International Journal of Reconfigurable and Embedded Systems (IJRES)
Vol. 15, No. 2, July 2026, pp. 406~415
ISSN: 2089-4864, DOI: 10.11591/ijres.v15.i2.pp406-415

Matter protocol-enabled device onboarding for cross-platform internet of things systems

Geetishree Mishra, Hemavathi, Harish V Mekali
Department of Electronics and Communication Engineering, B.M.S. College of Engineering, Bengaluru, India

Article Info

Article history:

Received Jan 5, 2026
Revised Mar 18, 2026
Accepted May 30, 2026

Keywords:

Cross-platform
Ecosystem
Internet of things
Interoperability
Matter protocol

ABSTRACT

The Matter protocol, created by the connectivity standards alliance (CSA), comes in with a single standard to make sure these devices can connect and be controlled across platforms like Google Home, Apple HomeKit, Amazon Alexa, and Samsung SmartThings. The rapid expansion of the internet of things (IoT) is driving the urgent need for secure and efficient onboarding processes for a wide range of connected devices. It necessitates a robust framework to seamlessly integrate new additions into existing systems while upholding security standards. This initiative focuses on implementing the Matter protocol on ESP32 devices, employing a Raspberry Pi hub as the central communication point to facilitate smooth device-to-hub interactions. This work presents the onboarding devices for interconnected IoT systems using the Matter protocol. The Matter device is configured and tested within the Amazon ecosystem using an Alexa Echo Dot, as well as with the smart home assistant ecosystem along with a smartphone application. By configuring the Raspberry Pi hub as a designated Matter hub and exploring interactions within the home assistant ecosystem supporting diverse platforms like Apple HomeKit and Google Home, the work enhanced interoperability and broadened the utility of IoT devices within an interconnected network. This initiative forges a foundation for an adaptable and cohesive IoT environment.

Corresponding Author:

Geetishree Mishra
Department of Electronics and Communication Engineering, B.M.S. College of Engineering
Bull Temple Road, Bengaluru -560019, Karnataka, India
Email: geetishreemishra.ece@bmsce.ac.in

1. INTRODUCTION

The Matter protocol is a communication protocol for smart home devices. It provides a standardized and secure method of communication between smart devices, regardless of the brand or manufacturer. The introduction of Matter protocol in 2022, formerly known as project connected home over IP (CHIP), marks a significant step towards resolving interoperability challenges, backed by leading industries Amazon, Apple, and Google. The standard will also include emerging technologies such as blockchain for device certification and security. Matter represents an open-source standard designed to facilitate seamless integration and communication among smart devices. This protocol allows diverse devices and ecosystems to cooperate harmoniously. Manufacturers must adhere to the Matter standard to ensure their devices can operate with smart home and voice services like Amazon's Alexa, Apple's Siri, and Google's Assistant. Matter-compatible devices can work seamlessly with these platforms without the need for additional bridges or hubs. It also means that users can mix and match devices from different brands and manufacturers without worrying about compatibility issues. Employing wireless fidelity (Wi-Fi) and Thread network layers, the initial protocol employs Bluetooth low energy (BLE) for device configuration. Since Matter operates within

the local network, enhanced responsiveness is expected from smart home devices, ensuring continued functionality even during internet outages.

For transport, Matter uses Wi-Fi, Ethernet, and the Thread networking protocol, which is an IPv6-based wireless networking protocol designed for low-power devices (Figure 1). Thread provides a reliable and secure network for smart home devices, and it is optimized for devices with limited processing power and memory. Most Thread devices powered from the main supply can act as Thread mesh extenders (Thread routers) that expand the network's range and resilience as shown in Figure 1. Thread automatically adapts to devices being added or removed from the network [1].

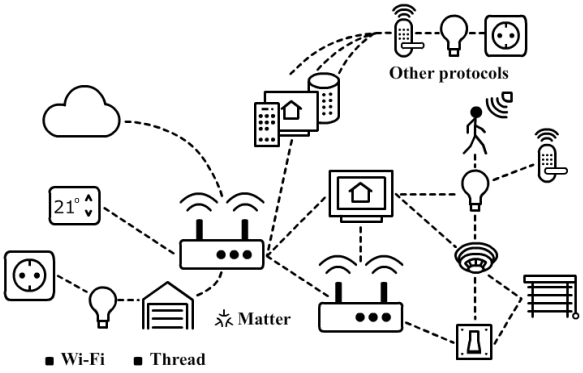


Figure 1. A Matter network using Wi-Fi and Thread connectivity

There are several advantages to the Matter protocol that make it a significant step towards creating a more unified smart home ecosystem. Here are some of the key advantages such as interoperability, security, multi-admin feature, simplified setup, industry support, backward compatibility, and improved user experience. The Matter protocol is designed to be scalable and flexible, which makes it suitable not just for use in the home, but also industrial and commercial environments. Matter can be used to create smart building systems that can help improve efficiency, reduce energy consumption, and enhance overall safety and security. The Matter protocol's focus on interoperability and ease of use makes it an attractive option for commercial and industrial settings, where there may be a variety of different devices and systems from different manufacturers in use [1]. The lack of interoperability among the ecosystems results in increased costs and support burdens for manufacturers and developers, who must allocate additional resources to sustain multiple ecosystems, thereby intensifying operational complexity and overhead.

The Matter accessory device can be remotely controlled over IPv6 network with the help of a Matter controller interfaced with BLE to establish a smart home ecosystem. Matter controller configured as a smart home hub along with the standalone devices that are equipped with the necessary hardware and software manages the smart home ecosystem. There are several apps available that can connect to Matter controllers, allowing users to control their smart home ecosystem directly from their mobile device. The app provides a user interface to communicate with Matter devices and manage their activities [2].

Z-Wave, or Zigbee enabled devices are required to be firmware upgraded to be matter compliant. According to the Alliance, 1,214 devices connected majorly to various home appliances have been certified as of October 2023. In this work a testbed is built which presents the architecture of the network for automated smart home utilizing cloud services. This architecture helps in exploring various aspects such as acquired data analysis, security and privacy issues in a smart home ecosystem built on Matter protocol.

For developers to create, publish, maintain, monitor, and secure APIs, Amazon Web Services (AWS) API gateway is a well managed service provider. Figure 1 shows Matter protocol enabled internet of things (IoT) devices of the smart home connected to the cloud platform that is AWS though this architecture can also function with other cloud services such as Microsoft, Google, or Oracle. AWS elastic kubernetes service (EKS), infrastructure-as-aservice (IaaS) can be provided to the smart homeowners on rent to create and operate Kubernetes clusters. AWS active directory enables directory-aware workloads and AWS cognito provides easy and secure access to the management of EKS. AWS S3 is object storage and AWS athena is an interactive platform in the web-based cloud storage service. The matter protocol testbed used in this work successfully demonstrated a smart door lock system using the J-Link real-time transfer (RTT) viewer. By elucidating Matter's functionality, it becomes evident that controllers and devices within a Matter network exhibits compatibility, fostering efficient and cohesive operations.

The research aims to:

- Explain the functionality of Matter, detailing the compatibility of controllers and devices within a Matter network.
- Highlight the benefits of using the Matter protocol for smart device communication.
- Explore the connectivity and communication processes of Matter-enabled devices.
- Evaluate how Matter facilitates smooth interoperability between devices of diverse manufacturers.

This work aims to improve the communication strategy for linking a singular Matter- enabled device with various ecosystems, regardless of differences in manufacturers and product types. In this work the Matter server is established on Raspberry Pi and integrating Matter devices tested within the Amazon ecosystem using an Alexa Echo Dot, as well as with the smart home assistant ecosystem. The demonstrated framework serves as a step towards achieving a universal IoT standard.

2. LITERATURE SURVEY

Emphasizing a security-by-design approach to ensure device resilience explores an automated and secure onboarding for system of systems (SoS) within IoT [3]. It highlights the use of service-oriented architecture (SoA) and the Eclipse Arrowhead framework for secure onboarding while addressing challenges in deployment and trust management. Which validates its approach through a smart charging use case. Matter standard, developed to resolve interoperability, security, and connectivity challenges in smart home ecosystems [4]. It emphasizes Matter's IP-based framework that unifies communication across devices and brands, simplifying installation and improving user trust. Matter standard establishes a unified, secure, and interoperable foundation for IoT and smart home devices [5]. Built on IP-based technologies like Wi-Fi, Ethernet, and Thread, Matter integrates strong cybersecurity and privacy principles aligned with general data protection regulation (GDPR) and global regulations.

The evolution of smart home connectivity from early automation efforts to today's IoT-driven era and introduces Matter as a unifying layer ensuring seamless interoperability [6]. Matter harmonizes diverse technologies—Ethernet, Wi-Fi, and Thread—under a single IP-based standard to overcome fragmentation caused by proprietary protocols. STMicroelectronics supports this initiative through its STM32WB series, accelerating Matter-based product development for a more connected and standardized smart home future. Security testing for the Matter protocol through fuzzing, used as a technique to uncover vulnerabilities in embedded systems [7]. The framework identifies bugs across Matter's seven-layer stack, supporting open-source collaboration to strengthen interoperability, reliability, and resilience in the smart home ecosystem. Wi-Fi technology extends beyond communication to perform environmental sensing tasks in smart homes [8]. The paper reviews recent advancements leveraging signal variations for activity tracking and contextual awareness, demonstrating Wi-Fi's potential to enhance smart home intelligence, adaptability, and user experience, marking a significant shift towards more efficient and user-friendly home automation systems.

A comprehensive model has analyzed the performance of compound transmission control protocol (C-TCP) in Industry 4.0 Wi-Fi networks, considering factors like packet loss, media access control (MAC-layer) collisions, and access point buffer overflows [9]. By integrating intelligent methods, the paper demonstrates improved performance and adaptability of industrial wireless communication systems under complex, real-world network conditions. The best practices for secure device onboarding and provisioning in industrial IoT (IIoT) environments have been studied [10]. The paper serves as a guideline for system integrators and service providers, focusing on cost-effective, secure, and reliable deployment methods aligned with modern IIoT requirements. Matter protocol as a unified standard designed to resolve interoperability and security challenges in smart home networks has been presented [11]. The study presents a hardware testbed and network architecture demonstrating Matter-based smart home automation, focusing on efficient cloud integration and data management.

The evolving security and privacy challenges in smart homes as IoT devices become increasingly interconnected have been presented [12]. The authors analyze threats across all layers of a smart-home ecosystem from sensing devices and communication networks to cloud services and user applications. The middleware platforms for the IoT explains how they act as a crucial bridge between heterogeneous devices, networks, and applications highlighting limitations [13], [14] for large-scale IoT deployments. Automating secure network onboarding of IoT devices introduces mechanisms such as per-device network credentials, zero-touch onboarding, configurable trust policies, and continuous assurance [15]. It offers a foundational framework of Matter within the context of secure onboarding for network-layer lifecycle management. Embedding zero-trust security into foundation models (FMs) used throughout IoT systems [16]. Artificial intelligence (AI-powered) IoT systems can maintain decentralized trust. Though not directly Matter-related, their blueprint for zero-trust onboarding and behavioral integrity highlights practical security enhancements that could augment Matter-based ecosystems especially in edge intelligence and autonomous device

management. Lightweight large language models (LLMs) tailored for IoT threat detection and mitigation [17]. They show how fine-tuned LLMs, deployed in a modular, dockerized architecture, can detect anomalies and initiate context-aware responses in real time all optimized for resource-constrained devices.

A secure architecture for sensor networks based on IEEE P1451.1.6, leveraging the broader P1451.0 security framework has been proposed [18]. It demonstrates how standard-based security models can be embedded at the device level complementing Matter's ecosystem with structured metadata and fine-grained access control, especially in mixed or industrial environments. Generative AI (GenAI) techniques can both fortify and threaten IoT security [19]. Through an in-depth survey and case studies, potential applications such as synthetic data generation for training, anomaly detection, and predictive threat modeling, while also acknowledging risks like adversarial manipulation have been highligted. An empirical comparison of smart-home devices implemented with Matter, evaluating compatibility, performance, and usability across ecosystems has been presented [20]. Although full details require access, the study reinforces the practical maturity of Matter in real-world deployments aligning closely with testbed-based evaluations. Advancing the potential for smart home ecosystems in broader, cross-domain contexts has been verified with concrete groundwork [21]. The seamless integration of Matter devices into the one machine-to-machine (oneM2M) platform, enabling other applications to interact with them solely through one M2M standard interfaces has been demonstrated [22]–[25].

3. PROPOSED METHOD

The Matter protocol works by providing a standard language that smart home devices can use to communicate with each other. The language is based on open internet and networking standards, and it is designed to be interoperable across multiple devices and platforms. Matter uses the decentralized Thread networking protocol, which uses mesh topology for efficient communication over IPv6 based wireless network providing a reliable and secure network for smart home devices, with optimized processing power and memory usage. The initialization process for a new device addition to the matter network is quite simpler. It allows only authorized devices to join the network through an authentication device pairing. Once a device is connected to the Matter network, it can communicate with other devices using the Matter data model, a standard language used by smart home devices to communicate with each other. The Matter data model is designed to be interoperable with a wide range of platforms. Devices from different manufacturers can communicate with each other seamlessly, without the need for additional bridges or hubs. Figure 2 shows the flow diagram of the proposed method. The procedural flow goes like:

- Create a Matter server hub: in this step, a Matter server hub is established, running on a Raspberry Pi 3B+within a smart home assistant ecosystem.
- Create a Matter device: a Matter device is developed using an ESP32 development board. This device is assigned a unique product name and device ID for registration as a Matter device. This registration enables the device to connect and communicate with the Matter servers.
- Connect and control the Matter device: to effectively control the Matter device, both the device and the Matter server hub need to be connected to the same Wi-Fi network. Specific mobile applications are part of the ecosystem, facilitating easy access and control over the device. After the Matter device is commissioned and successfully linked to the Matter server hub, it can be controlled through various ecosystems like Amazon Alexa, Google Home, Apple HomeKit, or other compatible systems. This flow outlines the sequential actions involved in setting up a Matter server hub, creating a Matter device, and establishing the necessary connections for efficient control within a smart home ecosystem.

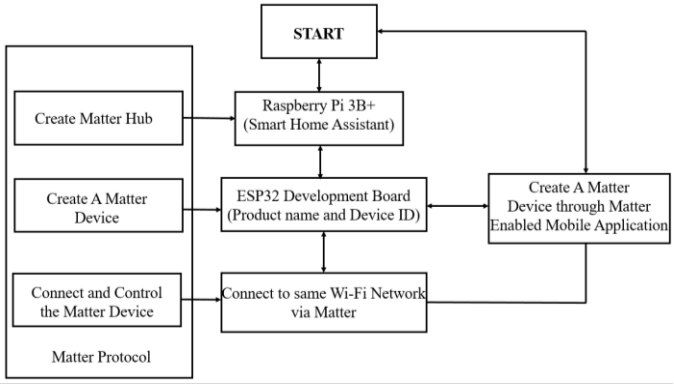


Figure 2. Flow diagram of proposed method

In the setup process, the creation of a Matter server hub is vital for seamless device communication within a smart home environment. This hub, hosted on a Raspberry Pi 3B+ device, serves as the central point for managing connected devices. Subsequently, the development of a Matter device, built using an ESP32 development board, is conducted. This device is uniquely identified with a product name and a device ID to enable registration within the Matter ecosystem. The complete workflow is depicted in Figure 3. This structured flow highlights the sequential actions involved in configuring a Matter server hub, designing a Matter device, and fostering connectivity to ensure efficient control and seamless integration within the broader smart home ecosystem.

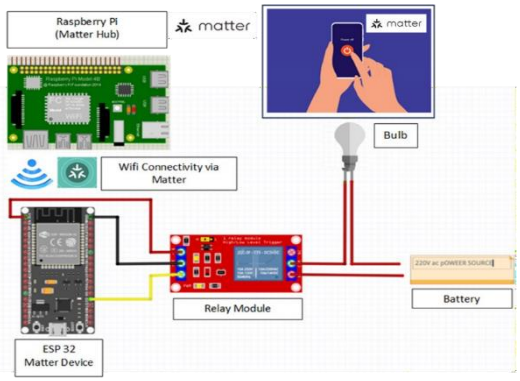


Figure 3. Implementation of Matter protocol

The ESP32 evaluation board is utilized to control the output spoofing by interfacing it with a general-purpose input/output (GPIO) pin. This connection enables the ESP32 to communicate with the Raspberry Pi network hub via Wi-Fi. Within this setup, the ESP32 functions as a "Matter" device distinguished by a specific device ID and a unique product name on the Raspberry Pi platform. The Raspberry Pi is specifically configured to run the home assistant operating system, which is integrated with support for the Matter protocol, serving as the central control hub for managing the ESP32 device. This registration is essential as it allows the device to establish connections with and communicate through the Matter servers, ensuring interoperability and functionality within the designated network.

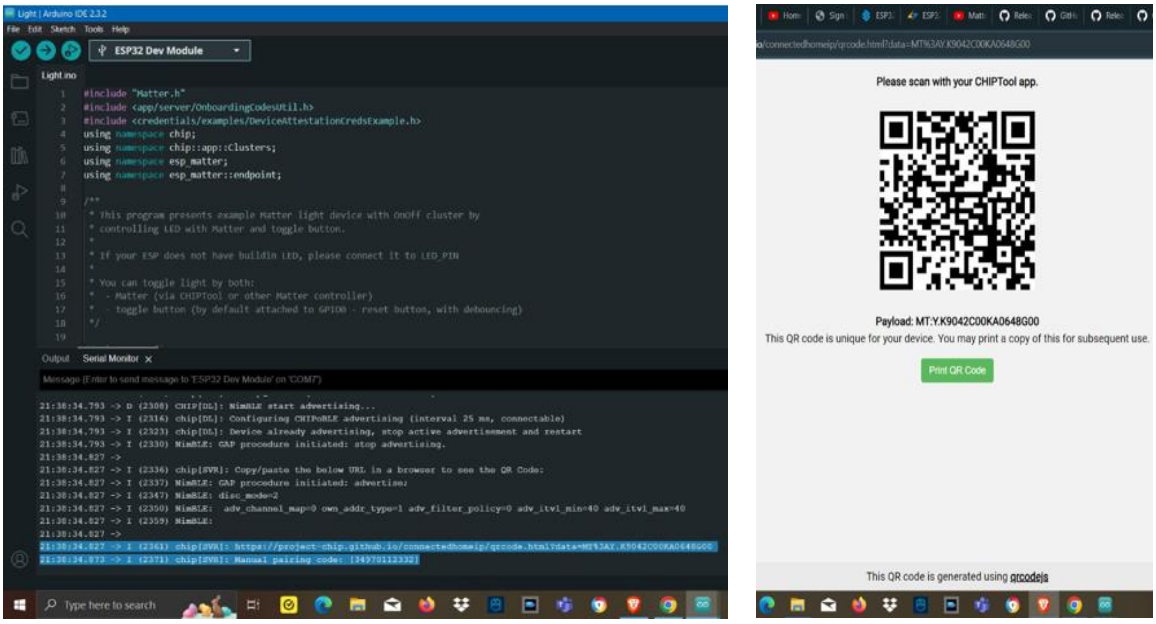
4. RESULTS AND DISCUSSION

The commissioning procedure at initializing a new device to the Matter network, starts with sending onboarding information to the controller which includes data of 27-bit setup passcode, 16-bit Product ID, 12-bit device discriminator and 8-bit discovery capabilities passcode as depicted in Figure 4. showing QR code in matter hub with two subdivisions Figure 4(a) depicting QR code for Matter device generated with product name and ID and Figure 4(b) shows registering the new Matter device via generating QR code in matter hub. Device commissioning steps as follows:

- Device discovery: new devices advertise their presence to the controller using any wireless communication protocol: BLE, domain name system- service discovery (DNS-SD), or Wi-Fi access point.
- Security setup: for establishing a secured session between devices the passcode-authenticated session establishment (PASE) protocol is used.
- Establish fail-safe: the new device backs up if the configured timer limit expires for the commissioning process.
- Preliminary node configuration: the new device is configured following the regulatory information by the controller including location and current universal time coordinated (UTC) time.
- Certificate verification: the controller checks validity of the new device considering the matter certification and attestation elements, the non compliance of which leads to verification failure.
- Install operational credentials: the node operation certificate (NOC) and operation ID are the essential elements for recognizing a device as a new node on the Matter fabric.
- Network commissioning: the controller connects new device to the operational network using credentials either through Wi-Fi or Thread.

- Operational discovery: using DNS-SD, the controller discovers the new node on the operational network.
- Security setup with CASE: for establishing a secured communication between devices the certificate-authenticated session establishment (CASE) protocol is used that is secured with a new pair of keys.
- Disarm fail-safe: the fail-safe timer is used by the new device to remove the configuration backup.

Post commissioning process, the new device is connected to the network and can start sending and receiving advanced encryption standard (AES)-encrypted messages.



(a) (b)

Figure 4. QR code in matter hub; (a) QR code for Matter device generated with product name and ID and (b) registering the new Matter device via generating QR code in matter hub

4.1. Set up the software environment for evaluation board

Espressif's software development kit (SDK) for Matter is built on top of the open source Matter SDK, provides simplified APIs, commonly used peripherals, tools, and utilities for security. The installation procedure of utility dependencies till the build flow of matter protocol and connecting various devices are given in steps as below:

- Install the dependencies, set up SDK (the espressif IoT development framework)
  $ sudo apt-get install git gcc g++ pkg-config libssl-dev libdbus-1-dev\libglib2.0-dev libavahi-client-dev ninja-build python3-venv python3-dev\python3-pip unzip libgirepository1.0-dev libcairo2-dev libreadline-dev screen
- Create a directory to contain the ESP-IDF
  $ mkdir ~/esp-idf_tools
- Clone the ESP-IDF from GitHub into this directory:
  $ cd ~/esp-idf_tools
  $ git clone -b v4.4.3 --recursive https://github.com/espressif/esp-idf.git
- Setup Matter SDK and Bootstrap the Matter development environment
  $ git clone https://github.com/project-chip/connectedhomeip.git
  $ cd ./connectedhomeip
  $ git fetch origin v1.0-branch
  $ git checkout FETCH_HEAD
- Create a new project in the Developer console by giving the product name and ID, device type and unique Vendor ID.
- Build the device, run the utility and program the device as depicted in Figure 5.
- A smart phone device to pair, connect and control as depicted in Figure 6.

In the process of verifying a Matter-enabled device within the smart home assistant ecosystem, detailed information about the device is prominently showcased on the dashboard (Figure 7). This facilitates

easy access and management for users, allowing them to monitor device status and configurations with clarity. Additionally, the integration of the Python Matter server plugin within the smart home assistant ecosystem is fully operational, enhancing compatibility and functionality. This plugin acts as a bridge, ensuring seamless communication between the Matter-enabled devices and the smart home assistant framework, thus enriching the overall user experience.

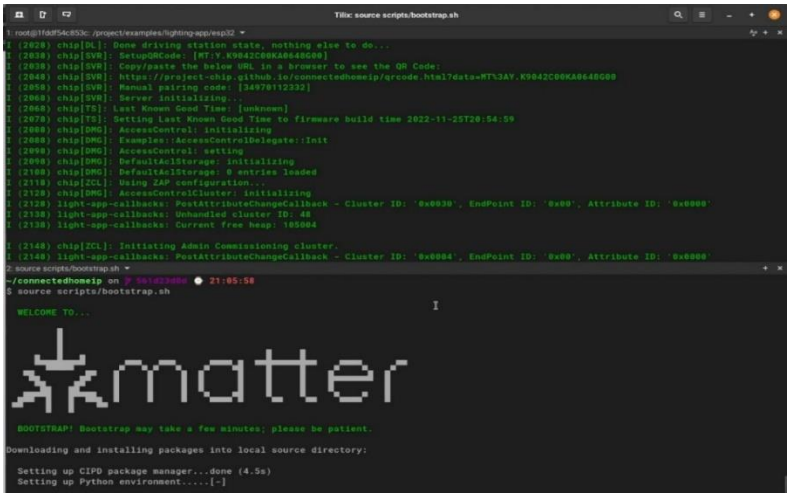


Figure 5. Building the Matter protocol

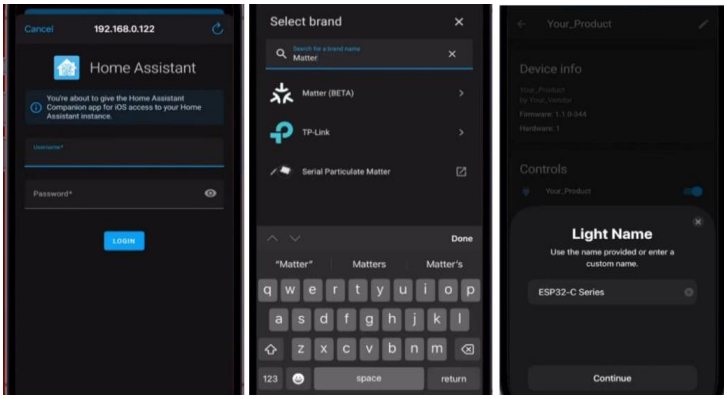


Figure 6. Setting up smart phone configuration for Matter device

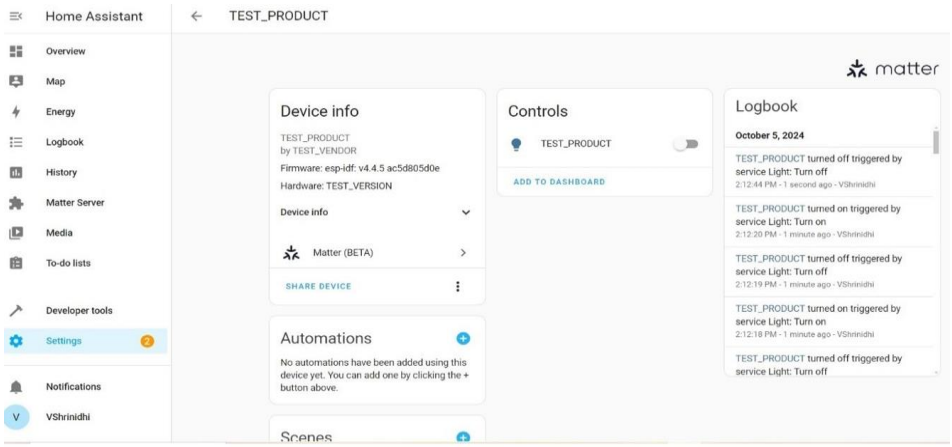


Figure 7. Home assistant ecosystem dashboard

Users can manage the ESP32 (Matter device) through the Raspberry Pi hub (running home assistant with Matter support). A smartphone connects to the hub via Wi-Fi, allowing users to add the ESP32 device to the mobile widget as shown in Figure 8. This enables control of the light emitting diode (LED) through a smartphone application using the Matter protocol.

The Amazon ecosystem includes the Amazon Alexa device Eco-Dot 3rd generation, which serves as a central hub for smart home management. Within this setup, the Matter-enabled ESP32 device has been configured and integrated. This allows the ESP32 to connect seamlessly to the Amazon Alexa ecosystem. Once connected, users can easily control the ESP32 device using either voice commands through the Amazon Alexa voice assistant or via the Amazon Alexa smartphone application. This versatility allows for convenient operation, whether at home or on the go.

Additionally, the Matter server is enabled by default within the host Amazon ecosystem, ensuring that the communication between the ESP32 and Amazon Alexa operates smoothly and efficiently. This setup leverages the benefits of the Matter framework, enhancing interoperability among smart devices and improving the overall user experience.

In this setup given in Figure 9 the Matter light effortlessly controlled using the voice assistant feature in Amazon Alexa. When the command, "Alexa, Turn ON/OFF Matter Light," was given the LED on the ESP32 (the Matter device) was functioning accordingly ON/OFF. This integration allowed for convenient voice-activated control of matter enabled device with amazon ecosystem.

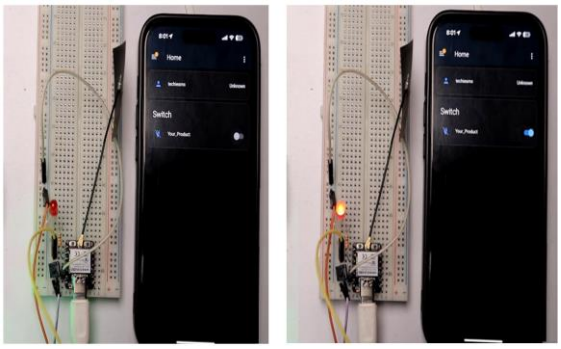


Figure 8. Controlling Esp32 C3 using a home assistant mobile application

Figure 9. Controlling Esp32 C3 using a Amazon Alexa voice assistant

5. CONCLUSION

This work presents a novel approach aimed at enhancing connectivity standards through the implementation of the Matter protocol. The central focus is on establishing a Matter server on the Raspberry Pi and seamlessly integrating Matter devices onto this server. In this work, the Matter device has been configured and tested within the Amazon ecosystem using an Alexa Echo Dot, as well as with the smart home assistant ecosystem. By configuring the Matter-enabled device to connect with the server or Matter hub, users gain direct control over the gadgets customized to their individual requirements. The primary objective was to provide interoperability, ensuring that the Matter-enabled device harmoniously interacts within diverse ecosystems such as Amazon Alexa, Google Home, and other platforms. This all-encompassing strategy improves the user experience and also sets the stage for a seamlessly interconnected IoT environment where devices communicate effortlessly across various platforms, ultimately paving the way for a smarter, more integrated future in the realm of IoT and smart home technologies.

The implementation highlights the transformative potential of Matter in realizing a truly interconnected and user-centric smart environment. By addressing existing challenges of compatibility and fragmented communication protocols, the work establishes a foundation for cross-platform collaboration among leading ecosystems such as Amazon, Google, and Apple. The demonstrated framework serves as a step towards achieving a universal IoT standard where devices communicate securely, efficiently, and intelligently, ultimately driving the integration of an adaptive smart home automation and IIoT systems.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Geetishree Mishra	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Hemavathi	✓		✓			✓	✓		✓	✓		✓		
Harish V Mekali						✓	✓	✓		✓	✓	✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

The protection of privacy is a legal right that must not be breached without individual informed consent. In cases where the identification of personal information is necessary for scientific reasons, authors should obtain full documentation of informed consent, including written permission from the patient prior to inclusion in the study. Incorporate the following (or a similar) statement: We have obtained informed consent from all individuals included in this study.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] A. Alshaeri and M. Younis, "Protocols for Secure Remote Access to Vehicle Onboard Diagnostic Systems in Smart Cities," *IEEE Intelligent Transportation Systems Magazine*, vol. 14, no. 5, pp. 209–221, Sep. 2022, doi: 10.1109/MITS.2022.3180688.

[2] W. Zegeye, A. Jemal, and K. Kornegay, "Connected Smart Home over Matter Protocol," in *2023 IEEE International Conference on Consumer Electronics (ICCE)*, IEEE, Jan. 2023, pp. 1–7, doi: 10.1109/ICCE56470.2023.10043520.

[3] S. Maksuti *et al.*, "Automated and Secure Onboarding for System of Systems," *IEEE Access*, vol. 9, pp. 111095–111113, 2021, doi: 10.1109/ACCESS.2021.3102280.

[4] Infineon Technologies AG, "The Matter Standard: Implementing Improved Security and Connectivity for the Smart Home," *White Paper*, 2022.

[5] N. Bak *et al.*, "Matter Security and Privacy Fundamentals," *CSA White Paper*, 2022.

[6] A. Mota, C. Serôdio, and A. Valente, "Matter Protocol Integration Using Espressif's Solutions to Achieve Smart Home Interoperability," *Electronics*, vol. 13, no. 11, p. 2217, 2024, doi: 10.3390/electronics13112217.

[7] M. Maugeri, "Fuzzing Matter(s): A White Paper for Fuzzing the Matter Protocol," in *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, 2024, pp. 446–451, doi: 10.5220/0012469200003648.

[8] H. Jiang, C. Cai, X. Ma, Y. Yang, and J. Liu, "Smart Home Based on WiFi Sensing: A Survey," *IEEE Access*, vol. 6, pp. 13317–13325, 2018, doi: 10.1109/ACCESS.2018.2812887.

[9] S. R. Pokhrel and S. Singh, "Compound TCP Performance for Industry 4.0 WiFi: A Cognitive Federated Learning Approach," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 2143–2151, Mar. 2021, doi: 10.1109/TII.2020.2985033.

[10] J. Fornehed, K. Caindec, and D. Meier, "Automated Onboarding and Device Provisioning Best Practices," *Industry IoT Consortium*, 2022.

[11] C. Paniagua and J. Delsing, "Industrial Frameworks for Internet of Things: A Survey," *IEEE Systems Journal*, vol. 15, no. 1, pp. 1149–1159, Mar. 2021, doi: 10.1109/JSYST.2020.2993323.

[12] J. Yang and L. Sun, "A Comprehensive Survey of Security Issues of Smart Home System: 'Spear' and 'Shields,' Theory and Practice," *IEEE Access*, vol. 10, pp. 124167–124192, 2022, doi: 10.1109/ACCESS.2022.3224806.

[13] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A Survey," *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70–95, Feb. 2016, doi: 10.1109/JIOT.2015.2498900.

[14] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," in *2013 Ninth International Conference on Computational Intelligence and Security*, Dec. 2013, pp. 663–667, doi: 10.1109/CIS.2013.145.

[15] M. Fagan *et al.*, "Towards Automating IoT Security: Implementing Trusted Network-Layer Onboarding," 2025, doi: 10.6028/NIST.CSWP.42.

[16] K. Li *et al.*, "Zero-Trust Foundation Models: A New Paradigm for Secure and Collaborative Artificial Intelligence for Internet of Things," *IEEE Internet of Things Journal*, vol. 12, no. 22, pp. 46269–46293, Nov. 2025, doi: 10.1109/JIOT.2025.3603957.

[17] S. Otoum, A. Nayak, and I. Stojmenovic, "LLM-Based Threat Detection and Prevention Framework for IoT Ecosystems," *arXiv preprint arXiv:2505.00240*, 2025, doi: 10.48550/arXiv.2505.00240.
[18] H. Nishi, J. Wejekoon, E. Y. Song, and K. B. Lee, "Security for IEEE P1451.1.6-based Sensor Networks for IoT Applications," in *IECON 2024 - 50th Annual Conference of the IEEE Industrial Electronics Society*, IEEE, Nov. 2024, pp. 1–6, doi: 10.1109/IECON55916.2024.10905544.
[19] M. Aung, J. Lee, and R. Gupta, "Generative AI for Internet of Things Security: Challenges and Opportunities," *arXiv preprint arXiv:2502.08886*, 2025, doi: 10.48550/arXiv.2502.08886.
[20] W. Zegeye *et al.*, "Comparing Smart-Home Devices that Use the Matter Protocol," in *2025 IEEE 22nd Consumer Communications & Networking Conference (CCNC)*, IEEE, Jan. 2025, pp. 1–6, doi: 10.1109/CCNC54725.2025.10976049.
[21] H.-T. Nguyen, V.-H. Pham, V.-T. Vu, and T.-T. Nguyen, "Web access as a service for CSA matter protocol: Bridging matter and the W3C Web of Things framework for smart home interoperability," *Internet of Things*, vol. 32, p. 101618, Jul. 2025, doi: 10.1016/j.iot.2025.101618.
[22] D. L. N. Thi, X. T. Kieu, T. S. Bui, T. L. Le, and V. C. Pham, "Towards interworking of matter and oneM2M: Design and implementation of a matter–oneM2M Interworking Proxy Entity," *Internet of Things*, vol. 27, p. 101313, Oct. 2024, doi: 10.1016/j.iot.2024.101313.
[23] A. Mota, C. Serôdio, and A. Valente, "Matter Protocol Integration Using Espressif's Solutions to Achieve Smart Home Interoperability," *Electronics*, vol. 13, no. 11, p. 2217, Jun. 2024, doi: 10.3390/electronics13112217.
[24] N. T. Dieu Linh and T.-T. Nguyen, "FIWARE IoT agent for Matter: Toward the integration of smart home devices into the FIWARE smart city platform," *Computer Communications*, vol. 245, p. 108369, Jan. 2026, doi: 10.1016/j.comcom.2025.108369.
[25] M. Mirza *et al.*, "Internet of thing based health monitoring system using wearable sensors networks," *International Journal of Reconfigurable and Embedded Systems (IJRES)*, vol. 13, no. 2, pp. 424–430, Jul. 2024, doi: 10.11591/ijres.v13.i2.pp424-430.

BIOGRAPHIES OF AUTHORS

Dr. Geetishree Mishra Ph.D. in Automotive Embedded Systems from Visvesvaraya Technological University (VTU), Belagavi, Karnataka. She is currently working as a Professor in the Department of Electronics and Communication Engineering at BMS College of Engineering, Bangalore. She has 18 years of teaching and research experience, and also over 7 years of industry experience in integrating and testing C-DOT switching systems. She has around 30 research publications in referred journals. She is a member of the IEEE and fellow member of IETE. Her research interests include artificial intelligence with deep learning and embedded systems design. She can be contacted at email: geetishreemishra.ece@bmsce.ac.in.

Dr. Hemavathi received her Ph.D. degree in Wireless Communication from B.M.S College of Engineering, VTU, Belagavi, Karnataka. Currently, she is working as an Assistant Professor at B.M.S College of Engineering in the Department of Electronics and Communication Engineering. She has 16 years of teaching and research experience. She is a member of the IEEE, life member IETE, and Indian Society for Technical Education (ISTE). She has around 12 research publications in referred journals. Her research interests are: wireless communication and networks, antenna theory and RF, and microwave networks. She can be contacted at email: hemavathi.ece@bmsce.ac.in.

Dr. Harish V Mekali is an Associate Professor in Electronics and Communication Engineering at BMSCE and a Ph.D. scholar (IIT Bombay) specializing in embedded systems and IoT. He established the Robotics and Embedded Systems Lab, has secured over ₹79.45 lakhs in research funding, and produced 19 publications along with patents and copyrights. Actively collaborating with industry and government bodies, he has served as a consultant and committee member. He is an IEEE Senior Member and holds memberships in ISTE, IETE, and ISOC, with research interests in IoT and robotics. He can be contacted at email: hvm.ece@bmsce.ac.in.