Leading Edge

Edge Computing and IoT Data Breaches: Security, Privacy, Trust, and Regulation

David Kolevski
School of Computing and Information Technology
University of Wollongong
Wollongong, NSW 2522, Australia

Katina Michael
School for the Future of Innovation in Society
Arizona State University
Tempe, AZ 85287 USA
and
School of Computing and Augmented Intelligence
Arizona State University
Tempe, AZ 85281 USA

Edge computing is an emerging computing paradigm representing decentralized and distributed information technology architecture [1]. The demand for edge computing is primarily driven by the increased number of smart devices and the Internet of Things (IoT) that generate and transmit a substantial amount of data, that would otherwise be stored on cloud computing services. The edge architecture enables data and computation to be performed in close proximity to users and data sources and acts as the pathway toward upstream data centers [2]. Rather than sending data to the cloud for processing, the analysis and work is done closer to where the source of the data is generated (Figure 1). Edge services leverage local infrastructure resources allowing for reduced network latency, improved bandwidth utilization, and better energy efficiency compared to cloud computing.

Digital Object Identifier 10.1109/MTS.2024.3372605
Date of current version: 12 April 2024.

Emergence of IoT and connected devices

The emergence of the IoT, and connected devices and services have changed the way consumers live, businesses work, and governments interact with their stakeholders. No matter where you look today, you will find a smart object affixed to something or someone, somewhere. According to Ni et al. [3], IoT will enable an evolution from the cloud to the edge and reduce computational constraints on cloud services. Smart devices come in many form factors and are increasingly mobile, lightweight and unobtrusive. Who has ownership of the device? Is the device actively generating and transmitting the data back to the edge node? And are citizens aware that they are actively monitored by these objects and devices?

0278-0097/24©2024 IEEE

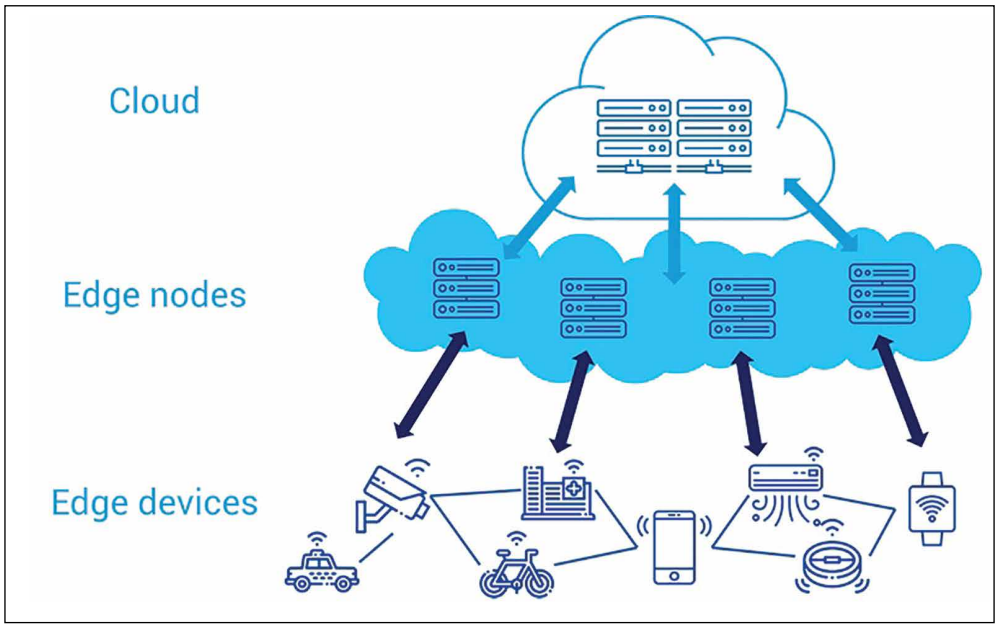

Figure 1. Cloud, edge nodes, and IoT/connected edge devices (Source: infoPLC, created 2 December 2019).

Edge computing enables computation to be performed at the edge of the network, at the point where users require access to services. [2]. Currently, many IoT devices are generating continuous data streams. To quantify the size of the edge computing challenge, there will be an estimated 29.42 billion IoT-connected devices by 2030 [4]. A city, for example, with 1 million people in 2019, was producing about 180 petabytes of data per day [5] with enormous potential benefits in data-driven innovation serving the public interest. With this constant streaming of various kinds of data emanating from IoT devices, it is important that data processing and storage is concentrated toward the edge of the network to negate the need for longer transmission times and continuous processing improvements. Increasingly, manufacturers of edge devices are building multifunctionality into their products and users simply take advantage of all available features without considering the network and storage implications and constraints. Smart cities will rely on edge devices to fuel the data-driven economy, providing new insights into local challenges and potential futures.

Socio-technical challenges

In a 2017 study by Lin et al. [6], it was found that edge services provide improved data processing, storage and quality of service (QoS), suitable for future IoT infrastructure solutions. Abbas et al. [7] also concluded that mobile cloud computing (MCC) faced challenges with high latency and inefficient energy device utilization which could be addressed by edge computing solutions. Thus, MCC was less suitable for real-time applications and scenarios requiring a high quality of service (QoS). These are just some of the design challenges that many businesses face with major implications for addressing systems objectives. Buyya et al. [8] present the outlook of edge computing, including the technology design, security architecture, and integration with cloud services, however, they neglect to centrally address the regulatory workings of distributed services. Similarly, Shi et al. [9] reviewed the social and technical challenges of edge computing providing recommendations for service utilization and consumption, but neglected the environmental issues prevalent in edge computing devices. With the predicted growth of the edge device sector, the energy requirements cannot be underestimated. This commentary will discuss the emergent security, privacy, trust, and regulatory issues linked to edge computing in the context of IoT and corresponding data breaches.

From the cloud to the network edge

The concept of edge computing stems back to the 1990s when content delivery networks (CDNs) were introduced to enhance web performance [10],

and load balancers were used in the data center to handle incoming traffic in the available servers, managing peak times of usage. AWS describes three generations of CDNs: 1) on data center replication and with a focus on intelligent network traffic management; 2) a concentration on multimedia content and especially on services like video-on-demand delivered right to the mobile/tablet/edge device; and 3) a shift in emphasis to the edge, away from web services that are centralized in the cloud toward the management of bandwidth consumption through intelligent communications using smart devices [11]. Akamai, founded in 1998, was one of a number of CDN providers enabling caching of web content to be stored and processed on CDN nodes.

While early use cases of edge computing share similar attributes to that of CDNs, the edge extends the boundary of data generation and processing. Abbas et al. [7] write that edge services will play a pivotal role in web optimization, such as enabling HTML content to be more available locally, rather than on the central server. This has major implications for how artificial intelligence (AI) and ultra-low power machine-learning (ML) applications will be incorporated into the network edge, and how breakthrough technologies, such as neuromorphic computing and TinyML will allow for enhanced user experiences, that were previously impossible [12]. IoT services, such as smart traffic lights, healthcare tracking, shopping cart management, and big data analytics will enjoy the advantages of edge computing [3].

Security

Edge computing presents a unique set of security challenges, such as the potential for the unauthorized access and capture of sensor information from connected devices by hackers. It is well-known that given the size and computing power available on some edge devices, there are inherent limitations in available security methods [5]. Shi and Dustdar [5] state that supporting edge security will continue to be a challenge due to the complexity and pervasive nature of the network topology. Similarly, Ni et al. [3] state that IoT devices are vulnerable to hacking due to their limited computing resources and low resilience to persistent attacks.

Lack of security impacts trust in relationships

Edge computing security challenges the existing trust that end-users have when using device-level services [13]. Better securing IoT devices increases the trust relationship between the user the manufacturer, and the service provider. However, many IOT-based surveillance cameras and alarm systems, for instance, carry default passwords like "0000" and, in other cases, do not have any security mechanism whatsoever, leaving them open for anyone who wishes to gain access to them [14]. When users of these devices find out about the lack of security onboard, particularly while the whole aim was to secure physical premises that contained expensive tools and assets, there is an instant loss of trust in technology and the designers and developers of the technology [15]. Sharan et al. [13] identify that the main weakness in such established relationships is a failure to understand that *both* security and privacy impact trust between the user and the service provider.

Characteristics of edge computing overcoming or posing new security challenges

The hierarchical network topology of edge computing is considered to be a "double-edged sword" [16]. On the one hand, it provides security protection by the distribution of data between the nodes, and, on the other hand, it also presents security vulnerabilities at the different layers of communication between the end device, the edge, and the cloud infrastructure. Consider, for example, a critical health application on an edge device that monitors a heart pacemaker in a patient, and then each night, the data is uploaded from the edge device to the cloud from the patient's home [17], with varying topologies and configurations given breakthroughs in wireless technologies. Other security challenges in edge computing relate to attacks performed between different interconnected devices, such as man-in-the-middle (MITM) attacks, eavesdropping, and tampering attacks [18]. Sendhil and Amuthan [18] describe how hackers are applying known types of attacks to edge services. Similarly, denial of service (DoS), tampering, eavesdropping, and waterhole attacks targeting lightweight IoT devices pose challenges that traditional cloud security methods could not entirely deter [19].

Additional studies demonstrate that security challenges in edge computing include authentication constraints, due to the distributed network design and multiple stakeholders engaged in flows of communication [7]. For example, in cloud services, the centralized entity is responsible for authenticating

users and devices. Distributed edge services are different in that they operate under a multidomain environment, and it is difficult to authenticate with centralized upstream services. According to Bangare and Patil [20], IoT is one of the most complex technology ecosystems, operating with diverse stakeholders. This complexity brings challenges with addressing the protocols associated with service delivery, service level agreements (SLAs), and cybersecurity frameworks. Similarly, [21] states that reduced performance metrics could breach the SLA between stakeholders while providing minimum service portability options to the user. Hassija et al. [22] discuss the issues related to device-to-device connectivity and the requirement for dynamic SLA security features. Special attention needs to be provided to SLAs which enforce agreements across multiple platforms as they allow IoT users the features required to safeguard them against attacks.

Addressing security at the network edge

Encryption

Threats and attacks on cloud computing have been extensively researched and these solutions do not scale at the network edge, due to device-related lightweight specifications. Ren et al. [16] promote the concept of trust and authenticating IoT devices within each layer, end device, edge, and cloud infrastructure. Similarly, Mosenia and Jha [23] state that strong encryption methods provide further resilience against IoT and edge computing services; however, IoT remains vulnerable to persistent attacks. IoT device limitations such as processing and memory capacities continue to cause a significant challenge for encryption methods.

Blockchain

Hassija et al. [24] propose blockchain technology and smart contracts to increase security in edge computing environments where governments tender services. The researchers identify that a decentralized tendering system could be applied to Ethereum allowing for the control of data because it is accessed based on identity authentication. Similarly, Li et al. [25] also investigated the blockchain ledger to address security and access control using Ethereum. The authors in the study applied Ethereum smart contract functionality to execute the required business logic sets to validate device identity and then validated the requested data via the ledger. In both [24] and [25], Ethereum was applied to validate the authentication and integrity of edge devices; and in [25] it was applied to a hospital-patient use case.

Blockchain microservices and virtualized applications

While cloud computing services have seen the advantages of rapid service deployment, bandwidth, connectivity, and latency are issues that continue to put strain on device and application usage [2]. Ren et al. [16] state that edge computing will increasingly use virtualization techniques, however, with a more lightweight approach to cloud services. Emerging technologies, such as Linux server configuration (LXC, isolating one operating system to one container) and Docker containers (isolating one application to one container) are applied on lightweight devices, enabling virtualization without compromising requirements. The rapid growth of cloud-based services led to an explosion of data being sent over the Internet requiring ever-increasing bandwidth capacity, which was plainly not optimal [26]. Therefore, the authors state microservice applications coupled with container virtualization could be deployed for simplified edge processing and storage services. Both [16] and [26] propose containers providing virtualization services, promoting fast boot time and lightweight energy inputs.

Privacy

"Privacy" can be interpreted in many different ways. There may be privacy 1) of the "person"; 2) of "behavior"; 3) of "communications"; and 4) of "personal data" [27]. We will be focusing on the latter two types, in this section. Personal data, which also goes by the name of "data privacy" or "information privacy," can be defined as an individual's right to have control over the data that is personally linked to them, whether available to other individuals, organizations they interact with, or even a third party that might store that data [28]. Privacy in communications is directly related to the network edge, given flows of transactions between components in a network setting that are vulnerable to attack.

Data privacy at the edge

Data privacy is a topic of major concern due to the pervasive nature of IoT devices. Satyanarayanan

[10] refers to the established concept of Cloudlets in their paper, which extends cloud fundamentals at a more granular level, toward edge nodes and the reduction of overcentralization. Edge computing extends privacy concerns with increasing functionality like location awareness and lightweight IoT devices which possess limited data protection methods [16]. Hagan et al. [29] note that cloud privacy and security breaches have become important challenges in centralized data processing and storage services, and while edge services are bringing these closer to the network boundary, breaches can still happen. All stakeholders need to be aware that the privacy of the end-user can be jeopardized without their immediate knowledge [30]. End-users are often one of the last stakeholders to learn that their data has been stolen, quite often only when a significant privacy breach has occurred and the breach is publicly announced due to mandatory data breach notification (MDBN) legislative requirements [19]. A distributed information technology architecture at the edge should generally have the advantage of minimizing privacy breaches "at scale." However, if an edge node is targeted by hackers, many edge devices can be affected all at once (refer to Figure 1). Whereas a cloud computing data breach might have compromised hundreds of millions of individual records in a single attack (e.g., due to an unsecured S3 bucket), in the future edge devices will be vulnerable to peer-to-peer network architectures, given the potential for malware to penetrate and spread in systems.

Access control and data protection

The primary use case for IoT integration is to share data between the huge number of devices that transmit sensor data. Thus, researchers are preoccupied with privacy implications relating to edge device access control. When edge devices are compromised and an individual's privacy has been breached, the device is said to have been the "target," although personal data is what the hacker can claim as an outcome. While we have yet to observe breaches of this kind "at scale" when compared to some of the major cloud computing hacks of the last decade, this is the next frontier as we move from 5G to 6G networks. These privacy breaches may fall into one or more of the following categories: 1) access offenses; 2) the impairment of data; 3) the misuse of devices; and 4) the interception of data [31, ch. 2–6].

IoT by its very nature makes the end-user vulnerable to "tech abuse" in particular contexts (e.g., the use of technology in the context of domestic violence [32]). Consider how a malicious actor may aim to penetrate the personal privacy of an end-user via an IoT device. There have been many reported examples of "smart abuse" by victims, and these will continue to increase [33] having asymmetric effects on individuals and their wellbeing. Imagine the possibility of an attack on edge devices on the home network that allowed the hacker to access the front door lock, smartTV, doorbell, home lighting, security cameras, speakers, and so on, remotely. The invasion of privacy would be so great that it would cause significant mental anguish in the victim of the attack.

According to Aleisa et al. [34], access control is integrated between the usability of the edge service and the flow of data between the devices and the user authentication process. Likewise, Shimahara and Nishi [35] investigated access control between integrated edge services and concluded that services should be determined by the level of access required by the users. The study also stated that access control needs to fulfill the requirements of data protection regulations [e.g., General Data Protection Regulation (GDPR)]. Li et al. [25] discuss IoT devices that share sensitive information such as healthcare and medical information that must adhere to health-related privacy regulations. The authors noted that service providers need to abide by encryption- and decryption-based rules during access control.

Disclosed PII

IoT devices continue to generate, store, and process enormous amounts of personally identifiable information (PII), usernames and passwords, financial information, location data, and health-related information [23]. Disclosed PII, financial, and location data are extensively surveyed in the literature with respect to cloud computing data breaches (e.g., [19]). We [19] investigated the 2011 Sony PlayStation Network (PSN), 2014 eBay, and 2014 Yahoo! cloud data breaches. The outcome of the study was that data breaches would continue to increase, requiring the security industry to further enhance data security methods. In an edge computing scenario, the threat landscape is further exacerbated by

the IoT device generating additional data that would have otherwise been limited in a cloud computing scenario [23].

Biometrics

A recent study by Cheng et al. [36] focuses on privacy protection in biometric systems, specifically facial recognition. The authors state that biometric authentication has been applied to e-commerce, banking, government, and military systems. Major concerns now reside with deepfakes and other morphing attacks [37]. While facial and fingerprint biometrics are now integrated into portable hard drives, smartphones, and other edge devices, duping attacks will become commonplace [38]. The introduction of AI into the hacker's toolkit will mean that proving one's own identity at the edge will become harder, likely necessitating two-factor authentication [59].

Location-based services

Location-based services (LBSs) have enjoyed popularity from online consumer purchases to business tracking inventory [39]. Edge computing brings LBS closer to the consumer using smartphones, smartwatches, and, in ever-increasing cases, implantable devices. Sendhil and Amuthan [18] state that IoT devices are susceptible to location privacy leakage with the attacker knowing the user's geographical location. There are also covert ways in which proximal geolocation can be determined, possibly placing users at risk, if they are unaware someone/something knows their whereabouts. This is especially troublesome in cases of stalking or the context of restraining orders. An edge device's location can also be spoofed, rendering a device somewhere other than where it actually is physically [40]. This latter scenario can create all sorts of problems for service providers, despite maintaining an individual's location privacy.

Trust

Users can gain trust in a service if they can observe stakeholders within that technology ecosystem taking responsibility for their actions [41]. Singh et al. emphasize that unless trust is embedded as a value in the systems design process, to begin with, the potential for IoT will not be realized. In a study by Sendhil and Amuthan [18] that investigated trust, privacy, and security issues in edge computing, it was found that user trust, in particular, needed to be addressed. One way to ensure trust, is through the use of new edge computing protocols and user interfaces, so that people can interact with their devices to learn more about a given context. Along with new user interfaces, transparency around security patches and protecting IoT device integrity is a key measure in increasing user trust. This position is supported by Cheryl et al. [42], who stated that users who have more control of their IoT device, including better user interfaces and ownership of data, have an increased trust in their service provider. The three studies highlight the importance of trust within an edge and IoT ecosystem. The latter study is unique in that it uses a case study method to evaluate end-user trust and data protection in the Malaysian context, offering findings relevant to that market. Another trust-enhancing feature is the implementation of blockchain technology in IoT services. Boudguiga et al. [43] examined the availability and accountability of IoT services and one of the outcomes was to implement blockchain solutions for access control, contracts and agreements, and storage facilities.

Regulation

Previous research we conducted with Abbas and Freeman in 2021, on regulating emerging technologies [19], [44], investigated the environmental implications of data flow in cloud computing. We identified the importance of regulating data flow between stakeholders that allowed continued innovation providing optimum outcomes for all stakeholders in the cloud value chain. While the utilization of cloud services is more mature than edge services, it is important that stakeholders within the edge collaborate up and down the network (with end devices and cloud computing stakeholders) to enhance data flow services to incorporate security-related functions (Table 1). With an increased focus on data protection, regulating edge computing and IoT has gained attention from policymakers and legislators. The following sections focus on data protection by promoting stakeholder accountability, self-regulation, and revisiting existing regulations.

Increased data protection through stakeholder accountability

Studies identify that stakeholder accountability can be achieved through data protection regulation when implementing edge and IoT services. For instance, Urquhart et al. [47] state that the lack of

Table 1. Comparing the value chains of cloud computing and edge computing.

Cloud Computing	Edge Computing
Facility	Facility
ODM/OEM*	Hardware
IT Infrastructure	Network
Systems Infrastructure Software	Edge Cloud Infrastructure
Application	Application/Software
Application Development and Deployment	Integration and Services
Presentation/Access	Open Source & Forums

Source: Adapted from sources [45], [46].
*Original Design Manufacturing/Original Equipment Manufacturing

user interfaces inhibits accountability and direct feedback for users to understand the information that is collected, stored, and processed at the device level. Furthermore, the researchers state that sensor and lightweight devices function with minimum user interfaces and often rely on lights or sounds alone. They further outlined the data flow between services which underpin accountability from the GDPR perspective [47]. Complementarily, Li et al. [25] promote stakeholder accountability through better security and existing data protection regulations. From a systems design perspective they applied Ethereum and the U.S. Health Insurance Portability and Accountability Act (HIPPA) to analyze software-defined infrastructure (ChainSDI) services.

Another form of stakeholder accountability comes in the form of software system maintenance and firmware patches [48]. There is a fine balance that must be achieved between better data protection and usability of a given device [47]. At a more granular level, Singh et al. [41, p. 57] note that "technology producers are not currently legally obliged to explain how the technology works." This immediately prevents users from having full transparency and provides manufacturers and service providers the right to offer limited visibility in what might be called black-box technology, regarding the inner workings of a product or service. Thus, any firmware patch updates are always at the discretion of the service provider. While all stakeholders want to be viewed as doing the right thing by users, accountability is not always practiced in tangible ways.

Promoting self-regulation between edge computing stakeholders

Pokrovskaia et al. [49] introduced self-regulation as a form of data protection to allow users of the system to auto-organize their relationships. They also presented blockchain as a technology platform to organize working relationships between edge stakeholders. Bhadauria and Chennamaneni [50] examined self-regulation and concluded that service providers offering better security incentives were perceived to value data protection. Duarte and de Lima Prestes [51] investigated self-regulation through a certification framework. The authors applied a collaborative research design across technical and nontechnical stakeholders with key components. The stakeholders and components established a security baseline of technical and nontechnical requirements and the solution demonstrated a collaborative multistakeholder environment where cooperation was key.

Abiding by existing data protection regulations

The sharing of data between heterogeneous IoT systems is a common function of data interoperability [52]. Varadi et al. [52] envisage an architecture enabling users, services, and devices to share common protocols and standards. Furthermore, the goal of the EU GDPR is to ensure that data protection is achieved by privacy by design. Garg et al. [53] review the GDPR and the U.S. Federal Trade Commission (FTC) regulation as related to cloud and edge services and conclude that the U.S. does have some sector regulations. However, the FTC definition of personal data varies across states and the balance of privacy protection falls on the stakeholders providing the services. Overall, these two studies point to the need for a unified approach data protection regulation, such as the GDPR.

Data breaches in edge computing services

According to Sullivan [54], a data breach is defined as the unauthorized access to personal data leading to accidental or unlawful data disclosure. Similarly, Kolevski et al. [19] have previously defined a data breach is when end-user information is accessed and disclosed to unauthorized entities, exploiting their PII, financial, and geolocation information. Likewise, edge computing faces similar challenges to cloud due to the number of IoT devices

connected to online services. While edge computing data breaches have yet to gain attention on front-page news and associated media coverage, the rapid uptake of edge services and IoT devices will be attractive to attackers. Pan and Yang [55] believe that edge computing faces cybersecurity challenges at scales never before seen due to the hyperconnectedness of IOT devices along with resource-poor attributes. Pan and Yang [55] highlight that large amounts of generated data, high-speed access availability, connectivity with cloud services, and decentralized network topology are ideal environments for attackers to penetrate at the edge.

It is essential to recognize the rise of the end-user's privacy and security needs from cloud to edge service provisions. However, the centralized concept of cloud services and its auditability functions could not easily be replicated in a distributed edge service [56]. Multiple points of interconnections, lightweight processing, and limited storage onboard devices allow for less auditability. While overhead data reduces service performance, it should not be reduced to the degree that it impacts on audit tracking capabilities.

The promise of edge computing and its approach to decentralization of devices, storage, and processing requirements is gaining momentum. The lightweight devices from sensors and RFID tags, to more powerful devices such as smartphones and vehicles, lead to a variety of devices functioning within the edge-to-cloud ecosystem. As a result of these heterogeneous devices rapidly continuing to increase in number, the attack landscape that was once concentrated in the cloud is now incorporating the edge. End-users are generating more data than ever, and dispersing data between multiple edge and cloud services, further increasing the threat scope. The question remains how will attacking the network edge benefit hackers? What do they have to gain from data breaches of this kind in the future? Will targeted attacks be aimed at individuals, groups of people, or specific manufacturers of devices with known vulnerabilities?

As we become reliant on edge devices and end-user devices, the discussion of what is possible begins to become a serious one. The sensitivity of the data being collected today could be "mission-critical" for more than just a business, but ensure the well-being of a human. The stakes are increasing as we get closer to the end user, and the repercussions of data breaches have a real human impact, beyond the concept of personal information being stolen. Rather we may be looking at data breaches at the edge causing significant local outages in smart cities, the potential for vehicular accidents (especially semi/autonomous vehicles), and even human casualties. In this context, safeguarding the edge and IoT services against hackers will likely become just as important as securing the cloud, if not more.

We speculate that the value chains for cloud computing [45] and the network edge [46] will begin to harmonize over the longer term and that the two very distinct models will co-exist—centralized versus decentralized—demanding data interoperability for the delivery of services (refer to Table 1). Decisions of where to store an application will come with an assessment of the type of data being gathered, its criticality, and whether data is being collected discretely, continuously, or on demand in real-time, among many other criteria. We advocate for privacy and security by design [57] approaches from the outset of the development of an IoT-based solution that, at the very least, abides by industry standards and recognized regulations [58]. ■

References

[1] ARM. (2024). *Edge Computing (vs. Cloud Computing)*. [Online]. Available: https://www.arm.com/glossary/edge-computing-vs-cloud-computing

[2] S. A. Noghabi et al., "The emerging landscape of edge computing," *GetMobile, Mobile Comput. Commun.*, vol. 23, no. 4, pp. 11–20, May 2020, doi: 10.1145/3400713.3400717.

[3] J. Ni et al., "Securing fog computing for Internet of Things applications: Challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 601–628, 1st Quart., 2018, doi: 10.1109/COMST.2017.2762345.

[4] L. S. Vailshery, "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030 (in billions)," *Statista*, Jul. 27, 2023. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[5] W. Shi and S. Dustdar, "The promise of edge computing," *Computer*, vol. 49, no. 5, pp. 78–81, May 2016, doi: 10.1109/MC.2016.145.

[6] J. Lin et al., "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*,

vol. 4, no. 5, pp. 1125–1142, Oct. 2017, doi: 10.1109/JIOT.2017.2683200.

[7] N. Abbas et al., "Mobile edge computing: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, Feb. 2018, doi: 10.1109/JIOT.2017.2750180.

[8] R. Buyya et al., "A manifesto for future generation cloud computing: Research directions for the next decade," *ACM Comput. Surv.*, vol. 51, no. 5, pp. 1–38, Sep. 2019, doi: 10.1145/3241737.

[9] W. Shi et al., "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016, doi: 10.1109/JIOT.2016.2579198.

[10] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, Jan. 2017, doi: 10.1109/MC.2017.9.

[11] Amazon Web Services (AWS), "What is a CDN? What is the history of CDN technology?" 2024. [Online]. Available: https://aws.amazon.com/what-is/cdn/

[12] Gestalt IT, "BrainChip brings AI to the edge and beyond," *Brainchip*, Oct. 28, 2020. [Online]. Available: https://brainchip.com/brainchip-ai-edge-beyond/

[13] B. Sharan, A. K. Sagar, and M. Chhabra, "A review on edge-computing: Challenges in security and privacy," in *Proc. Int. Conf. Appl. Artif. Intell. Comput. (ICAAIC)*, Salem, India, May 2022, pp. 1280–1286, doi: 10.1109/ICAAIC53929.2022.9792868.

[14] Shodan, "Search engine for the Internet of Everything," 2024. [Online]. Available: https://www.shodan.io/

[15] M. Elgan, "IoT Security: Thieves are targeting smart cameras—Here's how to stop them," *Secur. Intell.*, Jun. 3, 2021. [Online]. Available: https://securityintelligence.com/articles/iot-security-smart-camera-thieves/

[16] J. Ren et al., "A survey on end-edge-cloud orchestrated network computing paradigms: Transparent computing, mobile edge computing, fog computing, and cloudlet," *ACM Comput. Surv.*, vol. 52, no. 6, pp. 1–36, Nov. 2020, doi: 10.1145/3362031.

[17] S. Das et al., "Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices," *Heart Rhythm*, vol. 18, no. 3, pp. 473–481, Mar. 2021, doi: 10.1016/j.hrthm.2020.10.009.

[18] R. Sendhil and A. Amuthan, "A comparative study on security breach in fog computing and its impact," in *Proc. Int. Conf. Electron. Sustain. Commun. Syst. (ICESC)*, Coimbatore, India, Jul. 2020, pp. 247–251, doi: 10.1109/ICESC48915.2020.9155967.

[19] D. Kolevski et al., "Cloud data breach disclosures: The consumer and their personally identifiable information (PII)?," in *Proc. IEEE Conf. Norbert Wiener 21st Century (21CW)*, Chennai, India, Jul. 2021, pp. 1–9, doi: 10.1109/21CW48944.2021.9532579.

[20] P. S. Bangare and K. P. Patil, "Security issues and challenges in Internet of Things (IOT) system," in *Proc. 2nd Int. Conf. Advance Comput. Innov. Technol. Eng. (ICACITE)*, Greater Noida, India, Apr. 2022, pp. 91–94, doi: 10.1109/ICACITE53722.2022.9823709.

[21] V. Kjorveziroski, S. Filiposka, and V. Trajkovik, "IoT serverless computing at the edge: A systematic mapping review," *Computers*, vol. 10, no. 10, p. 130, Oct. 2021.

[22] V. Hassija et al., "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[23] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, Oct. 2017, doi: 10.1109/TETC.2016.2606384.

[24] V. Hassija et al., "A blockchain and edge-computing-based secure framework for government tender allocation," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2409–2418, Feb. 2021, doi: 10.1109/JIOT.2020.3027070.

[25] P. Li et al., "ChainSDI: A software-defined infrastructure for regulation-compliant home-based healthcare services secured by blockchains," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2042–2053, Jun. 2020, doi: 10.1109/JSYST.2019.2937930.

[26] S. Taherizadeh and V. Stankovski, "Auto-scaling applications in edge computing: Taxonomy and challenges," in *Proc. Int. Conf. Big Data Internet Thing (BDIOT)*, New York, NY, USA. Association for Computing Machinery, Dec. 2017, pp. 158–163, doi: 10.1145/3175684.3175709.

[27] R. Clarke, "What's privacy?" Jul. 28, 2006. [Online]. Available: https://www.rogerclarke.com/DV/Privacy.html

[28] R. Clarke, "Information technology and data veillance," *Commun. ACM*, vol. 31, no. 5, pp. 498–512, May 1988.

[29] M. Hagan, F. Siddiqui, and S. Sezer, "Enhancing security and privacy of next-generation edge computing technologies," in *Proc. 17th Int. Conf.* Privacy, *Secur.* Trust *(PST)*, Fredericton, NB, Canada, Aug. 2019, pp. 1–5, doi: 10.1109/PST47121.2019.8949052.

[30] S. Guynes, J. Parrish, and R. Vedder, "Edge computing societal privacy and security issues," *ACM SIGCAS Comput. Soc.*, vol. 48, nos. 3–4, pp. 11–12, Feb. 2020, doi: 10.1145/3383641.3383643.

[31] J. Clough, *Principles of Cybercrime*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[32] J. Slupska and A. Strohmayer, "Networks of care: Tech abuse advocates' digital security practices," in *Proc. 31st USENIX Secur. Symp.*, Boston, MA, USA, Aug. 2022, pp. 341–358.

[33] H. Holmes, "The rise of 'smart abuse'—My ex was spying on me through my TV," Holmes Family Law, Jun. 13, 2019. [Online]. Available: https://www.holmesfamilylaw.co.uk/media/the-rise-of-smart-abuse-my-ex-was-spying-on-me-through-my-tv/

[34] M. A. Aleisa, A. Abuhussein, and F. T. Sheldon, "Access control in fog computing: Challenges and research agenda," *IEEE Access*, vol. 8, pp. 83986–83999, 2020, doi: 10.1109/ACCESS.2020.2992460.

[35] S. Shimahara and H. Nishi, "Dataflow management platform for smart communities using an edge computing environment," in *Proc. 47th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Toronto, ON, Canada, Oct. 2021, pp. 1–6, doi: 10.1109/IECON48115.2021.9589430.

[36] Y. Cheng et al., "Research on privacy protection technology in face identity authentication system based on edge computing," in *Proc. IEEE Int. Conf. Artif. Intell. Ind. Design (AIID)*, Guangzhou, China, May 2021, pp. 438–449, doi: 10.1109/AIID51893.2021.9456477.

[37] S. Venkatesh et al., "Face morphing attack generation and detection: A comprehensive survey," *IEEE Trans. Technol. Soc.*, vol. 2, no. 3, pp. 128–145, Sep. 2021, doi: 10.1109/TTS.2021.3066254.

[38] T. Kumar, M. Ylianttia, and E. Harjula, "Securing edge services for future smart healthcare and industrial IoT applications," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Budapest, Hungary, Apr. 2022, pp. 1–6, doi: 10.1109/NOMS54207.2022.9789900.

[39] C. Naik et al., "Location privacy using data obfuscation in fog computing," in *Proc. IEEE Region 10 Conf. (TENCON)*, Kochi, India, Oct. 2019, pp. 1286–1291, doi: 10.1109/TENCON.2019.8929236.

[40] P. Toth, T. Babbitt, and T. Graziano, "Signals of opportunity: Spoof detection with low-cost hardware and edge devices," in *Proc. IEEE 14th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, New York, NY, USA, Oct. 2023, pp. 219–223, doi: 10.1109/uemcon59035.2023.10316011.

[41] J. Singh et al., "Accountability in the IoT: Systems, law, and ways forward," *Computer*, vol. 51, no. 7, pp. 54–65, Jul. 2018, doi: 10.1109/MC.2018.3011052.

[42] B.-K. Cheryl, B.-K. Ng, and C.-Y. Wong, "Governing the progress of Internet-of-Things: Ambivalence in the quest of technology exploitation and user rights protection," *Technol. Soc.*, vol. 64, Feb. 2021, Art. no. 101463, doi: 10.1016/j.techsoc.2020.101463.

[43] A. Boudguiga et al., "Towards better availability and accountability for IoT updates by means of a blockchain," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Paris, France, Apr. 2017, pp. 50–58, doi: 10.1109/EuroSPW.2017.50.

[44] D. Kolevski and K. Michael, "Cloud computing data breaches a socio-technical review of literature," in *Proc. Int. Conf. Green Comput. Internet Things (ICGCIoT)*, Greater Noida, India, Oct. 2015, pp. 1486–1495, doi: 10.1109/ICGCIoT.2015.7380702.

[45] W. Belmans and U. Lambrette, "The cloud value chain exposed key takeaways for network service providers," CISCO, Mar. 2012. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/sp/Cloud-Value-Chain-Exposed_030512FINAL.pdf

[46] STL Partners. (2024). *Edge Computing Ecosystem*. [Online]. Available: https://stlpartners.com/tools/edge-computing-ecosystem/

[47] L. Urquhart, T. Lodge, and A. Crabtree, "Demonstrably doing accountability in the Internet of Things," *Int. J. Law Inf. Technol.*, vol. 27, no. 1, pp. 1–27, Mar. 2019, doi: 10.1093/ijlit/eay015.

[48] M. K. Kagita, G. R. Bojja, and M. Kaosar, "A framework for intelligent IoT firmware compliance testing," *Internet Things Cyber-Phys. Syst.*, vol. 1, pp. 1–7, 2021, doi: 10.1016/j.iotcps.2021.07.001.

[49] N. Pokrovskaia, T. Khansuvarova and R. Khansuvarov, "Network decentralized regulation with the fog-edge computing and blockchain for business development," in *Proc. Eur. Conf. Manag., Leadership Governance*, 2018, pp. 205–212.

[50] V. S. Bhadauria and A. Chennamaneni, "Do desire, anxiety and personal innovativeness impact the adoption of IoT devices?" *Inf. Comput. Secur.*, vol. 30, no. 5, pp. 730–750, Nov. 2022, doi: 10.1108/ics-07-2021-0096.

[51] L. O. Duarte and J. A. de Lima Prestes, "IoT solution information security certification conceptual framework: IoT solution information

security on improving the transparency and accountability of IoT solutions through an open world perspective," in *Proc. XVII Brazilian Symp. Inf. Syst.* New York, NY, USA: Association for Computing Machinery, Jun. 2021, pp. 1–9, doi: 10.1145/3466933.3466983.

[52] S. Varadi, G. G. Varkonyi, and A. Kertesz, "Law and IoT: How to see things clearly in the fog," in *Proc. 3rd Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Barcelona, Spain, Apr. 2018, pp. 233–238, doi: 10.1109/FMEC.2018.8364070.

[53] R. Garg, S. Varadi, and A. Kertesz, "Legal considerations of IoT applications in fog and cloud environments," in *Proc. 27th Euromicro Int. Conf. Parallel, Distrib. Network-Based Process. (PDP)*, Pavia, Italy, Feb. 2019, pp. 193–198, doi: 10.1109/EMPDP.2019.8671620.

[54] C. Sullivan, "EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era," *Comput. Law Secur. Rev.*, vol. 35, no. 4, pp. 380–397, Aug. 2019, doi: 10.1016/j.clsr.2019.05.004.

[55] J. Pan and Z. Yang, "Cybersecurity challenges and opportunities in the new 'edge computing + IoT' world," in *Proc. ACM Int. Workshop Secur. Softw. Defined Netw. Function Virtualization*. New York, NY, USA: Association for Computing Machinery, Mar. 2018, pp. 29–32, doi: 10.1145/3180465.3180470.

[56] Y. Guan et al., "Data security and privacy in fog computing," *IEEE Netw.*, vol. 32, no. 5, pp. 106–111, Sep. 2018, doi: 10.1109/MNET.2018.1700250.

[57] A. Cavoukian, "Understanding how to implement privacy by design, one step at a time," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 78–82, Mar. 2020.

[58] Commend. *How Does Privacy and Security by Design Work?* [Online]. Available: https://www.commend.com/en-au/technology/cyber-security/psbd.html

[59] K. Michael, R. Abbas and G. Roussos, "AI in cybersecurity: The paradox," *IEEE Trans. Technol. Soc.*, vol. 4, no. 2, pp. 104–109, Jun. 2023, doi: 10.1109/TTS.2023.3280109.

David Kolevski is an enterprise network communications specialist. Kolevski has a Bachelor of Information Technology, a Master of Information Communication Technology, and a PhD in cloud computing from the School of Computing and Information Technology, University of Wollongong, Wollongong, NSW, Australia.

Katina Michael is a tenured professor at the School for the Future of Innovation in Society, Arizona State University, Tempe, AZ 85287 USA, and the School of Computing and Augmented Intelligence, Arizona State University, Tempe, AZ 85281 USA. She is also a senior global futures scientist at the Julie Ann Wrigley Global Futures Laboratory, Arizona State University.

■ Direct questions and comments about this article to David Kolevski, School of Computing and Information Technology, University of Wollongong, Wollongong, NSW 2500, Australia; dkolevski@protonmail.com.