GMR Institute of Technology
An Autonomous Institute Affiliated to JNTU-GV | GMRIT Training Tomorrow's Engineers Today

HOME SECURITY SYSTEM WITH INTRUDER ALERT

A Mini project report submitted in partial fulfilment of the requirement

for the award of degree of

BACHELOR OF TECHNOLOGY

In

ELECTRONICS AND COMMUNICATION ENGINEERING

Submitted by

G. YASASWI
(22341A0463)

D. PALLAVI
(22341A0447)

VITTAL PRAVEEN
(22341A0438)

D. TEJASWINI
(22341A0454)

D. CHANDU
(22341A0450)

D. PRAVEEN
(22341A0451)

Under the esteemed guidance of

Sri. P. Kalyan Chakravarthi

Assistant professor, Dept. of ECE

GMR Institute of Technology

An Autonomous Institute Affiliated to JNTU-GV, Vizianagaram

(Accredited by NBA, NAAC with 'A' Grade & ISO 9001:2015 Certified Institution)

GMR Nagar, Rajam – 532 127,
Andhra Pradesh, India
April-2025

GMR Institute of Technology
An Autonomous Institute Affiliated to JNTU-GV | GMRIT Training Tomorrow's Engineers Today

Department of Electronics and Communication Engineering

CERTIFICATE

This is to certify that the mini project entitled **HOME SECURITY SYSTEM WITH INTRUDER ALERT** submitted by **G. Yasaswi (22341A0463)**, **Ch. Vital Praveen (22341A0438), D. Pallavi (22341A0447), D. Tejaswini (22341A0454), D. Praveen (22341A0451), D. Chandu (22341A0450)** has been carried out in partial fulfilment of the requirement for the award of degree of **Bachelor of Technology** in **Electronics and Communication** of **GMRIT, Rajam** affiliated to **JNTU-GV, Vizianagaram** is a record of Bonafide work carried out by them under my guidance & supervision. The results embodied in this report have not been submitted to any other University or Institute for the award of any degree.

Signature of Supervisor	**Signature of HOD**
Sri. P. Kalyan Chakravarthi	**Dr. V. Jagan Naveen**
Assistant Professor	Professor & Head
Department of ECE	Department of ECE
GMRIT, Rajam.	GMRIT, Rajam.

The mini project report is submitted for the viva-voce examination held on ……………….

Signature of Internal Examiner   Signature of External Examiner

ACKNOWLEDGEMENT

It gives us an immense pleasure to express deep sense of gratitude to my guide,
Sri. P. Kalyan Chakravarthi, Assistant Professor, Department of Electronics and Communication Engineering of wholehearted and invaluable guidance throughout the mini project work. Without his sustained and sincere effort, this project work would not have taken this shape. He encouraged and helped us to overcome various difficulties that we have faced at various stages of our mini project work.

We would like to sincerely thank our Head of the Department, **Dr. V. Jagan Naveen**, for providing all the necessary facilities that led to the successful completion of our project work.

We would like to sincerely thank our Associate Dean Academics, **Dr. M. V. Nageswara Rao**, for extending his support with all the necessary facilities that led to the successful completion of our project work.

We would like to take this opportunity to thank our beloved Principal, **Dr. C. L. V. R. S. V Prasad**, for providing a great support to us in completing our mini project and for giving us the opportunity of doing the project work.

We would like to take this opportunity to thank our beloved Director Education, **Dr. J. Girish**, for providing all the necessary facilities and a great support to us in completing the mini project work.

We would like to thank all the faculty members and the non-teaching staff of the Department of Electronics and Communication Engineering for their direct or indirect support for helping us in completion of this mini project work.

Finally, we would like to thank all of our friends and family members for their continuous help and encouragement.

G. Yasaswi	**22341A0463**
Ch. Vital Praveen	**22341A0438**
D. Pallavi	**22341A0447**
D. Tejaswini	**22341A0454**
D. Praveen	**22341A0451**
D. Chandu	**22341A0450**

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IFTTT	**:** IF THIS THEN THAT
GSM	**:** GLOBAL SYSTEM FOR MOBILE COMMUNICATION
GPS	**:** GLOBAL POSITIONING SYSTEM
SMS	**:** SHORT MESSAGE SERVICE
GPRS	**:** GENERAL PACKET RADIO SERVICE
UART	**:** UNIVERSAL ASYNCHRONOUS RECEIVER TRANSMITTER
MFA	**:** MULTI FACTOR AUTHENTICATION
API	**:** APPLICATION PROGRAMMING INTERFACE

ABSTRACT

The "Home Security System with Intruder Alert" is a robust and intelligent solution designed to enhance the safety and security of residential spaces. This system integrates advanced sensors, surveillance cameras, and a centralized control unit to detect unauthorized access or suspicious activities. By leveraging motion detection, infrared sensors, and real-time video monitoring, the system ensures comprehensive coverage of the premises.

Upon detecting an intrusion, the system immediately triggers an alert mechanism, which includes sounding an alarm, notifying the homeowner via a mobile application, and sending live video feeds. Additionally, the system can be integrated with smart home devices and IoT platforms for enhanced automation and remote access.

This project aims to provide an affordable, user-friendly, and efficient security solution for homeowners. By incorporating modern technologies such as machine learning for anomaly detection and cloud connectivity for data storage, the system offers a proactive approach to home security. This ensures peace of mind and enhances the overall safety of individuals and their properties.

The increasing threat of home intrusions necessitates the development of intelligent security systems that provide real-time monitoring and alerts. With the increasing demand for smart home security solutions, the integration of the Internet of Things (IoT) and automation technologies has become essential. An IoT-based smart home security system that utilizes the IFTTT (If This Then That) alert system to provide real-time intrusion detection and automated responses.

Keywords: IoT-based security, Smart home security, Intruder detection, Arduino platform, IFTTT alert system, Home automation, Real-time monitoring, Motion sensors, Wireless security systems

CHAPTER 1
INTRODUCTION

In today's interconnected world, the integration of Internet of Things (IoT) technology with home security is transforming how we protect our homes. Traditional systems like alarms and cameras have evolved into smarter solutions, enabling remote monitoring and control. IoT devices, from smart door locks to motion detectors, make security more efficient and accessible. However, this connectivity also introduces new vulnerabilities, making cybersecurity essential. A modern Home Security System with Intruder Alerts, powered by IoT, enhances protection through real-time monitoring, automatic alerts, and remote control via smartphones. By combining sensors, cameras, and advanced algorithms with machine learning, these systems reduce false alarms and improve responsiveness. However, robust cybersecurity measures are crucial to safeguard against potential threats, ensuring the system remains secure from hackers and disruptions.

With the rise of smart home technologies, ensuring the safety and security of residential spaces has become a growing concern. Traditional security systems often rely on manual surveillance or standalone alarm systems, which may not be sufficient to prevent unauthorized access effectively. The integration of the Internet of Things (IoT) has revolutionized home security by enabling real-time monitoring, automated alerts, and remote access control.

A smart home security system with an intruder alert mechanism, leveraging IoT technologies and automation to enhance security measures. The system incorporates an Arduino-based platform with various sensors, such as motion detectors and door/window contact sensors, to detect unauthorized entry. Upon detecting an intrusion, the system triggers an instant notification using the IFTTT (If This Then That) alert system, allowing homeowners to receive real-time updates on their smartphones.

In addition to developing a prototype, this study systematically reviews existing smart home security solutions, focusing on Arduino-based implementations and their effectiveness in preventing security breaches. By integrating IoT, cloud computing, and automated alert mechanisms, this research aims to contribute to the development of a cost-effective and efficient home security system. The proposed solution ensures better accessibility, real-time threat detection, and improved control over home security, making it a valuable addition to modern smart home ecosystems.

1.1 ADVANTAGES:

Real-Time Intruder Detection: The system instantly detects unauthorized access using motion sensors, door/window sensors, and other security components.

Instant Alerts via IFTTT: Homeowners receive immediate notifications on their smartphones via the IFTTT (If This Then That) alert system, ensuring timely response to potential threats.

Remote Monitoring and Control: The system allows users to monitor their home security remotely through IoT-based connectivity, enhancing convenience and safety.

Cost-Effective Solution: Compared to traditional security systems, this Arduino based solution is more affordable while maintaining high efficiency.

Easy Installation and Scalability: The system is simple to install and can be easily expanded by adding more sensors, cameras, or access control mechanisms**.**

1.2 NEED OF THE PROJECT:

In today’s world, ensuring the security of homes has become a top priority due to rising crime rates and increasing security threats. Traditional security methods, such as manual surveillance and conventional alarm systems, have limitations in terms of real-time monitoring and remote accessibility. Therefore, the integration of IoT-based smart home security systems has become essential to enhance home safety, reduce risks, and provide real-time alerts.

1.3 LM2596 STEPDOWN CONVERTOR:

The LM2596 is a DC-DC step-down (buck) voltage regulator that efficiently converts a higher DC voltage to a lower stable DC voltage. It is widely used in power supply circuits to regulate voltage levels for microcontrollers, sensors, and other electronic components.

1.3.1 Key Features of LM2596:

Input Voltage Range: 4V to 40V DC

Output Voltage: Adjustable (1.23V to 37V)

Maximum Output Current: 3A (with proper heat dissipation)

Efficiency: Up to 90%, making it power-efficient

Switching Frequency: 150 kHz, ensuring fast response and lower heat generation

Thermal Shutdown & Overcurrent Protection: Protects against overheating and excess current

Low Ripple Output: Provides stable voltage with minimal fluctuations

1.3.2 Working Principle:

The LM2596 works as a buck converter, meaning it reduces the input voltage to a desired lower output voltage while maintaining high efficiency. It operates by rapidly switching an internal transistor on and off, storing energy in an inductor and then releasing it in a controlled manner.

1.3.3 Applications:

- Powering Microcontrollers & Sensors (Arduino, ESP32, Raspberry Pi, etc.)
- Battery-Powered Devices (Regulating voltage from lithium-ion batteries)
- Solar Power Systems (Efficient DC voltage regulation
- Robotics & IoT Devices
- Embedded Systems & Industrial Electronics

1.3.4 Common Variants:

- **LM2596-ADJ** – Adjustable output voltage (1.23V to 37V)
- **LM2596-5.0** – Fixed 5V output
- **LM2596-3.3** – Fixed 3.3V output
- **LM2596-12** – Fixed 12V output

1.3.5 Pin diagram of LM2596 Step down convertor:

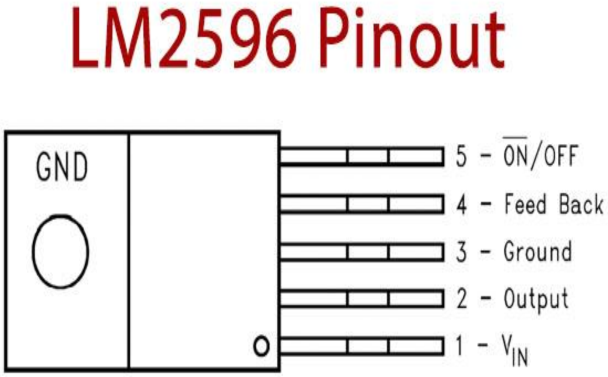


Fig 1: pin diagram of LM2596

1.3.6 Pin Configuration:

1. VIN (Input Voltage): Connects to the DC power source (4V–40V)
2. VOUT (Output Voltage): Provides the stepped-down regulated output
3. GND (Ground): Common ground connection
4. FB (Feedback): Used in adjustable versions to set the output voltage
5. ON/OFF (Enable Pin): Used to turn the regulator on or off

1.3.7 Advantages of LM2596

- **High efficiency** (compared to linear regulators like 7805)
- **Compact size** and easy to integrate
- **Low heat dissipation** due to high-efficiency switching
- **Supports higher current output (up to 3A)**
- **Built-in protection circuits** (thermal shutdown, overcurrent protection)

1.3.8 Disadvantages

- **Needs external components** (inductor, capacitor) for proper operation
- **Switching noise may require additional filtering** for sensitive applications
- **Requires a heat sink for high current loads (close to 3A)**

1.4 GSM MODULE:

A GSM (Global System for Mobile Communication) module is a hardware device that allows microcontrollers and embedded systems to communicate over a mobile network. It enables functionalities such as sending and receiving SMS, making calls, and connecting to the internet using SIM cards and cellular networks.

1.4.1 Popular GSM Modules:

Some commonly used GSM modules include:

i. SIM800L/SIM800C – Compact, supports GPRS, SMS, and calls

ii. SIM900/SIM900A – Older but widely used, supports SMS, calls, and basic internet functions

iii. SIM808 – Includes GPS functionality along with GSM

iv. SIM5320 – Supports 3G connectivity for faster data transmission

1.4.2 Key Features of GSM Modules:

- Supports SMS (Short Message Service) – Sending and receiving text messages
- Voice Call Capability – Can dial and receive phone calls
- GPRS/EDGE Support – Allows internet access for IoT applications
- UART Communication – Communicates with microcontrollers like Arduino, Raspberry Pi, ESP32 via serial communication (TX/RX pins)
- Operates on GSM Frequencies (850/900/1800/1900 MHz) – Works with global mobile networks
- Can be powered by 3.7V–5V (depending on the model)

1.4.3 Working Principle:

- Insert a SIM Card – Just like a mobile phone, the GSM module needs a SIM card to connect to the network.
- Connect to a Microcontroller – Uses UART (RX, TX) to communicate with controllers like Arduino or ESP32.
- Use AT Commands – Commands like AT+CMGS for SMS, ATD for dialling calls, etc., are used to control the module.
- Network Registration – The module connects to a nearby GSM tower and registers to the network.
- Perform Desired Functions – Sending SMS, making calls, fetching GPS data (if applicable), etc.

1.4.4 GSM Module diagram:

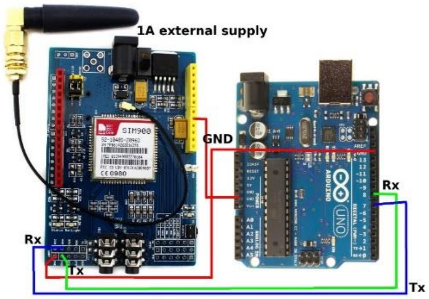


Fig 2: GSM module

1.4.5 Common AT Commands for GSM Modules:

Command	Function
AT	Check if module is working
AT+CSQ	Check signal strength
AT+CMGF=1	Set SMS mode to text
AT+CMGS="+91XXXXXXXXXX"	Send SMS to a specific number
ATD+91XXXXXXXXXX;	Make a call
ATH	Hang up a call
AT+CBC	Check battery status (for some models)

Table 1: common AT commands for GSM module

1.4.6 Applications of GSM Modules:

- Home Security Systems – Used to send intrusion alerts via SMS or calls
- IoT (Internet of Things) Devices – Enables remote monitoring and control via mobile networks
- Vehicle Tracking Systems – Integrated with GPS modules (SIM808, SIM7600) for live location tracking
- Smart Agriculture

1.4.7 Advantages of GSM Modules:

- **Global Connectivity** – Works anywhere with a mobile network.
- **Low Cost & Reliable** – Affordable and widely available.
- **Long-Distance Communication** – No range limitation like Wi-Fi or Bluetooth.
- **Supports Voice & Data Transmission** – Can handle both SMS/calls and GPRS-based data.

1.4.8 Disadvantages:

- **Depends on Network Coverage** – Requires a strong signal for reliable operation.
- **Higher Power Consumption** – Needs a stable power source for continuous operation.
- **Slower than Wi-Fi or LTE** – Internet speed via GPRS is limited.

1.5 ARDUINO/UNO:

The Arduino Uno is one of the most popular and widely used microcontroller development boards, based on the ATmega328P microcontroller. It is designed for beginners and professionals to build electronic projects, automation systems, IoT applications, and embedded systems.

1.5.1 Applications:

- **Home Automation** – Smart lighting, door locks, and security systems
- **IoT Projects** – Weather stations, remote monitoring, and smart farming
- **Robotics** – Controlling motors, sensors, and automation systems
- **Wireless Communication** – Integrating GSM, Wi-Fi, and Bluetooth modules
- **Energy Monitoring Systems** – Solar tracking, battery management
- **DIY Electronics & Prototyping** – Custom circuits and innovative projects

1.5.2 Arduino/UNO Image:

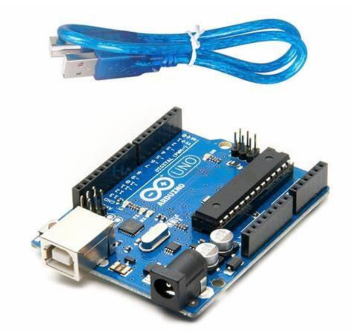


Fig 3: Arduino/UNO

CHAPTER 2
LITERATURE SURVEY

PAPER 1:

The title of this paper is **“IoT-Based Smart Home Security Prototype Using IFTTT Alert System”.**

Introduction to Smart Home Security:

With the rise of Internet of Things (IoT) technology, smart home security systems have evolved significantly. Traditional security measures, such as CCTV cameras and manual alarm systems, lack remote monitoring and automation. This paper explores a smart home security prototype that utilizes IFTTT (If This Then That) alerts for enhanced security, automation, and real-time notifications.

Review of Related Works

1) **IoT in Home Security**

   Several studies have demonstrated how IoT-based security systems enhance real-time monitoring by integrating smart devices like sensors, cameras, and wireless communication modules (GSM, Wi-Fi, and Bluetooth).

2) **Role of IFTTT in Smart Home Automation**

   IFTTT is a cloud-based automation service that connects various IoT devices and services.

3) **Arduino and Sensor-Based Security Systems**

   Several studies have explored the use of Arduino and PIR motion sensors to detect intruders and trigger alarms.

4) **GSM and IoT-Based Alert Mechanisms**

   Some researchers have implemented GSM modules (SIM800L, SIM900) for SMS-based intrusion alerts.

Conclusion

The literature suggests that IoT-based security systems significantly improve home security, and integrating IFTTT automation enhances real-time alert capabilities. This paper contributes to existing research by proposing a prototype that combines Arduino, IoT sensors, and IFTTT for an efficient, cost-effective, and automated security solution.

PAPER 2:

The title of this paper is **“Systematic Survey on Smart Home Safety and Security Systems Using Arduino Platform”**

Introduction to Smart Home Security Systems:

The rapid development of smart home security has led to the integration of IoT, embedded systems, and wireless communication technologies. Traditional security systems, such as manual locks and CCTV surveillance, lack real-time automation and remote monitoring. The Arduino platform has emerged as a low-cost, efficient solution for implementing smart security systems, allowing integration with sensors, actuators, and wireless communication modules to enhance home safety.

Review of Related Works

1) **Arduino-Based Home Security Systems**

   Several research studies have demonstrated the use of Arduino microcontrollers in smart home security due to their affordability and ease of use.

2) **Sensor-Based Intrusion Detection**

   Security systems often incorporate motion sensors (PIR), gas sensors (MQ-2), and door/window sensors (reed switches) for monitoring activities.

3) **Wireless Communication for Smart Security**

   IoT-based security systems integrate Wi-Fi (ESP8266, ESP32), Bluetooth, and GSM modules for remote alerts and monitoring.

4) **Home Automation & AI Integration**

   Modern smart home security systems also incorporate voice assistants (Alexa, Google Assistant), facial recognition, and AI-based monitoring.

Conclusion

The literature suggests that Arduino is a widely used platform for smart home security, enabling integration with various sensors and wireless modules. However, modern smart security systems require real-time IoT connectivity and AI-based automation for enhanced efficiency. The study systematically reviews existing Arduino-based security implementations and proposes an improved model with IoT-enabled real-time monitoring.

PAPER 3:

The title of this paper is **“Home Automation Security Integrating Device Fingerprinting into Smart Homes”**

Introduction to Smart Home Security & Device Fingerprinting:

The rapid advancement of smart home automation has increased concerns about security and unauthorized access to home networks. Traditional security measures, such as password authentication and motion sensors, provide basic protection but lack the ability to identify and track unauthorized devices in real-time. Device fingerprinting is an emerging security mechanism that identifies devices based on their unique hardware and network characteristics. This study explores the integration of device fingerprinting into smart home security, enhancing intrusion detection and access control.

Review of Related Works

1) **Traditional Smart Home Security Approaches**

   Smart home security systems typically rely on biometric authentication, PIN-based access, and IoT-based surveillance.

2) **Device Fingerprinting in Network Security**

   Device fingerprinting is commonly used in cybersecurity to identify unauthorized access attempts.

3) **Integration of IoT & Device Fingerprinting in Home Automation**

   IoT-based smart home systems use Wi-Fi, Zigbee, and Bluetooth for communication, making them vulnerable to unauthorized access and spoofing attacks.

4) **Challenges in Implementing Device Fingerprinting for Home Security**

   Privacy Concerns: Tracking device activity may raise user privacy issues if not properly managed.

Conclusion

The literature suggests that device fingerprinting can enhance smart home security by providing an additional authentication layer beyond traditional password or biometric-based systems. However, challenges such as privacy concerns, network overhead, and false positives need further research. This study explores the potential of device fingerprinting in smart home security, highlighting its applications, advantages, and challenges.

PAPER 4:

The title of this paper is – **“Secured Smart Home Switching System Based on Wireless Communication and Self-Energy Harvesting”**

Introduction to Smart Home Switching Systems:

Smart home automation has transformed traditional electrical systems by integrating wireless communication technologies and self-energy harvesting mechanisms. Conventional home switching systems depend on manual operation or wired control, which limits flexibility and efficiency. The introduction of wireless communication (e.g., Wi-Fi, Zigbee, Bluetooth) enhances remote control capabilities, while self-energy harvesting allows devices to operate without external power sources, reducing dependency on batteries and the grid. This paper focuses on a secured smart home switching system, integrating wireless technology and energy harvesting for sustainable and efficient home automation.

Review of Related Works

1) **Wireless Communication in Smart Home Switching**

   Wireless technology plays a crucial role in remote access and automation.

2) **Energy Harvesting for Smart Home Applications**

   Self-energy harvesting reduces the need for external power sources, improving sustainability.

3) **Security Challenges in Wireless Home Automation**

   Wireless switching systems are vulnerable to cyberattacks, unauthorized control, and signal interference.

4) **Integration of IoT, Wireless, and Energy Harvesting**

   Combining IoT-based control, wireless communication, and self-energy harvesting improves home automation efficiency.

Conclusion

The literature suggests that integrating wireless communication with self-energy harvesting can significantly improve smart home automation. However, challenges related to energy efficiency, security vulnerabilities, and scalability need further research. This study aims to develop a secured smart home switching system that overcomes these limitations, ensuring energy-efficient, wireless, and secure home automation.

PAPER 5:

The title of this paper is **“Smart Home Security and Efficient Multifactor Authentication**

Introduction to Smart Home Security & Multifactor Authentication (MFA):

The evolution of smart home security has led to the integration of advanced authentication methods to prevent unauthorized access and cyber threats. Traditional security mechanisms, such as password-based authentication, are vulnerable to hacking, brute force attacks, and phishing. Multifactor Authentication (MFA) enhances security by requiring multiple forms of verification, including biometrics, OTPs, and hardware tokens. This paper focuses on MFA strategies for securing smart home environments, ensuring reliable access control and user authentication.

Review of Related Works

1) **Traditional Authentication in Smart Homes**

   Early smart home security systems relied on PIN-based or password authentication, which is prone to hacking.

2) **Biometric Authentication in Smart Home Security**

   Biometrics (e.g., fingerprint, facial recognition, voice recognition) has improved authentication accuracy.

3) **Multifactor Authentication (MFA) for Enhanced Security**

   MFA combines something you know (password/PIN), something you have (smartphone/OTP), and something you are (biometrics)

4) **AI & Machine Learning in Smart Home Security**

   AI-based behavioral authentication detects anomalies in user behavior, enhancing security.

5) **Challenges in Implementing MFA for Smart Homes**

   Usability vs. Security: Complex authentication methods may reduce user convenience.

Conclusion

The literature suggests that MFA significantly enhances smart home security, but challenges related to user convenience, cybersecurity threats, and device compatibility require further research. This study aims to develop a robust and efficient MFA-based smart home security system, ensuring high security while maintaining ease of access.

GAP ANALYSIS:

Reference	Article Title	Limitations
Kaur, P. and Sharma, N., 2022, May. An IOT Based Smart Home Security Prototype Using IFTTT Alert System. In *2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON)* (Vol. 1, pp. 393-400). IEEE.	An IOT Based Smart Home Security Prototype Using IFTTT Alert System	The IFTTT free tier restricts the creation of only five applets. The study focuses on a prototype and emphasizes future improvements for adding more security features.
Sarhan, Q.I., 2020. Systematic survey on smart home safety and security systems using the Arduino platform. *IEEE Access*, *8*, pp.128362-128384.	Systematic Survey on Smart Home Safety and Security Systems Using the Arduino Platform	Suggested future enhancements include using LiDAR and Iris scanners for improved facial recognition accuracy beyond camera-based detection.
Muthumanickam Dhanaraju, Poongodi Chenniappan, Kumaraperumal Ramalingam, Sellaperumal Pazhanivelan, Ragunath Kaliaperumal	Improving Home Automation Security; Integrating Device Fingerprinting Into Smart Home	Devices present security risks, allowing attackers to gain unauthorized control, breach privacy, or hack data. Authentication may fail due to identifier mismatches.
Zungeru, A.M., Gaboitaolelwe, J., Diarra, B., Chuma, J.M., Ang, L.M.,	A Secured Smart Home Switching System Based on Wireless Communication and	Energy harvesting limitations, security concerns, and wireless communication

Kolobe, L., David, M. and Zibani, I., 2019. A secured smart home switching system based on wireless communications and self-energy harvesting. *IEEE Access*, *7*, pp.25063-25085.	Self-Energy Harvesting	limitations affect system performance and reliability.
Sarbishaei, G., Modarres, A.M.A., Jowshan, F., Khakzad, F.Z. and Mokhtari, H., 2024. Smart Home Security: An Efficient Multi-Factor Authentication Protocol. *IEEE Access*..	Smart Home Security and Efficient Multifactor Authentication Introduction to Smart Home Security & Multifactor Authentication (MFA):	Energy consumption, usability challenges, security limitations, network and communication issues, and environmental constraints impact the system's efficiency.

CHAPTER 3
METHODOLOGY

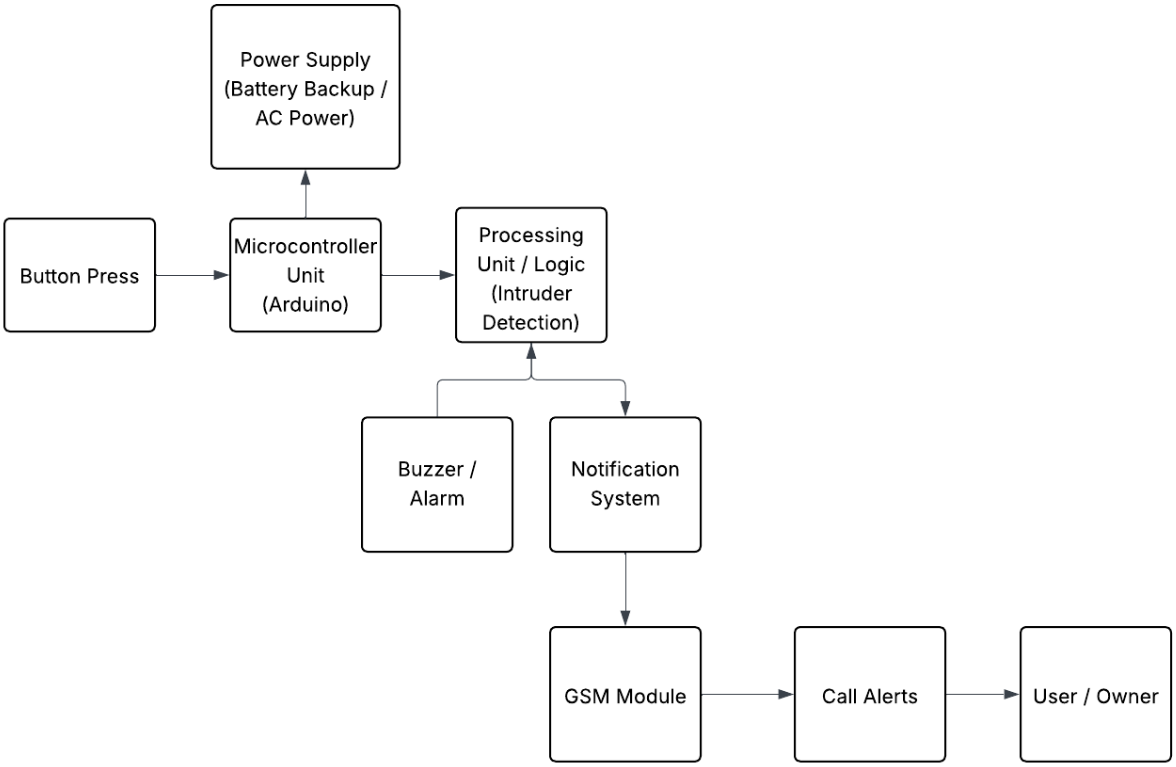

Power Supply (Battery Backup / AC Power)
Button Press
Microcontroller Unit (Arduino)
Processing Unit / Logic (Intruder Detection)
Buzzer / Alarm
Notification System
GSM Module
Call Alerts
User / Owner

Fig 4: Block diagram

3.1 Objectives of the System:

Detect and Prevent Unauthorized Entry:

- Continuously monitors the home environment using PIR sensors and surveillance cameras.
- Identifies whether the detected motion is from an authorized individual.
- Maintains event logs for future reference and activity tracking by homeowners.

Provide Real-Time Alerts via Calls, Emails, and Alarms

- Instantly triggers an audible alarm when an intruder is detected.
- Utilizes a GSM module and IFTTT service to place automated calls to the homeowner.
- Sends real-time email notifications and alerts local security or emergency services in case of repeated intrusion attempts.

Enhance Security with LED and Buzzer Alerts

- Activates LED lights and buzzers to provide immediate visual and audible deterrents.
- Increases the likelihood of preventing unauthorized access through rapid response mechanisms.
- Seamlessly integrates with smart home systems for improved coordination and overall security enhancement.

3.2 Automated Call Alert System:

Content:

The GSM module is integrated into the home security system to provide real-time intrusion alerts.

How It Works:

- When the intruder opens the door, the button which is placed at the door will be pressed
- The microcontroller processes the detection and triggers the GSM module.
- The GSM module dials the homeowner's registered number, alerting them of a possible intrusion.
- The homeowner receives the call and can take immediate action, such as alerting security personnel.

Benefits:

- Instant alert system, ensuring quick response.
- No reliance on internet connectivity, making it reliable.
- Can be integrated with multiple numbers for emergency response.

Advantages of the System:

- **Automated Alerts** – The system automatically detects motion and calls the homeowner, requiring no manual monitoring.
- **Cost-Effective Security** – Uses affordable IoT components and eliminates the need for expensive security services.
- **Easy to Install & Maintain** – Simple plug-and-play system with minimal wiring and setup.
- **Real-Time Intruder Alert** – Instant call notifications ensure quick homeowner response to potential threats.
- **Works Without Internet** – The GSM module functions independently of Wi-Fi, making

it reliable during outages.

- **Scalable & Expandable** – Can integrate with smart lights, sirens, or additional security features.

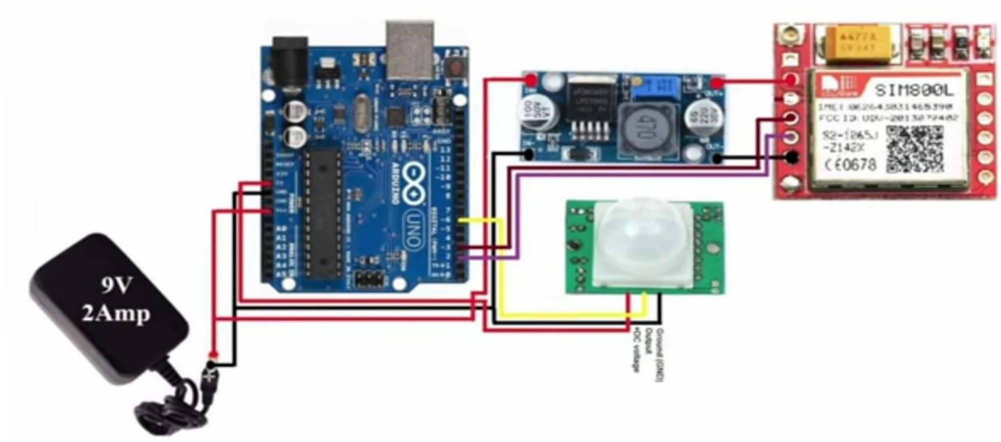


Fig 5: Circuit diagram

3.2 SOFTWARE DEVELOPMENT:

Development Environment:

1.Arduino IDE:

- This is the most common and user-friendly IDE for ESP32 development.
- It's based on C/C++ and provides a wide range of libraries and examples.
- It's cross-platform, compatible with Windows, macOS, and Linux.

ESP-IDF (ESP32 IoT Development Framework):

- A more advanced framework for ESP32 development.
- Provides greater control and flexibility but has a steeper learning curve.
- Typically used for professional or complex projects.

2. Programming Language:

C/C++:

The primary programming languages used for ESP32 development.

Offer low-level control and efficient performance.

3. Libraries:

WiFi.h:

Essential for establishing and managing Wi-Fi connections.

Provides functions for connecting to networks, sending HTTP requests, and handling network events.

TinyGPS++.h:

A lightweight and efficient library for parsing NMEA sentences from GPS modules.

Extracts latitude, longitude, altitude, and other relevant GPS data.

ThingSpeak.h:

Simplifies communication with the ThingSpeak platform.

Provides functions for sending data to ThingSpeak channels.

3.2 CODE:

```
#include <SoftwareSerial.h>
SoftwareSerial GSM(11, 10);
char phone_no[] = "+91XXXXXXXXXX";
#define bt_C  A1
void setup() {
Serial.begin(9600);
GSM.begin(9600);
pinMode(bt_C, INPUT_PULLUP);
Serial.println("Initializing....");
initModule("AT", "OK", 1000);
 }
void loop() {
  if (digitalRead (bt_C) == 0)
  {
    callUp(phone_no);
  }

  delay(5);
}
```

```
void callUp(char *number) {
  GSM.print("ATD + "); GSM.print(number); GSM.println(";");
  delay(20000);
  GSM.println("ATH");
  delay(100);
}
void initModule(String cmd, char *res, int t) {
  while (1) {
    Serial.println(cmd);
    GSM.println(cmd);
    delay(100);
    while (GSM.available() > 0) {
      if (GSM.find(res)) {
        Serial.println(res);
        delay(t);
        return;
      } else {
        Serial.println("Error");
      }
    }
    delay(t);
  }
}
```

3.2.1 Code explanation:

```
#include <SoftwareSerial.h>
```

- The **SoftwareSerial** library allows serial communication on digital pins other than the default TX (1) and RX (0) of the Arduino.
- This is required because the **SIM800L GSM module** communicates using serial but cannot use the hardware serial pins (0,1) as they are reserved for USB communication.

```
SoftwareSerial GSM(11, 10);
```

- Creates a **software serial port** named GSM using **pin 11 for RX** and **pin 10 for TX**.
- The **SIM800L module's TX pin** is connected to **Arduino pin 11**, and **SIM800L's RX pin** is connected to **Arduino pin 10**.

```
char phone_no[] = "+91XXXXXXXXXX"; //change with phone number to sms
```

- This variable stores the **phone number** where the system will make a call upon intrusion detection.
- Replace +91XXXXXXXXXX with the actual mobile number (**+91** is the country code for India).

```
#define bt_C  A1
```

- bt_C is assigned to **analog pin A1**, which is used as an input pin for a button.
- When pressed, it will trigger the GSM module to make a call.

```
Serial.begin(9600); // Communication with Serial Monitor
GSM.begin(9600);    // Communication with SIM800L Module
```

- **Serial.begin(9600);** enables debugging using the Serial Monitor.
- **GSM.begin(9600);** initializes communication with the **SIM800L module** at a baud rate of 9600.

```
pinMode(bt_C, INPUT_PULLUP); // declare bt_C as input
```

- Sets **bt_C (A1)** as an **input pin with an internal pull-up resistor**.
- The button is **active-low**, meaning it reads HIGH by default and LOW when pressed.

```
Serial.println("Initializing....");
initModule("AT", "OK", 1000);
```

- Sends the "AT" command to check if the **SIM800L module** is responding.
- If the response is "OK", it proceeds; otherwise, it retries.

```
if (digitalRead (bt_C) == 0)
```

- Reads the state of the **bt_C (A1)** button.
- If **button is pressed (LOW)**, the system will make a call.

```
callUp(phone_no);
```

- Calls the function callUp(phone_no);, which triggers the GSM module to dial the stored phone number.

```
delay(5);
```

- Adds a **small delay (5ms)** to avoid rapid repeated calls.

```
GSM.print("ATD + "); GSM.print(number); GSM.println(";");
```

- **ATD** is the **AT command** for dialing a number.
- The number is **concatenated (+ operator)** and sent to the SIM800L module.
- The **semicolon (;)** at the end is required to execute the dial command.

```
delay(20000);
```

- Waits **20 seconds** to allow the call to ring before hanging up.

```
GSM.println("ATH");
```

- **ATH** is the **AT command** to hang up the call.

```
delay(100);
```

- Adds a **100ms delay** before executing the next command.

```
void initModule(String cmd, char *res, int t) {
  while (1) {
    Serial.println(cmd);
    GSM.println(cmd);
    delay(100);
```

- This function sends **AT commands** (cmd) to the GSM module.
- The loop runs **continuously** until the expected response (res) is received.

```
while (GSM.available() > 0) {
  if (GSM.find(res)) {
    Serial.println(res);
    delay(t);
    return;
  } else {
    Serial.println("Error");
  }
}
```

- The GSM.find(res) function searches for the expected response (e.g., "OK").
- If found, it prints "OK" and exits.
- If the response is incorrect, it prints "Error" and retries.

```
delay(t);
```

- **Waits t milliseconds** before retrying the AT command

3.2.2 Execution steps:

1.Hardware Setup:

- **SIM800L GSM Module:**

  Connect the SIM800L GSM module to the Arduino using a SoftwareSerial connection**:**

  - TX of SIM800L to Pin 10 (RX on Arduino)
  - RX of SIM800L to Pin 11 (TX on Arduino)
  - GND of SIM800L to GND on Arduino
  - VCC of SIM800L to 5V on Arduino (or use an external power source if required, as SIM800L requires higher current for operation**)**
- **Button:**
  - Button pin (bt_C) connected to A1 on the Arduino. This is used as an input pin to trigger the call.
  - Ensure the button is wired with a pull-up resistor (either internally or externally) to work properly with INPUT_PULLUP.

2. Code Modifications:

- Change the phone number in the phone_no[]
- array to your target phone number:

  char phone_no[] = "+91XXXXXXXXXX"

3. Upload the Code to Arduino:

1. Open the Arduino IDE.
2. Select the correct board and port from Tools > Board and Tools > Port.
3. Paste the modified code into the Arduino IDE.
4. Upload the code to your Arduino by clicking the Upload button.

4. Operation:

- When the Arduino is powered on, it will initialize the SIM800L GSM module and check for a successful connection to the module.
- The button connected to pin A1 will act as a trigger. the Arduino will send an AT command to the SIM800L to initiate a call to the number defined in the phone_no[] array.
- The call will be placed, and after 20 seconds, the SIM800L will hang up the call automatically.

5. Debugging:

We have to monitor the serial output in the Arduino IDE’s Serial Monitor (set to 9600 baud rate) to observe the status of the system. It will print messages like "Initializing....", and AT command responses, such as "OK" or "Error".

6.Powering the SIM800L:

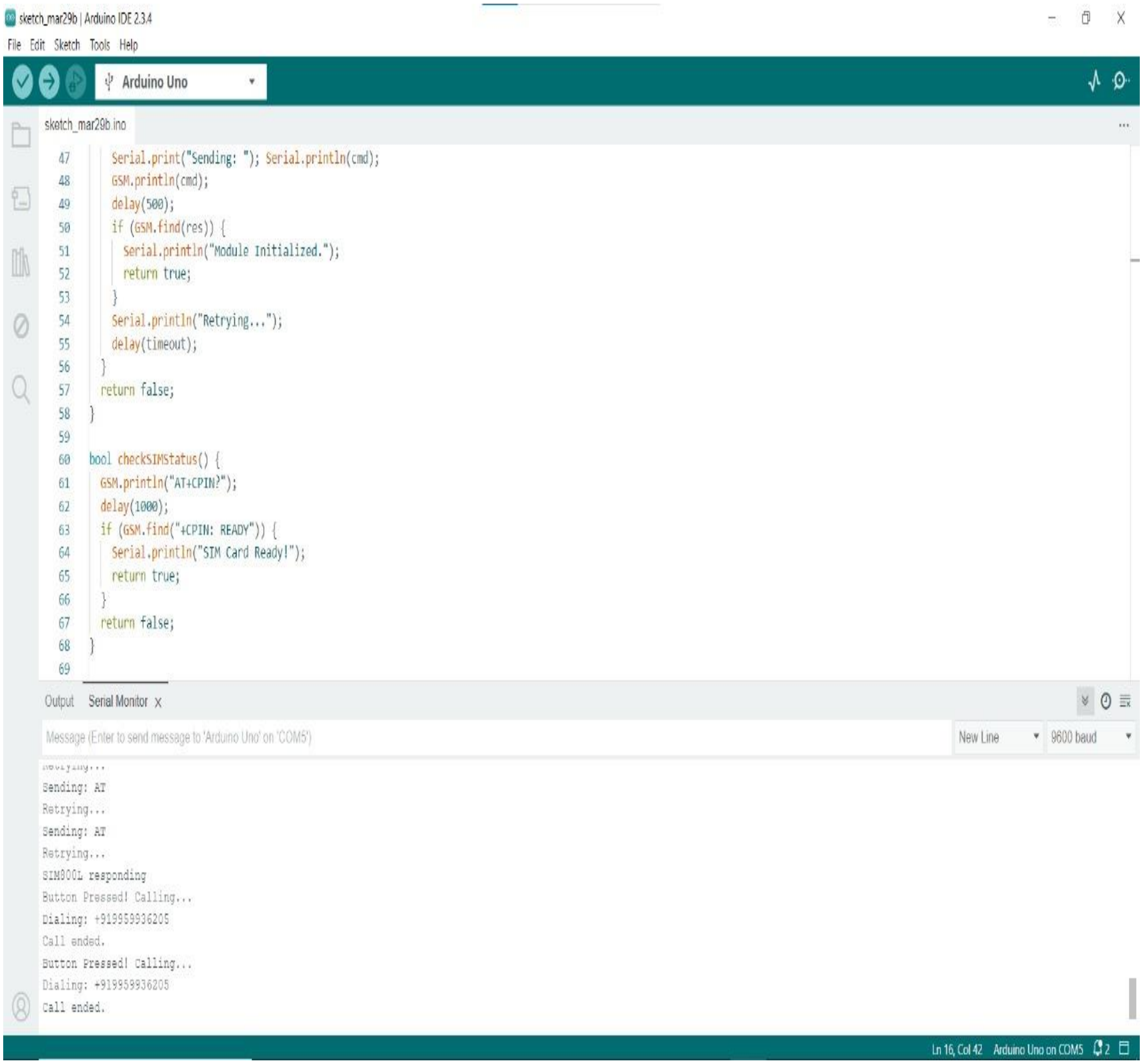
- The SIM800L GSM module requires a stable power source and a good-quality SIM cardwith active service for the GSM functionality.
- If the SIM800L doesn't power up properly from the Arduino's 5V pin, consider using a separate power supply (usually 3.7V-4.2V).

7. Expected Output:

- Upon pressing the button, the system will attempt to call the specified phone number.
- The call will last for 20 seconds, after which the system will hang up.
- The Serial Monitor will show relevant logs of the communication with the SIM800L GSM module.

CHAPTER 4
RESULTS

The expected result for a successful request is a phone call initiated via Arduino,Twilio, a SID logged in the console, and the response "Call initiated!" sent to the client.


sketch_mar29b | Arduino IDE 2.3.4
File Edit Sketch Tools Help
Arduino Uno
sketch_mar29b.ino
Output
Serial Monitor
Message (Enter to send message to 'Arduino Uno' on 'COM5')
Ln 16, Col 42
Arduino Uno on COM5
2

```
      Serial.print("Sending: "); Serial.println(cmd);
      GSM.println(cmd);
      delay(500);
      if (GSM.find(res)) {
        Serial.println("Module Initialized.");
        return true;
      }
      Serial.println("Retrying...");
      delay(timeout);
    }
    return false;
  }

  bool checkSIMStatus() {
    GSM.println("AT+CPIN?");
    delay(1000);
    if (GSM.find("+CPIN: READY")) {
      Serial.println("SIM Card Ready!");
      return true;
    }
    return false;
  }
```

New Line
9600 baud

```
Retrying...
Sending: AT
Retrying...
Sending: AT
Retrying...
SIM800L responding
Button Pressed! Calling...
Dialing: +919959936205
Call ended.
Button Pressed! Calling...
Dialing: +919959936205
Call ended.
```

Fig 5: Output

CHAPTER 5

CONCLUSION

The "**Home Security System with Intruder Alert"** project provides a comprehensive solution for protecting homes from unauthorized access and potential intrusions. By integrating various hardware components such as motion sensors, cameras, and communication modules (like GSM or Twilio), this system can detect any intrusion and promptly alert homeowners through multiple channels.

1. **Effective Intruder Detection**:
    - The system is designed to continuously monitor the premises for any unusual activity using sensors (such as PIR motion sensors) and cameras. Once an intruder is detected, the system immediately triggers an alert.

2. **Real-time Alerts and Notifications**:
    - In the event of an intruder, the system notifies the homeowner via SMS or Phone Call using communication modules like SIM800L GSM Module or Twilio API. The use of such notifications ensures that the homeowner is instantly informed about the threat, regardless of their location.

3. **Scalable and Customizable**:
    - The system is highly customizable, allowing for integration with various types of sensors and alert methods. Whether it's a camera feed or a simple motion sensor, the system can be adapted based on the specific needs and preferences of the user.
    - Additionally, the system can be enhanced with features such as remote monitoring, automatic door locking, and video surveillance.

4. **Cost-effective Security**:
    - By using readily available hardware (e.g., Arduino, GSM modules, and cameras), this system offers a low-cost alternative to expensive professional security systems, while still providing substantial protection.

5. **User-friendly Interface**:
    - The system provides an easy-to-use interface where the homeowner can easily configure settings, monitor the system's status, and view alerts. In case of a detected intruder, the system handles everything automatically, reducing the need for active monitoring.

6. **Remote Monitoring Capability**:
    - With the integration of communication tools like Twilio or a GSM module, the system supports remote notifications, allowing homeowners to stay informed of any threats in real-time, even if they are miles away.

7. **Potential for Future Enhancements**:
    - This system can be further enhanced with additional features such as **facial recognition**, **voice alerts**, and integration with home automation systems. It can also be connected to cloud-based storage for video feeds or even interfaced with smart home platforms.

The **Home Security System with Intruder Alert** project successfully addresses the growing need for smart and affordable home security. By utilizing simple yet powerful technologies like sensors, GSM, and cloud-based services, it offers an effective and reliable solution to protect homes from intrusions. The ability to send immediate alerts ensures a prompt response to security threats, enhancing safety and peace of mind for homeowners.

CHAPTER 6

REFERENCES

[1]. S. Kumar, P. Tiwari and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review", *J Big Data*, vol. 6, pp. 111, 2019.

https://ieeexplore.ieee.org/document/9850500

[2]. K. C. Sahoo and U. C. Pati, "IoT based intrusion detection system using PIR sensor", *2nd IEEE International Conference on Recent Trends in Electronics Information Communication Technology*, pp. 1641-1645, 2017.

https://ieeexplore.ieee.org/document/8256877

[3]. Y. Zhou, X. Yang and L. Wang, "A Wireless Design of Low-Cost Irrigation System Using ZigBee Technology", *IEEE 2009 International Conference on Networks Security Wireless Communications and Trusted Computing*, vol. 1, pp. 572-575, 2009.

https://ieeexplore.ieee.org/document/4908331

[4]. T. Gong, H. Huang, P. Chen, R. Malekian and T. Chen, "Improving Home Automation Security: Integrating Device Fingerprinting Into Smart Home", *Tsinghua Sci. Technol.*, vol. 21, no. 4, pp. 385-396, 2016

https://ieeexplore.ieee.org/document/7563403

[5]. P. Guo, J. Wang, X. H. Geng, C. S. Kim and J.-U. Kim, "**:** IoT-Based Smart Security and Home Automation System", *J. Internet Technol.*, vol. 15, no. 6, pp. 929-936, 2014

https://ieeexplore.ieee.org/document/7349214