VIVA-TECH IJRI
ANNUAL RESEARCH JOURNAL

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

SURVEY ON SMART HOME AUTOMATION

Vaishnavi Pisal[1], Aasmi Jugari[2], Sahil Kadam[3], Prof. Kirtida Naik[4]

[1](Department Computer Engineering, Mumbai University, India)
[2](Department Computer Engineering, Mumbai University, India)
[3](Department Computer Engineering, Mumbai University, India)
[4](Professor, Department Computer Engineering, Mumbai University, India)

Abstract: *This smart automation system enhances energy efficiency and convenience in homes and offices. Utilizing a camera-based detection mechanism, it monitors room occupancy and automatically turns off appliances like lights and fans when no one is present, reducing energy waste. At its core, the NodeMCU ESP8266 processes input from the camera and controls appliances via relay modules. A ZMPT101B voltage sensor monitors electrical status to ensure safe operation. The system integrates with Blynk.io, enabling remote control through mobile and web interfaces. Additionally, voice commands via Google Assistant and automation through IFTTT enhance usability. The system also features a soil moisture sensor and water pump for automated garden irrigation, along with a magnetic door lock for improved security. By combining energy conservation with modern IoT technology, this solution offers remote monitoring, voice control, and task automation. Scalable and versatile, it effectively meets the demands of smart home and office environments.*

Keywords - *Automation, Energy efficiency, IoT, Smart home, Voice control.*

I. INTRODUCTION

The widespread adoption of smart home technology, driven by advancements in the Internet of Things (IoT), has revolutionized how users interact with their living spaces. These systems enhance convenience, security, and energy efficiency through automation and remote control. However, despite their benefits, smart homes face significant challenges in automation reliability, cybersecurity, and energy management, which must be addressed to improve their performance and adoption. One of the primary concerns is automation consistency. As smart home environments become more interconnected, managing multiple device interactions can lead to conflicts, causing unpredictable system behavior. Research efforts have focused on developing intelligent automation frameworks that analyze and resolve conflicts dynamically, ensuring a smoother user experience. Security remains another critical issue, as many IoT devices lack robust protection mechanisms, making them vulnerable to cyber threats. Unauthorized access, weak authentication protocols, and insecure communication channels pose risks to user privacy and device functionality. To counter these challenges, modern smart home models incorporate stronger encryption techniques, AI-driven intrusion detection, and blockchain-based security protocols to fortify system defenses. Emerging security advancements such as quantum encryption and zero-trust security models are gaining attention for their potential to further enhance smart home security. Quantum encryption offers unbreakable data protection by leveraging quantum mechanics, while zero-trust models operate on the principle of never trusting any device by default, requiring continuous verification even for internal network devices. Integrating such future-ready security measures can mitigate evolving cyber threats and safeguard smart home ecosystems. Additionally, energy efficiency is a growing concern, as the increasing number of connected devices contributes to higher power consumption. Advanced energy management systems leverage artificial intelligence and predictive analytics to optimize energy use, adapting automation based on real-time usage patterns. These solutions not only reduce energy waste but also enhance the sustainability of smart home ecosystems. Furthermore, interoperability issues persist due to the diverse range of devices from different manufacturers. Standardization efforts and open-source platforms are helping bridge this gap, but they introduce new complexities in ensuring seamless integration and security. Emerging solutions, such as voice-controlled automation and AI-driven scripting systems, aim to simplify user interactions and enhance overall system flexibility. As research in smart home automation advances, integrating robust security measures, intelligent automation management, and energy-efficient solutions will be crucial in shaping the next generation of smart homes. These improvements will ensure that smart homes are not only more secure and reliable but also adaptable to evolving user needs and technological advancements.

II. REVIEW OF LITERATURE SURVEY

A survey was done on the existing literature and products to find out their shortcomings and research gaps in their systems. This survey consisted of 15 literature papers where the most relevant ones are listed below.

Adeeb Mansoor Ansari, Mohammed Nazir and Khurram Mustafa [1] introduces an innovative ontology-based method to address conflicts in automation rules within smart homes. Conflicts between automation rules can lead to erratic or unreliable behavior of devices. The proposed framework utilizes semantic web technologies to create models of interactions between devices, rules, and services. By analyzing these relationships, the system can identify conflicts as they arise and offer solutions promptly. This approach helps maintain consistency in rule execution, boosting the reliability and efficiency of smart home systems. It has significant implications for optimizing energy use, security measures, and user comfort, offering a more seamless experience for users.

Siok Wah Tay and Ning Zhang [2] focus on addressing the security challenges within existing smart home systems, which often prioritize convenience at the expense of robust protection. Their research emphasizes the need for a secure, communication-based authorization mechanism to control access to smart devices, preventing unauthorized usage. The authors propose a comprehensive model for smart home automation, factoring in device control, communication, and security. They explore various potential vulnerabilities in the authorization process and suggest the importance of establishing secure and effective access control systems. This work lays the foundation for enhancing the security and reliability of smart home automation, ensuring that privacy and user safety are maintained.

Ghazaleh Sarbishaei and Farahnaz Jowshan [3] The Internet of Things (IoT) has rapidly expanded with the increasing use of communication technologies, enhancing various sectors such as smart homes, healthcare, and transportation. In smart homes, IoT enables remote control of devices like thermostats, lights, and security cameras, offering convenience and energy efficiency. However, security remains a concern as IoT devices communicate over potentially insecure channels. To address this, efficient authentication protocols are essential. This paper introduces a lightweight multi-factor authentication scheme for smart homes, featuring mutual authentication between users, devices, and gateways. Key contributions include a new classification for IoT authentication schemes, a secure protocol using PUF chips, and a comparative analysis showing superior performance. The proposed system enhances IoT security without compromising efficiency, offering a scalable solution for smart home applications.

Aaesha Aldahmania and Bassem Ouni [4] examine the cybersecurity vulnerabilities in IoT devices used in smart homes, noting that these devices are increasingly at risk due to their limited processing capabilities and the lack of standardized security protocols. Their research highlights critical challenges, including the susceptibility of devices to cyberattacks and the necessity for robust protection measures like secure boot processes, encryption, and intrusion detection systems. Additionally, the study explores the potential of artificial intelligence and blockchain technologies to bolster security in IoT environments. This work contributes valuable insights into ongoing efforts to enhance the cybersecurity framework for smart home ecosystems, ensuring better protection and resilience.

Iván Froiz-Míguez and Paula Fraga-Lamas [5] present a voice-controlled home automation system designed to support low-resource languages and edge IoT devices. This novel system, primarily intended for Galician, offers a flexible and affordable solution for home automation, even in resource-constrained environments. Utilizing a voice recognition module, the system allows users to control appliances using verbal commands. Its architecture is built on fog computing, enabling fast, real-time processing to minimize latency. The system's successful evaluation proves its effectiveness in controlling home devices, boasting high recognition accuracy. This setup is particularly beneficial for individuals with disabilities or elderly people who may struggle with traditional interfaces. The system's scalability and adaptability to resource-limited devices make it an ideal solution for broader home automation applications.

Jiayi Kuang, Gang Xue, Zeming Yan, and Jing Liu [6] propose an innovative method for automating smart homes by generating scripts tailored to control and integrate a wide range of devices smoothly. This advanced approach combines natural language processing (NLP) with machine learning algorithms to analyze user preferences and create custom automation scripts. Users simply provide their desired automation commands in natural language, and the system deciphers the input to determine the relevant devices, actions, and conditions. The system then generates a personalized script that can be executed within the smart home setup. As it learns from user interactions, the technique adapts to evolving preferences, making automation more efficient and time-saving. The system is designed to seamlessly work with different smart devices, ensuring a cohesive automation experience. Features such as script editing and debugging tools also allow users to refine scripts and troubleshoot any potential issues. This approach has the potential to transform smart home automation, making it more user-friendly and accessible, even for complex scenarios.

Thilo Sauter and Albert Treytl [7] The Internet of Things (IoT) has revolutionized how smart devices are designed, deployed, and used globally. With forecasts predicting tens of billions of IoT devices by 2025, IoT enables devices to communicate over ubiquitous networks, mainly wireless like Wi-Fi, LoRaWAN, and mobile communication. IoT's reach extends beyond consumer electronics to sectors like Industrial IoT (IIoT), where IoT-enabled sensors aid in plant monitoring and safety. However, IoT's integration into industrial systems brings security challenges, as traditional security models (e.g., defense-in-depth) do not align with IoT's flat, wireless, and often insecure communication. Security risks include outdated software, unencrypted protocols, and poor access control, all exacerbated by IoT's vast attack surface. For instance, devices might bypass firewalls or establish unauthorized communication channels. Security measures, including IoT network segmentation, device hardening, and proper authentication, are crucial to mitigate risks and protect IoT-integrated systems in both industrial and consumer contexts.

Simran Singh and Sourabh Anand [8] introduce an advanced energy management system for smart homes, leveraging neurocomputing-based models to forecast energy consumption and optimize usage. By analyzing time-series load data, the system offers highly accurate energy consumption forecasts, helping homeowners reduce energy waste and optimize their usage patterns. The neurocomputing approach learns from past usage behavior, making it adaptable to changing needs. The system's energy decomposition feature provides granular insights into energy consumption, allowing users to identify inefficiencies and take corrective measures. Additionally, its forecasting capabilities predict energy demand, which aids in proactive management of energy usage. This energy-efficient system could contribute significantly to a more sustainable future by reducing overall consumption.

Naba M. Allifah and Imran A. Zualkernan [9] focus on the evaluation of security practices for IoT devices used in smart homes. Their study assesses 30 widely used IoT devices from 15 manufacturers, uncovering several common security weaknesses such as weak passwords, outdated software, and insufficient encryption. The authors rank these devices based on their security vulnerabilities and provide recommendations to enhance their safety. Their findings emphasize the critical need for standardized security measures and more rigorous testing protocols to protect users' smart home systems from potential threats.

Yu-Hsiu Lin, Huei-Sheng Tang, Ting-Yu Shen, and Chih-Hsien Hsia [10] review the state of smart home automation systems, focusing on key aspects such as system architecture, communication protocols, and automation technologies. The review highlights the role of artificial intelligence and the Internet of Things (IoT) in enhancing smart home systems. It emphasizes the need for security, privacy, and interoperability while addressing challenges like system complexity and energy efficiency. The authors also examine the diverse applications of smart home automation in healthcare, energy management, and home security, with an emphasis on improving the quality of life for people with disabilities or elderly individuals. This review serves as a crucial resource for those involved in the development of smart home systems, guiding future research and innovation.

Brian Setz, Sebastian Graef, and Desislava Ivanova [11] provide an in-depth evaluation of 20 open-source home automation systems, comparing them across features, design architecture, and usability. Their analysis outlines the strengths and limitations of several leading systems, offering guidance on selecting the best solutions based on different user requirements. The study also delves into the challenges associated with open-source platforms, such as their complexity and potential compatibility issues with certain devices. Their comprehensive review serves as an informative resource for developers and consumers interested in leveraging open-source solutions for home automation.

Muhammad Javed Iqbal, Muhammad Munwar Iqbal, Iftikhar Ahmad, and Muneer Ahmad [12] propose an intelligent electricity distribution system for smart homes, which incorporates artificial intelligence, IoT, and smart grid technology to optimize energy consumption. The system analyzes real-time data from smart meters, coupled with user preferences, to distribute electricity efficiently, reducing peak demand and minimizing waste. By adapting to the user's habits and offering personalized automation options, the system significantly improves energy efficiency. This smart approach has the potential to lower energy costs while contributing to a more sustainable and optimized home environment.

R. R. Thirrunavukkarasu, S. Mohan Kumar, and S. Ganesh Prabhu. [13] This paper explores a gesture-based drawing application that uses real-time hand tracking to transform hand movements into digital strokes, allowing users to interact with a canvas without traditional input devices. The system compares the user's drawing with a target shape and provides immediate feedback on its accuracy, fostering learning and improvement. With an intuitive interface, users are guided through the drawing process, enabling them to start, stop, and reset their creations with ease. The application is particularly beneficial for enhancing shape recognition and fine motor skills, especially for children, making it suitable for educational purposes. By incorporating a gamified approach, it encourages creativity and motivates users to practice their drawing skills in a fun and interactive environment. The system's real-time evaluation, powered by advanced computer vision algorithms, ensures that users receive instant and accurate feedback, helping them refine their drawings and achieve greater precision. This approach not only enhances educational outcomes but also has broader applications in virtual learning settings, offering versatility in both formal and informal education. The combination of interactive learning and advanced technology enables users to develop creative, motor, and cognitive skills in an engaging and effective manner.

Aaqib Raza and Mazhar H.Baloch [14] Automation technology plays a crucial role in daily life, with applications in fields such as industrial automation, appliance control, security, and more. Home automation systems, particularly those for elderly and disabled individuals, aim to provide easy interfaces to control and monitor home appliances. This system uses a combination of smartphones and embedded technology, including Arduino, Bluetooth, and relay modules. The system allows users to control home appliances via a mobile app or programmable controls. Arduino acts as the microcontroller, processing commands from the app through Bluetooth. The relay module acts as an electrically operated switch for appliances, while the app provides a user-friendly interface for control. The system is designed for efficiency, affordability, and ease of use. It is based on Bluetooth wireless communication and can be modified easily. By using Arduino and Bluetooth, it offers a low-cost, reliable solution for home automation, improving convenience and energy management.

Waheb A. Jabbar [15] describes the development and implementation of an affordable IoT-based smart home automation system that can be controlled through a smartphone or web browser. The system integrates Arduino Mega 2560 and Raspberry Pi 3 Model B+ with sensors to monitor and control various home devices. It provides users with remote access via the Blynk IoT platform, allowing for efficient energy management, increased security, and enhanced convenience. This hybrid system, offering both manual and automated control modes, demonstrates the potential to transform traditional homes into smart homes, promoting energy efficiency and improving quality of life.

III. DISCUSSIONS AND EVALUATION

The review of existing literature highlights significant advancements and persistent challenges in smart home automation. Various studies emphasize the need for robust security mechanisms, as IoT devices remain vulnerable to cyber threats due to weak authentication and outdated software. Researchers have explored solutions such as multi-factor authentication, encryption protocols, and AI-driven threat detection to enhance system security. Emerging security technologies such as quantum encryption and zero-trust security models are also gaining attention as future approaches to further strengthen smart home security. Another key concern is interoperability, where different smart devices and communication protocols often lack seamless integration, necessitating open-source platforms and standardized frameworks. The evaluation of the surveyed literature revealed that while open-source platforms provide flexibility, they often require technical expertise for setup and maintenance, limiting their accessibility to non-expert users. Standardization efforts are still evolving, and achieving true interoperability remains an ongoing challenge. Additionally, energy efficiency has been a major research focus, with AI-based forecasting models and automated energy management systems proving effective in optimizing consumption. Intelligent electricity distribution systems and smart grid integration have demonstrated potential to reduce peak-hour demand and improve overall energy efficiency. However, the deployment of these systems often demands high computational resources and real-time data availability, which can pose practical limitations. Automation reliability is another vital aspect. Studies addressing automation conflicts have introduced ontology-based conflict detection frameworks and AI-driven scripting systems. These approaches contribute to a more intuitive and user-friendly experience by ensuring consistent device behavior and enabling custom automation tailored to user preferences. Voice-controlled systems and natural language processing further enhance accessibility, especially for individuals with disabilities. Despite these advancements, gaps remain in ensuring cost-effective, scalable, and universally accessible smart home solutions. Security concerns continue to evolve as cyber threats become increasingly sophisticated, requiring continuous improvement in security protocols. Future research must prioritize hybrid approaches combining AI, IoT, and blockchain technologies while maintaining affordability and ease of deployment. The evaluation approach in this survey paper focused on identifying key enabling technologies such as AI, Blockchain, Natural Language Processing (NLP), and Security Protocols to assess their effectiveness in addressing the challenges faced by smart home automation systems. By addressing these concerns and leveraging cutting-edge technologies, smart home ecosystems can evolve into more reliable, secure, and intelligent living environments that cater to diverse user needs.

IV. ANALYSIS

Table 1: Analysis Table

Sr No	Year	Technology	Advantages	Disadvantages
[1]	(2024)	1.Ontology-Based Conflict Detection Frameworks 2. Semantic Web Technologies	1.Enables structured identification and resolution of rule conflicts. 2. Ensures reliability by maintaining consistent automation rules.	1.Building and managing ontologies require specialized knowledge and expertise.
[2]	(2024)	1.Secure Communication Protocols 2.Authentication Frameworks	1.Delivers secure communication and authorization mechanisms in smart homes. 2. Balances ease of use with robust security standards.	1.Complex implementation requiring security expertise. 2.Additional resource consumption or latency introduced by security protocols.
[3]	(2024)	1.Neurocomputing for Load Forecasting 2.AI-Driven Energy Optimization 3.Smart Grid Integration	1.Enhances energy load forecasting accuracy using advanced techniques. 2. Reduces energy costs optimizing consumption patterns.	1. High computational demands and complexity in modeling. 2.Substantial storage and processing power requirements.
[3]	(2023)	1.Embedded IoT Security Protocols 2.AI-Based Threat Detection	1.Strengthens device security to combat cyber threats.	1. Requires expertise for developing and managing comprehensive security measures.
[5]	(2023)	1.Edge Computing for Speech Recognition 2.IoT-Integrated Voice Control	1.Facilitates voice-controlled automation in low-resource languages. 2. Provides hands-free convenience for users.	1.Lower recognition accuracy for lesser-used languages. 2.Limited processing power of edge devices may impact system performance.
[6]	(2023)	1.AI-Powered Automation Scripting 2. Natural Language Processing for Rule Generation	1.Personalizes automation scripts for user needs. 2. Optimizes energy use and automates daily tasks.	1.Script management can be challenging for non-technical users. 2.Scripts may malfunction without thorough testing.
[7]	(2023)	1.IoT Sensors 2. Security Protocols	1.Identifies security challenges specific to IoT sensors in automation systems.	1. Advanced knowledge of IoT security is necessary. 2.Implementation of

			2.Proposes countermeasures to mitigate these challenges.	countermeasures may require significant resources.
[8]	(2023)	1.IoT Platforms 2. Home Automation Hubs 3. Sensors and Actuators	1.Automates daily tasks, making life more efficient. 2.Optimizes energy use, leading to cost savings.	1.High setup and maintenance costs for advanced systems. 2. Configuration may be complex and time-intensive.
[9]	(2022)	1.IoT Security Frameworks 2.Wireless Communication Protocols	1. Enhances automation and energy efficiency in IoT devices.	1. Vulnerable to hacking due to weak security measures.
[10]	(2022)	1.Multi-Factor Authentication (MFA) 2.Cryptographic Protocols	1. Enhances security by incorporating multiple layers of authentication. 2. Protects smart home systems from unauthorized access and data breaches.	1.Increased complexity in setup and usage for users. 2. May introduce delays in authentication processes due to multiple layers of verification.
[11]	(2021)	1. Open-Source Home Automation Frameworks	1.Supports numerous devices and services, ensuring versatility. 2.Large active community provides support and updates.	1.Challenging for beginners to configure. 2. Significant computing resources are necessary for optimal performance.
[12]	(2021)	1.Intelligent Electricity Dispatch Systems 2.AI-Driven Energy Distribution	1.Enables real-time data-based automation, optimizing energy use. 2.Operates locally, ensuring data privacy and faster response times.	1.Initial configuration may be challenging. 2. Energy dispatch rules require technical expertise and resources.
[13]	(2021)	1. IoT Customization Platforms 2. Personalized Smart Home Systems	1. Tailors automation to user preferences. 2.Provides better integration with existing smart home devices.	1. Limited scalability for large-scale applications. 2. Interoperability issues may arise with devices from different manufacturers.
[14]	(2020)	1.Arduino-Based Home Automation 2. Mobile App Control	1.Simple and affordable solution for basic home automation tasks. 2.Easy to use for beginners.	1. Limited range and functionality due to Bluetooth communication. 2.Not suitable for complex smart home scenarios.

[15]	(2019)	1.IoT-Based Automation Systems 2.Sensors and Actuators	1.Provides enhanced control over home devices. 2. Improves energy efficiency and convenience.	1. High setup cost for IoT infrastructure. 2. Potential privacy and security concerns.

V. CONCLUSION

The rapid evolution of smart home technologies has significantly enhanced convenience, energy efficiency, and security. However, challenges such as cybersecurity threats, automation rule conflicts, and interoperability issues remain critical concerns. Addressing these challenges requires a multi-faceted approach, including blockchain-based authentication, AI-driven automation reliability frameworks, and advanced encryption techniques to secure IoT devices. Research further emphasizes the need for AI-based energy optimization systems and adaptive learning models to personalize automation based on user behavior. Additionally, the development of global interoperability standards and the adoption of open-source platforms can improve smart home device compatibility and scalability. By integrating these innovations, smart home ecosystems can become more resilient, secure, and user-centric**,** ensuring they meet the evolving demands of modern users.

REFERENCES

[1] A. M. Ansari, M. Nazir and K. Mustafa, "Ontology-Based Classification and Detection of the Smart Home Automation Rules Conflicts," in *IEEE Access*, vol. 12, pp. 85072-85088, 2024.

[2] S. W. Tay, N. Zhang and S. AlJanah, "A Problem Analysis of Smart Home Automation: Toward Secure and Usable Communication-Based Authorization," in *IEEE Access*, vol. 12, pp. 18103-18121, 2024.

[3] G. Sarbishaei, A. Masoud Aminian Modarres, F. Jowshan, F. Zahra Khakzad and H. Mokhtari, "Smart Home Security: An Efficient Multi-Factor Authentication Protocol," in *IEEE Access*, vol. 12, pp. 106253-106272, 2024.

[4] A. Aldahmani, B. Ouni, T. Lestable and M. Debbah, "Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends," in *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 281-292, 2023.

[5] I. Froiz-Míguez, P. Fraga-Lamas and T. M. Fernández-CaraméS, "Design, Implementation, and Practical Evaluation of a Voice Recognition Based IoT Home Automation System for Low-Resource Languages and Resource-Constrained Edge IoT Devices: A System for Galician and Mobile Opportunistic Scenarios," in *IEEE Access*, vol. 11, pp. 63623-63649, 2023.

[6] J. Kuang, G. Xue, Z. Yan and J. Liu, "An Automation Script Generation Technique for the Smart Home," in *Journal of Web Engineering*, vol. 22, no. 2, pp. 221-254, March 2023.

[7] T. Sauter and A. Treytl, "IoT-Enabled Sensors in Automation Systems and Their Security Challenges," in *IEEE Sensors Letters*, vol. 7, no. 12, pp. 1-4, Dec. 2023.

[8] Singh, Simar & Anand, Sourabh & Satyarthi, Manoj. (2023). A Comprehensive Review of Smart Home Automation Systems. 61-66.

[9] N. M. Allifah and I. A. Zualkernan, "Ranking Security of IoT-Based Smart Home Consumer Devices," in *IEEE Access*, vol. 10, pp. 18352-18369, 2022.

[10] Y. H. Lin, H. -S. Tang, T. Y. Shen and C. -H. Hsia, "A Smart Home Energy Management System Utilizing Neurocomputing-Based Time-Series Load Modeling and Forecasting Facilitated by Energy Decomposition for Smart Home Automation," in *IEEE Access*, vol. 10, pp. 116747-116765, 2022.

[11] B. Setz, S. Graef, D. Ivanova, A. Tiessen and M. Aiello, "A Comparison of Open-Source Home Automation Systems," in *IEEE Access*, vol. 9, pp. 167332-167352, 2021

[12] M. J. Iqbal *et al*., "Smart Home Automation Using Intelligent Electricity Dispatch," in *IEEE Access*, vol. 9, pp. 118077-118086, 2021.

[13] R. R. Thirrunavukkarasu, S. Mohan Kumar, P. Praveen, T. Meera Devi, S. Pradeep and S. Ganesh Prabu, "Customization In Home Automation Using IoT," *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, 2021

[14] A. Raza *et al*., "A Home Automation Through Android Mobile App By Using Arduino UNO," *2020 IEEE 23rd International Multitopic Conference (INMIC)*, Bahawalpur, Pakistan, 2020

[15] W. A. Jabbar *et al*., "Design and Fabrication of Smart Home With Internet of Things Enabled Automation System," in *IEEE Access*, vol. 7, pp. 144059-144074, 2019.