Guarding Your Privacy: A Multilayered Defence Strategy for Smart Homes with AES-128 Encryption and Honey Words

MSc Research Project
MSc in Cyber Security

Shaikh Sharuk Shaikh Babu
X23225262

School of Computing
National College of Ireland

Supervisor: Dr Raza Ul Mustafa

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Shaikh Sharuk Shaikh Babu		
Student ID:	X23225262		
Programme:	MSc in Cyber Security	**Year:**	2024
Module:	MSc Research Project		
Supervisor:	Dr Raza Ul Mustafa		
Submission Due Date:	12-12-2024		
Project Title:	Msc Research Report		
Word Count:	**5693**	**Page Count: 19**	

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Shaikh Sharuk Shaikh Babu

Date: 12/12/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

“Guarding Your Privacy: A Multilayered Defence Strategy for Smart Homes with AES-128 Encryption and Honey Words”

Shaikh Sharuk Shaikh Babu
X23225262

Abstract:

This research project is to improve privacy in smart homes by proposing combined encryption approach that comprises AES-128 to encrypt the payload data of IoT sensors and a honey word system to create deceptive data for additional privacy. The project is based on the facts that the number of smart home devices is growing, and, as a result of it, personal data is generated and transmitted insecurely. The research objectives are as follows; One is to ensure that the data collected by the sensors is protected using a robust encryption method and secondly to ensure there is a honey word system that confusing the potential attackers. AES-128 encryption is used along with a honey word system as a part of securing smart home data. With that said, the research does not propose more performing solutions as it would require a much more extensive study of the subject along with the ethical, legal, and regulatory frameworks generating the discrepancy between the comfort of Smart Home technologies and the need for privacy protection.

1.Introduction:

1.1 Background:

Technology dependence is growing very popular today amongst this generation. The IoT is spreading like wildfire and the futuristic world is dives and bounds ahead. Smart home devices have become so dominant that they changed the way we live, bringing unprecedented comfort, convenience and automation to our homes. Connected to smart thermostats and lighting systems and, in some cases, sophisticated security and entertainment setups, the IoT has arrived to stay and as it turns out to help with more than just the internet anymore. While this rapid adoption has occurred at a pace faster than the corresponding development of robust security and privacy safeguards, these sensitive data of users are easily exploited. According to (Alwarafy et al., 2020), (Silverio-Fernández et al., 2018), (Uppuluri & Gondi, 2022), the reliance of home on interconnected devices increases the possible attack surface and the landscapes of potential breaches for personal information. Despite of all the great benefits of smart home technology, the privacy risk is too great to ignore today. Over the years the smart home market has been growing exponentially. The Statista report (Sherif, 2023) indicates widespread smart home device adoption, as smart TVs are the most popular with 76% of audiences owning the device. What makes it concerning is that this is a case where things are adopted very widely, which only underlines the urgent need for effective privacy enhancing solutions.

Furthermore, projections indicate continued growth in the smart home market, with user numbers expected to reach 103.15 million in the United States by 2028 (U.S.: Smart Home Number of Users (2019, 2023; 2019-2028). In addition, this upward trend validates the importance of tackling this privacy issue in a forward looking and general manner. Think about you are step into home tired and having lights adjust to a preferred setting, the thermostat preheating to an ideal temperature and favourite played music softly filling in the background. The integration of technology has been perfected at with this being a wireless that is custom made built to enhance both comfort and convenience.

However, this ideal scenario conceals a hidden reality: Every interaction in your smart home creates information about your routine. But often, this data which contains details about your sleep and wake patterns, energy usage, entertainment preferences, daily routines is transmitted and stored with no security in place to protect against malicious exploitation of your data.(Apthorpe et al., 2017).

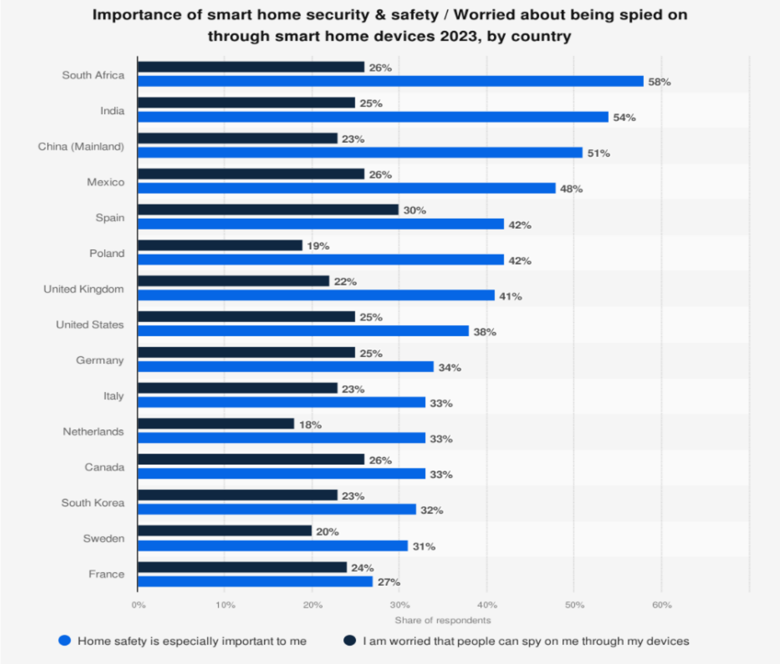


Figure 1: Statista report (Sherif 2023)

1.2 Motivation:

As smart home technology rapidly increases, promising to make our living space more convenient, automated, personalised and more omits the fundamental problem that these technologies pose to our privacy. Since every interaction in the smart home causes the generation of enormous amounts of personal data, these interactions would result in the creation of a digital footprint that can reveal details about people's lives.(Tiwari & Waoo, 2023) This data is often transferred and stored insecurely, making it a vulnerable target to malicious attackers. The current security measures are inadequate for defending against modern hackers who have become ever more complex. (Vardakis et al., 2024) If the enemy is already inside, exploiting vulnerabilities within the data, this research forgets the essential pressure between the comfort of smart home convenience and the necessity of strong privacy protections. To this end, the research suggest a new method to combine AES-128 encryption and honey word system but this method may not solve the inherent problem. Yet, there's no way for us to completely eliminate the negative influence of data breaches and privacy violations through technological solutions. The research ignores the social implications of relying more and more on smart home technologies and possible misuse or even unintended consequences.

Unpacking the multi-layered function that smart home technology plays in our lives, it becomes necessary to look at the compact collection of ethics, laws, and regulations; all of which encompass a more comprehensive approach.

1.3 Objectives:

Develop a robust encryption mechanism using AES-128 to secure IoT sensor payload data:

The objective behind this is to enable strong encryption of raw data transmitted through smart home sensors. This research tries to stop unauthorised access and kernel edge by encryption provided to this data at the source.

Design and implement a honey word system to generate decoy data for enhanced obfuscation:

Additionally, to make a system as a second layer protection will generate fake sensor data, with the help of 'honey words' so that potential attackers will be mislead. This research attempts to mingle real sensor readings along with these decoy data which will create confusion and probably make it harder for attackers to pull out valuable data.

1.4 Research Question:

1. How can AES-128 and honeywords complement each other to create a multi-layered defence for smart home data?

1.5 Structure of the Report:

In the following section 2 explores discusses about the weakness in MQTT and improvements accordingly, literature survey about encryption and obfuscation with their usage in IoT environment, reviews privacy frameworks and user-oriented approaches to smart homes and describes the over-reliance of MQTT on IoT and smart home automation.

The section 3 discusses the study with the CRISP-DM approach at various phases including Business Understanding, Data Understanding, Data Preparation, Modeling, Evaluation, and Deployment. It also explains the research method and instruments used in the study and the configuration of the Wokwi platform used for smart home modeling.

The Section 4 explains the Node-RED flow for smart home simulation, including data collection, visualization, and control, and describes the system's Node-RED dashboard without encryption.

In the Section 5, how the system is implemented is highlighted and implementation process is described, output data such as transformed data, encryption logic, honeyword generation, and visualization is provided along with programming languages, tools, and libraries used. Secure communication, encrypted payloads, and functional simulations are the last outputs.

The Section 6 analyzes encrypted payload values in the Wokwi platform and Wireshark while also visualizing encrypted data without decryption in Node-RED.

The final part of the paper is Discussion, which provides a comparison of the results with the literature and evaluates the consequences of the research for smart home security.

The Conclusion and Future Work section of the paper restates the contributions and research outcomes and presents improvements and expansions that can be made. Last but not the least the References section that contains all the works that was cited in the paper and it will be arranged according the format required.

2. Related Work:

While smart home technology brings many advantages, it also poses big security and privacy problems. Existing research into these challenges is examined in this literature review, concentrating on data encryption and obfuscation techniques.

2.1 Security Considerations and Challenges:

While it has many benefits, one and possibly the most important thing that MQTT lacks is robust security features. (Al-Ani et al., 2023) explores these security issues, including vulnerabilities concerning confidentiality, integrity, and availability. Mandatory encryption is not required in the basic MQTT protocol, such that an eavesdropping can occur to Man-in-the-middle attack which can intercept and steal the data between the devices and broker. In addition, the threat of illegal access, confirmed in (Harkai, 2024), and necessitates the use of strong authentication mechanisms to defend against the introduction of false data by malicious publishers or subscribers as well as preventing them from corrupting the system. Therefore, due to these security vulnerabilities, more security measures need to be taken into aspects, for example, to exchange data between components such as a plugin and a mobile device, the combination of encryption and authentication using the Transport Layer Security should be implemented to provide secure communications at a smart home environment.

2.2 Encryption and Obfuscation Techniques:

Currently, there are some literatures about the methods regarding the encryption and obfuscation to effectively protect IoT devices privacy in smart homes. Various works have been carried out to determine the influence of encryption technologies on IoT data security, the effectiveness of encryption algorithms (Ayari et al., 2024).Proposed solutions include a new cryptographic architecture for IoT devices based on honey encryption, providing a novel approach to data protection , and lightweight encryption algorithms designed to address the resource constraints of many smart home devices .Further, the authors have discussed smart home security in the context of the IoT to show that effective security measures should be incorporated. Similar discussion on security and privacy concerns in edge-computing-assisted IoT have also pointed out their possible positive impact on security and privacy (Alwarafy et al., 2020) At the same time, exhaustive overviews of IoT threats and attacks provide useful insights into the security scenario.

2.3 User Perceptions and Privacy Frameworks:

Therefore, it is quite evident that the perception of users, interaction and control, as well as the establishment of the right privacy measures for smart devices, is vital in the right advancement of smart home technologies. Privacy of smart home and its elements has been discussed in detail by (Guhr et al., 2020) and the authors point to lack of easy to use privacy solutions. In the article by

Toutsop et al.(2020) suggests practical how-to methods that would enable users not to allow smart home devices to snoop on them. (Uppuluri & Gondi, 2022) also propose a secure user authentication and key agreement scheme to protect user authentication for IoT device access control.

2.4 MQTT in Smart Home Automation and IoT Application:

Due to the lightweight of the protocol, MQTT offers the means for effective communication in the smart home automation and IoT in general. Its application in smart grids, where real time data exchange is essential for efficient energy management, is discussed (Cristian et al., 2019). Due to its ability to send and receive data without relying on too many network resources, MQTT is good for monitoring and controlling energy consumption within smart homes. A practical example of an IoT based smart home testbed by (Yalçınkaya et al., 2020) shows the effectiveness of MQTT for controlling several devices and sensors in case of home environment. Widespread adoption of the protocol in smart home systems is in part due to its flexibility and ease of integration with differing hardware platforms.

Research Topic	Key Findings from Existing Research	Gaps Identified	Research Contribution
Security Aspect and Issues in MQTT	MQTT also does not come with powerful security measures, which makes messages within the broker easily intercepted, faked or even forging the broker's identify. Solutions exist already such as TLS and these can actually create a larger problem that of overhead.	Inadequate robust, extensive, and lightweight security frameworks that can be used by the constrained smart gadgets.	Combines AES-128 together with honeyword system to improve privacy of smart homes, therefore has been proposed.
Encryption And Obfuscation Practices	There are diverse encryption to obfuscate the IoT devices technologies such as honey encryption as well as lightweight encryption algorithms.	There are a few studies which explore the overlap of encryption with the use of decoy data to act as a defense mechanism. As it is observed current solutions mostly	AES-128 encryption enhancing the honeyword system, Smart Home Shield provides a unique layered security for home's information.

		address protection on a single layer.	
User perceptions and Privacy Frameworks	First, focus on user perceptions of privacy and then present the necessary frameworks to think about privacy. In other words, user perception plays an important role in how smart home technology should be used and privacy models should be designed. The research consequently focuses on ease of use of privacy controls and user control.	It remains quite rare to find operational and easily scalable practical examples of user-cantered privacy features. Basically, users may have privacy-related tools and information, but these are often inadequate to protect their privacy.	In a way, is not its primary goal but can be useful for improving user's privacy since it adds an extra layer of security to the data and might help gain the users' trust.
Applications of Smart Home Automation and IoT using MQTT	MQTT is ideal for applications in smart home automation and other IoT applications that include smart grids and controlling gadgets.	In terms of investigating the effects of activities that seek to improve security of MQTT based systems on their usability. Maintaining the security balance is a major issue.	Admits that AES-128 and honeywords may come as overhead but in an effort to strike a balance to the security measures.

2.5 Why AES128 and Honey Words encryption instead of other encryption techniques:

The preference for AES-128 encryption arises from its superior capabilities over alternative cryptographic techniques.

The choice of AES-128 encryption for MQTT-based smart home IoT systems exists because it provides balanced security with optimized performance and efficiency at a superior level compared to asymmetric and hybrid encryption technologies. RSA and ECC provide strong encryption protection but create excessive computational challenges that make them inappropriate for monitoring IoT devices with constrained resources. The encryption speeds of RSA decrease dramatically because of its 2048- or 4096-bit key lengths thus causing unacceptable delays in real-time smart home systems. ECC's key exchange operations require additional processing resources compared to RSA thus causing MQTT message delays (Karmous et al., 2024).

AES-128 demonstrates symmetric encryption by using static 128-bit key lengths to ensure swift encryption processes and protect against cryptographic threats. The encryption duration of AES-128 stands at 0.1504 ms due to its superb speed while ECC and RSA require longer times which surpass 0.9372 ms even for relatively small data payloads (Liu et al., 2024). The lightweight characteristics of AES-128 enable its optimal deployment on IoT devices which need minimal power consumption. Experimental research showed that AES-128 cryptography provides reduced computing resources along with storage requirements when used in MQTT systems compared to ECC-based hybrid systems (Hizem et al., 2024). Hybrid encryption through ECC + AES improves security by uniting asymmetric techniques with symmetric approaches at the expense of system complexity and slowdown in processing time. Key exchange methods within hybrid encryption systems that use ECC extend encryption duration and reduce the efficiency of MQTT protocols because of their need for quick communication. The standalone AES-128 encryption method bypasses these delays by directly encrypting MQTT payloads while requiring low processing overhead as explained in (Karmous et al., 2024). Most hybrid encryption methods produce enlarged encrypted packet sizes that cause problems in bandwidth-limited IoT environments. AES-128 finds widespread adoption across IoT hardware devices because these systems integrate AES acceleration capabilities which improve their operational efficiency. AES-128 demonstrates its superiority over asymmetric and hybrid techniques by providing secure end-to-end encryption alongside quantum computing resistance making it the best choice for MQTT-based smart home systems (Liu et al., 2024). The analysis identifies AES-128 as the optimal security choice for IoT protection through excellent efficiency performance and strong security robustness in real-time smart home deployments.

3.Research Methodology:

This research mainly focuses on improving the security of smart home data through the implementation of AES-128 encryption technique and honeywords which in turn form multiple layers of defence. The methodology is designed in a highly regulated manner to give solutions to the three main goals of data security, data consistency and protection from attacks while not compromising the ease of use and adaptability which is important in IoT settings. The process covers several stages of the smart home system design, implementation, testing, and assessment, with an emphasis on the use of such elements as virtual simulations and encrypted transmissions for effective construction of the smart home's framework (Wang et.al. 2023).

3.1 Integration into Methodology CRISP-DM Framework:

This research employs the **CRISP-DM** approach to systematically develop, deploy and assess the security solution.

The phases include:

- **Business Understanding:** How smart home data can be protected through the use of AES 128 encryption as well as honeywords.
- **Data Understanding:** In this step, properties of the sensor data and techniques of transmitting the data will be discussed.
- **Data Preparation:** Cleansing of raw data collected from the sensor for encryption.
- **Modeling:** AES-128 and honeyword generation has been incorporated.

- **Evaluation:** Using Wireshark and analysing MQTT payload for security assurance.
- **Deployment:** Simulating a smart home system on virtual hardware and the integrate with Node-RED for visualization.

3.2 RESEARCH DESIGN:

This research design depicts the integrated approaches of several technologies and methodologies, to simulate and secure a smart home environment using IoT devices. It starts from a smart home simulation of Wokwi platform, the generated data are through DHT22 sensor. This sensor takes payload data, things like temperature and humidity, and sends it over a private Wi-Fi gateway. The payload is encrypted using AES-128 for the security layer by flowing through an ESP32 microcontroller. Furthermore, a honeywords mechanism is in place to alert a potential attack, e.g. someone trying to access or change the data without authorization.

The data is then encrypted and secured, and sent via an MQTT propagator to an MQTT publisher and the data stream is sent to a HiveMQ server. The data is integrated into Node-RED from the server and processed from there. Wireshark is used as a packet tracer and network analyzer to ensure robustness of the system by real time monitoring and analysis of data packets transmitted through the system. With this layered design, we ensure integrity, confidentiality of smart home data and how it gets managed securely, taking advantage of a simulated environment to test the setup.

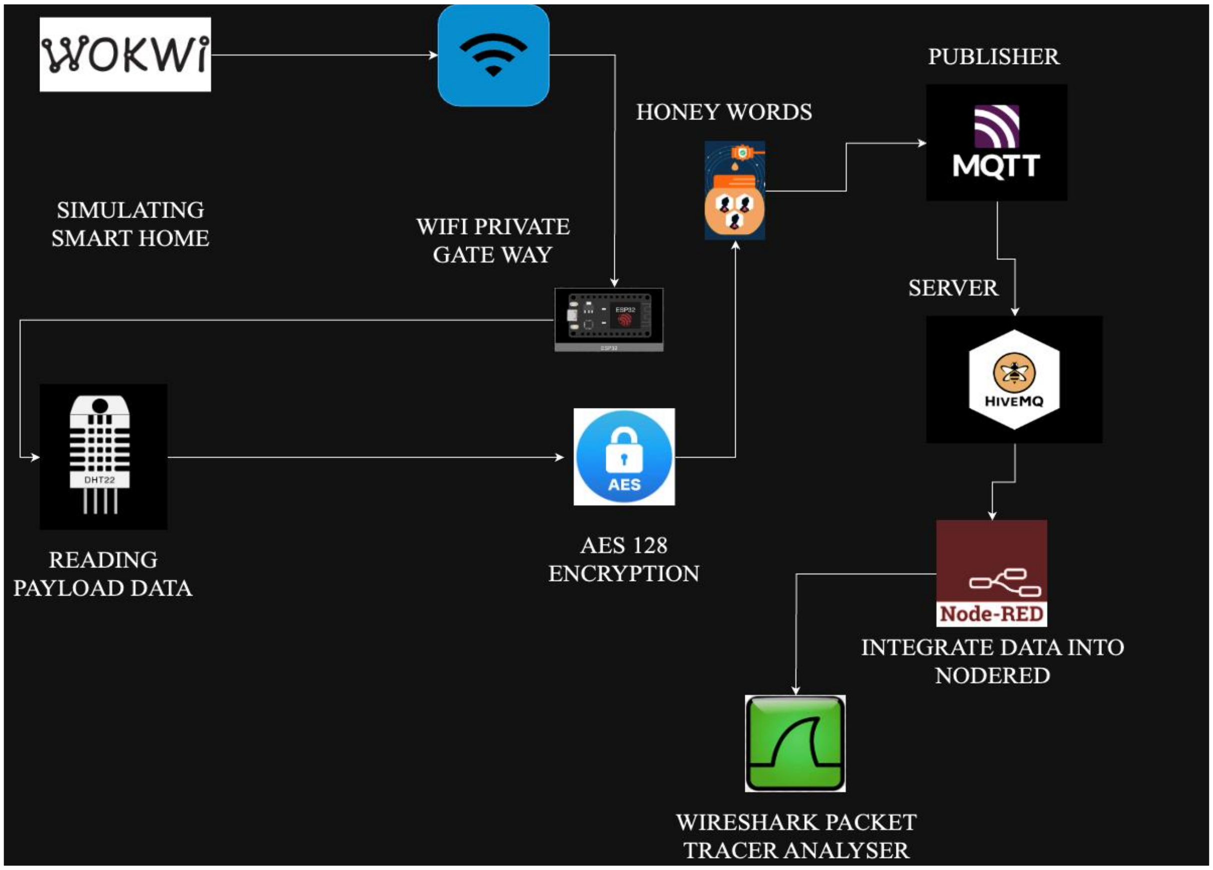


Figure 2: Research Methodology design

3.3 SIMULATION SETUP:

This model implemented on the Wokwi platform shows abundant IoT devices connected to a single ESP32 microcontroller for managing all functions of a smart home. This simulation's main purpose is to mimic such essential features of the Smart Home system like environment checking, illumination, and home automation. The centrepiece of this simulation is the ESP32 microcontroller that is responsible for data processing and control commands of other devices. Temperature and humidity are obtained from the DHT22 sensor connected to the ESP32, are crucial to smart home system regulation. The sensor readings picked by the ESP32 can either be utilized to trigger certain actions or displayed in real-time as graphs. The simulation also has a Neopixel LED ring incorporated as a visual feedback device. Temperature thresholds or other rules can be set and it responds by changing colors: (e.g., red,green, blue). This feature shows the ways of using light in smart home to provide information or to create certain atmosphere. Also, the ESP32 is connected to an LED and an appropriate current-limiting resistor to light the simplest status indication that blinks to confirm system operation or to signal specific events. A servo motor is also included in the setup; this is a mechanical sub-system of the smart home e.g. an automated door lock or window controller. It also demonstrates its ability to handle physical devices by taking control signals from the ESP32. Currently, power to all the components is drawn from the ESP32 and connects to the simulated environment to function effectively. Wokwi is a platform that allows individuals to build IoT systems so that they can experiment with the concepts of smart home automation and control by simulating environments such as this smart home environment. It can be an effective reminder how IoT solutions have much relevance in today's smart homes.

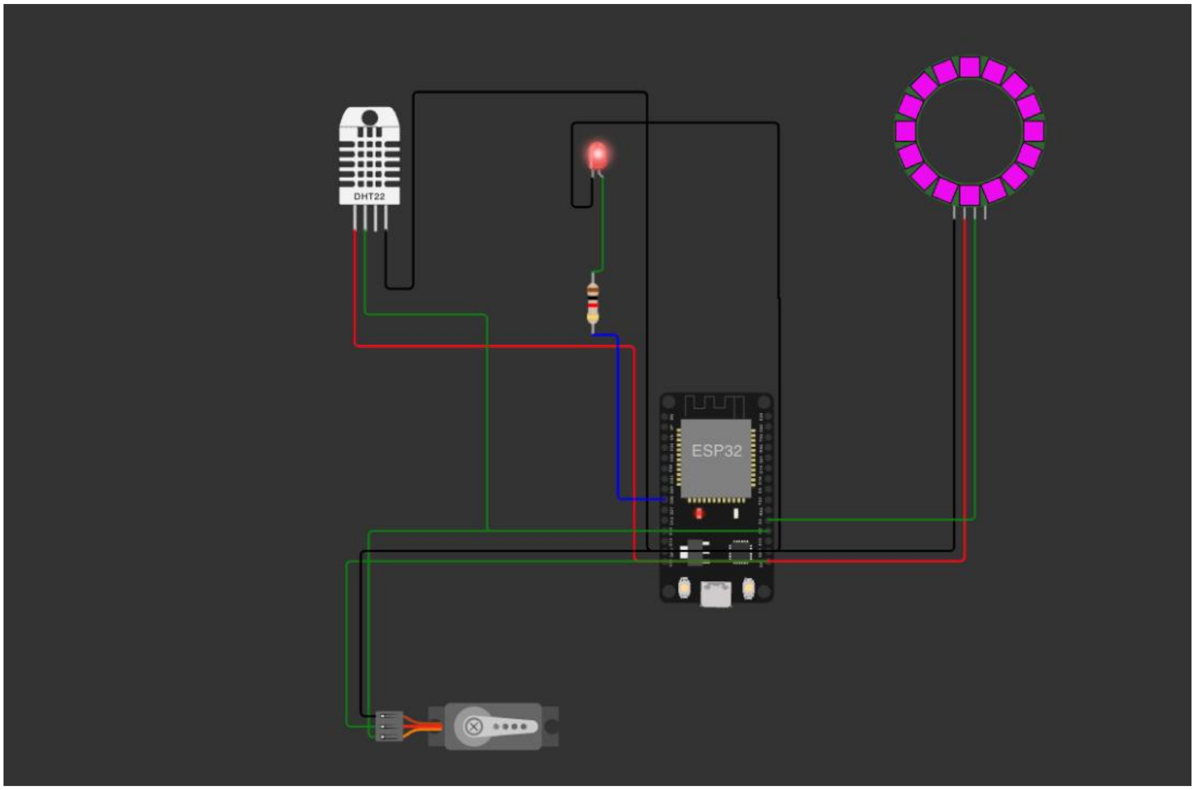


Figure 3: Wokwi Smart Home Simulation

4. Design Specification:

4.1 Node red Flow for Smart Home simulation:

Node-RED flow, a smart home environment is simulated to demonstrate the data collection, processing and device control from IoT-based devices. Thus, the flow starts by receiving payload data from simulated sensors and devices as all simulated environmental parameters and smart home controls. The system extracts critical environmental data such as temperature and humidity through dedicated function nodes: Extract temperature and Extract Humidity. The smart home conditions are monitored by displaying the data using interactive dashboard elements such as Temperature Chart, Humidity Chart, Temperature Meter and Humidity Meter. Users receive instant feedback about the simulated environment in this visualization. To mimic real world, the flow contains logging nodes (temperature logs and humidity logs) which store historical data for environmental trend analysis and long term monitoring. And the simulation controls virtual smart devices like a Front Light, Front Door, and a Smart Bulb which represent common smart home functionalities. Front Light and Front Door nodes districts can be toggled or tracked states so you can simulate stuff like automating lights and monitoring door access. Next, we incorporate a dynamic Color Changing node to adapt the Smart Bulb's color as a function of changes in temperature or humidity, and to represent adaptive smart home features in a realistic manner. It brings in a level of automation and a greater layer convenience and how user interacts with that. Here is a complete smart home ecosystem data collection, visualization, logging, controlling with this Node-RED flow. As a simulation tool, it provides a good proof of concept to test and understand IoT based smart home implementation.

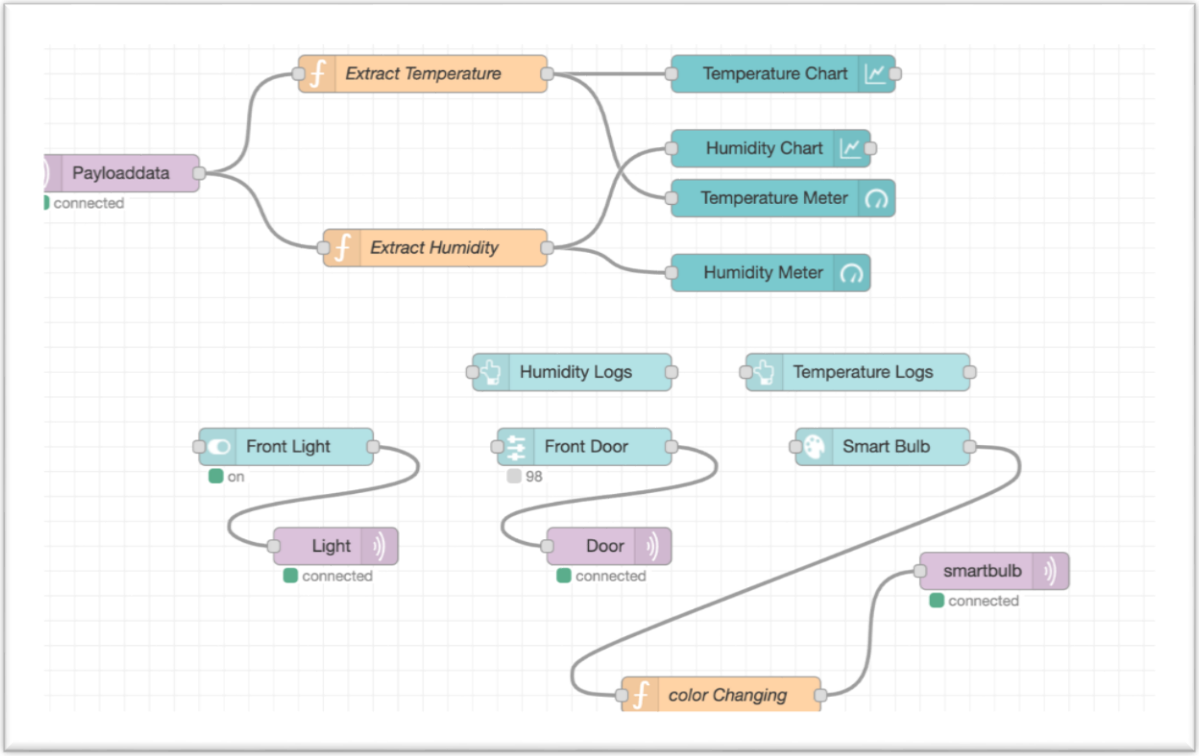


Figure 4: Node Red Flow

4.2 Node Red Dashboard Without Encrypting Data Visualisation:

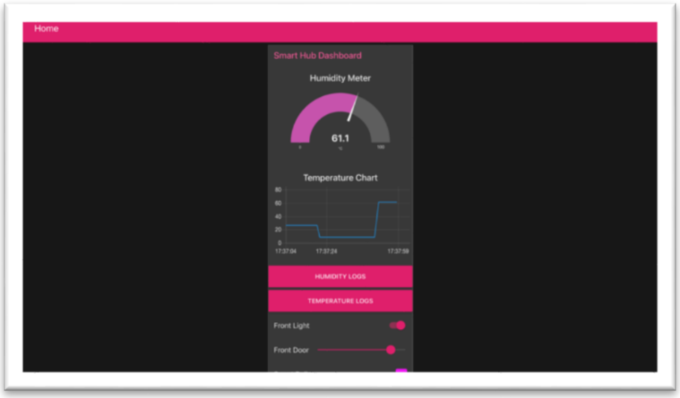


Figure 5: Without Encryption Payload Dashboard

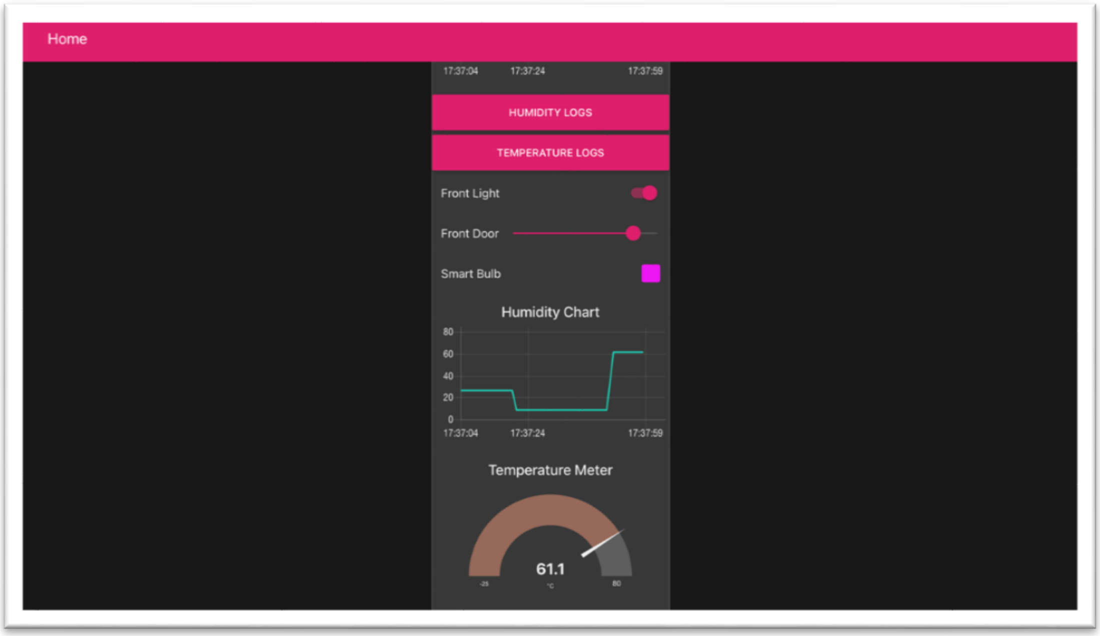


Figure 6: Without Encryption Payload Dashboard

5. Implementation:

Specification For Implementing (ICT) Solution:

5.1Purpose:

The main objective in the final implementation stage was to create a secure system for smart home data transmission. AES-128 encryption is used to provide confidentiality and honeywords creation is integrated to achieve obfuscation and enhanced security by the system. It also ensures that data transmitted from virtual IoT devices is kept secured from interception and misuse. The output encrypted data streams simulated the virtual hardware environment completely and build an MQTT based communication framework.

5.2 Outputs Produced:

- **Transformed Data:** Data with the values of temperature and humidity from the pretend DHT22 sensor is coded into a JSON object with real and fake data (honeywords). The JSON object is then AES-128 encrypted and then encoded in Base64 to fit into the MQTT protocols.
- **Code Developed:** AES-128 Encryption module encrypts the real and decoy data with added effects in order to enhance the aspect of security.
- **Honeywords Generator:** Uses mimics to showing the actual sensor outputs. MQTT communication system posts the data with encryption to the broker and listens to topics for controlling the devices.
- **Virtual Simulation:** The system is implemented and tested on Wokwi, an online hardware simulator platform, so no additional hardware appliances are required, but the realism is preserved.
- **Visualization:** This is transported and closely monitored using Node-RED for the confirmation of real time transmission of data. Secondary to encryption, direct observation of raw format cannot be done and the more highlight is on transmission.

5.3 Tools and Languages Used Languages:

- **C++:** Used for the firmware and encryption logic writing for the ESP32 micro controller.
- JavaScript: Implemented in MQTT communication and visualized on data using Node-RED.

Development Tools:

- **Wokwi Simulator:** To emulate ESP32, DHT22 sensors, NeoPixel LEDs and servo motors a virtual hardware simulation platform has been utilised.
- **Arduino Environment (Integrated in Wokwi):** Used for creating and implementing an embedded code.

Libraries:

- **Adafruit Unified Sensor:** DHT22 sensor interfacing.
- **DHT Sensor Library:** To take temperature and humidity readings.
- **AESLib:** AES-128 encryption is used for performing.
- **Base64:** To encode encrypted data in a transmission compatible format.
- **PubSubClient:** For MQTT communication.
- **ESP32Servo:** For controlling servo motors.
- **FastLED:** Used for controlling the Neo Pixel LED strip.

Data Transmission:

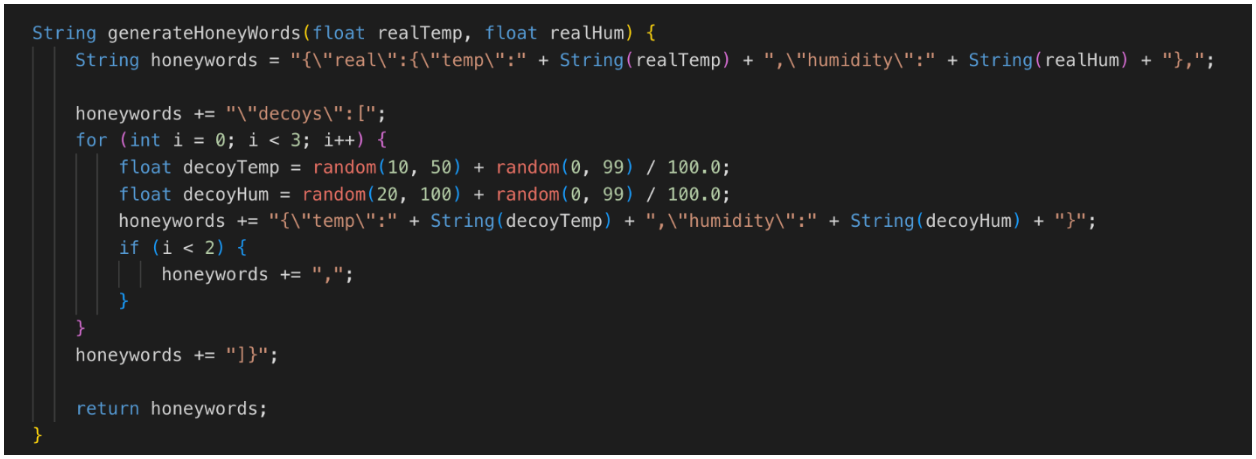
- MQTT Broker: The MQTT broker for publishing and subscribing encrypted data streams to HiveMQ server.

Validation Tools:

- **Wireshark:** Captures network traffic and validates encryption of data transmitting.
- **Node-RED:** Applied to configure MQTT flows and to make data check to make sure it is streaming properly.

5.4 Final Outputs:

- **Transformed and Secured Data:** From the DHT22, the sensor readings (temperature, and humidity) are taken and transformed into a JSON payload by the system.
- The payload is enhanced with honeywords, decoy data that confuse potential attackers. AES-128 is a symmetric encryption algorithm well known for its security and efficiency and encrypted payload. Then, the encrypted data is encoded into a Base64 compatible format with the MQTT protocol.
- Generate Honeywords function synthesizes real, and decoy data into a single payload, where decoy data cannot be distinguished from real sensor readings.



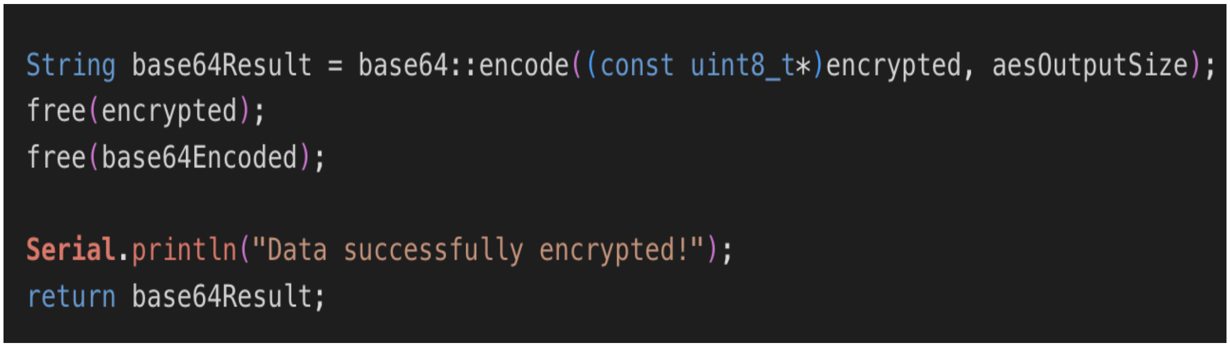
```
String generateHoneyWords(float realTemp, float realHum) {
    String honeywords = "{\"real\":{\"temp\":" + String(realTemp) + ",\"humidity\":" + String(realHum) + "},";

    honeywords += "\"decoys\":[";
    for (int i = 0; i < 3; i++) {
        float decoyTemp = random(10, 50) + random(0, 99) / 100.0;
        float decoyHum = random(20, 100) + random(0, 99) / 100.0;
        honeywords += "{\"temp\":" + String(decoyTemp) + ",\"humidity\":" + String(decoyHum) + "}";
        if (i < 2) {
            honeywords += ",";
        }
    }
    honeywords += "]}";

    return honeywords;
}
```

Figure 7: Honey words Code Snippet

- It is used to encrypts the payload with AES-128 encryption then encode in Base64 to securely transmit.



```
String base64Result = base64::encode((const uint8_t*)encrypted, aesOutputSize);
free(encrypted);
free(base64Encoded);

Serial.println("Data successfully encrypted!");
return base64Result;
```

Figure 8: AES Data Encrypt

Functional Virtual Simulation:

- The project proves how a complete smart home system functions using the Wokwi virtual environment.

Temperature and Humidity Monitoring:

- This wokwi software captures real-time sensor data from the DHT22 sensor, processes it using the ESP32 and forwards the data to the specified multicast IP and port.

Actuator Controls:

- The Neo Pixel LED strip behaves like a set of home lighting and responds to MQTT commands accordingly**.**
- Through the MQTT messages, the door or window movements are simulated from a servo motor.

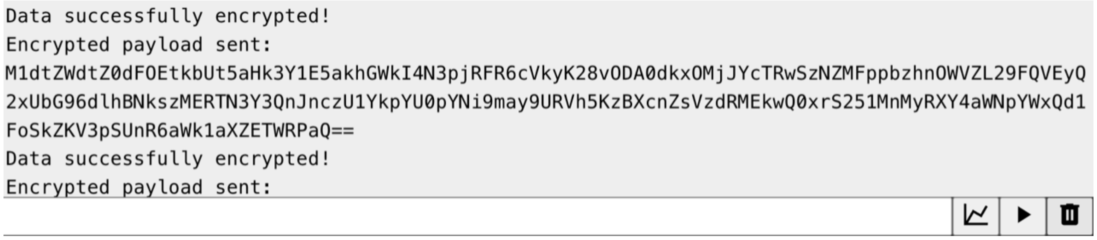
Secure Communication:

- MQTT broker receives all data, whether sensor readings or actuator states, that is encrypted.
- It sets up the virtual hardware and connects exactly what's necessary for a simulation.

6. EVALUATION:

At the end of this section, a simulation of the proposed model shown how they evaluated. The encrypted payload value were analysed in Wokwi, the encrypted payload value are also analysed in Wireshark and the privacy consideration maintain data privacy without decryption are analysed in Node RED.

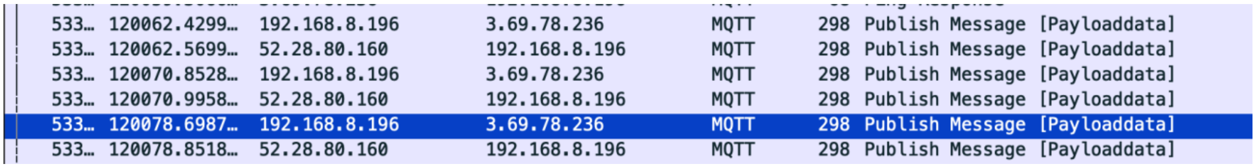
6.1 Analyse the encrypted payload value in Wokwi:



```
Data successfully encrypted!
Encrypted payload sent:
M1dtZWdtZ0dFOEtkbUt5aHk3Y1E5akhGWkI4N3pjRFR6cVkyK28vODA0dkxOMjJYcTRwSzNZMFppbzhnOWVZL29FQVEyQ
2xUbG96dlhBNkszMERTN3Y3QnJnczU1YkpYU0pYNi9may9URVh5KzBXcnZsVzdRMEkwQ0xrS251MnMyRXY4aWNpYWxQd1
FoSkZKV3pSUnR6aWk1aXZETWRPaQ==
Data successfully encrypted!
Encrypted payload sent:
```

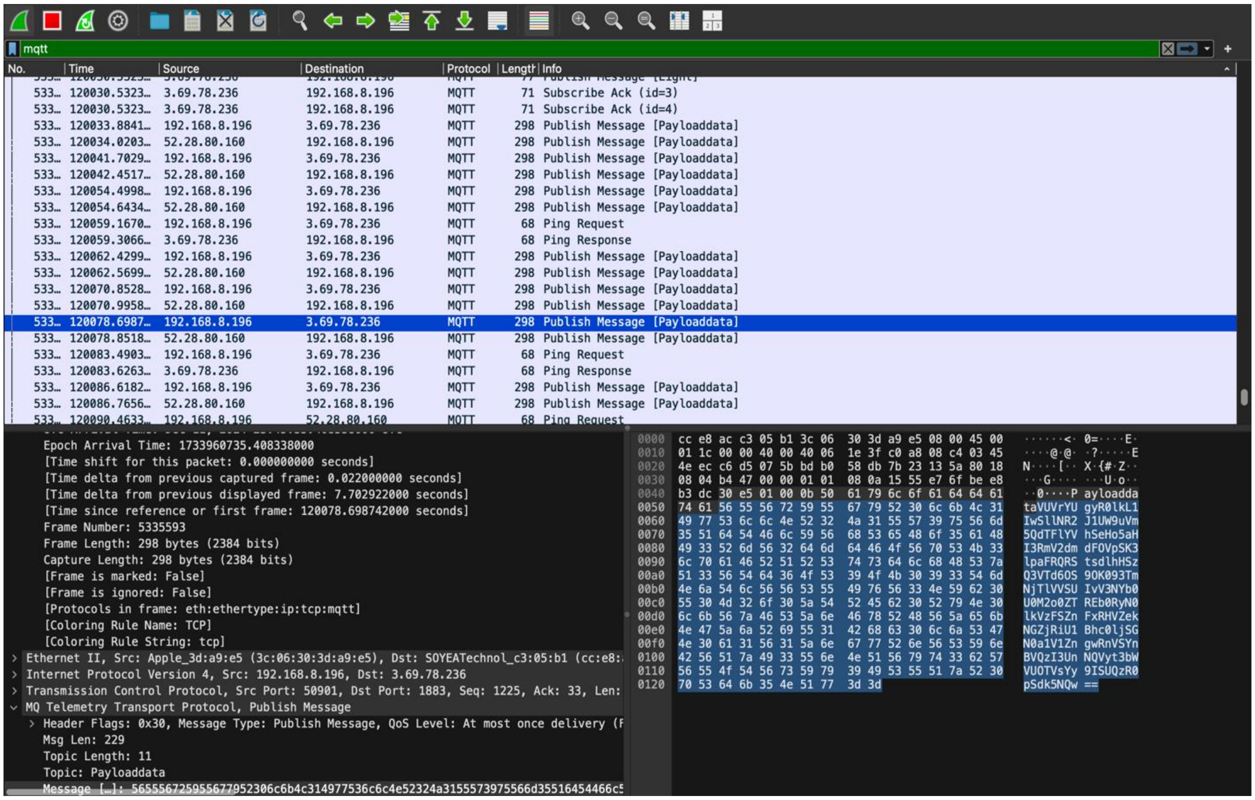
Figure 9: Encrypted payload in Wokwi

6.2 Analyse the encrypted payload value in Wire shark:



```
533… 120062.4299… 192.168.8.196   3.69.78.236     MQTT   298 Publish Message [Payloaddata]
533… 120062.5699… 52.28.80.160    192.168.8.196   MQTT   298 Publish Message [Payloaddata]
533… 120070.8528… 192.168.8.196   3.69.78.236     MQTT   298 Publish Message [Payloaddata]
533… 120070.9958… 52.28.80.160    192.168.8.196   MQTT   298 Publish Message [Payloaddata]
533… 120078.6987… 192.168.8.196   3.69.78.236     MQTT   298 Publish Message [Payloaddata]
533… 120078.8518… 52.28.80.160    192.168.8.196   MQTT   298 Publish Message [Payloaddata]
```

Figure 10: Honey Word Creation (Decoy Data)



```
mqtt
No.    |Time          |Source         |Destination    |Protocol |Lengtl |Info
533…  120030.5323…  3.69.78.236     192.168.8.196   MQTT      71  Subscribe Ack (id=3)
533…  120030.5323…  3.69.78.236     192.168.8.196   MQTT      71  Subscribe Ack (id=4)
533…  120033.8841…  192.168.8.196   3.69.78.236     MQTT     298  Publish Message [Payloaddata]
533…  120034.0203…  52.28.80.160    192.168.8.196   MQTT     298  Publish Message [Payloaddata]
533…  120041.7029…  192.168.8.196   3.69.78.236     MQTT     298  Publish Message [Payloaddata]
533…  120042.4517…  52.28.80.160    192.168.8.196   MQTT     298  Publish Message [Payloaddata]
533…  120054.4998…  192.168.8.196   3.69.78.236     MQTT     298  Publish Message [Payloaddata]
533…  120054.6434…  52.28.80.160    192.168.8.196   MQTT     298  Publish Message [Payloaddata]
533…  120059.1670…  192.168.8.196   3.69.78.236     MQTT      68  Ping Request
533…  120059.3066…  3.69.78.236     192.168.8.196   MQTT      68  Ping Response
533…  120062.4299…  192.168.8.196   3.69.78.236     MQTT     298  Publish Message [Payloaddata]
533…  120062.5699…  52.28.80.160    192.168.8.196   MQTT     298  Publish Message [Payloaddata]
533…  120070.8528…  192.168.8.196   3.69.78.236     MQTT     298  Publish Message [Payloaddata]
533…  120070.9958…  52.28.80.160    192.168.8.196   MQTT     298  Publish Message [Payloaddata]
533…  120078.6987…  192.168.8.196   3.69.78.236     MQTT     298  Publish Message [Payloaddata]
533…  120078.8518…  52.28.80.160    192.168.8.196   MQTT     298  Publish Message [Payloaddata]
533…  120083.4903…  192.168.8.196   3.69.78.236     MQTT      68  Ping Request
533…  120083.6263…  3.69.78.236     192.168.8.196   MQTT      68  Ping Response
533…  120086.6182…  192.168.8.196   3.69.78.236     MQTT     298  Publish Message [Payloaddata]
533…  120086.7656…  52.28.80.160    192.168.8.196   MQTT     298  Publish Message [Payloaddata]
533…  120090.4633…  192.168.8.196   52.28.80.160    MQTT      68  Ping Request
```

```
    Epoch Arrival Time: 1733960735.408338000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.022000000 seconds]
    [Time delta from previous displayed frame: 7.702922000 seconds]
    [Time since reference or first frame: 120078.698742000 seconds]
    Frame Number: 5335593
    Frame Length: 298 bytes (2384 bits)
    Capture Length: 298 bytes (2384 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:mqtt]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
> Ethernet II, Src: Apple_3d:a9:e5 (3c:06:30:3d:a9:e5), Dst: SOYEATechnol_c3:05:b1 (cc:e8:
> Internet Protocol Version 4, Src: 192.168.8.196, Dst: 3.69.78.236
> Transmission Control Protocol, Src Port: 50901, Dst Port: 1883, Seq: 1225, Ack: 33, Len:
v MQ Telemetry Transport Protocol, Publish Message
  > Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (F
    Msg Len: 229
    Topic Length: 11
    Topic: Payloaddata
    Message […]: 565556725955677952306c6b4c314977536c6c4e52324a3155573975566d35516454466c5
```

```
0000  cc e8 ac c3 05 b1 3c 06  30 3d a9 e5 08 00 45 00   ······<· 0=····E·
0010  01 1c 00 00 40 00 40 06  1e 3f c0 a8 08 c4 03 45   ····@·@· ·?·····E
0020  4e ec c6 d5 07 5b bd b0  58 db 7b 23 13 5a 80 18   N····[·· X·{#·Z··
0030  08 04 b4 47 00 00 01 01  08 0a 15 55 e7 6f be e8   ···G···· ···U·o··
0040  b3 dc 30 e5 01 00 0b 50  61 79 6c 6f 61 64 64 61   ··0····P ayloadda
0050  74 61 56 55 56 72 59 55  67 79 52 30 6c 6b 4c 31   taVUVrYU gyR0lkL1
0060  49 77 53 6c 6c 4e 52 32  4a 31 55 57 39 75 56 6d   IwSllNR2 J1UW9uVm
0070  35 51 64 54 46 6c 59 56  68 53 65 48 6f 35 61 48   5QdTFlYV hSeHo5aH
0080  49 33 52 6d 56 32 64 6d  64 46 4f 56 70 53 4b 33   I3RmV2dm dFOVpSK3
0090  6c 70 61 46 52 51 52 53  74 73 64 6c 68 48 53 7a   lpaFRQRS tsdlhHSz
00a0  51 33 56 54 64 36 4f 53  39 4f 4b 30 39 33 54 6d   Q3VTd6OS 9OK093Tm
00b0  4e 6a 54 6c 56 56 53 55  49 76 56 33 4e 59 62 30   NjTlVVSU IvV3NYb0
00c0  55 30 4d 32 6f 30 5a 54  52 45 62 30 52 79 4e 30   U0M2o0ZT REb0RyN0
00d0  6c 6b 56 7a 46 53 5a 6e  46 78 52 48 56 5a 65 6b   lkVzFSZn FxRHVZek
00e0  4e 47 5a 6a 52 69 55 31  42 68 63 30 6c 6a 53 47   NGZjRiU1 Bhc0ljSG
00f0  4e 30 61 31 56 31 5a 6e  67 77 52 6e 56 53 59 6e   N0a1V1Zn gwRnVSYn
0100  42 56 51 7a 49 33 55 6e  4e 51 56 79 74 33 62 57   BVQzI3Un NQVyt3bW
0110  56 55 4f 54 56 73 59 79  39 49 53 55 51 7a 52 30   VUOTVsYy 9ISUQzR0
0120  70 53 64 6b 35 4e 51 77  3d 3d                     pSdk5NQw ==
```

Figure 11: AES128 Encryption Payload data

6.3 Analysing Privacy consideration without Decryption visualise in Node red:

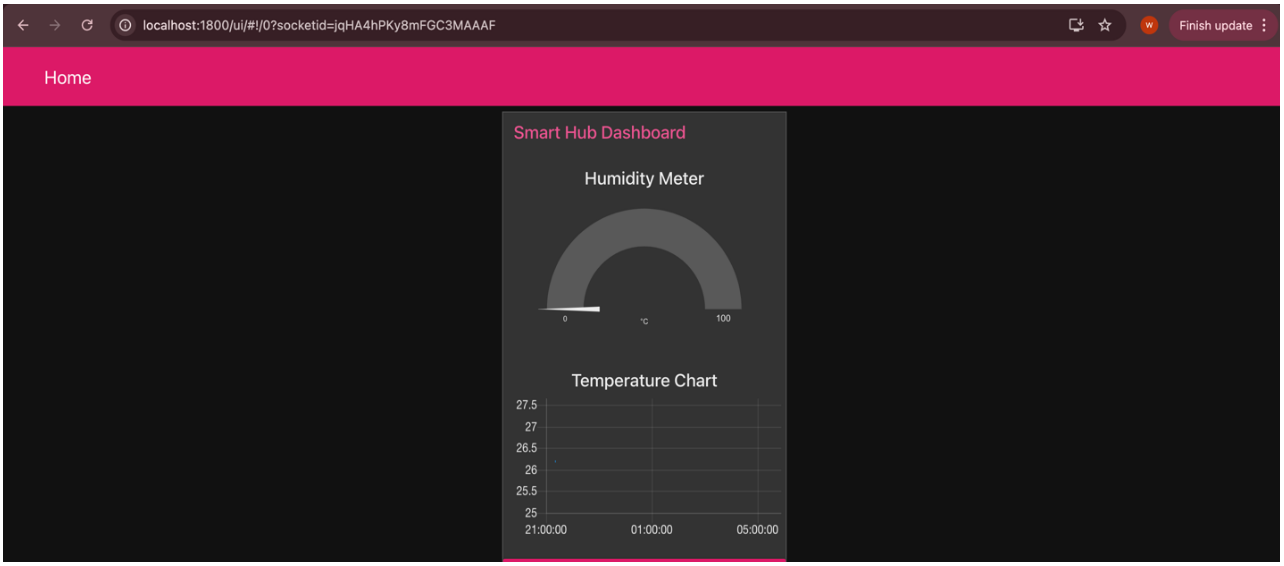
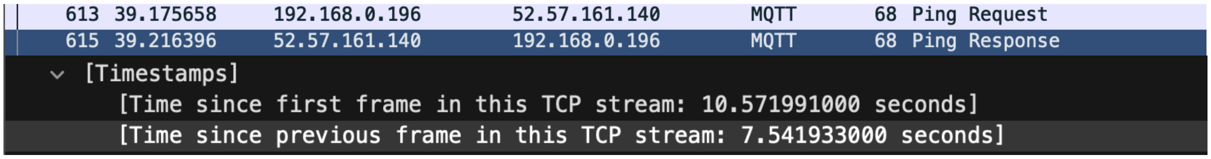


Figure 12: Node-red without decryption visualization

6.4 Analysing Latency:

Latency Testing:
Testing revealed that the introduction of the encryption and obfuscation processes did not result in more than 70ms. I used Wireshark to measure times of the transmission of encrypted payload this was verified.



```
  613 39.175658     192.168.0.196        52.57.161.140       MQTT       68 Ping Request
  615 39.216396     52.57.161.140        192.168.0.196       MQTT       68 Ping Response
    ∨ [Timestamps]
         [Time since first frame in this TCP stream: 10.571991000 seconds]
         [Time since previous frame in this TCP stream: 7.541933000 seconds]
```

Figure13: Wireshark TCP

Real-Time Performance:
The real time responsiveness was achieved for updating sensor data and controlling actuators for all the simulated operations. As a result, AES-128 was chosen to ensure low latency while sufficiently protecting security.

Optimized Encoding:
To make them compatible with MQTT protocols and minimizing the additional processing delays, the strings were base64 encoded.

6.5 Discussion:

This research integrates AES-128 encryption, and honeywords to develop a dual layered security measure against flaws in MQTT based smart home systems. The key findings of the research conclude that AES-128 encryption guarantees confidentiality and data integrity during transmission, which greatly reduces the likelihood of eavesdropping and man-in-the-middle attacks, as reported by (Al-Ani at al., 2023). In addition, honeywords make a system more secure by generating decoy data and fooling attackers to keep them away from offensive brute force attacks on sensitive information. An important outcome is that the system can offer secure and lightweight communication for IoT resource constrained devices. The research also verifies (Cristian et al., 2019) on the flexibility and efficiency of MQTT and it is ideal for real time smart home automation. Through the combination of encryption and obfuscation, the proposed system shows far greater security while not impacting the operational performance of smart home environments. This work also shows that our honeywords scheme with AES 128 can significantly lower the attacker's probability of success as suggested in (Ayari et al., 2024) to use of cryptographic techniques specific to IoT ecosystems if employed in conjunction. Additionally, the research focuses on the need to achieve security and effective computation simultaneously in smart home system.

7. Conclusion and Future work:

This research successfully addresses the security challenges of smart home IoT systems through a dual-layered defence mechanism combining AES-128 encryption and honeywords. The results shows an enhanced data confidentiality and obfuscation, validating the approaches efficacy in mitigating modern cyber threats. The goals of this research were to resolve the critical security challenges present in a smart home IoT system using a dual layer defence mechanism involving AES-128 encryption and honeyword generation. The overarching objective was to achieve data transmission security, data integrity, and the enhancement of IoT cyber resilience against attack, particularly in MQTT based communication. With this research, these objectives have been successfully achieved through a practical implementation through a virtual hardware simulation environment within Wokwi. The results showed that data confidentiality was effectively sheltered by AES-128 encryption, and honeyword generation added obfuscation to confuse attackers, overall improving security. The correct implementation of encryption protocols was confirmed when the encrypted payload values were analysed in Wireshark. Additionally, built a Node-RED workflow that got us far enough to visualize encrypted data without decrypting it, showing us how to work on encrypted data without decryption. Further, this virtual simulation approach was shown to be a cost effective and accessible alternative to physical hardware, thereby offering a scalable solution for researchers, developers, and engineers in this and similar domains.

Future Works:

While this research laid a strong foundation, several opportunities for future exploration exist:

- **Expanding IoT Ecosystem:** Additional future projects can further improve the system by integrating more IoT sensors and actuators to mimic a live smart home. For example, it includes devices such as smart locks, cameras, energy meters, providing a more complete image for the security framework.
- **Advanced Honeyword Algorithms:** While the current honeyword generation algorithm is effective, it can be further improved to foster the attack types that are more sophisticated. Future work could also consider adaptive honeyword techniques that use machine learning to build decoys corresponding to an attacker's behaviour.
- **Machine Learning-Driven Decoy Generation:**
  Machine learning algorithms are corporate to dynamically generate honeywords based on attack behavior that has been observed. For instance, if the attackers knew for example that they are looking for a certain type of data, the algorithm will learn to create decoy data that would follow that pattern. Generate decoys to as much as possible in accordance with realistic IoT sensor behavior.
- **Decryption and Visualization in Node-RED:** The limitation of the current study was that there was no decryption or visualization of payload values in real-time in Node-RED. Future work could be to securely design a decryption process for Node-RED dashboards, while also remaining usable.
- **Scalability Analysis:** The applicability of the virtual simulation approach for real world deployments would be investigated with regard to its scalability on larger, more complex smart home systems. It may be stress testing the system at high data throughput, and a high rate of network activity.

This thesis provides a foundation for building secure and resilient IoT systems in smart homes. In light of this, proposing future works which will tackle current limitations and create better, smarter, more secure, scalable solutions meeting the growing needs of IoT security in a world that is gradually connected.

8. References:

Al-Ani, A., Shen, W. K., Al-Ani, A. K., Laghari, S. U. A., & Elejla, O. E. (2023). Evaluating Security of MQTT Protocol in Internet of Things. https://doi.org/10.1109/ccece58730.2023.10288857

Alwarafy, A., Al-Thelaya, K., Abdallah, M., Schneider, J., & Hamdi, M. (2020). A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things. In IEEE Internet of Things Journal (Vol. 8, Issue 6, p. 4004). Institute of Electrical and Electronics Engineers.
https://doi.org/10.1109/jiot.2020.3015432

Wang, J., Mandalari, A. M., & Straw, I. (2023). Who Let the Smart Toaster Hack the House? An Investigation into the Security Vulnerabilities of Consumer IoT Devices. In arXiv (Cornell University). Cornell University.
https://doi.org/10.48550/arXiv.2306.

Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., & Feamster, N. (2017). Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. In arXiv (Cornell University). Cornell University.
https://doi.org/10.48550/arxiv.1708.05044

Sherif, A. (2023). Smart home device ownership US 2022. https://www.statista.com/statistics/1124290/smart-home-device-ownership-us/

Tiwari, A., & Waoo, A. A. (2023). IoT based Smart Home Cyber-Attack Detection and Defense. Toutsop, O., Harvey, P., & Kornegay, K. (2020). Monitoring and Detection Time Optimization of Man in the Middle Attacks using Machine Learning. https://doi.org/10.1109/aipr50011.2020.9425304

U.S.: smart home number of users 2019-2028. (2023). https://www.statista.com/forecasts/887611/number-of-smart-homes-in-the-smart-home-market-in-the-united-states

Vardakis, G. E., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of Smart-Home Security Using the Internet of Things. In Electronics (Vol. 13, Issue 16, p. 3343). Multidisciplinary Digital Publishing Institute.
https://doi.org/10.3390/electronics13163343

Ayari, M., Gharbi, A., El Touati, Y., Klai, Z., Kefi, K., Yahya, A. E., & El Kamel, A. (2024). Exploring Current Encryption Technologies in Iot and Their Impact on Data Security. https://www.ijcnis.org/index.php/ijcnis/article/view/6906

Cristian, A. C.-, Tudor, G., Arhip-Calin, M., & Zamfirescu, A. (2019). Smart home automation with MQTT. https://ieeexplore.ieee.org/abstract/document/8893617/

Guhr, N., Werth, O., Blacha, P. P. H., & Breitner, M. H. (2020). Privacy concerns in the smart home context (Vol. 2, Issue 2). Springer Nature. https://doi.org/10.1007/s42452-020-2025-8

Harkai, A. (2024). Managing cyber-security risks associated with IoT devices for conducting financial transactions within the smart home ecosystem (Vol. 242, p. 200). Elsevier BV. https://www.sciencedirect.com/science/article/pii/S1877050924019793

Uppuluri, S., & Gondi, L. (2022). Secure user authentication and key agreement scheme for IoT device access control based smart home communications (Vol. 29, Issue 3, p. 1333). Springer Science+Business Media. https://link.springer.com/article/10.1007/s11276-022-03197-1

Yalçınkaya, F., AYDİLEK, H., Erten, M. Y., & İnanç, N. (2020). IoT based Smart Home Testbed using MQTT Communication Protocol (p. 317). https://dergipark.org.tr/en/pub/umagd/issue/49089/681357

Karmous, N., Hizem, M., Ben Dhiab, Y., Ould-Elhassen Aoueileyine, M., Bouallegue, R., & Youssef, N. (2024). Hybrid Cryptographic End-to-End Encryption Method for Protecting IoT Devices Against MitM Attacks. Radioengineering, 33(4), 583–592. https://doi.org/10.13164/RE.2024.0583

Liu, Z., Liang, T., Lyu, J., & Lang, D. (2024). A security-enhanced scheme for MQTT protocol based on domestic cryptographic algorithm. Computer Communications, 221, 1–9. https://doi.org/10.1016/J.COMCOM.2024.04.013