IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, April 2025
Impact Factor: 7.67

User-Centric Smart Home Security System with GSM Alerts

Dr. Chandrashekhar Reddy S[1], B Shivani[2], M Akhila[3], CH Anusha[4], M Pranay[5]
[1]Asst. Professor in EEE, Dept. of Electrical & Electronics Engineering,
[2,3,4,5]UG Student, Dept. of Electrical & Electronics Engineering
Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India

Abstract: *The increased rate of theft necessitates advanced anti-theft mechanisms. Our project aims to develop a comprehensive security system integrating Gas, Flame, Passive infrared (PIR), Infrared (IR) and biometric sensors[1]. The existing systems are limited to their singular focus, such as motion detection or biometric verification alone, which results in incomplete security. This project is designed to overcome those limitations of single-method detection and providing a robust and comprehensive security system. The project aims to detect hazardous gas leaks, sense unusual motion via PIR&IR sensors, detect unauthorized access through biometric verification and detect the presence of flames to mitigate the fire risks [2]. The successful implementation of this project could set a new standard in Security technology, enhancing safety measures and offering an enhanced piece of mind to the users. User-centric smart home security systems with GSM alerts offer a compelling blend of convenience, security, and efficiency for modern homeowners [3]. These systems empower users with remote monitoring capabilities and immediate alerts via SMS or calls, ensuring prompt response to potential security breaches even during internet outages. Integration with other smart devices enhances functionality, allowing for seamless automation and personalized control over home environments [4]*

Keywords: Solenoid Lock, Fingerprint Sensor, Microcontroller, GSM

I. INTRODUCTION

In today's rapidly evolving technological environment, the need for robust and user- centric smart home security systems has become increasingly vital. Traditional security measures often fall short in providing comprehensive protection, leaving homes vulnerable to various threats such as burglary, and gas leaks. The primary challenge facing conventional home security systems lies in their limited scope and responsiveness and depends only on alarms or passive surveillance cameras alone, which are reactive rather than attentive in nature .This reactive approach, can lead to delayed responses or false alarms, compromising the safety and peace of mind of homeowners[1].

By contrast, a user-centric smart home security system with GSM alerts leverages cutting- edge sensors and communication technologies to offer enhanced protection and real-time alerts. For instance, integrating a fingerprint sensor at the entry door ensures that only authorized persons can access the premises, effectively preventing unauthorized entry attempts. Gas sensor provides early detection of potential hazards, sending immediate alerts to homeowners and emergency services via GSM networks [3].

The system also includes PIR (Passive Infrared) sensors, which are sensitive to human radiation. These sensors detect movement inside your home and distinguish between normal activity and suspicious behavior, reducing false alarms and ensuring that you're only alerted when there's a genuine threat outside your home, IR (Infrared) sensors monitor for unusual vehicle movements, providing added security against potential intruders or suspicious activity around your property [5].

II. LITERATURE SURVEY

A comprehensive literature survey on user- centric smart home security systems with GSM alerts reveals a growing body of research and development in the field, driven by advancements in IoT technologies and increasing demand for

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, April 2025
Impact Factor: 7.67

enhanced residential security solutions [6]. Academic papers and industry reports emphasize the integration of sensors, and smart devices to create interconnected security ecosystems that prioritize user convenience, proactive monitoring, and effective response mechanism. Key studies highlight the importance of real-time notifications delivered via GSM of security breaches or emergencies [3]. This capability enhances situational awareness and allows for timely intervention, regardless of the user's location. User-centric design principles play a pivotal role in system development, focusing on intuitive interfaces, personalized settings, and seamless integration with other IoT devices within the home [7]. Research explores user preferences and behaviors, aiming to optimize system usability and user acceptance. Privacy and security concerns are addressed through discussions on encryption methods, data protection measures, and secure communication protocols [3].

Case studies and practical implementations provide insights into system effectiveness, user satisfaction, and operational challenges. These examples illustrate various deployment scenarios and highlight best practices in integrating smart home security solutions with GSM alerts [3]. Future research directions include enhancing system scalability, improving interoperability among different IoT devices, exploring advanced analytics for predictive security measures, and addressing regulatory implications related to data privacy and security standards [2]. In summary, the literature survey underscores the evolution of user-centric smart home security systems with GSM alerts, emphasizing technological advancements, user preferences, privacy considerations, and practical applications that collectively aim to redefine residential security standards in the era of IoT and connected living.

III. EMBEDDED SYSTEMS

An embedded system is a specialized computing system designed to perform specific tasks within larger devices or systems. Unlike general-purpose computers, which can run a wide range of software applications, embedded systems are tailored for dedicated functions. They are tightly integrated into the hardware they control and often operate in real-time environments.

User-centric smart home security systems have evolved to incorporate advanced technologies that prioritize both security and convenience. Integrating a fingerprint sensor for authorized access ensures that only approved individuals can enter the home. This biometric authentication method provides robust protection against unauthorized entry and is seamlessly integrated with GSM technology to send alerts via SMS or calls in case of any suspicious activity or attempted breaches.

In addition to the fingerprint sensor, PIR (Passive Infrared) sensors play a crucial role in detecting human motion within the premises and the integration of IR sensors for anti- vehicle theft alerting adds another layer of protection. These sensors are designed to detect the presence of vehicles in restricted areas or unauthorized attempts to access vehicles [9]. The inclusion of flame and gas sensors connected to a buzzer further enhances the safety features of these smart home security systems. These sensors detect the presence of hazardous conditions such as gas leaks or fires, immediately activating the buzzer to alert occupants of the potential danger. When triggered, the system activates a buzzer alert within the home, notifying occupants of potential threats [2]. This proactive measure helps deter vehicle-related theft incidents and provides homeowners with enhanced peace of mind knowing that their property is continuously monitored against such risks. Together, these integrated sensors and GSM alerts exemplify the comprehensive security and safety capabilities of modern user-centric smart home systems, providing homeowners with a proactive approach to protecting their homes and ensuring peace of mind [4].

IV. HOME SECURITY

Biometric authentication through fingerprint sensors ensures that access to the home is secure and convenient, eliminating the risks associated with lost or stolen keys. Motion detection sensors offer continuous monitoring and immediate alerts, empowering homeowners to respond swiftly to potential threats [10]. Vehicle detection sensors provide advanced perimeter security, detecting and alerting homeowners to the presence of vehicles near the property [11].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, April 2025
Impact Factor: 7.67

Environmental hazard sensors, including gas leakage sensor protects against internal threats, such as gas leaks, by detecting and alerting homeowners to hazardous conditions. The integration of GSM communication modules enables real-time remote monitoring and communication, ensuring that homeowners remain connected to their security system at all times. Whether at home or away, homeowners can receive alerts, monitor security status, and remotely control their system through their mobile devices. This capability enhances convenience and peace of mind, allowing homeowners to manage their home's security efficiently and effectively [12].

V. EXISTING SYSTEM

Existing home security systems relied on centralized monitoring stations, but advancements in Internet of Things (IoT) devices have enabled distributed and interconnected sensors for real-time monitoring and response [6]. Common issues arise from network, device, software, and security challenges, creating vulnerabilities in otherwise innovative setups. Network failures are a major concern. Most smart home devices rely on Wi- Fi or Bluetooth connections to function, making them highly susceptible to connectivity problems. Weak signals, network congestion, or router malfunctions can disrupt the communication between devices, causing them to become unresponsive. An overloaded network, with numerous connected devices, can also lead to performance slowdowns or interruptions [4]. Interoperability issues between devices from different manufacturers are another common cause of failure. Many smart home systems operate on different protocols (like Zigbee, Z-Wave, or Wi-Fi), and these may not always communicate seamlessly, resulting in compatibility problems or inefficient system integration. As more devices are added to a smart home, ensuring compatibility becomes increasingly complex. Software glitches and updates can also lead to system failures. Firmware updates can cause devices to malfunction or become incompatible with other components of the home automation setup. Outdated software may introduce bugs, causing devices to behave erratically or stop working entirely[7]. Security vulnerabilities are a critical concern in smart home automation. Devices are often exposed to hacking risks due to poor encryption or lack of security protocols. Weak default passwords, unpatched software, and insecure network connections can allow attackers to gain unauthorized access, potentially compromising both personal data and home security[6]. In sum, smart home automation failures can be traced back to network issues, device compatibility, software glitches, and security vulnerabilities. These failures can disrupt daily functionality and create significant risks if not properly managed.

VI. PROPOSED METHOD

The desire to enhance safety and peace of mind for homeowners is a driving force behind this system. Biometric authentication through fingerprint sensors ensures that access to the home is secure and convenient, eliminating the risks associated with lost or stolen keys. Motion detection sensors offer continuous monitoring and immediate alerts, empowering homeowners to respond swiftly to potential threats [13]. Vehicle detection sensors provide advanced perimeter security, detecting and alerting homeowners to the presence of vehicles near the property [11]. Environmental hazard sensors, including gas leakage sensor protects against internal threats, such as gas leaks, by detecting and alerting homeowners to hazardous conditions. The integration of GSM communication modules enables real-time remote monitoring and communication, ensuring that homeowners remain connected to their security system at all times. Whether at home or away, homeowners can receive alerts, monitor security status, and remotely control their system through their mobile devices [3]. The objectives of a user-centric smart home security system with GSM alerts are to bolster home security with real-time notifications for prompt responses, enable convenient remote management via mobile devices, integrate seamlessly with IoT devices for enhanced automation[14], ensure robust privacy through encryption and secure protocols, optimize user experience with intuitive interfaces and customizable settings, and facilitate scalability to accommodate evolving security needs and home configurations[4]. These goals collectively aim to deliver a comprehensive, user-friendly solution that enhances safety, convenience, and peace of mind for homeowners in managing and securing their residences.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, April 2025
Impact Factor: 7.67

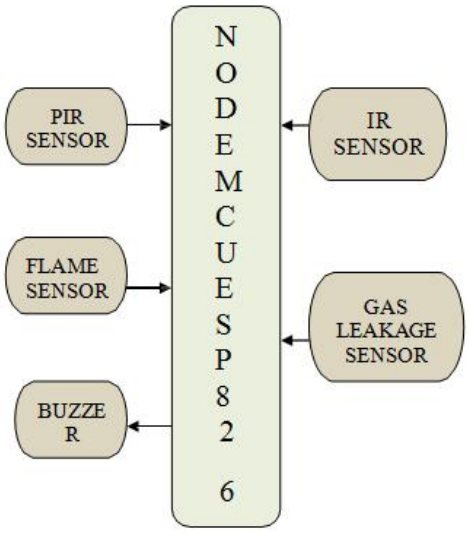

Figure 1: Block diagram of the proposed method for Smart home automation system.

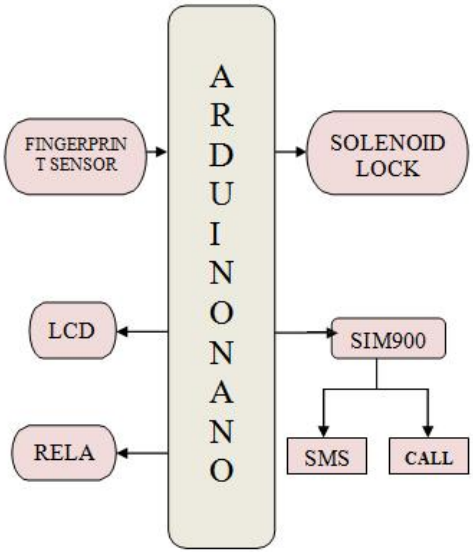

Figure 2: Block diagram of the proposed method for smart home security system.

VII. SOFTWARE EMPLOYED

The development of a user-centric smart home security system with GSM alerts using Arduino IDE and IoT cloud for remote monitoring requires a comprehensive understanding of software programming. The Arduino IDE provides a user-friendly environment for programming Arduino boards, making it accessible for beginners and non- programmers to develop complex systems.

The initial step in designing the system involves designing the circuit and selecting the necessary components, including Arduino boards, sensors, relays, and a display unit. The system's core functionality revolves around detecting unauthorized access to the home and sending an alert to home owner and also detects various potential threats like gas leaks, fires and burglaries and warns the home owners. The sensors used in this system include fingerprint sensor at the entry door, gas sensor, flame sensor, PIR sensor, and IR sensor for anti- vehicle thefting. These sensors provide real-time data to the system, enabling it to detect potential threats and send alerts to users' phones.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, April 2025
Impact Factor: 7.67

To construct the system, users begin by connecting the components according to the circuit diagram, ensuring proper wiring and connections. Arduino boards are programmed using Arduino IDE, where users can write the necessary code for the system's operation.

The system's operation can be monitored through the display unit, providing real-time feedback on the authentication process. This enables users to track the status of their smart home security system remotely, receiving notifications and alerts in case of any potential threats.

In conclusion, software plays a vital role in developing a user-centric smart home security system with GSM alerts using Arduino IDE and IoT cloud for remote monitoring. The Arduino IDE provides a user-friendly environment for programming Arduino boards, making it accessible for beginners and non-programmers to develop complex systems.

VIII. RESULTS & DISCUSSION

The expected result of the "USER CENTRIC SMART HOME SECURITY SYSTEM WITH
GSM ALERTS" project with integration of multiple sensors is a cutting-edge smart home security system that is designed to provide homeowners with a high level of security and convenience [9]. The fingerprint sensor authentication features will add an additional layer of security to the system, ensuring that only authorized individuals are granted access to the smart home [15]. The system is expected to be user-friendly and easy to use, making it accessible to homeowners of all ages and technical expertise. It will enable homeowners to control their smart homes, providing them with a high level of convenience[8].

In addition to the fingerprint sensor, PIR (Passive Infrared) sensors play a crucial role in detecting human motion within the premises and the integration of IR sensors for anti- vehicle theft alerting adds another layer of protection. These sensors are designed to detect the presence of vehicles in restricted areas or unauthorized attempts to access vehicles [9].

The inclusion of flame and gas sensors connected to a buzzer further enhances the safety features of these smart home security systems. These sensors detect the presence of hazardous conditions such as gas leaks or fires, immediately activating the buzzer to alert occupants of the potential danger. When triggered, the system activates a buzzer alert within the home, notifying occupants of potential threats [2].

This proactive measure helps deter vehicle- related theft incidents and provides homeowners with enhanced peace of mind knowing that their property is continuously monitored against such risks.

Together, these integrated sensors and GSM alerts exemplify the comprehensive security and safety capabilities of modern user-centric smart home systems, providing homeowners with a proactive approach to protecting their homes and ensuring peace of mind [4].

Result: The circuit successfully opens the door after authorized access is granted through verified fingerprint and activates the buzzer when the sensors detect suspicious activities like unauthorized entry of person/vehicle theft/gas leaks/fires.

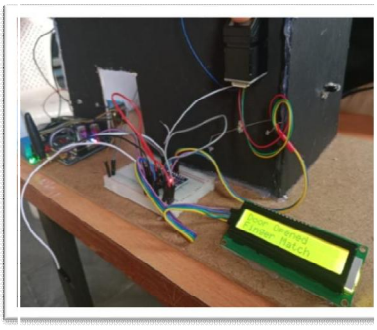

Figure 3: When door is opened after fingerprint verification and buzzer activated when detected suspicious activity.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, April 2025
Impact Factor: 7.67

Alert Notifications Output:

Figure 4: Alert Messages from Kit

IX. CONCLUSION

In conclusion, user-centric smart home security systems with GSM alerts offer a compelling blend of convenience, security, and efficiency for modern homeowners. These systems empower users with remote monitoring capabilities and immediate alerts via SMS or calls, ensuring prompt response to potential security breaches even during internet outages.

Integration with other smart devices enhances functionality, allowing for seamless automation and personalized control over home environments.

Despite their benefits, potential challenges include initial setup costs, dependence on stable internet connectivity, and privacy considerations regarding data collection and security. Maintenance requirements and the complexity of integrating diverse devices from different manufacturers also pose practical hurdles.

Nevertheless, the ongoing advancements in smart technology continue to improve these systems, promising greater reliability, usability, and integration with everyday living. As these technologies mature, addressing current limitations will be crucial to realizing their full potential in enhancing home security while accommodating user preferences and lifestyle needs.

X. FUTURE SCOPE

The user-centric smart home security system integrates advanced technologies to provide homeowners with comprehensive protection and peace of mind. A user-centric smart home security system with GSM alerts has significant future potential due to several emerging trends and technological advancements.

With the integration of advanced technologies such as artificial intelligence, machine learning, and block chain, the system can become even more robust and secure. One potential area of development is the integration of facial recognition technology with the fingerprint sensor at the entry door. This would enable more precise identification of authorized individuals and enhance the overall security of the system.

Another area of focus could be the development of a more comprehensive gas detection system, incorporating multiple sensors to detect various types of gases and provide real-time alerts to users. This could be particularly useful in detecting gas leaks or other hazardous conditions in the home.

The integration of smart home devices with the security system could also be explored, enabling users to control their lighting, temperature, and other appliances remotely through the IoT cloud platform. Moreover, the use of blockchain

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, April 2025
Impact Factor: 7.67

technology could ensure secure data storage and transmission, providing an additional layer of protection for sensitive information.

In addition, the development of a mobile app for users to remotely monitor and control their smart home security system could be a significant enhancement. The app could provide users with real-time notifications and updates, allowing them to respond quickly to any security breaches or potential threats. By incorporating these advanced technologies, the user-centric smart home security system can become an even more comprehensive and effective solution for protecting homes and families.

REFERENCES

[1] Jump up to: Hill, Jim (12 September 2015). "The smart home: a glossary guide for the perplexed". T3. Retrieved 27 March 2017.

[2] Jayashri B and Arvind S 2013 “Design and Implementation of Security for Smart Home based on GSM technology International Journal of Smart Home 7 201-08”

[3] Karri V and Daniel Lim J S 2005 “Method and Device to Communicate via SMS after a Security Intrusion 1st International Conf. on Sensing Technology Palmerstone North New Zealand 21-23 “

[4] Caccavale, Michael (September 24, 2018). "The Impact Of The Digital Revolution On The Smart Home Industry". Forbes. Retrieved 2019-11-07.

[5] Home Automation & Wiring (1 Ed.). New York: McGraw-Hill/TAB Electronics. 1999- 03-31. ISBN 978-0-07-024674-4.

[6] Pooja P, Mitesh P, Vishwa P and Vinit N 2016 “Home Automation Using Internet of Things Imperial Journal of Interdisciplinary Research (IJIR) 2 648-51”

[7] Rye, Dave (October 1999). "My Life at X10". AV and Automation Industry eMagazine. Archived from the original on September 30, 2014. Retrieved October 8, 2014.

[8] Mamun OF, Rahman M. “Design of Home Automation and Smart Security System”.

[9] Sowjanya G and Nagaraju S 2016 “Design and Implementation Of Door Access Control And Security System Based On Iot Inventive Computation Technologies (ICICT), International Conference on Inventive”

[10] Cristian C, Ursache A, Popa D O and Florin Pop 2016 “Energy efficiency and robustness for IoT: building a smart home security system Faculty of Automatic Control and Computers University Politehnica of Bucharest, Bucharest, Romania 43”.

[11] Govinda K and Sai Krishna Prasad K and Sai ram susheel 2014 “Intrusion detection system for smart home using laser rays International Journal for Scientific Research & Development (IJSRD) 2 176-78 “

[12] "1.5 Million Home Automation Systems Installed in the US". ABI Research. November 19, 2012. Retrieved 2016-11-22."ESP8266 Overview". Espressif Systems. Retrieved 2017-10-02.

[13] "Smart Home - United States | Statista Market Forecast". Statista. Retrieved 2019- 11-07

[14] Caccavale, Michael (September 24, 2018). "The Impact Of The Digital Revolution On The Smart Home Industry". Forbes. Retrieved 2019-11-07.

[15] Sadasivuni, Kishor Kumar; Houkan, Mohammad Talal; Taha, Mohammad Saleh; Cabibihan, John-John (August 2017). "Anti- spoofing device for biometric fingerprint scanners". 2017 IEEE International Conference on Mechatronics and Automation (ICMA). IEEE. Archived from the original on 17 January 2021. Retrieved 27 October 2020.