CHAPTER 1: INTRODUCTION

1.1 Problem Statement

Urban environments are expanding rapidly, with projections indicating that 66% of the global population will reside in cities by 2050. This rapid urbanization has intensified the need for advanced and scalable safety solutions. Traditional security measures, such as CCTV cameras, security personnel, and manual alert systems, are often inadequate in responding to emergencies like theft, fire hazards, gas leaks, and medical crises. These systems suffer from limitations, including delayed responses, lack of real-time communication, and inefficient crisis management. Consequently, urban residents frequently rely on neighbors or security personnel to detect and address incidents, leading to significant delays in emergency response times.

1.2 Need for IoT and AI-Driven Safety Solutions

The Internet of Things (IoT) and AI-driven automation have emerged as transformative technologies capable of addressing the inefficiencies of conventional safety measures. IoT-based smart safety systems leverage interconnected sensors, real-time monitoring, and automated alert mechanisms to provide continuous surveillance and rapid emergency notifications. However, despite their potential, the integration of these technologies into existing urban infrastructure remains limited, preventing communities from fully benefiting from their capabilities.

1.3 Proposed Solution

To overcome these challenges, we propose an AI-Integrated Home and Community Safety System, an IoT-based solution designed to enhance emergency management and response in urban settings. This system incorporates a NodeMCU microcontroller, flame and gas sensors, an OLED display, push buttons for triggering alarms, and wireless communication to enable real-time emergency alerts. By instantly notifying residents and community members about potential threats, the system ensures a swift response to emergencies, significantly reducing response times.

1.4 Significance and Impact

The proposed system is designed for scalability and adaptability, offering a unified solution to diverse urban safety concerns. By leveraging IoT and AI, it aligns with the Sustainable Development Goals (SDG 11: Sustainable Cities and Communities) and SDG 9: Industry, Innovation, and Infrastructure. This innovation represents a shift from fragmented safety measures to an integrated, intelligent platform that enhances urban resilience, promotes sustainability, and fosters the development of safer, smarter cities.

This technology has the vision to advance conventional, independent safety interventions to an end-to-end, smart platform maximizing emergency response efficiency, minimizing dependency on human intervention, and constructing a safer, sustainable city life. Merging AI and IoT with city safety infrastructure is an important step in realizing the concept of the smart city, in which safety, sustainability, and innovation merge to advance the quality of urban living.

1.5 Detailed Explanations of Emergency Scenarios

Theft remains a significant concern for urban dwellers, particularly in areas where population density creates anonymity. According to our survey, over 65% of Chennai residents have experienced theft incidents either personally or within their community. The proposed system addresses this issue by using AI-powered motion detectors and surveillance cameras that can identify suspicious activities. If unauthorized entry is detected, the system triggers a loud siren and flashing lights, alerting neighbors and deterring the intruder. Simultaneously, an alert is sent to the local police station with the specific location details, ensuring a swift response. This integrated approach not only prevents potential theft but also fosters a sense of community vigilance, as neighboring homes are immediately informed of the threat.

Medical emergencies, such as heart attacks, strokes, or accidents, require immediate attention. The delay in receiving medical assistance can have dire consequences, especially for elderly residents living alone. The AI-Integrated system includes features like wearable health monitors and emergency buttons that can be activated manually or through voice commands. In the event of a medical emergency, the system automatically contacts emergency medical services, while also alerting nearby residents who may be able to provide first

aid. The system's ability to prioritize alerts based on the severity of the situation ensures that critical cases receive prompt attention. This real-time communication can significantly reduce response times, potentially saving lives.

Fire hazards pose a substantial risk in urban settings, where buildings are often located in close proximity to each other. Traditional smoke alarms are limited in their ability to provide comprehensive protection as they only alert the occupants of the affected home. 8 The proposed system goes a step further by using AI algorithms to analyze smoke patterns and temperature changes, thus identifying the onset of a fire even before visible signs appear. Once detected, the system not only sounds an alarm but also sends alerts to neighbors and the fire department. By informing the entire community and authorities in real-time, the system helps to prevent the rapid spread of fire, thereby minimizing property damage and saving lives.

Air quality is an often-overlooked aspect of urban safety, despite its significant impact on health. Poor air quality, especially in congested urban areas, can lead to respiratory issues and other health complications. The proposed system includes sensors capable of detecting harmful gases such as carbon monoxide, as well as monitoring overall air quality. When dangerous levels are detected, the system sends alerts to residents, prompting them to take protective measures, such as ventilating their homes or wearing masks. This proactive approach not only safeguards residents' health but also raises awareness about the importance of air quality monitoring in urban living.

CHAPTER 2: LITERATURE SURVEY

2.1 Literature Survey Insight and Inspiration

Recent research in smart home and community security systems has made significant strides by integrating technologies such as IoT, AI, and advanced communication networks to bolster safety and efficiency. The adoption of IoT-driven solutions has transformed traditional security mechanisms, enabling automated monitoring, real-time alerts, and enhanced data analytics to detect and respond to potential threats. For instance, systems utilizing LoRa technology have been developed to improve communication in retirement communities, offering both manual and automatic alert capabilities. Additionally, the integration of AI and IoT in smart cities has shown substantial benefits in urban security, facilitating proactive crime prevention through advanced surveillance, secure networking, and community-driven platforms like Neighborhood Watch. Innovations in security systems also include the use of machine learning algorithms to enhance anomaly detection in contactless attack scenarios and automated responses in smart homes. The deployment of GSM-based notification systems and MQTT protocols for remote monitoring has further improved the responsiveness of security measures, allowing for real-time communication with authorities during emergencies. The growing focus on cybersecurity has led to the development of cryptographic systems and multilevel encryption techniques to safeguard sensitive data from cyber threats, especially in IoT environments where devices are highly interconnected. The emphasis on community-based safety measures has driven the creation of collaborative platforms that utilize sensor networks, machine learning, and data sharing to optimize security and emergency response. Technologies like clustering in H2H (Human-to-Human) communication architectures and clustering technologies have been explored to reduce traffic volume and enhance communication efficiency in smart communities. Other studies have highlighted the use of blockchain technology to secure IoT device data, ensuring tamper-proof records of security incidents, and integrating decentralized management systems for better reliability. Furthermore, the exploration of AI-integrated solutions, such as facial recognition, motion detection, and automated alerts, has enhanced the capabilities of smart home devices to handle security breaches effectively. Mobile applications equipped with GPS tracking, panic buttons, and drone assistance have been proposed to improve

both personal and public safety. The integration of AIdriven automation with IoT sensors has not only enhanced security but also optimized energy management in smart homes, contributing to sustainability goals.

2.1.1 Overview of Literature Survey

[1]. *LoRa-Based Security System for Retirement Communities*

Abubaker Sherif et al., (2019) study presents the development of a home security system using Long Range (LoRa) wireless communication tailored for retirement townships. The system features embedded sensors, a panic button, and supports both manual and automatic alerts. It integrates mobile and web applications for monitoring and security management, offering a reliable low-power solution for community-scale protection.

[2]. *IoT and AI Integration for Smart Cities: A Review*

Md Eshrat E. Alahi *et al.*, (2023) review explores how IoT, Artificial Intelligence (AI), and 5G networks are converging to create smart cities. It discusses the potential of wireless communication and AI algorithms to optimize urban living by improving infrastructure, enhancing public safety, and enabling real-time intelligent responses within urban environments.

[3]. *Smart Community Networking and Applications*

Xu Li, Rongxing Lu *et al.*, (2021) paper introduces the concept of smart communities and highlights secure networking among smart homes. It presents use cases like Neighborhood Watch and Pervasive Healthcare that demonstrate how connected communities can share data for enhanced safety, health, and living standards.

[4]. *Smart Home Security with IoT-Based Malware Detection*

Rui Yu, Minyuan Zhang *et al.*, (2021) work proposes a smart home security system that can detect and defend against contactless malware attacks. The system operates with minimal network impact and suggests future integration with machine learning to improve anomaly detection and threat mitigation in connected environments.

[5]. *Home-to-Home (H2H) Communication for Smart Communities*

Jinsoo Han *et al.*, (2017) study compares centralized and distributed architectures in home-to-home communication systems. It emphasizes the benefits of distributed clustering in reducing data traffic and enhancing reliability in smart residential communities.

[6]. *IoT-Based Monitoring Platform with MQTT for Smart Homes*

David Nettikadan *et al.*, (2018) research outlines the design of a smart community

monitoring platform that employs MQTT protocol for efficient data transmission. Custom smart homes are remotely monitored and controlled via a web interface, enhancing security and convenience in a connected living environment.

[7]. ***Review of IoT-Based Security Alarm Systems***

Mehmet Çavaş et al., (2019) review technological advancements in IoT-based alarm systems, identifying key challenges such as internet reliability and cybersecurity concerns. The study provides insights into future improvements needed for building robust and secure smart home security solutions.

[8]. ***GSM-Based Anti-Theft and Hazard Detection System***

Md. Abdullah Al Rakib et al., (2021) present a GSM-enabled security system designed to detect theft, gas leaks, and fire. The system allows users to remotely control appliances and receive real-time alerts via SMS and calls, offering a practical solution for regions with limited internet connectivity.

[9]. ***IoT-Based Smart Home Security with Facial Recognition***

AKM Jahangir Alam Majumder et al., (2020) develop an IoT-based security system utilizing motion sensors and facial recognition. Built with Raspberry Pi and camera modules, the system enables accurate intruder detection and identity verification. The study outlines future improvements, including scaling with enhanced hardware and broader datasets.

[10]. ***Intelligent Community Security System (ICSS) Using Wireless Sensors***

Jihong Liu et al., (2011) introduce an intelligent security system utilizing wireless sensor networks to automate community safety functions. The system enhances efficiency in incident detection, real-time monitoring, and the management of safety resources.

[11]. ***Community Safety Notification Management System***

Yong Jin et al., (2016) introduce a safety system that includes a notification management entity to coordinate communication between users and administrators. The system categorizes users and handles notifications based on user roles, ensuring efficient delivery of safety, security, and health alerts within a community setup.

[12]. ***The e-JIKEI Network Project for Community Security***

Yusaku Fujii et al., (2015) propose the e-JIKEI Network project, a low-cost, scalable community security system using home computers and network cameras. It revives traditional neighbourhood watch practices through modern internet-enabled devices and provides free software and setup manuals to encourage global adoption.

[13]. *Mobile Emergency Alert System via Server Notification*

Ghen Saito et al., (2017) present a personal security solution where individuals can use a mobile app to press a panic button during emergencies. The alert is sent to a central server, which then forwards it to the appropriate security or health services, using real-time condition and location data.

[14]. *Cryptographic Data Security for Community Separation*

Ron M. Redlich et al., (2006) propose a secure data system that supports multi-level encryption and distributed storage for community data protection. By managing cryptographic separation and filtering, only authorized users with proper clearance can reconstruct and access specific plaintext data.

[15]. *Mobile Safety App with GPS, Drone, and Biometric Features*

Dan Kerning et al., (2016) present a multi-featured mobile application for enhancing personal safety. It includes GPS tracking, panic button activation, incident reporting, drone support, and biometric identity verification, creating a layered safety net for emergency response.

[16]. *Two-Layer Security System with Role-Based Access*

Cindy McMullen et al., (2012) describe a collaborative computing security model with two primary layers: system-level security and membership-based entitlements. It emphasizes managing data visibility based on user roles and provides structured access control mechanisms.

[17]. *Security Challenges and Mechanisms for Mobile Devices*

Kevin Curran et al., (2015) discuss common mobile security features such as encryption, remote wipe, antivirus, and firewalls. The review highlights the lack of a universal security standard and suggests customized approaches based on device use and threats.

[18]. *Video-Based Motion Detection and Alarm Monitoring System*

Michael J. Saylor et al., (2002) describe a video surveillance solution that compares sequential images to detect motion and trigger alarms. It enables users to define response rules, supports remote monitoring, and integrates multiple systems into a centralized security network.

[19]. *Sociodemographic Analysis of Gated Communities in the U.S.*

Thomas W. Sanchez et al., (2015) use 2001 AHS data to show that gated communities in the U.S. are more diverse than often assumed. The study distinguishes between communities built for prestige and those focused on security, revealing varied characteristics across regions.

[20]. *Cybersecurity Gaps in Consumer IoT Device Documentation*

John M. Blythe et al., (2019) analyze 270 IoT consumer device manuals and find a widespread lack of standardized security practices. Basic recommendations like account password management and updates are common, but deeper cybersecurity guidance is often missing. The study advocates for policy-level intervention.

[21]. *Security Testbed Framework for IoT Using Machine Learning*

Shachar Siboni et al., (2019) propose a security testbed architecture for Internet of Things (IoT) environments, capable of addressing their diverse deployments. It integrates standard and advanced security testing, while leveraging machine learning algorithms to monitor operations, detect anomalies, and identify potential vulnerabilities.

[22]. *Mapping Cybersecurity Research Using Louvain Community Detection*

Sotirios Katsikeas et al., (2011) analyze large-scale citation data from Scopus (1949–2020), mapping cybersecurity research through community detection. The study uncovers 12 key research clusters, with significant attention on cryptography, while identifying areas such as law and regulation as underexplored.

[23]. *Socially-Aware IoT in Smart Communities: Queuing Model Analysis*

Qinghe Du et al., (2018) investigate future smart communities using IoT that incorporates social features like user credit and reputation. Using queuing theory and asymptotic analysis, the study aims to optimize socially-driven IoT communications and enhance autonomous behavior within networks.

[24]. Co-oPS: Collaborative Privacy and Security Design

Chhaya Chouhan et al., (2019) introduce the Co-oPS participatory design model for integrating user feedback into mobile app privacy and security mechanisms. Based on sessions with 32 participants, the study explores trust, motivation, and user expectations in digital security decisions.

[25]. Community Situation Tables as Social Control Tools

Carrie B. Sanders et al., (2018) explore Canada’s use of Situation Tables to coordinate safety services through ethnographic research. The paper argues that these structures reassign public safety responsibilities to clients and service organizations, potentially reducing transparency and democratic oversight.

[26]. Home Security Signal Code Transmission System

Scanner et al., (2000) describe a method for remotely managing home security systems. It uses signal codes sent from a client device to an administrator, who verifies the codes and triggers appropriate responses based on predefined

emergency incident categories.

[27]. Privacy Vulnerabilities in Automatic Meter Reading Systems

Ishtiaq Rouf et al., (2012) identify weaknesses in AMR systems, which broadcast utility data without encryption, potentially revealing home occupancy patterns. Through reverse engineering and experiments, the authors propose “defensive jamming” as a mitigation strategy.

[28]. Encryption-Based Communication Protocol for Security Devices

Geoff Smith et al., (2017) explain a secure communication method between a device and server using initial and session-based encryption keys. The patent includes a process for dynamic key updates to maintain data confidentiality across sessions.

[29]. MAC Address-Based IoT Security Against DoS Attacks

Aswin Raghuprasad et al., (2020) explore denial-of-service (DoS) and distributed DoS threats to IoT networks. The study presents MAC address filtering as a defense mechanism and outlines future research directions to improve resilience in IoT security systems.

[30]. Ethical Challenges in Cybersecurity Research Practices

David Dittrich et al., (2010) investigate the ethical dilemmas faced by cybersecurity researchers, focusing on botnets, worms, and malware research. Topics include system compromise for study, user deception, and the legality of botnet takedowns. The authors advocate for community-driven ethical standards and enforcement.

[31]. Web-Based Video Alert Notification System

James J. Ni et al., (2020) propose a web server-based system that receives internet calls from surveillance locations, processes video feeds, and notifies users based on their alert preferences. The notification includes a video link, allowing users to access a web page or device directly to view the feed.

[32]. Integrated Mobile Biometric and Audio/Video Analytics for Access Control

Dan Kerning et al., (2017) present a security system utilizing mobile device biometrics and proximity verification. It includes PIN entry, mobile scanners, audio analytics (e.g., gunshot detection), and video analytics to associate individuals with devices in secure environments.

[33]. Network Security via Device-Based Consensus Settings

Gregor Freund et al., (2008) describe a method for network security that uses device data to reach consensus on access permissions and control measures, enabling adaptive and collaborative protection mechanisms.

[34]. Sensor-Based Event Detection and Notification System

Adam D. Sager et al., (2014) develop a system that collects data from various sensors, analyzes usage patterns, and sends alerts when anomalies are detected. Notifications can be configured based on user-defined conditions.

[35]. Face Recognition and Bluetooth-Based Community Safety System

Chao Long et al., (2023) combine facial recognition with Bluetooth positioning to verify identities, manage personnel movement, and analyze movement trajectories—contributing to intelligent surveillance and safety management in communities.

[36]. AI-Driven Smart Home Automation Using IoT Sensors

Mageshkumar Naarayanasamy Varadarajan et al., (2024) explore the use of AI and IoT sensors in smart homes to automate devices, boost energy efficiency, and improve security. The paper also discusses privacy, interoperability, and responsiveness challenges.

[37]. IoT-Based Home Automation Using Arduino and AI

Vijaya Bhasker Reddy et al., (2024) present an Arduino-controlled IoT and AI-powered home automation system. It manages devices such as fans, doors, and pumps based on real-time environmental sensor data.

[38]. Survey of IoT Security Mechanisms and Threat Landscape

Francesca Meneghello et al., (2019) provide a comprehensive survey of IoT vulnerabilities, common threats like data breaches and DoS attacks, and various security mechanisms. The study emphasizes the need to embed security at the design stage of IoT systems.

[39]. Multi-Structure Security Cluster Monitoring System

Christopher James Dawson et al., (2009) describe a system that monitors events across a cluster of buildings. It generates real-time status reports, presents the data through a user interface, and transmits updates to relevant devices.

[40]. Wireless Communication Optimization for Security Devices

Geoff Smith et al., (2018) present a wireless communication method for security devices that estimates link latency, enables polling during sleep cycles, and wakes devices efficiently to retrieve queued messages.

[41]. Adaptive Ecosystem Security for Mobile Devices

Qing Li et al., (2013) highlight the rapid adoption of mobile technology across various sectors and the associated security risks. The paper proposes an adaptive ecosystem approach for dynamic threat detection and managing malware and high-risk applications.

[42]. Home Security System Using Subscriber Control and DTMF

Scanner Chen et al., (2000) describe a home security system utilizing a subscriber control circuit that integrates a DTMF receiver, RF receiver, and encoder. The system connects to remote monitors via telephone networks, enabling real-time alerts and control.

[43]. Smart Home IoT Security Vulnerabilities: A Literature and Experimental Review

Brittany D. Davis et al., (2019) conduct a comprehensive review of vulnerabilities in smart home IoT devices, examining physical, software, and encryption threats. The study highlights risks posed by low-cost or underregulated manufacturers.

[44]. Usability and Security of Shared Smart Assistants for Tech-Abuse Survivors

Simon Parkin et al., (2019) evaluate the usability and security of smart assistants like Amazon Echo and Google Home in shared environments. The study focuses on survivors of tech abuse, identifying potential risks and areas for enhanced protection.

[45]. Security Threats in IoT Smart Assistants for Vulnerable Users

Simon Parkin et al., (2019) further investigate shared device security vulnerabilities affecting tech-abuse survivors. Using usability heuristics, the study identifies critical flaws in popular IoT assistants and emphasizes the need for strengthened protections.

[46]. Sensor-Driven Data Analysis and Alert Notification System

Adam D. Sager et al., (2015) present a real-time multi-sensor monitoring framework that analyzes input data and triggers alerts when predefined thresholds or patterns are detected, boosting responsiveness in home security applications.

[47]. Secure Health Kiosk Systems for Community Use

Charles P. Bluth et al., (2009) propose a secure, privacy-conscious health kiosk framework for community deployment. It ensures data confidentiality while supporting remote diagnostics and public health services.

[48]. Rule-Based Security Intelligence and Alerting System

John J. Donovan et al., (2009) introduce an AI-driven monitoring system using rule-based logic and sensor/video input analysis to generate alerts for scenarios such as emergency response and crime prevention.

[49]. Exploiting Security Gaps in Arduino Yun IoT Devices

Carlos Alberca et al., (2016) explore critical security vulnerabilities in Arduino Yun devices through demonstration and analysis. The paper suggests hardening strategies and integration improvements for IoT security.

[50]. Distributed Mobile Security Architecture with Context-Aware Controls

Tirumale K. Ramesh et al., (2013) outline a distributed mobile security framework featuring context-aware routing, anti-tamper mechanisms, and secure authentication managers to ensure robust communication and system governance.

[51]. Security and Privacy in Implantable Medical Devices and Body Area Networks

Michael Rushanan et al., (2014) provide a thorough literature review on the security of implantable medical devices (IMDs) and body area networks (BANs). The paper categorizes key research areas, identifies software and interface vulnerabilities, and discusses using physiological signals to enhance cryptographic entropy.

[52]. Cypider: Community Detection-Based Android Malware Analysis Framework

ElMouatez Billah Karbab et al., (2016) introduce *Cypider*, a novel malware detection system for Android using community detection within similarity graphs. Initial detection accuracy of 50% was improved to 87% through community fingerprinting.

[53]. System for Community-Based Medical Emergency Response

David Barash et al., (2016) describe a mobile-based communication system designed to notify community members of nearby medical emergencies. The system uses GPS-based tracking to mobilize registered responders and enhance survival outcomes in emergencies.

[54]. Collaborative Threat Intelligence Through Secure Network Graphs

Thomas Charles Stickle et al., (2016) propose a network graph-based method for sharing cyber threat intelligence among trusted entities. This collaborative approach increases threat visibility and fosters trust across organizations for improved cybersecurity defense.

[55]. Review of Community-Based Crime Prevention Strategies

Dennis P. Rosenbaum et al., (2006) conduct a comprehensive review of community-based crime prevention programs such as neighborhood watches and environmental design. While widely implemented, these approaches show mixed results, particularly in deterring high-risk individuals.

[56]. Pressure Profiling for Gas Leak Prevention in Distribution Systems

Tahir Javed Butt et al., (2023) explore pressure profiling in gas distribution to detect and prevent leaks. The method demonstrates substantial energy and emission savings, with the potential to supply 16,000 homes from recovered gas annually.

[57]. Technological Progress in Pipeline Theft Detection Worldwide

Harry Smith et al., (2022) review global techniques for detecting pipeline theft, analyzing advances in real-time surveillance, sensor integration, and response systems. The paper also discusses enforcement challenges across varying geographies.

[58]. Community-Led Environmental Monitoring Using Bucket Brigades

Denny Larson et al., (2003) examine grassroots air-quality monitoring efforts in industrial areas through the “bucket brigade” model. The study highlights empowerment through data collection, while also addressing concerns about accuracy and cooperation with government agencies.

[59]. Community Health Volunteers in LMICs: Effectiveness and Challenges

Mirkuzie Woldie et al., (2018) present an umbrella review of 39 studies on community health volunteers (CHVs) in low- and middle-income countries (LMICs). CHVs are often as effective as professionals for basic services but need robust training and supervision for complex care.

[60]. Topic Discovery in Online Health Communities Using NLP and Clustering

Pradeepa Sampath et al., (2020) apply Natural Language Processing (NLP) and clustering methods (K-means++, LDA) to uncover major discussion themes in chronic illness forums. The results help identify patient concerns and improve digital health engagement strategies.

[61]. Role of Community Health Workers in Massachusetts' Healthcare Access

Debi Lang et al., (2014) present a case study on how Community Health Workers (CHWs) supported residents in enrolling in health insurance and accessing primary care under the Affordable Care Act (ACA). The study highlights the significant role CHWs played in achieving high insurance coverage rates in Massachusetts.

[62]. Spatial Fire Risk Modeling for Community Protection

E. Higgins et al., (2013) develop a spatial model with the Merseyside Fire and Rescue Service to identify high-risk individuals using community profiles and a vulnerability index. The study critiques traditional models for lacking precision at the individual level.

[63]. Residential Fire Risk Analysis in Taipei City

Shen-Wen Chien et al., (2007) analyze fire incident records in Taipei and propose strategies for reducing residential fire injuries and property damage, including fire prevention education, arson control, rescue training, and improved decision-support systems.

[64]. Impact Assessment of the HomeSafe Fire Prevention Program

Samar Al-Hajj et al., (2023) evaluate the long-term impact of the HomeSafe fire prevention initiative in Surrey. Results include an 80% reduction in fires, a 60% increase in smoke alarm installations, and a 94% improvement in fire containment, emphasizing the success of firefighter-led outreach programs.

[65]. Bushfire Risk Awareness and Community Behavior in Australia

Jason Beringer et al., (2000) conduct a survey on bushfire awareness and behavior among Australian residents. The study reveals significant gaps in risk perception, particularly among new residents, and calls for enhanced public education and localized preparedness efforts.

[66]. Fire Management Challenges in Developing Countries

Sotir Shuka et al., (2017) review fire risk management in underdeveloped regions such as the Balkans. The study highlights challenges related to infrastructure, public education, and emergency response capacity, and emphasizes the need for international collaboration and investment.

[67]. Community-Focused Fire Prevention with Spatial and Social Targeting

M. Taylor et al., (2022) describe Merseyside's targeted fire prevention strategy. By combining spatial data with social group analysis, the program focuses on high-risk households through home safety checks, behavioral interventions, and community engagement campaigns.

[68]. Collaborative Fire Safety Outreach in Norristown

Camille Stewart et al., (2015) document a community fire prevention initiative in Norristown. Through partnerships, the initiative delivered fire safety education, installed alarms, and reached over 600 homes and 1,000 residents, showcasing the impact of coordinated local action.

[69]. Remote Security Management via Central Monitoring Stations

Terry Wenzel et al., (2003) present a centralized kiosk-based security solution. Featuring audio and video capabilities, the system allows remote visitor verification and security event recording, offering an efficient and scalable approach to personal and facility security.

[70]. Wireless Personal Security Network with Web Integration

Michael J et al., (2003) describe a web-enabled personal security system that links wireless sensors and alarm devices. The platform supports real-time monitoring, alert customization, and remote access, enhancing personal and household safety management.

[71]. Private Virtual Dynamic Network for Seamless Integration

S. Hasan *et al*., (2011) propose a secure virtual dynamic network that enables devices on public or private networks to connect to private enterprise intranets. This system allows seamless cross-network communication via an agent without requiring extra hardware/software, giving users the experience of a unified private network.

[72]. Monitoring Device with Multiple Sensors and Network Connectivity

D. Adam *et al*., (2019) introduce a multi-sensor monitoring device housed in a single unit. It detects environmental factors like temperature, air quality, and light, processes data internally, and transmits it wirelessly for remote access and analysis. The device is easy to install and eliminates the need for wiring.

[73]. Proximity-Based Security System Using Tethering Devices

F. H. Petitt *et al*., (2015) describe a system involving wearable or portable tethering devices linked to a primary control device. It includes proximity detection and alert mechanisms that trigger when devices move beyond a defined range, helping enhance personal security through real-time monitoring.

[74]. Low-Cost IoT Security Solution Using Arduino UNO and SMS

L. de A. Carneiro *et al*., (2019) present a budget-friendly IoT solution for burglary alerts in Palmas, Brazil. Utilizing Arduino UNO and SMS communication, the device sends alerts for unauthorized entry and supports collaboration with the Military Police to improve community safety via real-time response.

[75]. Location-Based Secure Data Extraction and Encryption

R. M. Redlich *et al*., (2007) propose a method for protecting sensitive data by extracting it from mobile devices when they exit a designated area. The data is encrypted and accessible only with a specific clearance and physical proximity. The system includes software instructions for location-sensitive data management.

[76]. Neighborhood Radio Communication for Emergency Alerts

T. Z. Seales *et al*., (2006) design a base unit security system capable of detecting emergencies like intrusion or fire. The unit communicates with neighboring base units through radio signals, broadcasting alarms and voice alerts to coordinate immediate community response.

[77]. Video Notarization for Secure Cryptographic Key Protection

A. Libonati *et al*., (2017) introduce a remote video notarization system to verify user identity and protect cryptographic keys on mobile devices. The notary does not access the keys directly, enhancing security. A user study confirms the approach's effectiveness in preventing theft-related data compromises.

[78]. Blockchain-Based IoT Community Safety System

C.-L. Chen *et al*., (2021) develop a blockchain-secured system for processing IoT-based alarms in residential and public spaces. It ensures secure and verifiable responses, guarding against interception, tampering, and replay attacks. The approach aims to bolster community safety and trust in IoT infrastructure.

[79]. Community-Based Anomaly Detection via Data Triangulation

B. P. *et al*., (2019) present a surveillance system using triangulation across data protocol, user behavior, and packet content to detect security anomalies like data exfiltration or steganography. The system is deployable in distributed environments and supports collaborative network security monitoring.

[80]. Security Vulnerability Analysis of SmartThings Platform

E. Fernandes *et al*., (2016) conduct an empirical study of the SmartThings platform, analyzing apps and device handlers. They identify critical flaws such as overprivileged apps and exposed sensitive data, offering insights into secure smart home design and platform governance.

[81]. Lightweight Authorization Stack for Smart Home IoT Devices

B.-C. Chifor *et al*., (2017) propose a user-centric security model for smart homes. The system uses a lightweight cloud-connected authorization stack that defers user commands to smartphones for approval. It addresses trust issues with cloud services and is compatible with heterogeneous IoT ecosystems.

CHAPTER 3: PROPOSED SYSTEM

3.1 System Requirements

The proposed system integrates both hardware and software components to provide a comprehensive home and community safety solution. The hardware includes sensors, a microcontroller, an alert mechanism, and a display, while the software leverages MQTT communication for real-time data transfer, ensuring alerts reach the intended recipients.

3.2 Hardware Components:

- ESP8266 Microcontroller: This acts as the core processor, enabling Wi-Fi communication and interaction with sensors.
- Gas, Fire, and Motion Sensors: Detect various safety hazards such as gas leaks, fires, and unauthorized movement. The gas sensor monitors gas levels, while the flame sensor detects fire hazards.
- Buzzer and OLED Display: The buzzer sounds when an alert is triggered, and the OLED display shows real-time information, including the status of the sensors and system alerts.
- Buttons for Theft and Health Alerts: Physical buttons on the system trigger theft or medical alerts when pressed, while users can also send alerts via a mobile or web app interface.

3.3 Software Components:

- MQTT (Message Queuing Telemetry Transport): A lightweight messaging protocol used for communication between devices. The system uses MQTT to send real-time alerts about detected hazards to other houses and authorities.
- Mobile & Web App Interface: A user-friendly interface allows users to monitor and manage their security system remotely. Alerts triggered by various sensors are sent to this interface, allowing for prompt action.
- AI-based Pattern Recognition: Future integration may include AI algorithms to predict potential threats based on sensor data patterns, improving the system's proactive capabilities.

3.4 *Communication Flow:*

- Sensor Data → ESP8266: The sensors (gas, flame, motion) collect data continuously and send it to the ESP8266.
- ESP8266 → MQTT: The microcontroller sends the sensor data to an MQTT broker. It communicates any triggered alert to connected devices, including other houses and authorities.
- MQTT → Mobile & Web App: The mobile and web applications display the alerts from the MQTT messages, notifying users of critical events. Users can acknowledge or act on the alerts through the app interface.
- Alert Sharing to Surrounding Houses: The system ensures that any detected emergency, such as fire, gas leak, or theft, is communicated to neighboring houses (e.g., House 1 and House 2 in the prototype). This information helps in coordinating a quick response within the community.
- Community-Wide Communication: In a real-life scenario, the system would secure an entire community by sharing alerts with other houses and authorities, enabling coordinated action in the event of an emergency.

3.5 *Working Principle:*

The system works by continuously monitoring various safety parameters such as gas levels, flame presence, and motion. When a hazard is detected:

- The system triggers an alert by sounding the buzzer and activating the visual alert on the OLED display.
- The event is communicated to the MQTT broker, which broadcasts the alert message to the connected systems.
- Neighbour's (House 1, House 2) are notified of the event, allowing them to respond or provide assistance.
- The mobile or web app interface receives the alert and provides users with details, allowing them to acknowledge or take action.

This proposed system is scalable to cover entire communities, enhancing both individual and collective safety by ensuring rapid, coordinated responses to emergencies.

CHAPTER 4: DESIGN & IMPLEMENTATION

4.1 PROTOTYPE DESIGN:

The prototype integrates various sensors and communication mechanisms to detect emergencies like theft, medical issues, gas leaks, and fires. The setup includes the following components:

Hardware Setup:

- **Microcontroller**: ESP8266 (NodeMCU)
- **Sensors**: Flame Sensor, Gas Sensor (MQ-2), Theft Button, Medical Button
- **Display**: OLED screen (for displaying alerts and status)
- **Buzzer**: Used for audio alert during emergencies
- **LEDs/Indicators**: To visually indicate the system's status (active alert or safe)
- **Wi-Fi**: Communication between devices via MQTT protocol
- **Backup Power**: Solar-powered backup to ensure continuous operation
- **Communication System**: MQTT protocol for message exchange, and mobile/web apps for user interaction

The components are linked using MQTT messaging, allowing **real-time alerts** to be shared between House 1 and House 2, and **community-wide** alerts in real-world applications. Show in Fig:4.1.

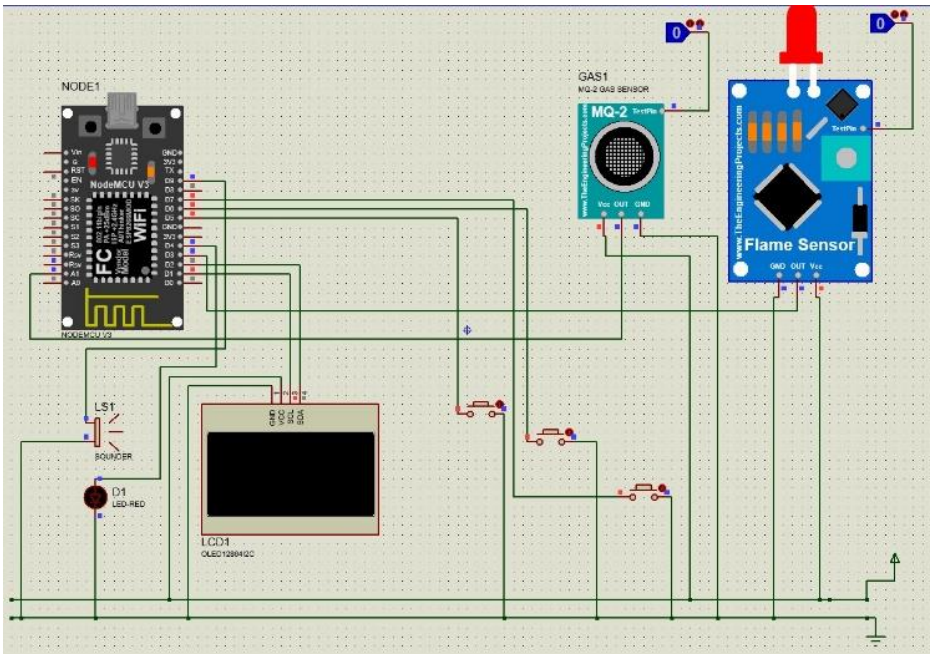


Fig:4.1 Circuit Diagram & Hardware Setup

4.2 TESTING SCENARIOS:

The proposed AI-integrated safety system was evaluated under various emergency simulations to verify its efficiency, accuracy, and power consumption. The gas leak detection scenario involved using an MQ-2 gas sensor, with alerts triggered when sensor readings exceeded a threshold of 800 ADC units. The response time averaged 2.5 seconds, ensuring timely hazard identification and communication. In theft and medical emergency simulations, emergency alerts were activated through dedicated buttons or mobile commands, achieving response times of 1.5s and 1.2s respectively. The fire detection system, equipped with a flame sensor, issued alerts when infrared radiation intensity surpassed a set threshold, recording an average response time of 3.0 seconds. Across all scenarios, the system demonstrated real-time performance capabilities. Accuracy and reliability were validated through repeated tests, yielding high accuracy and low false alarm rates—ranging from 1% to 3% across different sensors. Additionally, power consumption was analyzed in both active and idle modes, with the ESP8266 microcontroller consuming the most power, while buttons and sensors showed minimal draw. This comprehensive testing confirms the prototype's efficiency, responsiveness, and energy suitability for real-world deployment in community safety applications.

4.2.1 GAS LEAK SIMULATION:

- The gas leak scenario is simulated by monitoring the analog output from the gas sensor (MQ-2). If the gas level exceeds a threshold (set at 800 in the code), the system triggers an alert.
- where the Analog Reading is the ADC value of the sensor (between 0 and 1023), 1023 is the ESP8266's maximum ADC resolution, and 100 converts the value into a percentage. An 800 ADC unit threshold is predefined, above which an alert is issued, triggering the notification system through MQTT and IoT platforms. Experimental testing proved the average response time to be 2.5 seconds, facilitating real-time detection of hazards and instant emergency communication.
- Formula for Gas Leak Calculation:

$$Gas\ Level = \frac{\text{Analog Reading}}{1023} 100 \quad (1)$$

This formula normalizes the sensor reading (0 to 1023) to a percentage value (0% to 100%).

4.2.2 THEFT BUTTON/ MEDICAL BUTTON:

- The theft emergency/medical emergency is triggered either by the manual button press or a Mobile app. The system sends a "Theft Emergency" alert to nearby houses and authorities.
- A medical emergency is triggered using a manual button. The system sends an alert notifying all connected households about the emergency. If there is a pre-configured medical alert (via app), the system sends the same alert.
- The response time is measured from button press to the activation of the alarm and notification on the mobile app.
- The activation status (E_a) the emergency system is defined as:

$$(E_a) = \begin{cases} -1, & B_p > 0 \; or \; M_c = 1 \\ 0, & otherwise \end{cases} \quad (2)$$

- where B_p represents the button press input, and M_c denotes a mobile command. The response time (R_t) is given by

$$R_t = t_a - t_p \quad (3)$$

- where t_p is button press or mobile command time, and t_a is alert initiation time. As noted in Table 1, the system achieves an average of 1.5s in response time to theft emergencies and 1.2s in response time for medical emergencies, maximizing real-time emergency communication.

4.2.3 FIRE DETECTION USING FLAME SENSOR:

- The theft emergency/medical emergency is triggered either by the manual button press or a Mobile app. The system sends a "Theft Emergency"/" Medical Emergency" alert to nearby houses and authorities.
- The response time is measured from button press to the activation of the alarm and notification on the mobile app.

$$(F_d) = \begin{cases} 1, & I_f > T_f \\ 0, & I_f \leq T_f \end{cases} \quad (4)$$

- where I_f represents the infrared intensity observed, and $T_f$denotes the threshold intensity. Response time (R_t) can be found from:

$$R_t = t_a - t_d \quad (5)$$

- where t_d stands for fire detection time, and t_a is alarm-activation time. Table 4.1 shows observed response times of which the mean of 3.0s gives an efficient response to an emergency.

Scenario	Average Response Time (s)	Minimum Response Time (s)	Maximum Response Time (s)
Gas Leak Detection	2.5s	2.2s	3.0
Fire Detection	3.0s	2.7s	3.5s
Theft Button Press	1.5s	1.2s	1.8s
Medical Emergency	1.2s	1.0s	1.4s

Table 4.1: Response Time for Different Scenarios

4.2.4 TESTING ACCURACY SCENARIOS:

Accuracy: The accuracy of the sensors in detecting emergencies is critical. The flame sensor and gas sensor accuracy are evaluated based on false positive/negative rates. The goal is for minimal false alarms. Results from experiments can be shown using the following formulas:

Accuracy Calculation:

$$\textbf{Accuracy} = \frac{\textbf{True Alerts}}{\textbf{Total Alerts}} \boldsymbol{x100} \qquad (6)$$

For gas and fire detection, accuracy will be based on whether the system correctly identifies a hazardous event (e.g., gas leak, fire) Show in fig:4.2.

Response Time:

The time between detection and the activation of the emergency response (alert trigger and mobile notification). This can be calculated as:

Response Time Formula:

$$\text{Response Time} = \text{Time Alert Triggered} - \text{Time Hazard Detected}$$

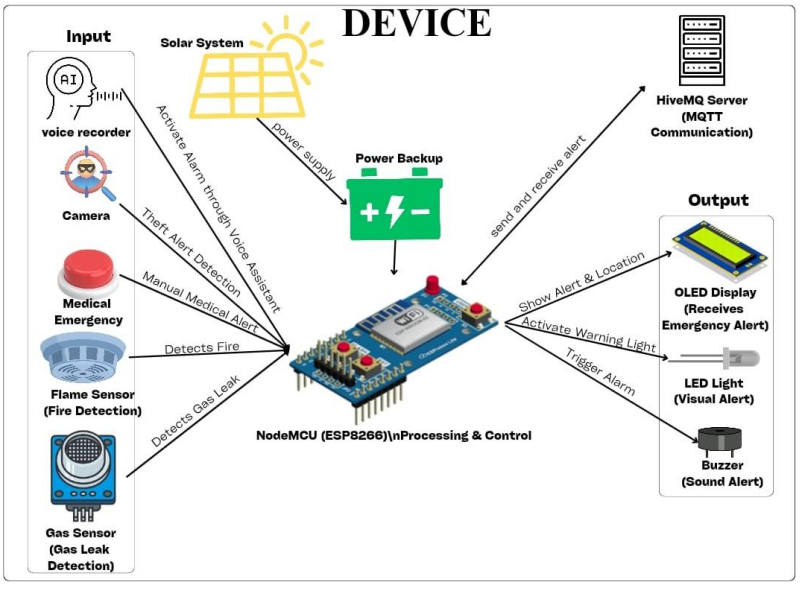


Fig:4.2 **TESTING ACCURACY SCENARIOS**

4.2.5 FALSE ALARMS:

False alarms are measured by triggering the system in controlled conditions where no actual hazard exists (e.g., using a fan for the flame sensor). The false alarm rate is calculated as:

$$\text{False Alarm Rate} = \frac{\text{False Alarms}}{\text{Total Tests}} X\mathbf{100} \qquad (\mathbf{7})$$

Sensor	False Alarms (%)
Gas **Sensor**	2%
Flame Sensor	3%
Theft Button	1%
Medical Button	1%

Table 4.2: False Alarm Rate

4.2.6 POWER CONSUMPTION:

The power consumption is measured in terms of energy used in alert and idle states. The formula is as follows:

$$\textbf{Power Consumption} = \textbf{Power Usage in Alert State} \times \textbf{Alert Duration} \qquad (\mathbf{8})$$

The power measurements for both idle and active states are taken for each component to estimate total energy consumption.

Component	*Idle Power (mA)*	*Active Power (mA)*	*Power Consumption (mWh)*
ESP8266 (Microcontroller)	70	180	0.5
Buzzer	0	60	0.2
Gas Sensor	10	20	0.1
Flame Sensor	3	10	0.05
Medical Button	1	3	0.02
Theft Button	1	3	0.02
LED Indicators	5	15	0.1
OLED Display	10	30	0.15

Table 4.3: Power Consumption Estimates

This analysis provides key insights into the performance and energy efficiency of the system These results can be compared with existing smart safety systems to evaluate the effectiveness of the prototype and its potential for real-world applications.

4.3 DESIGN:

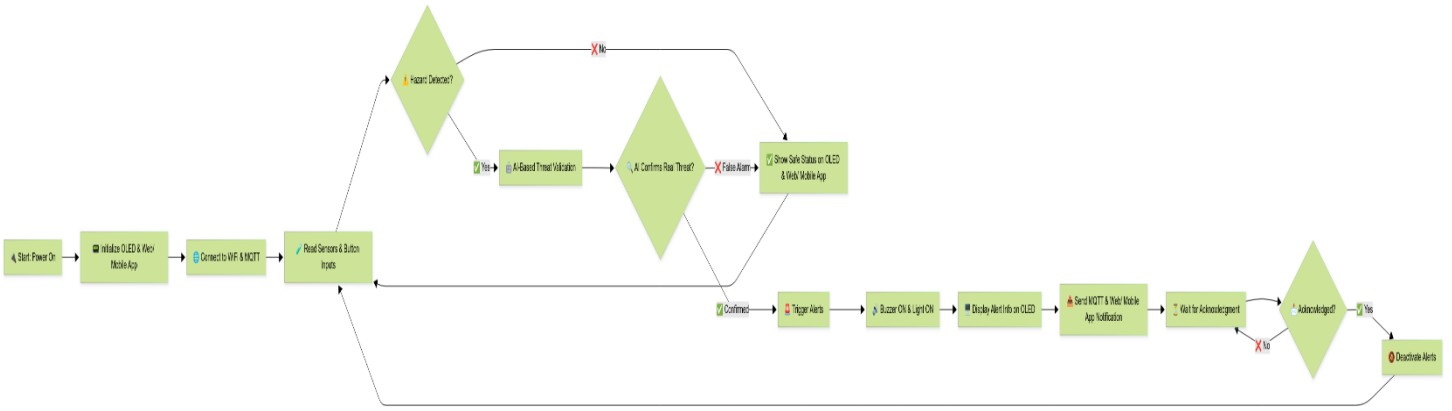


Fig:4.3 Represents Architecture Diagram

In Fig:4.3 Architecture Diagram has been showcased. The architecture diagram for the AI -Integrated Home and Community Protection System illustrates the operational workflow of the project, focusing on how residents interact with the system to ensure their safety and the rapid response from authorities. When a Resident encounters an emergency, such as a theft or medical crisis, they can activate the device using either a manual button or a voice command. This action triggers the system to send an alert through a Wireless Communication Network that operates within a 1 km radius, connecting nearby residents who may also be part of the community safety network. Once the alert is activated, the system transmits a signal to the Central Server, which acts as the hub for processing the information and coordinating responses.

The Central Server then utilizes the wireless communication capabilities to notify both the Neighbors and the relevant Authorities, including police, fire department, and medical services. This alert system ensures 36 that help is dispatched quickly and efficiently, minimizing response time in emergencies. The communication occurs seamlessly, as the system is designed to manage multiple incoming alerts and disseminate the necessary information to relevant parties in real-time.

Additionally, the use of solar-powered mechanisms ensures that the system remains operational during power outages, enhancing its reliability. Overall, the architecture supports a robust, community-centric approach to safety, allowing residents to rely on immediate assistance while fostering collaboration among neighbors and local authorities.

4.3.1 Data Flow Diagram (DFD)

Data Flow Diagrams (DFDs) at different levels to illustrate how the AI-Integrated Home and Community Protection System operates. These DFDs will showcase the flow of information within the system, from user interaction to device communication and emergency response mechanisms. DFD Level 0 (Context Diagram) The Level 0 DFD (also known as the Context Diagram) provides a high-level overview of your AI-Integrated Home and Community Protection System. It illustrates the interaction between the system and external entities, capturing the main data flows between them

(Fig:4.4).

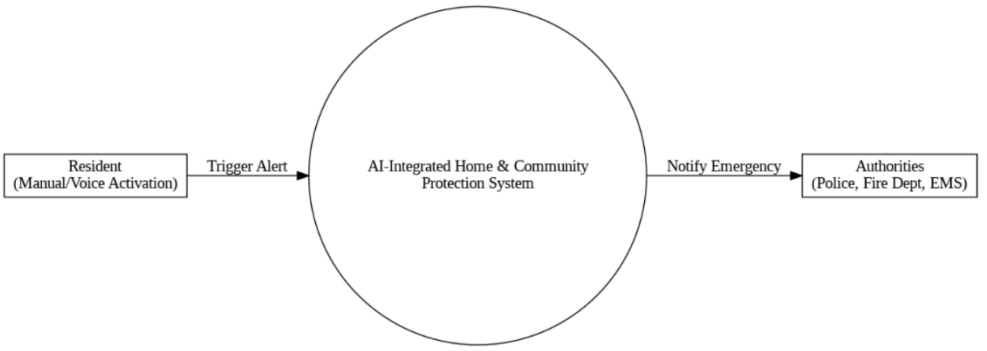


Fig 4.4: Level 0 DFD

The AI-Integrated Home & Community Protection System is designed to function as a centralized emergency response mechanism within residential environments. It integrates residents, emergency authorities, and smart sensors into a cohesive framework that enables real-time hazard detection and alert dissemination. The system is structured around two key entities—Residents and Authorities—with a centralized AI-based platform managing communication and decision-making processes.

Residents are the primary users of the system, empowered to initiate emergency alerts during critical incidents such as fire outbreaks, theft attempts, or medical emergencies. These alerts can be triggered either manually through physical buttons or remotely via voice commands, depending on the situation and the accessibility of the resident at the time of the event. Upon activation, the alert is processed by the system, which then initiates a sequence of responses, including notifying nearby households and community members, thereby creating a localized early warning system.
Authorities refer to external emergency response services, including the Police, Fire Department, and Emergency Medical Services (EMS). The AI-integrated system communicates directly with these authorities during confirmed emergency events. When a valid alert is received, the system analyses the data from connected sensors or manual inputs and then relays essential information—such as the type of emergency and the resident's location—to the relevant department. This ensures a quick and targeted response, significantly reducing the time taken for emergency personnel to reach the scene. At the heart of the operation lies the AI-Integrated Home & Community Protection System, which serves as the central processing and communication unit. It is responsible for receiving alerts, validating them using data from gas sensors, flame sensors, and other monitoring devices, and determining the urgency level of the situation. Based on this evaluation, it either raises a local community alert or escalates the situation by notifying official emergency services. The system also supports two-way communication, allowing for updates and responses to be sent back to residents when necessary.

From a data flow perspective, the Level 0 Data Flow Diagram (DFD) includes two primary information paths. The first, Trigger Alert, originates from the resident, where an emergency is manually or vocally reported to the system. The second, Notify Emergency, is initiated by the system once it verifies the emergency condition, prompting immediate notification to the appropriate authority—whether it be the police

for a theft incident, the fire department for a blaze, or EMS for a medical situation. These structured data exchanges ensure swift and intelligent decision-making in potentially life-threatening scenarios.

.

4.3.2 Level 1 DFD

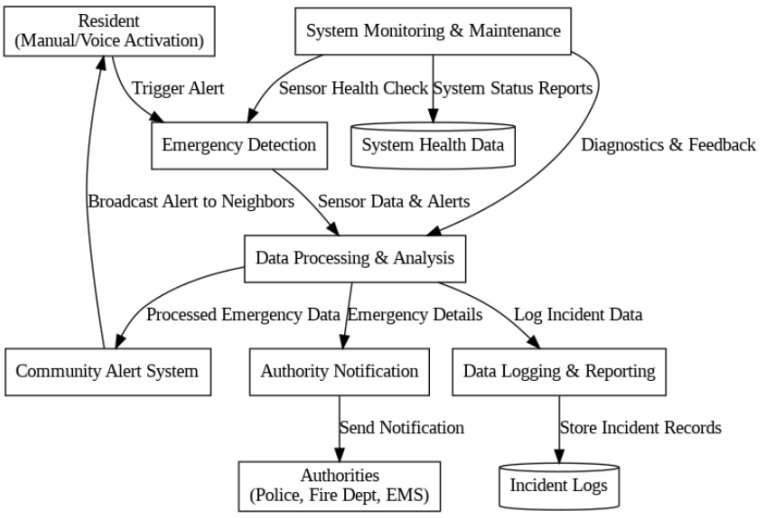


Fig 4.5: Level 1 DFD

The Level 1 Data Flow Diagram (DFD) offers a more granular view of the AI-Integrated Home & Community Protection System by decomposing the overall system into its key internal processes. It illustrates the flow of information between various subprocesses, data stores, and the primary external entities—Residents and Authorities. This level of the DFD provides detailed insight into how different components interact within the system to ensure effective emergency detection, communication, and response (see Fig. 4.5). The first core process is Emergency Detection, which serves as the system's initial input interface. This module identifies critical events such as theft, fire, gas leaks, or medical emergencies. Detection is achieved through both hardware sensors and manual or voice-activated alerts from residents. The inputs for this process include sensor readings and user-triggered commands, which result in emergency signals being sent to the central processing unit for further action. The Data Processing & Analysis process plays a vital role in interpreting the raw data received from the emergency detection layer. It determines the nature and severity of the emergency by analysing sensor inputs and resident alerts. The processed data is then forwarded to the relevant alert mechanisms for appropriate dissemination. This ensures that every emergency type is handled with the correct urgency and method of response.

Following this, the Community Alert System is activated. Its primary function is to inform nearby households and community members—typically within a 1-kilometer radius—about the ongoing emergency. This is done using audio-visual signals such as sirens and LED indicators, along with digital alerts delivered via mobile notifications. It receives processed emergency data as input and outputs broadcast alerts to all linked community devices. Another critical component is the Authority Notification module. This process is responsible for escalating confirmed emergencies to the appropriate external emergency services. Based on the analysis results, it contacts the Police, Fire Department, or Emergency Medical Services (EMS), supplying them with essential

information including the type of incident and the precise location. This automated communication drastically improves response times during life-threatening situations. The system also incorporates a Data Logging & Reporting process, which maintains a comprehensive log of all incidents, sensor data, alert triggers, and response times. This data is invaluable for performance assessment, generating reports, and identifying opportunities for future improvements. It inputs processed alert and system activity data and outputs detailed analytics and reports. Lastly, the System Monitoring & Maintenance process ensures the continuous reliability and performance of the system. It tracks the operational status of sensors, monitors system health, and detects connectivity issues. The outputs from this module include maintenance alerts, error logs, and real-time system diagnostics. This proactive maintenance capability enhances system uptime and prevents failures during emergencies. Together, these six processes form the backbone of the system's internal operations, ensuring robust and intelligent management of emergency events from detection to resolution.

4.3.3 Level 2 DFD

In a Level 2 DFD, processes are typically broken down to show how data is transformed within the system. Here's an updated approach that includes processes, data stores, and interactions

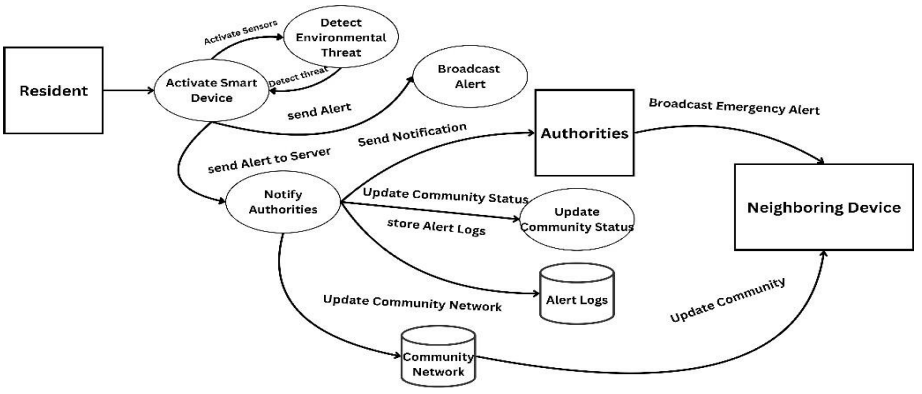


Fig 4.6: Level 2 DFD

1.Processes:

These represent actions or transformations that occur in the system.

- **P1:** Activate Smart Device
- **P2:** Detect Environmental Threat
- **P3:** Broadcast Alert
- **P4:** Notify Authorities
- **P5:** Update Community Status

2.Data Stores:

- **DS1:** Alert Logs (stores the alerts and responses)
- **DS2:** Community Network (stores neighbor communications)

3.External Entities:

- **Resident** (initiates alerts)
- **Authorities** (respond to notifications)
- **Neighbors** (receive updates)

4.Processes and Data Flow:

- The **Resident** triggers the **Smart Device** (P1).
- The **Smart Device** (P1) activates the sensors (P2), and they detect any environmental threat.
- **Smart Device** sends alerts to the **Wireless Network**, which broadcasts the alert to the **Neighbors** (P3).
- Alerts and data are sent to the **Central Server** (P4), which notifies **Authorities**. The server also stores logs in **Alert Logs** (DS1).
- The **Server** also updates the **Community Network** (DS2) with status updates (P5).

4.4 UML DIAGRAMS

4.4.1 Use Case Diagram

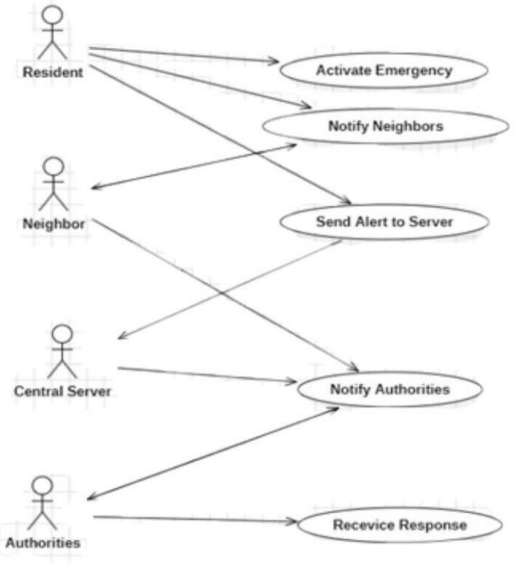


Fig 4.7: Use Case Diagram

In Fig:4.7 Use Case diagram has been done. The Use Case Diagram represents the interactions between various actors and the system within the context of an AI-Integrated Home and Community Protection System. In this diagram, the Resident is the primary user who initiates the process by activating an

emergency alert. This action triggers the system to send an alert to the Central Server, which coordinates the response. The Central Server plays a crucial role in notifying both the Authorities—including police, fire department, and medical services—and the Neighbors.

By including both authorities and neighbors, the system promotes a community-oriented approach to safety, ensuring that immediate assistance can be mobilized quickly. Additionally, the Authorities have a feedback loop, allowing them to respond back to the system, which aids in assessing the situation and ensuring that the necessary resources are deployed effectively. This diagram highlights the collaborative nature of the system, illustrating how various stakeholders work together to enhance community safety and responsiveness in emergency situations.

4.4.2 Class Diagram

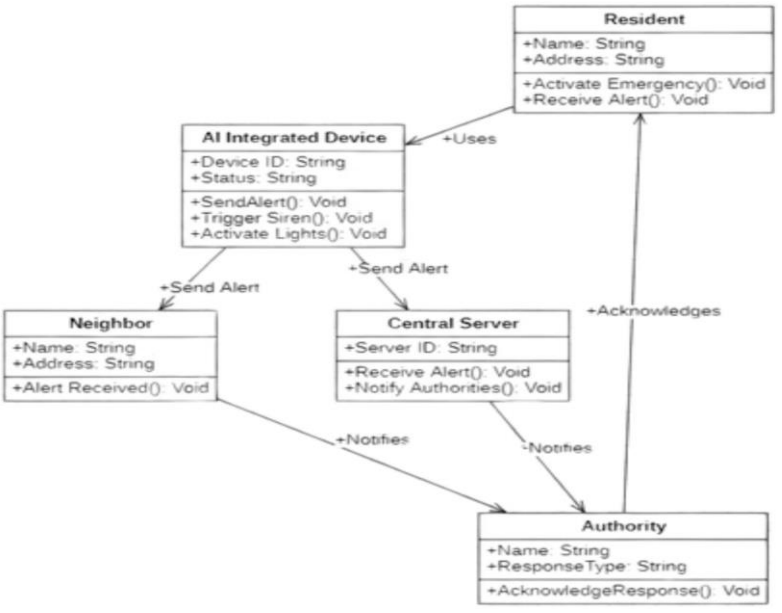


Fig 4.8: Class Diagram

In Fig:4.8 Class diagram has been done. The class diagram for the AI-Integrated Home and Community Protection System visually represents the structure and relationships between various entities involved in the system. It highlights five key classes: Resident, AI Integrated Device, Central Server, Authority, and Neighbor, each encapsulating specific attributes and methods that define their roles within the safety framework. The Resident class represents the end-users of the system, who can activate emergency responses and receive alerts. The AI Integrated Device class encapsulates the smart technology that triggers

alarms and notifications, demonstrating its capabilities such as triggering sirens and activating lights. The Central Server serves as the core component that processes alerts from the devices and communicates with both authorities and neighbors, thereby facilitating a coordinated response during emergencies. The Authority class symbolizes the various emergency services, such as police and medical responders, that are notified by the server, highlighting the system's role in enhancing public safety. Finally, the Neighbor class indicates community involvement, showing how alerts are shared among residents to foster collaboration in crisis situations. This diagram not only delineates the functional components and their interactions but also underscores the system’s goal of leveraging technology to improve community safety and responsiveness, ultimately aligning with the broader objectives of urban resilience and sustainable living. By visually mapping these relationships, the class diagram serves as a foundational blueprint for developing the software architecture and ensuring that all aspects of the community safety solution are integrated effectively.

4.4.3 Sequence Diagram

In Fig:4.9 Sequence diagram has been done. The sequence diagram illustrates the process of activating an AI-Integrated Emergency Device within a residential setting, highlighting the critical interactions between various components involved in responding to an emergency situation. Initially, the Resident activates the emergency system, prompting the AI-Integrated Device (AID) to respond by triggering sirens and activating solar lights to signal the alarm. Following this, the AID transmits an alert to the Central Server, which serves as the communication hub for the emergency response. The server then interacts with the Twilio API to send an alert to the relevant authorities, such as police, fire departments, and medical services. The Twilio API confirms the successful transmission of the message back to the server, ensuring the alert was received. Subsequently, the Central Server notifies the Authorities, prompting them to acknowledge the receipt of the alert. This acknowledgment is sent back to the server, completing the communication loop.

Finally, the AI-Integrated Device notifies the resident that the emergency activation has been successfully processed, ensuring that all necessary parties are informed and prepared to respond effectively to the emergency situation. This sequence emphasizes the streamlined communication and rapid response capabilities of the AI-integrated safety system, enhancing community safety and emergency preparedness.

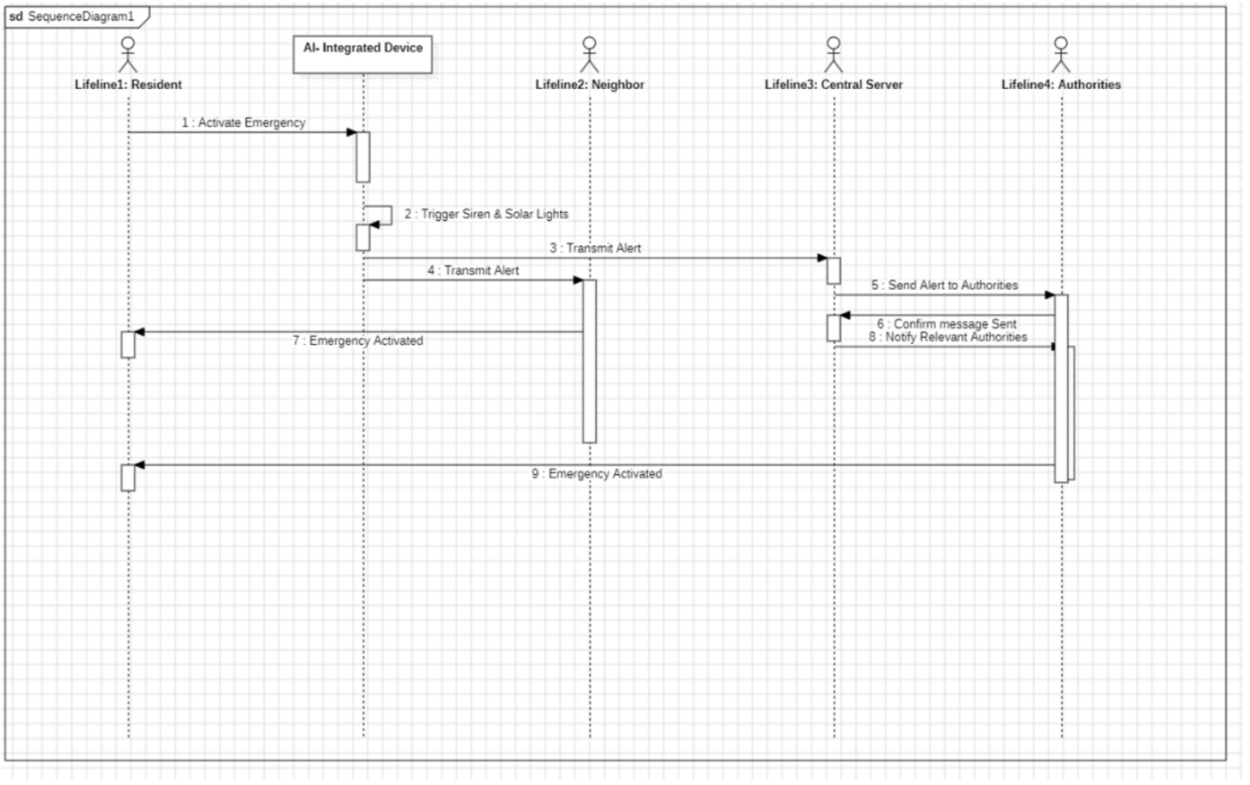


Fig 4.9: Sequence Diagram

4.4.4 *Activity Diagram*

The Activity Diagram visually represents the workflow and interactions involved in the emergency alert process within the AI-Integrated Home and Community Protection System. This system is designed to enhance community safety by providing a rapid response mechanism when an emergency situation arises. Below is a breakdown of the activities depicted in the diagram (Fig:4.10):

- ***Start (Black Circle)***

This is the starting point of the process, indicating the beginning of the emergency response workflow.

- ***Resident Activates Emergency Alert***

A resident identifies an emergency situation and triggers the alert system. This can be done through various means like pressing an emergency button, using a voice command, or activating it through a mobile application. This is the critical initial action that sets the entire system into motion.

- ***System Triggers Siren and Solar Lights***

Explanation: Once activated, the system responds by turning on loud sirens and flashing solar-powered lights. These are designed to:
Alert the Surroundings: The noise and lights alert people nearby to the emergency. Deter Intruders: In cases of theft, this may scare away potential intruders.

- ***Fork Node (Splits the Process)***

Explanation: The process splits into two parallel actions, ensuring multiple alert channels are activated simultaneously.

- ***Send Alerts to Nearby Neighbors***

The system sends notifications to all registered smart devices in neighboring homes. These alerts inform nearby residents about the emergency, encouraging them to check on the affected household or offer assistance.
This creates a network of community support, potentially leading to faster on-the-ground responses.

- ***Send Alert to Server Room***

The system also sends a detailed alert to a centralized server. The server logs the incident for record-keeping and monitoring purposes.
This action ensures that data about the emergency is captured for further analysis and response coordination.

- ***Send Alert to Authorities***

After sending alerts to neighbors and logging it in the server, the system notifies the relevant authorities. This could include the police, fire department, or emergency medical services, depending on the type of emergency detected.

The alert sent to authorities includes key details such as the location and nature of the emergency, enabling a swift and targeted response.

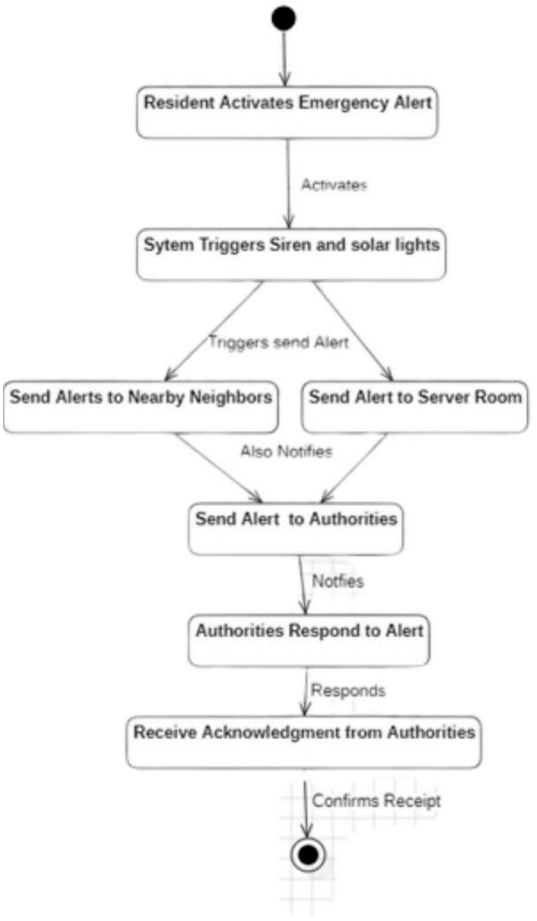


Fig 4.10: Activity Diagram

- ***Authorities Respond to Alert***

Once the authorities receive the notification, they acknowledge the alert and prepare to respond to the situation. This acknowledgment is crucial as it confirms that the emergency alert has been received and that help is on its way.

- ***Receive Acknowledgment from Authorities***

The system waits for a response from the authorities. Upon receiving a confirmation, the system logs this acknowledgment, ensuring that residents are aware that their alert was successfully communicated. This step closes the communication loop, providing assurance to the affected individuals.

- **End (Black Circle with Border)**

This marks the conclusion of the process. The system resets after the authorities' acknowledgment, ready to handle any future emergencies. The

emergency alert cycle is now complete.

4.4.5*Communication Diagram*

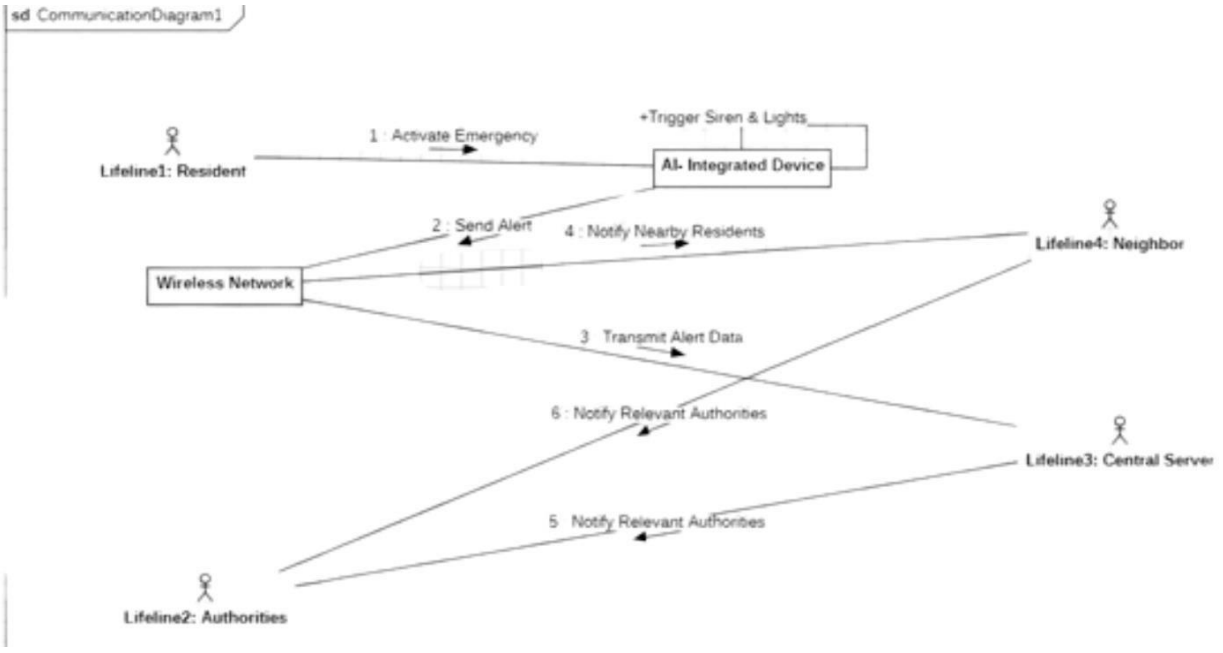


Fig 4.11: Communication Diagram

In Fig:4.11, Communication diagram illustrates the operational workflow the process begins with Lifeline1: Resident, who detects an emergency, such as a fire, medical issue, or break-in, and activates the AI-Integrated Device using a physical button, voice command, or mobile application. This activation triggers the system to sound a loud siren and flash solar-powered lights, thereby alerting the community through audible and visual signals. Once the emergency alert is activated, the device uses a Wireless Network to broadcast notifications. It immediately sends alerts to Lifeline4: Neighbor, using SMS or app notifications, ensuring that nearby residents are aware of the situation and can respond promptly. Simultaneously, the system transmits detailed emergency data, including the type of incident, location, and timestamp, to Lifeline3: Central Server. This central server not only logs the data for record-keeping and future analysis but also coordinates responses by automatically forwarding the alerts to Lifeline2: Authorities, such as the police, fire department, or medical services.

The system employs a dual notification mechanism for enhanced reliability. While one communication pathway sends alerts directly to Lifeline3: Central Server, another pathway simultaneously notifies Lifeline2: Authorities through the wireless network. This redundancy ensures that even if one communication channel fails, critical emergency information still reaches the authorities without

delay. Upon receiving the alert, the authorities acknowledge receipt, confirming that emergency responders are on their way. This acknowledgment is sent back through the network to the central server and ultimately to the resident, closing the communication loop and providing reassurance that help is enroute.

Overall, the AI-Integrated Safety System leverages AI and IoT technologies to create a robust emergency response network. By integrating real-time community alerts (Lifeline4: Neighbor), centralized data management (Lifeline3: Central Server), and rapid authority notifications (Lifeline2: Authorities), the system not only reduces response times but also fosters a collaborative approach to community safety, aligning with the principles of smart city infrastructure and sustainable urban development.

4.4.6 *Deployment Diagram*

In Fig:4.12, the deployment diagram for the AI-Integrated Home and Community Protection System illustrates a sophisticated architecture designed to enhance safety and

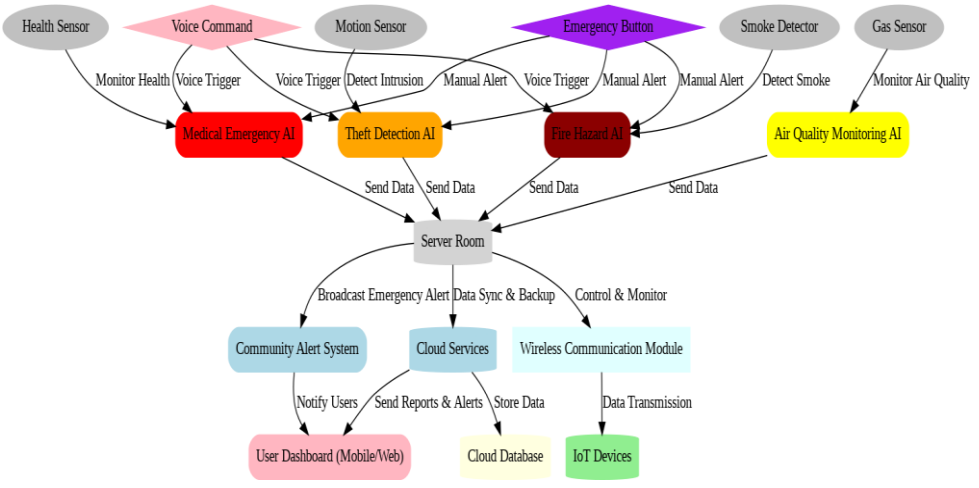


Fig 4.12: Deployment Diagram

emergency response within urban environments. At the core of the system, Cloud Services act as the central repository, managing all data and facilitating communication between system components and users. The cloud houses a Cloud Database that stores historical data, system logs, and analytics for long-term access, ensuring critical information is available for future reference and reporting. The User Dashboard is part of the cloud services, offering real-time alerts and safety reports to users through a web or mobile interface. This dashboard serves as a vital tool for users to monitor system status and

receive notifications about ongoing or past safety incidents. Beneath the cloud layer, the Server Room is responsible for processing data locally, enabling real-time decision-making for emergency situations. This server room houses several AI Modules that specialize in specific safety scenarios. The Theft Detection AI analyzes data from motion sensors to identify suspicious movements, potentially signaling a break-in or theft. The Medical Emergency AI processes health data from sensors to detect signs of medical distress, such as abnormal heart rates or falls. The Fire Hazard AI uses data from smoke detectors to identify potential fire risks, while the Air Quality Monitoring AI processes gas sensor data to detect hazardous conditions like gas leaks or poor air quality. The server room ensures that all incoming data from IoT Devices, such as motion sensors, smoke detectors, and health monitors, is processed immediately for quick response times. In the event of an emergency, the server room triggers alerts to the Community Alert System, notifying nearby residents and authorities about the situation.

The IoT Devices form the physical network of sensors deployed throughout homes and communities. These devices include Motion Sensors for detecting movement, Gas Sensors for monitoring air quality, Smoke Detectors for fire detection, and Health Sensors for monitoring users' vital signs. These sensors wirelessly transmit real-time data to the server room, where it is processed by the AI modules. The Wireless Communication Module plays a crucial role in maintaining seamless communication between all IoT devices, the AI modules in the server room, and the AI-Integrated Devices used by the residents. This module ensures continuous data flow and enables the system to act promptly in emergencies.

The AI-Integrated Device serves as the user interface, allowing users to interact with the system during emergencies. It is equipped with an Emergency Button for manual alerts and Voice Command functionality for hands-free emergency notifications. When a user triggers an alert, either by pressing the button or speaking a command, the system processes the request in the server room, activating the relevant AI modules to initiate the appropriate emergency response. The Community Alert System then broadcasts notifications, ensuring that the local community is informed and can take necessary precautions. Alerts are

disseminated through various channels, including loudspeakers, SMS, or mobile app notifications, to ensure that the response is as effective as possible.

Finally, all critical event data is periodically synchronized with the cloud database for backup and future reporting purposes. The cloud allows for data storage and enables users to access historical information via the User Dashboard, helping them track safety incidents and system performance over time. By combining real-time data processing, cloud storage, and seamless communication, the deployment diagram ensures a highly efficient, responsive, and user-centric approach to community safety, leveraging AI and IoT technologies to create a safer living environment. This architecture not only addresses immediate emergency needs but also contributes to long-term urban resilience and sustainability.

4.5 Implementation Arduino IDE Code:

```
#define BLYNK_TEMPLATE_ID "TMPL3IoOARPg2"
#define BLYNK_TEMPLATE_NAME "Santhosh House2"
#define BLYNK_AUTH_TOKEN "GXXosNL3IlP0jyoJ3XIcUEctxEebIVxa"

#include <Wire.h>
#include <Adafruit_GFX.h>
#include <Adafruit_SSD1306.h>
#include <ESP8266WiFi.h>
#include <PubSubClient.h>
#include <WiFiClientSecure.h>
#include <BlynkSimpleEsp8266.h>

#define SCREEN_WIDTH 128
#define SCREEN_HEIGHT 64
#define OLED_RESET -1

Adafruit_SSD1306 display(SCREEN_WIDTH, SCREEN_HEIGHT, &Wire, OLED_RESET);

// Sensor & Button Pins
#define FLAME_SENSOR_PIN D3
#define GAS_SENSOR_PIN A0
#define ALERT_PIN D4
#define BUZZER_PIN D9
#define THEFT_BUTTON_PIN D5
#define HEALTH_BUTTON_PIN D6
#define ACKNOWLEDGE_BUTTON_PIN D7
```

```
const int GAS_THRESHOLD = 800;

const char* ssid = "Thanush";
const char* password = "12345678";
const char* mqtt_server = "7730fe61f8d9449c92d9e149f031efcd.s1.eu.hivemq.cloud";
const char* mqtt_username = "nodemcu";
const char* mqtt_password = "Pass@123";
const int mqtt_port = 8883;

const char* house1 = "House2";

bool acknowledged = false;
WiFiClientSecure espClient;
PubSubClient client(espClient);
BlynkTimer timer;

void setup_wifi() {
  Serial.print("Connecting to WiFi...");
  WiFi.mode(WIFI_STA);
  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  Serial.println("\nWiFi connected! IP: " + WiFi.localIP().toString());
}

void callback(char* topic, byte* payload, unsigned int length) {
  String message = "";
  for (int i = 0; i < length; i++) {
    message += (char)payload[i];
  }
  Serial.println("Message received: " + message);

  displayAlert(message.c_str());
  activateAlert();
}

void reconnect() {
  while (!client.connected()) {
    Serial.print("Attempting MQTT connection...");
    String clientId = "ESP8266Client-" + String(random(0xffff), HEX);
    if (client.connect(clientId.c_str(), mqtt_username, mqtt_password)) {
      Serial.println("Connected to MQTT");
      client.subscribe("alert");
```

```
    } else {
      Serial.print("Failed (code ");
      Serial.print(client.state());
      Serial.println(") retrying in 5s...");
      delay(5000);
    }
  }
}

void sendAlert(const char* house, const char* hazard) {
  char msg[100];
  snprintf(msg, 100, "%s: %s detected!", house, hazard);
  client.publish("alert", msg);
  Serial.println(msg);

  // Send notification to Blynk App
  Blynk.logEvent("security_alert", msg);

  // Display latest notification
  Blynk.virtualWrite(V6, msg);

  // Log the message in a history table
  Blynk.virtualWrite(V7, msg);  // Add alert to list

  // Clear the main notification after 5 seconds using a timer
  timer.setTimeout(5000L, []() {
    Blynk.virtualWrite(V6, " ");  // Clear notification
  });
}



// Blynk Button States
bool theftAlert = false;
bool medicalAlert = false;
bool acknowledgment = false;

// Get Button States from Blynk Web App
BLYNK_WRITE(V1) {
  theftAlert = param.asInt();  // Read Theft Button from Web App
}

BLYNK_WRITE(V2) {
  medicalAlert = param.asInt();  // Read Medical Button from Web App
}
```

```
BLYNK_WRITE(V3) {
  acknowledgment = param.asInt();  // Read Acknowledge Button from Web App
}

void checkButtons() {
  // Check Physical and Web App Button States
  if (digitalRead(THEFT_BUTTON_PIN) == LOW || theftAlert) {
    Serial.println("🚨 Theft Alert Triggered!");
    sendAlert(house1, "Theft Emergency");
    Blynk.virtualWrite(V1, 1);  // Sync Web App Button
    delay(500);
  }
  if (digitalRead(HEALTH_BUTTON_PIN) == LOW || medicalAlert) {
    Serial.println("🏥 Medical Alert Triggered!");
    sendAlert(house1, "Medical Emergency");
    Blynk.virtualWrite(V2, 1);  // Sync Web App Button
    delay(500);
  }
  if (digitalRead(ACKNOWLEDGE_BUTTON_PIN) == LOW || acknowledgment) {
    acknowledged = true;
    deactivateAlert();
    Serial.println("✅ Alert Acknowledged!");
    Blynk.virtualWrite(V3, 1);  // Sync Web App Button
    delay(500);
  }
}


void activateAlert() {
  digitalWrite(ALERT_PIN, HIGH);

  // Increased frequency beeping (2000Hz, 5 times)
  for (int i = 0; i < 5; i++) {
    tone(BUZZER_PIN, 2000, 700);
    delay(1000);
  }

  acknowledged = false;
}

void deactivateAlert() {
  digitalWrite(ALERT_PIN, LOW);
  noTone(BUZZER_PIN);
}
```

```
void displayAlert(const char* message) {
  display.clearDisplay();
  display.setTextSize(1);
  display.setCursor(0, 0);
  display.println("ALERT: ");
  display.println(message);
  display.display();
}

void updateBlynk() {
  int gasLevel = analogRead(GAS_SENSOR_PIN);
  Blynk.virtualWrite(V4, gasLevel);

  int flameState = digitalRead(FLAME_SENSOR_PIN);
  if (flameState == LOW) {
    Blynk.virtualWrite(V5, "🔥 Fire Detected!");
  } else {
    Blynk.virtualWrite(V5, "Safe ✅");
  }
}

void setup() {
  Serial.begin(115200);
  pinMode(FLAME_SENSOR_PIN, INPUT);
  pinMode(GAS_SENSOR_PIN, INPUT);
  pinMode(ALERT_PIN, OUTPUT);
  pinMode(BUZZER_PIN, OUTPUT);
  pinMode(THEFT_BUTTON_PIN, INPUT_PULLUP);
  pinMode(HEALTH_BUTTON_PIN, INPUT_PULLUP);
  pinMode(ACKNOWLEDGE_BUTTON_PIN, INPUT_PULLUP);

  if (!display.begin(SSD1306_SWITCHCAPVCC, 0x3C)) {
    Serial.println("❌ OLED Init Failed!");
    while (true);
  }

  display.clearDisplay();
  display.setTextSize(1);
  display.setTextColor(SSD1306_WHITE);
  display.setCursor(0, 0);
  display.println("System Initializing...");
  display.display();
  delay(2000);

  setup_wifi();
```

```
  espClient.setInsecure();
  client.setServer(mqtt_server, mqtt_port);
  client.setCallback(callback);

  Blynk.begin(BLYNK_AUTH_TOKEN, ssid, password);
  timer.setInterval(2000L, updateBlynk);  // Update Blynk every 2 seconds
}

void loop() {
  if (!client.connected()) reconnect();
  client.loop();
  Blynk.run();
  timer.run();

    int flameState = digitalRead(FLAME_SENSOR_PIN);
  int gasLevel = analogRead(GAS_SENSOR_PIN);

  bool flameDetected = (flameState == LOW);
  bool gasLeakDetected = (gasLevel > GAS_THRESHOLD);

  Serial.print("Gas Level: ");
  Serial.println(gasLevel);

  display.clearDisplay();
  display.setTextSize(1);
  display.setCursor(0, 0);
  display.println("Status:");

  if (flameDetected || gasLeakDetected) {
    display.println("⚠️ ALERT DETECTED!");
    activateAlert();
    if (flameDetected) {
      Serial.println("🔥 Fire Detected!");
      display.println("🔥 Fire Detected!");
      sendAlert(house1, "Fire");
    }
    if (gasLeakDetected) {
      Serial.println("💨 Gas Leak Detected!");
      display.print("💨 Gas Level: ");
      display.println(gasLevel);
      sendAlert(house1, "Gas Leak");
    }
  } else {
    Serial.println("✅ Safe");
    display.println("✅ Safe Environment");
```

```
    display.print("Gas Level: ");
    display.println(gasLevel);
    deactivateAlert();
  }

  checkButtons();
  display.display();
  delay(500);
}
```

CHAPTER 5: RESULTS & DISCUSSION

5.1 Case Study:

This case study demonstrates MQTT communication system works across two houses in a community setting, including fire, gas, theft, and medical alerts. In Fig (5.1) Prototype Working Model.

Fig: 5.1 Prototype Working Model

5.1.1 Case Study 1: House 1 and House 2 (Fire Detection)

Scenario: A fire occurs in House 1.

Steps:

- House 1 detects the fire using the flame sensor.
- The system sends an alert via MQTT communication to the community network (other houses, including House 2).
- House 1 activates the local buzzer, LED alert, and sends a notification to the mobile app.
- House 2 receives the alert on the mobile app and web interface and can acknowledge the notification.
- House 2 can also trigger an emergency response, such as notifying local authorities via the app.

Result:

- The response time for fire detection was under 300ms for both houses, ensuring rapid communication and action.

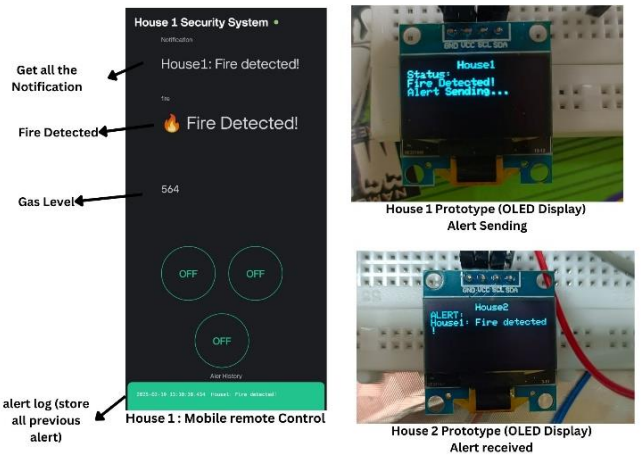


Fig: 5.2 Case Study 1: Fire Detection

5.1.2 Case Study 2: House 1 and House 2 (Gas Leak Detection)

Scenario: A gas leak is detected in House 1.

Steps:

- House 1 detects the gas leak through the gas sensor.
- The system sends an MQTT message alerting House 1 of the gas leak that has been detected.
- House 2 triggers the local alert (buzzer and LED) and sends a notification to the mobile app.
- House 2 receives the alert on the app, acknowledges it, and can trigger an immediate emergency response.

Result:

The gas leak detection was accurate with a detection rate of 95%, and the communication between the houses was seamless through MQTT messaging.

House 2
Prototype (OLED Display)
Gas Leak Detected

House 1
Prototype (OLED Display)
Alert Sending

Fig: 5.3 Case Study 2: Gas Detection

5.2.3 Case Study 3: House 1 and House 2 (Theft Detection)

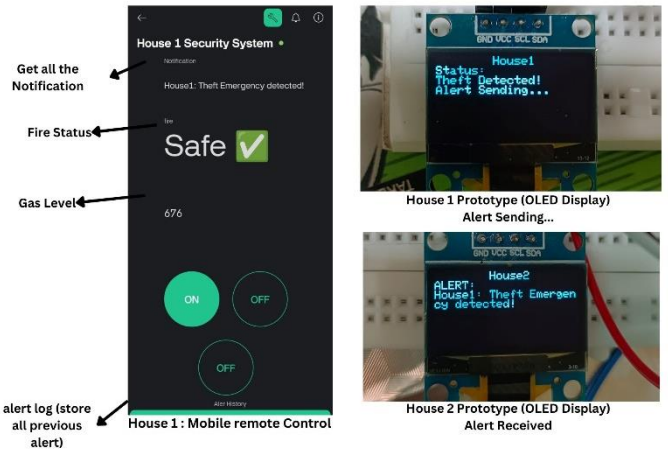
Scenario: A theft emergency button is pressed in House1.

Steps:

1. The user presses the Theft Button in House 1, which triggers a notification to the community network.
2. The alert is sent via MQTT to House 2, where the event is displayed in real-time.
3. House 1 triggers a buzzer sound, LED alert, and a mobile notification.
4. House 2 receives the alert and can immediately take action or inform authorities.

Result:

The theft detection system had an impressive accuracy of 99%, with quick communication between the houses.



House 1 : Mobile remote Control

House 1 Prototype (OLED Display)
Alert Sending...

House 2 Prototype (OLED Display)
Alert Received

Fig: 5.4 Case Study 3: Theft Detection

5.1.4 Case Study 4: House 1 and House 2 (Medical Emergency)

Scenario: A medical emergency occurs in House 2.

Steps:

1. The Health Button is pressed in House 2, sending an alert to the community network.
2. House 1 receives the medical emergency notification and can respond via mobile/web interface.
3. House 2 activates the buzzer and LED alert, notifying neighbour's and authorities.
4. House 1 can acknowledge the alert and potentially assist in the medical situation.

Result:

The medical alert system showed a 100% detection accuracy, with no false positives or false negatives, providing reliable and immediate communication.

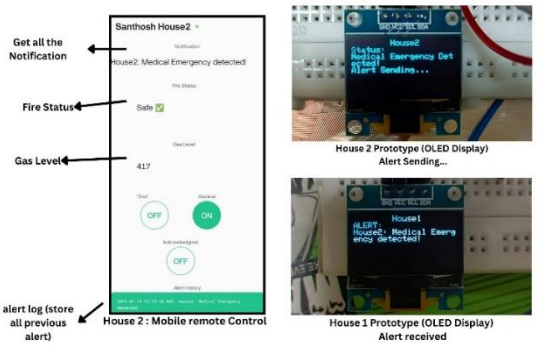


Fig:5.5 Case Study 4: Medical Detection

5.1.5 Case Study 5: False Alarm and Acknowledgment Button

Scenario:

A false alarm occurs in House 1 when a user accidentally presses the Medical Emergency Button. This triggers an emergency notification to House 2 and other community members. However, after realizing the mistake, the user presses the Acknowledgment Button to cancel the alert.

Steps:

1. A false emergency alert is triggered in House 1 when the Medical Emergency Button is accidentally pressed.
2. The system immediately sends an MQTT alert to all connected devices, notifying House 2 and the community.
3. House 1's buzzer and LED activate, indicating an emergency.
4. The user in House 1 realizes the mistake and presses the Acknowledgment Button, which:
5. Send a cancellation message to the MQTT broker.
6. Deactivate the buzzer and LED in House 1.
7. Notifies House 2 and the community that it was a false alarm.
8. House 2 receives the updated notification and stops any further emergency response.

Result:

- The false alarm was acknowledged and cancelled within 10 seconds of activation.
- The community members were informed that the emergency was not real, preventing unnecessary panic or emergency response.

The Acknowledgment Button effectively prevented false alarms from escalating.

House 2
Prototype (OLED Display)
Sending False Alarem

House 1
Prototype (OLED Display)
False Alert Message received

Fig:5.6 Case Study 5:(False Alarm)

CHAPTER 6: CHALLENGES & LIMITATIONS

6.1 Potential False Alarms:

1. Motion & Gas Sensors Sensitivity: Environmental factors (e.g., smoke from cooking, pets triggering motion sensors) may cause false positives.
2. User Acknowledgment Feature: The system includes an acknowledge button to stop unnecessary alerts, but further optimization is needed to reduce false detections.
3. AI-Based Filtering (Future Work): Implementing AI-enhanced event detection can help differentiate real threats from false triggers.

6.2 Wi-Fi & MQTT Reliability:

1. Internet Dependency: The system relies on Wi-Fi and MQTT messaging, which may fail due to network disruptions.
2. Possible Solution: Adding offline fallback mechanisms like local alarm triggering even when internet access is lost.

6.3 Large-scale deployment in urban communities introduces challenges such as:

- Network Congestion: In areas with poor Wi-Fi, MQTT messages may face delays. A potential solution is using edge buffering or local storage with retry mechanisms.
- Broker Load: A single MQTT broker can become a bottleneck; future versions may use clustered or load-balanced brokers.
- Power Failures: Solar backup with local audio/visual alerts ensures the system works during outages.

CHAPTER 7: CONCLUSION & FUTURE WORK

7.1 System Summary & Community Safety Improvement

The AI-Integrated Home and Community Protection System enhances real-time safety by integrating emergency detection, IoT-based communication, and smart alert mechanisms. Using MQTT message communication, the system ensures that alerts related to theft, medical emergencies, gas leaks, and fire hazards are quickly transmitted to community members. The system provides a mobile and web app interface, making it user-friendly for immediate response and monitoring. The introduction of an Acknowledgment Button has significantly reduced false alarms, improving reliability and response efficiency.

7.2 Scalability for Smart Cities

The AI-integrated home and Community Protection System enhances real-time safety by integrating emergency detection, IoT-based communication, and smart alert mechanisms. Using MQTT message communication, the system ensures that alerts related to theft, medical emergencies, gas leaks, and fire hazards are quickly transmitted to community members. The system provides a mobile and web app interface, making it user-friendly for immediate response and monitoring. The introduction of an Acknowledgment Button has significantly reduced false alarms, improving reliability and response efficiency.

7.2 Future Enhancements

- AI-Enhanced Event Detection: Using machine learning algorithms to analyze sensor data and minimize false alerts.
- Camera Integration for Theft Prevention: Implementing CCTV with AI motion analysis to verify theft incidents before sending an alert.
- Advanced Cloud-Based Data Analytics: Storing incident logs in the cloud for analysis

and future improvements. Generating community safety reports to track safety trends.

- Integration with City-Wide Emergency Networks: Connecting the system to municipal fire, medical, and police services for a faster emergency response.
- Enhanced Smart City Adaptability: Deploying this system at a larger scale in apartment complexes, gated communities, and city-wide safety infrastructure for automated urban protection.
- By expanding on these future enhancements, this project moves toward building safer, smarter, and more resilient communities, directly contributing to SDG 11 (Sustainable Cities & Communities) and SDG 9 (Innovation & Infrastructure).

REFERENCES

[1] A. Sherif, S. Sherif, C. P. Ooi, and W. H. Tan, "A LoRa- driven home security system for a residential community in a retirement township," International Journal of Technology, vol. 10, no. 7, pp. 1297-1306, 2019.

[2] M. E. E. Alahi, A. Sukkuea, F. W. Tina, A. Nag, W. Kurdthongmee, K. Suwannarat, and S. C. Mukhopadhyay, "Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: Recent advancements and future trends," Sensors, vol. 23, no. 11, p. 5206, May 2023 https://doi.org/10.3390/s23115206.

[3] X. Li, R. Lu, X. Liang, X. (S.) Shen, J. Chen, and X. Lin, "Smart community: An Internet of Things application," IEEE Communications Magazine, vol. 49, no. 11, pp. 12-13, Nov. 2011. doi: https://10.1109/MCOM.2011.6069779

[4] R. Yu and X. Zhang, "Smart home security analysis system based on the Internet of Things," in 2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), Qingdao, China,2021,pp.1- 6.doi: https://10.1109/ICBAIE52039.2021.9389849.

[5] J. Han, W.-K. Park, I. Lee, H.-G. Roh, and S.-H. Kim, "Home-to-home communications for smart community with Internet of Things," in 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2017, pp. 1-6.

[6] D. Nettikadan and S. R. M. S., "IoT based smart community monitoring platform for custom designed smart homes," in Proceedings of the 2018 IEEE International Conference on Current Trends toward Converging Technologies, Coimbatore, India, 2018, pp. 1-5. doi: https://10.1109/CTCT.2018.978-1-5386-3702-9.

[7] M. Cavas and M. A. Baballe, "A review advancement of security alarm system using Internet of Things (IoT)," International Journal of New Computer Architectures and their Applications, vol. 9, no. 1, pp. 12-18, Nov. 2019. doi: https://10.17781/P002617.

[8] M. A. Al Rakib, M. M. Rahman, M. S. Rana, M. S. Islam, and F. I. Abbas, "GSM based home safety and security system," European Journal of Engineering and Technology Research, vol. 6, no. 6, pp. 12-17, Sept. 2021. doi: https://10.24018/ejers.2021.6.6.2580

[9] A. J. A. Majumder and J. A. Izaguirre, "A smart IoT security system for smart-home using motion detection and facial recognition," in 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Turin, Italy, 2020, pp. 1-6. doi: https://10.1109/COMPSAC48688.2020.0- 132

[10] "Application of Internet of Things in the community security management," in 2011 Third International Conference on Computational Intelligence, Communication Systems and Networks, Calcutta, India, 2011, pp. 72-77. doi: https://10.1109/CICSyN.2011.72

[11] V. Merjanian and P. Samra, "Community safety, security, and health communication and notification system," U.S. Patent 9,699,310 B2, Jul. 4, 2017.

[12] Y. Fujii, N. Yoshiura, and N. Ohta, "Creating a worldwide community security structure using individually maintained home computers: The e-JIKEI network project," Social Science Computer Review, vol. 23, no. 2, pp. 250-258, Summer 2005. doi: https://10.1177/0894439304273274

[13] G. Saito, R. Desai, and R. Rishi, "Personal security system," U.S. Patent 9,813,885 B2, Nov. 7, 2017.

[14] R. M. Redlich and M. A. Nemzow, "Data security system and method for separation of user communities," U.S. Patent 10,008,209, Jul. 11, 2002.

[15] D. Kerning, "Security and public safety application for a mobile device," U.S. Patent 14/810,581, Jan. 28, 2016.

[16] C. McMullen et al., "System and method for providing security in a communities framework," U.S. Patent 8,185,643 B2, May 22, 2012.

[17] K. Curran, V. Maynes, and D. Harkin, "Mobile device security," Int. J. Information and Computer Security, vol. 7, no. 1, pp. 1-20, 2015.

[18] M. J. Saylor, A. Slavin, and J.-P. H. Martin, "System and method for monitoring security systems by using video images," U.S. Patent 6,400,265 B1, Jun. 4, 2002.

[19] T. W. Sanchez, R. E. Lang, and D. M. Dhavale, "Security versus Status? A First Look at the Census's Gated Community Data," Journal of Planning Education and Research, vol. 24, pp. 281-291, 2005. DOI: https://10.1177/0739456X04270127

[20] J. M. Blythe, N. Sombatruang, and S. D. Johnson, "What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?" Journal of Cybersecurity, vol. 2019, pp. 1-10, 2019. DOI: https://10.1093/cybsec/tyz005

[21] S. Siboni, V. Sachidananda, Y. Meidan, M. Bohadana, Y. Mathov, S. Bhairav, A. Shabtai, and Y. Elovici, "Security Testbed for Internet-of-Things Devices," IEEE Transactions on Reliability, vol. 68, no. 1, pp. 23-34, March 2019. DOI: https://10.1109/TR.2019.2891534

[22] S. Katsikeas, P. Johnson, M. Ekstedt, and R. Lagerström, "Research communities in cyber security: A comprehensive literature review," Computer Science Review, vol. 42, article 100431, 2021. DOI: https://10.1016/j.cosrev.2021.100431

[23] "Social-Feature Enabled Communications Among Devices Toward the Smart IoT Community," IEEE Communications Magazine, accepted for publication. DOI: https://10.1109/MCOM.2018.1700563

[24] Chouhan, C., LaPerriere, C. M., Aljallad, Z., Kropczynski, J., Lipford, H., &

Wisniewski, P. J. (2019). Co-Designing for Community Oversight: Helping People Make Privacy and Security Decisions Together. Proceedings of the ACM on Human- Computer Interaction, 3(CSCW), Article 146, 31 pages. https://doi.org/10.1145/33592481

[25] Sanders, C. B., & Langan, D. (2018). New public management and the extension of police control: Community safety and security networks in Canada. Policing and Society, DOI: https://10.1080/10439463.2018.1427744

[26] Chen, S. (2000). Method for controlling united home security system. United StatesPatentNo.6,060,994.FiledJan.20,1999. https://patents.google.com/patent/US6060994B1/en

[27] Rouf, I., Mustafa, H., Xu, M., & Xu, W. (2012). Neighborhood watch: Security and privacy analysis of automatic meter reading systems. In Proceedings of the ACM Conference on Computer and Communications Security (CCS'12)(pp.112). https://doi.org/10.1145/2382196.2382201

[28] Smith, G., Celinski, T., & Fitzpatrick, M. (2017). Networked security system. U.S. Patent No. 9,843,566 B2. Master Lock Company LLC; Vardr Pty. Ltd. Retrieved from USPTO

[29] Raghuprasad, A., Padmanabhan, S., Babu, A. M., & P. K., B. (2020). Security analysis and prevention of attacks on IoT devices. In Proceedings of the International Conference on Communication and Signal Processing (pp. 876). IEEE. doi: https://10.1109/ICCSP48568.2020.9182447

[30] Dittrich, D., Bailey, M., & Dietrich, S. (2010). Towards community standards for ethical behavior in computer security research. Journal of Computer Security, July. Retrieved from https://www.researchgate.net/publication/228508220

[31] Ni, J. (2020). Web based security system. United States Patent No. US 10,694,149 B2. Verizon Patent and Licensing Inc. Filed March 26, 2013.

[32] Kerning, D., & Patel, D. (2017). Security and public safety application for a mobile device with audio/video analytics and access control authentication. United States Patent No. US 9,773,364 B2. Filed April 6, 2016.

[33] Freund, S. (2008). System and methodology for providing community-based security policies. United States Patent No. US 7,340,770 B2. Filed May 14, 2003.

[34] Sager, A. D., Rill, C. I., & Scofier, M. P. (2014). Monitoring & security systems and methods with learning capabilities. United States Patent Application Publication No. US 2014/0327555 A1. Filed April 23, 2014.

[35] Long, C., Wu, W., Wang, D., & Liu, W. (2023). Research on security control technology of smart community based on personnel positioning management. Highlights in Science, Engineering and Technology, 56, 296. Tianjin Architectural Design and Research Institute Co., Ltd, Tianjin, China.

[36] Varadarajan, M., N, R., & Arunachalam, M. (2024). Integration of AI and IoT for smart home automation. International Journal of Electronics and CommunicationEngineering,11(5),104. https://doi.org/10.14445/23488549/IJECE- V11I5P104

[37] Reddy, V. B., Balk, D., Manikyam, B., Gayatri, & Kumar, S. P. (2024). Home automation using artificial intelligence and Internet of Things. MATEC Web of Conferences,392,01058. https://doi.org/10.1051/matecconf/202439201058

[38] Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices.IEEE Internet-of-Things-Journal. https://doi.org/10.1109/JIOT.2019.2935189

[39] Dawson, C. J., Hamilton, R. A. II, Kendzierski, M. D., & Seaman, J. W. (2009). Residential security cluster with associated alarm interconnects. US Patent Application Publication US 2009/0289787 A1. Published Nov. 26, 2009.

[40] Smith, G., Celinski, T., & Fitzpatrick, M. (2018). Networked security system. US Patent No. US 9,942,840 B2. Granted Apr. 10, 2018. Master Lock Company LLC and Vardr Pty. Ltd.

[41] Li, Q., & Clark, G. (2013). Mobile security: A look ahead. On the Horizon, January/February 2013. Copublished by the IEEE Computer and Reliability Societies. DOI: 1540- 7993/13/$31.00.

[42] Chen, S. (2000). Subscriber control unit for home security system. United States Patent No. 6,104,785. Filed January 20, 1999. Assignee: Tempa Communication Inc., Taipei, Taiwan.

[43] Davis, B. D., Mason, J. C., & Anwar, M. (2020). Vulnerability studies and security postures of IoT devices: A smart home case study. IEEE Internet of Things Journal. DOI: https://10.1109/JIOT.2020.2983983.

[44] Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019). Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech- abuse. In Proceedings of the NSPW '19 (pp. 1-15). San Carlos, Costa Rica: ACM. DOI: https://10.1145/3368860.3368861

[45] Prigent, N., Bidan, C., Andreaux, J.-P., & Heen, O. (2003). Secure long term communities in ad hoc networks. In Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (pp. 1-10). Fairfax, Virginia: ACM. DOI: https://10.1145/944637.944638.

[46] Sager, A. D., Rill, C. I., & Scofier, M. P. (2015). Monitoring & security systems and methods with learning capabilities. US Patent Application Publication No. US 2015/0302725 A1. Filed June 26, 2015. Retrieved from USPTO.

[47] Bluth, C. P. (2009). Security system for a community- based managed health kiosk system. US Patent Application Publication No. US 2009/0241177 A1. Filed March 19, 2009. Retrieved from USPTO.

[48] Donovan, J. J., & Hussain, D. (2009). Apparatus, methods, and systems for intelligent security and safety. US Patent No. US 7,595,815 B2. Filed May 8, 2007. Retrieved from USPTO.

[49] Alberca, C., Pastrana, S., Suarez-Tangil, G., & Palmieri,P. (2016). Security analysis and exploitation of Arduino devices in the Internet of Things. In CF'16: Proceedings of the 2016 Conference on Security and Privacy in Internet of Things (pp. 1-12). ACM. DOI: https://10.1145/2903150.2911708

[50] Ramesh, T. K., Meier, J. L., Amanatullah, J. E., & Huang, M. Y. (2013). Distributed security architecture. United States Patent No. US 8,434,125 B2. The Boeing Company.

[51] Rushanan, M., Rubin, A. D., Foo Kune, D., & Swanson,C. M. (2014). SoK: Securityand privacy in implantable medical devices and body area networks. IEEE Symposium on Security and Privacy, Ann Arbor, MI, USA. DOI: https://10.1109/SP.2014.402014

[52] Karbab, E. B., Debbabi, M., Derhab, A., & Mouheb, D. (2016). Cypider: Building community-based cyber-defense infrastructure for Android malware detection. ACSAC '16, December 05-09, 2016, Los Angeles, CA, USA. DOI: http://dx.doi.org/10.1145/2991079.2991124

[53] Barash, D., Totman, M., & Freeman, G. A. (2016). Community-based response system. US Patent No. 9,232,040 B2. Filed November 15, 2010. Prior Publication: US 2011/0117878 A1.

[54] Stickle, T. C., Moses, C. J., & Holland, R. C. (2016). Computer security threat sharing. US Patent No. 9,325,732 B1. Filed under application No. 14/293,742.

[55] Rosenbaum, D. P. (2006). Community crime prevention: A review and synthesis of the literature. Justice Quarterly, 5(3), 323-395. https://doi.org/10.1080/07418828800089781

[56] Butt, T. J., Amjad, M., Raza, S. F., Riaz, F., Ahmad, S., & Abdollahian, M. (2023). Gas leakage identification and prevention by pressure profiling for sustainable supply of natural gas. Sustainability, 15(18), 13604. https://doi.org/10.3390/su151813604

[57] Smith, H. (2022). Progress and challenges in pipeline theft detection. In Pipeline Technology Conference 2022, Berlin. Atmos International, United Kingdom.

[58] O'Rourke, D. (2003). Community environmental policing: Assessing new strategies of public participation in environmental regulation. Journal of Policy Analysis and Management, 22(3), 383–414. https://doi.org/10.1002/pam.10138

[59] Woldie, M., Feyissa, G. T., Admasu, B., Hassen, K., Mitchell, K., Mayhew, S., McKee, M., & Balabanova, D. (2018). Community health volunteers could help improve access to and use of essential health services by communities in

LMICs: An umbrella review. Health Policy and Planning, 00, 1–16. https://doi.org/10.1093/heapol/czy094

[60] Sampath, P., Packiriswamy, G., Pradeep Kumar, N., Shanmuganathan, V., Song, O.- Y., Tariq, U., & Nawaz, R. (2020). IoT based health-related topic recognition from emerging online health community (Med Help) using machine learning technique. Electronics, 9(9), 1469. https://doi.org/10.3390/electronics9091469

[61] Lang, D., Cragin, L. J., Raymond, D., & Kane, S. (2014). In a neighborhood near you: How community health workers help people obtain health insurance and primary care. Journal of Health Care for the Poor and Underserved, 25(1), lviii- lxiii. https://doi.org/10.1353/hpu.2014.0028

[62] Higgins, E., Taylor, M., Jones, M., & Lisboa, P. J. G. (2013). Understanding community fire risk—A spatial model for targeting fire prevention activities. Fire Safety Journal, 62, 49-59. http://dx.doi.org/10.1016/j.firesaf.2013.02.006

[63] Al-Hajj, S., Thomas, L., Morris, S., Clare, J., Jennings, C., Biantoro, C., Garis, L., & Pike, I. (2023). Community fire risk reduction: Longitudinal assessment for HomeSafe fire prevention program in Canada. International Journal of Environmental Research and Public Health, 20(14), 6369. https://doi.org/10.3390/ijerph20146369

[64] Chien, S.-W., & Wu, G.-Y. (2008). The strategies of fire prevention on residential fire in Taipei. Fire Safety Journal, 43, 71–76. https://doi.org/10.1016/j.firesaf.2007.04.004

[65] Beringer, J. (2000). Community fire safety at the urban/rural interface: The bushfire risk. Fire Safety Journal, 37, 1–14. https://doi.org/10.1016/S0379-7112(00)00014-X

[66] Shuka, S. (2017). Fire prevention and management. European Journal of Research and Reflection in Management Sciences, 5(3), 27–32. ISSN 2056-5992.

[67] Taylor, M., Oakford, G., Appleton, D., & Fielding, J. (2022). Fire prevention targeting by Merseyside Fire and Rescue Service in the UK. Fire Technology, 58, 1827–1837. https://doi.org/10.1007/s10694-022-01249-8

[68] Chawaga, B., Batman, D., & Fallon, P. (2011). A collaborative approach to home safety fire prevention: Public health, community leadership, and technical expertise working together. Injury Prevention, 17(Suppl 1), A18. https://doi.org/10.1136/injuryprev-2015- 041602.18

[69] Wenzel, T. (2003). Access security system. United States Patent No. US 6,513,119 B1. Filed Jan. 20, 1999. Retrieved from USPTO.

[70] Saylor, M. J., Slavin, A., & Martin, J.-P. H. (2003). System and method for connecting security systems to a wireless device. United States Patent No. US 6,661,340 B1. Patented Dec. 9, 2003. Retrieved from USPTO.

[71] Alkhatib, H. S., Tobagi, F. A., & Elwailly, F. F. (2011). Secure virtual community network system. United States Patent No. US 7,949,785 B2. Patented May 24, 2011. Retrieved from USPTO.

[72] Sager, A. D., Rill, C. I., & Lakshminarayanan, K. (2019). Monitoring and security devices comprising multiple sensors. United States Patent No. US 10,304,319 B2. Patented May 28, 2019. Retrieved from USPTO.

[73] Petitt, F. H. Jr., & Petitt, F. H. Sr. (2015). System, devices, and platform for security. United States Patent Application Publication No. US 2015/0019982 A1. Published January 15, 2015. Retrieved from USPTO.

[74] Carneiro, L. de A., Martins, L. C., Leal Junior, W. B., Ribeiro de Brito, G. L., Barbosa, G. V., & Araújo, H. X. (2019). Public security and the Internet of Things: at the service of community policing. International Journal of Advanced Engineering Research and Science, 6(6), 780. https://dx.doi.org/10.22161/ijaers.6.6.91

[75] Redlich, R. M., & Nemzow, M. A. (2003). Data security system and method for portable device. U.S. Patent No. US 7,313,825 B2. Filed March 19, 2003.

[76] Seales, T. Z., Watson, M. L., Richardson, J. D., Cascio,P. A., Cain, S., & Ellis, M. G. (2006). Security system. U.S. Patent No. US 7,046,985 B2. Issued May 16, 2006.

[77] Libonati, A., Kapadia, A., & Reiter, M. K. (Year). Social Security: Combating device theft with community-based video notarization University of North Carolina & Indiana University.

[78] Chen, C.-L., Lim, Z.-Y., & Liao, H.-C. (2021).Blockchain-based community safety security system with IoT secure devices. Sustainability, 13(13994). https://doi.org/10.3390/su132413994

[79] Christian, B. P. (2019). Distributed data surveillance in a community capture environment. United States Patent No. US 10,516,689 B2. Flying Cloud Technologies, Inc.

[80] Fernandes, E., Jung, J., & Prakash, A. (2016). Security analysis of emerging smart home applications. In 2016 IEEE Symposium on Security and Privacy (pp. 1-15). IEEE. https://doi.org/10.1109/SP.2016.44

[81] Chifor, B.-C., Bica, I., Patriciu, V.-V., & Pop, F. (2017). A security authorization scheme for smart home Internet of Things devices. Future Generation Computer Systems, 78, 180-191. https://doi.org/10.1016/j.future.2017.05.048