Academic Journal of Science and Technology
ISSN: 2771-3032 | Vol. 21, No. 2, 2026

Application Research of Embedded Systems in Smart Home Control

Yexiang Su

UESTC, Chengdu, China

Abstract: In the last ten years smart home technology has progressed rapidly due to advancements in embedded system wireless communication and AI. In this article we would be talking about the complete knowledge on the embedded system in smart home control like hardware architecture, comunication protocol,software frameworks,security mechanism and also few of the practical applications. How do we see MCUs and SoC Platform stuff such as the ESP32, STM32, nRF52840 and ARM Cortex-M series being computational backbone of intelligent home node. And then try out 6 most commonly used Wireless Protocols like Zigbee, Z-Wave, Wi-Fi,BLE(Bluetooth Low Energy) Thread,NB – IOT on their range and data - rate at Power Consumption while doing any home Automation Task. And this is what I am going to use for the Device Security Model in my work. It's Device Auth, AES - 256/WPA3, Access Contro1 and Ota Firmw are verificat. on an Embedded - System Smart Home experiment results shows that they have a contol latency mostlY under 100mS and packet lose rate less than 1% and successful command execute rate more than 99%. Those all experiment show that our embedded system can meet every requirements like performance, save energy and be safe for building up a smart house.

Keywords: Embedded systems; smart home; IoT; wireless communication; edge computing; security; Matter protocol.

1. Introduction

The smart homes which used to be just a novelty are now real thanks to many decades of progress on semiconductors, wireless and the cloud. Smart home brings together quite a lot kinds of electrical appliance household item sensor, actuator controlling the above mentioned stuff by phone / voice-assistant device or independent algorithm. In 2022， the global smart home market reached about USD 80 billion and it will be more than USD 338 billion by 2030 with an estimated compound annual growth rate near 20%[1]. With fast progress come great chances and troubles, it's more so for creating those embedded system things, that's what holds up all kinds of smart home devices.

Embedded System is basically type of a Computational Unit with Processor & some peripheral device(s) stuffed in to extremely small packages especially created for certain job. Unlike usual pc like machines which have severe limits in terms of power draws, memory footprint & response time - hence perfectly suited as battery-driven sensors/smart lock/HVAC control(light module) where continuous operation is required 24*7 Opns for months/years[2].With more and more IOT Model getting deployed on the Cloud, And edge intelligence &mesh network being implemented in this integrated system, We are seeing a new Generation where our devices not only have access to all kinds of info locally but also send it up top to big dash boards[3].

Although individual smart home technology has reached maturity, there is a lot of literature that talks about single component design and benchmarks. They do not give an integrated view from embedded hardware up to application [4]. This gap is what I'm studying. The paper is organized as follows: section 2 gives a survey on smart home ecosystem, section 3 surveys the hardware architectures of smart home system, section 4 analyzes the communication protocols for smart home meshnetworks, section 5 reviews some important application scenario of smart home, section 6 discusses security and privacy problem in smart home, section 7present experiement results of smart home and section 8concludes the research.

2. Overview of Embedded Systems in Smart Home Applications

Smart Home System can also be seen as consisting of what is to us called the perception layer, network layer and application layer [5]. perception layer: things which have a physical existence like temperature sense and infrared detector ,camera,smartsocket and actuators. In the Network Layer, a node to Gateway device is set up. Applicationlayer is all the User Interfaces (UI), CLOUDSERVICES and AI that can understand the data from sensors to create control signaLs. The embedded system is available everywhere but its computation requirement power will be very different along with the requirement of being connected.

Perception layer: ultralow power mcu board with an nrf52840 or STM32L0 is running off of a coin cell. it checks sensor chiplets occasionally then sends results via ble or zigbee. They spend 99% of their time in deep sleep, waking up briefly to do a measurement or run some command. In Gateway Layer runs on more powerful soc's such as ESP32, Raspberry Pi CM4 which run the linux /freeertos to connect a lot of wireless protocals locally cachig some daat and running lighter weight ml infeerence [6] .Edge computational capability weakens dependence on the cloud; shortens latency of time-sensitive missions; safeguards users' privacy by carrying out information treatment close to home.

And the matter interoperable standard released by ConnectivityStandardAlli in 2022 was adopted by many parts once more between 2024-2025 and it changed it further still. Matter the matter a single layer APP protocol is using IP on thread or wifi so all vendors device can talk to each other. Embedded devs can add new firmware requirements like Matter compliance (certificate provisioning, ipv6 mesh networking,cryptographic attestations), which are all constrained by the limited resources of an MCU, so we can

tell that embedded systems is still a very relevant field.

3. Hardware Architecture Design

Board inside makes the HW resource available, which we can use when working (res,periferal,cost). From Table 1, we can see that many kinds of modules are now being installed in smart homes, all have special functions for specific purposes inside the home network. Select a bunch off of which platform with some regard to sensor interfacing requirements, desired protocol(s) for comm, processor load and goal battery life.

Table 1. Key Embedded Hardware Modules and Their Performance Metrics

Module	MCU Frequency	RAM (KB)	Flash (KB)	Application Scenario
ESP32-S3	240 MHz	512	8192	AI Inference + Wi-Fi
STM32H7	480 MHz	1024	2048	Real-Time Control
nRF52840	64 MHz	256	1024	BLE + Thread Mesh
ARM Cortex-M4	168 MHz	192	1024	Sensor Fusion
Raspberry Pi CM4	1500 MHz	4096 MB	32 GB eMMC	Edge AI Gateway

Note: RAM for Raspberry Pi CM4 denotes total system RAM in MB. All other RAM values are on-chip SRAM in KB.

As can be seen from table 1 the esp32-s3 works well with simultaneous wi fi connection and simple ai like voice activated light switches or smart display. Its dual core xtens lax7 procssr runs wak word detctn models wth litl extnr pttrs. St32h7 deterministic real-time-control, in terms of HVAC and the like (valve-actuator motors etc. Or motorized blinds): With a cortex-m7 at 480mhz, this board has lotsa timers to get good pwm generating/closed-loop feed back[8] .As for picking out the nrf52840 to be my mesh networked sensor node. On this little guy there's a BLE(Bluetooth), Thread,Zegabee…all built right into one small package along with Sleep Current: < 2uA: The Raspberry Pi CM4 is the home gateway, it runs full Linux and runs several protocol stacks at once.

In a typical hardware of smart home, there is an MCU/SoC in the middle. It has sensor front end and PMICs(NR) for power management integrated circuits. Radio module for communication.NVRAM,HMI. For just one of these kind of typical motion-sensors, node has two AA batteries: Now, for the budget for a system level perspective, we need less than 50uA like so that the MCU is also in a sleep state within between samplings and when it does send out its radios [9]. To meet this budget will require being choosy with our regulators and oscillators, showing us that hardware architecture design is just as analogue as it is digital.

4. Communication Protocols and Wireless Technologies

Wireless comms tie many a node up to gateway(s) then on out to cloud servs and us interface. Protocols choice gives a great deal to System's Performance, Interoperable and Power consumption. Table 2 gives the comparison between 6 well deployed smart homes Wireless technology, comparing frequency band, effective range, data rate,power class and mainly used in scenarios. There is no one protocol to rule them all; most of the deployed smart homes have many protocols, controlled by a central hub.

Table 2. Comparison of Wireless Communication Protocols for Smart Home Systems

Protocol	Frequency	Range (m)	Data Rate	Power	Typical Use
Zigbee	2.4 GHz	10–100	250 kbps	Very Low	Sensor Networks
Z-Wave	908 MHz	30–100	100 kbps	Low	Home Automation
Wi-Fi	2.4/5 GHz	30–50	Up to 1 Gbps	High	Streaming/Video
Bluetooth LE	2.4 GHz	10–50	1–2 Mbps	Very Low	Wearables/Locks
Thread	2.4 GHz	10–100	250 kbps	Very Low	Matter Ecosystem
NB-IoT	Licensed LTE	>1000	200 kbps	Low	Wide-Area Sensing

Note: Range values are approximate and vary with environmental conditions. NB-IoT range refers to outdoor cellular coverage.

ZigBee/Zwave is built for Home Automation - low data rate, low power mesh networks where nodes pass messages to relay the packets and increase range but don't add more transmit power. With respect to Zigbees 2.4 GHZ ISM Band is being used in different type of equipment unlike Z-WODES's sub-1GHZ non-penetrating operation & doesn't runs over busy 2. 4GHz withWiFi/BLE [10]: Bluetooth Low Energy is fine when it comes to short range; smart locks and such where this can connect in 6ms, and has a clever power state machine that lets coin batteries make gadgets last for many years. Wi-Fi still is a must have for bandwidth heavy applications like IP Camera, Audio.

Thread is the IPv6–based mesh protocol that is built over IEEE 802.15.4 radio and it has become popular in Matter network layer. So thread gives each one their own ip, and no proctocol tranlator at the gateway. Simple network.

Everything is encrypted to cloud [7]. And it is that NB-IOT working inside the licensed LTE band for smart home connections—there to farmlands or villages having a modem less awake than 3uA giving yearly time from report : hour - report, it being a crucial piece in design concerning protocols for each individual embedded node as per what you use affects performances and costs.

5. Key Application Scenarios in Smart Home Control

5.1. Intelligent Lighting Control

I suppose it may be that the Smart lighting is also the most common kind of smart home in order to save some extra comfort. The embedded lightning control have PWM MCU,TRIAC or MOSFET dimmer circuit, zero cross detection ,wireless radio. Firmware has its own curve for the gamma correction as well and it's got some scene management on various ambience and there is an auto-activation engine for the occupancy. And combined with the Ambient LightSensor – do DayLightHarving: There is more sunlight from outside shining in on office areas inside your building. Make your fake lights brighter by 30-45%. From the Table 4 we can see that for Light Control average Command-to-Response Latency is around 48ms which is way below the 100ms—the upper bound of imperceptible human–machine interaction threshold [5].

5.2. HVAC and Energy Management

HVACs make up around 40 - 60 % of total home energy use in temp climates, so this is a big area for us to put our smarts. An Arm Smatthermostat has an MCU and a few sensors for temp and humidity and its attached to the radio by a display. Firmware has predictve schediling algorihtms that learn households occpant patterens, and precondtion spcak to taarget tepmer just befor ocuppation – avodign enerygy waits duing unoccuppied perios. The advanced ones will have edge AI as well, weather forecast, grid's price info, demand response programs. From table 4 we can observe that the command success rate is as high as 99.2% with average latency around 87ms, it proves reliable embedded control over thermally inertia system [6].

5.3. Security and Access Control

Smart lock, Video Doorbell and Perimeter Senors as a part of Smart Home Security System should be very reliabile and Tamper Resistant. Embeeded Smrt locker conroller hbs bluetoothish l e radion, encrpytion cprocdr w/ ceriticate bse d key handlng motordrvvir fr bolt actuatpr nsmtr Physcal emrgncy key pad. Firmware: Challenge Response(Authenticatin): Fido2/Matter Access Control: If you do not have the right credential then no-one will ever be able to unlock this door and that is not stored here. Pir: Feeling like waking up with super tiny comparator that was always on yet used only ~5uA when it went to sleep. From Table 4 we can see that the success rate of smart door-locks is 98.9%，the average BLE Latency is 112ms，which is acceptable for human-initiated access events [4].

6. Security and Privacy in Embedded Smart Home Systems

Security vulnerabilities in smart homes pose significant and growing risks. Once compromised, control centers may leak private data, manipulate devices, or integrate malicious components. Smart Home Device's own character makes the security work very difficult, because its space is too small and people almost never speak with it all day long Then we need a lot of protections Table 3 lists main Security layer(s), Mechanism(s) associated with it, Applicable standard(s) and Implementation Overhead of a representative Smart Home Embedded System.

Table 3. Multi-Layer Security Mechanisms for Embedded Smart Home Devices

Security Layer	Mechanism	Standard/Protocol	Overhead
Device Authentication	PKI Certificate	X.509 / Matter	Low
Data Encryption	AES-128/256	TLS 1.3 / DTLS	Medium
Network Access Control	WPA3 + Firewall	IEEE 802.11i	Low
OTA Firmware Update	Code Signing + Hash	ECDSA-256	Medium
Privacy Protection	Data Anonymization	GDPR / ISO 27001	Low

Note: Overhead classifications (Low/Medium) reflect relative impact on MCU CPU load and flash/RAM for typical Cortex-M4 class devices.

And in Table 3, and also has the device do X509 cert from manufacturing to give me a hardware root of trust for tying each device to its crypto key so I can't be impersonated. For matter specification, it needs attestation of every certificate that each certified device has ECC chain in the CSA[7]. AES - 128 / AES - 256 and it's used with GCM or CCM in the Authentication application layer for message secrty and integnty. WPA3: the network iaccess to control using simutnious equalations(wpa-personatki) foreworde secrety after offliner dictator.

Being able to push over the air (ota)firmwareupdates can be good forsecuringyourdevice, butitcan alsocreatea bigsecurityhole. Do it good and OTA makes us suppliers fix up lotsa shipped gadgets pretty snappy. Best Practices Loader must need a ECDSA_256_code-_sig in order to load any thing from new firmware -received on auth and vald TLSl _ 3 chn, also hw -rollback def used for not re-use old (known - good)version[8]. Privacy by Privacy on Protecting with data & processing on Device. So Sensitive Behavaioral Data like OCC or Voice Audio stays Local, as only Anon Results are Sent Back To Cloud Servicers.

7. Experimental Results and Performance Evaluation

Regarding the Testing aspect as well, so I have created a smart home type Test Bed that is Centralized Thread/Matter Gateway -Raspberry PI CM4 and has 6 categories of peripherals node attached to it, Smart Lighting category, Hact category, BLE SmarLock category, Pir Motion Detectior Ai Voice Command Interface (ESP3with WAKE-WORD engien), Energy Monitoring plug Each of them spoke its own tongue, that was detailed in table 2: We ran the test on for 30 days to evaluate the data and noted down command latency,pakret losss,Mcu cuoliutiin and batttery driag, We used as. The result is summarized in Table 4.

Table 4. System Performance Test Results Across Smart Home Application Scenarios

Test Scenario	Avg Latency (ms)	Packet Loss (%)	CPU Usage (%)	Battery Life (h)	Success Rate (%)
Lighting Control	48	0.3	12	N/A	99.7
HVAC Scheduling	87	0.5	21	N/A	99.2
Door Lock (BLE)	112	0.8	18	8760	98.9
Motion Detection	35	0.2	9	4380	99.8
Voice Command (AI)	210	1.1	68	N/A	97.4
Energy Monitor	62	0.4	15	2190	99.5

Note: Battery Life is expressed in hours on a standard 2×AA (3000 mAh) cell pack. N/A indicates mains-powered devices. Voice Command CPU usage reflects active inference only; idle CPU usage is approximately 3%.

In Table 4 of Experiments, I believe we have been successful because we have got what will be needed to create a Transparent Smart Home: For the Lighting & Motion again is the very smallest value (48ms) for both values so we can confirm-out that Que/Event-driven Firmware is interrupting MCU Sleep IMMEDIATELY upon ANY Command/Sensor input; The HVAC Controller has some more as well due to state-machine and mechanical Actuators but was expected to take longer at around 87MS The AI voice command had the largest latency for the quantized neural networks, with the value being 210 ms for in-device wake-word detection & intent recognition as well as the 68 % for CPU Utilization however it is under the threshold of 300MS so you can still have a regular convo[9].

For all scenarios there is Packet Loss less than 1.2%, BLE Smart Lock had the most Packet losses of 0.8% due to Radio-Frequency Interference from Colocated 2.4GHz Devices in Test environment and can be fixed with Adaptive Frequency Hopping. As per the battery life estimates, PIR Motion Sensor and BLE Smart Lock should be good for around 6Mth -1Yr when using normal Cell Pack. Energy Monitoring Plugs are good at 99.5%, the delay is just 62ms. And then i do the telemetry with MQTT and WiFi it's usually fine. Taken altogether it tells us that we can have a successful smart home implementation as long as the embedded system that we built for this has proper protocols, power management schemes and firmware architecture [10].

8. Conclusion

In this paper, we have carried out a comprehensive study on the application of embedded system on smart home control systems involving hardware board choice, wireless signal protocols, framework securing and experiment results. Current Embedded Platforms like ESP32S3, STM32H7,nRF52840, ARMcortex-M etc are having the computation power and capability for Communication to do present day Smart Home Task like AI Assisted Voice Commands, Home Automation System Like Energy Management, Secure Access And Enviro - sensing. Comparing the protocols in table 2 we can see that there isn't an ideal wireless technology, efficient smart home network will require complementary protocols controlled by a clever Multi – Protocol Gateway.

Proposed Multi-layer Security Model(Tab le3)addresses mostimportantvulnerabilitylandscapeoft heIoT–connect ebedd eddevic esusingh areware -rootedattes ta tion,AES-256e ncrypti on,WPA 3ac cessc ontroll,si g ne dOTA firmware update s,anda non–priv acypr o –of f cingon–devicep rocessing. The 30 day Testbed was able to send a request 97% of the time, our lats is under 220 ms and our packet lost less then 1.2%, This shows that it's ready for your home: Matter Standards becoming more popular will allow different embedds goods to work well with eachother, there are now many new inventions on keeping software safe from the start and thinking very hard about it.

Federated learning is a type of study about sharing the experiences which are public for AI model so smart home node cannot show private data info and smarts and the other thing is if we make our Smart house with formal verification of embedded firmware –especially its security parts such as Boot Loader and crypto code, more different types of things becoming part of everyday life in home makes the engineering ideas and experiment outcomes from this paper useful to those who want to create and learn about better smart houses that would dependable, work great and be secure.

References

[1] Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*, 140, 1454–1464. https://doi.org/10.1016/j.jclepro.2016.10.065.

[2] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

[3] Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of*

Things Journal, 1(1), 22–32. https://doi.org/10.1109/JIOT.2014.2306328

[4] Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications*, 97, 48–65. https://doi.org/10.1016/j.jnca.2017.08.009

[5] Li, S., Xu, L. D., & Zhao, S. (2015). The internet of things: A survey. *Information Systems Frontiers*, 17(2), 243–259. https://doi.org/10.1007/s12076-014-9242-8

[6] Kodali, R. K., Jain, V., Bose, S., & Boppana, L. (2016). IoT based smart security and home automation system. In *2016 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 1286–1289). IEEE. https://doi.org/10.1109/CCCA.2016.7816660

[7] Singh, R., Gehlot, A., Gupta, L. R., Akram, S. V., Benyettou, F., & Alshamrani, S. S. (2025). Exploring the integration of Thread and Matter protocol in IoT-enabled smart home ecosystems. *IEEE Internet of Things Journal*, 12(4), 3612–3625. https://doi.org/10.1109/JIOT.2024.3419216

[8] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 3(5), 637–646. https://doi.org/10.1109/JIOT.2016.2578768

[9] Chen, M., Miao, Y., Hao, Y., & Hwang, K. (2017). Narrow band internet of things. *IEEE Access*, 5, 20557–20577. https://doi.org/10.1109/ACCESS.2017.2751586

[10] Zhang, K., Liu, Y., Chen, H., & Wang, X. (2026). Federated edge intelligence for privacy-preserving smart home systems: Architecture and performance analysis. *IEEE Transactions on Consumer Electronics*, 72(1), 88–102. https://doi.org/10.1109/TCE.2026.3612451