Securing Edge Services for Future Smart Healthcare and Industrial IoT Applications

Tanesh Kumar*, Mika Ylianttia*, Erkki Harjula*
*Centre for Wireless Communication, University of Oulu, Finland
{firstname.lastname}@oulu.fi*

***Abstract*—Secure and intelligent environments are crucial for fostering future IoT applications such as digital healthcare and Industry 4.0. Such smart environments must enable needed digital services to the respective users ubiquitously and fulfill critical requirements such as ensuring security, privacy, and low latency. This paper summarizes the dissertation work [1] through three major contributions, i) a lightweight biometrics-based user authentication mechanism in the smart and gadget-less healthcare environment, ii) a conceptual three-tier mechanism for secure nodes bootstrapping and secure users access for digital services, and iii) a Blockchain and Edge computing based network architecture for IIoT use case to fulfill the needed requirements such as low-latency, trust management, and security among others. The performance evaluation of the proposed framework is carried out, and the obtained results highlight valuable insight of this work for enabling a secure future hyperconnected environment for various applications.**

***Index Terms*—Security, Blockchain, Edge Computing, Industrial IoT, Smart Healthcare, Smart Environments.**

I. Introduction

Gadgets have already been considered the most popular and convenient mode for accessing digital services. For example, smartphones, laptops, tablets, PDAs are widely used in almost all domains of daily life and provide numerous valuable services, e.g., in the healthcare and banking sector [2], [3]. Recent advancements in communication, networking, and sensing technologies, along with the advent of 5G and beyond systems, allow the changing trend for service composition from the device-centric to the user-centric [4], [5]. In the next major digital transition, users can acquire the desired digital services without the assistance of hand-held gadgets. Instead, the nearby smart and intelligent surrounding spaces will offer the needed services to the users [6]–[8]. This vision of the gadget-free world is also known as the 'Naked World' with the main idea is that users are without hand-carry devices (i.e., naked is without carrying explicit gadgets) [9]–[11].

In order to realize the vision of a smart and gadget-free environment, appropriate mechanisms or solutions must be placed to address the number of key challenges. For example, one of the forefront challenges is to ensure the security and privacy of such intelligent environments [12]. Since the users in the smart surrounding will not have gadgets to input any text or PIN to authenticate themselves, the traditional two-factor authentication protocols may not be suitable in such situations [6]. Biometrics-based authentication schemes emerge as a prominent solution for the authentication of legitimate users in gadget-free surroundings [7], [13]. Furthermore, the network infrastructure of the future smart environment will comprise resource-constrained sensors or devices; it is, therefore, vital to develop an efficient and lightweight biometrics-based authentication mechanism.

In addition to security and privacy, enabling low-latency services are crucial for future smart delay-critical applications [14]. For example, smart healthcare and industrial IoT use cases may contain life-threatening or environment hazardous processes or phases requiring faster actions or rapid responses. Conventional cloud computing-based solutions are highly successful for different IoT applications in providing higher resources (e.g., computation and processing capabilities and storage). However, it may take longer delays, and therefore only cloud-based solutions are not optimal for latency-critical applications [15], [16]. In this context, Edge Computing (EC) can provide the needed low-latency services by bringing some of cloud computing capabilities near to the data source [17], [18]. Moreover, the concept of Mist computing or extreme edge will further take some computational capabilities and resources locally, i.e., near the sensors or devices [19], [20]. Hence, securing the edge and local networks is also a key requirement in smart environments.

Furthermore, Blockchain technology (Distributed Ledger Technologies) can serve the future intelligent environments by offering key characteristics such as decentralization, distributed trust, immutability, transparency, and authenticity, among others [21], [22]. Blockchain can combine with the edge-enabled network and communication architecture for future smart applications to attain utmost benefits presented by these two technologies [23], e.g., Edge computing helps provide low-latency services, and Blockchain can enable characteristics such as distributed trust and authentication.

Following are the key research questions considered in the dissertation [1]:

- How can a lightweight biometrics-based user authentication mechanism be formulated to access the services in a future hyperconnected smart environment optimally?
- How can an edge-based secure mechanism be designed for secure service accessibility in the future smart environment?
- How can the integration of the edge and blockchain integration benefit future smart applications?

978-1-6654-0601-7/22/$31.00 © 2022 IEEE

The rest of the paper is organized as follows: Section II provides the background for the dissertation. The main contributions of the thesis are elaborated in Section III and Section IV concludes the work.

II. Background

A. Towards future smart environments

The recent developments in Information Communication Technologies (ICT) have already indicated a digital transformation in the current way of accessing digital services. Instead of depending on gadget-based services, the future digital services can obtain by the nearby smart and intelligent surroundings without requiring the explicit gadgets [24]. This vision is known as the gadget-free world, or the Naked world, which assumes the user is entirely gadget-less, and the desired services will be provided by the smart environment [8], [11]. The transition from gadget to the gadget-free world is roughly categorized in three phases [7]. The first phase is 'Bearables,' which refers to the current gadget-oriented world. 'Wearables' is the second phase where users can get the required services from wearable devices such as smartwatches and smart clothes. The final phase in this transition will be 'Nearables' that refers to a gadget-free smart environment where the users can access similar services without hand-carry gadgets.

B. Enabling technologies for future smart environment

To enable the future smart environments, three major enabling technologies are identified from the state-of-the-art, i.e. IoT and Edge paradigms and Blockchain technology. IoT is considered as fully connected digital ecosystem where enormous smart things (sensors and computing devices etc.) connected through network and communication technologies to execute the needed tasks or deliver required services [25]. Cloud computing platform offers richer resource capabilities to massive IoT networks, but it can also cause higher network delays and might not be suitable for delay-intolerant applications [26]. The concept of edge computing fill this gap by introducing an intermediate tier between the local or device layer and public cloud that can provide part of the cloud services near to the user or the device [27]. Mist computing even bring some of the computation and processing capabilities at the local network, i.e. on the nodes/devices [28]. Blockchain technology is another key technology enabler for the future smart environment that brings several key features such as decentralization, immutability, and transparency among others [21], [22].

C. Overview of IoT edge models

The state-of-the-art study presents three major IoT-edge models, as highlighted in Fig. 1. The first one is the traditional cloud-IoT model, which has been widely used over the years in various applications [29], [30]. In this model, the IoT nodes or device layer is used to sense and gather the information and then send it to the cloud platform for further processing, analysis, and storage. The second model is a two-tier IoT-edge model that enables edge networks capabilities at the access level (between the IoT nodes and cloud) and is considered highly useful for latency-critical applications [29]. The third one is the three-tier IoT edge model that can be seen as an extension of the previous model that brings some computational capabilities at the local networks [24]. In this work, a model is formulated which combines the capabilities of edge computing and Blockchain for IIoT applications to attain different requirements such as low-latency services and trust management [31].

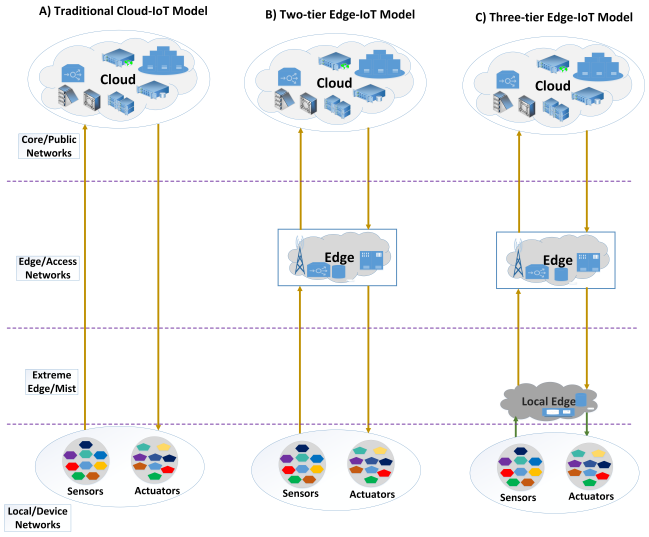

Fig. 1. Various IoT edge models [1].

D. Security overview for smart environment

In order to access the requested services from the nearby smart surroundings, it is vital to have a secure authentication mechanism for gadget-free users. Traditional two-factor and three-factor authentication protocols proposed in the literature are mainly preferred in the cases when users carry any form of gadgets with them, but they might not be well-fit for the gadget-free users [32], [33]. Biometrics-based authentication mechanisms have emerged as one of the most viable solutions in such smart environments [13]. In addition, since the edge computing-based network architecture is expected to play a huge role in the future smart environment, it is essential to develop solutions to secure the edge networks [34]. Furthermore, managing the privacy of the user's sensitive information is one of the forefront requirements in such environments because, unlike the gadgets, there will not be a separate or private display screen for the users. Along with privacy, establishing trust among users and various involved network entities is vital for intelligent environments [35], [36].

III. Contributions of Thesis

Before going through details of the actual contributions, it is important here to first briefly mention the two different use

cases used for this research work, i.e., future smart gadget-free healthcare environment and Industrial IoT [7], [37].

Smart Gadget-Free Healthcare Use Case: The main idea behind this use case is that a user without hand-held gadgets (e.g., smart phone, tablets, PDAs) can able to access the medical services in a hospital environment or even remotely at home. For example, disabled persons, patients requiring emergency services, and patients who can not make much physical effort go through the different formalities in the hospital to acquire the needed medical services. The gadget-free healthcare environment will allow the user's to get the required services from a nearby smart environment, e.g., registration of the user and providing primary healthcare services.

IIoT Use Case: A smart "log-house construction" scenario is the second use case considered in this thesis work. This use case comprises multiple key industrial phases such as i) harvesting of woods from the forest, ii) collection and delivery of the harvested woods through transportation, iii) making wood logs from raw material in a factory, iv) storage in the warehouse and v) taking to the construction site. The key objective is to monitor the critical industrial phases, enable secure and trusted data sharing among various stakeholders, ensure low-latency services in unstable network conditions, and maintain the records for all phases.

A. Lightweight biometrics authentication mechanism in smart environment

The main objective of this research contribution is to ensure that the needed medical services are only accessed by authorized gadget-free users in the smart healthcare environment. For this purpose, a lightweight biometrics-based authentication protocol is formulated [6], [7]. As shown in Fig. 2, the major entities used in the protocol include the Access Points (AP_S), the Central Access Points (AP_C), the Registration Center (RC), the Medical Server (MS), the End Nodes (EN_S), and the User (U).

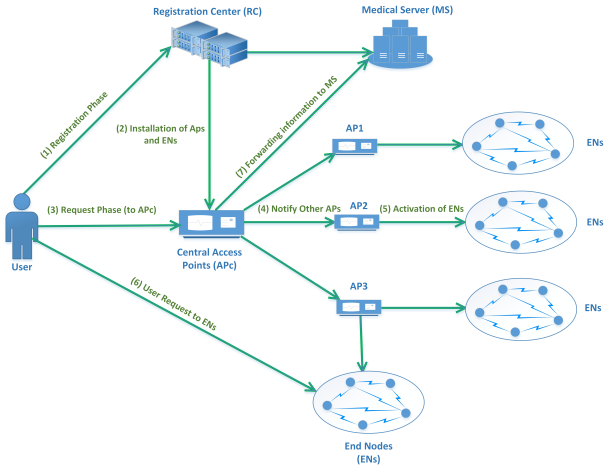

Fig. 2. System model for multiple user authentication in smart healthcare [1].

The proposed authentication scheme constitutes seven key steps, and their working is as follows: in the first step, the registration of the user's biometrics and sent to (RC). In the next step, (EN_S) and (AP_S) install the suitable key material. Next, the user requests the required services using the (AP_C) by capturing the user's biomedical credential, and on the successful verification, the (AP_C) will inform other (AP_S) in the network regarding the authenticated user and the desired healthcare services. Various (AP_S) deployed in different hospital locations triggered their associated medical sensors. The users can access the needed medical services with a particular pin code. In the end, (EN_S) will notify (MS) regarding the services through the central (AP).

Security analysis of the proposed authentication is performed using a formal verification tool, i.e., Cryptographic-protocol Development and Verification Tools with Attack Detection (CDVT/AD) tool, and it resists the well-known security threats. Furthermore, the proposed scheme's performance is evaluated in terms of communication and computational cost and compared with state-of-the-art schemes. According to the empirical results, the communication and computation costs of the proposed scheme has performed better as compared with the other remote-user authentication schemes for the two major steps i.e. request and answer phase.

B. Conceptual design of edge based secure services

In this research contribution, an edge-enabled conceptual three-tier security mechanism is formulated to mitigate the potential security threats on three-tier IoT edge network architecture. The first part of this contribution identifies seven key threat vectors for the three-tier architecture that can consider as seven major attack points where the adversaries can potentially launch the attacks and compromise the network [8]. These vectors can be represented by V1, V2, and up to V7, as shown in Fig. 3. Furthermore, V1 refers to the security threats on the different nodes at the local IoT cluster, V2 is the potential vulnerabilities at the communication channels of the local IoT clusters, V3 are attacks between the communication channel of local and edge networks, and so on.

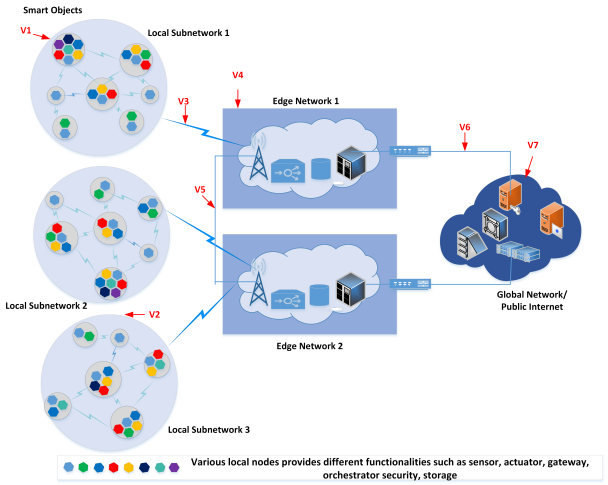

Fig. 3. Three-tier edge IoT architecture for smart environment [1].

The next part of this research proposes the conceptual security mechanism for three-tier architecture that enables mechanisms for; i) secure nodes bootstrapping and secure user access to the digital services from the smart and ambient environment. The secure nodes bootstrapping mechanism allows only legitimate nodes or smart objects to join or leave the network and access or share the available resources. Secure user accessibility mechanism can only grant permission to the authorized users to access the requested services from the nearby smart surroundings. The proposed secure user access framework is based on three-tier network and communication architecture, i.e., the local tier can deliver basic, lightweight and highly latency-critical secure services, the edge networks can also provide low-latency but high computational services compared to the local tier, and the global tier can provide highly computation and resource intensive services.

The final part of this contribution evaluated the performance and efficiency of the three-tier IoT-edge model and compared it with the traditional cloud-IoT model and two-tier edge-IoT model [29]. The Performance of the model is evaluated in terms of three key network parameters, i.e., latency, energy consumption, and network utilization, as shown in Fig. 4-6. The results demonstrate that the complexity (millions of instructions per task, MI) of the control algorithm directly impacts the end-to-end latency of the network. The latency has the most optimal values until the complexity is less than 1.0E4 MI. With the increase in complexity, the edge layer is the most appropriate location for placement for the application. The power consumption of the network rise with the increase in the computations. In the case of network usage, when all control/logic is running at the local layer, there is a higher network load at the local tier. When the control or logic is divided on both the local and edge tier, the network usage is also inflicted on both layers.

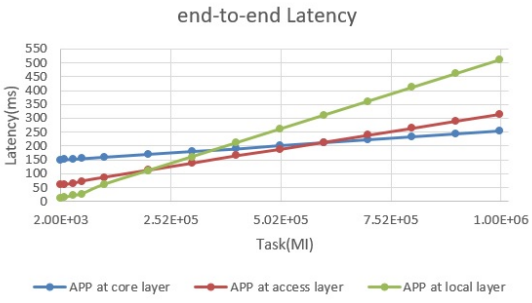

Fig. 4. End-to-end latency comparison [29].

C. BlockEdge framework for smart applications

The final contribution of this thesis introduces the concept of blockchain technology for three-tier IoT edge architecture to fulfill the various essential requirement in the current IIoT networks such as low-latency services, network reliability, trusted computing platform, security, and privacy, among others. For this purpose, a Blockchain-Edge (BlockEdge) enabled three-tier framework for IIoT use case is formulated

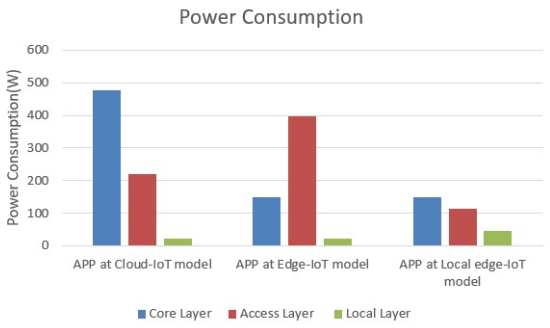

Fig. 5. Power consumption comparison [29].

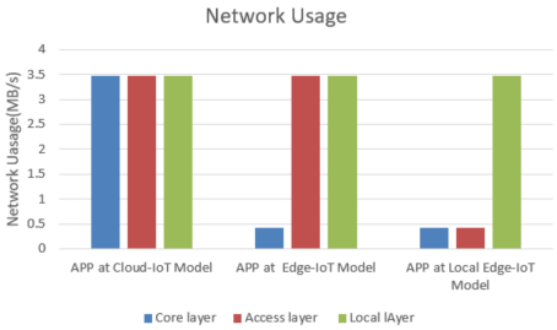

Fig. 6. Network usage comparison [29].

in this research [37]. As shown in Fig. 7, the local network (also known as IoT-edge) contains the IoT cluster having resource-constrained nodes connected to their respective edge devices to ensure the availability of the resources for running the local processes. Lightweight permissioned blockchain is deployed at various edge devices of the local networks to enable trusted data sharing, authorized access, and monitoring/tracking various processes. Fog networks possess higher resources and computation than the local network and can provide computational intensive services. At fog networks, permissionless blockchain is deployed to enable a trusted computing environment for various involved stakeholders. The global networks or public clouds are the layers with the maximum resources and computational capabilities.

Next, the performance of the proposed BlockEdge framework is evaluated in the context of the three main network parameters, i.e., end-to-end latency, power consumption, and network utilization, and compared with the non-blockchain IoT-edge models. The result shows that when the complexity (MI) is less than 2.02E5MI, the local network for both BlockEdge model and non-Blockchain IoT model is the optimal location for the placement of the algorithm. However, the latency taken by the proposed BlockEdge Framework is marginally better than the non-Blockchain because only very delay-critical service requests are processed at the local network, and the rest are forwarded to the Fog network for needed processing, as shown in Fig 8 (a, b). The values for power consumption and network utilization of the BlockEdge

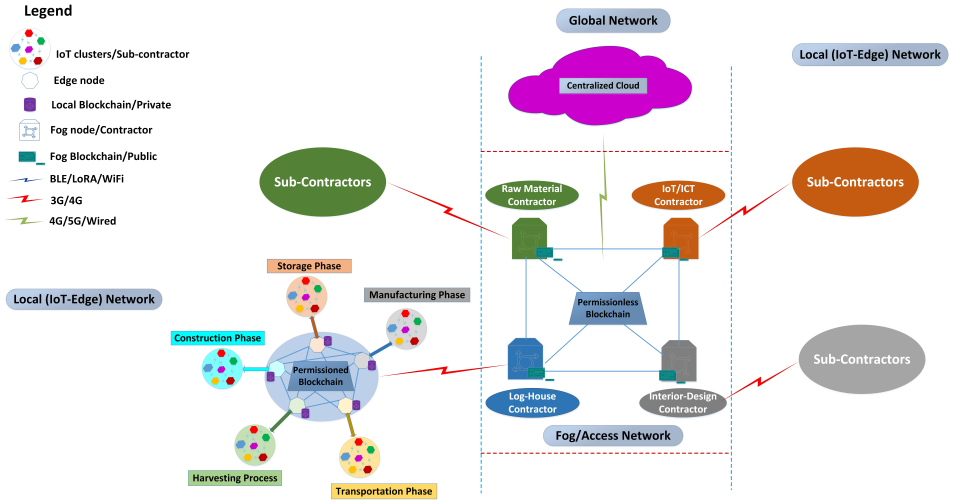

Fig. 7. BlockEdge Framework [1].

framework are higher than the non-blockchain models due to the higher computational and processing tasks with the inclusion of Blockchain in the network.

The final part of this research contribution deals with the identification of the potential security attacks in the BlockEdge framework for the IIoT use case [31]. In order to analyze the threats, the proposed framework can be divided into four key layers, i.e., local layer, edge layer, global layer, and ledger layer. Adversaries can target the local tier through various attacks, e.g., on the lightweight virtualization platform (docker containerization), the short-range communication protocols, and local nodes or devices. The edge layer can have several vulnerabilities on edge virtual machines, devices, and gateway nodes. The traditional cloud layer may have well-known threats, e.g., Dos/DDoS attacks. Several attacks are possible at the ledger tier, such as smart contract threats (in coding), platform-based threats (DAO), and 51% attacks.

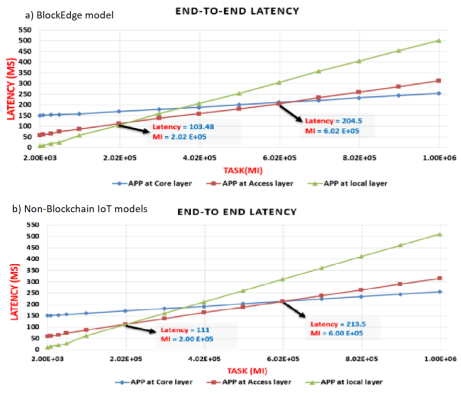

Fig. 8. End-to-end-latency: a). BlockEdge framework, b) Non-Blockchain IoT models [37].

IV. Conclusions

The dissertation elaborated in this paper examined the various mechanisms to ensure secure edge-enabled services for future smart environments. Smart healthcare and an IIoT use case have been taken to demonstrate the proposed security mechanism and analyze the obtained results. First, the thesis proposed a lightweight biometrics-based authentication protocol in a gadget-free hospital scenario, and the validation of the protocol is performed using the CDVT/AD tool. Moreover, the performance evaluation of the proposed authentication is made in the context of communication and computation costs, and optimal results are obtained compared with state-of-the-art authentication mechanisms.

Second, conceptual three-tier secure nodes bootstrapping and user accessibility mechanisms are formulated. The performance of three-tier IoT-edge architecture is evaluated in terms of end-to-end latency, energy consumption, and network utilization and shows better performance when compared with state-of-the-art IoT models. Third, Blockchain and Edge integrated three-tier 'BlockEdge' framework is proposed, and the performance is evaluated and compared with the non-Blockchain IoT-edge models. The proposed BlockEdge model performed slightly better than the non-Blockchain models in terms of latency. However, the energy consumption and network utilization of non-blockchain are marginally better than BlockEdge because the proposed framework has taken more processing and computation resources to run the Blockchain.

Acknowledgment

This work was funded by the Finnish Funding Agency for Innovation (TEKES) projects: The Naked Approach and Towards Digital Paradise. This work was also supported by Academy of Finland, under the projects: Industrial Edge and 6G Flagship projects (grant 318927). Further support provided by Nokia Foundation, Riita and Jorma J. Takanen, HPY Foundation, KAUTE Foundation, and University of Oulu Graduate

School (UniOGS). Authors would also like to acknowledge Nokia Foundation for providing support through Jorma Ollila Grant 2021 and to the DigiHealth Project (grants 326291) funded by the Academy of Finland.

REFERENCES

[1] T. Kumar, "Secure edge services for future smart environments, d.sc. dissertation, university of oulu, 2020. [online]. http://jultika.oulu.fi/record/isbn978-952-62-2798-6."

[2] 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.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] I. Yaqoob, L. U. Khan, S. M. A. Kazmi, M. Imran, N. Guizani, and C. S. Hong, "Autonomous driving cars in smart cities: Recent advances, requirements, and challenges," *IEEE Network*, vol. 34, no. 1, pp. 174–181, 2020.

[10] L. U. Khan, I. Yaqoob, N. H. Tran, S. M. A. Kazmi, T. N. Dang, and C. S. Hong, "Edge computing enabled smart cities: A comprehensive survey," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.

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

[17] 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.

[18] 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.

[19] J. Islam, T. Kumar, I. Kovacevic, and E. Harjula, "Resource-aware dynamic service deployment for local iot edge computing: Healthcare use case," *IEEE Access*, vol. 9, pp. 115 868–115 884, 2021.

[20] M. Ejaz, T. Kumar, I. Kovacevic, M. Ylianttila, and E. Harjula, "Healthblockedge: Blockchain-edge framework for reliable low-latency digital healthcare applications," *Sensors*, vol. 21, no. 7, p. 2502, 2021.

[21] 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.

[22] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Computers & Security*, p. 101966, 2020.

[23] 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.

[24] E. Harjula, P. Karhula, J. Islam, T. Leppänen, 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.

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

[26] 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.

[27] 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.

[28] P. Galambos, "Cloud, fog, and mist computing: Advanced robot applications," *IEEE Systems, Man, and Cybernetics Magazine*, vol. 6, no. 1, pp. 41–45, 2020.

[29] M. Ejaz, T. Kumar, M. Ylianttila, and E. Harjula, "Performance and efficiency optimization of multi-layer iot edge architecture," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*, 2020, pp. 1–5.

[30] 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.

[31] 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.

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

[33] 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.

[34] Y. Li, Q. Cheng, X. Liu, and X. Li, "A secure anonymous identity-based scheme in new authentication architecture for mobile edge computing," *IEEE Systems Journal*, pp. 1–12, 2020.

[35] 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.

[36] 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.

[37] T. Kumar, E. Harjula, M. Ejaz, A. Manzoor, P. Porambage, I. Ahmad, M. Liyanage, A. Braeken, and M. Ylianttila, "Blockedge: Blockchain-edge framework for industrial iot networks," *IEEE Access*, vol. 8, pp. 154 166–154 185, 2020.