Protecting Edge Services for Upcoming Industrial IoT and Smart Healthcare Uses

Chinkal Arunkumar Parmar

Babubhai Patel Physician PC, New York

ABSTRACT

Ensuring secure and intelligent environments is essential for advancing IoT applications like digital healthcare and Industry 4.0. These environments must support ubiquitous digital services for users while meeting critical security, privacy, and low latency requirements. This paper presents a summary of the dissertation [1], focusing on three main contributions: i) a lightweight biometrics-based user authentication mechanism tailored for innovative healthcare environments without the need for gadgets, ii) a conceptual three-tier approach for secure node bootstrapping and secure user access to digital services, and iii) a Blockchain and Edge computing-based network architecture designed for IIoT applications. This architecture addresses crucial needs such as low-latency communication, trust management, and enhanced security. Performance evaluations of the proposed frameworks provide valuable insights into enabling secure hyperconnected environments for diverse applications in the future.

INTRODUCTION

Gadgets have traditionally served as the primary means of accessing digital services, with devices like smartphones, laptops, and tablets widely adopted across various sectors, including healthcare and banking [2], [3]. However, advancements in communication, networking, and sensing technologies, coupled with the evolution towards 5G and beyond, are reshaping service delivery from device-centric to user-centric paradigms [4], [5]. This transition envisions users accessing digital services directly from intelligent environments without needing handheld gadgets, a concept known as the 'Naked World' [9]–[11].

Realizing this vision necessitates addressing several challenges. Security and privacy are paramount among these challenges in intelligent environments where traditional authentication methods may only suffice with user gadgets for inputting text or PINs [6]. Biometrics-based authentication emerges as a robust solution for verifying users in gadget-free environments [7], [13], especially given the resource constraints of future intelligent environments which require lightweight authentication mechanisms.

In addition to security concerns, ensuring low-latency services is critical for time-sensitive applications such as intelligent healthcare and industrial IoT [14]. While cloud computing offers significant computational capabilities, it may introduce delays unsuitable for latency-sensitive applications [15], [16]. Edge Computing (EC) addresses this issue by bringing computational resources closer to data sources, while concepts like Mist computing enhance local processing capabilities [17]–[20]. Securing these edge and local networks becomes imperative in intelligent environments.

Blockchain technology offers promising features such as decentralization, distributed trust, and immutability, which can augment future intelligent environments [21], [22]. Integrating Blockchain with edge-enabled architectures can enhance innovative applications by combining low-latency services with distributed trust and authentication capabilities [23].

The dissertation [1] addresses the following research questions:

- How can a lightweight biometrics-based user authentication mechanism be optimized for accessing services in future hyperconnected intelligent environments?

- How can secure edge-based mechanisms be designed to ensure service accessibility in future intelligent environments?

- What are the benefits of integrating edge computing and Blockchain for future intelligent applications?

In summary, this paper explores solutions to enable secure, low-latency, and user-centric digital services in upcoming intelligent environments, emphasizing the integration of advanced technologies like biometrics, Edge Computing, and Blockchain to effectively meet these evolving demands.

BACKGROUND

Evolution towards Smart Environments

Recent advancements in Information Communication Technologies (ICT) have revolutionised digital access to digital services. Rather than relying on device-centric services, future digital services aim to leverage nearby smart and intelligent environments, eliminating the need for explicit gadgets [24]. This vision, known as the gadget-free world or the Naked world, envisions a scenario where users operate without gadgets, receiving services directly from innovative environments [8], [11]. This transition from gadgets to a gadget-free world can be broadly categorized into three phases [7]. The first phase, 'Bearables,' represents the current gadget-oriented era. The second phase, 'Wearables,' involves accessing services through wearable devices like smartwatches and bright clothing. The final phase, 'Wearables,' describes a future where users access similar services without handheld gadgets within intelligent environments.

Enabling Technologies for Future Smart Environments

Enabling the realization of future intelligent environments are three pivotal technologies identified from the current state-of-the-art: IoT, Edge computing paradigms, and Blockchain technology. IoT forms a connected digital ecosystem where myriad smart devices (sensors, computing devices, etc.) communicate via network technologies to execute tasks or deliver services as needed [25]. While cloud computing platforms offer extensive resources to vast IoT networks, they may introduce higher network delays and prove unsuitable for delay-sensitive applications [26]. Edge computing bridges this gap by introducing an intermediary tier between local devices and the public cloud, enabling some cloud services closer to users or devices [27]. Further enhancing this concept is Mist computing, which brings computation and processing capabilities directly onto local networks or devices [28]. Blockchain technology, another crucial enabler for future intelligent environments, offers decentralization, immutability, and transparency [21], [22].

Overview of IoT Edge Models

A comprehensive study of IoT edge models reveals three significant paradigms, illustrated in Figure 1. The traditional cloud-IoT model, widely adopted across various applications, involves IoT nodes or devices sensing and gathering data, which is then transmitted to cloud platforms for further processing, analysis, and storage [29], [30]. The two-tier IoT-edge model enhances this approach by integrating edge network capabilities at the access level (between IoT nodes and the cloud), proving invaluable for latency-critical applications [29]. Extending this further is the three-tier IoT edge model, which incorporates computational capabilities within local networks, thereby enhancing processing efficiency [24]. Recent work has proposed models integrating edge computing and Blockchain for Industrial IoT (IIoT) applications, catering to diverse requirements such as low-latency services and robust trust management [31].

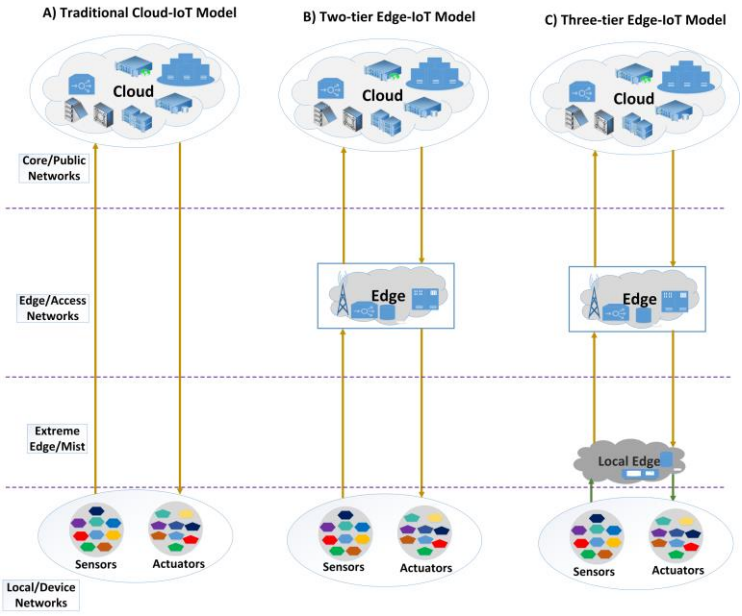

Fig. 1. Various IoT edge models [1].

Security Considerations in Smart Environments

Accessing services within nearby innovative environments requires a secure authentication mechanism, especially for users without handheld gadgets. Traditional authentication methods like two-factor or three-factor protocols, which rely on user gadgets, may not be suitable for gadget-free users [32], [33]. Biometrics-based authentication has emerged as a robust solution for such innovative environments [13]. Additionally, securing edge networks becomes imperative as edge computing gains prominence in future innovative environments [34].

Managing user privacy is another critical requirement, given the absence of separate private display screens typical of gadgets. Privacy management and establishing trust among users and network entities are pivotal in intelligent environments [35], [36].

RESEARCH METHODOLOGY

Before delving into specific contributions, it's essential to outline the two primary use cases considered in this research: future innovative gadget-free healthcare environments and Industrial IoT [7], [37].

Smart Gadget-Free Healthcare Use Case: This scenario focuses on enabling users without handheld gadgets to access medical services in hospitals or remotely at home. Examples include disabled persons or patients in need of emergency care who face challenges in traditional hospital procedures. The gadget-free healthcare environment facilitates user registration and delivery of primary healthcare services from nearby intelligent environments.

IIoT Use Case: This use case involves a clever "log-house construction" scenario encompassing phases such as wood harvesting, transportation, manufacturing into logs, warehouse storage, and delivery to construction sites. The objectives include monitoring industrial phases, ensuring secure data sharing among stakeholders, enabling low-latency services under unstable network conditions, and maintaining comprehensive records.

Lightweight Biometrics Authentication Mechanism in Smart Environments

This research aims to restrict access to essential medical services to authorized gadget-free users in innovative healthcare environments. A lightweight biometrics-based authentication protocol has been developed [6], [7]. Figure 2 illustrates the key entities involved in this protocol: Access Points (APs), Central Access Points (APC), Registration Center (RC), Medical Server (MS), End Nodes (ENs), and the User (U).

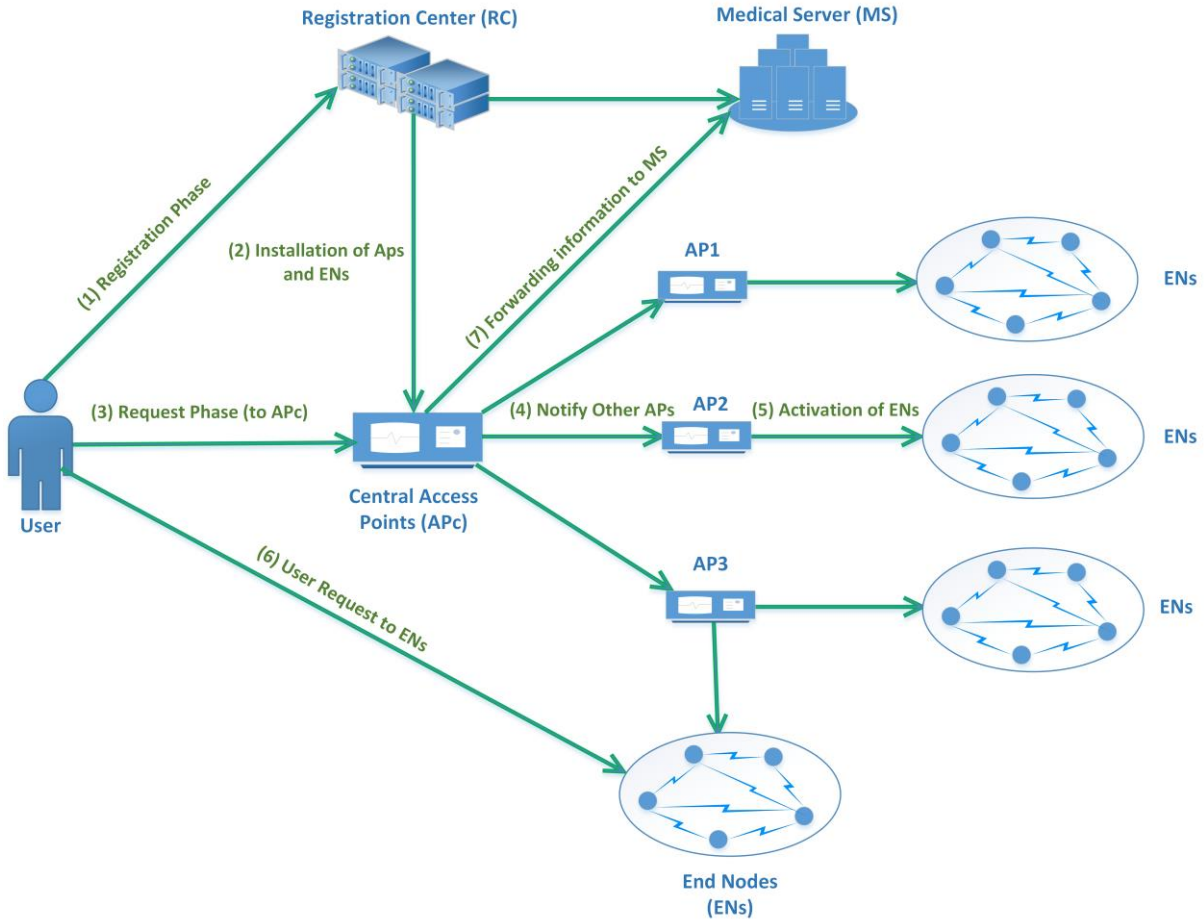

Fig. 2. System model for multiple user authentication in smart healthcare [1].

The proposed authentication scheme comprises seven key steps, detailed as follows:

1. Initially, the user's biometrics are registered and sent to the Registration Center (RC).

2. The Enrollment Server (ENS) and Authentication Processing Server (APS) then install appropriate key materials.

3. The user initiates service requests via the Authentication Processing Client (APC), capturing the user's biomedical credentials.

4. Upon successful verification by the APC, other APS nodes in the network are notified about the authenticated user and their requested healthcare services.

5. Various APS nodes deployed across hospital locations activate their associated medical sensors.

6. Users gain access to required medical services using a specific PIN code.

7. Finally, the ENS notifies the Medical Server (MS) regarding the requested services through the central Authentication Processor (AP).

The security of this authentication scheme is rigorously analyzed using the Cryptographic protocol Development and Verification Tools with Attack Detection (CDVT/AD) tool, demonstrating resilience against well-known security threats. Additionally, its performance in terms of communication and computational costs is evaluated and compared favourably with state-of-the-art remote-user authentication schemes, particularly excelling in the request and answer phases.

Furthermore, in the context of edge-enabled secure services, a conceptual three-tier security mechanism is formulated to address potential security threats within a three-tier IoT edge network architecture. This mechanism identifies seven key threat vectors (V1 to V7), representing major attack points where adversaries could potentially compromise the network:

- V1: Security threats on nodes within the local IoT cluster.

- V2: Vulnerabilities in communication channels of local IoT clusters.

- V3: Attacks between communication channels of local and edge networks.

- And so forth, up to V7, encompassing various aspects of the network architecture.

This conceptual framework aims to mitigate these identified threats through structured security measures tailored to the IoT edge network's specific layers and communication pathways.

The following section of this research introduces a conceptual security mechanism tailored for a three-tier architecture. This mechanism facilitates secure node bootstrapping and secure user access to digital services within smart and ambient environments.

The mechanism for secure node bootstrapping ensures that only legitimate nodes or smart objects can join or leave the network, thereby accessing or sharing available resources. Similarly, the secure user accessibility mechanism allows authorized users to access requested services exclusively from nearby smart environments.

The proposed framework for secure user access operates within a three-tier network and communication architecture:

- The local tier delivers essential, lightweight, and highly latency-critical secure services.

- Edge networks provide low latency but high computational services compared to the local tier.

- The global tier offers highly computational and resource-intensive services.

In the concluding part of this study, the performance and efficiency of the three-tier IoT-edge model are evaluated and compared with traditional cloud-IoT and two-tier edge-IoT models [29]. The evaluation focuses on three key network parameters: latency, energy consumption, and network utilization, as depicted in Fig. 4-6.

The results illustrate that the control algorithm's complexity (measured in millions of instructions per task, MI) directly impacts the network's end-to-end latency. Optimal latency values are observed until the complexity remains below 1.0E4 MI. Beyond this threshold, the edge layer emerges as the preferred location for deploying applications due to its ability to manage increased complexity effectively.

Furthermore, power consumption increases with higher computational demands. Regarding network usage, concentrating all control and logic at the local layer results in a higher network load at that tier. Distributing control or logic between the local and edge tiers distributes network usage accordingly across both layers.

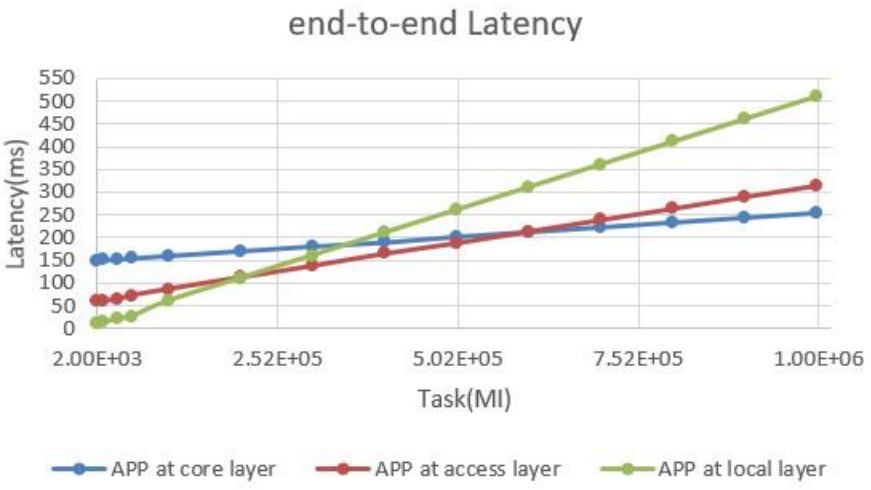

Fig. 4. End-to-end latency comparison [29].

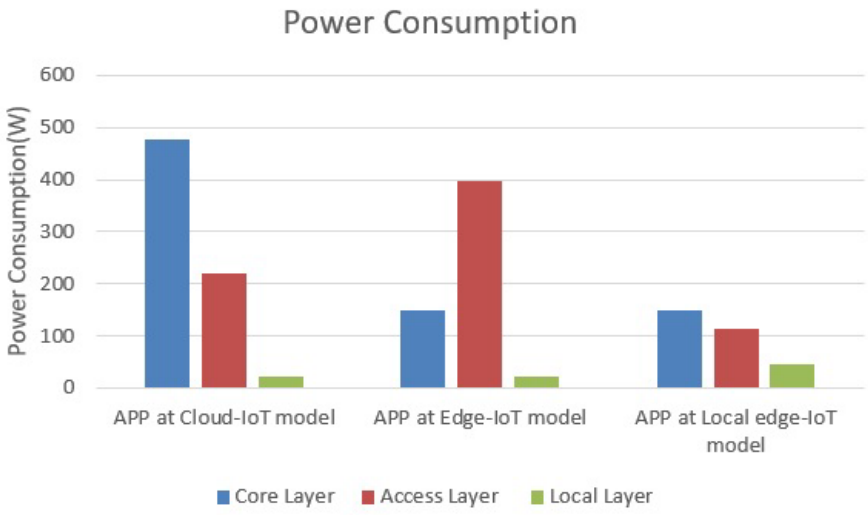

Fig. 5. Power consumption comparison [29].

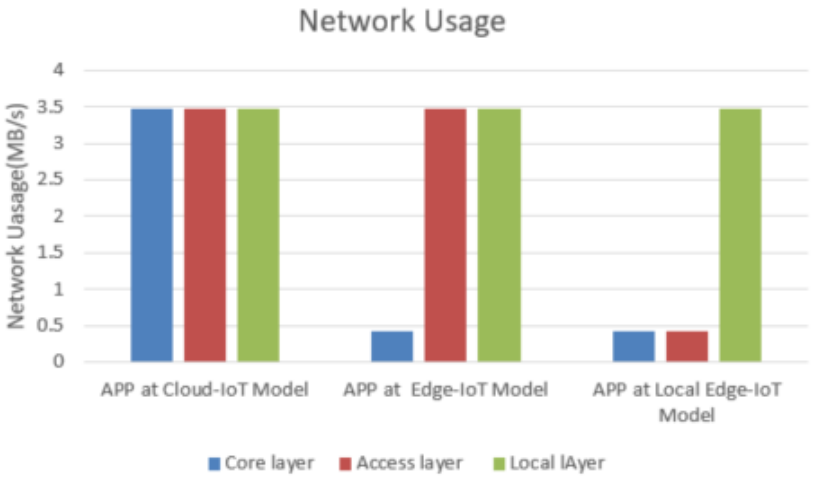

Fig. 6. Network usage comparison [29].

The final contribution of this thesis introduces a novel approach integrating blockchain technology into a three-tier IoT edge architecture to address critical requirements in IIoT networks. These include low-latency services, network reliability, trusted computing platforms, security, and privacy. This integration forms the Blockchain-Edge (BlockEdge) framework for IIoT applications [37].

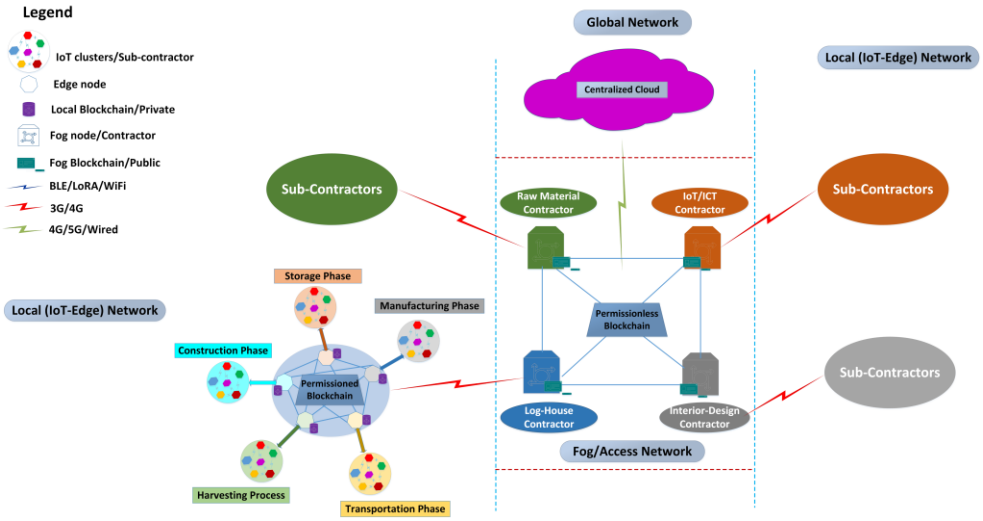

Fig. 7. BlockEdge Framework [1].

In this framework, depicted in Fig. 7, the local network (IoT-edge) comprises resource-constrained nodes connected to edge devices. Each regional network node hosts a lightweight, permissioned blockchain, enabling trusted data sharing, authorized access, and process monitoring. Fog networks possess more excellent computational resources than local networks and employ permissionless blockchains to ensure a trusted computing environment for stakeholders. With the highest computational capabilities, global networks or public clouds complete the three-tier architecture.

The performance of the BlockEdge framework is evaluated against three main network parameters: end-to-end latency, power consumption, and network utilization. Comparative analysis with non-blockchain IoT-edge models shows that both models find the local network optimal for tasks with complexity (MI) less than 2.02E5MI. However, the BlockEdge framework exhibits marginally better latency due to prioritizing delay-critical services locally and forwarding others to the Fog network (Fig. 8a, b). Notably, power consumption and network utilization in the BlockEdge framework are higher, attributed to additional computational tasks associated with blockchain integration.

Security is a critical consideration, and the thesis identifies potential threats across four layers of the BlockEdge framework: local, edge, global, and ledger. Threats range from attacks on lightweight virtualization platforms and short-range communication protocols at the local layer to sophisticated threats like 51% attacks at the ledger layer.

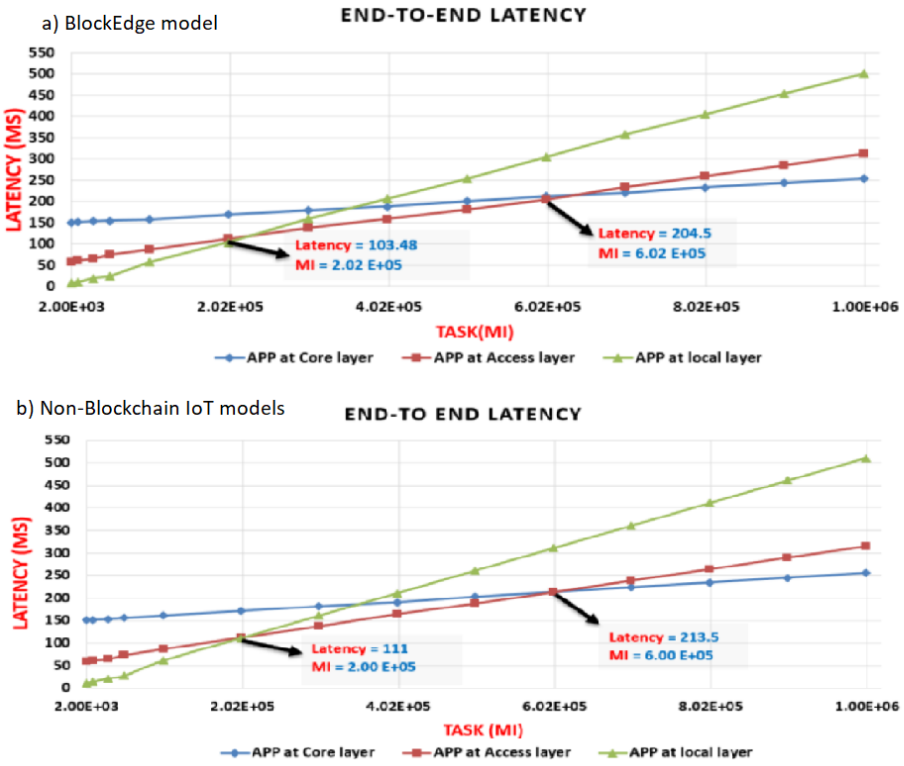

Fig. 8. End-to-end-latency: a). BlockEdge framework, b) non-Blockchain IoT models [37].

CONCLUSION

In conclusion, this research emphasizes secure edge-enabled services for intelligent environments, exemplified through applications in innovative healthcare and IIoT scenarios. Key contributions include a biometrics-based authentication protocol for gadget-free hospital environments and developing a secure three-tier IoT-edge architecture integrating blockchain technology. Performance evaluations highlight competitive advantages in latency while acknowledging increased resource demands in power consumption and network utilization compared to non-blockchain models.

REFERENCES

[1] A. Kamilaris and A. Pitsillides, “Mobile phone computing and the internet of things: A survey,” IEEE Internet of Things Journal, vol. 3, no. 6, pp. 885–898, 2016.

[2] M. M. Baig, H. GholamHosseini, and M. J. Connolly, “Mobile healthcare applications: system design review, critical issues and challenges,” Australasian physical & engineering sciences in medicine, vol. 38, no. 1, pp. 23–38, 2015.

[3] H. Xu and X. Geng, “People-centric service intelligence for smart cities,” Smart Cities, vol. 2, no. 2, pp. 135–152, 2019.

[4] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, “Security for 5g and beyond,” IEEE Communications Surveys Tutorials, vol. 21, no. 4, pp. 3682–3722, 2019.

[5] T. Kumar, A. Braeken, M. Liyanage, and M. Ylianttila, “Identity privacy preserving biometric based authentication scheme for naked healthcare environment,” in 2017 IEEE International Conference on Communications (ICC), 2017, pp. 1–7.

[6] T. Kumar, A. Braeken, A. D. Jurcut, M. Liyanage, and M. Ylianttila, "Age: authentication in gadget-free healthcare environments," Information Technology and Management, pp. 1–20, 2019.

[7] T. Kumar, P. Porambage, I. Ahmad, M. Liyanage, E. Harjula, and M. Ylianttila, "Securing gadget-free digital services," Computer, vol. 51, no. 11, pp. 66–77, 2018.

[8] I. Ahmad, T. Kumar, M. Liyanage, M. Ylianttila, T. Koskela, T. Braysy, A. Anttonen, V. Pentikinen, J.-P. Soininen, and J. Huusko, "Towards gadget-free internet services: A roadmap of the naked world," Telematics and Informatics, vol. 35, no. 1, pp. 82–92, 2018.

[9] T. Kumar, M. Liyanage, A. Braeken, I. Ahmad, and M. Ylianttila, "From gadget to gadget-free hyperconnected world: Conceptual analysis of user privacy challenges," in 2017 European Conference on Networks and Communications (EuCNC), 2017, pp. 1–6.

[10] K. Halunen, J. H¨aikiö, and V. Vallivaara, "Evaluation of user authentication methods in the gadget-free world," Pervasive and Mobile Computing, vol. 40, pp. 220–241, 2017.

[11] N. Hassan, S. Gillani, E. Ahmed, I. Yaqoob, and M. Imran, "The role of edge computing in internet of things," IEEE Communications Magazine, vol. 56, no. 11, pp. 110–115, 2018.

[12] Y. Sahni, J. Cao, S. Zhang, and L. Yang, "Edge mesh: A new paradigm to enable distributed intelligence in internet of things," IEEE Access, vol. 5, pp. 16 441–16 458, 2017.

[13] M. Satyanarayanan, "The emergence of edge computing," Computer, vol. 50, no. 1, pp. 30–39, 2017.

[14] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for internet of things realization," IEEE Communications Surveys Tutorials, vol. 20, no. 4, pp. 2961–2991, 2018.

[15] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," IEEE Communications Surveys Tutorials, vol. 19, no. 4, pp. 2322–2358, 2017.

[16] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," IEEE Communications Surveys Tutorials, vol. 21, no. 1, pp. 858–880, 2019.

[17] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 1972–1983, 2019.

[18] E. Harjula, P. Karhula, J. Islam, T. Lepp¨anen, A. Manzoor, M. Liyanage, J. Chauhan, T. Kumar, I. Ahmad, and M. Ylianttila, "Decentralized iot edge nanoservice architecture for future gadget-free computing," IEEE Access, vol. 7, pp. 119 856–119 872, 2019.

[19] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, "Internet-ofthings- based smart environments: state of the art, taxonomy, and open research challenges," IEEE Wireless Communications, vol. 23, no. 5, pp. 10–16, 2016.

[20] M. Gusev and S. Dustdar, "Going back to the roots—the evolution of edge computing, an iot perspective," IEEE Internet Computing, vol. 22, no. 2, pp. 5–15, 2018.

[21] Y. Nikoloudakis, S. Panagiotakis, E. Markakis, E. Pallis, G. Mastorakis, C. X. Mavromoustakis, and C. Dobre, "A fog-based emergency system for smart enhanced living environments," IEEE Cloud Computing, vol. 3, no. 6, pp. 54–62, 2016.

[22] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the internet of things," IEEE Access, vol. 6, pp. 6900–6919, 2018.

[23] T. Kumar, A. Braeken, V. Ramani, I. Ahmad, E. Harjula, and M. Ylianttila, "Sec-blockedge: Security threats in blockchain-edge based industrial iot networks," in 2019 11th International Workshop on Resilient Networks Design and Modeling (RNDM), 2019, pp. 1–7.

[24] W. Li and P. Wang, "Two-factor authentication in industrial internet-ofthings: Attacks, evaluation and new construction," Future Generation Computer Systems, vol. 101, pp. 694–708, 2019.

[25] C.-L. Lei and Y.-H. Chuang, "Privacy protection for telecare medicine information systems with multiple servers using a biometric-based authenticated key agreement scheme," IEEE Access, vol. 7, pp. 186 480– 186 490, 2019.

[26] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," Journal of network and computer applications, vol. 42, pp. 120–134, 2014.

[27] T. Kumar, M. Liyanage, I. Ahmad, A. Braeken, and M. Ylianttila, "User privacy, identity and trust in 5g," A Comprehensive Guide to 5G Security, pp. 267–279, 2018.