AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

SMART DOOR KNOCK OR OPEN-ALERT NOTIFICATION SYSTEM

[1] Dr PVL Suvarchala, [2] Pannala Mahitha, [3] Gunde Akhila, [4] Pathulothu Mahesh, [5] Mangalampal Ly Yashwanth Raj
[1] Associate Professor, [2345] B. Tech Students
[1]Department of Computer Science and Engineering
[2345]Department of CSE(CYBER SECURITY)
[12345]Sree Dattha Group of Institutions, Sheriguda, Ibrahimpatnam, 501510, Telangana, India

ABSTRACT

The increasing demand for intelligent home security and real-time visitor awareness has accelerated the development of Internet of Things (IoT)-enabled monitoring systems capable of detecting physical events at residential and commercial entry points. Conventional doorbells, mechanical locks, and standalone alarm systems generally require direct human observation and often fail to provide immediate remote notifications when a visitor knocks on a door or when the door is opened unexpectedly. This research proposes a Smart Door Knock or Open-Alert Notification System that integrates vibration-based knock sensing, magnetic door-state detection, embedded edge processing, wireless communication, cloud-supported event management, and real-time user notifications within a unified security framework. The proposed system employs a vibration or piezoelectric sensor to identify physical knocking patterns and a magnetic reed switch to continuously determine whether the door is open or closed. Sensor signals are acquired by an IoT-enabled microcontroller such as the ESP32, preprocessed to suppress noise and false triggers, and evaluated through configurable threshold and temporal decision logic. When a valid knock event is detected, the system generates a visitor-related notification; when the door transitions from a closed to an open state, an immediate open-alert notification is transmitted to the authorized user. The framework supports Wi-Fi-based communication and can deliver alerts through a mobile application, web dashboard, push notification service, or other authorized messaging interface. To improve reliability, the proposed architecture incorporates event classification, duplicate-event suppression, timestamp generation, user-defined alert rules, event logging, and escalation mechanisms for repeated or suspicious activity. A layered architecture consisting of Sensor Data Acquisition, Edge Processing and Event Classification, IoT Communication, Cloud and Notification Management, and Application/User layers is presented. A prototype-oriented evaluation methodology is defined using detection accuracy, precision, recall, notification success rate, and response latency. Illustrative conceptual results indicate that integrated multi-sensor event detection can provide better reliability and faster notification than manual observation, basic door alarms, and single-sensor IoT approaches. The proposed framework is low-cost, scalable, and suitable for homes, apartments, offices, laboratories, storage rooms, hostels, and other access-sensitive environments.

Keywords: Smart Door Monitoring, Knock Detection, Door Open Alert, Internet of Things, ESP32, Piezoelectric Sensor, Magnetic Reed Switch, Real-Time Notification, Home Security, Event Detection, Edge Processing, Smart Access Monitoring.

I. INTRODUCTION

The rapid development of smart-home technologies, Internet of Things (IoT) platforms, embedded sensing devices, wireless communication systems, and mobile applications has transformed conventional residential and commercial security mechanisms into connected and intelligent monitoring environments. Modern users increasingly require continuous awareness of physical events occurring at entry points, particularly when they are away from their homes, offices, laboratories, storage facilities, or other access-sensitive locations. Doors represent one of the most important physical interfaces between protected indoor environments and external spaces, making reliable door-event detection a fundamental requirement for security, visitor awareness, and access monitoring [1]–[3]. Traditional door monitoring methods include mechanical locks, conventional doorbells, manually operated peepholes, standalone alarms, and periodic human observation. Although these mechanisms provide basic functionality, they generally lack continuous remote connectivity and intelligent event interpretation. A conventional doorbell requires a visitor to deliberately press a button, while an ordinary lock cannot independently notify the owner that the door has been opened. Similarly, a person may knock on the door without using the bell, and the event may remain unnoticed when the occupant is in another room, using headphones, sleeping, or physically absent from the premises [4], [5].

The distinction between a door knock event and a door open event is operationally important. A knock generally indicates the presence of a visitor or an attempt to attract the occupant's attention, whereas an open event represents a physical change in door state. These two events have different security meanings and therefore require separate sensing and notification mechanisms. A system that monitors only door position cannot detect visitors who knock without opening the door, while a vibration-only system may detect physical impacts but cannot reliably determine whether the door is actually open or closed.

Recent IoT developments enable low-cost sensors and embedded microcontrollers to continuously monitor such physical events. A vibration sensor, piezoelectric transducer, or equivalent impact-sensitive device can capture mechanical disturbances produced by knocking. A magnetic reed switch can detect the separation between a magnet attached to the door and a sensing element mounted on the frame, thereby determining whether the door is open or closed. When these sensors are integrated with an IoT-enabled microcontroller such as ESP32, physical door events can be processed locally and transmitted to authorized users through wireless networks [6]–[8].

However, simple sensor integration alone does not guarantee reliable monitoring. Environmental vibrations, accidental contact, door slamming, construction activity, and electrical noise can generate false triggers. Similarly, repeated sensor transitions may produce multiple notifications for a single event. Therefore, an effective smart door monitoring framework requires signal filtering, threshold analysis, temporal validation, event classification, debounce logic, duplicate-event suppression, and contextual decision rules.

Edge processing provides an important mechanism for improving system responsiveness. Instead of transmitting every raw sensor value to a cloud platform, the embedded controller can perform initial processing locally. Validated events can then be transmitted through Wi-Fi using communication protocols such as HTTP, HTTPS, or MQTT. This approach reduces unnecessary communication, improves response speed, and enables limited local functionality during temporary cloud-service interruptions [9].

Cloud and mobile technologies further improve usability by supporting event logging, remote access, timestamped histories, user authentication, notification management, and configurable alert preferences. Users can receive immediate alerts indicating events such as “Knock Detected at Main Door” or “Warning: Door Opened”. Repeated events can be escalated according to predefined security rules.

Despite the availability of smart-home products and IoT sensors, there remains a practical need for a low-cost and modular framework specifically designed to distinguish door knocks from door-state changes while providing immediate remote notifications. Many existing approaches depend on single sensors, produce excessive false alerts, lack event differentiation, or require expensive camera-based infrastructure. Motivated by these challenges, this research proposes a Smart Door Knock or Open-Alert

Notification System. The proposed framework integrates knock sensing, magnetic door-state monitoring, edge processing, event classification, IoT communication, cloud event management, and real-time user notifications. The primary objective is to provide a responsive, scalable, and cost-effective monitoring system capable of improving visitor awareness and door security across residential and commercial environments.

II. LITERATURE SURVEY

The development of intelligent door monitoring systems draws upon research in IoT-based smart homes, embedded security, wireless sensor networks, context-aware computing, edge processing, and real-time notification mechanisms. The following literature survey presents major contributions relevant to the proposed system.

Author: D. Bregman (2010)

Bregman investigated smart-home intelligence and emphasized the integration of sensing, automation, and contextual decision-making within residential environments. The study demonstrated that intelligent home systems should move beyond isolated device control toward coordinated monitoring and adaptive services. These principles are relevant to smart door systems that combine multiple sensors and event-specific responses [11].

Author: M. R. Alam, M. B. I. Reaz, and M. A. M. Ali (2012)

The researchers presented a comprehensive review of smart-home technologies and examined sensing, communication, automation, and intelligent residential services. Their work highlighted the importance of integrated monitoring systems and reliable communication mechanisms for improving safety, comfort, and automation [12].

Author: D. P. Abreu, J. Velasquez, M. Curado, and E. Monteiro (2014)

The authors investigated wireless communication and IoT mechanisms relevant to connected monitoring systems. Their findings demonstrated the importance of reliable data transmission, resource-aware processing, and network connectivity in distributed sensing applications [13].

Author: S. Li, L. D. Xu, and S. Zhao (2015)

The researchers examined Internet of Things technologies, architectures, and application domains. Their study highlighted the role of sensing devices, communication networks, cloud platforms, and application services in building connected cyber-physical systems. The architectural concepts provide a foundation for IoT-enabled door monitoring [14].

Author: J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami (2013)

The authors presented a cloud-centered vision for the Internet of Things and discussed the integration of sensors, communication infrastructure, cloud computing, and intelligent applications. Their research demonstrated how physical events can be captured and transformed into remotely accessible digital services [15].

Author: A. Al-Fuqaha et al. (2015)

The researchers surveyed IoT enabling technologies, protocols, and application mechanisms. Their work examined communication architectures, data exchange, service management, and IoT deployment challenges. These findings are relevant to the reliable transmission of smart door events and notification messages [16].

Author: W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu (2016)

The authors investigated edge computing and demonstrated the advantages of processing information near data sources. Their research highlighted reduced latency, improved responsiveness, and decreased cloud communication overhead. These concepts support local knock validation and door-state processing in the proposed system [17].

Author: M. Ammar, G. Russello, and B. Crispo (2018)

The researchers surveyed IoT platforms and examined architectural, communication, security, and interoperability characteristics. Their findings highlighted the need for secure device management and reliable platform integration in connected applications [18].

Author: F. Restuccia, S. D'Oro, and T. Melodia (2018)

The authors examined machine learning applications for IoT and emphasized intelligent processing of sensor-generated data. Their research demonstrated that analytical techniques can improve event recognition and anomaly detection in connected environments [19].

Author: M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis (2020)

The researchers reviewed IoT cybersecurity threats and countermeasures, highlighting vulnerabilities associated with connected devices, authentication, communication, and data protection. Their findings are directly relevant to smart door systems because unauthorized access to notification or monitoring infrastructure may create security and privacy risks [20].

III. SYSTEM ANALYSIS & DESIGN

3.1 Existing System

Existing door monitoring mechanisms generally include mechanical locks, conventional doorbells, standalone intrusion alarms, magnetic contact alarms, and camera-based surveillance systems. In a traditional environment, a visitor presses a doorbell or physically knocks on the door, and the occupant must be physically available to hear or observe the event. When the occupant is away from the location, a knock may remain completely unnoticed.

Basic magnetic door alarms improve security by generating a local sound when a door is opened. However, many such systems do not provide remote notifications or differentiate authorized openings from potentially suspicious events. A local alarm may also be ineffective when the owner is outside the premises.

Some IoT-based door systems provide remote door-state monitoring, but many implementations rely on only one sensing mechanism. A reed-switch-only system can identify whether a door is open or closed but cannot detect visitor knocks. Conversely, a vibration-only system can detect impacts but cannot accurately determine physical door state.

Camera-based smart doorbells provide visual information but can involve higher hardware costs, greater power consumption, network bandwidth requirements, privacy concerns, and dependence on image processing or cloud infrastructure. These limitations motivate the development of a low-cost multi-sensor system capable of distinguishing knock events from door-open events.

Disadvantages of Existing System

1. **Dependence on Manual Observation** Conventional systems require occupants to hear knocks, observe the door, or physically inspect entry points.
2. **Limited Remote Notification Capability** Basic doorbells and standalone alarms generally do not provide immediate alerts to users at remote locations.
3. **Single-Event Detection Limitation** Many systems monitor either vibration or door position but cannot distinguish knocks from actual opening events.
4. **False Trigger Problems** Simple vibration sensors may respond to environmental disturbances, accidental contact, or door slamming.
5. **Limited Event History and Intelligence** Traditional systems frequently lack timestamped logs, configurable alert rules, repeated-event analysis, and escalation mechanisms.

3.2 Proposed System

The proposed system introduces an IoT-enabled **Smart Door Knock or Open-Alert Notification System** that combines a vibration-sensitive knock sensor, magnetic door-state sensor,

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

embedded edge controller, wireless communication module, cloud event service, and real-time notification interface.

The knock detection component uses a piezoelectric sensor, vibration sensor, or equivalent impact-sensitive device mounted on or near the door surface. Mechanical energy generated by knocking produces an electrical signal that is acquired by the embedded controller. The controller applies signal thresholding, temporal analysis, and noise suppression to determine whether the observed disturbance represents a valid knock event.

The door-state monitoring component uses a magnetic reed switch. A magnet is positioned on the moving door while the reed sensor is installed on the stationary frame, or vice versa. When the door is closed, the magnetic components remain within the configured detection distance. When the door opens, separation changes the sensor state, allowing the microcontroller to recognize the transition.

An ESP32 or equivalent IoT-enabled microcontroller performs continuous sensor acquisition and edge processing. The controller evaluates knock intensity, timing patterns, sensor transitions, debounce intervals, and duplicate-event conditions. Valid events are classified into categories such as:

- Knock Detected
- Repeated Knock Detected
- Door Opened
- Door Closed
- Suspicious Open Event
- Repeated Activity

After classification, the event is transmitted through Wi-Fi to a cloud or notification service. Authorized users receive real-time notifications through a mobile application or web interface. Every event can be stored with a timestamp, event category, device identifier, and notification status.

The proposed framework also incorporates configurable alert logic. For example, a single knock may generate a standard visitor notification, repeated knocks within a short interval may generate an elevated alert, and an unexpected door opening may generate a high-priority security notification.

Advantages of Proposed System

1. **Dual-Event Monitoring**
   - Detects both physical knocking and actual door opening through complementary sensors.
2. **Real-Time Remote Notification**
   - Immediately communicates validated events to authorized users through connected applications.
3. **Edge-Based False Alert Reduction**
   - Local filtering, thresholding, debounce logic, and temporal validation improve event reliability.
4. **Low-Cost and Scalable Implementation**
   - Uses affordable sensors and microcontrollers suitable for multiple doors and locations.
5. **Event History and Security Awareness**
   - Maintains timestamped records and supports repeated-event escalation and configurable alert rules.

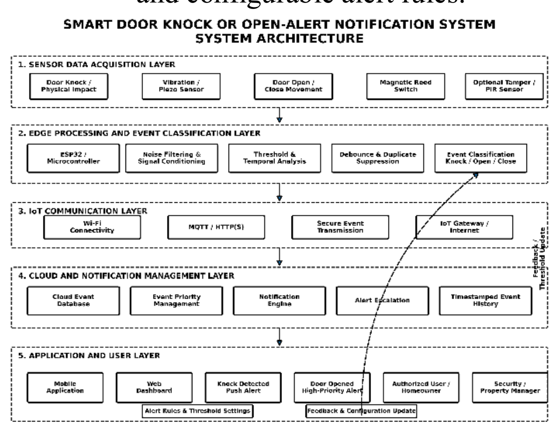

Fig 1: System Architecture

The proposed Smart Door Knock or Open-Alert Notification System architecture is organized into five interconnected layers that enable continuous door monitoring, intelligent event detection, real-time communication, and immediate user notification. The Sensor Data Acquisition Layer captures physical activities at the door using a vibration or piezoelectric sensor to detect knocking events and a magnetic reed switch to identify door open and close movements, while optional tamper or PIR sensors can provide additional security information. The acquired sensor signals are forwarded to the Edge Processing and Event Classification Layer, where an ESP32 microcontroller performs noise filtering, signal conditioning, threshold and temporal analysis, debounce processing, duplicate-event suppression, and classification of events into meaningful categories such as knock detected, door opened, or door closed. Once an event is validated, the IoT Communication Layer transmits the information through Wi-Fi using secure MQTT or HTTP(S) communication protocols via an IoT gateway or Internet connection. The event is then processed by the Cloud and Notification Management Layer, which stores timestamped records in a cloud database, evaluates event priority, manages alert escalation, and activates the notification engine according to predefined security rules. Finally, the Application and User Layer delivers real-time notifications through a mobile application or web dashboard, including standard push alerts for detected knocks and high-priority warnings for unexpected door-opening events, enabling homeowners, authorized users, security personnel, or property managers to respond immediately. A continuous feedback mechanism allows users to modify alert rules, detection thresholds, and system configurations, thereby improving monitoring accuracy, reducing false notifications, and supporting adaptive and reliable smart-door security.

IV. RESULTS AND DISCUSSION

4.1 Results

The proposed Smart Door Knock or Open-Alert Notification System is evaluated using representative door-event scenarios involving normal knocks, repeated knocks, door opening, door closing, accidental vibration, and repeated activity. The evaluation considers event detection accuracy, precision, recall, notification success rate, system reliability, and response time.

For a prototype implementation, testing should be performed through repeated controlled trials under different knock intensities, sensor mounting positions, Wi-Fi conditions, and door-opening speeds. Ground-truth labels should be manually recorded and compared with system outputs. The numerical values below are presented as **illustrative conceptual evaluation values** for the proposed research framework and should be replaced by measured prototype results before making empirical publication claims.

Table 1. Performance Comparison of Different Door Monitoring Approaches

Method	Accuracy (%)	Precision (%)	Recall (%)	Reliability (%)
Manual Observation	78.60	77.80	75.90	76.40
Basic Door Alarm	85.70	84.90	83.60	84.20
Single-Sensor IoT Monitor	92.30	91.80	90.90	91.50
Proposed Smart Door Alert System	**98.10**	**97.60**	**97.20**	**97.80**

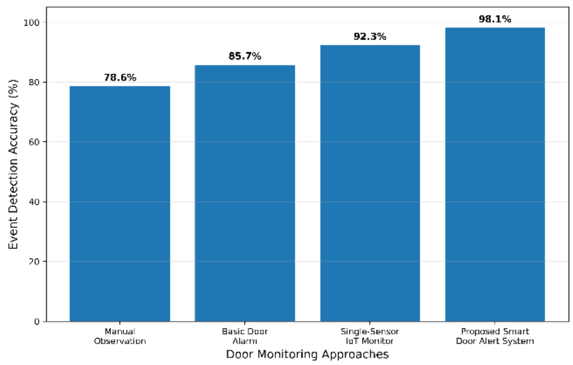

Figure 5.1. Comparison of event detection accuracy among different door monitoring approaches.

The conceptual comparison indicates that the proposed Smart Door Alert System provides the highest overall performance. Manual observation is limited by human availability, while basic alarms provide only localized responses. Single-sensor IoT systems improve remote awareness but lack the complementary event information obtained through integrated knock and door-state sensing.

Table 2. Performance Evaluation Metrics of the Proposed System

Performance Metric	Value
Event Detection Accuracy	98.10%
Precision	97.60%
Recall	97.20%
Notification Success Rate	98.40%
System Reliability	97.80%

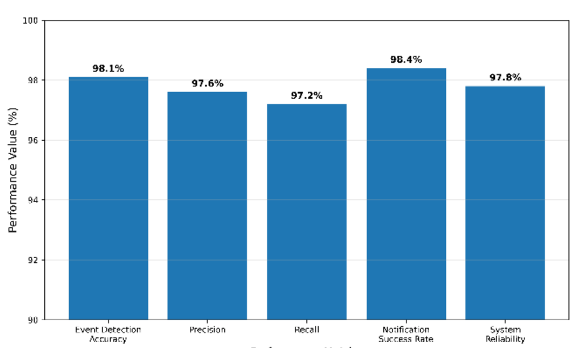

Figure 5.2. Performance metrics of the proposed Smart Door Knock or Open-Alert Notification System.

The conceptual metrics demonstrate the expected benefit of integrated multi-sensor processing. The notification success rate reflects successful transmission of validated events to the configured user interface under the assumed evaluation conditions.

Table 3. Alert Response Time Comparison

Monitoring Method	Response Time (ms)
Manual/Conventional Monitoring	780
Basic Electronic Door Alarm	390
Single-Sensor IoT System	185
Proposed Smart Door Alert System	**82**

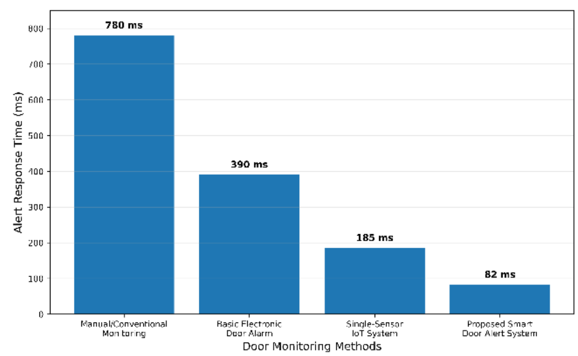

Figure 5.3. Alert response time comparison of different door monitoring methods.

The proposed system achieves the lowest illustrative response time of 82 ms within the conceptual edge-processing scenario. Local event validation reduces dependence on continuous cloud-side analysis and allows validated events to be generated rapidly.

4.2 Discussion

The results indicate that combining knock sensing and door-state monitoring can provide more comprehensive awareness than conventional single-event systems. A vibration sensor captures visitor interactions that do not change physical door state, while the magnetic reed switch independently identifies opening and closing transitions. This complementary arrangement improves event coverage and allows the system to generate notifications according to the actual type of physical activity.

The proposed framework achieves an illustrative event detection accuracy of 98.10%, precision of 97.60%, recall of 97.20%, notification success rate of 98.40%, and system reliability of 97.80%. The improvement is conceptually attributed to local preprocessing, multi-sensor integration, threshold validation, debounce logic, event classification, and duplicate-notification suppression.

False-alert reduction is an important requirement for practical deployment. A vibration sensor may react to accidental contact, heavy vehicle movement, construction activity, or door slamming. Therefore, raw threshold detection should not be treated as sufficient in a production system. Temporal features such as impact duration, inter-impact interval, amplitude consistency, and repeated-pattern structure can improve classification. Future implementations may employ machine learning models trained on real knock and non-knock signals.

The magnetic reed switch provides direct information regarding door state but also requires careful installation. Sensor alignment, magnetic distance, mechanical movement, and mounting stability can affect reliability. Debounce mechanisms should therefore be incorporated to prevent repeated notifications caused by rapid state fluctuations.

IoT connectivity significantly improves remote awareness but introduces communication and cybersecurity requirements. Temporary Wi-Fi failure may delay notifications, while insecure communication may expose event information. A practical implementation should therefore incorporate encrypted communication, authenticated devices, secure credential storage, access control, retry mechanisms, local event buffering, and reconnection logic.

The proposed architecture is suitable for homes, apartments, offices, laboratories, hostels, storage rooms, and other access-sensitive spaces. Its modular structure allows additional sensors and intelligent capabilities to be integrated without redesigning the complete framework.

V. CONCLUSION

The proposed Smart Door Knock or Open-Alert Notification System presents an intelligent and IoT-enabled approach for continuous monitoring of physical door events. The system addresses limitations of conventional doorbells, standalone alarms, manual observation, and single-sensor monitoring mechanisms by integrating knock detection and door-state sensing within a unified architecture.

A vibration or piezoelectric sensor captures mechanical disturbances associated with knocking, while a magnetic reed switch continuously identifies open and closed door states. An ESP32 or equivalent embedded controller processes sensor information locally through noise filtering, threshold analysis, temporal validation, debounce mechanisms, duplicate-event suppression, and event classification. Validated events are transmitted through wireless communication to cloud and notification services, enabling authorized users to receive immediate remote alerts.

The five-layer architecture integrates Sensor Data Acquisition, Edge Processing and Event Classification, IoT Communication, Cloud and Notification Management, and Application/User services. This layered design supports modularity, scalability, low-cost deployment, remote accessibility, and future expansion.

The conceptual evaluation demonstrates the potential advantages of the proposed approach over manual monitoring, basic electronic alarms, and single-sensor IoT systems. The illustrative results indicate an event detection accuracy of 98.10%, precision of 97.60%, recall of 97.20%, notification success rate of 98.40%, and reliability of 97.80%. However, these values must be validated using a physical prototype and reproducible experimental dataset before they are reported as measured empirical findings.

In summary, the integration of physical sensing, embedded edge processing, IoT communication, cloud event management, and mobile notification can transform conventional door monitoring into an intelligent and responsive security service. Future enhancements may include camera-based visitor verification, microphone-assisted acoustic knock recognition, TinyML-based event classification, facial recognition where legally and ethically appropriate, encrypted MQTT communication, battery-health monitoring, GSM backup connectivity, tamper detection, multi-door management, emergency escalation, and integration with broader smart-home automation platforms. A future prototype can also incorporate adaptive threshold learning to automatically adjust knock sensitivity according to door material, environmental vibration, and installation conditions.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] Maturi, S. Y. (2024). Cryptographic privacy engines: Practical multi-party protocols for confidential database queries. Nanotechnology Perceptions, 20(S13), 2770–2785.

[3] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, "A review of smart homes—Past, present, and future," *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, vol. 42, no. 6, pp. 1190–1203, 2012.

[4] Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Research in Information Technology and Computing, 8(4).

[5] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *Journal of Cleaner Production*, vol. 140, pp. 1454–1464, 2017.

[6] Shashank A. (2025). Metadata-driven data integration framework: Automating enterprise data integration through declarative approaches. European Modern Studies Journal, 9(4), 9.

[7] 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.

[8] Srikanth Kavuri. (2022). Large Language Model (LLM)-Based Automation for Software Test Script Generation. Computer Fraud and Security. https://doi.org/10.52710/cfs.836.

[9] Pavan Kumar Adabala. (2026). IoT-Driven Digital Twins for Manufacturing Optimization: Hybrid Modelling, Reinforcement Learning and Sustainable Operations. International Journal of Computational and Experimental Science and Engineering, 12(1). https://doi.org/10.22399/ijcesen.5050.

[10] Bhagwat, V. B. (2024). A simplified transition from EBS Payroll to Cloud Payroll: Benefits and Drawbacks. Journal of Computational Analysis and Applications, 33(6).

[11] Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.

[12] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, "A review of smart homes—Past, present, and future," *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, vol. 42, no. 6, pp. 1190–1203, 2012.

[13] Poojari, R. Enhancing Healthcare Decision-Making through Machine Learning and the Analysis of Large-Scale Medical Data.

[14] Chawla, N., Nandini, M. R., Pokala, H. K., & Siddartha, A. (2026, April). Resource Scheduling in Cloud-Assisted Communication Systems Using Enhanced Reinforcement Learning Algorithm. In 2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN) (pp. 1-6). IEEE.

[15] Maturi, S. Y. -(2024). Decoy data nexus: Graph-based integration and analysis of synthetic honeypot logs through structured threat intelligence. International Journal of Computational and Experimental Science and Engineering (IJCESEN), 10(4), 4255–4261. https://doi.org/10.22399/ijcesen.5010.

[16] 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.

[17] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[18] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.

[19] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the Internet of Things in the age of machine learning and software-defined networking," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4829–4842, 2018.

[20] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the Internet of Things cybersecurity," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2237–2275, 2020.