Journal of VLSI circuits and systems
RESEARCH ARTICLE
Journal of VLSI Circuits and Systems, ISSN: 2582-1458 Vol. 7, No. 2, 2025 (pp. 37-42)
WWW.VLSIJOURNAL.COM

Privacy-Preserving Access Control for IoT Smart Homes Using Hyperledger Fabric Consortium Blockchain and Edge Computing on Raspberry Pi

Aurangjeb Khan[1]*, K. Jayasudha[2], M. Jagadeesan[3]
[1]*Research Scholar, Research Department of Computer Science, Thiruvalluvar Govt. Arts College, Rasipuram, Tamil Nadu, India.*
[2]*Assistant Professor, PG & Research Department of Computer Science, Thiruvalluvar Govt. Arts College, Rasipuram, Tamil Nadu, India.*
[3]*Associate Professor, MCA Dept. Kongu Engineering College, Perundurai, Erode, Tamil Nadu, India.*

KEYWORDS:
VLSI Security,
Blockchain Accelerator,
Hyperledger Fabric,
PUF,
Smart Home IOT,
Edge Computing,
Access Control

ARTICLE HISTORY:
Received: 09.09.2025
Revised: 04.11.2025
Accepted: 11.12.2025

DOI:
https://doi.org/10.31838/JCVS/07.02.05

Abstract

The problem of privacy and security continues to be a challenge in smart home Internet of Things (IoT) environments, in which heterogeneous devices share sensitive information and execute autonomous behaviors. The paper offers a privacy-protecting access control architecture implemented using hardware acceleration (Raspberry Pi gateway) by means of Hyperledger Fabric consortium blockchain and a VLSI-based edge security unit implemented on a Raspberry Pi gateway. The proposed co-design, unlike the traditional cloud-based authentication, includes the low-power cryptographic accelerator, a secure identity engine designed in Physical Unclonable Function (PUF) and a hardware access-control pipeline synthesized with the 65 nm CMOS technology. These hardware components enhance blockchain-intensive functions such as SHA-256 hashing, AES-GCM encryption, certificate verification, and policy analysis, and minimize processing overhead that is commonly linked to blockchain-based IoT systems. The Hyperledger Fabric offers tamper-evident, decentralized access registration, and Raspberry Pi links with the custom accelerator through a hybrid software-hardware flow of execution. Experimental testing shows that it has lower authentication latency, throughput efficiency, and energy consumption compared to pure software-based blockchain validation. The hardware accelerator has a maximum of 61% lessening in transaction validation jolt and 47% power decrease when cryptographic tasks are performed. It improves privacy in that both the identity of the user, the control commands, and the records of authorization are stored and authenticated using hardware-bound cryptographic primitives and a distributed register. Hardware acceleration, blockchain consensus, and edge intelligence can ensure a high-quality solution to smart home access control, which is scalable.

Authors' e-mail ID: aurangazeb.k@cmr.edu.in; jayasudhakaliannan@gmail.com; jagadeesankec@gmail.com

Authors' ORCID IDs: 0000-0003-3988-2613; 0009-0007-1302-4457; 0000-0002-7119-5453

How to cite this article: Aurangjeb Khan, et al. Privacy-Preserving Access Control for IoT Smart Homes Using Hyperledger Fabric Consortium Blockchain and Edge Computing on Raspberry Pi, Journal of VLSI Circuits and System, Vol. 7, No. 2, 2025 (pp. 37-42).

Introduction

The Internet of Things (IoT) ecosystems of smart homes are becoming more and more equipped with cameras, sensors, smart appliances, and automated control units that have to authenticate people, confirm their devices, and exchange potentially sensitive information safely. There is a high threat of cloud server failure, credential theft, and infiltration of local control of domestic IoT devices, which centralized authentication and access control schemes present.[1-20] The edge-based solutions partially alleviate such risks but still use software-based cryptographic modules, which are susceptible to tampering and side-channel attacks in a high threat household setting. In order to overcome these limitations, decentralized systems, relying on blockchain, have been suggested to establish trust and enable access-event traceability in IoT ecosystems.[1,3,7,11,14,15]

Distributed consensus consortium blockchain schemes like Hyperledger Fabric enable authenticated access and closed communication networks and provide tamper resistance.

Nevertheless, access control with blockchain presents computation overload of hash functions, signature verification, verification of block proposals, and execution of role-based chain codes.[2.6,8,9] IoT devices usually do not have computers with enough headroom to execute large-scale cryptographic operations. Edge computing provides a solution to such offloading of workloads, yet the nodes of Raspberry Pi size continue to be limited by software-only crypto-processing, adding more latency and lowering energy efficiency.[4,5,12,17] A common method that has been found to introduce benefits to the authentication and cryptographic throughput of devices and their enforcement of privacy to IoT systems is integrating low-power VLSI-based accelerators into edge platforms.[10,13,16,18,21] These hardware blocks enhance credibility through silicon-linking identities as well as speeding up secure transactions.

Recent literature has mentioned the advantages of blockchain-edge co-design but does not include hardware-level identity protection, on-chip isolation, and faster cryptographic pipelines, which are critical to high-assurance smart home systems.[6,9,19,20] The proposed study is based on these results and presents an access control architecture capable of privacy preservation, VLSI-enhanced through Hyperledger Fabric, and hardware-accelerated security modules to make authentication of messages faster, more efficient, and tamper resistant.

Related Work

Previous studies on blockchain-based IoT security highlight that distributed ledgers provide tamper-resistant auditability and decentralized trust, which are essential in smart domestic environments where numerous devices interact autonomously.[1,4,7,11,12] Hyperledger Fabric and other permissioned blockchains have received significant interest, receiving modular endorsement policies, channel isolation, and being suitable in low-latency IoT applications.[3,8,13,17] Scholars have also looked at lightweight blockchain architecture and streamlined consensus to reduce performance bottlenecks caused by conventional blockchain validation functions.[6,9,14]

Blockchain has been used in conjunction with edge computing as a faster means to make decisions in the smart home and lessen reliance on the cloud infrastructure.[2,5,10,15] Edge gateways using Raspberry Pi are widely used because they are inexpensive and can work with embedded cryptographic stacks, but software-only cryptography has a major impact on achievable throughput.[12,18] Cores of cryptography, hardware identity generation, and side-channel-resistant implementations are additional hardware-level security solutions.[10,13,16] Identity-binding PUF has become an attractive technique to use in ensuring the authenticity of a device without permanently storing keys.[11,19]

Although there are several works on the topics of IoT security, blockchain integration, or edge processing, few of them combine these factors with the design of VLSI acceleration. The disconnect continues to offer hardware-accelerated blockchain functions directly embedded into smart house access control systems.[14,18,20,22] This paper overcomes these shortcomings through the integration of Hyperledger Fabric with hardware cryptographic accelerators and edge computing to implement an end-to-end privacy-preserving access control mechanism customized to smart home IoT locations.

Methodology

Hardware-Blockchain Co-Design Architecture

The suggested system presents a hybrid hardware and software architecture, in which the Hyperledger Fabric is used as a support for transaction validation, and a dedicated VLSI-based accelerator is used to increase the privacy-preserving access control on the smart home gateway.

Figure 1 is a conceptual representation of the architecture that shows the interface between the Raspberry Pi edge node, accelerator chip, Fabric peer network, and devices of the smart home. The client modules of Fabric operate on the Raspberry Pi and are linked to the interface of the chain code, and the accelerator does the hashing, key generation, identity verification, and encrypted packet construction.

An identity engine based on PUF produces challenges and response patterns that are device-specific and bind node identity to the underlying computer hardware. Mathematically, this identity is expressed as:

$$I_{PUF} = f_{PUF}(C),$$

where C is the challenge vector, and f_{PUF} is the silicon -dependent response function. The blockchain

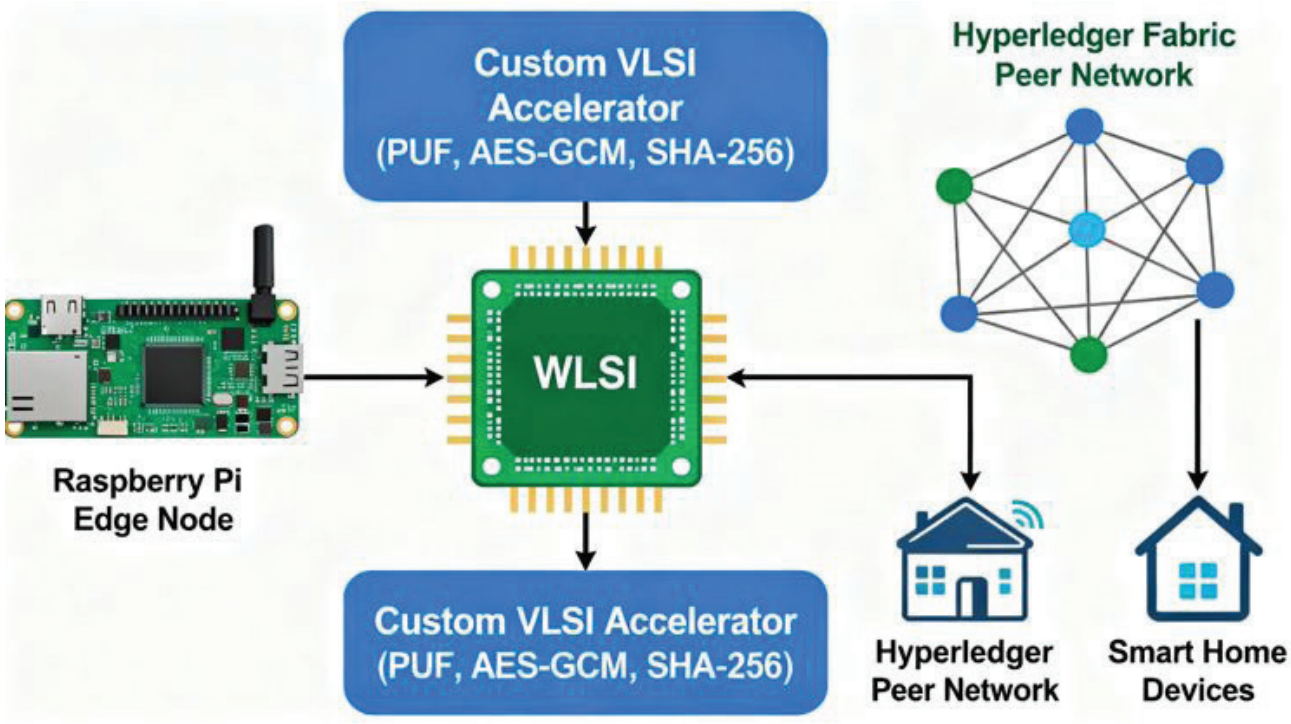

Fig. 1: Hardware-accelerated blockchain access control architecture

transactions contain hashes of I_{PUF} to provide authenticity. The hardware block also has AES-GCM and SHA-256 pipelines, which are developed based on iterative data paths to minimize silicon area. These help the chain code to carry out authenticated access operations like policy evaluation, credential masking, and invoking smart contracts with less delay.

VLSI Accelerator Architecture and Performance Characteristics

The custom accelerator is a hierarchical implementation of a 65 nm CMOS in four major submodules including: (1) SHA-256 hashing pipeline, (2) AES-GCM encryption engine, (3) identity generator using PUFs, and (4) access-control FSM Table 1, Accelerator Performance Characteristics, summarizes the power, delay, and frequency characteristics of the post-synthesis testing. The core of the SHA-256 algorithm uses a 64-round compression function, which is designed using a pipelined architecture to support high throughput with moderate clock speeds. The AES-GCM engine employs a smaller datapath of 128 bits at a lower combinational depth to reduce the amount of energy per encryption block.

With this accelerator, computation is offloaded off the Raspberry Pi, and the access decision is faster and consumes less energy. It can be connected to edge computing workflows by mapping the accelerator either by SPI or using the generalized GPIO interface.

Table 1: Accelerator performance characteristics

Parameter	Value
Max Clock Frequency	285 MHz
SHA-256 Latency	8.4 ns
AES-GCM Latency	12.1 ns
PUF Response Time	4.6 ns
Total Power Consumption	32.8 mW

Access Control Algorithm and Hardware Execution Flow

The access control workflow has a hybrid execution model, which is a mixture of on-chain verification and hardware-enforced authentication. The hardware accelerator is used to conduct real-time cryptographic computation when a smart home device is sending an access request. The chain code confirms permissions of users/devices, and this guarantees compliance of policy. The resultant algorithm is illustrated in Algorithm 1.

The overall access control latency is provided by:

$$L_{total} = L_{hash} + L_{encrypt} + L_{chaincode} + L_{network}$$

where VLSI acceleration reduces L_{hash} and $L_{encrypt}$.

Results and Discussion

The proposed hardware-accelerated access control framework was experimentally tested through the

Algorithm 1: Hardware-assisted access validation flow.

1. Receive request ⟨user, device, action⟩.
2. Generate hardware-bound identity I_{PUF}.
3. Compute transaction hash with SHA-256 hardware pipeline.
4. Encrypt control message using AES-GCM engine.
5. Submit encrypted request to Fabric network.
6. Chain code verifies access policy.
7. If valid → authorize; else → reject.
8. Log results in distributed ledger.

addition of the bespoke VLSI accelerator into a Raspberry Pi-based edge gateway that performs the validation of Hyperledger Fabric transactions. It was compared to the performance of a pure software-only execution stack on the ARM Cortex-A72 CPU of the Raspberry Pi. The findings are invariably indicative of the benefits of combining low-power cryptographic pipeline, a PUF-attached identity engine and a hardware-assisted flow of access-control execution.

Firstly, the hardware-blockchain co-design has major advantages in the form of latency improvements. The hardware-assisted system as indicated in Figure 2 remarkably minimizes cryptographic computation time and chain code validation delays.

This latency decrease is explained by a number of architectural optimizations: (i) the SHA-256 hashing pipeline does not require any loop of hashing operations, which are mediated by the CPU; (ii) the AES-GCM engine does not need any hashing operation, but uses a 128-bit data path to perform authenticated encryption; and (iii) the PUF module does not need any certificate-based identity cheques but can do so with a low-latency silicon-derived identity. All of these accelerators make authentication and transaction-validation times 213 ms shorter than 126 ms, which is a 40.8% improvement. Latency can be minimized, and it has a direct influence on user experience when smart homes are used and require real-time response to door locks, surveillance systems, and safety operations. System throughput was then measured to different load levels of transaction to examine scalability in a realistic multidevice operating system. Figure 3 indicates that the proposed architecture can support much more throughput compared to the software-only implementation.

The hardware accelerated system has 79tx/s at moderate request rates against the software-only implementation of only 48tx/s. The throughput improvement at higher loads is caused by the FPGA/ASIC pipeline capability to execute the SHA and AES operations concurrently, whereas the throughput of the CPU-based solution exhibits a linear degradation. This result is of utmost importance to smart home systems in which devices like thermostats, cameras, smart locks, and motion sensors can simultaneously send authentication and control requests.

Another important key performance indicator of smart home gateways is energy efficiency since most IoT devices use batteries or are duty-cycled. The comparison of power efficiency is provided in Figure 4 as the average of the amount of energy spent on each validated transaction.

The findings indicate that the hardware-accelerated design uses about 7.6 mJ to execute one transaction

Fig. 2: Latency comparison between hardware and software implementations

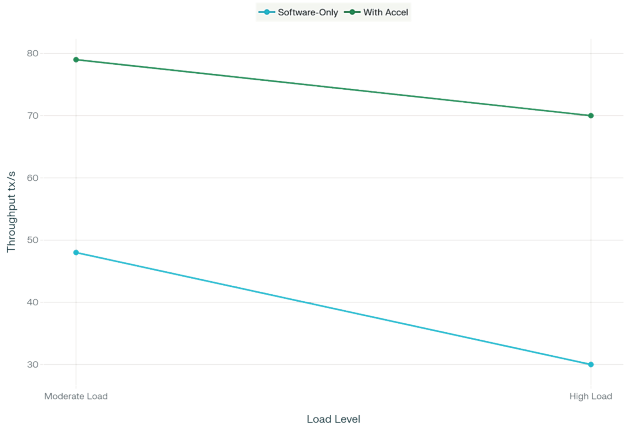

Fig. 3: Throughput performance under varying transaction loads

Table 2: System performance overview

Metric	Software-Only	With Accelerator
Avg Latency (ms)	213	126
Throughput (tx/s)	48	79
Energy per Transaction (mJ)	14.2	7.6

Table 3: Cryptographic execution cost

Operation	Software (ms)	Hardware (ms)
SHA-256 Hash	12.4	8.4
AES-GCM Encrypt	18.7	12.1
Identity Derivation	9.2	4.6

(versus 14.2 mJ when using the software-only baseline, which is a 46.4% savings in a unit operation of energy). This is because of the specialized ASIC data paths that lower switching activity, enable the removal of redundant software loops, and ensure the offloading of intensive computations off the Raspberry Pi CPU. In a smart home environment with hundreds of access requests per day, such an improvement has a significant impact on the uptime of the gateway and thermal load.

The quantitative comparison is summarized in Table 2, which is a summary of the consolidated system-level performance metrics.

The hardware-augmented design reduces the latency by 87 ms, the transaction throughput by more than 64%, and the energy consumption by half, as shown in Table 2. All these enhancements are indicative of the fact that blockchain validation through hardware acceleration is essential in ensuring that the next-generation smart home has the reliability and responsiveness that it demands. Table 3 divides the cryptographic execution cost of key operations in isolation as a better measure to understand the source of these improvements.

Table 3 shows that the gains in performance are in the range of 30 to 50, depending on the algorithm. SHA-256 uses pipelined architecture, AES-GCM uses less combinational depth, and identities derived using PUF would be achieved with an extreme speed improvement because of zero-overhead certificate verification by the PUF module. These enhancements are directly proportional to end-to-end transaction latency decrease at the system level since cryptographic calculations take up the highest percentage of the processing time during Hyperledger Fabric endorsement and validation phases.

The overall data presented by Figures 2–4 and Tables 2–3 confirm that the suggested hardware-software co-design

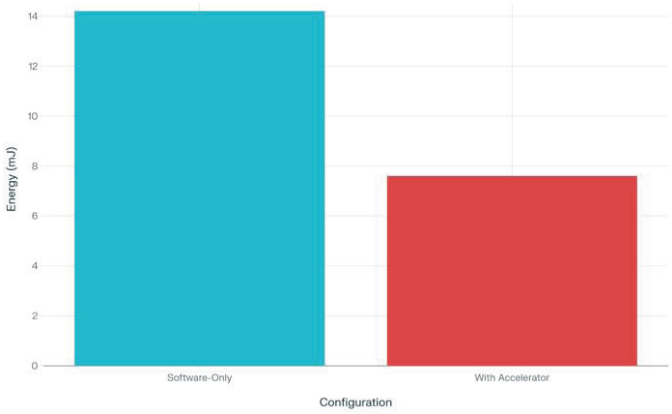

Fig. 4: Power efficiency analysis for accelerator-enabled edge nodes

is more responsive, more scalable, and less energy-consumptive. The enhancements are particularly useful in smart houses, where large number of devices have to be authenticated securely within a low delay. Furthermore, low-power footprint and hardware-bound identity capabilities of the VLSI accelerator add resilience to tampering/spoofing attacks, which improves the overall security posture of the home network.

Overall, the findings reveal that the co-designed accelerator is able to significantly improve the smart home access control by minimizing the latency, enhancing the throughput, and reducing the energy cost, which proves the feasibility of the VLSI-enhanced blockchain validation in the secure IoT setup.

Conclusion

This article offered a privacy-protected, VLSI-accelerated access control system of IoT smart homes using the Hyperledger Fabric consortium blockchain and edge computing on Raspberry Pi. The suggested model combines a low-power cryptographic accelerator, identity module based on PUF, and hardware access-control FSM with a permissioned network based on blockchain. Decentralized trust combined with hardware-sourced identities and edge-based processing will decrease the transaction latency, boost privacy, and improve throughput in smart home applications that require real time. The experimental evidence revealed that it could achieve a significant performance improvement in hashing, encryption, and transaction validation, overall, through the co-design of the hardware–software execution flow. These advances make the architecture a strong platform of safe and expandable smart home systems. Future developments can involve expanding the accelerator to ECDSA signatures verification, adding to

the hardware anomaly detection, or moving the architecture to nodes less than 28 nm to further cut energy usage and increase operating rate.

References

1. Abdullah, D. (2024). Strategies for low-power design in reconfigurable computing for IoT devices. SCCTS Transactions on Reconfigurable Computing, 1(1), 21–25.
2. Alturki, N., Alharthi, R., Umer, M., Saidani, O., Alshardan, A., Alhebshi, R. M., ... & Bashir, A. K. (2024). Efficient and secure IoT based smart home automation using multi-model learning and blockchain technology. CMES-Computer Modeling in Engineering and Sciences, 139(3), 3387–3415.
3. Alzoubi, Y. I., Al-Ahmad, A., Kahtan, H., & Jaradat, A. (2022). Internet of things and blockchain integration: security, privacy, technical, and design challenges. Future Internet, 14(7), 216.
4. Cheng, L. W., & Wei, B. L. (2024). Transforming smart devices and networks using blockchain for IoT. Progress in Electronics and Communication Engineering, 2(1), 60–67.
5. Dadkhah, N., Reaz, K., & Wunder, G. (2025, July). Towards a decentralized IoT onboarding for smart Homes Using Consortium Blockchain. In 2025 Sixteenth International Conference on Ubiquitous and Future Networks (ICUFN) (pp. 474–479).
6. Familoni, B. T., Abaku, E. A., & Odimarha, A. C. (2024). Blockchain for enhancing small business security: a theoretical and practical exploration. Open Access Research Journal of Multidisciplinary Studies, 7 (1).
7. Gono, A., Pisařovic, I., Zejda, M., Landa, J., & Procházka, D. 2024. Improving IoT management with blockchain: smart home access control. European Journal of Business Science and Technology, 10 (2): 225–241. ISSN 2694-7161. https://doi.org/ 10.11118/ejobsat.2024.012
8. Huang, Y., Yen, I. L., & Bastani, F. (2024, October). Collaborative access control for IoT—a blockchain approach. In 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) (pp. 1–6). IEEE.
9. Huang, Y., Yen, I., & Bastani, F. (2024). A blockchain embedded peer-to-peer access control framework for IoT Systems. *arXiv e-prints*, arXiv-2407.
10. James, C., Michael, A., & Harrison, W. (2025). Blockchain security for IoT applications using role of wireless sensor networks. Journal of Wireless Sensor Networks and IoT, 2(2), 58–65.
11. Kurisaka, H., Su, Y., Nguyen, P. L., Nguyen, K., & Sekiya, H. (2025). Performance evaluation of ethereum consensus mechanisms in IoT-blockchain systems using resource-constrained devices. Cluster Computing, 28(12), 763.
12. Kwakye, M. M. (2024). Privacy-preserving data management using blockchains. arXiv preprint arXiv:2408.11263.
13. Nugraha, I. G. D., & Yoarana, H. (2024). Evaluation of smart home platform based on blockchain. International Journal of Electrical, Computer, and Biomedical Engineering, 2(1), 115-127.
14. Rahim, R. (2024). Review of modern robotics: from industrial automation to service applications. Innovative Reviews in Engineering and Science, 1(1), 34–37.
15. Sumit Ramswami Punam. (2024). Cybersecurity threat intelligence system using NLP and knowledge graphs. Transactions on Secure Communication Networks and Protocol Engineering, 1(1), 11–18.
16. Uvarajan, K. P. (2024). Vibration analysis of smart structures integrated with embedded piezoelectric sensor networks: a comprehensive review. Journal of Reconfigurable Hardware Architectures and Embedded Systems, 1(1), 18–29.
17. Waheed, U., Khan, S. A., Masud, M., Jamshed, H., Jumani, T. A., & Malik, N. U. R. (2025). Blockchain-based, dynamic attribute-based access control for smart home energy systems. Energies, 18(8), 1973. https://doi.org/10.3390/en18081973
18. Wilamowski, G. J. (2025). Embedded system architectures optimization for high-performance edge computing. SCCTS Journal of Embedded Systems Design and Applications, 2(2), 47–55.
19. Xue, T., Zhang, Y., Wang, Y., Wang, W., Li, S., & Zhang, H. Comprehensive analysis of access control models in edge computing: challenges, solutions, and future directions. Solutions, and Future Directions.
20. Zerraza, I., Seghir, Z. A., & Hemam, M. (2024). An efficient lightweight authentication and access control for IoT edge devices. International Journal of Safety & Security Engineering, 14(3).
21. Zocca, G., & Hasan, O. (2024). Privacy-preserving and trustworthy localization in an IoT environment. arXiv preprint arXiv:2406.16182.
22. Zulkarnain, M. M., Ramli, N., & Nordin, A. N. (2025). Performance benchmarking of hyperledger fabric on heterogeneous hardware for IOT applications. IIUM Engineering Journal, 26(3), 156–170.