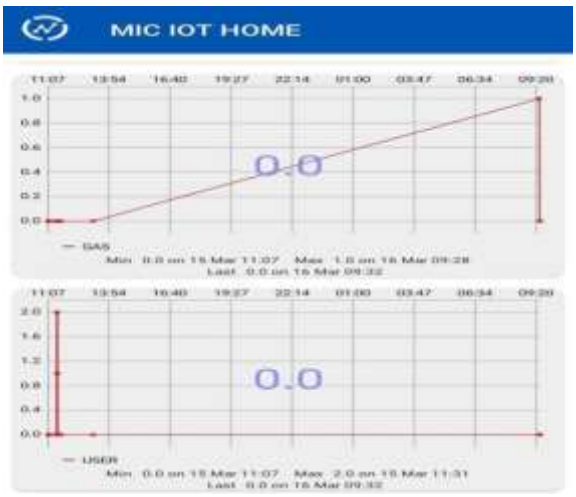

Fig 4.2 GAS ANALYSIS AND USER

Fig 4.3 User Interface

5. Conclusion

The development of a smart home system utilizing HTTP protocol for device communication and machine learning algorithms for intelligent decision-making represents a significant advancement in home automation technology. This approach not only automates routine tasks butalso adapts and responds to the unique preferences and behaviors of its users, thereby enhancing comfort, security, and energy efficiency.

The HTTP protocol serves as a reliable and widely adopted foundation for communication betweenthe central control system and individual smart devices, such as door locks and fans. It enables the remote control of these devices over the internet, offering users unparalleled convenience and flexibility. Through secure implementations like HTTPS, the system ensures that all communications are encrypted, protecting users' privacy and security.

The integration of HTTP protocol and machine learning into smart home systems embodies the convergence of connectivity and intelligence. It enables the creation of truly smart environments that not only connect devices but also imbue them with the ability to learn, predict, and adapt. This technology holds the promise of making homes more comfortable, secure, and efficient, significantly improving the quality of life for their inhabitants.

In conclusion, the use of HTTP protocol and machine learning algorithms in smart homes marks a forward leap in our journey towards more intelligent, responsive, and user-centric living spaces. By leveraging these technologies, we can create homes that not only listen and respond to our commands but also anticipate our needs and adapt to make our lives easier, safer, and more enjoyable.

REFERENCES

[1] Rajendrakumar, Shiny, V. K. Parvati, B. D. Parameshachari, KM Sunjiv Soyjaudah, and Reshma Banu. "An intelligent report generator for efficient farming." In 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques(ICEECCOT), pp. 1-5. IEEE, 2017.

[2] Ukil, S. Bandyoapdhyay, C. Puri and A. Pal, "IoT Healthcare Analytics: The Importance of Anomaly Detect ion". IEEE 30th International Conference on Advanced Information Networking and Applications (A.I.N.A.), Crans-Montana, 2016. pp 994-997.

[3] Doan, Tri, and Jugal Kalita. "Selecting machine learning algorithms using regression models." 2015 IEEE International Conference on Data Mining Workshop (I.C.D.M.W.). IEEE,2015.

[4] Han, Guangjie, et al. "K.C.L.P.: A k-Means Cluster-Based Locat ion Privacy Protect ion Scheme in W.S.N.s for IoT." IEEE Wireless Communications, 2018. Vol. 25, Issue 6, pp 84-90.

[5] Gai, Keke, and Meikang Qiu. "Optimal resource allocat ion using reinforcement learning forIoT content -cent ric services". Applied Soft Computing. 2018. Vol. 70, pp 12-21.

[6] F. Chen, P. Deng, J. Wan, D. Zhang, A.V. Vasilakos, X. Rong, Data mining for the Internetof

things: literature review and challenges, Int. J. Distrib. Sens. Netw. 2015 (2015) 12.
[7] Ng, Jin Ren, et al. "Identification of Road Surface Conditions using IoT Sensors and Machine Learning." Computational Science and Technology, 2019. pp 259-268.
[8] Li, Wenjuan, et al. "Design of multi-view based email classificat ion for IoT systems via semi-supervised learning." Journal of Network and Computer Applications, 2019. Vol. 12, Issue8, pp 56-63.
[9] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi, Internet of things for smart cities,IEEE Internet Things J. 1 (1) (2014) 22–32.
[10] Souza, Alberto MC, and Joseé RA Amazonas. "An out lier detect algorithm using big data processing and internet of things architecture." Procedia Computer Science 52, 2015. pp 1010- 1015.