International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 06 – NOV-DEC 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

Intelligent Home Automation Using IoT and Context-Aware Computing

Dr. Yuki T. Watanabe

Senior Research Scientist, University of Tokyo, Japan

Abstract

Intelligent home automation has evolved from simple remote-control systems into interconnected computing environments capable of sensing household conditions, interpreting contextual information, and autonomously controlling appliances and services. The Internet of Things (IoT) provides the connectivity infrastructure required to integrate smart appliances, sensors, actuators, gateways, and cloud services, while context-aware computing enables these systems to adapt their behavior according to user activities, environmental conditions, time, location, preferences, and device states. This paper examines an intelligent home automation framework that combines IoT technologies with context-aware computing to support adaptive, personalized, energy-efficient, and secure residential environments. The proposed conceptual framework integrates environmental sensors, occupancy detection, wearable and mobile-device information, IoT gateways, edge processing, context-management mechanisms, decision engines, and smart actuators.

The methodology evaluates the architecture according to contextual accuracy, automation capability, energy efficiency, responsiveness, interoperability, usability, privacy, and security. The analysis demonstrates that context-aware IoT automation can provide significant advantages over conventional rule-based home automation by enabling systems to infer household situations and dynamically modify device behavior. For example, lighting, heating, cooling, ventilation, security, and entertainment systems can be coordinated according to occupancy, user preferences, environmental conditions, and temporal context. Edge computing can improve responsiveness by processing sensitive contextual information locally, while cloud services can support historical analytics and system-wide optimization.

Nevertheless, challenges related to heterogeneous IoT devices, contextual ambiguity, privacy, cybersecurity, interoperability, energy consumption, and user trust remain important barriers. The study concludes that intelligent home automation requires more than simple device connectivity; it requires context modeling, reliable sensing, intelligent decision-making, and secure control mechanisms. Future research should focus on privacy-preserving context inference, explainable artificial intelligence, adaptive learning, interoperable IoT architectures, and resilient security mechanisms. The integration of IoT and context-aware computing therefore represents a significant direction for developing intelligent residential environments that are responsive, personalized, sustainable, and capable of autonomous decision-making.

International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 06 – NOV-DEC 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

Keywords: Internet of Things, Smart Home, Home Automation, Context-Aware Computing, Intelligent Systems, Edge Computing, IoT Security, Smart Appliances, Ambient Intelligence, Context Management

1. Introduction

The rapid development of the Internet of Things has transformed residential environments into interconnected digital ecosystems in which appliances, sensors, smartphones, security devices, and environmental controllers can exchange information. Traditional home automation generally relies on predefined rules, timers, or direct user commands. Although such systems can automate repetitive activities, they have limited ability to understand changing household situations. Intelligent home automation extends this functionality by combining connected devices with computational mechanisms capable of interpreting environmental and user-related context. Such systems can automatically adjust household services according to occupancy, activity, time, environmental conditions, and user preferences.

Context-aware computing provides an important foundation for intelligent residential automation. Context refers to information describing the circumstances surrounding a user, device, or computational activity. In a smart home, relevant context can include room occupancy, user location, temperature, humidity, time of day, lighting conditions, appliance status, motion patterns, and historical preferences. By combining these contextual signals, a home automation system can determine the most appropriate action without requiring explicit instructions for every situation. This allows automation to become adaptive rather than merely rule-based.

IoT technologies provide the sensing and communication infrastructure required for context-aware home automation. Sensors can detect movement, temperature, light intensity, air quality, door status, and energy consumption, while smart appliances and actuators can execute control decisions. Gateways can aggregate information from heterogeneous devices and provide connectivity to edge or cloud computing platforms. The resulting architecture enables continuous monitoring and automated interaction between physical household environments and computational intelligence. However, effective automation depends on the quality, reliability, and interpretation of contextual information.

Intelligent home automation also introduces important concerns related to privacy and cybersecurity. Smart-home devices can collect detailed information about household routines, occupancy patterns, device usage, and user behavior. Unauthorized access to such information can expose sensitive aspects of private life. In addition, insecure IoT devices may become entry points for attackers seeking to compromise other systems. Consequently, intelligent automation must incorporate secure authentication, encrypted communication, access control, device management, privacy-preserving data processing, and continuous monitoring.

This research examines intelligent home automation using IoT and context-aware computing from a computer science and information technology perspective. The study develops a conceptual architecture integrating IoT sensors, contextual information, edge processing, context management, intelligent decision-making, and smart actuators. It evaluates the potential benefits and limitations of context-aware automation in terms of responsiveness, personalization, energy efficiency,

interoperability, privacy, and security. The research also identifies key implementation challenges and future research opportunities for developing intelligent residential environments.

2. Objectives

2.1 Primary Objective

The primary objective of this study is to examine how IoT technologies and context-aware computing can be integrated to develop intelligent home automation systems capable of sensing household conditions, understanding contextual information, and autonomously controlling connected devices. The study further evaluates the security, privacy, interoperability, responsiveness, energy efficiency, and usability requirements of such intelligent residential environments.

2.2 Development of Context-Aware Automation

The first objective is to analyze the role of context-aware computing in improving home automation. The study considers contextual information such as occupancy, location, time, environmental conditions, user preferences, device states, and behavioral patterns. These contextual variables can be combined to determine appropriate automation actions, allowing household systems to adapt dynamically rather than depending exclusively on predefined commands.

The study also examines contextual reasoning mechanisms that can convert raw sensor observations into meaningful household situations. For example, motion detection combined with time, room location, and historical behavior may indicate that a user has entered a room for a particular activity. Such contextual interpretation can support intelligent control of lighting, temperature, entertainment, security, and other residential services while reducing unnecessary manual interaction.

2.3 Evaluation of IoT Integration and Automation

The second objective is to evaluate how IoT devices, communication networks, gateways, edge platforms, and smart actuators can support intelligent home automation. The study examines the flow of information from sensors to decision-making components and ultimately to controlled appliances. Particular attention is given to interoperability, communication latency, device availability, and system scalability.

The research further evaluates how edge and cloud computing can support residential intelligence. Edge devices can perform real-time contextual processing within the home, while cloud platforms can support historical data analysis, model training, remote management, and long-term optimization. This combination can provide responsive automation while limiting unnecessary transmission of sensitive household information.

2.4 Security, Privacy, and User-Centric Automation

The third objective is to identify security and privacy requirements for context-aware smart homes. Since residential IoT devices may collect information about occupancy, routines, and personal preferences, protecting contextual data is essential. The study examines device authentication, encrypted

communication, access control, secure updates, data minimization, and privacy-aware processing as important security mechanisms.

The study also considers user trust and usability. Intelligent automation should provide convenient services without becoming unpredictable or difficult to control. Users should be able to understand, configure, override, and disable automated decisions when necessary. Consequently, user-centered design, transparent decision-making, explainable automation, and appropriate control interfaces are considered essential characteristics of practical intelligent home environments.

3. Review of Literature

3.1 IoT-Based Smart Home Systems

IoT-based smart homes connect appliances, sensors, gateways, and software services through communication networks. Early home automation systems primarily focused on remote control, allowing users to switch appliances or adjust environmental settings using centralized interfaces. Modern IoT architectures extend these capabilities through continuous sensing, cloud connectivity, mobile applications, and intelligent analytics. Smart homes can therefore support automated lighting, climate control, security monitoring, energy management, entertainment, and appliance coordination.

However, heterogeneous IoT environments create interoperability challenges because devices may use different communication protocols, data formats, operating systems, and security mechanisms. A smart home may contain products from multiple vendors that were not designed to operate as a unified ecosystem. Middleware, gateways, standardized protocols, and device abstraction mechanisms can help address these limitations. Scalable architectures must also support dynamic device discovery, configuration, firmware management, and secure communication.

3.2 Context-Aware Computing

Context-aware computing enables software systems to use information about their surrounding circumstances when determining appropriate behavior. In residential environments, context can be obtained from sensors, smartphones, wearable devices, smart appliances, calendars, location systems, and historical interactions. Context management involves collecting, representing, interpreting, and reasoning over these heterogeneous information sources.

Context-aware systems can provide more natural forms of automation because they respond to situations rather than isolated sensor events. For example, a lighting system may consider occupancy, ambient light, time, and user activity before deciding whether illumination is necessary. Context reasoning can therefore reduce unnecessary automation actions and improve personalization. However, inaccurate sensors or ambiguous contextual observations can lead to incorrect decisions, making context quality and uncertainty management important research areas.

3.3 Intelligent Automation and Ambient Intelligence

Ambient intelligence combines pervasive computing, sensing, communication, and intelligent software to create environments capable of responding to human activities. Smart homes represent an important application domain for ambient intelligence because household environments contain numerous physical

International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 06 – NOV-DEC 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

and digital resources that can be coordinated automatically. Machine learning can support activity recognition, user preference prediction, anomaly detection, and adaptive automation.

Recent intelligent home architectures increasingly use edge computing to process contextual information locally. This can reduce latency and limit the transmission of sensitive household data to remote services. Cloud platforms remain valuable for large-scale analytics and long-term learning. A hybrid edge-cloud architecture can therefore provide both local responsiveness and centralized computational capacity. Nevertheless, the increasing intelligence of home environments creates additional concerns regarding privacy, explainability, security, and user control.

4. Methodology

4.1 Research Design and Conceptual Framework

This study adopts a conceptual analytical research design to investigate intelligent home automation through the integration of IoT and context-aware computing. The proposed framework consists of five primary layers: sensing, communication, context management, intelligent decision-making, and actuation. Sensors continuously capture information about environmental and user-related conditions, while communication infrastructure transfers observations to gateways or processing units. Context-management mechanisms combine raw observations into meaningful contextual representations.

The framework is designed to support adaptive decision-making based on multiple contextual variables rather than isolated sensor events. A decision engine receives information from the context-management layer and determines whether an automation action should be initiated. The resulting command is transmitted to smart appliances or actuators. Feedback from controlled devices is returned to the system, allowing the automation process to be continuously monitored and adjusted. This creates a closed-loop intelligent control architecture.

4.2 Context Acquisition and Representation

Context acquisition involves collecting information from heterogeneous sources within the home. Environmental sensors can provide temperature, humidity, illumination, air-quality, and motion information, while smartphones and wearable devices can contribute location or activity-related information. Smart appliances can provide operational states such as power consumption, active mode, and availability. Combining multiple sources provides a richer representation of household conditions than relying on a single sensor.

Context representation converts raw measurements into structured information that can be processed by intelligent algorithms. The methodology considers contextual variables according to their temporal, spatial, and semantic characteristics. Sensor readings may be combined with user preferences and historical behavior to infer higher-level situations. Because sensor information may be incomplete or uncertain, the framework also considers confidence levels and contextual validation to reduce incorrect automation decisions.

International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 06 – NOV-DEC 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

4.3 Intelligent Decision-Making and Control

The decision-making layer analyzes contextual information and selects appropriate actions. Depending on implementation requirements, rule-based reasoning, machine learning, probabilistic models, or hybrid intelligent approaches can be used. A rule-based mechanism may provide predictable automation for simple situations, while machine learning can support more complex behavioral patterns. The framework emphasizes adaptive decision-making in which the system can modify its behavior based on observed household conditions and user feedback.

Key decision-making capabilities include:

- Occupancy-based lighting control
- Context-aware temperature adjustment
- Adaptive energy management
- Activity-aware appliance control
- Intelligent security responses
- Personalized entertainment settings
- Abnormal activity detection
- User preference learning

The control layer communicates decisions to smart actuators while maintaining feedback about the resulting state. This enables the system to determine whether an intended action was successfully executed and whether further adjustment is necessary.

4.4 Security, Privacy, and Performance Evaluation

Security evaluation considers IoT device authentication, encrypted communication, authorization, firmware security, network monitoring, and protection against unauthorized device control. Since context-aware systems can collect sensitive behavioral information, privacy evaluation emphasizes data minimization and local processing. Edge computing can be used to analyze selected contextual information within the home instead of transmitting all raw data to external cloud platforms.

Performance evaluation considers contextual accuracy, response time, energy efficiency, device interoperability, automation reliability, and user interaction. A useful intelligent home system should respond quickly enough for real-time activities while minimizing unnecessary computation and communication. The methodology therefore evaluates the balance between intelligent functionality and resource consumption. System performance is considered across sensing, communication, processing, and actuation rather than through a single technical metric.

5. Analysis

5.1 Intelligent Home Automation Architecture

The proposed architecture connects sensing devices, IoT communication infrastructure, context-management components, intelligent decision engines, and actuators. The sensing layer captures environmental and user-related information, while the communication layer transports information between devices and processing components. Context management combines observations and creates

International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 06 – NOV-DEC 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

meaningful representations. The decision layer evaluates the contextual state and selects appropriate actions. Finally, actuators execute decisions and provide feedback to the system.

This architecture differs from basic IoT automation because actions are determined from multiple contextual variables. For example, a lighting system can consider occupancy, ambient illumination, time, and user preference simultaneously. Such reasoning reduces unnecessary device activation and enables more personalized automation.

Table 1: Functional Architecture of Intelligent IoT-Based Home Automation

Layer	Components	Primary Function	Example
Sensing Layer	Motion, temperature, light, humidity, air-quality sensors	Context acquisition	Detect occupancy and room conditions
IoT Communication Layer	Wi-Fi, Bluetooth, Zigbee, gateways	Device connectivity	Transfer sensor observations
Context Layer	Context database, semantic models, context processor	Context interpretation	Infer household situations
Intelligence Layer	Rules, ML models, decision engine	Automated decision-making	Determine appropriate device action
Edge Layer	Local gateway, edge processor	Low-latency processing	Local activity recognition
Cloud Layer	Storage, analytics, remote management	Historical analysis	Preference and energy analysis
Actuation Layer	Smart lights, HVAC, locks, appliances	Execute decisions	Adjust lighting or temperature
User Layer	Mobile apps, dashboards, voice interfaces	User interaction	Override or configure automation

Interpretation: Table 1 demonstrates that intelligent home automation depends on cooperation among sensing, communication, contextual reasoning, intelligent decision-making, and actuation layers. IoT connectivity provides the communication foundation, but context processing and intelligent reasoning distinguish an adaptive smart home from conventional remote-control systems. Edge processing is particularly useful for time-sensitive and privacy-sensitive operations. Cloud infrastructure complements the local architecture by supporting historical analysis and remote management. The layered design also facilitates scalability by allowing individual components to be upgraded without replacing the entire system.

International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 06 – NOV-DEC 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

5.2 Context-Aware Automation Performance

Context-aware computing can improve automation performance by allowing systems to consider multiple conditions before executing an action. A conventional rule may switch lights on whenever motion is detected, whereas a context-aware system can determine whether the room is occupied, whether sufficient natural light is available, what time it is, and whether the user prefers automatic lighting. This contextual reasoning can reduce false activations and improve user satisfaction.

Context-aware automation can also improve energy efficiency. Heating, cooling, lighting, and appliance operation can be adjusted according to occupancy and environmental conditions. When a room is unoccupied, unnecessary energy consumption can be reduced. When occupancy is detected, the system can restore appropriate environmental settings. Intelligent algorithms can additionally learn recurring patterns and identify opportunities for optimization. However, automation decisions should remain controllable by users to prevent unwanted behavior.

5.3 Security, Privacy, and Usability Analysis

Smart homes create a substantial volume of contextual data that may reveal personal routines, household occupancy, preferences, and behavioral patterns. Therefore, privacy must be treated as a fundamental design requirement. Local processing can reduce the need to transmit sensitive raw information, while encryption and access control can protect data exchanged among devices. Device authentication is also essential because unauthorized control of household appliances can create both privacy and physical security risks.

Table 2: Key Evaluation Dimensions for Context-Aware Smart Homes

Evaluation Dimension	Potential Benefit	Major Risk	Recommended Mechanism
Context Accuracy	Better automation decisions	Sensor errors	Multi-sensor fusion
Response Time	Faster device control	Network latency	Edge processing
Energy Efficiency	Reduced unnecessary consumption	Excessive sensing	Adaptive sampling
Personalization	User-specific automation	Incorrect preference inference	User feedback
Privacy	Reduced data exposure	Behavioral profiling	Local processing and minimization
Security	Protection of connected devices	Unauthorized access	Authentication and encryption
Interoperability	Integration of	Protocol	Standardized interfaces

International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 06 – NOV-DEC 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

Evaluation Dimension	Potential Benefit	Major Risk	Recommended Mechanism
	heterogeneous devices	incompatibility	
Usability	Convenient interaction	Unpredictable automation	Explainable controls and overrides

Interpretation: Table 2 shows that intelligent home automation involves a balance between automation benefits and implementation risks. Greater contextual awareness can improve personalization but may also increase privacy concerns. Edge processing can reduce latency and limit external data transmission, while sensor fusion can improve contextual accuracy. Interoperability remains necessary because modern homes frequently contain devices from different vendors. User controls and explainable automation are also important because highly autonomous systems may become frustrating if users cannot understand or override automated actions.

6. Discussion

6.1 Contextual Intelligence in Residential Environments

The integration of IoT and context-aware computing enables residential environments to respond to situations rather than individual sensor events. Contextual intelligence allows the system to interpret relationships among occupancy, environmental conditions, time, user activity, and appliance state. This creates more sophisticated automation and reduces the need for repetitive manual commands. The architecture can support lighting, climate control, security, entertainment, and energy-management applications through a common contextual framework.

The effectiveness of contextual intelligence depends on the quality of available information. A single motion sensor may not reliably determine whether a person is actively using a room. Combining multiple sensors and historical information can increase confidence in contextual interpretation. However, additional sensing also increases system complexity and may introduce privacy concerns. Therefore, intelligent context acquisition should focus on collecting only the information necessary to support useful automation.

6.2 Energy Optimization and Personalized Automation

Context-aware systems can contribute significantly to residential energy management by coordinating appliances according to occupancy, environmental conditions, and user preferences. Lighting can be reduced when natural illumination is sufficient, while heating and cooling can be adjusted based on occupancy. Intelligent scheduling can also coordinate high-consumption appliances according to user routines and system conditions. These mechanisms can transform home automation from convenience-oriented control into an intelligent energy-management platform.

Personalization provides another major advantage. Different household members may have different preferences regarding temperature, lighting, entertainment, and device operation. Context-

aware computing can incorporate individual preferences when determining appropriate actions. However, personalization models should remain transparent and adaptable. Users should be able to modify learned preferences, review automation decisions, and manually override actions. Such mechanisms can increase trust and prevent excessive dependence on automated inference.

6.3 Security, Privacy, and Trust

Security must be integrated throughout the smart-home architecture because IoT devices may provide attackers with direct access to physical appliances and household information. Weak device credentials, outdated software, insecure communication, and poor access controls can create significant vulnerabilities. A compromised device may also be used as a platform for attacking other devices on the home network. Consequently, device identity, secure communication, network segmentation, secure updates, and continuous monitoring are important.

Privacy is equally significant because contextual data can reveal household routines even when explicit personal information is not collected. Systems should therefore minimize data collection, process sensitive information locally where possible, and provide users with meaningful control over data sharing. Privacy-preserving context inference can reduce exposure while maintaining intelligent functionality. Trust in smart-home automation will depend on both technical security and transparent user-centered policies.

7. Challenges

7.1 Context Ambiguity and Sensor Reliability

Context-aware automation depends heavily on accurate interpretation of sensor observations. Environmental sensors may generate noisy or incomplete measurements, while motion detection may not always represent actual user activity. Multiple household members can also create overlapping contextual states that are difficult to interpret. Incorrect context inference may result in unwanted appliance activation or failure to execute necessary actions. Sensor fusion, confidence-based reasoning, contextual validation, and adaptive learning can reduce these problems, but reliable interpretation remains a major technical challenge.

7.2 Device Heterogeneity and Interoperability

Smart homes commonly contain devices manufactured by different vendors using different communication protocols and software architectures. Such heterogeneity can prevent seamless device integration and make system management complex. Proprietary ecosystems may restrict interoperability and increase dependence on specific platforms. Standardized communication interfaces, common data models, device abstraction layers, and interoperable middleware can address some of these limitations. However, maintaining compatibility as new devices and technologies are introduced remains an ongoing challenge for intelligent home automation.

7.3 Privacy and Cybersecurity

The continuous collection of household context creates significant privacy risks. Information about occupancy, routines, preferences, and device usage can potentially be exploited for surveillance, profiling, or malicious purposes. IoT devices can also contain software vulnerabilities that attackers may exploit to obtain unauthorized access. Strong authentication, encryption, secure firmware updates, network segmentation, access control, and local processing are necessary safeguards. Nevertheless, security must remain adaptive because smart-home environments continuously change as new devices, applications, and users are introduced.

8. Future Research

8.1 Explainable Context-Aware Artificial Intelligence

Future research should investigate explainable AI techniques that allow users to understand why a smart-home system performed a particular action. Explainability can improve user trust and make automated decisions easier to verify or correct. Research should focus on interpretable context models that can communicate the relationship between sensor observations, inferred situations, and automation decisions. Such approaches may be particularly important when intelligent systems control security devices, heating systems, access mechanisms, or other household functions with significant consequences.

8.2 Privacy-Preserving Context Inference

Future research should develop context-aware intelligence that can operate without unnecessarily exposing sensitive household information. Federated learning, secure computation, differential privacy, and local edge inference may provide mechanisms for learning behavioral patterns while minimizing centralized data collection. Research should investigate how these techniques affect contextual accuracy, computational cost, latency, and user experience. Privacy-preserving architectures should also provide users with clear controls over which contextual information is collected, stored, processed, or shared.

8.3 Adaptive and Interoperable Smart Homes

Future intelligent homes should support devices from multiple vendors and adapt dynamically as household environments change. Research should focus on self-configuring IoT architectures capable of discovering new devices, determining their capabilities, establishing secure connections, and integrating them into existing automation workflows. Adaptive systems should also learn changing user preferences without becoming unpredictable. Standardized device descriptions, interoperable protocols, AI-assisted configuration, and resilient security mechanisms can contribute to scalable smart-home ecosystems capable of long-term autonomous operation.

9. Conclusion

Intelligent home automation using IoT and context-aware computing represents an important development in modern computer science and information technology because it transforms connected residential devices into adaptive computational environments. The integration of sensors,

communication networks, context-management mechanisms, intelligent decision engines, edge platforms, cloud services, and smart actuators enables homes to respond to changing environmental and user conditions. Unlike conventional automation systems based primarily on predefined schedules or direct commands, context-aware architectures can combine occupancy, location, time, environmental measurements, device states, and user preferences to determine appropriate actions. This capability can improve convenience, personalization, energy efficiency, responsiveness, and the overall intelligence of residential environments.

The analysis also demonstrates that intelligent automation introduces substantial technical and organizational challenges. Contextual decisions depend on reliable sensing and accurate interpretation, while heterogeneous IoT devices can create interoperability difficulties. Smart homes continuously generate information that may reveal household routines, making privacy protection essential. Cybersecurity is equally important because compromised devices can expose personal data or provide unauthorized control over physical appliances. The use of edge computing can reduce latency and allow sensitive contextual information to remain within the home, while encryption, authentication, access control, secure firmware, and network segmentation can strengthen device security. At the same time, users must retain meaningful control over automated decisions through configuration mechanisms, manual overrides, and understandable system interfaces.

Overall, the convergence of IoT and context-aware computing provides a strong foundation for next-generation intelligent residential environments. Future systems should move beyond simple automation rules toward adaptive, explainable, privacy-preserving, and interoperable intelligence. Advanced machine learning can support activity recognition and preference learning, while edge computing can provide low-latency contextual processing. Privacy-preserving technologies can reduce unnecessary exposure of behavioral information, and standardized interfaces can improve compatibility among heterogeneous devices. Successful intelligent home automation will ultimately depend on balancing autonomy with user control, personalization with privacy, and connectivity with cybersecurity. By addressing these requirements systematically, IoT-enabled context-aware computing can create residential environments that are more responsive, efficient, secure, and capable of supporting evolving household needs.

References

1. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805.
2. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660.
3. Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context aware computing for the Internet of Things: A survey. *IEEE Communications Surveys & Tutorials*, 16(1), 414–454.
4. Abowd, G. D., Dey, A. K., Brown, P. J., Davies, N., Smith, M., & Steggles, P. (1999). Towards a better understanding of context and context-awareness. *Handheld and Ubiquitous Computing*, 304–307.
5. Dey, A. K. (2001). Understanding and using context. *Personal and Ubiquitous Computing*, 5, 4–7.

6. Cook, D. J., Augusto, J. C., & Jakkula, V. R. (2009). Ambient intelligence: Technologies, applications, and opportunities. *Pervasive and Mobile Computing*, 5(4), 277–298.
7. Kortuem, G., Kawsar, F., Fitton, D., & Sundramoorthy, V. (2010). Smart objects as building blocks for the Internet of Things. *IEEE Internet Computing*, 14(1), 44–51.
8. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. *IEEE Internet of Things Journal*, 1(1), 22–32.
9. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376.
10. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164.
11. Gungor, V. C., & Hancke, G. P. (2009). Industrial wireless sensor networks: Challenges, design principles, and technical approaches. *IEEE Transactions on Industrial Electronics*, 56(10), 4258–4265.
12. Stankovic, J. A. (2014). Research directions for the Internet of Things. *IEEE Internet of Things Journal*, 1(1), 3–9.
13. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 3(5), 637–646.
14. Satyanarayanan, M. (2017). The emergence of edge computing. *Computer*, 50(1), 30–39.
15. Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and Internet of Things: A survey. *Future Generation Computer Systems*, 56, 684–700.
16. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*, 57(10), 2266–2279.
17. Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, 54, 1–31.
18. Razzaque, M. A., Milojevic-Jevric, M., Palade, A., & Clarke, S. (2016). Middleware for Internet of Things: A survey. *IEEE Internet of Things Journal*, 3(1), 70–95.
19. Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A. (2019). A secure Internet of Things architecture for smart homes. *IEEE Internet of Things Journal*, 6(5), 1–12.
20. Cook, D. J. (2012). How smart is your home? *Science*, 335(6071), 1579–1581.
21. Yang, L., Ge, Y., Li, W., Rao, W., & Shen, W. (2014). A home mobile healthcare system for smart home environments. *Sensors*, 14(3), 4987–5005.
22. Chan, M., Campo, E., Estève, D., & Fourniols, J. Y. (2009). Smart homes—Current features and future perspectives. *Maturitas*, 64(2), 90–97.
23. Marikyan, D., Papagiannidis, S., & Alamanos, E. (2019). A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change*, 138, 139–154.
24. Talebkhah, M., Sali, A., Marjani, M., Gordan, M., & others. (2020). Smart home applications and IoT technologies: A review of architectures and challenges. *IEEE Access*, 8, 1–15.
25. Xu, L. D., He, W., & Li, S. (2014). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 10(4), 2233–2243.