# Secure Edge Computing in IoT Systems: Review and Case Studies

Mohammed Alrowaily
Department of Electrical Engineering
University of South Florida
Tampa FL 33620, USA
malrowaily@mail.usf.edu

Zhuo Lu
Department of Electrical Engineering
University of South Florida
Tampa FL 33620, USA
zhuolu@usf.edu

***Abstract*—Today, the architectures for efficient and secure network system designs, such as Internet of Things (IoT) and big data analytics, are growing at a faster pace than ever before. Edge computing for an IoT system is data processing that is done at or near the collectors of data in an IoT system. In this paper, we aim to briefly review the concepts, features, security, applications of IoT empowered edge computing as well as its security aspects in our data-driven world. We focus on clarifying different aspects that should be taken into consideration while creating a scalable, reliable, secure and distributed edge computing system. We also summarize the basic ideas regarding security risk mitigation techniques. Then, we explore the presented challenges and opportunities in the field of edge computing. Finally, we review two case studies, smart parking and content delivery network (CDN), and analyze different methods in which IoT systems can be used to carry out daily tasks.**

***Index Terms*—Edge computing, Security, Internet of Things (IoT)**

## I. Introduction

The Internet of Things (IoT) [1] has been involved in playing vital functions with the advancing growth in technology. Millions of devices interconnected with each other gather/exchange data among themselves via network infrastructures linked by a countless number of distributed nodes. At that point, a range of IoT apps can efficiently deliver a lot more reliable and precise network services for individuals. In this scenario, a growing number of gadgets /sensors are connected through IoT approaches, which results in producing massive data to consumers. In cloud computing, all data should be sent to a central server where the majority of computing is carried out. Then, the results of that computation need to be returned to these gadgets and sensors. This procedure generates a tremendous amount of pressure in the cost of data transmission and affects network performance.

The direction of future computing will go beyond conventional computing. Specifically, IoT systems are integrated into day-to-day lives quickly. Physical devices and endpoints include wearable fitness bands, smart vehicles, sensor units, and actuators, which represents a massive future jump in the scope of data manufacturing.

Edge computing is an essential approach for IoT networks. As a result of data transferring along with a restricted system efficiency, a central cloud computing infrastructure could in fact run beyond its capability for analyzing the significant amount of data gathered from IoT units. The vast collection of data from users can also raise substantial security and privacy concerns. An edge computing platform can eliminate the data processing burden at the centralized infrastructure as well as personal privacy issues as the data created from IoT gadgets are kept and processed within nodes in the edge network.

Edge computing is pulling raising interests simultaneously from the academia and the industry. The idea and advancement of developing secure edge computing is currently in a reasonably early stage. A number of technical obstacles are ahead to be fixed from both academic and industrial viewpoints.

The primary purpose of this paper is to briefly review the concepts, features, security, and applications of IoT empowered edge computing as well as its security aspects in our data-driven world. In particular, we focus on the following aspects of IoT empowered secure edge computing.

- Architecture and security issues: We review the architecture of IoT systems in edge computing. Edge computing offers minimized latency and better quality of service (QoS), although data processing nodes in edge computing have lesser computation power compared to the cloud servers. We also review security requirements for edge computing, including security strategies and techniques as well as identity management in a privacy-preserving scenario.
- Challenges and opportunities: There are many distinctive challenges and opportunities in edge computing environments, including public accessibility of edge nodes, tasks offloading, optimization metrics, and user privacy. We summarize them in detail and outline potential research directions.
- Case studies: Two case studies are presented to illustrate the edge computing vision in a detailed manner. First, we study a smart parking system that minimizes traffic jam on a parking slot. Second, we investigate using the content delivery network (CDN) to reduce the latency of data transmission and enhance web content availability.

The remainder of this paper is organized as follows. In Section II, we introduce the edge computing architecture and its security issues. In Section III, we discuss the possible

challenges and opportunities of edge computing. In Section IV, show some use case scenarios related to edge computing. Finally, we conclude the paper in Section V.

## II. Edge Computing: Architecture and Security

In this section, we briefly introduce the architecture and tasks of edge computing. Then, we review the basic ideas regarding security evaluation and risk mitigation techniques to assure that edge computing users/operators can achieve their security purposes.

### A. Architecture and Tasks

Edge Computing is a distributed architecture, simply defined as the processing of data when it is collected. It has been emerged to minimize both bandwidth and time response in an IoT system. The use of an edge computing technique is required when the latency is required to be optimized to avoid network saturation [2] as well as when the data processing burden is high at a centralized infrastructure. An extended version of edge computing is fog computing, which is an architecture that makes use of edge gadgets to accomplish a considerable amount of computation, storage, communication regionally, which undoubtedly possesses input and output from the real world referred to as transduction. Fog nodes determine whether to process the data locally from several data sources or send the data out to cloud [3].

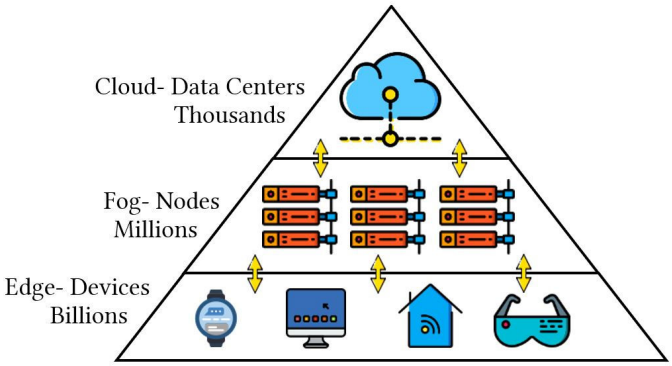


Fig. 1. Typical edge computing architecture.

Fig. 1 represents the communication from numerous edge devices, such as smartphones, smart TV's, health and fitness activity tracker bands, to fog nodes and then to cloud data centers. Specifically, fog nodes are attaching links between the cloud and the edge devices. Edge devices are interfaces between individuals or various items connecting with them and the cloud [3].

Fig. 2 summarizes the tasks of edge computing, which people carry out in a daily manner. There are three basic elements: input, processing, and output as summarized based on [4].

- Data sources: As the input, any endpoint which records and collects data from clients or its environments is described as a data source.

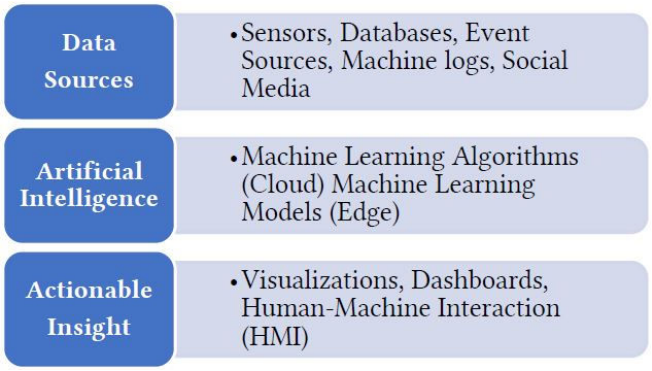


Fig. 2. Major tasks of edge computing.

- Artificial intelligence: As the processing function, it is the main facet after data collected to uncover practical observations, locate patterns and trends, produce individualized recommendations, and improve the performance based on machine learning or data analytics models.
- Actionable insights: The results from the previous stage succeed only when an individual can act and make any informed selection. Thus, within this stage, the insights appear in a transparent manner in type of control panels, visualizations, alerts and so on, which motivates communication between machines and humans, therefore generating a beneficial feedback loop.

### B. Privacy and Security

An organization should oversee and ensure privacy and security of their IoT framework. Multiple terminologies used in privacy-preserving management are enumerated in the following [5].

- Pseudonymity: where the pseudonym is used as an ID to ensure that an individual can utilize the source (e.g. pseudonym) without revealing the source's real identity. However, a user could still be responsible for usage.
- Unobservability: assuring that an individual could utilize a resource or service without other third parties and having the ability to observe that the resource or service is being used.
- Unlinkability: ensuring that a third party (e.g., an attacker) cannot identify whether two objects are linked to each other or not.
- Anonymity: an individual may make use of a resource without revealing his identity.

According to [6], there are several crucial components for evaluating system security.

- Confidentiality: assuring only the data proprietor and an individual can access the personal information in the edge computing. It protects against unapproved parties' access to the data when the individual's data is transferred and also collected in edge or core network framework, as well as when the data is kept or handled in edge or cloud nodes.

- Integrity: assuring the proper and steady transmission of data to the accredited individual without unauthorized modification of the data. Privacy of individuals can be impacted due to the lack of integrity measures.
- Availability: ensuring the accredited party manages to access the edge services in any regions based on individuals' needs. This also implies that an individual's data held in edge or cloud nodes along with the ciphertext format can be handled under various practical needs.
- Access control and authentication: access control imitates a linking point of all privacy and security demands by the access control technique. Authentication ensures that the identification of an individual is accredited.

### C. Measures and Risk Reduction

Risks associated with IoT infrastructures should be also managed and characterized by organizations for risk mitigation using the following methods [7], [8].

- Strong Password Policy: ensure that individuals comply with the ideal security password policies. Passwords should not be a thesaurus word, but have high entropies, i.e., a mixture of lowercase and uppercase letters with a combination of special characters. Random password generators could be utilized for generating strong passwords.
- Encryption: organizations need to encrypt inbound and outbound communications by using the state-of-the-art ciphers and continuously have a disaster recovery backup plan to be prepared for potential data violations or breaches.
- Two-Factor Authentication (2FA): by making use of 2FA, people are required to verify their identities, which is after they have initial access after entering their username and password. It improves security by imposing one more level of checking and verification based upon elements like ATM PIN, password, biometrics (e.g., voiceprint and iris patterns).

In addition, 2FA could be further categorized as follows.

- SMS texting and voice-based: a code received by an SMS text; and reading the numbers aloud via an automated voice call for secure login.
- Hardware tokens: a small hardware device with a built-in screen to generate a one-time password (OTP) for each transaction.
- Software application tokens: a replacement of traditional hardware token, which is a secure software application installed in an token app downloaded to an end-user's smartphone.
- Push notification: a pop-up "push" message that turns up on a user' device through the internet to validate the identity of the user as a second-factor authentication.

## III. Challenges and Opportunities

Today's digital world surrounded by billions of sensors embedded in interconnected IoT devices, which communicate with each other. Indeed, those sensors are influencing human interactions with the digital world, thus ensuring a seamless connection between humans and devices. Along with an ever-rising number of sensors and the increasing amount of data discarded/produced by them, we face a few challenging problems [9].

- User privacy: user privacy in today's world includes any information that can potentially disclose a user's identity, behavior, and location. The goal of safeguarding a user's private information increasingly contradicts the broader deployment of IoT-enabled devices. Therefore, a reliable system must be designed to collect and process a large amount of data without revealing a user's private information.
- Optimization metrics: there are several layers with various computation abilities in edge computing. Deciding what layer to deal with the workload complexity or the number of assigned assignments is a challenging task. However, there are four optimization metrics for choosing an optimal workload allocation: a) latency, which is due to networking and computation, b) energy consumption, c) cost to construct and maintain, and d) bandwidth.
- Tasks offloading: In task offloading, the duties/tasks of a system should be outsourced. Computational offloading is eye-catching for IoT systems and could take place in all sorts of IoT edge devices. Nonetheless, utilizing edge nodes for computation offloading is a concern due to the problem of adequately segmenting computational tasks in an automated way.
- Public accessibility of edge nodes: When an edge device (e.g., a base station, switch, and router) is intended to be used for public access, lots of challenges need to be dealt with. A public/private company has to specify the threats related to their own devices without compromising the desired purpose of the device (e.g., a router) to be used as an edge node. Multi-tenancy of edge nodes is only feasible with modern technologies that put security as their own consideration. In addition, other concerns include the cost of maintenance, data locations, and workload for establishing appropriate price models making edge nodes readily available.

## IV. Case Studies of Edge Computing

Two case studies are presented in this section to illustrate the edge computing vision comprehensively. First, we analyze a smart parking system that lessens traffic when an individual is navigating for a car parking space. Second, we explore utilizing the CDN to minimize the latency of transmitted data as well as enhance Internet content availability.

### A. Smart Parking System

Consider a system that allows individuals to promptly find an available parking place on one click of a key on a smart device. This system will significantly decrease the time devoted to looking for a parking slot and inhibit vehicle parking violations [10]. The smart parking system is usually

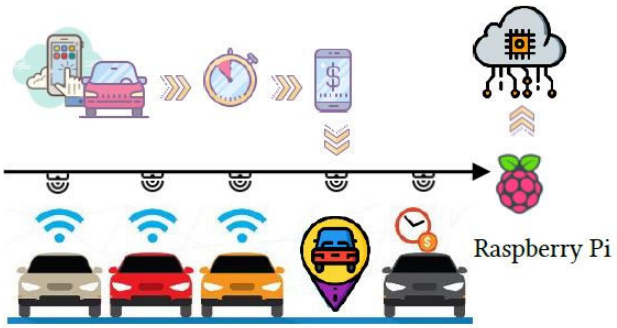


Fig. 3. Example of a smart parking system.

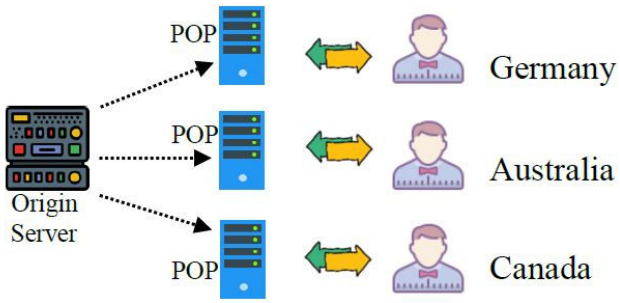


Fig. 4. Example of a content delivery network.

powered via RFID, ultrasonic detector, and infrared sensing units, as shown in Fig. 3.

*1) Flow of Execution:* A common flow of execution works as follows for a smart parking system.

1) Log in to the smartphone parking application.
2) Choose the parking area near the customer's location.
3) Browse between randomly available parking slots, then select a preferable slot.
4) Select the desired timeframe to park the vehicle.
5) Pay off the parking fee for a chosen timeframe.
6) When a customer parks the car via navigation and confirms his parking, the time countdown starts.
7) On departure, the customer can pay any additional charge if he exceeds the allowed time.

*2) Benefits:* Smart parking may minimize traffic for an automobile navigating for a slot, can be useful for many people and decrease vehicles emissions, making for an even more environmentally friendly city. It can also boost accessibility for businesses and grocery stores by enhanced optimization of available parking slots.

*3) Future Scope:*

- The system may be adjusted to integrate future self-driving automobiles and assure real-time communication between several vehicles such that an individual possesses no interactive burden with the system.
- More efficient parking algorithms could be established for the optimal consumption of resources, such as availability of slots and parking durations. For example, a deep learning model can be trained for real-time space allocation.

### B. Content Delivery Network

A CDN is one of the most promising solutions to address the issue of massive web traffic, by distributing many servers efficiently in different geographical locations, thereby delivering web content in a faster way. The CDN is a special case of edge computing. Today, a lot of Internet websites, such as Facebook, eBay, and Netflix, leverage the CDN architecture to efficiently provide web content.

*1) Architecture:* Consider an application with a large number of users in large geographical areas. Providing requests to every user from a central location can easily result in substantial network latency. If such an application is service essential, service level agreement (SLA) violations can also occur. CDN addresses precisely the issue in this use case, as an example shown in Fig. 4. The origin server is connected to several exchange points (IXP). These servers named as Point of Presence (POPs). They are distributed throughout different geographical areas. POPs play a significant role because the caching system relies on the performance of these servers. The CDN architecture enhances the reliability of the entire system. If one POP server is down, traffic will be re-routed to other PoPs. Individuals can be delivered services with their nearest POP server.

*2) Advantages:* There are many advantages for consumers under the CDN architecture [11].

- Website security improvement: a CDN with the help of distributed denial of service (DDoS) mitigation can enhance and maintain the website security from DDoS attacks that can severely interrupt and degrade the service accessibility.
- Faster website page loading: a CDN can be utilized to provide static web content, which decreases the webpage load time.
- Botnet and spam defense: a CDN can be set up with firewall policies which obstruct unwanted spamming and botnet probing against the system.
- Enhancing global content availability: a CDN can manage massive traffic and hold up against failure as compared with central services.
- Handling website traffic spikes: a CDN provides better load balancing between servers and offers fast horizontal scaling.

## V. Conclusion

In this paper, we review the concept and architecture of edge computing in the IoT era. We summarize the security and privacy requirements of edge computing, and also discuss the challenges and opportunities that emerge among this new trajectory in the landscape of edge computing. Finally, we discuss two use-case scenarios related to smart parking system and CDN. Edge computing is still in its early stage, and we hope this paper will acquire the interest of the community and motivate even more research studies in the field of edge computing.

## ACKNOWLEDGMENT

The work at University of South Florida is supported in part by NSF CNS-1717969.

## REFERENCES

[1] K. Ashton *et al.*, "That internet of things thing," *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.

[2] C. M. Fernández, M. D. Rodríguez, and B. R. Muñoz, "An edge computing architecture in the internet of things," in *2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC)*. IEEE, 2018, pp. 99–102.

[3] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19 293–19 304, 2017.

[4] M. Schaberg, *Partnering on your Journey*. KLM Services, LLC, 2017. [Online]. Available: https://www.klmservices.com/mt-content/uploads/2017/12/our-journey-presentation-osme-120417.pdf

[5] A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology," *Version v0*, vol. 31, p. 15, 2008.

[6] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18 209–18 237, 2018.

[7] B. Archana, A. Chandrashekar, A. G. Bangi, B. Sanjana, and S. Akram, "Survey on usable and secure two-factor authentication," in *Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on*. IEEE, 2017, pp. 842–846.

[8] Authy. what is two-factor authentication (2fa)? [Online]. Available: https://authy.com/what-is-2fa/

[9] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick, and D. S. Nikolopoulos, "Challenges and opportunities in edge computing," *arXiv preprint arXiv:1609.01967*, 2016.

[10] A. Khanna and R. Anand, "Iot based smart parking system," in *Internet of Things and Applications (IOTA), International Conference on*. IEEE, 2016, pp. 266–270.

[11] Cloudflare. What is a cdn? how does a cdn work? [Online]. Available: https://www.cloudflare.com/learning/cdn/what-is-a-cdn/