

Research Paper

Iot-Enabled Theft Detection And Automatic Alert Notification System For Smart Security Monitoring

¹Dr. A. Swetha,²Kokkanti Keerthana,³Mangala Venkata Sai Lakshmi,⁴Paturi Sindhu,⁵Segu Manvitha,⁶Thelladala Radhika

¹Professor, Department of Electronics and Communication Engineering, Dr. K.V. Subba Reddy Institute of Technology

^{2,3,4,5,6}B. Tech Student, Department of Electronics and Communication Engineering, Dr. K.V. Subba Reddy Institute of Technology

ABSTRACT

The increasing occurrence of theft and unauthorized intrusions across homes, vehicles, offices, and commercial facilities highlights the need for intelligent, automated security systems. Traditional surveillance methods, such as CCTV cameras and manual monitoring, often fail to provide real-time alerts and immediate response. This research proposes an Internet of Things (IoT)-based theft control and auto-alerting system designed to detect unauthorized access and instantly notify the owner or security personnel through mobile notifications. The system integrates sensors such as PIR (Passive Infrared), vibration sensors, magnetic door sensors, and cameras with an IoT microcontroller like ESP8266/ESP32. Upon detecting suspicious activity, the device sends real-time alerts through cloud platforms (e.g., Blynk, MQTT, or Firebase), activates alarms, and records evidence. The system also supports GPS-based tracking for theft scenarios involving vehicles. The proposed framework ensures low-cost, real-time monitoring, remote visibility, and rapid preventive action. The integration of IoT and automation enhances security, minimizes human dependency, and creates an effective anti-theft solution suitable for homes, vehicles, shops, and industrial applications.

Keywords: Internet of Things (IoT), Theft Detection, Smart Security Monitoring, Intrusion Detection System, ESP8266/ESP32 Microcontroller, PIR Sensor, Vibration Sensor, Magnetic Door Sensor, Real-Time Alert Notification, Cloud-Based Monitoring.

I. INTRODUCTION

Security concerns have become increasingly significant due to the rise in property theft, break-ins, and unauthorized intrusions in residential and commercial environments. Traditional security systems rely heavily on human involvement and require constant monitoring to be effective. However, in most cases, theft incidents occur when premises are unattended or when the owner is unable to respond immediately. IoT technology offers a transformative solution by enabling continuous monitoring, wireless communication, and smart automation. An IoT-based theft control system integrates sensors, controllers, and cloud communication to detect intrusions instantly and send real-time notifications to the user's smartphone. These systems can be deployed in homes, offices, vehicles, and storage units to provide robust, reliable, and intelligent security. The proposed solution enhances efficiency through remote access, automation, and data logging. By leveraging IoT platforms, users can monitor their property from anywhere, receive alerts instantly, and initiate preventive actions, significantly reducing security risks and enhancing overall safety.

II. Related Words

The rapid growth of the Internet of Things (IoT) has significantly influenced the development of intelligent monitoring and security systems. IoT enables the interconnection of physical devices through

sensors, communication networks, and cloud platforms, allowing real-time data collection and automated decision-making. Early research on IoT highlighted its capability to integrate smart devices and provide advanced automation across various applications such as smart homes, healthcare, and security monitoring. Atzori et al. discussed the fundamental architecture and communication models of IoT systems, emphasizing the importance of connectivity between heterogeneous devices for building intelligent environments [1]. Similarly, Evans explained how IoT technologies can transform traditional systems into smart and automated solutions capable of improving efficiency and safety in multiple domains [2].

Security and privacy remain critical concerns in IoT-based applications, especially in surveillance and intrusion detection systems. Several researchers have explored IoT frameworks to enhance security monitoring and intrusion detection. Abomhara and Køien examined the current challenges related to IoT security and identified vulnerabilities that arise from network connectivity and device heterogeneity [3]. Ning and Liu proposed a cyber-physical-social security architecture to strengthen IoT systems by integrating sensing devices with secure communication layers [9]. These studies highlight the importance of secure architectures for ensuring reliable monitoring and protection in IoT-based environments.

Researchers have also explored the integration of IoT with smart city infrastructures to enhance public safety and monitoring. Zanella et al. demonstrated how IoT technologies can support smart city applications such as traffic management, environmental monitoring, and urban security through sensor networks and cloud-based data analysis [5]. Madakam et al. provided a comprehensive literature review discussing IoT applications in smart homes and surveillance systems, emphasizing the role of sensors and wireless networks in building automated monitoring frameworks [4]. These works show that IoT-based monitoring systems can improve situational awareness and enable real-time decision-making.

Several studies have focused on the architecture and communication protocols required for IoT-based systems. Sethi and Sarangi analyzed different IoT architectures and communication protocols, highlighting the importance of lightweight communication mechanisms for efficient device interaction [6]. Granjal et al. investigated security protocols for IoT environments and identified the need for secure communication channels to protect data transmitted between sensors and cloud platforms [7]. Similarly, Al-Fuqaha et al. presented an extensive survey on IoT technologies, protocols, and applications, emphasizing the integration of sensing devices, cloud computing, and wireless communication for intelligent system

development [8].

Recent research also emphasizes the role of IoT frameworks in enabling scalable and reliable applications. Want et al. described the technological advancements that enable IoT devices to communicate seamlessly across networks, enabling applications such as smart surveillance and automated alert systems [10]. Weyrich and Ebert proposed reference architectures for IoT systems that support scalable deployment and interoperability among devices [11]. Li et al. further discussed IoT frameworks that support real-time monitoring and data analysis through distributed networks [12]. Additionally, studies such as those by Rose et al. and Vermesan and Friess provide comprehensive overviews of IoT technologies and their potential applications in security and monitoring systems [13], [15]. The routing and communication infrastructure supporting IoT devices has also been addressed through protocols such as RPL, which enables efficient communication in low-power and lossy networks commonly used in sensor-based IoT systems [14].

Overall, previous studies demonstrate that IoT technologies provide an effective platform for building intelligent monitoring and security systems. However, many existing solutions focus mainly on connectivity and data collection, while limited attention has been given to integrated theft detection mechanisms combined with real-time alert notifications

and automated response systems. Therefore, the proposed IoT-enabled theft detection and automatic alert notification system aims to address these gaps by integrating multiple sensors, real-time monitoring, and cloud-based alert mechanisms to provide an efficient and cost-effective smart security solution.

III. PROPOSED MODEL

The proposed IoT-Enabled Theft Detection and Automatic Alert Notification System for Smart Security Monitoring is designed to provide real-time monitoring and immediate alerts when unauthorized access or suspicious activity is detected. The system integrates multiple sensors, an IoT-enabled microcontroller, cloud communication platforms, and alert mechanisms to create an intelligent and automated security framework. The primary objective of the proposed model is to enhance safety in homes, vehicles, offices, and commercial areas by detecting intrusion attempts and instantly notifying the owner or security personnel.

In the proposed system, various sensing components such as Passive Infrared (PIR) sensors, vibration sensors, and magnetic door sensors are deployed at strategic locations to monitor movement, door status, and unusual disturbances. These sensors continuously collect environmental data and transmit it to an IoT microcontroller such as ESP8266 or ESP32. The microcontroller processes the sensor inputs and determines whether the detected activity indicates a

potential intrusion. When an abnormal event such as unauthorized motion, forced entry, or vibration is identified, the controller triggers an alert mechanism and initiates communication with the cloud platform.

The system uses IoT cloud services such as Blynk, MQTT, or Firebase to transmit real-time data from the microcontroller to the user's mobile device or monitoring application. Through this cloud-based communication, users can remotely monitor the status of their property and receive instant notifications when suspicious activity is detected. Additionally, the system activates local security measures such as buzzers or alarm systems to deter potential intruders. The integration of cameras enables the system to capture images or video footage during intrusion events, providing evidence for further investigation. To further enhance security, the proposed model can incorporate GPS modules for vehicle tracking, allowing users to locate their vehicle in case of theft. The IoT platform also supports remote monitoring and control, enabling users to view sensor data, receive alerts, and manage the system through a smartphone or web interface. This connectivity ensures that the user remains informed about security events regardless of their physical location.

Overall, the proposed model provides a cost-effective, scalable, and intelligent security monitoring solution by combining sensor-based detection, IoT communication, and automated alert mechanisms. The integration of multiple sensing technologies

and cloud connectivity improves the reliability and efficiency of theft detection while minimizing human intervention. This system offers a practical solution for smart security monitoring across residential, commercial, and industrial environments.

IV. PROPOSED SYSTEM

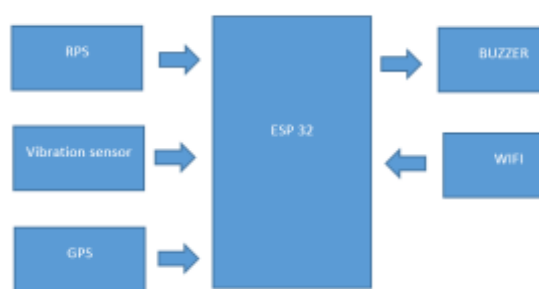


Fig.1. Block diagram

The diagram represents the architecture of the IoT-Enabled Theft Detection and Automatic Alert Notification System. In this system, the ESP32 microcontroller acts as the central processing unit that connects and manages multiple sensors and communication modules. The PIR sensor (RPS in the diagram) detects human motion or unauthorized presence, while the vibration sensor identifies unusual movements or forced tampering such as breaking doors, windows, or vehicle parts. The GPS module is used to track the location of the asset, which is especially useful in vehicle theft scenarios. All sensor data is continuously monitored and processed by the ESP32 controller. When suspicious activity is detected, the controller activates a buzzer to produce an alarm that warns nearby people and deters intruders. Simultaneously, the

system uses the Wi-Fi module integrated with the ESP32 to transmit real-time alerts and location information to the user through an IoT cloud platform or mobile application. This architecture enables real-time monitoring, quick theft detection, and immediate notification, making the system an effective smart security solution.

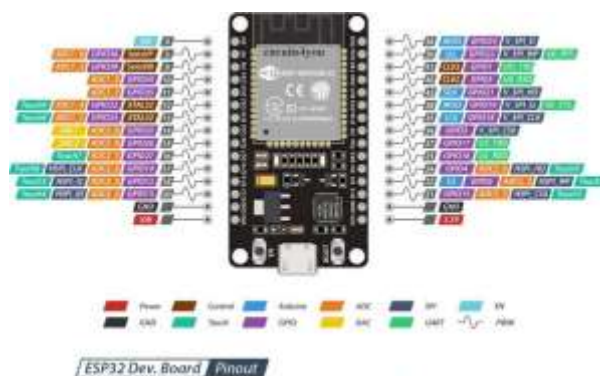


Fig.2. ESP32 WROOM32 DevKit Pinout

V. RESULTS AND DESCUSSIONS

The proposed IoT-Enabled Theft Detection and Automatic Alert Notification System for Smart Security Monitoring enhances security monitoring by integrating IoT communication, embedded processing, and sensor-based intrusion detection. The system continuously monitors secured areas such as homes, vehicles, offices, and commercial facilities using multiple sensors connected to the ESP32 microcontroller. Sensors such as the PIR motion sensor, vibration sensor, and magnetic door sensor detect unauthorized access, forced entry, or unusual disturbances. When suspicious activity is identified, the ESP32 controller processes the sensor data and immediately activates alert mechanisms such as a buzzer alarm and mobile notifications through Wi-Fi connectivity. This real-time monitoring

and alerting capability enables users to respond quickly to potential theft attempts. The specifications of the components used in the proposed system are presented in Table 1. The ESP32 microcontroller acts as the central controller responsible for processing sensor inputs and enabling IoT communication. The PIR motion sensor detects human presence or movement in restricted areas, while the vibration sensor identifies unusual disturbances such as forced entry or tampering. The GPS module enables real-time location tracking in case of vehicle theft scenarios. The Wi-Fi module, integrated within the ESP32 controller, enables wireless communication between the system and cloud platforms such as Blynk or Firebase. The buzzer acts as an alarm system that alerts nearby individuals when suspicious activity is detected.

TABLE 1: SENSOR AND COMPONENT SPECIFICATION

Sl.NO	Components	Specifications
1	ESP32 Microcontroller	Operating Voltage: 3.3–5V, Built-in Wi-Fi, Dual-core processor
2	PIR Motion Sensor	Operating Voltage: 5V, Detection Range: 3–7 m
3	Vibration Sensor	Detects shock, tampering, or forced movement
4	Magnetic Door	Detects door or

Sl.NO	Components	Specifications
	Sensor	window opening
5	GPS Module	Provides real-time location tracking
6	Wi-Fi Module	Wireless communication for IoT monitoring
7	Buzzer	Audible alarm for intrusion alert
8	Power Supply	Battery or regulated power source for system operation

The hardware implementation integrates all sensing components with the ESP32 microcontroller to create an intelligent security monitoring system. During operation, the sensors continuously monitor environmental conditions and send data signals to the ESP32 controller. The PIR sensor detects motion and human presence in protected areas, while the vibration sensor detects unusual movements such as breaking doors, windows, or forced entry attempts. The magnetic door sensor monitors door or window status and sends signals to the controller if unauthorized opening occurs. These sensor inputs allow the system to identify possible intrusion events in real time.

Once suspicious activity is detected, the ESP32 controller activates the buzzer alarm to warn nearby individuals and deter potential intruders. Simultaneously, the system sends instant notifications to the user through the IoT cloud platform using Wi-Fi connectivity. These notifications may

include alert messages, sensor status, and location information if the GPS module is enabled. This real-time communication allows users to monitor their property remotely through a mobile application or web-based interface.

The experimental results demonstrate that the proposed system effectively detects intrusion attempts and provides timely alerts. The PIR sensor accurately detects human motion within its operational range, while the vibration sensor reliably identifies abnormal disturbances caused by tampering or forced entry. The Wi-Fi communication module ensures stable transmission of alert notifications and monitoring data to the remote platform. Additionally, the GPS module successfully provides location information for mobile assets such as vehicles, enabling users to track their assets in case of theft.

Overall, the implementation of the proposed system significantly improves security monitoring by enabling continuous surveillance, automated intrusion detection, and real-time alert notifications. The integration of IoT communication with sensor-based monitoring reduces human dependency and enhances the efficiency of theft prevention mechanisms. By combining embedded systems, intelligent sensing technologies, and wireless communication networks, the proposed system provides a cost-effective, scalable, and reliable smart security solution suitable for residential, commercial, and industrial environments.

VI. CONCLUSION AND FUTURE

SCOPE

Conclusion:

IoT-enabled theft control systems offer a powerful solution to the limitations of traditional security methods by enabling real-time monitoring, automated detection, and instant mobile notifications. The literature highlights the evolution from simple sensor-based alarms to intelligent, cloud-connected and edge-processing security frameworks. The proposed IoT theft control system integrates sensors, cloud communication, and real-time alerting to provide an efficient and scalable security solution. Whether deployed in homes, shops, offices, or vehicles, such systems enhance safety by ensuring immediate detection and rapid intervention. With future improvements in AI, image recognition, and edge computing, IoT security systems will continue to become more robust, intelligent, and responsive.

Future Scope:

The proposed IoT-Enabled Theft Detection and Automatic Alert Notification System for Smart Security Monitoring can be further enhanced by integrating advanced technologies to improve security, reliability, and scalability. In future developments, the system can incorporate artificial intelligence and machine learning algorithms to analyze sensor data and identify suspicious behavior more accurately. This would enable the system to distinguish between normal movements and potential threats, thereby reducing false alarms and improving detection accuracy.

Another possible enhancement is the integration of facial recognition and image processing techniques using camera modules. By implementing computer vision algorithms, the system could identify authorized individuals and detect unknown intruders automatically. This feature would add an additional layer of security by combining biometric authentication with sensor-based monitoring.

The system can also be expanded by integrating cloud-based data analytics and mobile applications for advanced monitoring and control. Cloud storage can maintain historical records of security events, which can be useful for analyzing intrusion patterns and improving security strategies. Additionally, the development of a dedicated mobile application could provide users with a more interactive interface for real-time monitoring, alert management, and remote control of security devices.

Furthermore, the system can be enhanced with low-power communication technologies such as LoRa or NB-IoT to support long-range monitoring and reduce power consumption. This would make the system suitable for large-scale applications such as industrial facilities, warehouses, and smart city infrastructure. Future versions may also integrate solar-powered energy systems to ensure continuous operation in remote locations.

Overall, these advancements can transform the proposed system into a fully intelligent smart security platform capable of providing

predictive security monitoring, improved threat detection, and enhanced automation for modern IoT-based surveillance systems.

VII. REFERENCES

[1]. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

DOI:

<https://doi.org/10.1016/j.comnet.2010.05.010>

[2]. D. Evans, "The Internet of Things: How the next evolution of the Internet is changing everything," *Cisco Internet Business Solutions Group*, 2011.

DOI:

<https://doi.org/10.1109/INFCOM.2011.5934998>

[3]. M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," *International Conference on Privacy and Security in Mobile Systems*, 2014.

DOI:

<https://doi.org/10.1109/PRISMS.2014.6970594>

[4]. S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A literature review," *Journal of Computer and Communications*, vol. 3, no. 5, pp. 164–173, 2015.

DOI:

<https://doi.org/10.4236/jcc.2015.35021>

[5]. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32,

2014.
DOI:
<https://doi.org/10.1109/JIOT.2014.2306328>
- [6]. P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, protocols, and applications," *Journal of Electrical and Computer Engineering*, vol. 2017, pp. 1–25, 2017.
DOI: <https://doi.org/10.1155/2017/9324035>
- [7]. J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.
DOI:
<https://doi.org/10.1109/COMST.2015.2388550>
- [8]. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.
DOI:
<https://doi.org/10.1109/COMST.2015.2444095>
- [9]. H. Ning and H. Liu, "Cyber-physical-social based security architecture for future Internet of Things," *Advances in Internet of Things*, vol. 2, no. 1, pp. 1–7, 2012.
DOI: <https://doi.org/10.4236/ait.2012.21001>
- [10]. R. Want, B. Schilit, and S. Jenson, "Enabling the Internet of Things," *Computer*, vol. 48, no. 1, pp. 28–35, 2015.
DOI: <https://doi.org/10.1109/MC.2015.12>
- [11]. M. Weyrich and C. Ebert, "Reference architectures for the Internet of Things," *IEEE Software*, vol. 33, no. 1, pp. 112–116, 2016.
DOI: <https://doi.org/10.1109/MS.2016.20>
- [12]. S. Li, L. Da Xu, and S. Zhao, "The Internet of Things: A survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.
DOI: <https://doi.org/10.1007/s10796-014-9492-7>
- [13]. K. Rose, S. Eldridge, and L. Chapin, "The Internet of Things: An overview," *Internet Society*, 2015.
DOI:
<https://doi.org/10.1109/INTERNET.2015.7116334>
- [14]. T. Winter et al., "RPL: IPv6 routing protocol for low-power and lossy networks," *IETF RFC 6550*, 2012.
DOI: <https://doi.org/10.17487/RFC6550>
- [15]. Mahesh Ganji. (2025). Enhancing Oracle Cloud HR Reporting Through AI-Driven Automation. *Journal of Science & Technology*, 10(6), 28–36.
<https://doi.org/10.46243/jst.2025.v10.i06.pp28-36>
- [16]. Todupunuri, A. (2023). The Role of Artificial Intelligence in Enhancing Cybersecurity Measures in Online Banking Using AI. *International Journal of Enhanced Research in Management & Computer Applications*, 12(01), 103–108.
<https://doi.org/10.55948/ijermca.2023.01015>
- [17]. The Future of Conversational AI in Banking: A Case Study on Virtual Assistants and Chatbots*: Exploring the

- Impact of AI Powered Virtual Assistants on Customer Service Efficiency and Satisfaction. (2024). International Research Journal of Economics and Management Studies, 3(10). <https://doi.org/10.56472/25835238/irjems-v3i10p124>
- [18]. Todupunuri, A. (2025). Utilizing Angular for the Implementation of Advanced Banking Features. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.5283395>
- [19]. Sushma Babburi. (2025). Token-Based Data Accounting System For Transparent Model Training And Cost Allocation. American Journal of AI Cyber Computing Management, 5(4), 463–474. <https://doi.org/10.64751/ajaccm.2025.v5.n4.pp463-474>
- [20]. Snigdha Gaddam. (2025). SOFTWARE STACK PREPARED FOR AI TRANSITIONING FROM MODULES TO MODELS. American Journal of AI Cyber Computing Management, 5(4), 451–462. <https://doi.org/10.64751/ajaccm.2025.v5.n4.pp451-462>
- [21]. Gaddam, S. INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING.
- [22]. Bajarang Bhagwat, V. (2023). Optimizing Payroll to General Ledger Reconciliation: Identifying Discrepancies and Enhancing Financial Accuracy. JOURNAL OF ADVANCE AND FUTURE RESEARCH, 1(4). <https://doi.org/10.56975/jaafr.v1i4.501636>
- [23]. Suhasnadh Reddy Veluru, Sai Teja Erukude, and Viswa Chaitanya Marella. 2025. Multimodal Detection of Fake Reviews using BERT and ResNet-50. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). IEEE, 877–882.
- [24]. Doragacharla, V. R. (2026). AI-Enabled Commerce Platforms in Cloud Computing Environments: An Architectural and Socio-Economic Analysis. Journal of Computational Analysis & Applications, 35(1).
- [25]. Jay Bharat Mehta. (2025). AUTONOMOUS PATCH VALIDATION FOR ZERO-DAY EXPLOITS IN ENTERPRISE CLOUDS. International Journal of Applied Mathematics, 38(4s), 1270–1285. <https://doi.org/10.12732/ijam.v38i4s.685>
- [26]. Reddy, S. K. (2025). Hyperpersonalization driven by AI is expected to be at the Lead in shaping the future of loyalty rewards. Journal of Emerging Technologies and Innovative Research.
- [27]. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
- [28]. Poojari, R. (2026). Privacy-Preserving Generative AI in Healthcare Systems Using Federated Learning Approaches. International Journal of Data Science and IoT Management System, 5(1), 78-88.
- [29]. Kalae, U. K. (2021). Enhancing data analytics and reporting efficiency using

Power BI and SQL in cloud computing environments. Journal of Computational Analysis and Applications, 29(6), 2021. <https://doi.org/10.48047/jocaaa.2021.29.06>.

48

[30]. Kalae, U. K. (2025). Optimizing cost-effective cloud data pipeline orchestration across multiple cloud providers. Journal of Information Systems Engineering and Management, 10(63s), e726–e741.

[31]. Saikumar, B. (2023). Enhancing Client Engagement through AI-Driven Real-Time Reporting and Automated Alerts. International Journal of Enhanced Research in Science, Technology & Engineering, 12(11), 111–117. <https://doi.org/10.55948/ijerste.2023.1115>

[32]. Saikumar, B. (2024). Optimizing Crew Scheduling and Absence Management using Microservices: Enhancing Reliability and Efficiency in Crew Management Systems. International Journal of Enhanced Research in Management & Computer Applications, 13(11), 50–55. <https://doi.org/10.55948/ijermca.2024.0116>

[33]. O. Vermesan and P. Friess, *Internet of Things – From Research and Innovation to Market Deployment*. River Publishers, 2014.

DOI: <https://doi.org/10.1007/978-3-319-05029-4>