International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

A Comprehensive Review of Secure and Intelligent Smart Home Automation Systems Integrating Speech Recognition and Energy Monitoring

[1]Reena Ahirwar, [2]Dr. Puneet Nema

[1]Mtech Scholar, Department of Computer Science and Engineering, Lakshmi Narain College of Technology, Bhopal

[2]Assistant Professor, Department of Computer Science and Engineering, Lakshmi Narain College of Technology, Bhopal

[1]imreenaahiwar@gmail.com , [2]puneetnema11@gmail.com

ABSTRACT:

The smart home automation systems have appeared to be the transforming solution that had been taken upon enhancing convenience, security, and energy efficiency in modern living environments. This review paper discusses a detailed explanation of secure and smart home automation systems integrating speech recognition and power measurement functions. In the context of smart home technologies, the paper discusses the gradual upward movement of artificial intelligence, IoT, and embedded systems in deploying home automation. Particular attention is vested on speech recognition approaches, which enables the controlling of household appliances with spoken commands, thus easing access and user experience. The hybrid power-measurement module had been integrated and investigated for energy measurement applications combining real-time energy monitoring with cost and set-point implementation. The paper also reviews the different academically adopted security measures in place to secure the smart home network against cyber-attacks, including encryption protocols, authentication mechanisms, and intrusion detection systems. Comparative analysis examines various existing models for their strengths, weaknesses, and evaluation from Performance points of view like accuracy, latency, and energy efficiency. Also addressed are the challenges such as data privacy, system interoperability, scalability, and reliability. The review also highlights new paradigms including edge computing, AI for automation, and blockchain for afterward improvement of security. Finally, the article offers a comprehensive source for rightr design and implementation for secure, feasible, user-friendly smart homes that can then steer future research and development in this dynamic area.

Keywords: Smart Home Automation, Speech Recognition, Energy Monitoring, IoT Security, Machine Learning, Power Measurement

1. INTRODUCTION

Rapid progress in syllabus and high technology visualization has tremendously revolutionized the modern environment of living, characterizing the automatic attenance smart home system as being very instrumental in the intelligent infrastructure. These systems showcase embedded devices, sensors, and communication networks providing automatic control of household systems such as the light set-ups, security, and the monitoring of energy usage. There has been considerable upsurge in demand for convenience, safety, and energy conservation in various

applications thus accounting for the increasing application of smart-home technologies in both residential and commercial set-up. This paper review takes a broad look at the scope of secure and intelligent smart home automation systems, with a greater focus on the integration of speech recognition and energy monitor. The smart home automation is, in nature, driven generally by the convergence of technologies dealing with the Internet of Things (IoT) with artificial intelligence (AI) techniques along with Embedded Systems-the products that use in use for making the digital naturally controlled life come into the comfort zone [1]. This convergence between AI-the knowledge-driven part of human beings and IoT-the infustructyre of machine makes communicating between devices possible, using invisible means of communication using standards of wireless networking such as Zigbee, WiFi, Bluetooth. It is also noted that AI bolsters the intelligence of such systems and complements them with decision-making ability, pattern recognition, and analysis of predictives. Embedded systems are the key hardware aspects of this kind of infrastructure. Thus far this linkage of the three technologies together has resulted in the endless comfort-optimized blend of both living resources. One of the most demanding events that has unfolded in smart household technologies has included the utilization of voice control. This allows for the command of the devices in the most natural of ways, which is to orally communicate with them instead of reaching for physical interfaces such as switches or relying on a mobile application [2]. Elderly people and weak individuals are the ones who would extend the maximum benefit; with this particular feature included in the design of the devices, systems can further establish ease and accessibility. Powered by modern learning algorithms deep learning models—speech recognition works on the accuracy and robustness aspects of mostly noisy environments. These systems execute virtually in real time to enable proper appliance management such as lights, fans, heating or cooling, and entertainment systems all from voice commands. Besides convenience and access, energy-saving is also a significant issue eliciting the interest of smart home automation [3]. Measurement of power and modules for energy monitoring makeit possible for users to monitor their electrical consumption on a real-time basis. In this way, Smart meters and sensors gather data concerning the usage patterns of various appliances which is then analyzed to pinpoint operating inefficiencies and select most efficient consumption of energy. This will not only cause a reduction in electricity bills but also will contribute to environmental sustainability by reducing energy wastage. The state-of-art machines may present automated recommendations or create some proactive events such as switching off devices that are not being used or changing configurations as considerate of user behavior and environmental conditions. Deploying smart home systems has introduced key security and privacy challenges while coming with TONS of advantages. Smart homes run on interconnected networks and cloud-based services, making them vulnerable to various cyber threats such as unauthorized access, data theft, or malicious attacks. In the wrong hands, security holes in communication protocols or device firmware could give the attackers total control over home automation systems and cause severe user safety and privacy breaches [4]. Assurance against these threats would require an intelligent design to induce rigorous security mechanisms within the smart home. In general, such mechanisms would protect any sensitive

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

data and prohibit any unauthorized access through deployment of encryption, secure access, authorization, and intrusion detection systems.

Interoperability signifies the balance of various devices and systems being used to function together seamlessly. This diversity of manufacturers and communication protocols often creates problems of compatibility, resulting in a very hard time integrating devices into a whole system. To address this problem, scientists and developers are deep diving into standardized frameworks and protocols that are open to regulate potential interoperability. These are the prerequisites for building flexible, future-proof smart home ecosystems that assimilate new devices and technologies.**Figure 1** Illustrates the integration of IoT devices, sensors, controllers, and communication networks for automated and intelligent home management [5].

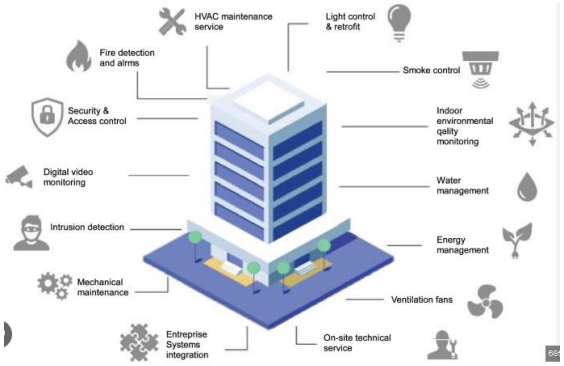

Figure 1: Smart Home Automation Systems

Integration between edge and cloud computing has significantly boosted performance and efficiency within the smart home system. Data processing performed at edge greatly minimizes delays along signal paths, thereby helping improve response time. It is imperative for real-time applications such as speech recognition and security monitoring. On the contrary, cloud computing ensures data analysis, remote access, and model training through providing a scalable storage and computing resource. So shouldering the load together, edge and cloud computing help achieve balance in data processing, ensuring both efficiency and scalability. Some of the advanced technologies such as blockchain and federated learning are suggested to strengthen security and privacy implications, considering the recent research trends. Application of the blockchain technology creates a decentralize tamper-proof framework for handling data while the federated learning lets models in machine learning get trained in multiple devices without transferring raw data [6]. These methods not only address privacy-related concerns, they also raise the trustworthiness of smart home systems.

This review paper targets an in-depth examination of secure and intelligent smart home automation systems that feature speech recognition and energy monitoring. It scrutinizes the architecture, technologies, and key components of the systems and presents their advantages and constraints [7]. A comparative evaluation of existing approaches is discussed with respect to performance in terms of accuracy, efficiency, and security. Furthermore, the paper raises a few current challenges and suggests a few ways future research may go. Modern-day home automation systems have undergone some considerable progress, providing high levels of convenience, energy efficiency, and security. Integration of voice recognition and power-

metering technologies into the home automation paradigm further enhances its features and usability. Deals with security, privacy, interoperability, and thereby scalability problems before the technology can take off massively. This paper review describes quite briskly where the plays of smart-home technology currently lie while paving the road for future innovative areas within a dynamic space.

2. SMART HOME SYSTEM ARCHITECTURE

The smart home automation architectures provide the seamless integration into a communication path; control path and monitoring mode of different home devices into one actual smart whole, instead of an empty smart-sounding display. These will always have sensors, communications, processing, and an application layer, each with valuable function to ascertain the efficient and smooth navigation of the system. It is mostly logical to conceive that the most critical layer of the sensing layer is buttons and actuators. Basically, sensors in the form of experience temperature, humidity, immersion, probing, smoke, etc.-collect real-time data from the surroundings, while the actuators make possible the act of adjusting those things like appliances for on and off; adjusting the degree diffuse of lighting and regulating temperature. These are the-footprint-that drives the smart home systems interaction with the environment.

The communications layer supports the exchange of data between devices at the peripheral level and the central control unit. The Ethernet physical media fires implement wired communication while devices with connected devices can be interconnected wirelessly via their radios. Nowadays, wireless communication is gaining popularity due to the unmatchable flexibilities, scalability, and ease of installation. The integration uses gateways/hubs to provide and manage connection points between protocols and devices functioning in the home photoe-system. Therefore, the incurred agendas are too strong to diverge. Processing tier is characterized with data analysis, decision-making, and system intelligence, given microcontrollers, embedded systems, edge devices, and cloud servers. Edge computing is significant by performing local data processing, reducing latencies, and providing real-time responses to critical applications like security monitoring and speech recognition. Cloud computing, in the same light, serves as a support and offers long-term storage and advanced analytics and machine learning benefits. These technologies together give way to predictive automation, trend-spotting, and tailored user experiences.

International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

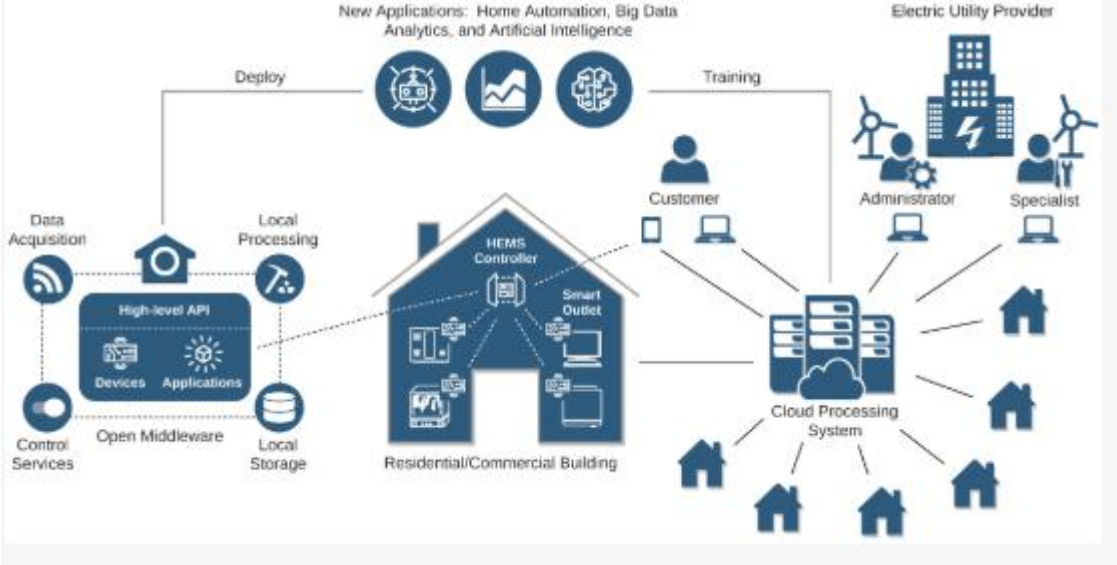

Figure 2: Overall system architecture foe smart homes.

Figure 2 depicts the layered structure integrating sensors, communication networks, processing units, and user interfaces for efficient smart home automation. Upon the application layer lies the graphical user interface of the system that puts Homeowners in control of the system through a variety of means, particularly mobile applications, web interfaces, etc. The speech recognition technology is a function within the component that allows users to give natural language commands in working with devices. The application layer also offers monitoring in real time, alert features, scheduling, and remote access-features that actually improve convenience and usability. User preferences and behavioral patterns are retrieved and analyzed so as to help in the provision of customized automated services. Security appears critical in each blooming light. Symmetric encryption techniques, authentication protocols, and access control methods are only a few examples of the myriad security rules engineered throughout the design. IDSs are also linked into the design to look for threats and actions in real time. The arrangement of the smart home building system serves to present a complex and dynamic frame that engages sensors, communications, processing, and application spaces, offering an efficient environment, flexible nature, and the ability to maintain convergence and gradual relatives of modern technologies, lending fine-groundwork to the smart home systems in the new era.

3. SPEECH RECOGNITION TECHNIQUES

Some recent works helped to define the progress of smart homes in terms of the integration of technology and the ways of improvement in energy efficiency, comfort, trust, and security in modern domestic environment. The studies in [2] dig deep into the discussion of integration of the IoT with smart homes and explore the ways that greater communication can foster automation and a greater level of intelligence in such systems. The study that was undertaken within [3] explains the design and the development of an IoT-driven system that offers an array of services that allow for the monitoring and control of home electronics with energy efficiency. The study [4] provides a review of security-centric applications handling issues relating to security in smart homes, intrusion detection, and prevention methods, protecting the home from

unauthorized access. The article on different scalable IoT architectures discussed within [5] explains the designs that could be useful in the future in large-scale deployments, as chosen for flexibility in integrating existing systems and devices.

Highlighted in AI-based recent methods [6] of analysis are how effective overall system management is made by the amalgamation of communications, energy management, and cybersecurity. This is where IoT-enabled secure, low-energy framework for intelligent living environment for the mutual problems consist of scalability and reliability. Furthermore, the issues concerning advanced low-latency and high-speed communication technologies such as 5G are addressed [8], which hugely pertain to boosting the overall smart home performance. Cyber-physical system integration hinted at [9] bears about the coordinate role between the physical wares and computer power, letting the two together enhance automation and responsiveness. Noteworthy, edge-wireless networks have also incorporated into the AI discussion, with the provision of real-time processing and carried out by edge-computing infrastructure [10]; latency is minimized whilst system efficiency level is much improved.

Deep learning-based security mechanisms in [11] enhance threat detection accuracy and strengthen smart home protection systems. Privacy-preservation approaches integrating edge AI and blockchain are presented in [12] to foster secure and individually satisfying user experiences. Voice-driven IoT systems presented in [13] take user interaction to the next level, offering natural language control: a good balance between convenience and ease of use in lenient automation. Advanced frameworks for multimodal AI agents [14] are meant to bring about adaptive, context-aware home automation in smart homes. Finally, the integration of machine learning and AI in IoT environments is highlighted in [15], which has exhibited transformative applications to enhance predictive capabilities and overall system intelligence.

4. POWER MEASUREMENT AND ENERGY MANAGEMENT

New studies since [16] focus on the user-centered design of smart homes to promote utilization of optimization methods to improve hygiene, usability, and user satisfaction concerning the household smart gadgets. [17] extensively presents the energy-consumption patterns observed in late low-light-merged smart home assistant systems, which add so much insight into the power requirements of low-cost devices that they point toward designing an energy-conscious system. Intelligent smart home approaches entail the activities of language processes and IoT confluence for practically executing friction-free voice-based control and human–system interaction [18].

An alternative section of [19] illuminates the way in which practically energy-efficient, low-latency, real-time smart homes can be achieved, all with offline speech recognition combined with IoT. The consideration of automation in [20] reveals even heightened dimensions to housing security, energy efficiency, and user satisfaction while showing the impact intelligent devices have had on modern housing. An actual demonstration of voice-controlled automation systems that are constructive in any interaction hazards with regard to friendly interfaces, are in turn used to exercise control over appliances by use of solutions on the Internet and things (IoT).

The study conducted here [22] considers multimodal interaction between gestures and speech recognition aimed at increasing as far as accessibility and flexibility within smart-home environments to encompass a wide range of individual user needs and interaction preferences.

5. SECURITY AND PRIVACY MECHANISMS

The security and privacy are critical parameters in smart home automation systems due to the close linkage between interconnected devices, wireless networks, and cloud services. Internet of things (IOT) devices are extending how much smart homes are at risk of different cyberattacks which includes external accesses, data breaches, eavesdropping, malware attacks, and denial of service (DoS) attacks. Therefore, robust security and privacy mechanisms are necessary to ensure a smart home's operation safely and consistently. One of the basic security techniques employed in secure homes is encryption of data, protected during transmission between devices and servers. Encryption algorithms such as Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) create the necessary confidentiality to transfer sensitive information like user credentials and device data. Secure communication protocols including Transport Layer Protection and Secure Sockets Layer (SSL) provide yet again additional data protection by inhibiting layer-interception and tampering [13].

Authorization and access control methods go far in removing unauthorized users from accessing the home system. Different methods such as password-based authentication, multi-factor authentication (2FA), biometric fingerprint or voice recognition, and token-based authentication are widespread today. Role-based access control (RBAC) ensures that users have secure access to only those devices and functionalities that have been authorized, thereby minimizing possible security risks. In the same way, the use of intrusion detection systems (IDS) and intrusion prevention systems (IPS) is represented as a significant mechanism. These systems monitor network traffic and device behavior to determine unusual activities or anomalies. An IDS utilizing machine learning may detect new or zero-day attacks by comparing patterns and distinguishing behavior falling off the normal path, achieving good performance in dynamic smart home settings.

One initiative under the limelight is the advent of blockchains as an effective remedy to security and privacy specifications in smart homes. It creates a decentralized and immutable data store that exists without authorities. The benefit offered by blockchain lies in giving data integrity, transparency, and a reliable device authentication, therefore minimizing the chances of data distortion and security breaches. With edge computing, data becomes independent and confidential because it is processed locally. This allows the mitigation of the risk of data exposure and the lowering of latency, thereby enabling the faster performance and heightened security level of a decision-making process. Another aspect of federated learning is when machine learning models are trained across different devices without actually sharing raw data; this way, the user enjoys privacy and results from collaborative learning. However, as promising as these relevant firms are, many challenges continue to linger. For example, most IoT devices have limited computational and energy resources, thereby making it difficult for more complex security algorithms to be adopted [19]. Moreover, the absence of standardized frameworks of security secures that there will be inconsistencies in the protective levels of

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

devices made by various companies. Privacy issues regarding continuous data collection and monitoring are a great issue, as this continuous observation could expose personal information if not elegantly handled. Issues are being tackled by researchers and their focus is on lightweight cryptography, standardized security protocols, and AI-based detection of threats. Indeed, regular updates installation, secure firmware design, and awareness amongst users are also necessary to keep systems up-to-date in terms of security. **Table 1** Presents and compares various security methods used to protect smart home data, devices, and communication from cyber threats. Table 2 Summarizes and compares existing research on smart home architectures based on technologies, performance, and limitations.

Table 1: Security and Privacy Techniques in Smart Home Systems

Technique	Description	Advantages	Limitations
Encryption (AES, RSA)	Secures data during transmission	High data confidentiality	Computational overhead
SSL/TLS Protocols	Secure communication channels	Prevents data interception	Requires certificate management
Multi-Factor Authentication (MFA)	Multiple verification methods	Strong user authentication	User inconvenience
Biometric Authentication	Uses fingerprint/voice recognition	High accuracy and security	Privacy concerns
Role-Based Access Control (RBAC)	Restricts user permissions	Improved access management	Complex configuration
Intrusion Detection Systems (IDS)	Detects suspicious activities	Identifies unknown attacks	False positives
Intrusion Prevention Systems (IPS)	Prevents detected threats	Real-time protection	Resource intensive
Blockchain Technology	Decentralized secure data storage	Tamper-proof and transparent	High complexity and cost
Edge Computing	Local data processing	Reduced latency and better privacy	Limited processing power
Federated Learning	Decentralized model training	Preserves user data privacy	Communication overhead

Table 2: Literature Review on Smart Home System Architecture

Ref	Key Contribution	Architecture/Technology Used	Results/Findings	Limitations
[1]	Historical and technological	Integrated IoT-based framework	Improved energy efficiency and comfort	Limited focus on real-time implementation

	evolution of smart homes			
[2]	IoT integration in smart homes	IoT with ML models	Enhanced automation and connectivity	Complexity in large-scale deployment
[3]	Raspberry Pi-based smart home system	IoT + Embedded system	Cost-effective and efficient monitoring	Limited scalability
[4]	Smart home security and intrusion prevention	IoT-based security framework	Improved threat detection	High dependency on network stability
[5]	Scalable IoT architecture design	Modular IoT architecture	High scalability and flexibility	Implementation complexity
[6]	AI integration in smart systems	AI + IoT + Cybersecurity	Enhanced decision-making and automation	High computational requirements
[7]	Secure and energy-efficient framework	IoT with secure protocols	Improved security and energy efficiency	Limited real-world validation
[8]	Use of 5G in smart homes	5G network slicing	Low latency and high-speed communication	Infrastructure dependency
[9]	Cyber-physical smart home systems	CPS + IoT	Better system integration	Security vulnerabilities
[10]	Intelligent wireless networks	Edge computing + IoT	Reduced latency and improved efficiency	High setup cost
[11]	Deep learning in smart home security	DL-based architecture	High accuracy in threat detection	Data privacy concerns
[12]	Privacy-preserving smart systems	Edge AI + Blockchain	Enhanced privacy and personalization	Complex implementation
[13]	Voice-driven automation	IoT + Speech recognition	Improved user interaction	Noise sensitivity

[14]	AI agent-based smart homes	LLM-based framework	Intelligent automation and adaptability	High resource usage
[15]	AI and ML in IoT environments	ML + IoT integration	Improved predictive automation	Requires large datasets
[16]	User-centered smart device design	AI-based optimization models	Enhanced user satisfaction	Limited generalization
[17]	Energy consumption analysis	LLM-enabled IoT systems	Insights into energy usage	High energy consumption
[18]	NLP-based voice control	NLP + IoT	Efficient voice interaction	Language limitations
[19]	Offline speech recognition system	Edge AI + IoT	Low latency and energy efficiency	Limited vocabulary support
[20]	AI-powered smart home system	AI + IoT architecture	Improved security and efficiency	Integration challenges
[21]	Voice-controlled automation system	IoT + Voice modules	User-friendly control system	Limited scalability
[22]	Gesture and speech-based automation	Multimodal interaction system	Enhanced accessibility	Increased system complexity

6. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

The realm of smart home automation has witnessed an increasing proliferation of advanced technologies, specifically the Internet of Things, artificial intelligence, and embedded systems, to offer intelligent and efficient living environments. In this survey review, both secure and smart home architectures are also explored in terms of their capabilities in speech recognition coupled with kilowatt power metering, revealing the promotion of convenience, accessibility, and energy efficiency. Speech-based control systems eventually attempt to enhance interaction between them and humans by allowing for natural communication, while an energy management system aims at real-time control and optimization of appliance loads to save energy and increase environmental sustainability. Evidently, this study also examines mechanisms securing various devices, including encryption, authentication, and intrusion detection systems, from cyber threats threatening the smart home environment. Some challenges will forever remain. For example, data privacy concerns may remain as a challenge;

there will still be interoperability issues between various devices; it will be limited in scalability; and needs an extremely low-latency processing. Besides, integration of these multiple non-standardized technologies grows way too complex, hence demanding strongly structured frameworks to ensure their reliability and smooth operation. Future research should focus on the creation of security, scalability, and energy efficiency in smart home systems. This can be achieved through incorporating emerging technologies, such as AI, Blockchain, and federated learning, which may give means to ensuring privacy, interoperability, and real time performance.

REFERENCES

1. Lucchi, Elena. "Smart home: historical framework, technological integration, and current trends in energy efficiency, human comfort, and security." Home Digital Twins (2026): 13-22.
2. Prajapati, Akash Kumar, et al. "Integration with IoT for Smart Homes." Machine Learning in Nanoelectronics: Devices, Circuits and Systems (2026): 409-448.
3. Ahmed, S. Feroz Shah, et al. "Iot-Driven Smart Home Automation And Monitoring System Using Raspberry PI." International Journal of AI Electronics and Nexus Energy 2.1 (2026): 387-396.
4. Bhagyasri, Yerra, et al. "IoT based security & smart home intrusion prevention system." International Journal of Computer Technology and Electronics Communication 9.2 (2026): 457-462.
5. Bozorgi, Mohammad, Gabriel J. Assaf, and Constantine J. Katsanis. "Configuration and execution of a scalable IoT architecture for smart home automation." Internet of Things (2026): 101900.
6. Malik, Maaz Tahir, et al. "Artificial Intelligence Applications in Smart Cities: Integrating Communication, Energy Management, Cybersecurity and Internet of Things." The Journal of Engineering 2026.1 (2026): e70166.
7. Naidu, B. Amarnath, et al. "Next-Generation IoT-Enabled Smart Home Framework: A Secure, Scalable and Energy-Efficient Solution for Intelligent Living Environments." Proceedings Copyright 767: 773.
8. Ashok, P., and Garudadri Sai Praneeth. "Leveraging 5g Network Slicing For Advanced Smart Home Systems." Recent Advances in Electrical and Electronic Engineering 19 (2026).
9. Gomez, Enrique Colon Ferruzola, et al. "Cyber-physical systems in the smart home: a review." International journal of computational innovations, intelligent systems and AI 2.1 (2026): 92-121.
10. Ishrat, Mohammad, et al. "Intelligent wireless networks: Edge computing, sensors, real-time computing, security, and emerging applications." Deep Learning Approaches in Intelligent Wireless Networking (2026): 199-223.
11. Ashokkumar, N. "Deep learning for smart home security systems." International Journal of Medical Engineering and Informatics 18.2 (2026): 162-175.

12. Harsha, M. S., et al. "A Privacy-Preserving Multimodal Smart Mirror with Edge AI, Blockchain Security and Quantum-Inspired Optimization for Personalized Wellness." 2026 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE). IEEE, 2026.
13. Muthumanikandan, V., Shajeth, and V. Sathya. "Voice-driven IoT: Revolutionizing home and hospital automation for enhanced security." AIP Conference Proceedings. Vol. 3383. No. 1. AIP Publishing LLC, 2026.
14. Mohanaprasad, K., et al. "HARMONY: A Framework for Multimodal LLM-Powered AI Agents in Smart Homes via the Model Context Protocol." IEEE Access (2026).
15. Ananthakrishnan, Gayathri, Baiju Babu Vimala, and S. Thamizharasan. "Synergizing Machine Learning and Artificial Intelligence in Internet of Things Environments: Transformative Applications and Future Direction." IoT Cybersecurity. Auerbach Publications 173-194.
16. Xu, Rui, et al. "Design of a user-centered intelligent shoe cabinet for smart home hygiene using Kano–AHP–TRIZ." Scientific Reports (2026).
17. Velaga, Krishna Sruthi, Anik Mallik, and Yifan Guo. "How Energy is Consumed by LLM-enabled Smart Home Assistant Systems on Low-Cost Devices: An Empirical Study." 2026 IEEE 23rd Consumer Communications & Networking Conference (CCNC). IEEE, 2026.
18. Reddy, S. Lokesh, and P. Ajay Kumar Reddy. "Intelligent smart home operations through NLP and IoT-driven voice control." Advancing Innovation through AI and Machine Learning Algorithms. CRC Press, 2025. 196-203.
19. Huang, Peng, et al. "Towards Energy-Efficient and Low-Latency Voice-Controlled Smart Homes: A Proposal for Offline Speech Recognition and IoT Integration." arXiv preprint arXiv:2506.07494 (2025).
20. Jahid, MKA Shahinoor Rahman. "AI-Powered Smart Home Automation: Enhancing Security, Energy Efficiency, And User Experience In Modern Housing." American Journal of Interdisciplinary Studies 6.02 (2025): 76-114.
21. Eduku, Stephen, et al. "Design and Implementation of a Voice-Controlled Smart Home Automation System." International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN (2025): 2278-3075.
22. Gayathri, M., Ch Lohith, and Ch Nanda Vaibhav. "Home Automation Using Gestures and Speech Recognition." 2025 6th International Conference on Inventive Research in Computing Applications (ICIRCA). IEEE, 2025.