PROJECT REPORT - INTER DISCIPLINARY

AI-INTEGRATED HOME AND COMMUNITY PROTECTION SYSTEM SUPPORT SDG 11

(PROJECT PHASE- II)

submitted in partial fulfillment of the requirements

for the award of the degree in

BACHELOR OF TECHNOLOGY

By

PIOUS NIRANJAN.A (211051101615)
DHANUSH RAJ.N (211051101005)
THANUSH K (211191101159)
SANTHOSH R (211191101131)

DEPARTMENT OF
CIVIL ENGINEERING & COMPUTER SCIENCE ENGINEERING

Dr. M.G.R.
EDUCATIONAL AND RESEARCH INSTITUTE
DEEMED TO BE UNIVERSITY
University with Graded Autonomy Status
(An ISO 21001 : 2018 Certified Institution)
Periyar E.V.R. High Road, Maduravoyal, Chennai-95. Tamilnadu, India.

APRIL 2025

Dr. M.G.R.
EDUCATIONAL AND RESEARCH INSTITUTE
DEEMED TO BE UNIVERSITY
University with Graded Autonomy Status
(An ISO 21001 : 2018 Certified Institution)
Periyar E.V.R. High Road, Maduravoyal, Chennai-95. Tamilnadu, India.

DEPARTMENT OF CIVIL ENGINEERING & COMPUTER SCIENCE ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report (Project Phase-II) is the bonafide work of

Mr. PIOUS NIRANJAN A	Reg. No:	211051101615,
Mr. DHANUSH RAJ N	Reg. No:	211051101005,
Mr. THANUSH K	Reg. No:	211191101159,
Mr. SANTHOSH R	Reg. No:	211191101131,

Who Carried out the project entitled **"AI-Integrated Home and Community Protection System Support SDG 11"** under our supervision from Dec 2024 to Apr 2025.

Internal Guide	Project Coordinator	Department Head
Dr.V. PRIYADARSHINI **Associate Professor** **Dept of CIVIL** Dr. MGR Educational and Research Institute, Deemed to be University	**Dr.T.KAVITHA** **Professor & HOD** **Dept of CIVIL** Dr. MGR Educational and Research Institute, Deemed to be University	**Dr.T.KAVITHA** **Professor & HOD** **Dept of CIVIL** Dr. MGR Educational and Research Institute, Deemed to be University

Mrs.A.MAHESWARI **Asst.Professor & Deputy HOD** **Dept of CSE(DS&AI)** Dr. MGR Educational and Research Institute, Deemed to be University	**Mr. M. ARUN** **Assistant Professor** **Dept of CSE** Dr. MGR Educational and Research Institute, Deemed to be University	**Dr. S. GEETHA** **Professor & HOD** **Dept of CSE** Dr. MGR Educational and Research Institute, Deemed to be University

Submitted for Viva Voce Examination held on _____

Internal Examiner **External Examiner**

DECLARATION

We **PIOUS NIRANJAN A (211051101615), DHANUSH RAJ N (211051101005), THANUSH K (211191101159), SANTHOSH R (211191101131)** hereby declare that the Project Report (Project Phase-II) entitled **"AI-Integrated Home and Community Protection System Support SDG 11"** is done by us under the guidance of **Dr.V.PRIYADARSHINI, Associate Professor & Mrs.A.MAHESWARI, Asst.Professor & Deputy HOD** is submitted in partial fulfillment of the requirements for the award of the degree in BACHELOR OF TECHNOLOGY in Civil Engineering & Computer Science Engineering.

DATE:

PLACE:

1.
2.
3.
4.

SIGNATURE OF THE CANDIDATE(S)

ACKNOWLEDGEMENT

We would first like to thank our beloved Founder Chancellor **Thiru**.**Dr. A.C.SHANMUGAM, B.A., B.L.,** President **Er. A.C.S.Arunkumar, B.Tech., M.B.A.,** and Secretary **Thiru A.RAVIKUMAR** for all the encouragement and support extended to us during the tenure of this project and also our years of studies in his wonderful University.

We express my heartfelt thanks to our Vice Chancellor **Prof. Dr. S. GEETHALAKSHMI** in providing all the support of my Project (Project Phase-II).

We express my heartfelt thanks to our Head of the Department, **Prof. Dr. S.Geetha**,**Dr.T. KAVITHA**, **CSE & CIVIL** who has been actively involved and very influential from the start till the completion of our project.

Our sincere thanks to our Project Coordinators **Mr. M Arun, Dr.T. KAVITHA, CSE & CIVIL** and Project guide **Mrs.A.MAHESWARI , Dr.V.PRIYADARSHINI** for their continuous guidance and encouragement throughout this work, which has made the project a success.

We would also like to thank all the teaching and non-teaching staffs of Computer Science and Engineering & CIVIL Engineering department, for their constant support and the encouragement given to us while we went about to achieving my project goals.

CONTENTS

Acknowledgment Button

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
NLP	Natural Language Processing
IoT	Internet of Things
SDGs	Sustainable Development Goals
MQTT	Message Queuing Telemetry Transport

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Safety in the community is still a major issue in smart city planning, with growing issues of theft, fire risks, gas leaks, and delayed emergency responses. A survey of residential communities in Chennai found that 65.2% of the respondents had theft incidents, mostly in community areas (83.5%), and 55.6% had gas leaks, with 72.8% showing high concern for safety threats. To counteract the limitations, we developed an AI-Based Home and Community Safety System based on IoT-based sensors, real-time communication protocols, and mobile-based monitoring interface. The system consists of flame and gas sensors, OLED display, theft, medical, and false alarm push buttons, and buzzers and LED indicators for notification. A wireless communication framework based on MQTT protocol supports real-time emergency notification among the households to provide immediate response and risk reduction. There is also an IoT dashboard on mobile provided for real-time remote monitoring and controlling of the system, which facilitates ease of access and user interaction. The survey also reflected high community interest in AI-based safety systems with 67.4% considering them to be highly effective and 79.7% willing to trial the system. Prototype testing proved low-latency notifications, efficient hazard detection, and enhanced emergency response systems. The suggested system is in compliance with Sustainable Development Goals (SDG 11 & SDG 9) by increasing the resilience of cities and encouraging smart safety infrastructure.

Keywords: Community safety, AI, IoT, MQTT, Smart cities, Emergency response, Sustainable Development Goals, Urban resilience, IoT dashboard, Remote monitoring.

MAJOR DESIGN CONSTRAINTS AND DESIGN STANDARDS TABLE

Student Group	A.Pious Niranjan (211051101615)	N.Dhanush Raj (211051101005)	K.Thanush (211191101159)	R.Santhosh (211191101131)
Project Title	AI-Integrated Home and Community Protection System Support SDG 11			
Program Concentration Area	Smart cities and Urban Development, Internet of Things (IoT) and AI Integration, Sustainable Development and Resilience			
Constraints Example	Technical Constraints, Cost Constraints, Environmental Constraints, User Adoption and Acceptance Constraints, Maintenance and Support Constraints			
Economic	Yes			
Environmental	Yes			
Sustainability	Yes			
Implementable	Yes			
Ethical	N/A			
Health and Safety	Yes			
Social	Yes			
Political	No			
Other	Power Modulation from Solar Panel			
Standards				
1	ISO/IEC 23894:2023			
2	IEEE 1451			
3	IEEE 802.11			
4	IEEE P2413			
5	NFTA 72			
6	UL268			
Prerequisite Courses for the Major Design Experiences	1. IoT and Smart System Integration 2. Artificial Intelligence for Security Applications 3. Wireless Communication and Networking			

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.

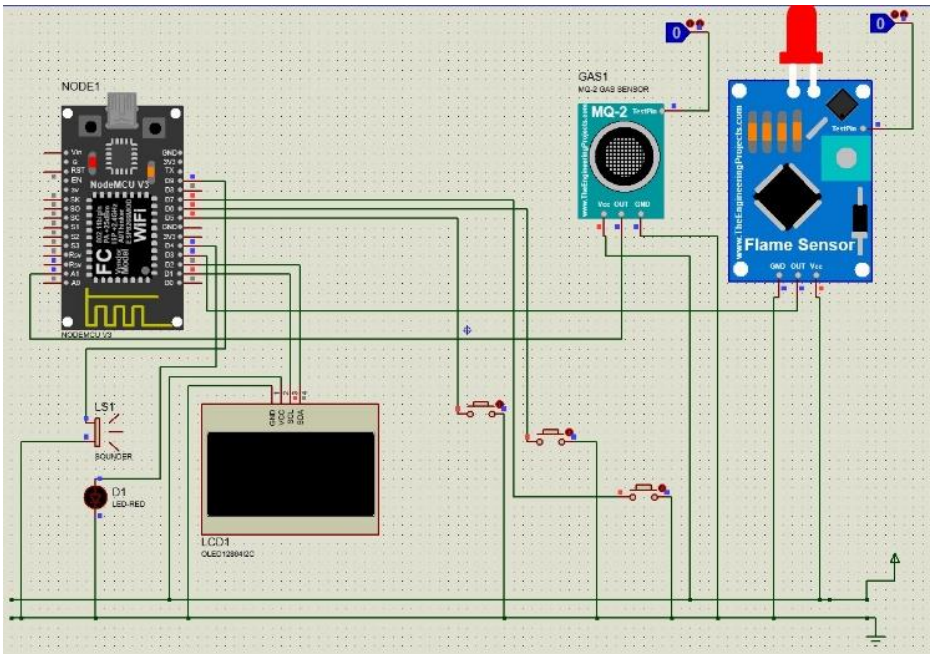


Fig:4.1 Circuit Diagram & Hardware Setup

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:

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

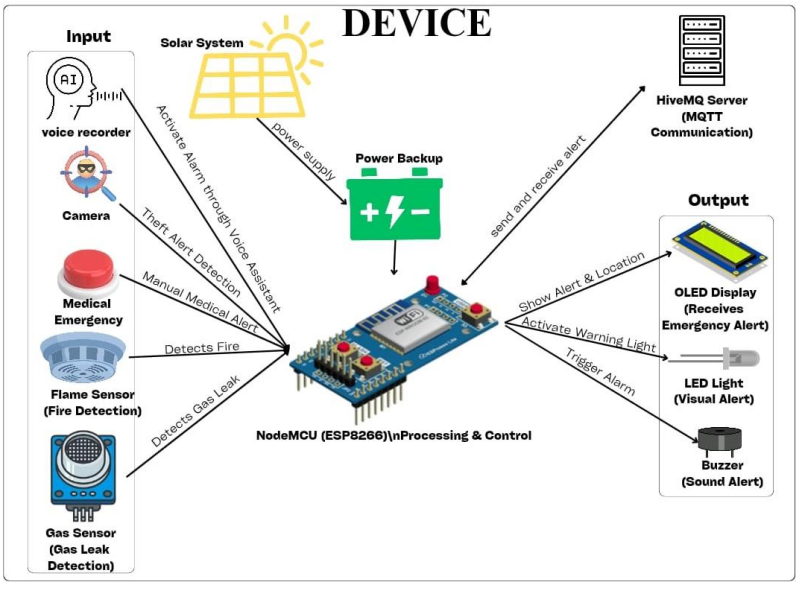


Fig:4.2 **TESTING ACCURACY SCENARIOS**

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:

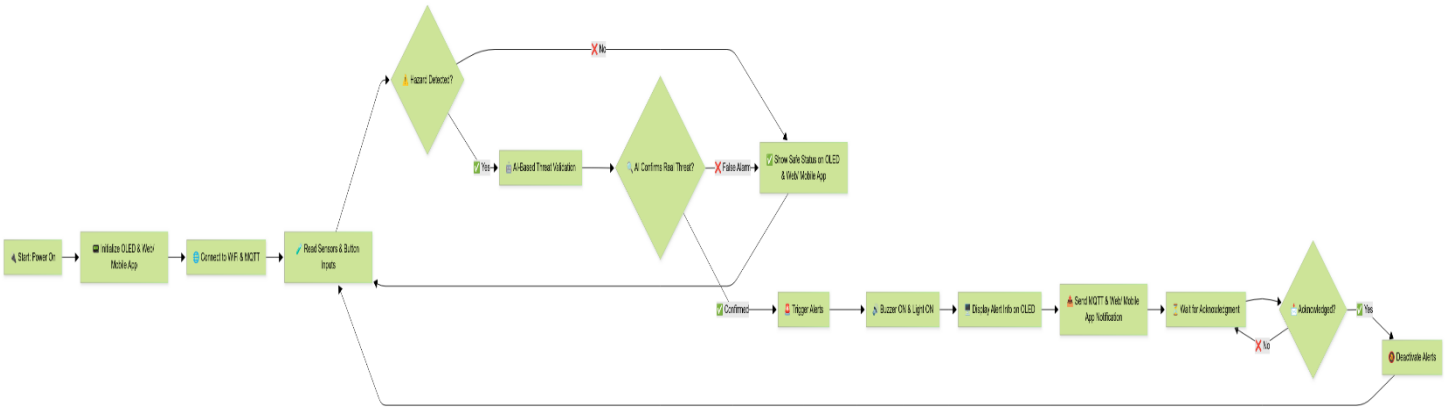


Fig:4.3 Represents Architecture Diagram

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).

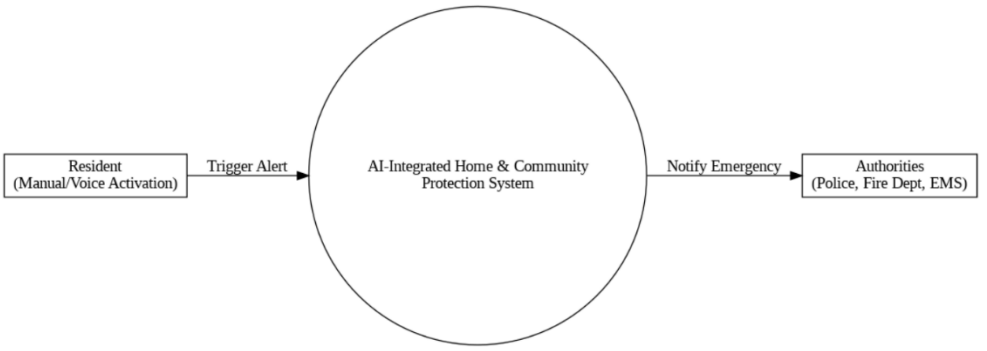


Fig 4.4: Level 0 DFD

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

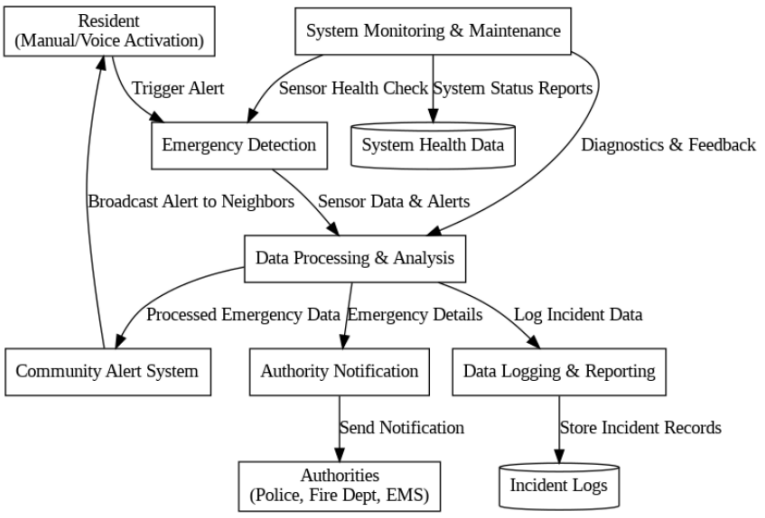


Fig 4.5: Level 1 DFD

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

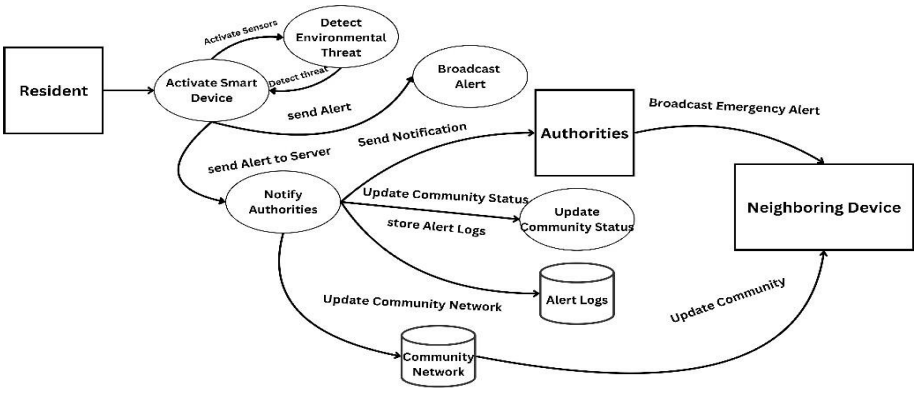


Fig 4.6: Level 2 DFD

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

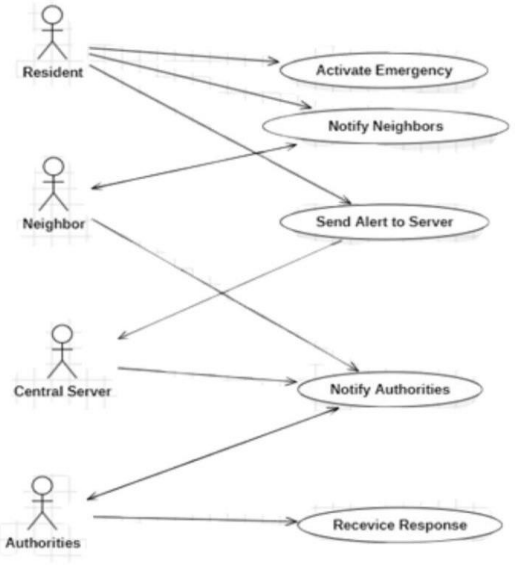


Fig 4.7: Use Case Diagram

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

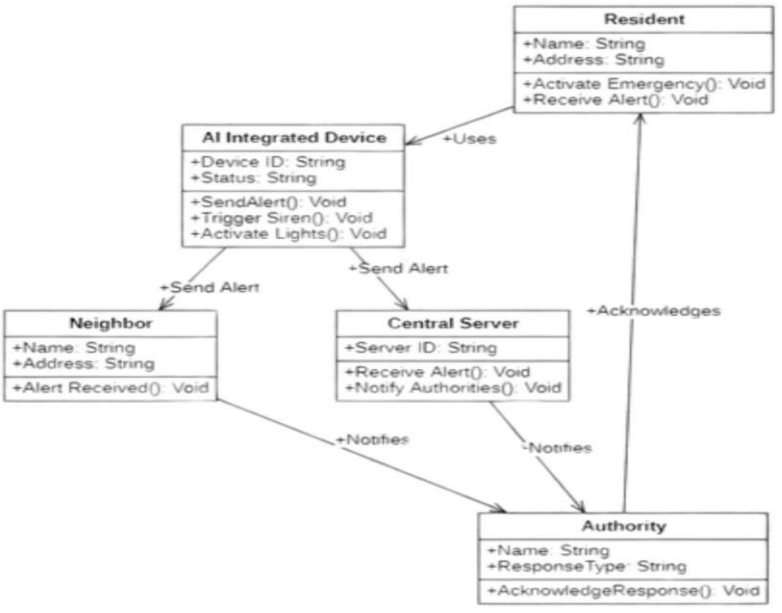


Fig 4.8: Class Diagram

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.

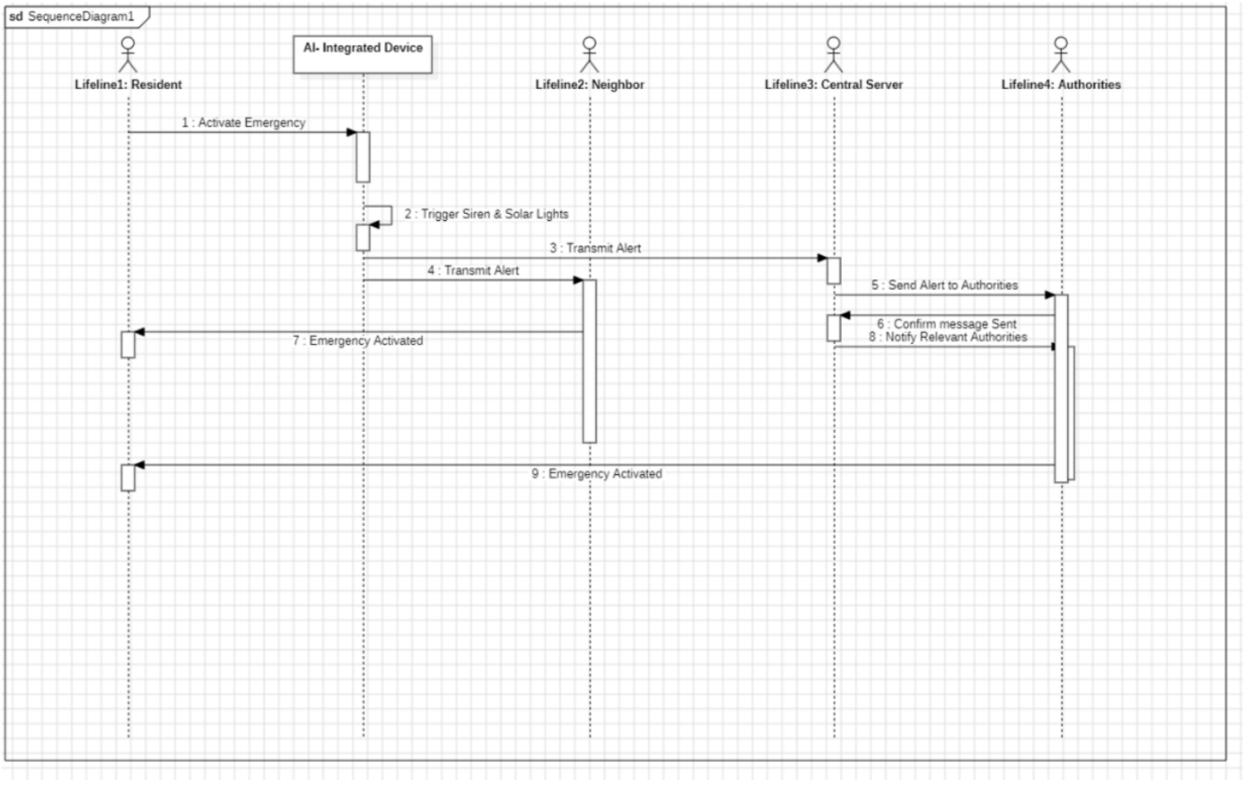


Fig 4.9: Sequence Diagram

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.

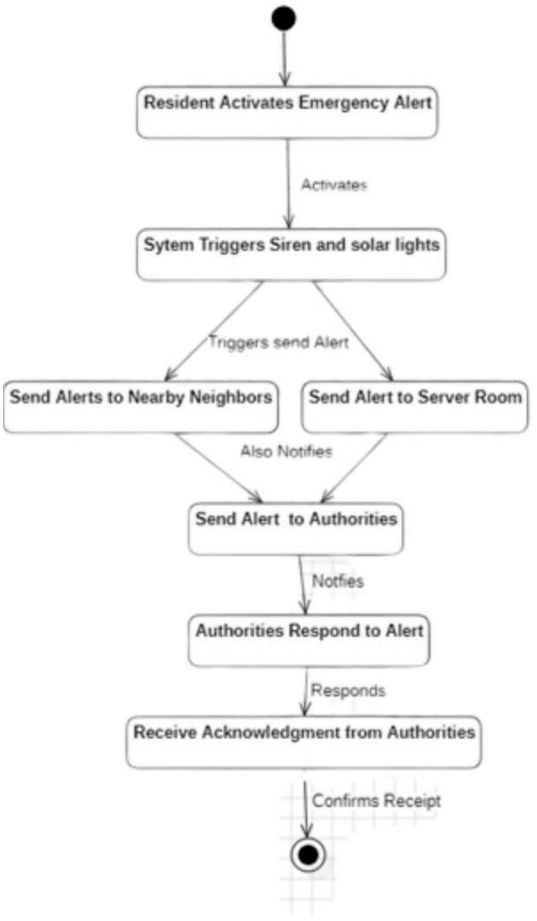


Fig 4.10: Activity Diagram

- ***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*

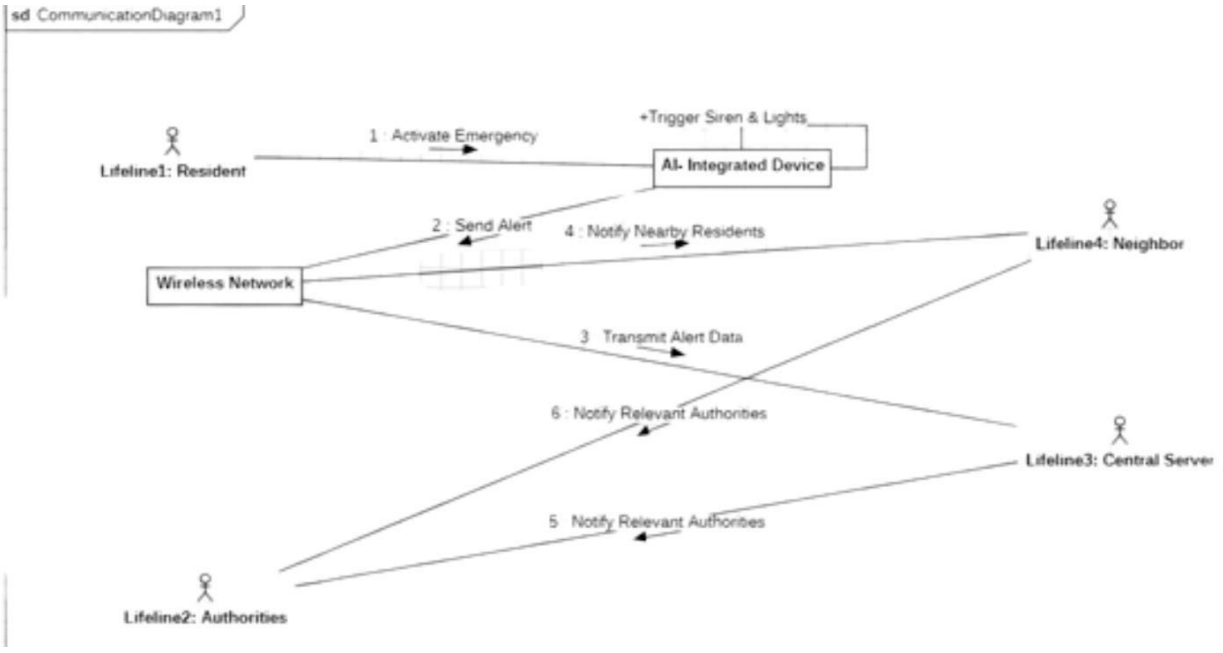


Fig 4.11: Communication Diagram

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

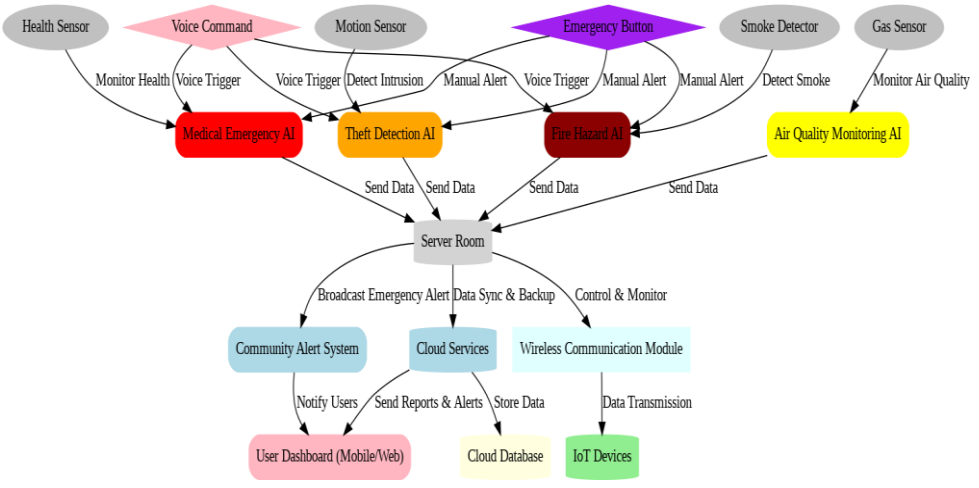


Fig 4.12: Deployment Diagram

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.

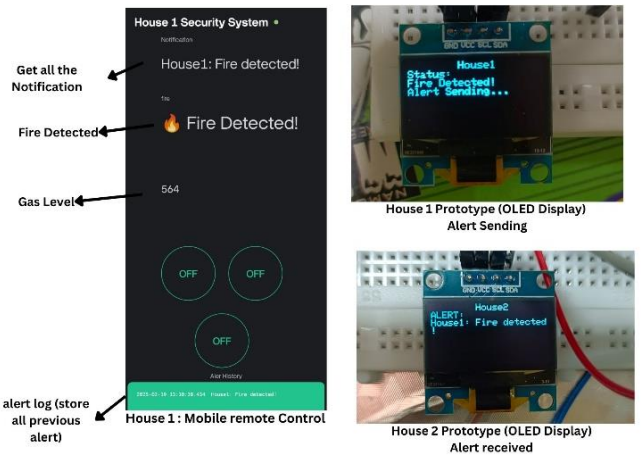


Fig: 5.2 Case Study 1: Fire Detection

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)

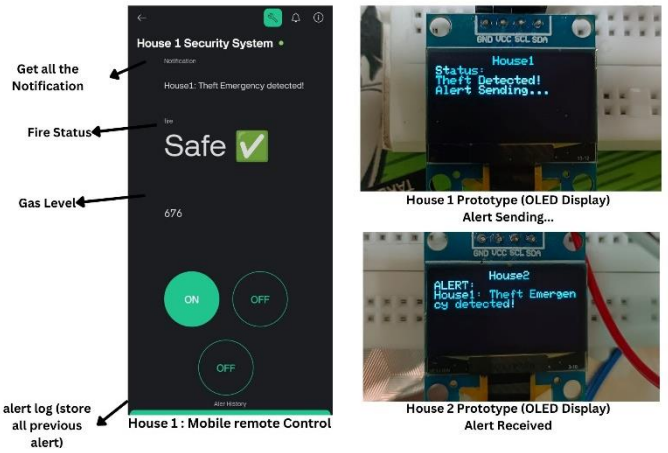
Scenario: A theft emergency button is pressed in House1.

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.

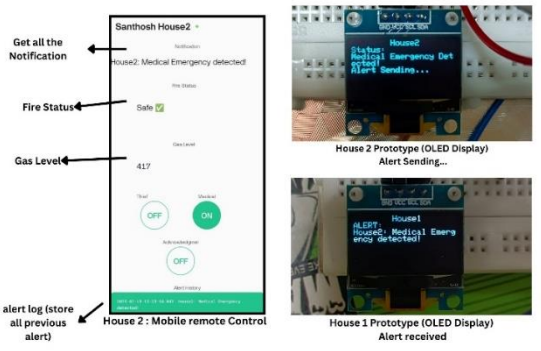


Fig:5.5 Case Study 4: Medical Detection

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

(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :05/02/2024

(21) Application No.202441007573 A
(43) Publication Date : 28/03/2025

(54) Title of the invention : AI INTEGRATED COMMUNITY SAFETY GADGETS

(51) International classification :G10L0015220000, G06F0021440000, G06F0003160000, H04W0004020000, C25D0017000000
(86) International Application No :NA
Filing Date :NA
(87) International Publication No : NA
(61) Patent of Addition to Application Number :NA
Filing Date :NA
(62) Divisional to Application Number :NA
Filing Date :NA

(71)**Name of Applicant :**
1)Dr. MGR Educational and Research Institute
Address of Applicant :Dr. MGR Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu 600095, India Chennai ---------- ----------
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)P S KRISHNA
Address of Applicant :Dr. MGR Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu 600095, India Chennai ---------- ----------
2)K THANUSH
Address of Applicant :Dr. MGR Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu 600095, India Chennai ---------- ----------
3)A PIOUS NIRANJAN
Address of Applicant :Dr. MGR Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu 600095, India Chennai ---------- ----------
4)S SRISOWMIYA
Address of Applicant :Dr. MGR Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu 600095, India Chennai ---------- ----------
5)M MOHAN
Address of Applicant :Dr. MGR Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu 600095, India Chennai ---------- ----------
6)K.ANITHA
Address of Applicant :Dr. MGR Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu 600095, India Chennai ---------- ----------
7)Dr.L.RAMESH
Address of Applicant :Dr. MGR Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu 600095, India Chennai ---------- ----------
8)Dr.S.GEETHA
Address of Applicant :Dr. MGR Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu 600095, India Chennai ---------- ----------
9)Dr.T.KAVITHA
Address of Applicant :Dr. MGR Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu 600095, India Chennai ---------- ----------
10)Dr.N.KANYA
Address of Applicant :Dr. MGR Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu 600095, India Chennai ---------- ----------
11)Dr.K.SARAVANAN
Address of Applicant :Dr. MGR Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu 600095, India Chennai ---------- ----------

(57) Abstract :
The objective of the present invention is to protect a group of the houses from the thief/medical/fire emergency. This Device is primarily to protect from the thief first and the secondary to solve either the medical problem or will be fire problem accidents that happen in the community of houses. It protects us from the thief, Medical and fire issues. There we added some features to secure our community. Security and Safety System for the Community through the chain connectivity device which can act according to the command from either keys or voice assistant with the color variants of lights blinks ,siren alert message and communicate to the Control Room. (Refer Fig. 1, 2)

No. of Pages : 18 No. of Claims : 1

SUSTAINED'24 - Provisional Acceptance Notification on your Manuscript titled "Study on Community Safety & Recommendations for Proposed AI-Integrated Community Devices Towards SDG 11" with the Paper ID "435"

1 message

Microsoft CMT <email@msr-cmt.org>
Reply to: Dr. Brahma Nand Agrawal <brahmaagrawal.set@mriu.edu.in>
To: Thanush Kannan <thanushlokesh1@gmail.com>
Cc: sustained@mriu.edu.in

Sat, 19 Oct, 2024 at 11:47 am

Dear Thanush Kannan,

We are pleased to inform you that your paper titled "Study on Community Safety & Recommendations for Proposed AI-Integrated Community Devices Towards SDG 11" with the Paper ID "435" has been reviewed. Please find below the reviewer comments. You can also access the reviewer's comments in the author feedback section on Microsoft CMT.
Based on the reviews received, your manuscript has been provisionally accepted for presentation and publication in SUSTAINED-2024, which is subject to satisfactory revision (if required) and registration. Please incorporate the reviewer's stated concerns, highlight the changes with a red colour in the revised manuscript, and complete the registration for SUSTAINED-2024.

Comments of Conference Chair
1. Paper needs to be linked with the theme of the conference i.e sustainability. SDGs may be used in the paper in abstract, introduction, main body, results and conclusion sections. Authors may identify any SDG which can match with their work in the paper.
2. Length of the paper to be limited to 6 pages as per IEEE. Beyond 6 pages INR 1000/- will be applicable per page up to maximum permissible 8 pages in total.
3. The paper needs to be reformatted in IEEE format. (Can be downloaded from conference website https://www.sustained2024.in/ in the download section)
4. Points related to sustainability may be used in title, abstract, introduction, conclusion to highlight the alignment of the paper with the conference theme

Reviewer 1

Figures seem to be copied from other sources, kindly cite the sources and take proper permission from the publisher or redraw the figures in original.
The study offers valuable insights into public perceptions of AI-integrated safety solutions in Chennai.

The survey highlights theft concerns, emphasizing the need for stronger security measures in neighborhoods.

Gas leak worries were prevalent, prompting interest in AI-driven solutions like environmental sensors.

Public knowledge of SDGs is broad, but AI's role in achieving them remains largely unclear.

Strong community support for AI in security suggests its potential to improve safety and sustainability.

Not matched with the theme of conference. It is Rejected

Reviewer 2

1. References cited in the text are not as per IEEE format.
2. Formatting should be as per the IEEE guidelines.
3. The title is too long. Use the keywords.
4. Give citation for figures

Reviewer 3

Suggestion: Clearly distinguish between the challenges the paper aims to solve (e.g., specific safety issues) and the technology proposed (AI-driven devices). The research objectives need to be outlined more explicitly in the introduction.
2. The methodology section can benefit from more detail on how the survey was conducted (e.g., was it an online or offline survey? How was the sample selected?). This transparency will strengthen the study's reliability.
3. Consider providing a deeper statistical analysis of the survey results. Graphs or tables showing correlations between factors like location and safety perceptions could make the findings more impactful. For instance, do people in certain areas perceive gas leaks as a bigger threat than others? Why?
4. The link to SDGs needs to be elaborated. While SDG 11 is mentioned, the connection between AI technologies and how they specifically contribute to achieving SDG 11 should be more thoroughly discussed. How do the proposed AI solutions directly contribute to sustainable urban development?
5. Provide more concrete examples of AI solutions (e.g., specific technologies like smart surveillance, AI-powered gas detectors). Discuss any challenges or potential drawbacks of implementing these solutions (e.g., cost, data privacy concerns).
6. Consider refining some of the language to enhance clarity. There are some areas where the writing is somewhat dense or unclear, particularly when transitioning between safety issues and technological solutions. Simplifying these transitions could improve the readability for a broader audience.

suggest revisions, especially in the areas of methodological transparency, detailed analysis of results, and clearer connections to the SDGs and AI technologies.

You are requested to submit the following documents to the author feedback section on the Microsoft CMT portal:.
1.Revised Paper with Highlighted Changes in RED Colour (word file).
File Name: Highlighted_Revised_Paper_ID
2.Receipt of Registration Fee paid (Pdf file). File Name: Fee Receipt_Paper ID.
3.Response to Reviewers comments (word file). File Name: Response to Reviewer_Paper ID

You are required to register for the conference within 1 week of the receipt of this acceptance mail.
Registration Link https://rb.gy/8pxy9v

Kindly follow the submission guidelines while preparing the revised manuscript mentioned on the conference website.
https://www.sustained2024.in/call-for-papers

Registration Account Details

Name of Account	Manav Rachna International Institute of Research and Studies
Account Number	201004119068
IFSC Code	INDB0000702
Bank Name	IndusInd Bank
SWIFT CODE	INDBINBB

Registration Fee Details: Registration fee details for different categories of authors may be found out at
https://www.sustained2024.in/registration

Important Notes:
•Camera ready paper must be in IEEE format.
•Please adhere on paper limit of 6 pages, otherwise extra per page fee shall be added.
•Students must produce a valid id card issued by the concerned institute to register in the student's category.
•To claim IEEE member must produce a valid id card issued by the concerned by IEEE.
•Registration fee does not include accommodation and transportation expenses.
•A minimum of one registration is mandatory for a paper to be a part of proceedings. If the author/co-author wishes to attend the conference and requires a separate proceeding and certificate along with the conference kit, in that case the author/coauthor needs to pay full registration fees individually.
•Accommodation could be arranged in the campus of MRIIRS, Faridabad or nearby hotels as per the availability on a payment basis for which the organizers will provide necessary assistance if informed well in advance.
•You are requested to follow the Plagiarism policy of the conference where the maximum acceptable similarity is 10%. Kindly make the required changes accordingly..

Please note that you must prepare the response to each comment of the reviewers.

Please feel free to contact us for any queries. Looking forward to your kind response and cooperation.

Best Regards
Organizing Team SUSTAINED- 2024
School of Engineering and Technology
MRIIRS, Faridabad, India
Landline No. +91 129-4259000
M +91 7838682667 Dr. Prateek Mittal, ME, SET, MRIIRS, Faridabad, India
Weblink: https://www.sustained2024.in/

AI-Integrated Community Safety Solutions for Smart Cities: A Study Towards SDG 11

K.Thanush,R.Santhosh
Department of CSE,
Dr. M.G.R. Educational and Research Institute,
Chennai, India.
santhosh.ai.dev@gmail.com

A.Pious Niranjan, N.Dhanush Raj
Department of Civil,
Dr. M.G.R. Educational and Research Institute,
Chennai, India.
igen.pious@gmail.com

L.Ramesh
Department of EEE,
Dr. M.G.R. Educational and Research Institute,
Chennai, India.
prof.greenramesh@gmail.com

S.Geetha,T.Kavitha
Department of CSE & CIVIL,
Dr. M.G.R. Educational and Research Institute,
Chennai, India.

K.Anitha,A.Maheswari,V.Priyadarshini
Department of EEE, CSE & CIVIL
Dr. M.G.R. Educational and Research Institute,
Chennai, India.

J.Balamurugan
Member - IGEN SUPERCEN,
The Institution of Green Engineers,
Chennai, India.

***Abstract*— Safety in rapidly urbanizing cities like Chennai is becoming an increasingly difficult task as human populations and density of cityscape continues to grow, exposing the insulation of traditional measures in theft prevention, managing medical emergencies and fire hazards. The conventional approaches are usually reactive, fragmented and do not have real time coordination and integrated response resources. This paper shows the need for extremely advanced technological responses, namely AI based technologies, to deal with these urban safety problems. Across Chennai, 408 residents from different North, South, East and West regions had been included in a public opinion survey. The survey tried to find out about perceptions of the community safety, incidents of theft and gas leak, awareness about Sustainable Development Goals (SDGs) and open towards AI facilitated safety technologies. Results show varied perceptions for perceived safety, massive crime experiences, and major fears of gas leaks. Much is known about SDGs in general, with SDG 11 & SDG 9 in particular, but there is little awareness about what an AI can do to help reach these goals. This, however, is backed by strong support for AI driven enhancements in safety including smart alarms, surveillance systems and environmental sensors. The findings show that AI will play a critical role in enhancing community safety with real time monitoring, quick response mechanisms along with proaction of threat. It highlights how AI enabled safety technology can contribute to urban resilience and sustainability by setting the course of AI enabled smart home and community safety systems to resonate with the needs of urban residents and sustainable development goals.**

***Index Terms*-- AI-Integrated Safety Solutions, Community safety, Smart City Technologies, Sustainable Development Goals (SDGs), IoT-Driven Community Safety**

I. INTRODUCTION

Promising community safety in today's urban context has become a complex task, especially in fast-growing cities like Chennai as population density increases and population agglomerations develop into actual cities the new dynamic and more traditional approaches towards risk reduction become under pressure. Raising concerns about lack of solutions to fight theft, medical urgencies and fire risks situations. These issues not only pose threats to the welfare of its members but also compromise the general health of the society, a reason there is a need to address the issue with an importance of reviewing the current literature. Measures concerning safety and the application of high technological solutions.

Urban safety encounters significant threats such as theft, medical AEDs, and fire threats which are compounded by the restraints of old-style systems and confined spaces. One form of insecurity that has continued to rear its head is theft and here, commonly used security measures such as installation of barriers and Alert Neighbor type programs are inadequate for contemporary techniques. Likewise, medical emergencies also reveal that structural responses for handling emergencies are not efficient and timely because of the legacy technologies that remain prevalent, and understate the potential of AI-IoT solutions for constant vigilance as well as timely follow-up actions. Potential fire threats add to these challenges, considering that the fire protection systems are weak in urban centers like Chennai due to a weak infrastructure. Upgrading securities using artificial intelligence, sensors, and intellectual security systems can change urban security by improving the identifying and repelling mechanisms and emergency interventions. Though, this needs an elaborate approach that incorporates the following issues: How to foster coordination, the cost of deploying such a solution, and patient data protection that has been deemed critical.

Chennai's safety mechanisms are at present more or less isolated, and are only triggered at the onset of a danger, risk or emergency the security against theft, medical facilities, and against fires are in the main confined to siloed infrastructures, and as such, the comfort of the people living in the city is not well secured to its full potential. A synergy incorporating AI and IoT heralds a solution package that addresses data processing, pattern identification, and incidence forecasting in an augmented, speedier, and coordinated way. IoT devices still act to maintain a continuous monitoring and connection to keep safety systems alert with threats. However, challenges which will impede the deployment of both AI and IoT include lack of awareness, costs of implementation, and data privacy another sign that the uptake should be strategic and nonexclusive. The use of AI- IoT to strengthen community safety systems is in line with the United Nations Sustainable Development Goals (SDGs) agenda and will support SDG 11 that addresses targets 11.1, 11.3 and 11.8 aimed at affordable housing, inclusive and sustainable urban development and ways to strengthen urban- rural relations. This project improves safety, advisory and security from theft, medical

emergencies, and fire and is made possible by technology. It also contributes to SDG 9 for the inclusion of innovative and infrastructure facilities. Based on people's perception to safety risk, existence of daily accidents and awareness of SDGs in target communities, the study outlines areas that AI and IoT can be applied in enhancing safety solutions and ways to involve the community. The purpose of the findings is to offer practical strategies for designing and implementing safe, long-lasting, and livable cities and town environments and supporting the economic, social and environmental relationship between urban, peri-urban, and rural areas.

II. Literature Review

A. Community Safety

Community safety is one of the most emergent challenges in defining the safety of populations within contexts of urban areas where new risks and vulnerable elements arise. In general, the issue needs management solutions that would ensure the desired outcome. Recent studies have focused towards the various facets of safety with respect to a given community in the following way. New methods that can assist with enhancing safety measures against theft, diseases or fire outbreaks.

Lang (2014) described the function of Community Health as CHWs in promoting general health among the analyzing the situation and identifying ways to increase the enrolment rate in health insurance by increasing the participation of CHWs. Their work also addresses the need of doing intervention through community based in enhancing safety and wellbeing. To an effort to provide an answer to this question Higgins (2013) produced a spatial model of fire. Prevention, emphasizing on the point that hazards are always specific. To minimize cases of wrong identification of vulnerable groups in the concerned community. Chien (2007) provided a detail larger scale of fire behavior that divides the fire behavior into further categories. Preventions measures based on Taipei City Fire Department, it's major focuses included reducing the frequency of fire incidences and fatalities in residential structures. These studies show that there is an increased consciousness of the significance of this is why measures intended to improve safety have to be specific and clearly communicated with respect to the community issues.

Al-Hajj (2023) conducted a study of the Home Safe Fire Prevention Program by tracking the fire rates for twelve years and paid witness to the effectiveness of enhancing the fire safety measures in the society. Thus, the efficacy of results achieved within the context of this program indicates that extended and community-based approaches could prove beneficial in improving fire safety conditions. In like manner, Beringer (2000) aimed to establish Australia's bushfire risk perception and precautionary measures taken by the residents without sufficient information and participation. Shuka (2017) provided an overview of fire management issues in the developing countries with supporting call for development of enhanced abilities for disaster response and improvement of the international cooperation. In corporately, this sort of findings also emphasis that the community based and educate approaches are key in increasing safety.

B. AI & IoT in Community Protection

The AI integration in the industry and IoT can help in getting better control over the processes as well as mitigating the threats of failure. Here, the measures of integrating the Internet of Things (IoT) into the community safety systems could be regarded as a large stride to approach the problem of urbanization safety challenges. The discussions on the role of AI and IoT prove that these two belong without a doubt to the most significant trends of the present-day world. In order to create the necessary shift in how communities define organizational protect and respond to manage safety incidents.

Kerning (2017) presented a mobile device based biometric identified proposal based on proximity. PIN entry, and identification of incidence. Such as gunshots. In short, this system shows how Artificial Intelligence could enhance possibly new forms of identification and new ways to identify incidents to increase the standard of personal protection. For example, in smart homes technology reliant on AI coupled with IoT sensors, Varadarajan (2024) studied the use of AI in conjunction with IoT sensors to automate the elements of protection and energy consumption. It further necessitates for both AI and IoT to work in consort development or integration to boost the home security and to effectively manage the home resources. Reddy (2024) described how people can use AI and Arduino controller to control home appliance based on environment information and increase safety and efficiency through the application of robots as an automation.

In general, studies have been done to investigate the security vulnerabilities of other device types (In particular, IoT), meneghello (2019) as cited, base their emphasis on security and preventive actions to ward off as much as possible risks. According to Dawson (2009), based on interfaces and communication appliances, this method allows improving the coordination of responses to the events in a security cluster of structures. These such kinds of studies show that how AI and IoT are used across different industries as well as context like: through better such enhanced surveillance system automation and coordination to improve community safety. Chen (2021) constructs integration blockchain technology and IoT devices to advance community safety through the working of alarms and their recording in especially. Tamper-proof data storage. This focuses on the roles in understanding what the contribution of secure data management is to the emphasis on safety system reliability. Likewise, Fernandes (2016) had also carried out the analysis of the SmartThings smart home platform and vulnerability analysis of smart apps and device handlers as well as proposed improvements to the protective gear that is even more effective. Smart home requires a lightweight authorization stack (Chifor 2017). Request or a transaction made by a user can be more secure requests, as an IoT device tries to forward commands to a user's smartphone to make him authenticate or to approve action, or otherwise. These studies demonstrate the importance of the very strong security and protected information. management, which are necessary to resourceful deploying AI and IoT technologies.

C. Sustainable Development Goals (SDGs) Towards Safety Review

The combination of the use of AI and IoT in community safety requirements in integrated health information technology systems embraces several Sustainable Development Goals, especially those of urban area in specific Sustainable Development Goals (SDGs) dx specific Sustainable Development Goals (SDGs) development and innovation. Especially, the goal of Sustainable Cities and Communities

which has the number 11 in the list of SDGs. (Communities) stresses the importance of designing safe and sustainable communes. and efficient and sustainable urban setups. The use of advanced technologies to improve community safety caters to by enhancing the ways of handling the safety risks in achieving the above goal. promoting resilience.

Sager (2015) formulated a system that would help parse data information. multiple sensors to give alert when certain Aim at improving the safety of cities, consistent with criteria implementing Sustainable Development Goal 11. through technology. Likewise, Smith (2018) narrated alone of the wireless communication technique for handling messages presenting the time relationship between security devices and servers, with the special concern on link latency. and message storage. This approach supports SDG 9 To achieve the UN Sustainable Development Goal 9 (Industry, Innovation, and Infrastructure), the following strategy will be adopted leveraging technology for enhancing health care business as well as health care delivery system. safety systems. Parkin (2019) evaluated the feasibility and concerns that smart assistant technology poses to security of the survivors of tech abuse, discovering major usability problems that affect the reason from field to field is based on the real world concerning the efficacy of safety technology. This research we help enhance SDG 3 which is Good Health and Well-being. focusing on the topic of technology and safety. Rushanan (2014) analyzed security and privacy types and challenges, improvements for implantable healthcare equipment and body associated networks, that means paying attention to the security of software and sensor interfaces to safeguard the person's health information.

Bluth (2009) suggested means and ways of enhancing security features thereby personal records of individual health in the community health facilities aiming at kiosks. emphasizing the need to protect the data that is collected in improving the health-Related Safety. Donovan (2009) introduced an alert and monitoring system that is intelligent numerical and video inputs with the rule of machine learning for crime prevention and safety. This system contributes to the realization of SDG11 in the following way using IT to enhance the security within a community response capability.

To summarize, it can be seen from the literature that there is an increasing awareness of a need for higher technologies in order to solve community safety challenges. The integration of AI and IoT provides great opportunity to improve existing safety systems. while the association of SDGs enhances and assures the global orientation. on the applicability of these technologies to sustainable urban form. Subsequent research should extend knowledge of new and less investigated approaches in the sphere. solutions and to judge whether they facilitate or hinder the enhancement of functions and purposes such as community safety and of resilience.

III. Public Opinion & Survey Results

A. Demographic Overview

The survey carried out in the five zones of Chennai – North, East, Central, West and South received 408 responses that could shed light on safety concerns in those communities. The distribution of responses was as follows: North Chennai represented 30.4% of the respondents (124 responses), East Chennai represented 19.4% (79 responses), Center Chennai represent 18.6% (76 responses), West Chennai represented 14.2% (58 responses), and South Chennai represented 17.4% (71 responses).

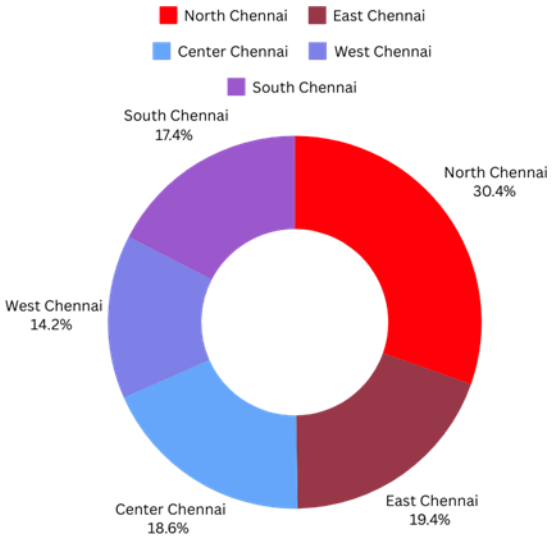


Figure 1: Responses by Geographic Region in Chennai Community Safety Survey

Therefore, North Chennai area should have presented more responses in terms of higher safety concern due to its contribution to nearly a third of the overall responses. This implies that there are differential safety risks in this area and possibly will need special approaches. On the other hand, East and South Chennai zones, with 19.4% and 17.4% of responses. Expressing significant safety concerns, but at a relatively lesser representation than North Chennai, 4% and 17.4% of the responses were noted. The two regions of Center and West Chennai still show considerable amount of response to Community Safety with 18.6% and 14.2% respectively.

Such variability in the distribution of responses to these regions suggests that people in these areas are subjected to dissimilar safety risks. According to the **Figure 1**, Analyzing the data collected from each area will make it easier when trying to analyze the different ways that we can help to enhance the community safety measures for all the residents in the Chennai.

B. Experiences with Theft

Out of all respondents 65.2% reported having been a direct victim or having known someone who has been a victim of theft and this highlighted a major insecurity issue that need to be addressed in most establishments. Notably, 83.5% of the respondents who dwelled on theft said the crime took place outside homes and not in homes themselves, therefore calling for involvement area safety measures. Additionally, 55.6% of participants reported experiencing gas leaks or expressed.

Figure 2: Incidence of Theft Experiences Among Survey Respondents

As shown in **Figure 2**, The received positive feedback on the effectiveness of AI based safety devices only supports the view of these technologies being useful in improving communal safety. All in all, these results depict severe safety hazards that require emergence of enhanced safety measures in Chennai.

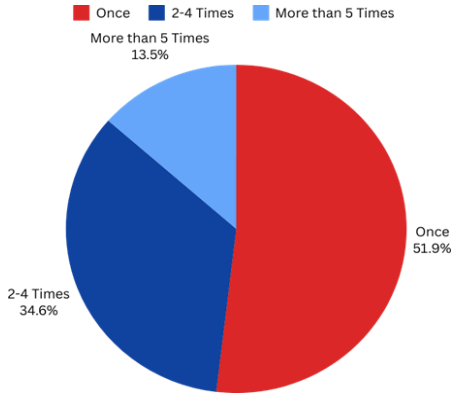


Figure 3: Frequency of Theft Incidents Reported by Respondents in the Community

As shown in **Figure 3**, The number of theft incidents reported was also quite high. Of the respondents who claimed to have fall victims to theft, 13.5 % of them said that such incidences had happened more than five time in the few years in their community. This was followed by 34.6% who reported incidents occurring 2-4 times, and 51.9% who experienced theft only once. These statistics further bring out the fact that theft issues in different societies are long-term, more so requiring hard and consistent efforts put in place for security measures to work effectively.

C. Identification and Communication of Theft

Different methods of identifying theft in the given communities came out in the responses and such disenfranchising reactions are some of the various facets of effort to ensure safety of such communities. The most common method was through reports from neighbors via physical communication, accounting for 33.8% of responses. This goes to show why much emphasis on direct neighborly surveillance in cases of theft is deemed critical. Perceived by security guards, answers 22.9% of respondents; while focus on importance of security guards in observing and reporting potential theft incidents took light. Among thefts 28.2% involved personal observation showing that a significant portion of the community relies on the incident. Communication through phone calls with neighbors was used in 11.3% of cases, barking dogs, as an example of an extralegal method of detection, were used in 3.8%. As seen in **Figure 4**, This data refutes a reductionist approach to theft detection, in which there are part and parcel a combination of structural and informal prevention styles.

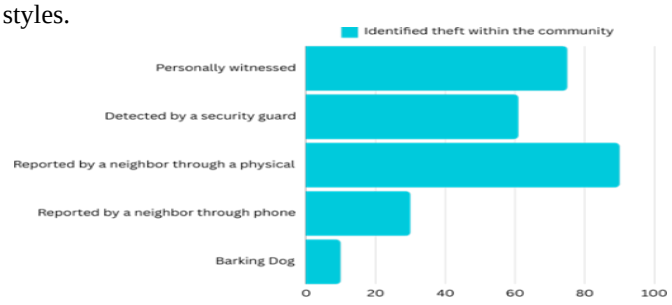


Figure 4: Methods of Theft Identification Reported by Respondents in the Community

Out of all the response options regarding to means of reporting theft, the largest number of respondents (48.1%) preferred to call the nearest neighbor directly. This was followed by using social media and community apps to inform everyone (9%). Other methods included communicating through phone to nearby neighbors (18.4%) and calling the police (24.4%). As illustrated in **Figure 5,** The use of direct and highly localized forms of communication as preferred illustrates the availability of timely methods to pass information on theft instant in neighborhoods

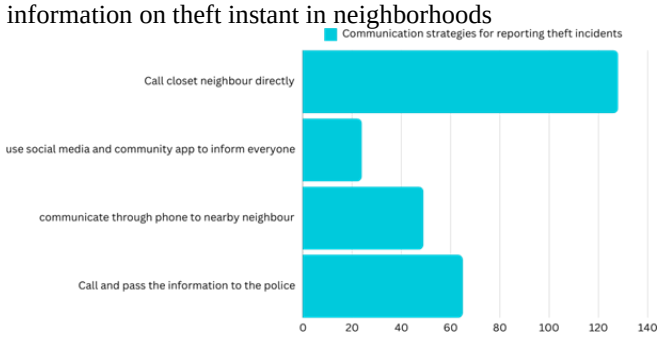
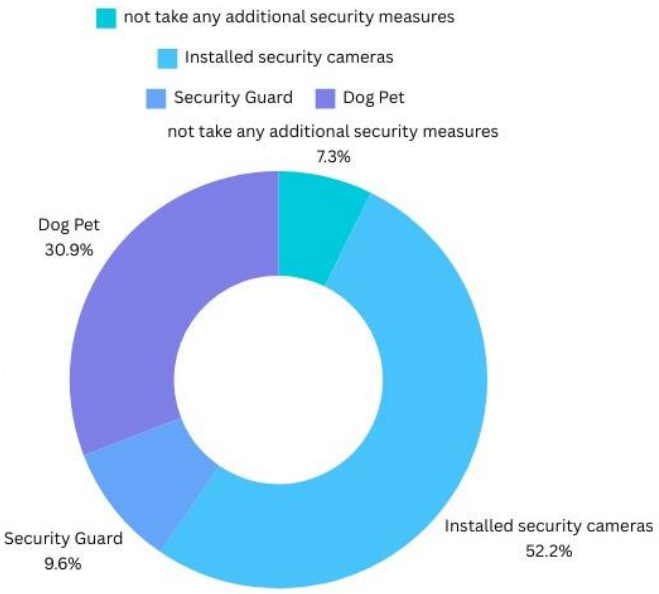


Figure 5: Preferred Communication Strategies for Reporting Theft Incidents

D. Additional Security Measures

When asked in a survey whether they have done anything extra after theft incidents, only 66.9% of respondents have. Of those that did, the most popular ones were security cameras (52.2%), employing security guards (9.6%), and using pet dogs for security (30.9%). A home security system was another feature found significantly less frequently, with the 7.3% of the respondents having it. The equally high rating given to security guards and even more emphasis laid on cameras can be interpreted as a preference for active safety increasing objects and personnel. As illustrated in **Figure 6&7** security guards and dogs show that Nuru has a strong inclination towards individual security assessment, and control as opposed to mechanical security measures.



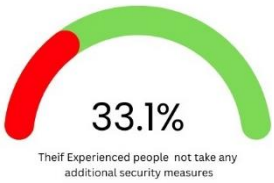


Figure 6 & 7: Security Measures Taken by Respondents After Theft Incidents

E. Awareness and Concerns about Gas Leaks

The survey investigated community's attitudes towards actual gas leaks and found out that 55.6% of the participants reported to have Come across with the menace of gas leaks in their home. Asked how concerned they are about the leakage of gas 72.8% said they are very concerned while 17.9% said they are concerned. 4.9 percent were non-committal and another 1.5 percent could be categorized as marginally concerned. Notably, 2.9% of participants were "not concerned," As shown in **Figure 8**, which highlights a widespread anxiety about this hazard.

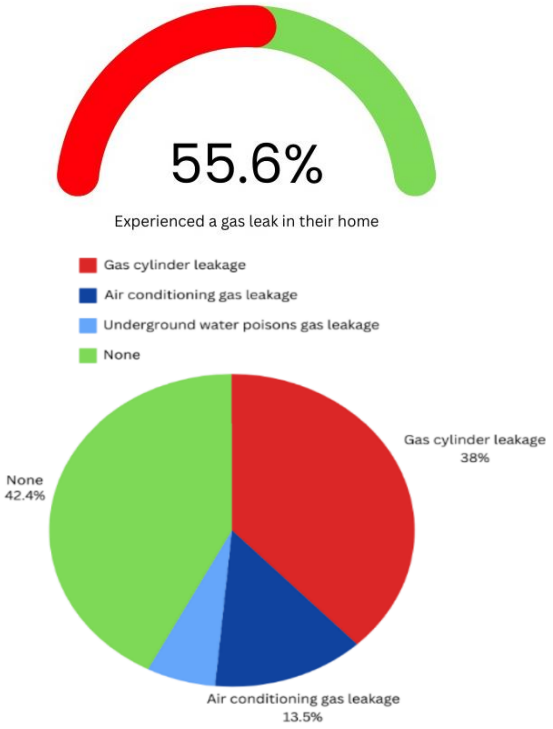


Figure 8 & 9: Respondents' Experiences and Concerns Regarding Gas Leaks

The data also shows variability in the types of gas leaks reported. 38% of respondents experienced cylinder leaks, 13.5% reported air conditioning leaks, and 6.1% encountered underground gas leaks. This variation makes it possible for there to be certain risks making their regions that influence the perception of the people towards gas leaks. For example, areas that register higher proportion of gas usage see more leakages probably due to increased commercial or dominance in densely inhabited residential areas hence higher concern from the people. This is in agreement with the findings depicted in **Figure 9,** Thus, it underlines the need to develop proper objective safety programmers' in risky populations to mitigate the hazard of varying gas leakage.

F. Awareness of Sustainable Development Goals (SDGs)

The survey assessed the respondents' perception of the UN Sustainable Development Goals (SDGs) more specifically, the goals of cutting co2 emissions by 2030. Shockingly, 85.3% of respondents never heard of these goals, which shows a lack of awareness relating to sustainable projects. Among the few who were aware, the most favored SDGs included Zero hunger (SDG 2), Good Health and Well- being (SDG 3), Quality education (SDG 4), and Affordable and Clean Energy (SDG 7). As shown in **Figure 10**, The fact that respondents are not familiar with most of the goals reviewed earlier means that people, in general, require more education when it comes to SDGs and how they can enhance safety in their communities and preserve the environment.

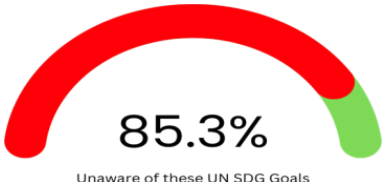


Figure 10: Respondents' Awareness and Preferences Regarding UN Sustainable Development Goals (SDGs)

G. Feedback on AI Integrated Community Safety Gadgets

The intended AI Integrated Community Safety Devices were the focal concern of the survey conducted aimed at gathering constructive opinions. The effectiveness of these devices was also high, where 67.4 per cent perceived these devices as highly effective, and 23.8 per cent seeing it as very effective. A paltry 2.2%-described them as being moderately effective, while 2% said they were not effective at all. This positive feedback informs a strong embracement of AI based safety solutions within the communities. Furthermore, 248 (79.7%) respondents stated their interest to undergo further testing or to provide more feedback, according to the results presented in **Figure 11.**

Figure 11: Respondents' Feedback on AI Integrated Community Safety Devices

IV. Proposed AI-CSD Project

A. Scope of the AI-Integrated Home and Community Protection System

The AI-Integrated Home and Community Protection System is expected to change community safety by establishing a functional prototype to prevent and respond to events like theft, fire, medical events, and poor air quality. This system embraces artificial intelligent (AI) and internet of things (IoT) technologies to help provide efficient emergency response in both the Urban and the Rural context.

System Overview: The prototype is smart devices placed ideally in homes to respond to emergencies by monitoring the environment. All the devices are operated both by buttons and voice, in the case of the emergency report, while

the set of the sensors includes voice and toxic air and fire detectors. It starts visual and audio alarms including bells and solar- charged lights should there be an emergency in informing the centr al community about the emergency. It also instantly sends a text message or a call to the police or an ambulance or fire-brigade and operates from a control room. As it is exemplified in Figure 12, Utilizing a serialized LAN based communication network, the devices guarantee that the signal does not stop even if one part is a loss.

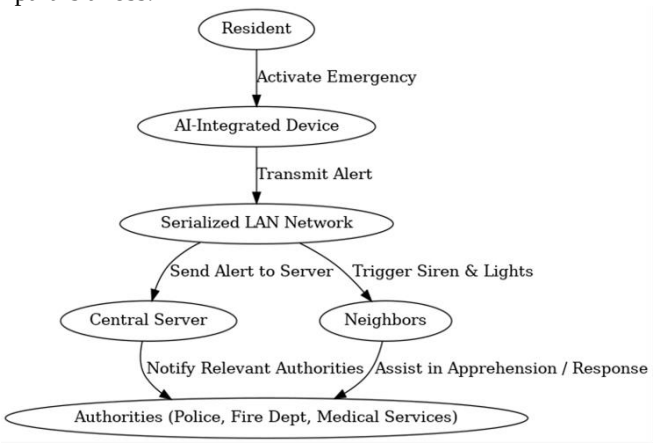


Figure 12: AI Integrated Community Safety Devices (CSD)Work Flow

B. **Key Features:**

- Emergency Detection:
  - **Manual:** Push buttons for reporting theft, fire, and medical emergencies.
  - **Voice Command:** Separate voice commands for each emergency situation (e.g., "Fire," "Thief," "Air," "Medical") to trigger the system if the user cannot press the buttons.
- **AI-Based Air Quality Monitoring:** Gas detectors such as the one used to identify the concentrations of carbon monoxide and problems such as leakages in air conditioning systems.
- **Community Communication Network:** Alerts neighbors and authorities through a serialized LAN network within a 1 km radius.
- **Siren and Solar-Powered Lighting:** Used to sound sirens and solar installed light in the neighboring compound to create awareness during emergencies.
- **Central Control Room Communication:** It listens to signals coming from the devices and sends messages to the emergency facilities.
- **Solar Power Supply:** It can function mostly through the use of solar power with an interface for plugging in a secondary source of power.

C. ***Importance of the AI-Integrated System:*** The integration of AI and IoT technologies in the AI-Integrated Home and Community Protection System brings forth numerous benefits, particularly in the context of achieving the Sustainable Development Goals (SDGs), including SDG 11 & SDG 3.

Comprehensive Emergency Response Mechanism: The smart device situated in the neighborhood basically includes a pouch of several buttons for system activation, and a Voice Recognition Module, which when pressed or used to report emergencies, allows fast response irrespective of the stressful state of the person in charge. Every device is equipped with basic sensors as follows; the MQ-135 Air Quality Sensor for detecting toxic gases, the Flame Sensor for fire detection and the DHT22 Temperature and Humidity Sensor for environmental checks. All these components ensure that a rich safety-net is developed thus improving he public health and safety.

Resilience and Community Engagement: A serialized LAN architecture of the Community Communication Network within the system guarantees that an alert will spread to neighbors and necessary authorities within a 1 KM radius even if one communication line is out of order. It also helps in the creation of partnership towards safety of the community since the residents can defend themselves against threats.

Alignment with Sustainable Development Goals: This project helps in the achievement several of the United Nations Sustainable Development Goals (SDGs) mainly for SDG 3 – Good Health and Well Being As a result of completing this project, you will be contributing the achievement of Targets 11.1, 11.3 and 8 under the United Nations Sustainable Development Goals (UN SDG) 11- Sustainable Cities and Communities which seek to provide access to adequate, safe and affordable housing, Goals of prompt emergency identification and reporting fit into SDG 3 because efficient medical intervention is important to save lives and enhance community health. Apart from rescuing the people's health from the threat of poor air quality, the AI-based monitoring also contributes to the achievement of another non-communicable goal formulated in SDG 11, which is to make the cities sustainable.

Effective Alert Systems: Visual Led by the Mini Buzzer/Speaker and the Solar-Powered LED Lights, the end-users receive alerts in both visions and hearings, notifying the households near them promptly of the emergencies. The central control room is a voice and message-sending center, which reduces the need for delay and increases the cohesiveness of communities when contacting emergency services.

V. CONCLUSION

Instead, the innovative Home and Community Protection System is an actual advancement in today's world to address the challenges in emergency management and protecting the members of the community. Based on over 408 individuals' structured questionnaires collected both online and offline, the current work contributes novel insights into the current state of community safety and effectiveness of the proposed technical solutions. According to the poll, over 65.2% of respondents had either experienced theft themselves or knew someone who had. This implies that theft is an issue that affects most people in their day-to-day life activities. Moreover, the frequency recorded for theft cases supports the need for an efficient security system. As we know, expanding the use of AI systems enhances the capability to discover and prevent theft, medical emergency cases, fire hazards, and air quality problems significantly. Some of these technologies are real- time data

processing technology, and automated alarm technology. Conversely, the study shows that a very high proportion of respondents, 55.6%, report that they either discovered gas leaks in their houses or are highly sensitive to them. This problem is directly solved by the AI Integrated System for the ability to track air quality and determine that substances are dangerous and provide instant alerts and precautions. Encouraging remarks with regard to the effectiveness of AI safety devices also support the possibility of a vast future influence on community safety. Subsequent development of the AI-Integrated Home and Community Protection System will focus on fine-tuning the design of the current prototype; increasing its scalability; and improving the caliber of voice recognition and the sensors involved in this project contribute to the realization of Targets 11.1, 11.3, and 11.8 of SDG 11 by promoting housing availability, and integrated urbanization, and bridging urban-rural divides. It calls for smarter, safer urban systems that can respond more nimbly and flexibly to meet the needs of the community while at the same time, the pursuit of the SDGs.

VI. Reference

[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.

[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 States Patent No. 6,060,994. Filed Jan.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 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.

CERTIFICATES

MANAV RACHNA vidyanatariksha | NAACA++ ACCREDITED | SET School of Engineering & Technology | IEEE INDIA COUNCIL | IEEE 140 YEARS | MOBILITY

SUSTAINED-2024

IEEE Conference Record #63638

13th - 14th December, 2024

1st International Conference on Sustainability and Technological Advancements in Engineering Domain

Organized by

School of Engineering & Technology,

Manav Rachna International Institute of Research and Studies, Faridabad

in Association with SDA Committee IEEE India Council

Certificate of Presentation

Paper ID – 435

This is to certify that **Santhosh R** from Department of CSE, Dr. M.G.R. Educational and Research Institute, Maduravoyal, Chennai-95, TamilNadu has presented a paper titled **"Study on Community Safety & Recommendations for Proposed AI-Integrated Community Devices Towards SDG 11"** authored by Thanush Kannan, Santhosh R, Pious Niranjan A, L. Ramesh, S. Geetha, T. Kavitha, A. Maheswari, V. Priyadarshini and Dhanush Raj N.

Conference Chair & Convener
Prof. (Dr.) Brahma Nand Agrawal
Professor, Department of Mechanical Engineering
MRIIRS, Faridabad

General Chair
Prof. (Dr.) Pardeep Kumar
Pro-Vice Chancellor
MRIIRS, Faridabad

Patron
Prof. (Dr.) Sanjay Srivastava
Vice Chancellor
MRIIRS, Faridabad

MANAV RACHNA vidyanatariksha | NAACA++ ACCREDITED | SET School of Engineering & Technology | IEEE INDIA COUNCIL | IEEE 140 YEARS | MOBILITY

SUSTAINED-2024

IEEE Conference Record #63638

13th - 14th December, 2024

1st International Conference on Sustainability and Technological Advancements in Engineering Domain

Organized by

School of Engineering & Technology,

Manav Rachna International Institute of Research and Studies, Faridabad

in Association with SDA Committee IEEE India Council

Certificate of Presentation

Paper ID – 435

This is to certify that **Thanush Kannan** from Department of CSE, Dr. M.G.R. Educational and Research Institute, Maduravoyal, Chennai-95, TamilNadu has presented a paper titled **"Study on Community Safety & Recommendations for Proposed AI-Integrated Community Devices Towards SDG 11"** authored by Thanush Kannan, Santhosh R, Pious Niranjan A, L. Ramesh, S. Geetha, T. Kavitha, A. Maheswari, V. Priyadarshini and Dhanush Raj N.

Conference Chair & Convener
Prof. (Dr.) Brahma Nand Agrawal
Professor, Department of Mechanical Engineering
MRIIRS, Faridabad

General Chair
Prof. (Dr.) Pardeep Kumar
Pro-Vice Chancellor
MRIIRS, Faridabad

Patron
Prof. (Dr.) Sanjay Srivastava
Vice Chancellor
MRIIRS, Faridabad

MANAV RACHNA vidyanatarikshat | NAACA++ ACCREDITED | SET School of Engineering & Technology | IEEE INDIA COUNCIL | IEEE 140 YEARS | MOBILITY

SUSTAINED-2024

IEEE Conference Record #63638

13th - 14th December, 2024

1st International Conference on Sustainability and Technological Advancements in Engineering Domain

Organized by

School of Engineering & Technology,

Manav Rachna International Institute of Research and Studies, Faridabad

in Association with SDA Committee IEEE India Council

Certificate of Presentation

Paper ID – 435

This is to certify that **Pious Niranjan A** from Department of CIVIL, Dr. M.G.R. Educational and Research Institute, Maduravoyal, Chennai-95, TamilNadu has presented a paper titled **"Study on Community Safety & Recommendations for Proposed AI-Integrated Community Devices Towards SDG 11"** authored by Thanush Kannan, Santhosh R, Pious Niranjan A, L. Ramesh, S. Geetha, T. Kavitha, A. Maheswari, V. Priyadarshini and Dhanush Raj N.

Conference Chair & Convener	General Chair	Patron
Prof. (Dr.) Brahma Nand Agrawal	Prof. (Dr.) Pardeep Kumar	Prof. (Dr.) Sanjay Srivastava
Professor, Department of Mechanical Engineering, MRIIRS, Faridabad	Pro-Vice Chancellor, MRIIRS, Faridabad	Vice Chancellor, MRIIRS, Faridabad

MANAV RACHNA vidyanatarikshat | NAACA++ ACCREDITED | SET School of Engineering & Technology | IEEE INDIA COUNCIL | IEEE 140 YEARS | MOBILITY

SUSTAINED-2024

IEEE Conference Record #63638

13th - 14th December, 2024

1st International Conference on Sustainability and Technological Advancements in Engineering Domain

Organized by

School of Engineering & Technology,

Manav Rachna International Institute of Research and Studies, Faridabad

in Association with SDA Committee IEEE India Council

Certificate of Presentation

Paper ID – 435

This is to certify that **Dhanush Raj N** from Department of CIVIL, Dr. M.G.R. Educational and Research Institute, Maduravoyal, Chennai-95, TamilNadu has presented a paper titled **"Study on Community Safety & Recommendations for Proposed AI-Integrated Community Devices Towards SDG 11"** authored by Thanush Kannan, Santhosh R, Pious Niranjan A, L. Ramesh, S. Geetha, T. Kavitha, A. Maheswari, V. Priyadarshini and Dhanush Raj N.

Conference Chair & Convener	General Chair	Patron
Prof. (Dr.) Brahma Nand Agrawal	Prof. (Dr.) Pardeep Kumar	Prof. (Dr.) Sanjay Srivastava
Professor, Department of Mechanical Engineering, MRIIRS, Faridabad	Pro-Vice Chancellor, MRIIRS, Faridabad	Vice Chancellor, MRIIRS, Faridabad

IEEE COPYRIGHT AND CONSENT FORM

To ensure uniformity of treatment among all contributors, other forms may not be substituted for this form, nor may any wording of the form be changed. This form is intended for original material submitted to the IEEE and must accompany any such material in order to be published by the IEEE. Please read the form carefully and keep a copy for your files.

AI-Integrated Community Safety Solutions for Smart Cities: A Study Towards SDG 11

Thanush Kannan, Santhosh R, Pious Niranjan A, Dhanush Raj N, L.Ramesh, S.Geetha, T.Kavitha, K.Anitha, A.Maheswari, V.Priyadarshini, J.Balamurugan

2024 1st International Conference on Sustainability and Technological Advancements in Engineering Domain (SUSTAINED)

COPYRIGHT TRANSFER

The undersigned hereby assigns to The Institute of Electrical and Electronics Engineers, Incorporated (the "IEEE") all rights under copyright that may exist in and to: (a) the Work, including any revised or expanded derivative works submitted to the IEEE by the undersigned based on the Work; and (b) any associated written or multimedia components or other enhancements accompanying the Work.

GENERAL TERMS

1. The undersigned represents that he/she has the power and authority to make and execute this form.
2. The undersigned agrees to indemnify and hold harmless the IEEE from any damage or expense that may arise in the event of a breach of any of the warranties set forth above.
3. The undersigned agrees that publication with IEEE is subject to the policies and procedures of the IEEE PSPB Operations Manual.
4. In the event the above work is not accepted and published by the IEEE or is withdrawn by the author(s) before acceptance by the IEEE, the foregoing copyright transfer shall be null and void. In this case, IEEE will retain a copy of the manuscript for internal administrative/record-keeping purposes.
5. For jointly authored Works, all joint authors should sign, or one of the authors should sign as authorized agent for the others.
6. The author hereby warrants that the Work and Presentation (collectively, the "Materials") are original and that he/she is the author of the Materials. To the extent the Materials incorporate text passages, figures, data or other material from the works of others, the author has obtained any necessary permissions. Where necessary, the author has obtained all third party permissions and consents to grant the license above and has provided copies of such permissions and consents to IEEE

You have indicated that you DO wish to have video/audio recordings made of your conference presentation under terms and conditions set forth in "Consent and Release."

CONSENT AND RELEASE

1. ln the event the author makes a presentation based upon the Work at a conference hosted or sponsored in whole or in part by the IEEE,

the author, in consideration for his/her participation in the conference, hereby grants the IEEE the unlimited, worldwide, irrevocable permission to use, distribute, publish, license, exhibit, record, digitize, broadcast, reproduce and archive, in any format or medium, whether now known or hereafter developed: (a) his/her presentation and comments at the conference; (b) any written materials or multimedia files used in connection with his/her presentation; and (c) any recorded interviews of him/her (collectively, the "Presentation"). The permission granted includes the transcription and reproduction of the Presentation for inclusion in products sold or distributed by IEEE and live or recorded broadcast of the Presentation during or after the conference.

2. In connection with the permission granted in Section 1, the author hereby grants IEEE the unlimited, worldwide, irrevocable right to use his/her name, picture, likeness, voice and biographical information as part of the advertisement, distribution and sale of products incorporating the Work or Presentation, and releases IEEE from any claim based on right of privacy or publicity.

BY TYPING IN YOUR FULL NAME BELOW AND CLICKING THE SUBMIT BUTTON, YOU CERTIFY THAT SUCH ACTION CONSTITUTES YOUR ELECTRONIC SIGNATURE TO THIS FORM IN ACCORDANCE WITH UNITED STATES LAW, WHICH AUTHORIZES ELECTRONIC SIGNATURE BY AUTHENTICATED REQUEST FROM A USER OVER THE INTERNET AS A VALID SUBSTITUTE FOR A WRITTEN SIGNATURE.

A.Pious Niranjan	10-01-2025
Signature	Date (dd-mm-yyyy)

Information for Authors

AUTHOR RESPONSIBILITIES

The IEEE distributes its technical publications throughout the world and wants to ensure that the material submitted to its publications is properly available to the readership of those publications. Authors must ensure that their Work meets the requirements as stated in section 8.2.1 of the IEEE PSPB Operations Manual, including provisions covering originality, authorship, author responsibilities and author misconduct. More information on IEEE’s publishing policies may be found at http://www.ieee.org/publications_standards/publications/rights/authorrightsresponsibilities.html Authors are advised especially of IEEE PSPB Operations Manual section 8.2.1.B12: "It is the responsibility of the authors, not the IEEE, to determine whether disclosure of their material requires the prior consent of other parties and, if so, to obtain it." Authors are also advised of IEEE PSPB Operations Manual section 8.1.1B: "Statements and opinions given in work published by the IEEE are the expression of the authors."

RETAINED RIGHTS/TERMS AND CONDITIONS

- Authors/employers retain all proprietary rights in any process, procedure, or article of manufacture described in the Work.
- Authors/employers may reproduce or authorize others to reproduce the Work, material extracted verbatim from the Work, or derivative works for the author's personal use or for company use, provided that the source and the IEEE copyright notice are indicated, the copies are not used in any way that implies IEEE endorsement of a product or service of any employer, and the copies themselves are not offered for sale.
- Although authors are permitted to re-use all or portions of the Work in other works, this does not include granting third-party requests for reprinting, republishing, or other types of re-use.The IEEE Intellectual Property Rights office must handle all such third-party requests.

- Authors whose work was performed under a grant from a government funding agency are free to fulfill any deposit mandates from that funding agency.

AUTHOR ONLINE USE

- **Personal Servers**. Authors and/or their employers shall have the right to post the accepted version of IEEE-copyrighted articles on their own personal servers or the servers of their institutions or employers without permission from IEEE, provided that the posted version includes a prominently displayed IEEE copyright notice and, when published, a full citation to the original IEEE publication, including a link to the article abstract in IEEE Xplore. Authors shall not post the final, published versions of their papers.
- **Classroom or Internal Training Use.** An author is expressly permitted to post any portion of the accepted version of his/her own IEEE-copyrighted articles on the author's personal web site or the servers of the author's institution or company in connection with the author's teaching, training, or work responsibilities, provided that the appropriate copyright, credit, and reuse notices appear prominently with the posted material. Examples of permitted uses are lecture materials, course packs, e-reserves, conference presentations, or in-house training courses.
- **Electronic Preprints.** Before submitting an article to an IEEE publication, authors frequently post their manuscripts to their own web site, their employer's site, or to another server that invites constructive comment from colleagues. Upon submission of an article to IEEE, an author is required to transfer copyright in the article to IEEE, and the author must update any previously posted version of the article with a prominently displayed IEEE copyright notice. Upon publication of an article by the IEEE, the author must replace any previously posted electronic versions of the article with either (1) the full citation to the IEEE work with a Digital Object Identifier (DOI) or link to the article abstract in IEEE Xplore, or (2) the accepted version only (not the IEEE-published version), including the IEEE copyright notice and full citation, with a link to the final, published article in IEEE Xplore.

Questions about the submission of the form or manuscript must be sent to the publication's editor.
Please direct all questions about IEEE copyright policy to:
IEEE Intellectual Property Rights Office, copyrights@ieee.org, +1-732-562-3966

Acceptance/ Registration Notification – IEEE International Conference on Data Science and Business Systems' 25

1 message

Microsoft CMT <email@msr-cmt.org>
Reply to: Rajkumar R Ramareddy <rajkumar2@srmist.edu.in>
To: Thanush Kannan <thanushlokesh1@gmail.com>
Cc: shanthia@srmist.edu.in

Wed, 2 Apr, 2025 at 12:15 pm

Dear Author

We are pleased to inform you that your paper, ID: 2490 with title "AI-Driven Smart Safety Framework for Community Protection", has been accepted for presentation at International Conference on Data Science and Business Systems, to be held on 17th and 18th of April 2025 at SRM Institute of Science and Technology, Kattankulathur, Chennai, India.
The decision was based on a rigorous review process, and we appreciate your valuable contribution to the field of Data Science and Business Systems. Your paper will be included in the conference proceedings, and we look forward to your presentation.
Next Steps:

1. Final Camera-Ready Submission: Please submit the final version of your paper by 05.04.2025, following the formatting guidelines provided on our website. If you have received review comments in CMT from the reviewers, we request you to kindly update your papers and keep it ready for submission. The IEEE paper format is attached herewith.

2. Author Registration: At least one author must complete the registration process by 04.04.2025 to ensure inclusion in the proceedings. The registration fee for the conference is specified in the website for which one author shall be invited for presenting the paper in the conference. For every additional author Rs 1000 need to be paid in addition. Please note only the first author will receive the conference kit. All presenting authors will receive certificates.
The registration fee has to be paid to the following account
Name of the Bank/Branch: City Union Bank Ltd/Tambaram Branch
Account Name: SRM INSTITUTE DEPARTMENT OF DATA SCIENCE AND BUSINESS SYSTEMS
Account No: SB 500101012990507
IFSC Code : CIUB0000117
Swift Code: CIUBIN5M (Only for overseas participants paying in USD)

Post registration, kindly fill the form provided here.

https://forms.gle/PtJjN32NvqLc3JUf9

3. Foreign Author: The paper is considered to be a foreign author paper if anyone of the author is from institutions abroad
4. Presentation Details: We will provide further details on the presentation schedule and format soon.
5. Reviewers Comments: Reviewers comments shall be sent to you separately, if not received kindly contact the below mentioned mail ID.
6. We advise you to expedite the registration process as early as possible as the conference papers will be published in IEEE Xplore.
For any queries, please contact us at icdsbs.2025@srmist.edu.in.
We congratulate you on your acceptance and look forward to welcoming you in our conference.

Please visit conference website for detailed information

Best regards,
Dr. Kavitha V
HoD, Department of Data Science and Business Systems
Chair - IEEE ICDSBS'25
2nd International Conference on Data Science And Business Systems - SRMIST

AI-Driven Smart Safety Framework for Community Protection

K.Thanush,R.Santhosh
Department of CSE,
Dr. M.G.R. Educational and Research Institute,
Chennai, India.
santhosh.ai.dev@gmail.com

A.Pious Niranjan, N.Dhanush Raj
Department of Civil,
Dr. M.G.R. Educational and Research Institute,
Chennai, India.
igen.pious@gmail.com

L.Ramesh
Department of EEE,
Dr. M.G.R. Educational and ResearchInstitute,
Chennai, India.
prof.greenramesh@gmail.com

S.Geetha,T.Kavitha
Department of CSE & CIVIL,
Dr. M.G.R. Educational and Research Institute,
Chennai, India.

Anton Xavier Bronson, Maheswari,V.Priyadarshini
Department of CSE & CIVIL
Dr. M.G.R. Educational and Research Institute,
Chennai, India.

Amudhan Panneerselvam
Department of ECE,
Director,
Workbeetles llp

Abstract **- Safety in the community is still a major issue in smart city planning, with growing issues of theft, fire risks, gas leaks, and delayed emergency responses. A survey of residential communities in Chennai found that 65.2% of the respondents had theft incidents, mostly in community areas (83.5%), and 55.6% had gas leaks, with 72.8% showing high concern for safety threats. To counteract the limitations, we developed an AI-Based Home and Community Safety System based on IoT-based sensors, real-time communication protocols, and mobile-based monitoring interface. The system consists of flame and gas sensors, OLED display, theft, medical, and false alarm push buttons, and buzzers and LED indicators for notification. A wireless communication framework based on MQTT protocol supports real-time emergency notification among the households to provide immediate response and risk reduction. There is also an IoT dashboard on mobile provided for real-time remote monitoring and controlling of the system, which facilitates ease of access and user interaction. The survey also reflected high community interest in AI-based safety systems with 67.4% considering them to be highly effective and 79.7% willing to trial the system. Prototype testing proved low-latency notifications, efficient hazard detection, and enhanced emergency response systems. The suggested system is in compliance with Sustainable Development Goals (SDG 11 & SDG 9) by increasing the resilience of cities and encouraging smart safety infrastructure.**

Index Terms **- Community safety, AI, IoT, MQTT, Smart cities, Emergency response, Sustainable Development Goals, Urban resilience, IoT dashboard, Remote monitoring**

I. INTRODUCTION

With the cities continuing to expand, communities' safety is now a city's number-one priority worldwide. With projections indicating that 66% of the world's population will reside in cities by the year 2050, cities are increasingly faced with the imperative of finding effective, scalable, and innovative solutions to safety issues. Traditional security systems are usually ineffective in the event of an emergency situation such as theft, fire hazards, gas leaks, and medical issues. Conventional methods like CCTV cameras, security personnel, and human monitoring systems are normally hindered by delayed response, non-real-time communication, and inefficiencies in emergency handling. Urban dwellers consequently often have to count on neighbors or security officers to notice and respond to events, adding to emergency response delays.

The Internet of Things (IoT) and artificial intelligence (AI)-based automation are the groundbreaking technologies that pose the potential to transform urban safety by providing interconnected, real-time monitoring solutions. IoT equipment, with intelligent sensors and automated alert mechanisms, offer real-time surveillance and instant alerts and are thus mandatory for addressing the issues of urban safety. Nevertheless, their adoption into current urban infrastructure is limited, which prevents them from fully realizing their capability to advance community security.

The system is scalable and flexible in nature, providing an end-to-end and integrated solution for various safety requirements. With the use of IoT and AI technologies, the system facilitates the attainment of Sustainable Development Goals (SDG 11: Sustainable Cities and Communities) and SDG 9: Industry, Innovation, and Infrastructure. The technologies not only make cities more resilient but also facilitate the creation of smarter and safer cities with automation and real-time response.

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.

II. RELATED WORK

Current smart home security systems are mostly based on traditional technologies like CCTV monitoring, alarm systems, and smart locks. Although these technologies provide some level of security, they have serious limitations, such as response time lags, high expense, and absence of AI-based real-time intervention. This section discusses recent developments in smart security systems, outlining current gaps

and explaining why there is a need for an AI-based home and community safety solution.

A. *Smart Home Security Solutions*

The conventional security methods, including CCTV and alarm systems, have been well researched. Sherif et al. [1] have suggested a home security system driven by LoRa that combines manual and automatic alert capabilities. Yet, its manual dependency restricts real-time automated action. Alahi et al. [2] have studied IoT and AI usage in smart cities, but their model prioritized surveillance over active threat protection. Yu and Zhang [3] proposed a contactless attack detecting smart home system, with eventual prospects of employing AI for anomaly detection. Analogously, Han [4] contrasted centralised and decentralised home-to-home (H2H) communication in intelligent communities but had no AI-dependent real-time warnings for crisis.

IoT-based security systems have been explored extensively. Nettikadan [5] used MQTT for real-time data transmission by deploying an IoT-based monitoring platform. But its system did not include AI for predictive analysis. Çavaş [6] surveyed IoT-based security alarm systems and found connectivity and cyber attacks to be major issues. Al Rakib et al. [7] created a GSM-based remote security system, and Alam Majumder et al. [8] incorporated motion sensing and facial recognition into IoT-based security systems. Although these works improve automation, they do not include AI-based decision-making for emergency response.

B. *Communication and Alert Mechanisms*

Current security systems are based on different modes of communication and alert systems. Merjanian et al.[9] designed a community safety notification system that classifies users into groups for specific safety notifications. Fujii et al. [10] presented the e-JIKEI Network, utilizing household computers and open-source software to enhance neighborhood watch schemes. Although such systems augment communication, they lack real-time AI-based event forecasting. Mobile-based security systems have also received interest. Saito [11] designed a mobile security system that alerts authorities in emergency situations. Redlich [12] proposed a cryptographic security system with multi-level encryption for secure data protection. Kerning [13] also designed a mobile app with GPS tracking, a panic button, and drone-supported surveillance. Although these systems enhance personal safety, they do not create a community-wide AI-powered response system.

C. AI and IoT-Based Security Enhancements

Recent studies highlight AI's role in enhancing home security. Ni et al. [14] developed a web-based communication system that delivers live video alerts, but it lacked predictive AI capabilities. Freund [15] proposed a consensus security framework among connected devices, while Long [16] integrated facial recognition with Bluetooth positioning to improve community security. Varadarajan [17] explored AI-integrated IoT sensors for smart home automation, emphasizing energy management. But these are disjointed systems and do not have a singular AI-based security system for live community safety. Dawson [18] presented a security cluster model to handle multiple safety devices in real-time with notifications, yet not with AI-driven event forecasting.

D. Research Gaps and Proposed Improvements

Even with the improvements in smart security, existing systems are still reactive in nature and tend to act in silos without integration towards coordinated action. Solutions available emphasize mostly on stand-alone aspects such as surveillance, alarm systems, or mobile notification, without actual real-time use of AI-coordinated responses. These systems usually rely on manual intervention by the user, thus causing delays in emergency response.

The suggested AI-Integrated Home and Community Safety System aims to solve these issues using IoT sensor networks and MQTT-based communication to provide hassle-free connectivity. The system allows real-time emergency alerts, predictive analytics, and automated response to multiple types of hazards, including theft, medical distress, and fire risks. The web and mobile app interface is a friendly interface that offers users a platform to observe their surroundings and be alerted instantly by the system. Additionally, the system supports SDG 11 (Sustainable Cities and Communities) and SDG 9 (Industry, Innovation, and Infrastructure) to provide a sustainable and intelligent solution for community safety. With real-time communication, predictive features, and AI-based automation, this system improves emergency response time and encourages proactive security for households and neighborhoods.

III. PROPOSED SYSTEM

System Architecture: The system proposed herein integrates both hardware and software components to obtain an end-to-end home and community security solution. Hardware includes sensors, a microcontroller, an alert system, and a display, whereas software employs MQTT communication for real-time data transfer such that alerts reach the intended parties.

A. Hardware Components:

The hardware design of the system revolves around the ESP8266 microcontroller as the processing element that is responsible for Wi-Fi communication and optimized interaction with other sensors. In end-to-end safety monitoring, the system features gas, fire, and motion sensors that detect potential threats such as gas leakage, fire hazards, and intrusions. The toxic gas sensor continuously monitors the toxic gas concentration, and the fire sensor, the flame sensor, detects the anomalies of fire in real-time. A buzzer and an OLED screen are also incorporated to provide local immediate alarm. The buzzer alarm goes off with a sound warning signal when any risk is detected, and the OLED screen presents real-time system status and sensor condition. In addition, the system consists of medical and theft alert buttons that enable individuals to activate emergency alerts manually. These alerts are either activated using physical buttons on the device or through a web and mobile application interface, thus making remote activation possible and easy for a fast emergency response.

B. Software Components:

The system's architecture employs MQTT as a light-

weight and efficient device-to-device messaging protocol. The system also incorporates a web and mobile app interface, where users have a central platform through which they can remotely monitor and manage security alarms. Sensor threat indications are communicated in real time to this interface to facilitate a rapid response mechanism. AI plays a critical role in improving decision-making by analyzing patterns in sensor data (e.g., gas levels, flame detection, button press duration). A lightweight decision tree algorithm is used at the edge level to differentiate between real and false threats based on historical input values and context (e.g., time of day, frequency). This allows the system to suppress false alarms and prioritize genuine emergency events. Additionally, anomaly detection techniques are used to flag unusual sensor behavior that may indicate system tampering or unseen emergencies.

C. Communication Flow:

The system to be proposed adopts a systematic communication pattern to provide effective real-time transmission of security alerts. Data from gas, and fire sensors are initially gathered and processed by the ESP8266 microcontroller, which acts as the central processing unit for data acquisition and transmission.When an anomaly is identified, the ESP8266 forwards the sensor information to an MQTT broker, which forwards the alert to all registered devices, including adjacent homes and the respective authorities. This provides a quick, automatic response to possible emergencies.The alert information is also posted to the web and mobile app interfaces, where users can view critical event details and respond accordingly. In the event of fires, gas leaks, or burglaries, the system provides automatic alerts to surrounding residences (House 1 and House 2) to enable immediate community-based response. Besides individual homes, the system also facilitates community-level communication, where all the registered members of a given area receive synchronized security alerts, which facilitates a response system to provide collective security and crisis management.

D. System Advantages over Existing Solutions:

The proposed system differs from existing solutions in the following ways:

- **Multi-Trigger Detection:** Combines flame, gas, theft, and medical alerts with both sensor and manual inputs.
- **AI Filtering:** Uses AI to reduce false alarms based on sensor behaviours.
- **MQTT over TLS:** Ensures faster, secure communication compared to traditional GSM alerts.
- **Real-Time Dashboard**: Integrates for immediate status updates and control.
- **Scalability:** Supports integration into both individual homes and gated communities.

IV. Implementation & Experimentation

A. Prototype Design:

The proposed prototype uses various sensors, communication media, and alarm systems to detect and respond to emergencies such as theft, health issues, gas leakage, and fire hazard. The system consists of the following principal hardware components:

For real-time messaging, the system uses the MQTT protocol to provide instant Wi-Fi-based messaging between associated devices. This allows for instantaneous notifications between single households (e.g., House 1 and House 2) and provides community-wide alerting in actual deployments. To provide uninterrupted service, a solar-powered backup power source is built into the system. The internet and mobile applications offer remote monitoring and control to users to identify and act on alerts in an efficient manner. The hardware setup and circuit diagram are illustrated in Figure 1, which explains the connection between sensors, communication modules, and alert devices.

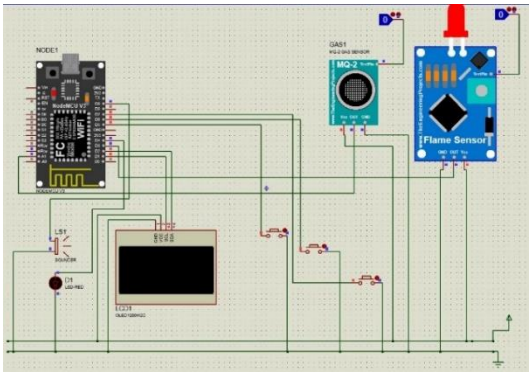


Figure 1: Circuit Diagram & Hardware Setup

B. Testing Scenarios:

1) Gas Leak Simulation:

The gas leakage detection system is provided with an MQ-2 gas sensor, and it provides an analog voltage output that is proportional to the gas concentration within the ambient air. The threshold is fixed at 800 ADC units in such a way that it generates an alarm. The gas concentration can be computed using the following formula:

$$Gas\ Level(\%) = \left(\frac{Analog\ Reading \times 100}{1023}\right) \quad (1)$$

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.

2) Theft Button/Medical Button:

The theft and medical emergency system facilitates quick response by manual or remote activation. The theft emergency is activated by pressing the Theft Button or using a mobile application, immediately sending an "Emergency Theft" alarm to nearby houses and authorities. Similarly, a medical emergency is activated via the Medical Button, notifying all connected households. If a pre-configured medical alert exists in the mobile app, the system autonomously dispatches the notification.

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.

3) Fire Detection using Flame Sensor:

The fire alarm system in the prototype uses a flame sensor to monitor the level of infrared radiation continuously. Whenever the intensity detected is above a given threshold, the system issues an emergency notification to nearby households and emergency responders for prompt hazard communication. Fire detection is established through:

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

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 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 1: Response Time Analysis for Emergency Detection and Alerts

C. *Testing Scenarios:*

The performance of the system is measured in terms of accuracy and response time. Accuracy is a measure of the dependability of fire and gas sensors to detect emergencies with minimal false alarms. It is computed as:

$$\text{Accuracy} = \left(\frac{True\ Alerts}{Total\ Alerts}\right) \times 100 \quad (6)$$

Response time, denoted as Equation (5), is the duration between hazard detection and alert activation. Where t_d is the hazard detection time and t_a is the alert activation time. A lower response time ensures rapid emergency intervention. Figure 2 illustrates the testing scenario workflow.

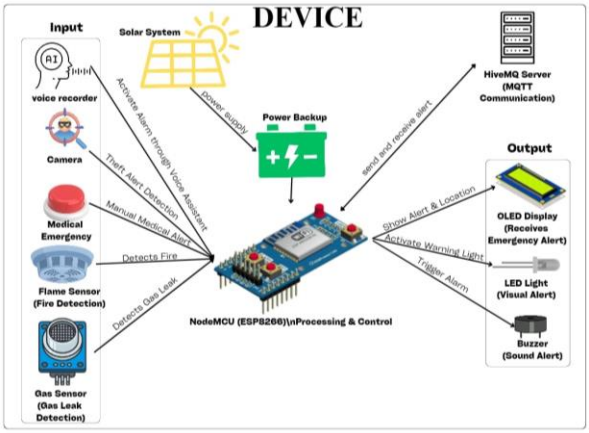


Figure 2: Testing Scenario Workflow for Emergency Detection System

D. False Alarms:

False alarms are assessed by testing the system under controlled conditions where no actual hazard exists, such as using a fan to test the flame sensor's sensitivity. Table 2 Presents the false alarm rate. The false alarm rate is calculated as:

$$\text{False Alarm Rate} = \left(\frac{False\ Alarms}{Total\ Tests}\right) \times 100 \quad (7)$$

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

Table 2: False Alarm Rate

E. Power Consumption:

The system's power consumption is examined in terms of energy consumption in alert and idle modes. The overall power consumption is determined as:

$$P_c = P_a \times T_a \quad (8)$$

Where P_c is the overall power consumption, P_a is the power consumption in the alert mode, and T_a is the duration in the alert mode.

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 3: Power Consumption Estimates

Each component is measured to calculate total energy consumption. Table 3 provides estimates of power consumption, allowing a comparative analysis with current smart safety systems to gauge the suitability of the prototype for practical applications.

V. Results & Discussion

A. Case Study:

This case study shows MQTT communications system operation between two houses in a community setting, including fire, gas, theft, and medical alarms.

1) Case Study 1: Fire Detection and MQTT-Based Alert Propagation

This case study explores the efficiency of real-time communication of the proposed MQTT-based fire detection and alert system. When a fire is sensed in House 1, the flame sensor initiates an emergency alarm, sending out a local buzzer, LED light, and an OLED display notification with "ALERT SENDING". At the same time, an MQTT message is sent to adjacent houses and the all the nearby houses in the community, like House 2, where the system reads the alert and shows "HOUSE 1: FIRE DETECTED" on its OLED display and also the surrounding houses receive the signal from the house 1. The alarm is also conveyed via the mobile app and web interface to the neighbor's community also, where residents can confirm the alert and escalate the alert to local authorities (as presented in Figure 3). Experimental testing proved a fire detection and alert distribution time of below 300 ms, which allows for quick hazard notification and response coordination throughout the community.

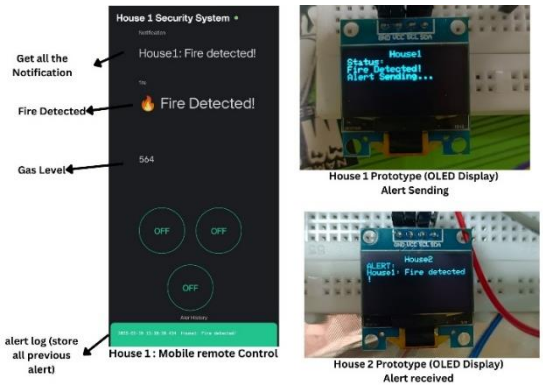


Figure 3: Fire Detection Communication Between House 1 and House 2

2) Case Study 2: Gas Leak Detection and MQTT-Based Alert Propagation

In this case study, the efficiency of the gas leak detection system and MQTT communication is tested. When there is a gas leak in House 1, the gas sensor can detect the occurrence of dangerous levels of gas and send an alert.The system displays "GAS LEAK DETECTED" on the OLED screen of House 1 while simultaneously triggering an MQTT alert. House 2 gets the alert, ringing its buzzer and LED light, with the mobile app informing residents of the alert.On acceptance, House 2 can escalate the response by notifying emergency services (as shown in Figure 4). Experimental results indicate a 95% accuracy in gas leak detection, offering high reliability, while communication offers smooth and real-time hazard alerting.

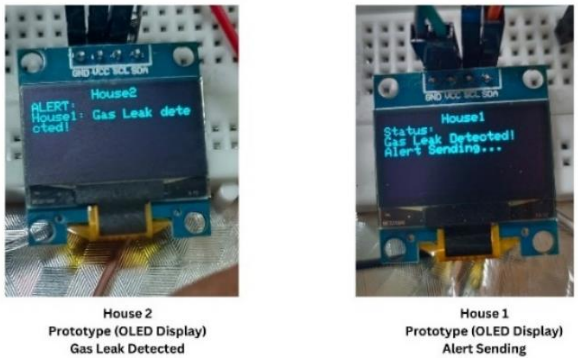


Figure 4: Gas Leak Detection Communication Between House 1 and House 2

3) Case Study 3: Theft Detection and Emergency Response

This case study measures the response efficacy of the theft alarm system employing an emergency button and MQTT-based communication. On triggering a theft emergency in House 1 through the Theft Button, the system shows "THEFT ALERT SENT" on the OLED display of House 1, triggers the buzzer, LED indicator. At the same time, an MQTT warning is sent to House 2, whose OLED display is updated with "HOUSE 1 THEFT ALERT," and a mobile alert is dispatched to the residents. House 2 is then able to judge the situation on its own, act locally, or forward the alert to the authorities (as in Figure 5). The experimental results reflect 99% accuracy in detecting theft, thus enabling fast emergency communication.

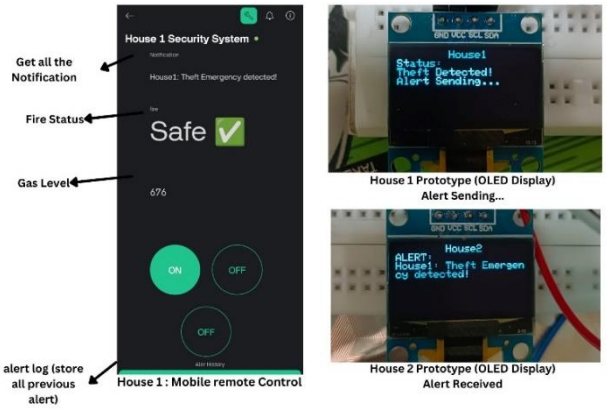


Figure 5: Theft Detection and Emergency Communication Between House 1 and House 2

4) Case Study 4: Medical Emergency Detection and Response

This case study discusses the effectiveness of the medical emergency alert system through an MQTT-based network communication. On the triggering of a medical emergency in House 2 through the Medical Button, the system indicates "MEDICAL ALERT SENT" on House 2's OLED display,

This case study discusses the effectiveness of the medical emergency alert system through an MQTT-based network communication. On the triggering of a medical emergency in House 2 through the Medical Button, the system indicates "MEDICAL ALERT SENT" on House 2's OLED display, the buzzer sounds, and an LED indicator is flashed. At the same time, an MQTT alert is sent to House 1, where the OLED display is refreshed with "HOUSE 2 MEDICAL ALERT" and a mobile alert is issued to the occupants. The alert in House 1 can be received through the mobile/web interface and respond immediately or refer the matter to medical authorities (refer Figure 6). Experimental results validate a 100% detection rate, providing a zero false-positive and false-negative rate at high-speed and effective emergency communication.

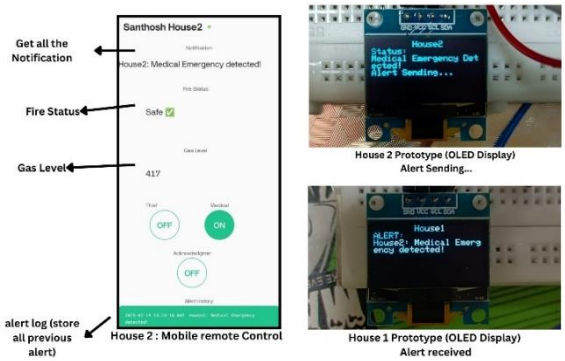


Figure 6: Medical Emergency Detection and Response Between House 1 and House 2

5) Case Study 5: False Alarm Detection and Acknowledgment Mechanism

This case study assesses the performance of the false alarm acknowledgement mechanism in the MQTT-based emergency network. A wrong press of the Medical Emergency Button in House 1 initiates a community-wide emergency warning. The OLED screen in House 1 displays "MEDICAL ALERT SENT", and the buzzer and LED turn on, indicating an emergency. The alert is immediately transmitted to House 2, whose OLED displays "HOUSE 1 MEDICAL ALERT", and a mobile alert is prompted to the inhabitants. The user in House 1 activates the Acknowledgment Button once the false alarm has been discovered, which transmits an immediate cancellation signal via MQTT. This sends House 1's OLED to "ALERT CANCELED", quiets the buzzer, and turns off the LED (as indicated in Figure 7). At the same time, House 2 and the public are given a revised alert stating false alarm in order to avoid unnecessary emergency response. Experimental

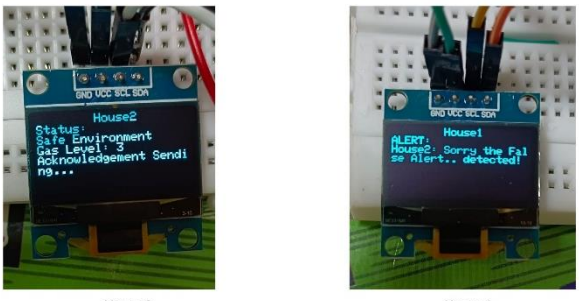


Figure 7: False Alarm Detection and Acknowledgment System

outcomes prove that false alarms were corrected within 10 seconds, ensuring quick correction and avoidance of public panic.

B. Comparison of our system with existing community safety solutions

System Type	*False Alarm Rate*	*Avg. Response Time*	*Multi-Scenario Detection*	*AI Integration*
GSM-Based System [X]	8%	6 seconds	No	No
IoT-Based Basic [Y]	5%	4 seconds	Partial	No
Proposed System	1.75 %	3 seconds	Yes	Yes

Table 4: Benchmark Comparison of our system with existing community safety solutions

Table4, presents a benchmark comparison of our system with existing community safety solutions. Compared to GSM-based alert systems and non-AI IoT models, our AI-IoT integrated solution achieves a lower false alarm rate (1.75% average) and faster emergency response (under 3 seconds for button alerts). Moreover, the system supports multi-scenario threat detection, unlike traditional systems that focus on single-event detection.

VI. Challenges & Limitations

A. Potential False Alarms:

The system's effectiveness is influenced by external environmental factors that may cause unintended activations. Motion and gas sensors are particularly sensitive, with possible triggers from non-threatening elements such as cooking smoke or pet movement, leading to false alarms. Although the Acknowledgment Button serves as a mitigation measure, further enhancements are necessary to optimize detection accuracy. Future enhancements will incorporate AI-based filtering to sort out true threats from false positives, minimizing the number of unwanted alerts.

B. 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.

- **Security & Privacy:** Implementing secure MQTT (TLS), user access control, and encrypted local data logs is essential for large-scale trust.

VII. Conclusion & Future Work

A. System Summary & Community Safety Enhancement

The AI-Based Home and Community Safety System ensures safety in real-time by the utilization of emergency detection, IoT communication, and smart alerting features. The system based on MQTT message communication has enabled timely forwarding of notifications regarding theft, health issues, leakage of gas, and fire incidents to the community. The system is complemented by a mobile and web app interface, making it even more user-friendly for prompt response and monitoring.

B. Scalability for Smart Cities

The system architecture supports multi-dwelling integration, making it scalable for large-scale smart city use. With improved area networking, different homes can be alerted in cases of emergencies, enhancing overall community security. Integration with future development with municipal emergency services can be added to enhance response time.

C. Future Enhancements

Certain improvements are suggested in order to enhance efficiency and scalability of the system. AI-based event detection via machine learning algorithm-powered AI minimizes false alerts extensively by recognizing between real threat and environmental fluctuation. Additionally, integration of city-wide emergency networks guarantees uniform coordination with law enforcement, medical, and fire agencies for automated quick response. Further broadening the scope of application, integration of smart city resilience can extend the solution to cover multi-unit residential buildings and urban security networks, promoting autonomous community safeguarding. These innovations are consistent with (SDG 11 & SDG 9), which endorse the status of AI-based safety solutions as a determinant for building city resilience and sustainable growth.

VIII. 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: 10.1109/MCOM.2011.6069779.

[4] 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.

[5] 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: 10.1109/CTCT.2018.978-1-5386-3702-9.

[6] 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: 10.17781/P002617.

[7] 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: 10.24018/ejers.2021.6.6.2580.

[8] 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: 10.1109/COMPSAC48688.2020.0-132.

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

[10] 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: 10.1177/0894439304273274.

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

[12] 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.

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

[14] 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.

[15] 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.

[16] 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.

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

[18] 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.

CERTIFICATES

DEPARTMENT OF DATA SCIENCE AND BUSINESS SYSTEMS
SCHOOL OF COMPUTING,
COLLEGE OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR - 603 203

2nd INTERNATIONAL CONFERENCE ON DATA SCIENCE AND BUSINESS SYSTEMS - (ICDSBS 2025)

Certificate of Presentation

BEST PAPER

This is to certify that ~~Dr./Ms.~~/Mr. THANUSH KANNAN of DR. M.G.R. EDUCATIONAL AND RESEARCH INSTITUTE has presented a paper entitled AI - DRIVEN SMART SAFETY FRAMEWORK FOR COMMUNITY PROTECTION in the 2nd International Conference on Data Science and Business Systems (ICDSBS 2025) organized by the Department of Data Science and Business Systems, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu, India during 17-18th April 2025.

Convenor, ICDSBS 2025 | Dr. V. Kavitha, Professor & Head | Dr. C. Lakshmi, Professor & Associate Chairperson | Dr. Revathi Venkataraman, Professor & Chairperson

SRM School of Computing IEEE IEEE COMPUTER SOCIETY INSTITUTION INNOVATION COUNCIL Great Learning Atos

DEPARTMENT OF DATA SCIENCE AND BUSINESS SYSTEMS
SCHOOL OF COMPUTING,
COLLEGE OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR - 603 203

2nd INTERNATIONAL CONFERENCE ON DATA SCIENCE AND BUSINESS SYSTEMS - (ICDSBS 2025)

Certificate of Presentation

BEST PAPER

This is to certify that ~~Dr./Ms.~~/Mr. SANTHOSH R of DR. M. G. R. EDUCATIONAL AND RESEARCH INSTITUTE has presented a paper entitled AI - DRIVEN SMART SAFETY FRAMEWORK FOR COMMUNITY PROTECTION in the 2nd International Conference on Data Science and Business Systems (ICDSBS 2025) organized by the Department of Data Science and Business Systems, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu, India during 17-18th April 2025.

Convenor	Dr. V. Kavitha	Dr. C. Lakshmi	Dr. Revathi Venkataraman
ICDSBS 2025	Professor & Head	Professor & Associate Chairperson	Professor & Chairperson

NAAC A++ ACCREDITED | Category I with UGC Status | QS (2025) World Ranking One among 46 Indian Universities | nirf (2024) 12th Ranked University | QS I-Gauge Platinum Rated | THE (2025) World Ranking One among 187 Indian Universities | SHANGHAI RANKING (2024) World Ranking Ranked 5-7 in Indian Universities | nature index (2024) Ranked 20th in India

SRM School of Computing | IEEE | IEEE COMPUTER SOCIETY | INSTITUTION INNOVATION COUNCIL | Great Learning | Atos

DEPARTMENT OF DATA SCIENCE AND BUSINESS SYSTEMS
SCHOOL OF COMPUTING,
COLLEGE OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR - 603 203

2nd INTERNATIONAL CONFERENCE ON DATA SCIENCE AND BUSINESS SYSTEMS - (ICDSBS 2025)

Certificate of Presentation

BEST PAPER

This is to certify that ~~Dr./Ms./~~Mr. PIOUS NIRANJAN A ..... of DR. M.G.R. EDUCATONAL AND RESEARCH INSTITUTE ..... has presented a paper entitled AI - DRIVEN SMART SAFETY FRAMEWORK FOR COMMUNITY PROTECTION ..... in the 2nd International Conference on Data Science and Business Systems (ICDSBS 2025) organized by the Department of Data Science and Business Systems, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu, India during 17-18th April 2025.

Convenor	Dr. V. Kavitha	Dr. C. Lakshmi	Dr. Revathi Venkataraman
ICDSBS 2025	Professor & Head	Professor & Associate Chairperson	Professor & Chairperson

NAAC A++ ACCREDITED | Category I with 129 Status | (2025) World Ranking One among 46 Indian Universities | (2024) 12th Ranked University | QS I-Gauge Platinum Rated | (2025) World Ranking One among 197 Indian Universities | (2024) World Ranking Ranked 5-7 in Indian Universities | (2024) Ranked 20th in India

SRM School of Computing IEEE COMPUTER SOCIETY INSTITUTION INNOVATION COUNCIL Great Learning Atos

DEPARTMENT OF DATA SCIENCE AND BUSINESS SYSTEMS
SCHOOL OF COMPUTING,
COLLEGE OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR - 603 203

2nd INTERNATIONAL CONFERENCE ON DATA SCIENCE AND BUSINESS SYSTEMS - (ICDSBS 2025)

Certificate of Presentation

BEST PAPER

This is to certify that ~~Dr./Ms./~~Mr. DHANUSH RAJN of DR. M.G.R. EDUCATIONAL AND RESEARCH INSTITUTE has presented a paper entitled AI- DRIVEN SMART SAFETY FRAMEWORK FOR COMMUNITY PROTECTION in the 2nd International Conference on Data Science and Business Systems (ICDSBS 2025) organized by the Department of Data Science and Business Systems, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu, India during 17-18th April 2025.

Convenor	Dr. V. Kavitha	Dr. C. Lakshmi	Dr. Revathi Venkataraman
ICDSBS 2025	Professor & Head	Professor & Associate Chairperson	Professor & Chairperson

NAAC A++ ACCREDITED QS nirf SHANGHAI RANKING