International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 03(March),2026
Received: 10-02-2026 Accepted: 17-03-2026 Published: 23-03-2026

Multimodal Anti-Theft Alarm System using a Floor Mat Sensor and Laser Beam Sensor

Annareddy Sravani,
Dept. of Electronics and
Communication Engineering,
Annamacharya Institute of Technology
and Sciences, Kadapa, India.
annareddysravani51@gmail.com

Syed Saleem,
Dept. of Electronics and
Communication Engineering,
Annamacharya Institute of Technology
and Sciences, Kadapa, India.
saleema7253362@gmail.com

K. Sai Sowmya,
Dept. of Electronics and
Communication Engineering,
Annamacharya Institute of Technology
and Sciences, Kadapa, India.
kanadamsaisowmya@gmail.com

K. Durga Harikeswari,
Dept. of Electronics and
Communication Engineering,
Annamacharya Institute of Technology
and Sciences, Kadapa, India.
harikeswari312@gmail.com

M. Lokesh,
Dept. of Electronics and
Communication Engineering,
Annamacharya Institute of Technology
and Sciences, Kadapa, India.
madinenilokesh8@gmail.com

K. Manohar,
Dept. of Electronics and
Communication Engineering,
Annamacharya Institute of Technology
and Sciences, Kadapa, India.
mk7078713@gmail.com

Abstract*—Industrial settings need robust security against theft and illegal access since they contain priceless machinery, private information, and ongoing manufacturing processes. Conventional security techniques including camera-based surveillance systems, single-sensor alarms, and human monitoring frequently have high computing demands, many false alarms, slow reaction times, and reliance on steady internet access. A multimodal anti-theft alarm system is suggested as a solution to these problems. To increase detection reliability, the system combines three sensing techniques. A laser-LDR pair monitors beam disruption to detect unwanted entry, and an infrared sensor detects motion within the secured area. A force sensor also senses pressure or physical contact with surfaces or equipment that is restricted. The system increases intrusion detection accuracy and decreases false alarms by integrating many sensor methods. As the central processing unit, an ESP32 microcontroller continuously gathers sensor data and manages system activities in real time. Real-time status updates are provided by an I2C LCD display, and when suspicious behavior is identified, a buzzer immediately sounds a warning. Authorized users receive immediate notifications from a GSM module for remote monitoring. In order to guarantee continuous functioning in the event of a power outage, the system additionally incorporates a controlled power supply with battery backup. Improved detection accuracy and quicker reaction times are shown by experimental results.

Keywords*—Multi-Model Anti-Theft System, Industrial Internet of Things, ESP32 Microcontroller, Sensor Fusion, Laser-LDR Intrusion Detection, Force Sensor, Infrared Motion, GSM Alert System, Industry 4.0 Security, Embedded Surveillance System.

I. INTRODUCTION

Protecting sensitive data, restricted areas, and valuable equipment has become essential in modern industrial environments. Facilities such as factories, warehouses, and laboratories rely heavily on cost machinery and continuous production processes, which makes them susceptible to theft, unauthorized access, and disruptions in workflow [1]. With the increasing integration of interconnected digital technologies, security concerns now extend beyond physical protection to also include cyber-physical systems and networked infrastructures [2]. As a result, the demand for smart monitoring systems with real-time detection and quick reaction capabilities is rising [3]. Conventional security techniques, such as separate alarm systems, manual surveillance, and simple SCADA-based monitoring, frequently have a number of disadvantages, including slow response times, poor detection accuracy, and a high frequency of false alarms [4-6]. By combining cyber-physical components, automation, and networked sensors, Industry 4.0 technologies are turning industrial settings into intelligent systems to solve these problems [7-8]. Through powerful sensing devices and industrial communication networks, these technologies enable effective communication across huge facilities, dispersed monitoring, and real-time data collecting [9-11]. Additionally, by identifying abnormal situations early and facilitating prompt preventive actions, analytical and data-driven control systems enhance safety [12-13]. Multi-model sensing techniques have received a lot of attention lately in contemporary security systems. Several sensors cooperate in these systems to reduce false alarms and confirm intruder incidents [14]. For instance, laser beam sensors use beam disruption to detect unauthorized access, while pressure- sensitive flooring uses weight changes to detect human presence [15-16]. When compared to single-sensor systems, detection accuracy is greatly increased by combining various sensing techniques [17]. These systems enable automatic monitoring, intelligent response mechanisms, and real-time warning creation when paired with embedded controllers and Industrial Internet of Things platforms, supporting safe and effective Industry 4.0 infrastructures [18-20].

II. RELATED WORK

The use of Wireless Sensor Networks to monitor restricted areas within industrial facilities has been the subject of recent advancements in industrial security. Through the deployment of numerous interconnected sensor nodes, WSNs enables continuous sensing and monitoring across wide areas. However, systems that mainly depend on individual sensors may experience lower detection accuracy due to environmental disturbances and the absence of multi-sensor verification mechanism [21]. Internet of Things-based security solutions further improve monitoring by enabling

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 03(March),2026
Received: 10-02-2026 Accepted: 17-03-2026 Published: 23-03-2026

real-time alerts and remote access through cloud connectivity. Although these systems provide greater accessibility and flexibility, their effectiveness in demanding industrial environments can be affected by data transmission errors, communication delays, and reliance on stable network connectivity [22-23]. Vision-based monitoring systems that use camera surveillance and video analytics enhance situational awareness and allow detailed visual inspection of industrial spaces. However, these systems usually require significant processing power and can be influenced by external factors such as varying lighting conditions, physical obstructions, and changing industrial environments [24]. Alternatively, motion-based and pressure-based sensing techniques provide cost-effective and privacy-friendly security monitoring solutions. Nevertheless, systems that rely on a single sensor often led to inaccurate detections and frequent false alarms [25-26]. To overcome these limitations, sensor fusion approaches combine overcome these limitations, sensor fusion approaches combine multiple sensing technologies to improve detection accuracy and reduce errors, resulting in more reliable system performance [27-28]. Despite these advancements, many existing security systems remain complex and still lack strong physical-layer verification techniques for intrusion detection [29]. To address this issue, the proposed multi-modal anti-theft system integrates laser beam interruption detection with floor-mat pressure sensing, enabling accurate real-time monitoring while minimizing false alarms in confined industrial environments [30].

III. EXISTING SYSTEM

A Raspberry Pi functions as the main controller in the existing IoT-based theft detection system, as illustrated in Fig. 1. A piezoelectric sensor is used to detect pressure variations caused by physical contact, while a PIR sensor is responsible for identifying motion. The signals received from these sensors are processed by the Raspberry Pi, which uses Python and OpenCV to capture images and perform face identification. Whenever unusual activity is detected, the system automatically captures images and transmits them to the authorized user through a Wi-Fi connection. At the same time, a buzzer is triggered to generate a local audio alert, enabling both automated monitoring and remote notification. Despite these benefits, the system has several limitations. Environmental disturbances can cause unnecessary sensor activation, which may result in false alarms and reduced detection reliability. In addition, camera-based verification becomes less effective in low-lighting conditions or when the camera's field of view is partially obstructed. Continuous image processing also increases the computational workload, making the system relies heavily on stable internet connectivity, which limits its functionality during network outages and reduces its overall reliability in critical security applications [31].

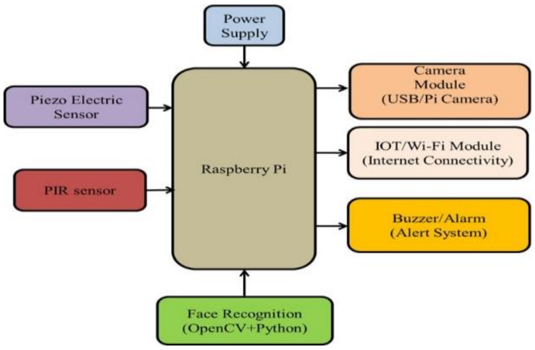
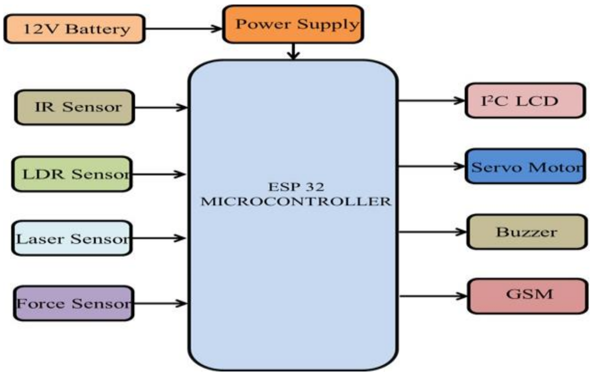

Power Supply
Piezo Electric Sensor
PIR sensor
Raspberry Pi
Camera Module (USB/Pi Camera)
IOT/Wi-Fi Module (Internet Connectivity)
Buzzer/Alarm (Alert System)
Face Recognition (OpenCV+Python)

Fig. 1. Block Diagram of Existing IoT-based Theft Detection System [31]

IV. PROPOSED SYSTEM

The proposed anti-theft system enhances intrusion detection by integrating multiple sensors, including an infrared motion sensor, a laser-LDR pair, and a floor pressure mat. Working together, these sensors detect unauthorized access by identifying motion, pressure variations, and interruptions in the laser beam. The signals produced by these sensors are continuously observed by an ESP32 microcontroller, which processes the data to minimize false alarms. As illustrated in Fig. 2, all components receive power from a regulated power supply supported by a 12V battery. Acting as the central controller, the ESP32 collects and analyzes input from each sensor to monitor system activity. When an intrusion is detected, the device immediately activates a buzzer alert and triggers a servo motor to automatically lock. For local monitoring, the system status is simultaneously shown on an I2C LCD.



Furthermore, a GSM module enables real-time monitoring and prompt response to possible security concerns by sending alert messages to authorized users.

Fig. 2. Block Diagram of the Proposed Multi-Model Anti-Theft System

A. *Methodology / Principle of Operation*

The system operates by continuously monitoring the environment and responding quickly to potential intrusions. The infrared sensor monitors motion, the force sensor identifies pressure caused by footsteps, and the laser-LDR pair detects intrusion when the laser beam is interruption. The ESP32 analyzes the signals received from these sensors and activates the buzzer alarm when an intrusion is detected. In addition, it updates the system status on the LCD display to provide immediate notification, controls the servo motor to lock the system, and utilizes the GSM module to place a phone alert to the authorized user.

B. *Hardware Implementation and Alert Mechanism*

The ESP32 functions as the central controller in this Internet of Things system, handling sensing, communication, display, and control operations. The infrared sensor identifies motion within the area, while the laser-LCD pair monitors any interruption of the beam at

Received: 10-02-2026 Accepted: 17-03-2026 Published: 23-03-2026

entry points. The floor mat sensor detects pressure when someone steps on it. The I2C LCD displays the current status of the system, and the buzzer triggers an alarm whenever an intruder is detected. At the same time, the servo motor locks the door to prevent unauthorized access. In addition, the GSM module sends call alerts to authorized users, enabling continuous monitoring and a quick response to potential threats.

C. Power Supply and System Requirements

All system components are powered by a controller 12V DC Power source, and uninterrupted functioning during power outages is guaranteed by a rechargeable battery backup. The system reduces false alarms and improves detection accuracy by integrating several sensors. The LCD shows the current state of the system, the servo motor initiates automatic locking, the GSM module notifies users of the incursion. Additionally, the ESP32-based architecture makes it simple to integrate IoT applications, enabling more advanced and intelligent security monitoring.

V. Result and Description

The hardware implementations of the suggested multi-model anti-theft system is shown in Fig. 3. As the primary controller, the ESP32 is linked to an infrared sensor for intrusion detection, a force sensor, and a laser-LDR module. The system status is continuously shown in real time on an I2C LCD. The buzzer sounds an alarm, the GSM module notifies the user, and the servo motor initiates automatic locking when an intrusion is detected. The feasible design and real-time operation of the suggested security system are demonstrated by this prototype.

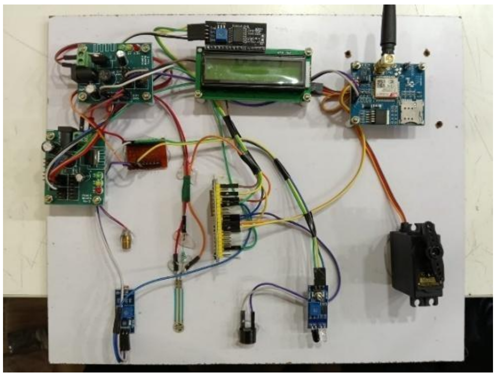


Fig. 3. Hardware Prototype of the Proposed Anti-Theft System

When the system detects an intrusion, the user's mobile phone receives an emergency alert, as shown in Fig. 4. In order to notify the user of the identified a safety incident and enable prompt action, the GSM module automatically sends a warning message to the registered number.

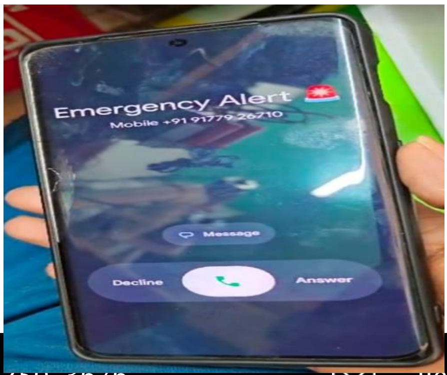
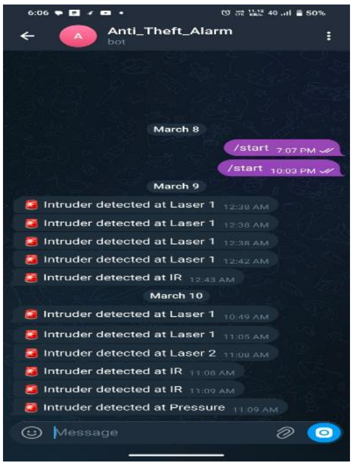


Fig. 4. GSM Emergency Alert Notification

The intrusion alert messages obtained via a Telegram bot are displayed in Fig. 5. The system enables remote monitoring and prompt knowledge of possible incidents of security by sending a real-time message via Telegram to the user when sensors like the laser, infrared, or pressure sensor detect unauthorized activity.



6:06 50%

Anti_Theft_Alarm
bot

March 8

/start 7:07 PM

/start 10:03 PM

March 9

🚨 Intruder detected at Laser 1 12:38 AM

🚨 Intruder detected at Laser 1 12:38 AM

🚨 Intruder detected at Laser 1 12:38 AM

🚨 Intruder detected at Laser 1 12:42 AM

🚨 Intruder detected at IR 12:43 AM

March 10

🚨 Intruder detected at Laser 1 10:49 AM

🚨 Intruder detected at Laser 1 11:05 AM

🚨 Intruder detected at Laser 2 11:08 AM

🚨 Intruder detected at IR 11:08 AM

🚨 Intruder detected at IR 11:09 AM

🚨 Intruder detected at Pressure 11:09 AM

Fig. 5. Telegram Bot Intrusion Alert

The system is shown in Fig. 6 when it is operating normally and no intrusions are found. The LCD shows the sensor readings and the message SAFE MODE while the system remains in a secure standby mode. Real-time monitoring is made possible via the I2C interface, which permits constant connection between the microcontroller and the display.

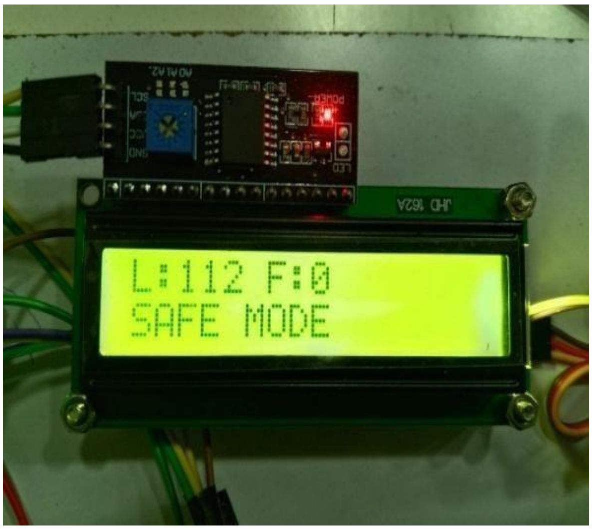


Fig. 6. LCD Display Showing SAFE MODE During Normal Monitoring

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 03(March),2026
Received: 10-02-2026 Accepted: 17-03-2026 Published: 23-03-2026

Fig. 7 shows how the system behaves during an intrusion event. When unauthorized activity is detected, the LCD displays a high sensor reading along with the message THEFT ALERT. After the signal is processed, the microcontroller immediately activates the servo motor to lock the system, triggers the buzzer alarm, and the buzzer alarm, and sends an alert message through the GSM module.

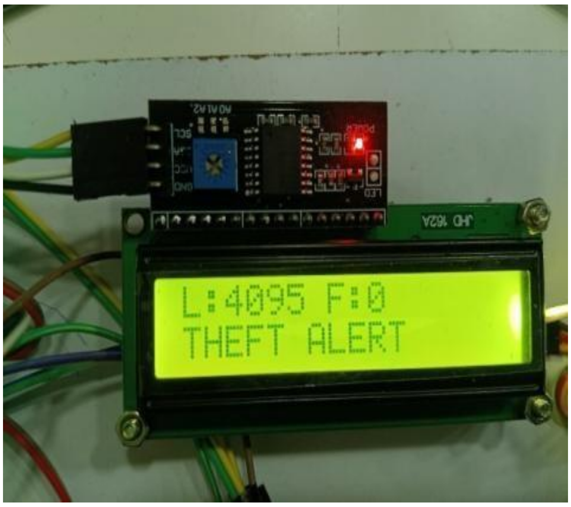


Fig. 7. LCD Display Indicating THEFT ALERT During Intrusion Detection

TABLE I. Comparison Between Existing Systems and the Proposed Anti-Theft System

Parameter	Existing Systems	Proposed System
Controller	Basic controllers with limited processing	ESP32 with real-time multi-sensor processing
Footstep Detection	PIR/switch-based, less reliable	Force sensor for accurate pressure detection
Entry Monitoring	Magnetic or single-beam sensors	Laser–LDR for precise intrusion detection
Motion Detection	Standalone PIR with higher false alarms	IR sensor with multi-sensor validation
Detection Accuracy	Single-sensor, less reliable	Multi-sensor fusion for improved accuracy
Alert System	Local alarm only	Buzzer with GSM-based remote notification
Response Action	No automatic action	Servo-based automated locking mechanism
User Interface	No real-time display	I2C LCD with live system status
Power Supply	No backup during power failure	Battery-backed reliable power supply
Control Method	Manual operation	Simple switch-based system control

TABLE I compares the proposed anti-theft solution with traditional security techniques. The proposed system is better suited for modern security applications because it improves detection accuracy through multi-sensor integration, delivers real-time alerts using GSM communication, enables automatic responses through a servo-based locking mechanism, and ensures reliable operation with battery backup support.

TABLE II presents the experimental evaluation of the proposed anti-theft system under various test conditions. In normal monitoring mode, the system continuously observes the sensor inputs and quickly identifies intrusions whenever any sensor is activated. When an intruder is detected, the LCD displays the message THEFT ALERT, the servo motor activates the locking mechanism, the buzzer alarm is triggered, and a warning notification is sent to the user. The integration of multiple sensors improves intrusion detection accuracy while ensuring reliable real-time performance of the system.

TABLE II. Experimental Results of the Proposed Anti-Theft System

Parameter	Normal Monitoring	Footstep Detected	Beam Interrupted	Motion Detected	Multi-Sensor Trigger
Sensor Activated	None	Force Sensor	Laser + LDR	IR Sensor	All Sensors
LCD Status	Safe Mode	Theft Alert	Theft Alert	Theft Alert	Theft Alert
Buzzer	OFF	ON	ON	ON	ON
SMS Alert	No	Sent	Sent	Sent	Sent
Servo Action	Idle	Lock Action	Lock Action	Lock Action	Lock Action
Result	System operates normally	Intrusion detected	Un-authorized entry detected	Movement detected	High-accuracy detection

TABLE III. Comparison of Different Intrusion Detection Approaches

Parameter	[21]	[24]	[31]	Proposed System
Sensors	Wireless	Camera-Motion	PIR-Pressure	Force-Laser-IR
Detection	General	Vision	Motion	Multi-Layer
Boundary	No	Limited	No	Yes
False Alarms	High	Medium	Medium	Low
Processing	Moderate	Very High	High	Low
Reliability	Medium	Medium	Medium	High

A comparison of several intrusion detection strategies based on sensor type, detection capability, and overall system performance is presented in TABLE III. Wireless sensing techniques offer wide-area monitoring but often lack accurate intrusion confirmation, while camera-based solutions depend heavily on lighting conditions and require considerable processing power. PIR and pressure sensors can detect motion-related events but have limitations when it comes to identifying perimeter breaches. In contrast, the proposed system integrates force sensors, laser-LDR boundary monitoring, and infrared motion detection within a multi-stage validation process. This combined approach effectively reduces false alarms, enhances reliability for real-time security applications, and simplifies processing complexity.

VI. Conclusion

A multimodal anti-theft alarm system has been developed using force sensing, laser-LDR detection, and infrared motion monitoring to improve detection accuracy and reduce the false alarms commonly observed in single-sensor systems. Every time an incursion is detected, the ESP32 microcontroller interprets the sensor

Received: 10-02-2026 Accepted: 17-03-2026 Published: 23-03-2026

data in real time and initiates security measures like buzzer alerts, GSM messages, and servo-based lockdown. According on experimental evaluation, the system offers trustworthy battery backup during power outages, quick response times, steady operation, and dependable performance. Particularly in industrial and resource-constrained settings, the suggested method is scalable, affordable, and ideal for Industry 4.0 security applications.

REFERENCES

[1] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

[2] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," Computers in Industry, vol. 101, pp. 1–12, 2018.

[3] M. Valera and S. A. Velastin, "Intelligent distributed surveillance systems: A review," IEE Proceedings – Vision, Image and Signal Processing, vol. 152, no. 2, pp. 192–204, 2005.

[4] A. Khanna and S. Kaur, "Evolution of Internet of Things applications in industrial automation," International Journal of Advanced Networking and Applications, vol. 10, no. 1, pp. 3752–3759, 2019.

[5] D. Bailey and E. Wright, Practical SCADA for Industry. Oxford, U.K.: Elsevier, 2003.

[6] J. Fraden, Handbook of Modern Sensors: Physics, Designs, and Applications, 5th ed. New York, NY, USA: Springer, 2016.

[7] K. Schwab, The Fourth Industrial Revolution. New York, NY, USA: Crown Business, 2017.

[8] S. Monk, Practical Electronics for Inventors, 4th ed. New York, NY, USA: McGraw-Hill, 2016.

[9] R. Zurawski, Industrial Communication Technology Handbook, 2nd ed. Boca Raton, FL, USA: CRC Press, 2015.

[10] P. Zhang, Industrial Control Technology: A Handbook for Engineers and Researchers. Oxford, U.K.: William Andrew Publishing, 2010.

[11] A. Willig, "Recent and emerging topics in wireless industrial communications: A selection," IEEE Transactions on Industrial Informatics, vol. 4, no. 2, pp. 102–124, 2008.

[12] S. Yin, O. Kaynak, and H. Gao, "Data-driven monitoring, fault diagnosis and control for industrial systems," IEEE Transactions on Industrial Electronics, vol. 61, no. 11, pp. 6413–6423, 2014.

[13] B. Galloway and G. P. Hancke, "Introduction to industrial control networks," IEEE Communications Surveys & Tutorials, vol. 15, no. 2,
pp. 860–880, 2013.

[14] T. Wang, G. Zhang, A. Liu, M. Z. A. Bhuiyan, and Q. Jin, "A secure IoT-based intelligent security system," IEEE Sensors Journal, vol. 18, no. 11, pp. 1–10, 2018.

[15] J. Wilson, Sensor Technology Handbook. Burlington, MA, USA: Newnes, 2005.

[16] H. K. Khalil, Nonlinear Systems and Embedded Control Applications. Prentice Hall, 2002.

[17] A. Mahmood, E. Sisinni, L. Guntupalli, R. Rondon, S. A. Hassan, and
M. Gidlund, "Industrial IoT security: Challenges, solutions, and future directions," Journal of Network and Computer Applications, vol. 149, 2019.

[18] J. Lee, B. Bagheri, and H. A. Kao, "A cyber-physical systems architecture for Industry 4.0-based manufacturing systems," Manufacturing Letters, vol. 3, pp. 18–23, 2015.

[19] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context-aware computing for the Internet of Things: A survey," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 414– 454, 2014.

[20] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," Journal of Industrial Information Integration, vol. 6,
pp. 1–10, 2017.

[21] I. F. Akyildiz et al., "Wireless sensor networks: A survey," Computer Networks, vol. 38, no. 4, pp. 393–422, 2002.

[22] D. Bandyopadhyay and J. Sen, "Internet of Things: Applications and challenges," Wireless Personal Communications, vol. 58, no. 1, pp. 49–69, 2011.

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

[24] A. Hampapur et al., "Smart video surveillance: Exploring the concept of multiscale spatiotemporal tracking," IEEE Signal Processing Magazine, vol. 22, no. 2, pp. 38–51, 2005.

[25] N. Hasan et al., "Human activity recognition using pressure sensors: A review," Sensors, vol. 19, no. 3, 2019.

[26] S. Mukhopadhyay, "Wearable sensors for human activity monitoring," IEEE Sensors Journal, vol. 15, no. 3, pp. 1321–1330, 2015.

[27] H. Luo, Y. Zhao, and M. Ye, "Sensor fusion for smart security systems," Information Fusion, vol. 21, pp. 1–12, 2015.

[28] M. Li and Y. Liu, "Underground structure monitoring with wireless sensor networks," ACM Transactions on Sensor Networks, vol. 5, no. 2, 2009.

[29] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, no. 12, pp. 2292–2330, 2008.

[30] R. Want, B. N. Schilit, and S. Jenson, "Enabling the Internet of Things," Computer, vol. 48, no. 1, pp. 28–35, 2015.

[31] A. Mishra, M. Alekhya, and E. Tamrakar, "Theft Detection System," International Journal of Engineering Research and Development, vol. 21, no. 5, pp. 44–50, May 2025.