ITER | SOA

Institute of Technical Education and Research

PROJECT REPORT

on

Developing A Secure Network Protocol For IoT devices in the Smart Home Systems

Submitted By:

Name	Registration No
Kingshu Rakshit	2141018044
Dipyaman Shau	2141019137
Swayam Pratik Das	2141004019
Debashish Maharana	2141013030

Executive Summary

This case study addresses the development of a secure network protocol developed for IoT devices within smart homes.

The increasing adoption of Internet of Things (IoT) devices in smart home systems has introduced new security risks and challenges. As the number of connected devices grows, so does the attack surface, making it essential to develop a secure network protocol to protect these devices and their users.

The problem arises from the increasing vulnerability of smart home networks to cyber threats due to insufficiently secure protocols.

Implementation requires a phased approach with initial testing on a small scale, followed by broader deployment and continuous monitoring

Introduction

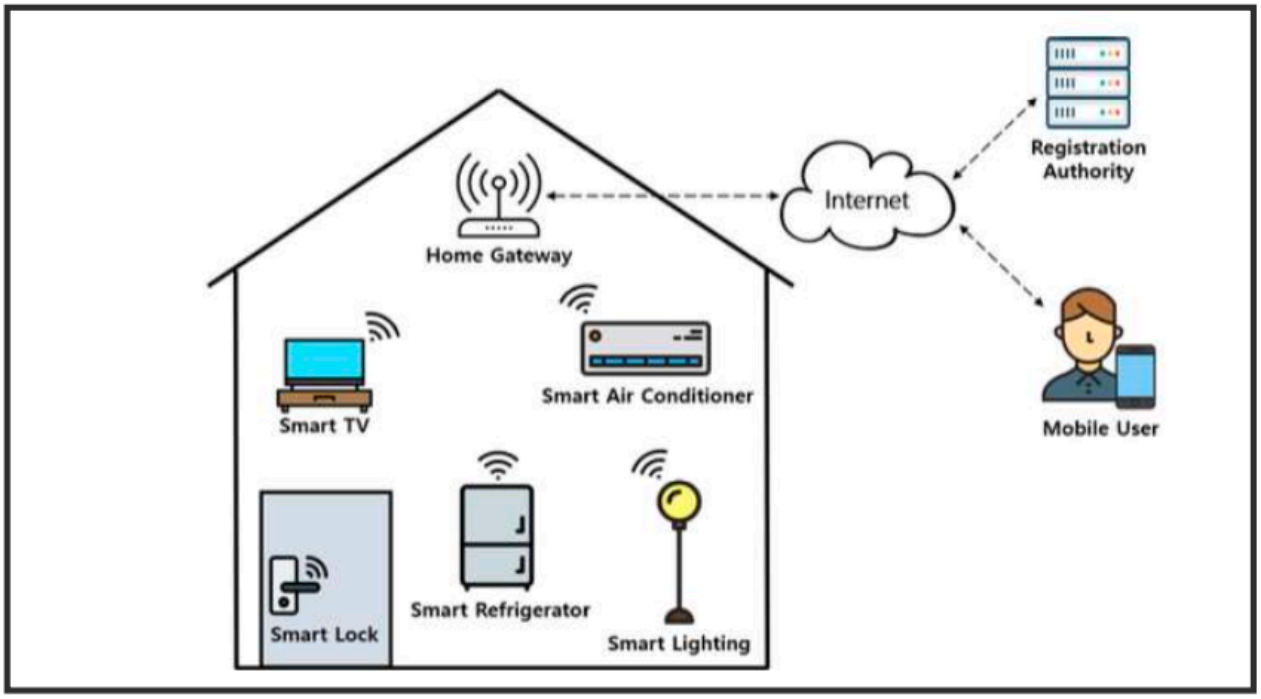
A typical smart home architecture consists of four entities:

1.Registration authority (RA) : RA is a trusted entity that mainly authorizes the gateway as the home registration center.

2.Gateway : Gateway is a semi-trusted entity that helps users to communicate with smart home devices and is responsible for registration.

3.Smart devices (IoT devices) : Smart device refers to all kinds of smart home appliances in the family, such as smart refrigerators, smart air conditioners, etc., where they are semi-trusted entities, and are connected to the gateway by wireless networks to provide users with various services.

4.Users : Only family members can register with the gateway to become legal users.



(**Fig 1.** Smart Home Architecture)

In this architecture, **users** need to connect the **home devices** via the **gateway**, and then operate the home devices through the **smart home APP or voice assistant, such as adjusting the indoor temperature, switching lights, adjusting curtains, playing music, etc.**

Although the smart home has changed people's lives, **it faces many security threats and challenges.** For example, since smart home devices are connected to the Internet, malicious attackers can access users' private information by intercepting transmitted messages via open channels. Therefore, ensuring a secure smart-home IoT access control scheme is very important.

Analysis

Current Protocols and Vulnerabilities:

- Design prioritizing convenience over security: Many IoT devices are designed with ease of use in mind, rather than security, resulting in devices with default passwords, open ports, and other vulnerabilities.
- Outdated and legacy operating systems: The use of outdated and legacy operating systems on IoT devices makes them more vulnerable to attacks.
- Limited resources and capabilities of IoT devices: The limited processing power, memory, and storage capacity of many IoT devices make it challenging to implement robust security measures.
- Lack of awareness and education among consumers: Consumers are often unaware of the security risks associated with IoT devices and do not follow proper security practices, exacerbating the problem.
- Lack of standardized security protocols and regulations: IoT device manufacturers are not held to a common set of security standards, leading to a proliferation of devices with inadequate security features.

Key Findings:

- Standardization Gap: The absence of a common security standard leads to varied and often inadequate security measures.
- Design Flaws: Convenience-oriented design choices create security loopholes.
- System Vulnerabilities: Outdated systems and limited resources impede the deployment of effective security solutions.
- Consumer Practices: Poor consumer practices and lack of awareness contribute to the vulnerability of smart home networks.

Solution

The proposed secure network protocol for smart homes involves four key entities: **Mobile User (MU)**, **Smart Device (SD)**, **Home Gateway (HGW)**, and **Registration Authority (RA)**. Each plays a specific role in ensuring secure interactions within the smart home environment. Here's a detailed breakdown of the proposed system and how it addresses the identified security challenges:

System Components:

1. Registration Authority (RA):

- **Role:** Acts as a trusted entity responsible for the initial setup of the system and the registration of all components (MU, SD, HGW).
- **Function:**
  - Initializes the system and stores information for MU and SD.
  - Maintains a database of all authentication information needed by HGW to verify MU and SD.
  - Ensures that only authorized entities are allowed access and services.

2. Home Gateway (HGW):

- **Role:** Serves as the central communication hub between the smart devices and the mobile user.
- **Function:**
  - Facilitates mutual authentication and session key agreement between MU and SD.
  - Uses the authentication information stored by RA to verify and authorize devices and users.
  - Manages secure communication channels and enforces security policies within the smart home network.

3. Mobile User (MU):

- **Role:** The user's mobile device interacting with the smart home network.
- **Function:**
  - Registers with RA to gain access to smart home services.
  - Engages in mutual authentication with SD via HGW.
  - Uses session keys for secure communication with smart devices.

4. Smart Device (SD):

- **Role:** IoT devices within the smart home that provide various services (e.g., smart thermostats, security cameras).
- **Function:**
  - Registers with RA to participate in the smart home network.
  - Performs mutual authentication with MU via HGW.
  - Uses session keys for secure operation and communication.

Detailed Process Flow

1. Registration:

- **MU Registration:**
  - The MU initiates registration with RA to gain access to the smart home services.
  - RA stores the MU's credentials and necessary information in the mobile device of the MU.
- **SD and HGW Registration:**
  - SD and HGW also register with RA to be part of the smart home network.
  - RA stores relevant information in the memory of SD and the HGW's database for authentication purposes.

2. Authentication and Key Agreement:

- **Mutual Authentication:**
  - MU and SD perform mutual authentication with each other through HGW.
  - HGW uses the stored credentials and information from RA to authenticate both MU and SD.
- **Session Key Agreement:**
  - Once authenticated, MU and SD agree on a session key (Flag) with the help of HGW.
  - This session key is used to encrypt and secure communications between MU and SD.

3. Secure Smart Home Services:

- **Communication:**
  - With the session key in place, MU and SD can securely exchange data and commands.
  - The HGW manages and enforces security policies to maintain a secure smart home environment.

Justification:

1. Centralized Control and Trust: RA and HGW are trusted entities that centralize authentication and key management, ensuring a secure setup and ongoing operation.

2. Secure Registration and Authentication: By registering MU, SD, and HGW with RA and using mutual authentication, the system ensures that only authorized devices and users are granted access.

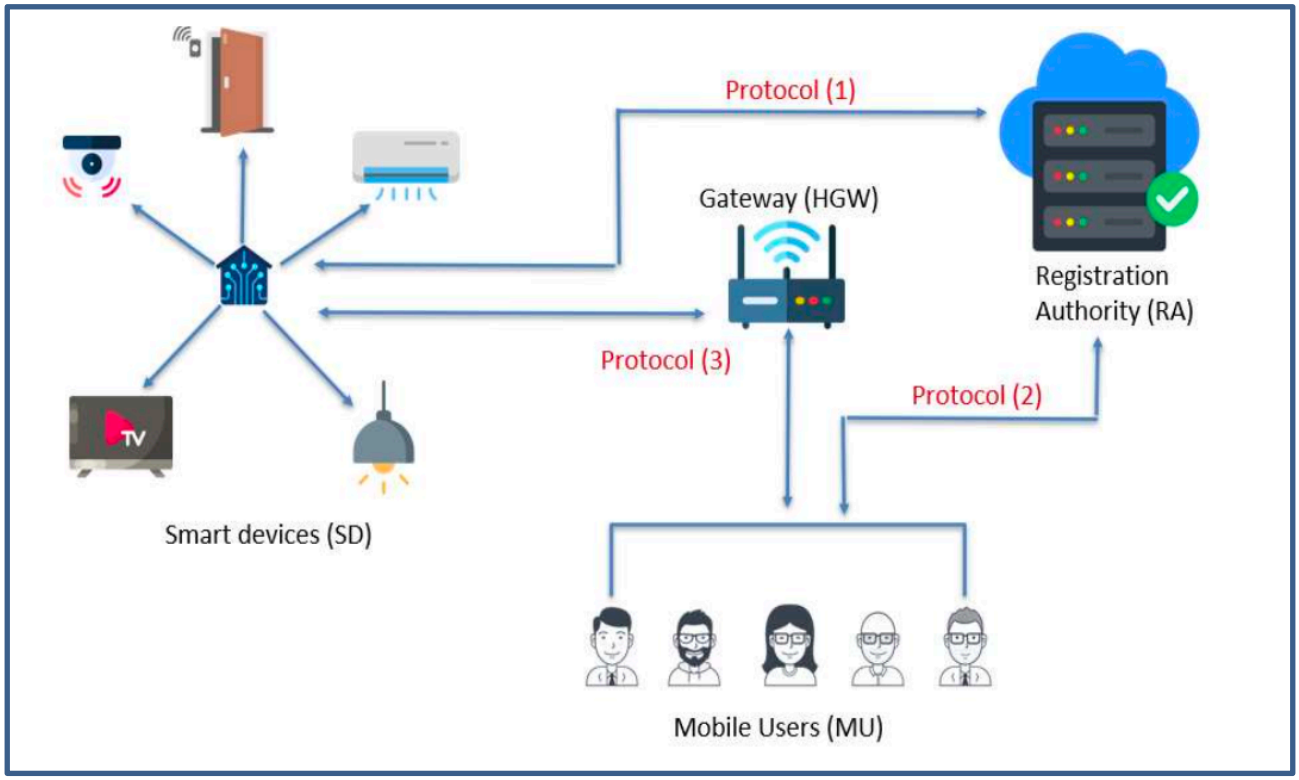
3. Session Key Utilization: The use of session keys for communication ensures that all data exchanged between MU and SD is encrypted, protecting it from eavesdropping and tampering.

4. Scalability and Flexibility: The system allows for the addition of new devices and users by simply registering them with RA, making it scalable and adaptable to evolving smart home environments.

Recommendations

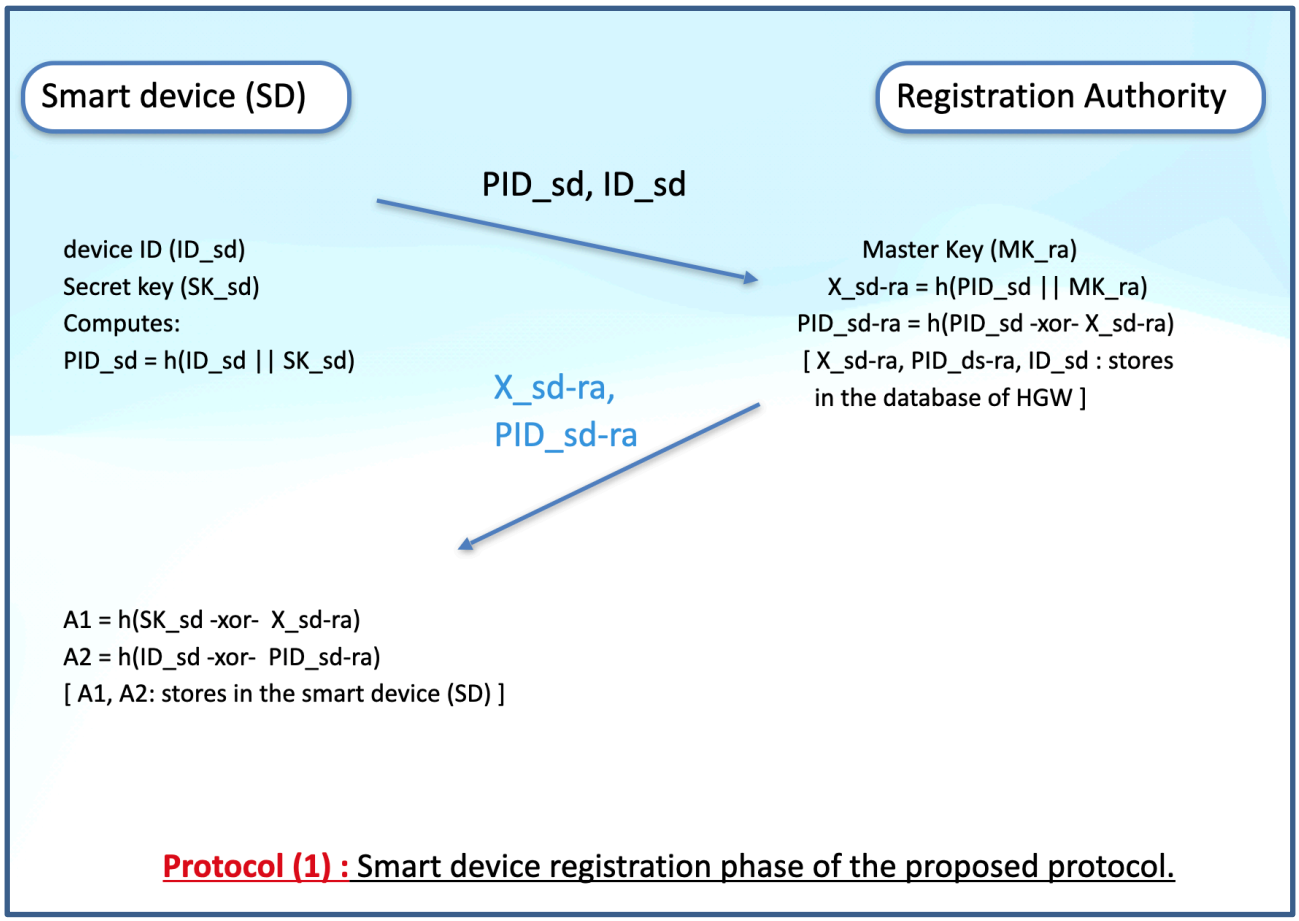
Implement the Proposed System: Adopt the outlined protocol for a secure smart home network, integrating RA, HGW, MU, and SD as described.

Enhance Security Measures: Regularly update the system to address new security threats and ensure that all components follow the latest security best practices.



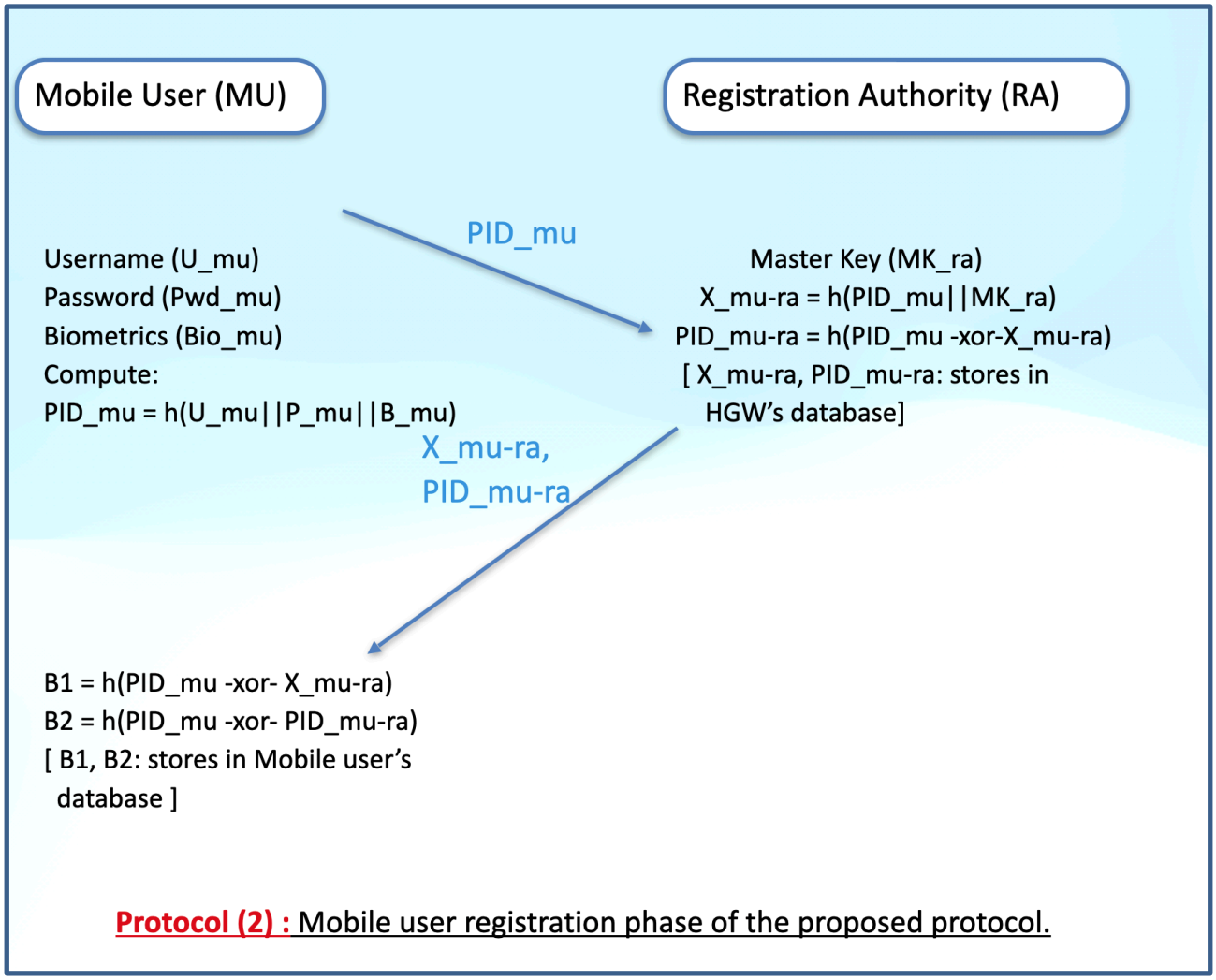
(**Fig 2.** Network Model for Smart Home)

Proposed Protocols



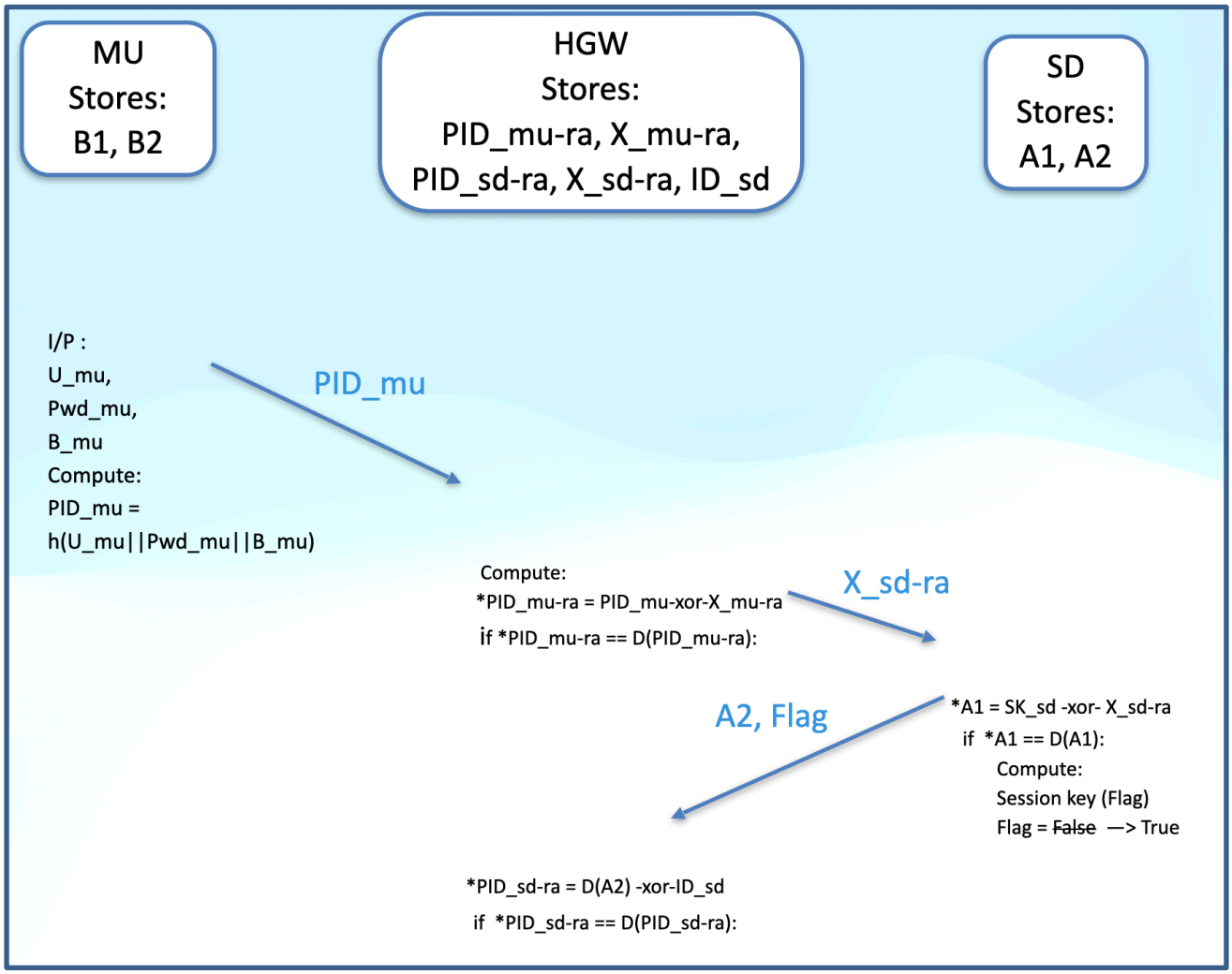
Protocol (1) : Smart device registration phase of the proposed protocol.

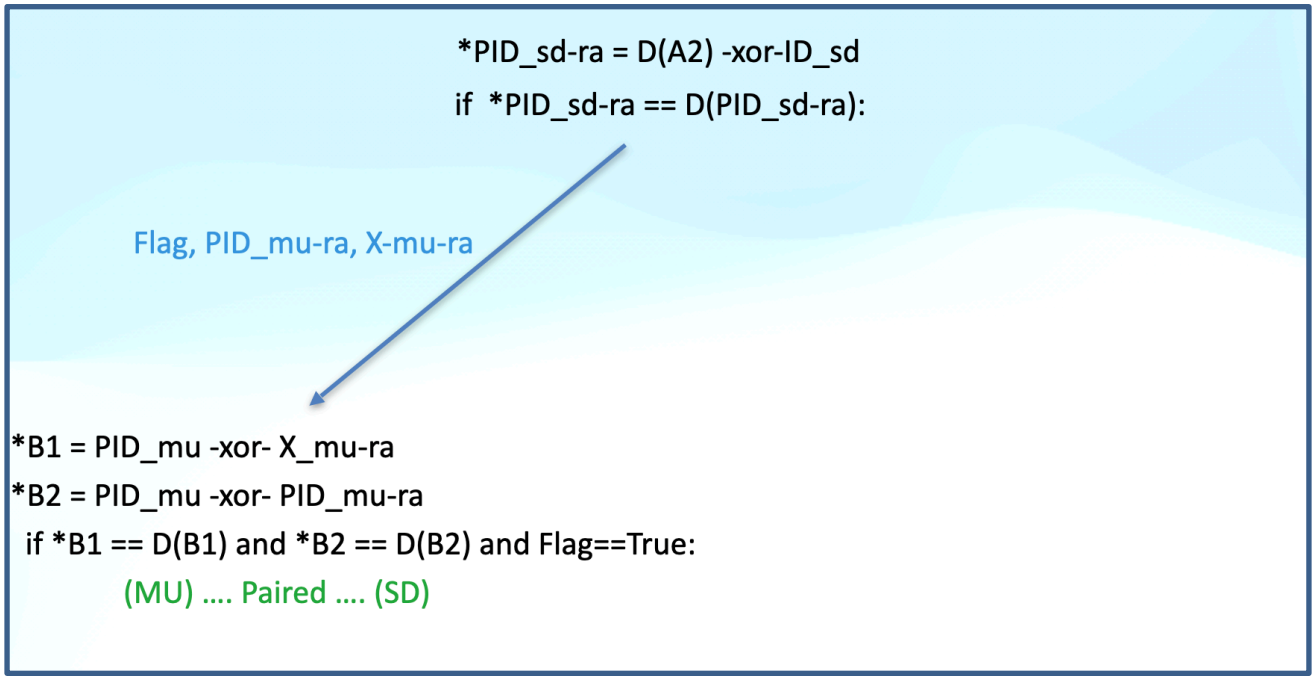
(**Fig 3.**)



Protocol (2) : Mobile user registration phase of the proposed protocol.

(**Fig 4.**)

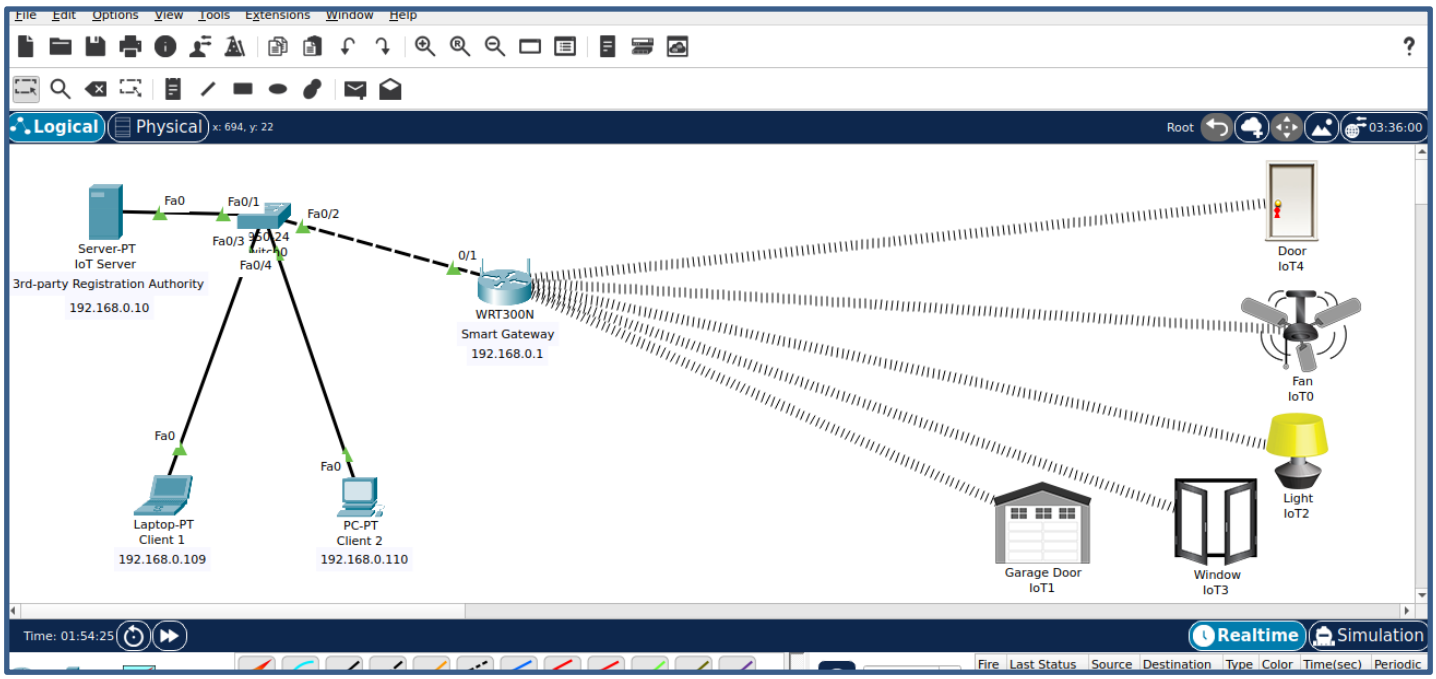




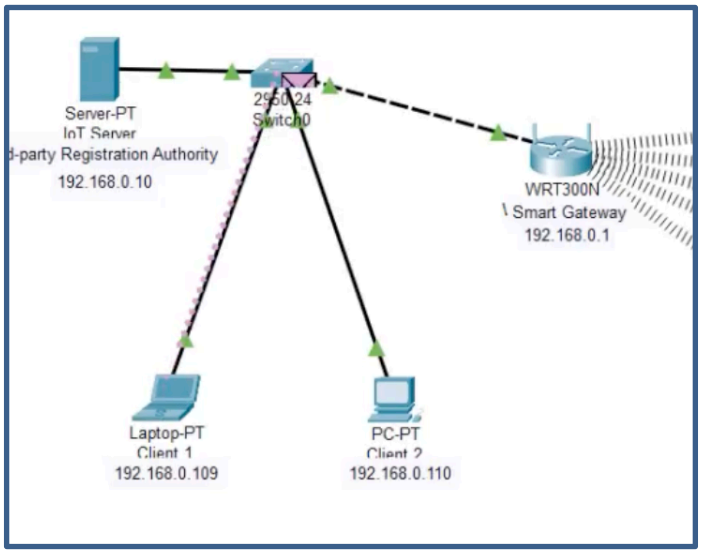
Protocol (3) : Authentication and key agreement phase.

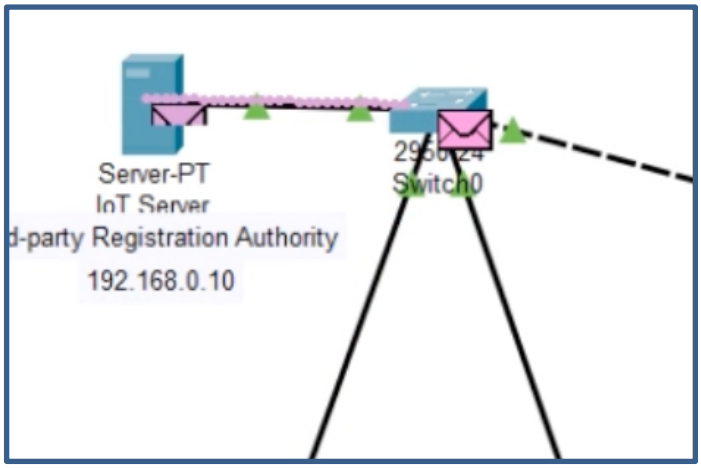
(**Fig 5.**)

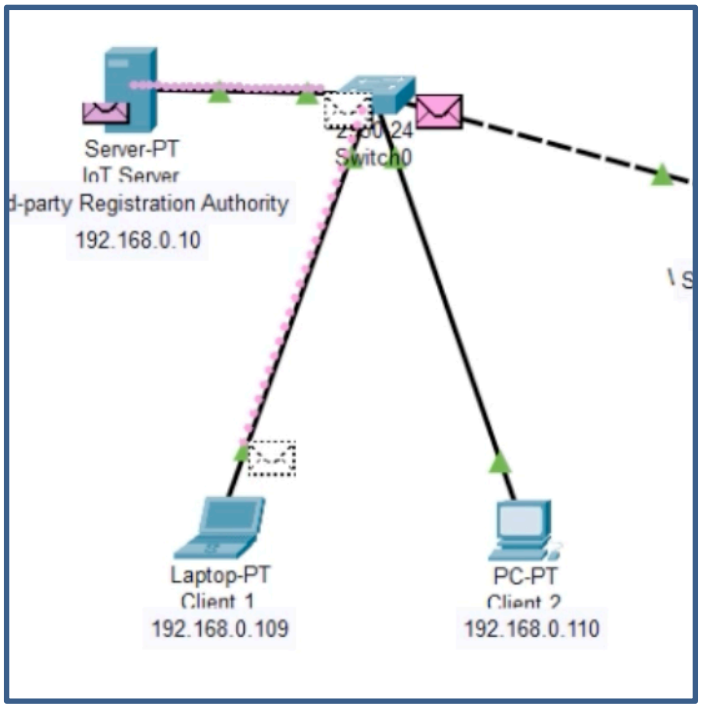
Implementation



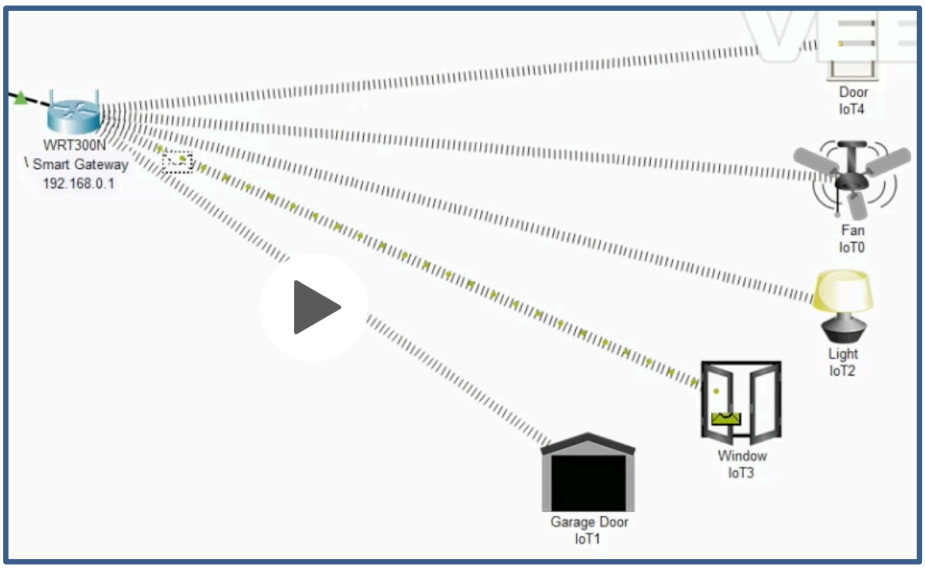
(**Fig 6.** Implementing Network Model using CISCO Packet Tracer)

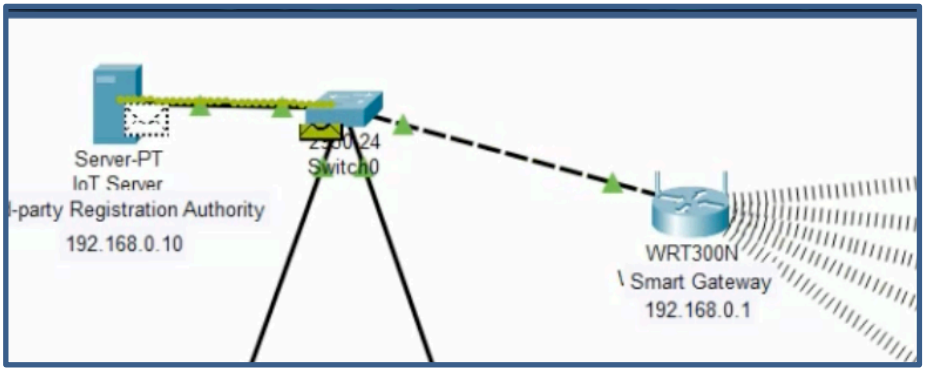


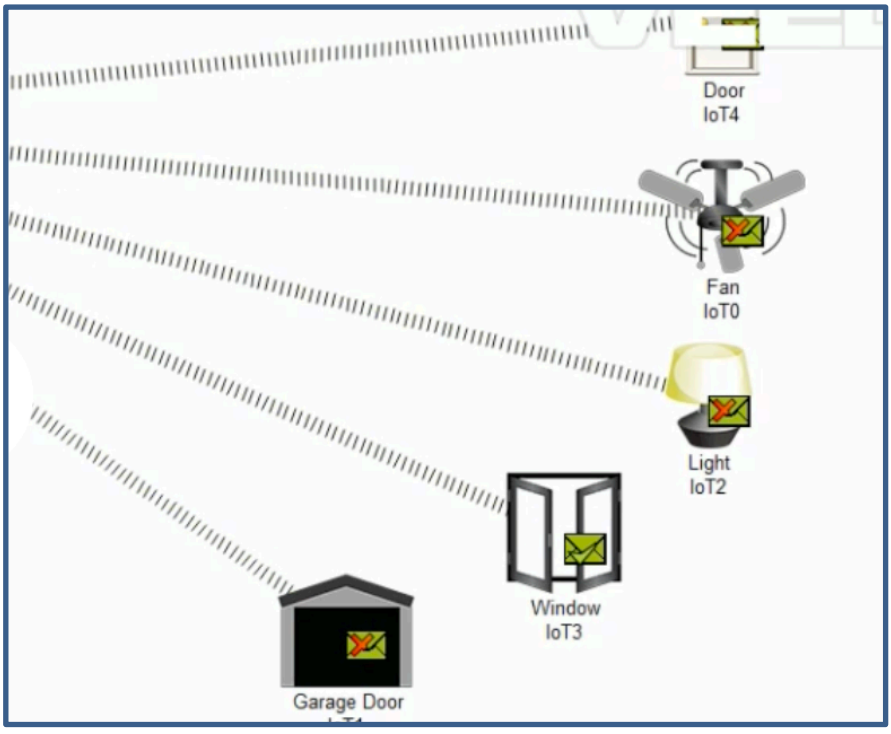




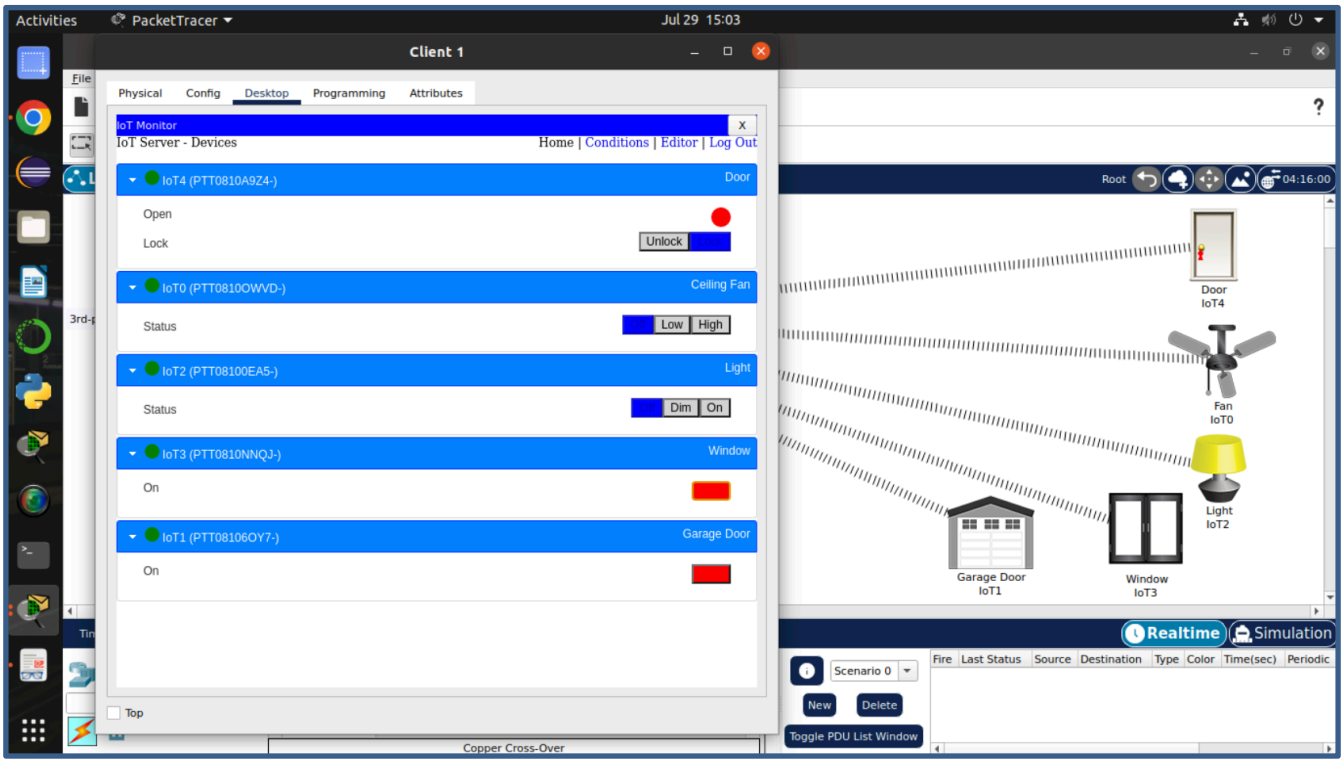
(**Fig 7.** Registration between (MU) and (RA))







(**Fig 8.** Registration between (SD) and (RA))



(**Fig 9.** After (MU) and (SD) are paired , User gets to managed all the IoT devices connected to his/her Smart Home using the Control Panel.)

Conclusion

- The integration of IoT devices in smart homes has undoubtedly brought about numerous conveniences and improvements to our daily lives.
- However, it has also introduced a plethora of security risks that cannot be ignored. The vulnerabilities of IoT devices, combined with the interconnected nature of smart home systems, create a perfect storm of potential security breaches.
- It is imperative that manufacturers, policymakers, and consumers alike take proactive steps to address these risks and develop robust security protocols to protect the integrity of home networks and the safety of their occupants.
- By doing so, we can ensure that the benefits of IoT technology are realized without compromising our privacy, security, and well-being. The future of smart homes depends on it.

References

Towards a Secure Smart-Home IoT Access Control Scheme Based on Home Registration Approach.

Authors: Tsu-Yang Wu, Qian Meng, Yeh-Cheng Chen, Saru Kumari and Chien-Ming Chen
Publication: MDPI (Academic Open Access Publishing)
URL: https://www.mdpi.com/2227-7390/11/9/2123

Smart Assistive Architecture for the Integration of IoT Devices, Robotic Systems, and Multimodal Interfaces in Healthcare Environments

Authors: Alberto Brunete, Ernesto Gambao, Miguel Hernando and Raquel Cedazo
Publication: MDPI (Academic Open Access Publishing)
URL: https://www.mdpi.com/1424-8220/21/6/2212