International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902003

IoT Based Security & Smart Home Intrusion Prevention System

Yerra Bhagyasri [1], Potaraju Bhargavi [2], Thatipamula Akshaya [3], Sakarman Pavansai [4]

Dr. Prasad Dharnasi [5], A. Jitendra [6]

[1]UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology &Science, Bogaram, Keesara, Telangana,India

[2]UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology &Science, Bogaram, Keesara, Telangana, India

[3]UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology &Science, Bogaram, Keesara, Telangana, India

[4]UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology &Science, Bogaram, Keesara, Telangana, India

[5]Professor, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science, Telangana, India

Associate Professor, Department of Computer Science and Engineering, Holy Mary Institute of Technology &Science, Telangana, India

Publication History: Received: 12.02.2026; Revised: 01.03.2026; Accepted: 05.03.2026; Published: 08.03.2026.

ABSTRACT: Smart home environments are increasing due to the rapid growth of Internet of Things (IoT) technologies. However, this smart homes introduces security vulnerabilities, unauthorized access and intrusions. For preventing intrusion using IoT sensors we are introducing proposed smart home system. Home Intrusion Prevention System is mainly used for, wireless communication, and automated alert mechanisms. Smart home system continuously monitors entry points using sensors such as PIR (Passive Infrared), ultrasonic, and door/window magnetic sensors. Alarm triggers, light detects when an unauthorized access is detected through a smartphone through a cloud-based platform or mobile application. Additionally, system can activate preventive responses such as locking doors or turning on lights to deter intruders. Current project focuses on low-cost implementation, real-time monitoring, and user-friendly control, making it suitable for residential security. This solution ultimately provides a reliable and efficient intrusion prevention system that increases safety, reduces human dependency, and enhances the overall smart home experience.

KEYWORDS: IoT, Smart Home, Intrusion Detection, Security System, PIR Sensor, Real-Time Monitoring, Cloud Communication, Home Applications.

I. INTRODUCTION

In recent years, smart homes are increasing due to the advance technologies and IoT(Internet of Things). Smart home systems allow users to control and monitor household devices remotely, improving safety, energy efficiency, and overall lifestyle. Smart home systems have several advantages mainly unauthorized detection and security . Current smart home security mostly operated manually it need lots of efforts and it may fail sometimes.

In this advanced generation we need advanced artificial intelligence because many intrusions are happening. Iot provides platforms for communicating with devices, detecting unusual activities and sensors .By using this sensors, detectors we can easily detect unauthorized users and can take action immediately.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902003

Our project is to enhance the smart homes by preventing intrusions by combining IoT sensors, wireless communication, and automated alert mechanisms. Smart home system monitors entry points such as doors, windows, and surrounding areas using sensors like PIR, ultrasonic, and magnetic sensors. When unusual movement or intrusion is detected, the system immediately activates alarms and sends notifications to the homeowner through a mobile application or cloud-based platform. In addition, the system can trigger preventive actions such as switching on lights or locking doors to discourage intruders.

The main objective of this project is to develop a cost-effective, reliable, and user-friendly home security solution that reduces human dependency while ensuring real-time monitoring. The proposed system aims to provide enhanced safety and improve the overall smart home experience.

II. LITERATURE REVIEW

A literature survey is an important part of any project that explains the previous research and developments related to the selected topic. In 2019, researchers developed basic IoT based home automation systems using sensors and microcontrollers to control appliances like lights and fans remotely. In 2020, several studies introduced mobile application-based control systems that allowed users to monitor and operate home devices from anywhere, improving convenience. In 2021, Kumar et al. developed an IoT based smart home system using Arduino and wireless communication, which improved automation but had limited security features. In 2022, Sharma et al. proposed a smart security system using motion sensors and surveillance cameras to detect unauthorized access, but it increased system cost and maintenance. In 2023, researchers focused on integrating both automation and security using IoT platforms to provide efficient and user-friendly systems. Based on these developments, this project aims to design an IoT based security and smart home system that provides better safety, remote monitoring, and cost-effective automation.

III. PROBLEM STATEMENT

The existing home systems require manual control and often provide only security or automation features separately. This makes them less efficient and difficult to monitor remotely. The problem is the need for a simple, low-cost system that provides both security and home automation. The proposed IoT based security and smart home system helps users monitor their homes and control appliances remotely.

IV. RESEARCH METHODOLOGY

1. Research Design

The research design is based on developing an IoT based security and smart home system using a system development approach. It is mainly for identifying user requirements such as home security monitoring, intrusion detection, and remote control of household appliances. After analyzing these requirements, suitable hardware components like sensors, microcontroller, communication modules, and internet platforms are selected.

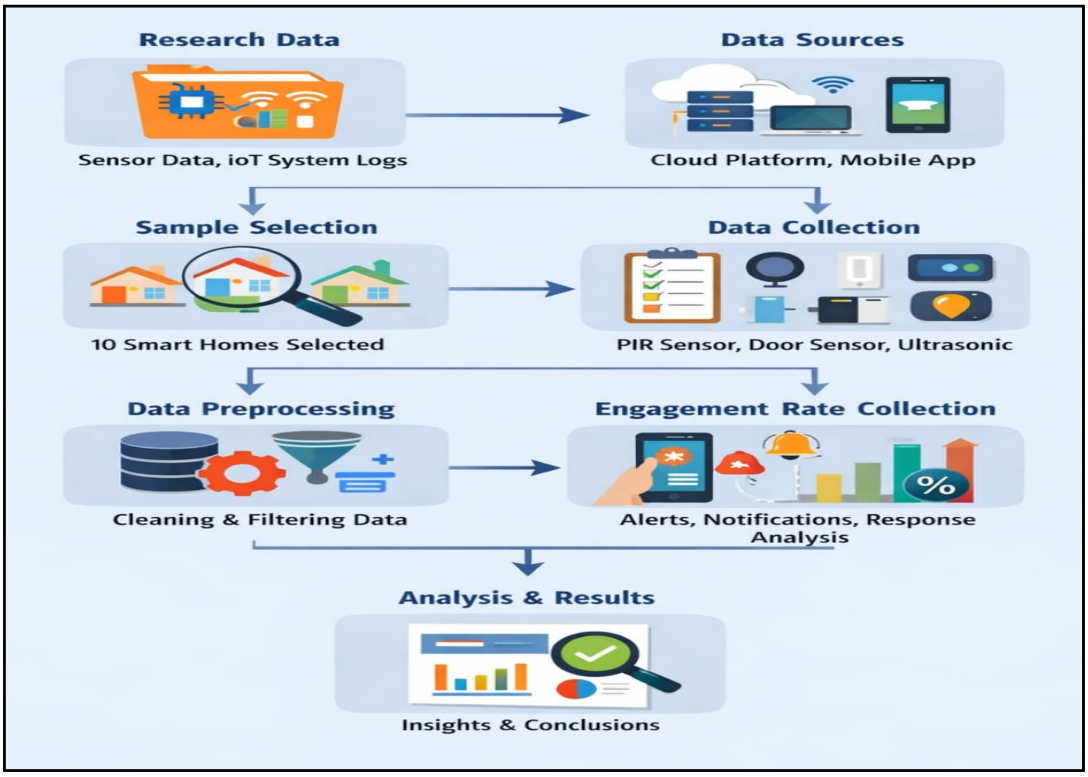
The smart system is designed to collect data from sensors such as motion detectors and temperature sensors. This data is processed by the microcontroller and transmitted to users through internet-based applications or mobile devices. Our project design also focuses on making the system user-friendly, cost-effective, and reliable.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902003



2. Data Sources

The data used in this research is obtained from **public profiles of coding influencers** across multiple social media platforms:

Sensor Readings Hardware Testing data IoT cloud logs GitHub

Only publicly accessible metrics are considered to ensure ethical data usage and compliance with platform policies.

3. Sample Selection

A purposive sampling technique is used to select suitable components and technologies for the development of the IoT based security and smart home system based on the following criteria:

- Components related to home security and automation
- Reliable sensors and microcontroller modules
- Low-cost and easily available hardware devices
- Efficient internet and communication modules
- Compatibility with mobile or web-based control systems
- Proper functioning and testing under different condition

4. Data Collection Parameters

The following parameters are collected for the IoT based security and smart home system:
Sensor Metrics: Motion detection, temperature, smoke or gas detection, door or window status
Security Metrics: Intrusion alerts, alarm activation, camera monitoring
Device Control Metrics: Appliance ON/OFF status, remote control usage, device response
System Metrics: Network connectivity, data transmission, power consumption
Data is collected through sensors, microcontroller, and IoT platforms to monitor system performance and security.

5. Data Preprocessing

Before analysis, the collected data undergoes preprocessing:

- Removal of duplicate or unwanted sensor data
- Handling missing or incorrect data values
- Normalization of sensor readings and device status records
- Conversion of collected data into suitable digital format

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902003

- Verification of data accuracy and system performance

This processing ensures reliable monitoring and proper functioning of the IoT based security and smart home system.

6. Engagement Rate Calculation

Using the following standard formula, the performance rate of the IoT based security and smart home system is calculated:

System Response Rate (%) = (Successful Alerts + Successful Device Operations / Total Requests or Events) × 100

Where:

- Successful Alerts = Number of correctly generated security alerts
- Successful Device Operations = Number of appliances correctly controlled through the system
- Total Requests or Events = Total number of sensor detections, user commands, or security events

This calculation helps measure the efficiency, reliability, and performance of the smart home security system.

V. ANALYSIS

The proposed IoT-based security and smart home intrusion prevention system was analyzed in terms of performance, reliability, and real-time monitoring capability. To continuously monitor household activities the system uses door sensors, microcontrollers, and IoT sensors. During testing, the sensors responded effectively to intrusion events and transmitted alerts to the user through a cloud-based notification system with minimal delay under stable network conditions. The collected data was processed , enabling proper activation of alarms and remote control functions. Small variations in response time were observed due to network fluctuations, but overall system operation remained stable. The use of low-cost and easily available IoT components makes the system practical for residential deployment, while the modular design allows future expansion with additional sensors and automation features. This analysis shows that the proposed system provides a reliable, efficient, and scalable approach for improving smart home security

VII. CONCLUSION

The IoT based security and smart home system is developed to improve home safety, monitoring, and automation. The system successfully integrates sensors, microcontroller, and internet technology to detect security threats and control home appliances remotely. This smart home system mainly focusing on security and preventing intrusions using advanced sensors and artificial intelligence..

This smart home system is user friendly, reliable and suitable for modern lives. It reduces manual effort and increases convenience by enabling automatic and remote control of household appliances. The testing results show that the system performs efficiently and correctly under different conditions.

Overall, the project demonstrates that IoT technology plays an important role in improving home security and automation. Smart home system can be further improved by adding advanced features such as voice control, artificial intelligence, and improved data analytics to provide better performance and smart decision-making.

This project highlights the importance of IoT technology in improving home security and automation. It demonstrates how smart systems can provide better safety, comfort, and efficient resource management. In future, this system can be change or improved by providing more advanced technologies for a better living.

VII. FUTURE SCOPE

The proposed IoT-based security and smart home intrusion prevention system provides an effective and low-cost solution for improving residential security through real-time monitoring and automated alerts. In the future, the system can be enhanced by integrating Artificial Intelligence (AI) and Machine Learning (ML) techniques to analyze sensor data and detect suspicious activities more accurately while reducing false alarms. Advanced features such as facial recognition and smart camera surveillance can be added to automatically identify authorized and unauthorized persons. The system can also be connected to cloud platforms for secure data storage, remote access, and advanced analytics. Implementing strong encryption and secure communication protocols will further improve protection against cyber threats. Additionally, integration with voice assistants and smart energy management systems can increase user convenience and efficiency. These enhancements will make the system more intelligent, scalable, and suitable for real-world smart home and smart city applications.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902003

REFERENCES

1. Amitha, K., Ram Manohar Reddy, M., Yashwanth, K., Shylaja, K., Rahul Reddy, M., Srinu, B., & Dharnasi, P. (2026). AI empowered security monitoring system with the help of deployed ML models. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(1), 69–73.
2. Itoo, S., Khan, A. A., Ahmad, M., & Idrisi, M. J. (2023). A secure and privacy-preserving lightweight authentication and key exchange algorithm for smart agriculture monitoring system. IEEE Access, 11, 56875-56890.
3. Vaidya, S., Shah, N., Shah, N., & Shankarmani, R. (2020, May). Real-time object detection for visually challenged people. In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 311-316). IEEE.
4. Gogada, S., Gopichand, K., Reddy, K. C., Keerthana, G., Nithish Kumar, M., Shivalingam, N., & Dharnasi, P. (2026). Cloud computing/deep learning customer churn prediction for SaaS platforms. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(1), 74–78.
5. Devarajan, R., Prabakaran, N., Vinod Kumar, D., Umasankar, P., Venkatesh, R., & Shyamalagowri, M. (2023, August). IoT Based Under Ground Cable Fault Detection with Cloud Storage. In 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1580-1583). IEEE.
6. Akula, A., Budha, G., Bingi, G., Chanda, U., Borra, A. R., Yadav, D. B., & Saravanan, M. (2026). Emotion recognition from facial expressions using CNNs. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(1), 120–125.
7. Poornima, G., & Anand, L. (2025). Medical image fusion model using CT and MRI images based on dual scale weighted fusion based residual attention network with encoder-decoder architecture. Biomedical Signal Processing and Control, 108, 107932.
8. Kiran, A., & Kumar, S. A methodology and an empirical analysis to determine the most suitable synthetic data generator. IEEE Access 12, 12209–12228 (2024).
9. Varshini, M., Chandrapathi, M., Manirekha, G., Balaraju, M., Afraz, M., Sarvanan, M., & Dharnasi, P. (2026). ATM access using card scanner and face recognition with AIML. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(1), 113–118.
10. Thirumal, L., & Umasankar, P. (2026). Precision muscle segmentation and classification for knee osteoarthritis with dual attention networks and GAO-optimized CNN. Biomedical Signal Processing and Control, 111, 108244.
11. Feroz, A., Pranay, D., Srikar Sai Raj, B., Harsha Vardhan, C., Rohith Raja, B., Nirmala, B., & Dharnasi, P. (2026). Blockchain and machine learning combined secured voting system. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(1), 119–124.
12. Ananth, S., Radha, K., & Raju, S. (2024). Animal Detection In Farms Using OpenCV In Deep Learning. Advances in Science and Technology Research Journal, 18(1), 1.
13. Inbavalli, M., & Arasu, T. (2015). Efficient Analysis of Frequent Item Set Association Rule Mining Methods. International Journal of Scientific & Engineering Research, 6(4).
14. Tirupalli, S. R., Munduri, S. K., Sangaraju, V., Yeruva, S. D., Saravanan, M., & Dharnasi, P. (2026). Blockchain integration with cloud storage for secure and transparent file management. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(1), 79–86.
15. Prasanna, D., & Santhosh, R. (2018). Time Orient Trust Based Hook Selection Algorithm for Efficient Location Protection in Wireless Sensor Networks Using Frequency Measures. International Journal of Engineering & Technology, 7(3.27), 331-335.
16. Chandu, S., Goutham, T., Badrinath, P., Prashanth Reddy, V., Yadav, D. B., & Dharnas, P. (2026). Biometric authentication using IoT devices powered by deep learning and encrypted verification. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(1), 87–92.
17. Aashiq Banu, S., Sucharita, M. S., Soundarya, Y. L., Nithya, L., Dhivya, R., & Rengarajan, A. (2020). Robust Image Encryption in Transform Domain Using Duo Chaotic Maps—A Secure Communication. In Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020 (pp. 271-281). Singapore: Springer Singapore.
18. Singh, K., Amrutha Varshini, G., Karthikeya, M., Manideep, G., Sarvanan, M., & Dharnasi, P. (2026). Automatic brand logo detection using deep learning. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(1), 126–130.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902003

19. Neela Madheswari, A., Vijayakumar, R., Kannan, M., Umamaheswari, A., & Menaka, R. (2022). Text-to-speech synthesis of indian languages with prosody generation for blind persons. In IOT with Smart Systems: Proceedings of ICTIS 2022, Volume 2 (pp. 375-380). Singapore: Springer Nature Singapore.
20. Keerthana, L. M., Mounika, G., Abhinaya, K., Zakeer, M., Chowdary, K. M., Bhagyaraj, K., & Prasad, D. (2026). Floods and landslide prediction using machine learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(1), 125–129.
21. Gopinathan, V. R. (2025). Designing Cloud-Native Enterprise Systems by Modernizing Applications with Microservices and Kubernetes Platforms. International Journal of Research and Applied Innovations, 8(5), 13052-13063.
22. Kumar, A. S., Saravanan, M., Joshna, N., & Seshadri, G. (2019). Contingency analysis of fault and minimization of power system outage using fuzzy controller. International Journal of Innovative Technology and Exploring Engineering, 9(1), 4111-4115.
23. Dadigari, M., Appikatla, S., Gandhala, Y., Bollu, S., Macha, K., & Saravanan, M. (2026). Bitcoin price prediction with ML through blockchain technology. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(1), 130–136.
24. Chinthala, S., Erla, P. K., Dongari, A., Bantu, A., Chityala, S. G., & Saravanan, M. S. (2026). Food recognition and calorie estimation using machine learning. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(2), 480–488.
25. Dharnasi, P. (2025). A Multi-Domain AI Framework for Enterprise Agility Integrating Retail Analytics with SAP Modernization and Secure Financial Intelligence. International Journal of Humanities and Information Technology, 7(4), 61-66.
26. Vimal Raja, G. (2025). Context-Aware Demand Forecasting in Grocery Retail Using Generative AI: A Multivariate Approach Incorporating Weather, Local Events, and Consumer Behaviour. International Journal of Innovative Research in Science Engineering and Technology (Ijirset), 14(1), 743-746.
27. Chinthamalla, N., Anumula, G., Banja, N., Chelluboina, L., Dangeti, S., Jitendra, A., & Saravanan, M. (2026). IoT-based vehicle tracking with accident alert system. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 486–494.
28. Nagamani, K., Laxmikala, K., Sreeram, K., Eshwar, K., Jitendra, A., & Dharnasi, P. (2026). Disaster management and earthquake prediction system using machine learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 495–499.
29. Harish, M., & Selvaraj, S. K. (2023, August). Designing efficient streaming-data processing for intrusion avoidance and detection engines using entity selection and entity attribute approach. In AIP Conference Proceedings (Vol. 2790, No. 1, p. 020021). AIP Publishing LLC.
30. Prasad, E. D., Sahithi, B., Jyoshnavi, C., Swathi, D., Arun Kumar, T., Dharnasi, P., & Saravanan, M. (2026). A technology driven – solution for food and hunger management. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 440–448.
31. Archana, R., & Anand, L. (2025). Residual u-net with Self-Attention based deep convolutional adaptive capsule network for liver cancer segmentation and classification. Biomedical Signal Processing and Control, 105, 107665.
32. Saravanan, M., Kumar, A. S., Devasaran, R., Seshadri, G., & Sivaganesan, S. (2019). Performance analysis of very sparse matrix converter using indirect space vector modulation. Intern. Jou. of Inn. Techn. and Expl. Eng, 9(1), 4756-4762.
33. Saravanan, M., & Sivakumaran, T. S. (2016). Three phase dual input direct matrix converter for integration of two AC sources from wind turbines. Circuits Syst., 7, 3807-3817.
34. Rakesh, V., Vinay Kumar, M., Bharath Patel, P., Varun Raj, B., Saravanan, M., & Dharnasi, P. (2026). IoT-based gas leakage detector with SMS alert. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 449–456.