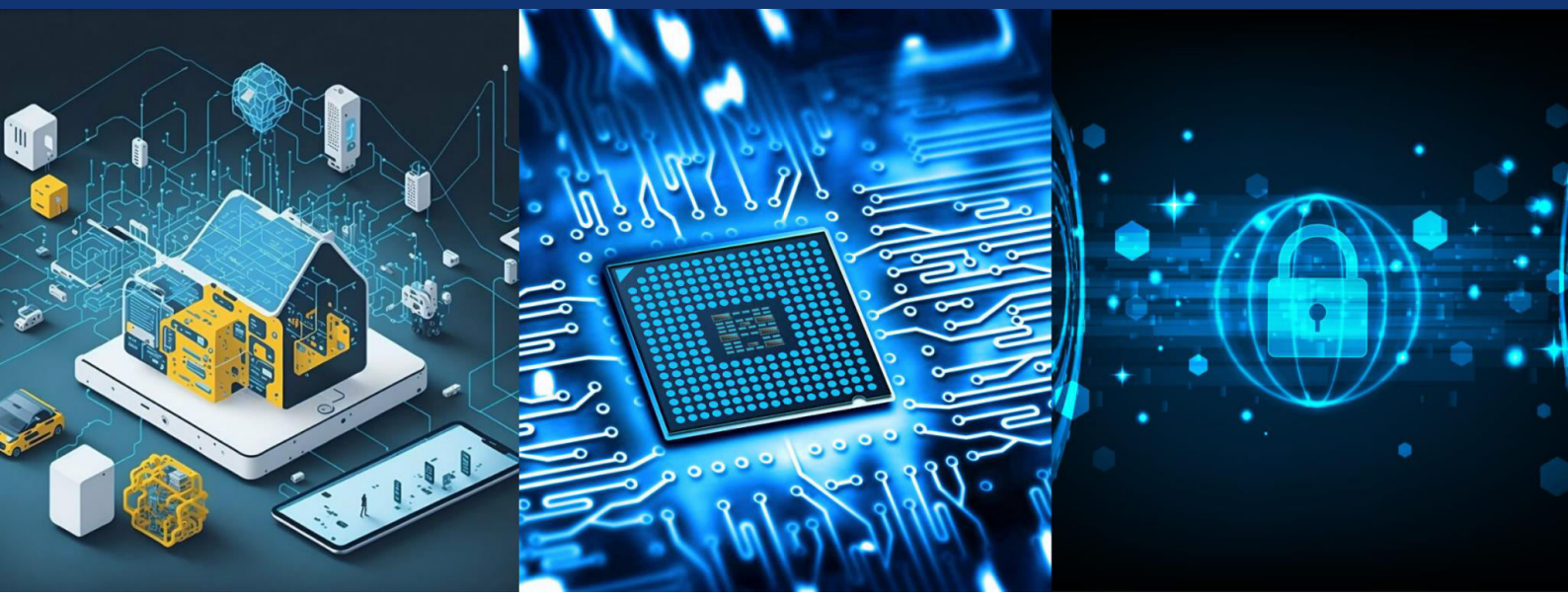
IJIRCCE

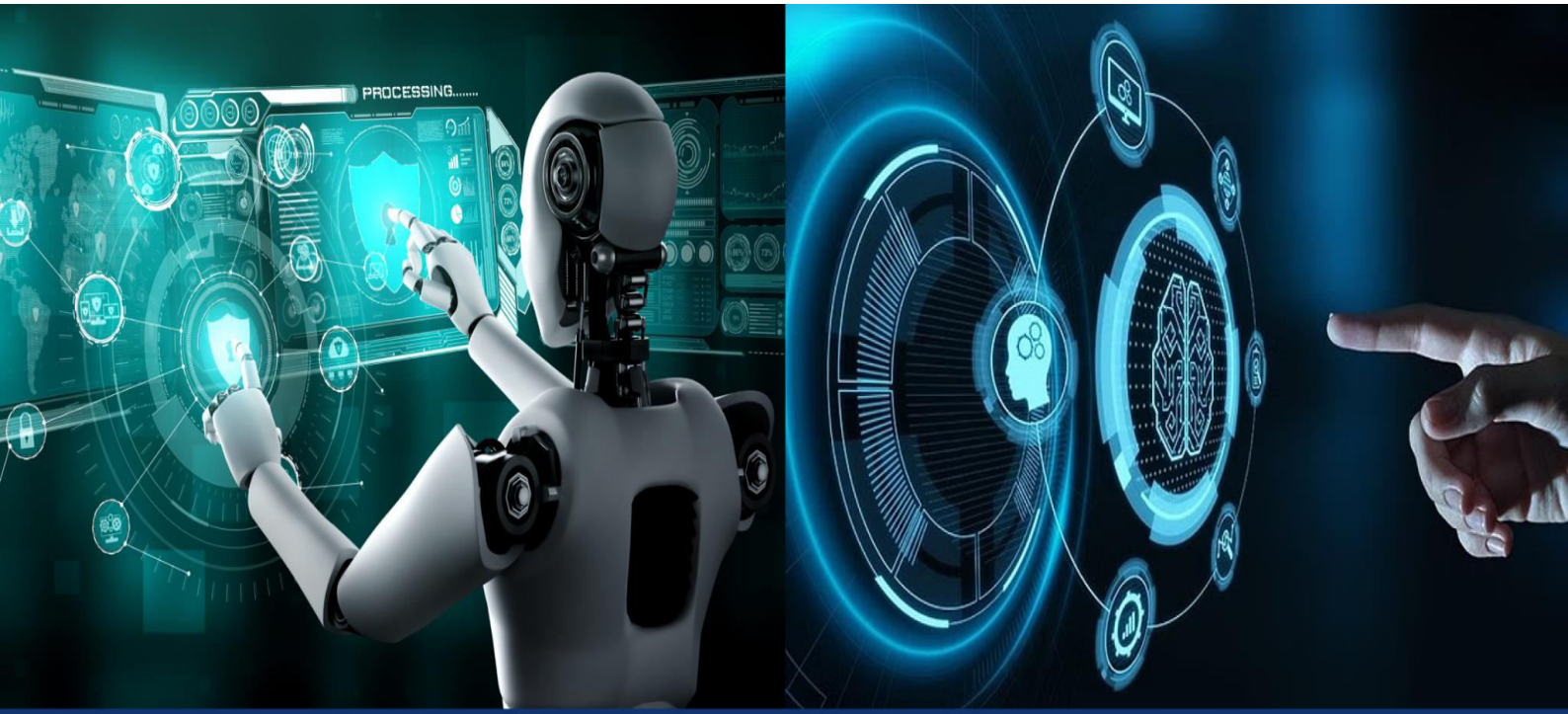
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 4, April 2025

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025 |DOI:10.15680/IJIRCCE.2025.1304263

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IOT Based Smart Security System

Riya Bhagat, Sanika Junghare, Akanksha Niwalkar, Laxmi Vaidya, Kalyan Shengraph

Assistant professor, Dept. of Computer Engineering, Ballarpur Institute of Technology [BIT], Ballarpur, Maharashtra, India

Department of Computer Engineering, Ballarpur Institute of Technology [BIT], Ballarpur, Maharashtra, India

ABSTRACT: The thesis knowledge is feasible since it covered all features of a normal security system. Low-cost accessories and easy-maintainability features were the only attributes that made it specific. The paper presents IoT-based smart security systems that encourage effective security for residential and commercial properties. It integrates different kinds of sensors such as motion detectors, sensors, and cameras with microcontroller like Arduino with a platform available for real-time alerts and data storage. Users can monitor their premises remotely through mobile application or web interface and receive instant notification whenever suspicious activity occurs. The intention of the project was to show a demonstration on how a basic smart security system works.

KEYWORDS: IOT-based security system, Low-cost accessories, Motion detectors, Camera, Arduino, Real-time alerts, Remote monitoring, Mobile application, Suspicious activity detection.

I. INTRODUCTION

The use of IoT in security systems has revolutionized the perception of safety and surveillance. The IoT-Based Smart Security Mega Project seeks to construct a smart, scalable, user-friendly solution that employs connected devices, real-time analytics, and automation to add safety to homes, businesses, and public spaces. This will entail clearing the way for full-fledged and responsive arrangements for safety that will address the ever-increasing necessity for safety in today's highly digital and urbanized world.

Such devices range from cameras to motion detectors, smart locks, and alarms-all of which communicate via a central hub. The system will avail users with real-time updates, automatic responses to various threats, and simple control of the security through either a mobile app or a web dashboard. Security will always be a priority, whether for individuals, companies, or governments. Today, the truth is that technology evolves too rapidly, rendering the manual characterization of a traditional lock-and-key no longer viable. Stressing on the necessity of such systems due to the prevalence of crime, unauthorized middlemen, cyber threats, and emergency events, states the fact that there is an imperative threat that demands a smarter system designed to identify threats in real-time and provided alerts on time. Smart Security Systems (SSS) have evolved into proactive advanced and intelligent systems built using an amalgamation of today's technologies like IoT, Artificial Intelligence (AI), Cloud Computing, and Biometrics. These systems comprise smart cameras or smart CCTV, motion sensors, and even details for remote access to help take necessary security measures, thus taking one step away from potential threats.

This project will integrate sensors like motion detectors, door sensors, and cameras with microcontrollers like Arduino. They will be connected to the platform, which has real-time alert messages and stores data. The users can keep track of their belongings even from afar through mobile applications and the web interface, as well as get instantaneous updates in case anything happens in their places of abode.

II.SYSTEM MODEL AND ASSUMPTIONS

An IoT-based smart security system usually is made up of some components and the placement of those components in a specific architecture which allows the system to support different-devices and services.

1. Cameras: To be able to carry out video surveillance, they are often presented with the features such as night vision and motion detection.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

2. Motion Sensors: The elements that can detect movements in a predefined area and if this happens, they can directly trigger alerts or another kind of action.

3. Sensors: They are the devices to notify about any change of the door or window's condition, i.e., if they are moved/opened or even closed.

4. Smart Locks: The ones which are capable of keeping doors open or closed away from home.

5. Alarm Systems: Devices that if triggered will send a message to the owner when there is an intrusion or emergency.

6. Environmental Sensors: The things that can measure any change in the environment such as smoke, carbon monoxide or water leaks.

7. Mobile App/Web Interface: The system of interaction between the user and the computer, where users can watch live streaming, receive warning messages, and also take control of the devices.

8. Cloud Services: Technologies that manage, store data, and analytics of the company your device belongs to.

9. IoT Gateway: The equipment which is connected to local devices that also have a connection to the internet and it is also the one which can process the local data in some cases.

10. Power Supply: It is responsible for the devices' proper operation, providing the necessary energy that can be backed up with batteries in the event of power failure.

III. IMPLEMENTATION AND SYSTEM ENVIRONMENT:

To deploy a smart security system IoT mega project, concentrate on setting up the system module, which involves choosing proper sensors, communication protocols, and a control unit. Create a secure environment by combining cloud services for data storage, providing strong security features, and offering an easy-to-use mobile app for real-time monitoring and control.

System Implementation:

Network Setup:
Set up a dependable Wi-Fi or wired network to connect your devices. Make sure to configure communication protocols (like MQTT or HTTP) for smooth data exchange.
Device Configuration:
Install sensors and cameras with the right settings, such as sensitivity and detection zones. Program the microcontroller to handle inputs from the sensors and manage outputs like alarms and notifications.
Mobile Application:
Create and set up the app for user interaction, ensuring it connects seamlessly to the backend services. Don't forget to implement user authentication and access control features.
Cloud Integration:
Establish cloud services for data storage and processing. Make sure to follow secure practices for data transmission and storage.

System Environment:

Physical Environment:
Identify and prepare the best spots for installing sensors and cameras to ensure they cover all necessary areas. Keep environmental factors in mind, like weatherproofing for outdoor devices.
Security Environment:
Use encryption for both data transmission and storage. Regularly update software and firmware to guard against vulnerabilities.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025 |DOI:10.15680/IJIRCCE.2025.1304263

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

User Environment**:** Offer training for users on how to effectively operate the system.

IV.SECURITY

Security of smart security systems based on IoT is an essential issue because these systems are more integrated into residential and business spaces. Main threats include unauthorized access, data compromise, tampering with the device, and denial-of-service attacks. Such threats may cause severe privacy intrusions, financial losses, and even bodily injuries. The major techniques involve in security are as follows:

1. Authentication and Access Control: Having strong authentication controls, like multi-factor authentication (MFA) and biometric authentication, can go a long way to prevent unauthorized access. Role-based access control (RBAC) can also make sure that the users have the correct permissions according to their roles.

2. Data Encryption: Encrypting data at rest and in transit is critical for preventing sensitive information from being intercepted and accessed inappropriately. Strong encryption protocols such as advanced encryption standards (AES) and secure communication protocol TLS/SSL are widely used to ensure data integrity and confidentiality.

3. Intrusion Detection Systems (IDS): With the help of machine learning algorithms, one can create intelligent intrusion detection systems to identify and act on unusual behaviour in real time. The systems can look for patterns of regular activity and report on deviations that can signify a security compromise.

4. Periodic Software Updates and Patch Management: Keeping all software and devices updated on a regular basis is essential for safeguarding against known vulnerabilities. Automated patch management tools can be used to ensure the security stance of IoT devices.

5. Secure Device Design: Including security functionality at the hardware level, e.g., secure boot procedures and hardware-based security modules (HSMs), can improve the resistance of IoT devices to tampering and physical attacks.

6. User Awareness and Education: Educating the users on the possible risks related to IoT devices and best practices for the security of their systems can go a long way in minimizing the chances of human mistake causing security breaches.

7. Privacy-Safeguarding Mechanisms: Use of privacy-safeguarding data aggregation anonymization mechanisms can help ensure user data protection without compromising the ability to monitor and analyze effectively.

8. Blockchain Technology: Utilizing blockchain for decentralized security can increase the integrity and traceability of data transactions across IoT networks, making it harder for malicious parties to tamper with data.

9. Collaboration and Standards: Encouraging collaboration between manufacturers, researchers, and policymakers to create industry standards and best practices can result in more secure IoT ecosystems.

V. RESULT AND DISCUSSION

The smart security system based on IoT is a revolutionary leap forward in home safety and security management. Through the capability of Internet of Things (IoT) technology, this system facilitates real-time remote monitoring and control of multiple security devices like cameras, motion sensors, and alarms.
Salient outcomes of the project include successful incorporation of future sensors and artificial intelligence (AI) technologies that immensely improve detection capabilities and eliminate false alarms. The user-friendly interface of the system enables residents to conveniently view and control their security settings anywhere, giving them peace of mind and more control over their home environment.

Additionally, the application of machine learning algorithms allows the system to learn from user behaviour and adjust to possible threats, further enhancing its responsiveness and reliability. Overall, the IoT-based smart security system

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

not only provides enhanced safety for homes but also creates a sense of security and empowerment for users, making it a worthwhile addition to contemporary living.

VI. CONCLUSION

It has been successfully demonstrated that the Smart Security is an IoT-enabled security system combining various modern technologies that improve safety at the home and property. The efficient monitoring, instant alerts, and remote-control features are achieved by making use of sensors, cameras, microcontrollers together with real-time data transmission on the IoT network. Moreover, the system increased responsiveness to security threats and reduced the dependency and human error.

The system detects and reacts to intrusion events and provides functionality allowing users to connect remotely with their environment. The system's key activities include motion detection, video surveillance, and even environmental monitoring, working in synergy to form a complete, robust security solution. Sensors and smart devices create an arrangement whereby weird and unusual things are rapidly detected and reported, thus significantly reducing response time with an efficient overall safety structure.

The easy and uses friendly interface, along with an interoperability with existing smart home technologies, has made our system available for a spectrum of users-the tech-savvy and those who are less informed of digital solutions. Such inclusiveness would strengthen efforts toward adoption among the general public.

REFERENCES

1. Nayak, Manjushree, and Ashish Kumar Dass. "GSM and Arduino based Smart Home Safety and Security System." Recent Trends in Information Technology and its Application 6.1 (2023): 20-25.
2. Ali, W.; Dustgeer, G.; Awais, M.; Shah, M.A. IoT based smart home: Security challenges, security requirements and solutions. In Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017; pp. 1–6.
3. GUPTA, SHIKHA, et al. "SMART HOME SECURITY SYSTEM USING ARDUINO AND GSM." Journal of Engineering Sciences 14.06 (2023).
4. Alsayaydeh, Jamil Abedalrahim Jamil, et al. "Development of programmable home security using GSM system for early prevention." ARPN Journal of Engineering and Applied Sciences 16.1 (2021): 88-97.
5. Efe, Eseosa Ehioghae, and Samson Ogunlere. "Design and Implementation of a Mobile-Based Home Security System." American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS) 72.1 (2020): 101-112.
6. Munawir Ihsan, A., and E. Mutia. "Wi-Fi and GSM Based Motion Detection in Smart Home Security System IOP Conf." Ser. Mater. Sci. Eng 536.1 (2019): 1-8.
7. Home Security System Using IOT Tanaya Department of Electronics and Communication Engineering, SRM Institute os Science and Technology, Chennai, India Volume 119 No. 15 2018, 1863-1868 ISSN: 1314-3395 (on-line version) url: http://www.acadpubl.eu/hub/ Special Issue.
8. HOME SECURITY SYSTEM Leya Laiju1, Sherin Shaju2, Janet Jose3, Willson Joseph C4 1,2,3UG.Scholar, 4Assisstant professor , VOLUME-5, ISSUE-2, 2018.
9. Gavra, V.D.; Dobra, I.M.; Pop, O.A. A survey on threats and security solutions for IoT. In Proceedings of the 2020 43rd International Spring Seminar on Electronics Technology (ISSE), Demanovska Valley, Slovakia, 14–15 May 2020; pp. 1–5.
10. Geneiatakis, D.; Kounelis, I.; Neisse, R.; Nai-Fovino, I.; Steri, G.; Baldini, G. Security and privacy issues for an IoT based smart home. In Proceedings of the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017; pp. 1292–1297.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details