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

AN INTELLIGENT INTRUSION DETECTION FOR ENHANCING MQTT PROTOCOL SECURITY IN IOT DEVICES USING ENSEMBLE MACHINE LEARNING

Prathyusha. Kuncha [1]*, Sunitha. Ravi [2]*, A. Ritesh Sai[3], B. Siva Krishna [4]
B. Prasanna Kumar[5], B. Praneeth Babu[6]
[1]Associate Professor, Department of ECE, NRI Institute of Technology, Vijayawada.
[2] Professor, Department of ECE, NRI Institute of Technology, Vijayawada.
[3,4,5,6] U.G Scholars, Department of ECE, NRI Institute of Technology, Vijayawada.

Abstract:
This paper offers an Internet of Things (IoT) security system that uses a Raspberry Pi as a MQTT server and NodeMCU devices with sensors as clients. Temperature and humidity readings are collected by the NodeMCU devices and sent to the Raspberry Pi via the MQTT protocol. Serving as the hub, the Raspberry Pi gathers data from various sources, interprets it, and uses a machine learning algorithm to detect possible attackers using distinct MAC addresses and patterns in the data. The incoming data is analysed by the machine learning system, which also creates baseline patterns for typical behaviour and spots anomalies that might be signs of unauthorised access. The system uses the IoT framework to provide notifications to the user when it detects questionable activities. The consumer can respond right away to these alerts in a number of ways, including email notifications or push notifications on a mobile device. This paper offers a complete and clever IoT security solution by combining NodeMCU, sensors, MQTT connectivity, Raspberry Pi, and machine learning. The system contributes to improved home or office security and peace of mind by not only monitoring environmental conditions but also ensuring the safety of the monitored area by recognising and alerting users to potential security risks.
Keywords: IoT security system, NodeMCU, MQTT, Raspberry Pi, machine learning, anomaly detection.

1. Introduction:

Confidentiality, integrity, and authentication are three essential security needs for Internet of Things networks that are covered in this study [1]. In order to reduce attack risks, it suggests disabling unnecessary features, avoids using default passwords, and educates users about device security before using it. It also categorises twelve different attack types into four levels: low, medium, high, and extremely high. The significance of investigating different security methods appropriate for IoT scenarios is also emphasised in the article. In order to solve security issues for devices with constrained resources, this study [2] explores the usage of a Raspberry Pi as an Intrusion Detection System (IDS) for Internet of Things environments.

The authors provide an intrusion detection system (IDS) architecture that uses a Raspberry Pi to find malicious network activities. Its efficacy in a dispersed IoT system is demonstrated by experimental findings, providing a workable security solution for devices with limited resources in the expanding IoT market. In order to address the communication requirements of Wireless Sensor Networks (WSNs), this research [3] describes MQTT-S, an adaption of the MQTT protocol that uses the publish/subscribe approach. Its lightweight design and compatibility with resource-constrained contexts enable seamless data interchange across WSNs and conventional networks. Implementation issues are recognised and planned for future development, with a focus on managing clients who are sleeping in WSNs. Because HTTP is frequently used for data transfer, this research [4] compares the

performance of HTTP with that of MQTT, a type of named-based transfer protocol. Nevertheless, this protocol has a significant overhead in IoT networks. Named based transfer protocols have been considered as a potential solution to this issue. The report also suggests improvements to MQTT in order to improve performance. Therefore, the performance of the MQTT protocol and several methods for improving the performance are covered in this study. In addition to providing an overview of suggested solutions and security challenges, this research [5] analyses and surveys IOT security. It draws attention to how important security is to the Internet of Things (IoT), a network that allows common things to exchange data and communicate with one another.

Three layers make up the conventional Internet of Things architecture: perception, network, and application. For an IoT system to be secure, each of these layers needs to have particular security concepts put into practice. Despite ongoing obstacles, researchers are actively working on countermeasures to solve security issues at every layer. The Internet of Things' (IoT) communication protocols are the main topic of this paper [6]. We now have billions of smart devices connected; therefore, connectivity must be reliable. The study examines the research patterns over the previous 20 years for three important protocols: MQTT, AMQP, and CoAP. Compared to the others, MQTT research has developed tremendously. The paper delves deeper into the uses of MQTT, the most widely used M2M/IoT protocol. The authors highlight different domains where MQTT is applied through a review of the literature. The study also compares the features, advantages, and drawbacks of recent MQTT research through a quantitative analysis.

In this paper [7], a unique method to network intrusion detection systems (NIDS) that puts efficiency and usability first is presented: Kitsune. In order to overcome these constraints, Kitsune uses unsupervised learning, which enables it to recognise local network threats automatically without the requirement for human data labelling. This paper explores Kitsune's main algorithm, KitNET, which distinguishes between normal and aberrant traffic patterns using a set of neural networks called autoencoders. In this research [8], we offer a DoS detection technique based on IP packet size entropy (IPSE), wherein an attack affects traffic and noticeably alters the entropy. Our investigation reveals that the IPSE-based scheme can identify short-term attacks as well as long-term ones that are outside the scope of volume-based schemes' detection capabilities. Passban, an intelligent intrusion detection system (IDS) created especially for safeguarding Internet of Things (IoT) devices, is presented in this study [9]. In order to solve this problem, Passban provides an IDS solution that can be installed straight into inexpensive IoT gateways. This method makes use of the idea of edge computing, which is processing and analysis that takes place in closer proximity to the data source—in this case, the networked Internet of Things devices.

The study demonstrates how Passban can detect a wide range of harmful actions with acceptable accuracy and low false positive rates, such as port scanning, brute-force assaults, and denial-of-service efforts. This shows that Passban could be a useful tool for improving the security of Internet of Things devices and networks. The limits of existing techniques like TLS and symmetric encryption for resource-constrained contexts are discussed in this work [10] along with the difficulties in securing communication for IoT devices. It presents a brand-new Value-to-HMAC mapping technique that preserves confidentiality and integrity while improving efficiency by using message signatures rather than encryption. The study highlights the trade-off between IoT security efficiency and resilience, and it suggests Value-to-HMAC as a solution that strikes a balance between performance and security and is suited to the requirements of IoT networks with limited resources.

Improving the Message Queue Telemetry Transport (MQTT) protocol for machine-to-machine (M2M) and Internet of Things (IoT) communication is the main goal of this paper [11]. Because the traditional MQTT architecture relies on a single broker, it is less suitable for edge-based IoT applications and introduces a single point of failure. The research suggests a unique MQTT broker design that increases system availability without broadcasting private client data in order to overcome these drawbacks. The calculations in the research show that this approach greatly lowers the quantity of messages sent back and forth between brokers, which may enhance scalability and efficiency. Because typical IDS systems are insufficient for IoT networks using MQTT, this paper [12] emphasises the necessity for IDS systems specifically designed for these contexts. It draws attention

to the lack of extensive datasets for both legitimate and fraudulent MQTT traffic. The authors use a specially created MQTT dataset to evaluate and propose six machine learning algorithms in order to address this. Their results demonstrate how well the models identify assaults that are peculiar to MQTT, highlighting the advantages of flow-based features over conventional packet-based features for accurate detection in MQTT networks. This highlights the requirement for security protocols that take into consideration the distinct communication patterns of MQTT networks.

2. Proposed Work:

The suggested IoT security system provides a thorough, proactive, and unobtrusive solution made specifically for the unique problems that arise in IoT contexts. It includes dynamic threat detection systems that use machine learning algorithms and behavioural analysis to detect anomalies in real-time and adaptively monitor network traffic. Effective control and monitoring are made possible by seamless connectivity with IoT devices, and administrators can access unified oversight and configuration capabilities through a centralised management panel. The suggested solution attempts to give enterprises strong defence against changing threats by combining these elements into a unified framework, protecting vital assets and data in Internet of Things installations. Utilising environmental data, particularly temperature and humidity readings, as markers of possible security breaches is the fundamental concept behind the suggested solution.

The system uses sensor-equipped NodeMCU devices to continuously monitor the surroundings. These gadgets function as clients, sending data over the MQTT protocol to a Raspberry Pi, which serves as the central server. This data is processed by the Raspberry Pi, which uses a machine learning technique to look for anomalies that might indicate unwanted access. The system notifies the user via many channels upon identifying such anomalies, facilitating prompt action in response to possible security risks.

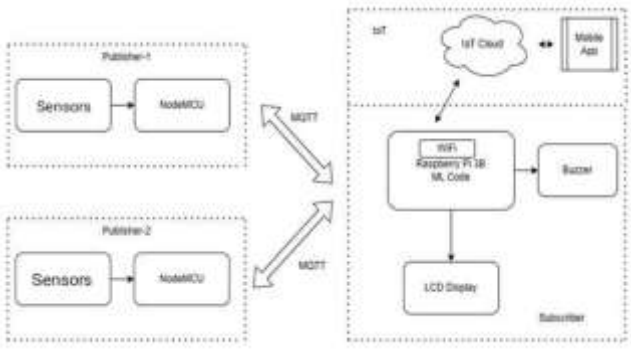

Fig 1: Block diagram

3. System Components:

Nodemcu Devices Capable of Sending DHT11:

These microcontroller boards can be used for Internet of Things applications because they have WiFi enabled. The DHT11 sensors that are attached to them measure humidity and temperature, giving the environmental data needed for analysis.

Server Central: Raspberry Pi:

Acts as the central component of the system, gathering information from every NodeMCU device.
Oversees the MQTT broker, ensuring secure and effective data transfer management.
Uses a machine learning algorithm to analyse the incoming data and find anomalies.

MQTT Standard:

A low-power and bandwidth messaging protocol that is perfect for Internet of Things applications, specifically made for small sensors and mobile devices. Enables dependable sensor data transfer from NodeMCU devices to the Raspberry Pi.

Algorithm for Machine Learning:
Establishes baseline patterns of normal conditions by analysing environmental data. Continually evaluates incoming data to these baselines to find deviations that might point to possible security breaches or unauthorised access.

Alert System:
The system may warn the user by email, SMS, or a dedicated app notice when it detects anomalies. It also enables quick action, such as confirming the alarm or starting a more thorough response.

4. Working of the Proposed System Data Collection:
Periodically, the NodeMCU devices gather temperature and humidity data, which they then send over MQTT to the Raspberry Pi.

Data Analysis and Processing:
This data is received by the Raspberry Pi, which is serving as the MQTT server. It is then analysed using the machine learning technique. In order to identify abnormalities, this technique compares the real-time data to recognised patterns of typical environmental circumstances.

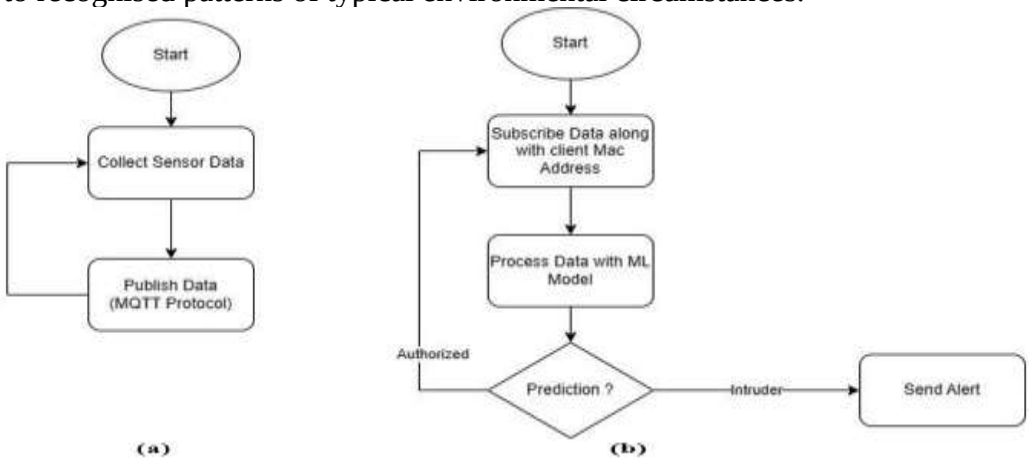

Fig 2: (a) Flow Chart for Data Collection (b) Flow Chart for Data Processing and Analysis

Identification of Anomalies:
A divergence from the norm is flagged by the machine learning system as a possible security violation. These variations may result from a number of things, like the abrupt opening of a door or window, which could cause temperature or humidity levels to change unpredictably.

Warning:
The alert mechanism is triggered by the system upon detection of an anomaly. The user can personalise this alert to suit their interests, which guarantees that they are instantly alerted to any potential security risks.

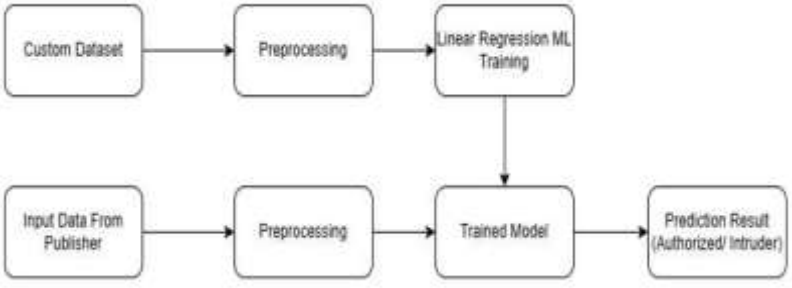

Fig 3: Flow Chart for Intrusion Detection

4. Results:

This model demonstrates the integration of many components that improve the MQTT Protocol Security in Internet of Things devices, such as the Raspberry Pi 3B+ NodeMCU, LCD screen, piezo buzzer, DHT 11 sensors, and PC.In this instance, clients are NodeMCU devices with DHT11 sensors, while the MQTT server is a Raspberry Pi. Temperature and humidity readings are collected by the NodeMCU devices and sent to the Raspberry Pi via the MQTT protocol.

Fig .4: Working Model of Developed System

IoT applications are becoming more widely available and adaptable thanks to the development of powerful, reasonably priced, and network-capable devices. A strong platform for monitoring and analysis is created when the MQTT protocol's efficiency for data transfer is paired with the computational capability of a Raspberry Pi. Using data patterns, this configuration makes use of the advantages of each component to continuously monitor the environment and identify possible intrusions.

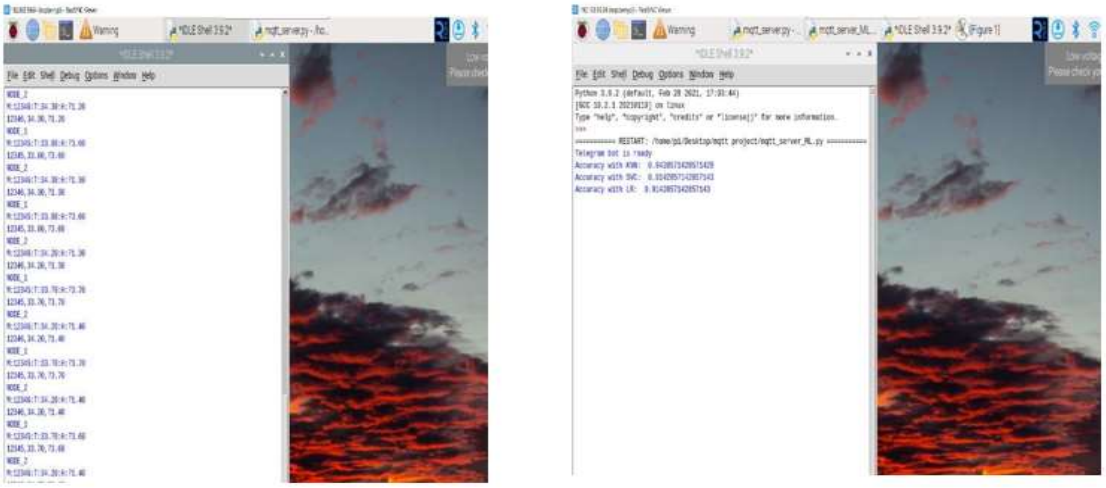

Fig 5: (a) Calculating Sensor Values (b) Calculating Accuracy of ML Algorithms

Here, the DHT 11 sensor computes the sensor values related to the NODEMCU, as seen in figure 5(a), and the machine learning algorithm's correctness is demonstrated in image 5(b). Following accuracy calculation, the confusion matrix is displayed in Fig 6. Using this, we may plot the accuracy of the ML algorithms.

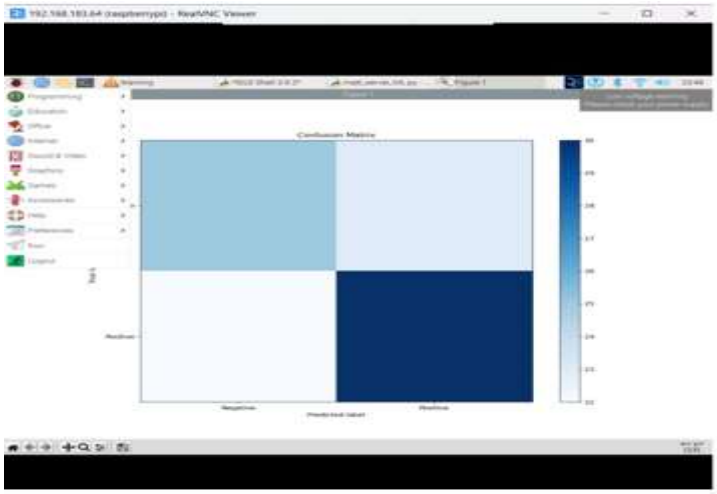

Fig 6: Confusion Matrix

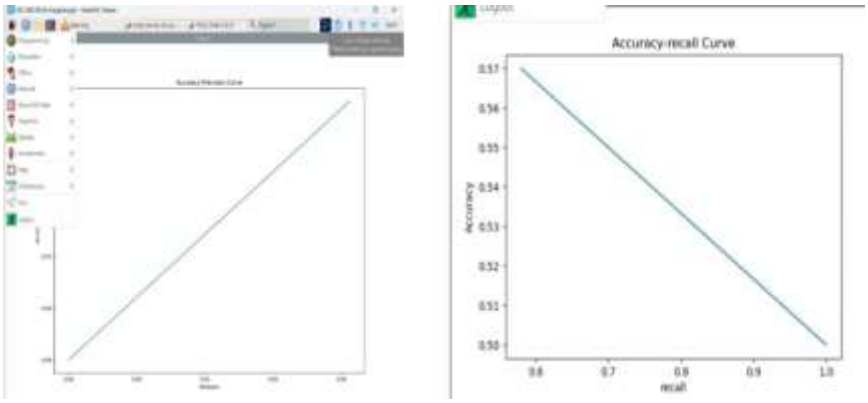

Fig 7: Accuracy Precision Curve, Accuracy Recall Curve

Figs 8 below depict the notification in the Telegram bot and LCD display when invasions happened, while figures 8 above illustrate the curves of accuracy, precision, and recall that are calculated from the confusion matrix.

Fig 8: Notification from The Telegram Bot (G) Alert Message on Lcd Display

4. Conclusion:

To sum up, this research effectively illustrated how to create an all-encompassing and sophisticated IoT security solution. The system efficiently collects environmental data and applies machine learning for anomaly detection using NodeMCU devices and Raspberry Pi. This makes it possible to identify possible security risks by looking for departures from predetermined benchmarks. The solution enables users to take prompt action by sending out timely alerts via emails or mobile applications. This study demonstrates how combining different technologies can result in strong, clever solutions for increased security in homes and workplaces that provide people peace of mind. But it's critical to recognise that there's always space for development. More sensors could be integrated into this work in the future to collect a larger variety of environmental data, which could result in more powerful anomaly detection capabilities.

Furthermore, as the machine learning system is developed further, it may become more adept at distinguishing between security concerns and real oscillations. All things considered, this work demonstrates how easily accessible technology may be used to build an intelligent and user-friendly security system. Research and development can lead to ever more advanced and integrated solutions for improved security in our living and working places as the Internet of Things continues to expand. The system has several benefits and a wide range of applications that help make home and business security more proactive and all-encompassing.

Reference

[1] C. Tankard, ``The security issues of the Internet of Things," Comput. Fraud Secur., vol. 2015, no. 9, pp. 1114, Sep. 2015.

[2] A. Sforzin, F. G. Marmol, M. Conti, and J.-M. Bohli, ``RPiDS: Raspberry pi IDSA fruitful intrusion detection system for IoT," in Proc. Int. IEEE Conferences Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People, Smart World Congr. (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), Jul. 2016,pp. 440448.

[3] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, ``MQTT-SA publish/subscribe protocol for wireless sensor networks," in Proc. 3rd Int. Conf. Commun. Syst. Softw. Middleware Workshops (COMSWARE), Jan. 2008, pp. 791798.

[4] T. Yokotani and Y. Sasaki, ``Comparison with HTTP and MQTT on required network resources for IoT," in Proc. Int. Conf. Control, Electron., Renew. Energy Commun. (ICCEREC), Sep. 2016, pp. 16.

[5] M. Ahmad, T. Younis, M. A. Habib, R. Ashraf, and S. H. Ahmed,``A review of current security issues in Internet of Things," in Recent Trends and Advances in Wireless and IoT-Enabled Networks. Cham, Switzerland: Springer, 2019, pp. 1123, doi: 10.1007/978-3-319-99966- 1_2.

[6] B. Mishra and A. Kertesz, ``The use of MQTT in M2M and IoT systems: A survey," IEEE Access, vol. 8, pp. 201071201086, 2020.