Edge Computing vs. Cloud Computing: Trade-offs in Latency, Privacy, and Scalability

Thaddeus Salwan
John Carroll University
Cleveland, United States
tsalwan26@jcu.edu

Stephen Loya
John Carroll University
Cleveland, United States
sloya25@jcu.edu

Francis Freeman
John Carroll University
Cleveland, United States
ffreeman26@jcu.edu

Justin Lupton
John Carroll University
Cleveland, United States
jlupton27@jcu.edu

Abstract—This research explores how cloud and edge computing work together to shape the way data is processed and managed today. This research takes a closer look at how cloud computing and edge computing work together to influence the way data is processed and managed in today's digital world. Cloud computing provides powerful, scalable resources for storing and analyzing large amounts of information, making it ideal for tasks that require significant processing or long term storage, while edge computing processes data closer to where it's created, whether that's a phone, a sensor, or a smart device. This makes responses faster and improves latency, and can even help protect the user privacy by keeping sensitive data local. By comparing key factors such as latency, privacy, reliability, and scalability, this research highlights that each approach comes with its own strengths and weaknesses. Rather than competing, cloud and edge computing complement one another when used together, creating faster, more secure, and more efficient systems. New innovations like Edge as a Service (EaaS) show how these two technologies are beginning to merge into a single, flexible solution for modern computing needs.

Index Terms—Edge Computing, Cloud Computing, latency, privacy, security

I. Introduction

Cloud vs edge computing has been a topic for debate for some time now. Tech companies have been questioning whether one should be used over the other, or even synchronizing both. The topic is important not only for tech companies, but for technology users as a whole. These two modern concepts emerged and were put into practice around the early 2000's, and have made a great impact on how different types of data is handled. Edge computing handles localized data in real time, typically private company information. Use cases would include cameras, sensors, and industrial machinery. Cloud on the other hand is used to store, track, and analyze large amounts of data over time on virtual servers. Cloud uses devices such as virtual machines and online servers, seen in tools such as Google Cloud Platform and Amazon Web Services (AWS).

The growing need for fast, scalable, and secure data processing has pushed debate on whether cloud or edge computing should be used for handling such a need. Discussion over both has led to agreements in integrating both approaches together. A hybrid approach can achieve both fast/low latency at an edge level, but still offer large scalable data storage for long term analysis at a cloud level. Although combining both practices
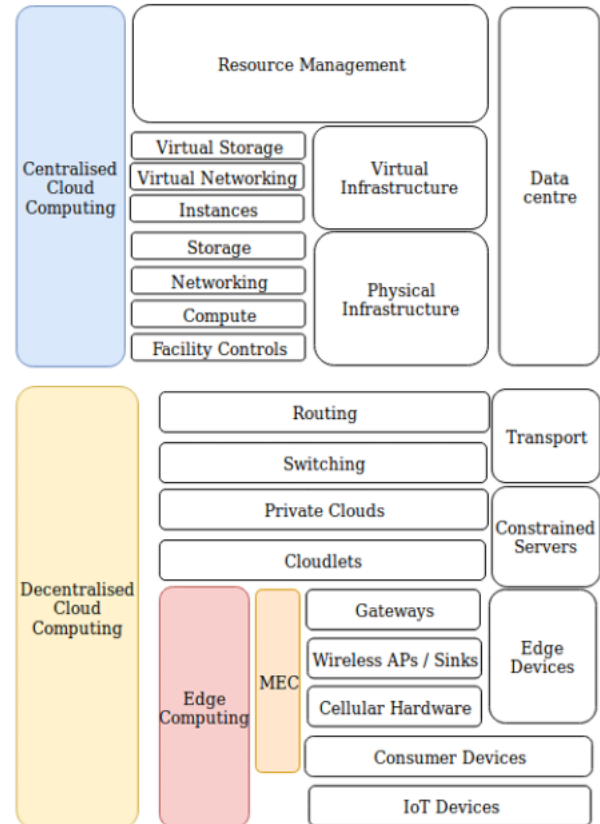

Fig. 1. A graph showing the various hardware and technologies associated with Centralized and Decentralized Cloud Computing.

provides the best of both worlds, it still falls short. Hybrid integration is expensive in terms of hardware and services, as well as providing skillful maintenance. It leads to other issues involving higher security threats, data synchronization issues, and overall harder scaling in a hybrid operation. The purpose of this research is to dive into the pros and cons of each service, comparing latency, privacy, and scalability of both, while explaining how they can complement or oppose each other in a hybrid approach.

II. AN OVERVIEW OF EDGE COMPUTING

Edge computing is a distributed architecture that pushes compute, storage, and networking closer to where data is generated rather than sending everything to distant centralized clouds. Processing locally to the data source cuts round trip distance over wide area networks, which in turn reduces latency, lowers bandwidth consumption, improves resiliency during intermittent connectivity, and can keep sensitive data local for privacy and compliance. Typical edge tiers range from on device runtimes, to gateways and micro data centers on premises. These are often coordinated with cloud services for fleet management, updates, and long term analytics. Shi et al. describe edge computing as a "complementary extension of the cloud" that enables faster, context aware processing by decentralizing workloads to the network periphery [7]. This approach improves privacy and compliance as well, since sensitive or regulated information can be processed locally before essential summaries are sent to the cloud.

In a typical deployment, an edge runtime handles local messaging, caching, and machine learning inference so devices keep operating even if the internet link drops. The system then syncs summaries or events to the cloud when connectivity returns. This hybrid pattern lets teams place time critical logic at the edge while using the cloud for heavy training, global orchestration, backups, and compliance archives. For example, AWS Internet of Things (IoT) Greengrass allows components to run directly on edge gateways, enabling real time data filtering, device communication, and local machine learning inference while maintaining secure synchronization with AWS Cloud services for storage and fleet management. Similar platforms, such as Microsoft Azure IoT Edge and Google Cloud IoT Core, adopt comparable strategies deploying modular containerized workloads that can operate independently when offline and reconnect seamlessly once network access is restored. These systems highlight how the edge extends the cloud's functionality rather than replacing it, creating a continuum of computation that adapts dynamically to latency, bandwidth, and data sensitivity needs. Broadly, cloud providers frame edge computing as an essential evolution of cloud architecture, bringing information storage, analytics, and decision making closer to the source to meet the growing demands of real time and data intensive applications that centralized infrastructures alone can no longer serve efficiently.

III. AN OVERVIEW OF CLOUD COMPUTING

Cloud Computing can best be described as a "computing model that enables on-demand access to a shared pool of configurable computing resources, such as servers, storage, and applications, over the internet" [2]. Cloud Computing resources are located off-site, usually in large data centers managed by a Cloud Service Provider (CSP) [2]. There are three common cloud service models offered to tenants. The first is Infrastructure as a Service (IaaS). IaaS provides tenants with hardware resources and infrastructure as well as a virtual interface to interact with those resources. The tenant uses its own operating system. A step up in service

Fig. 2. A table visualizing SaaS, PaaS, and IaaS service models.

is Platform as a Service (PaaS). PaaS provides the tenant with everything that is included in the IaaS model along with a base operating system and some development tools. This is mainly used for application development and deployment. The last model, Software as a Service (SaaS) fully provides the hardware resources, operating systems, and applications [6]. These Cloud Computing service models allow companies to focus on their business operations and product instead of computational infrastructure and resource management.

The greatest strength of Cloud Computing is its tremendous scalability. Most services offer "on-demand self-service" [2]; resources are automatically scaled and distributed across machines to handle workload without needing manual input from the CSP. Pairing this with pay-as-you-go pricing allows companies to effectively manage the IT related aspects of their business effortlessly while only paying for what they actually use. Even with great benefits, Cloud Computing still has shortcomings such as high latency and bandwidth consumption [2]. Data must be transferred between the tenant and the data center for storage or processing. The tenant and the data center are often miles away from each other, which results in long loading times and high latency. Cloud Computing helps companies focus on their business instead of IT resources by offering highly scalable and flexible hardware resources, but with a cost of high latency.

IV. EDGE COMPUTING VS. CLOUD COMPUTING: LATENCY

One of the most critical performance differences between edge and cloud computing is latency. Latency is the time delay between data generation and system response. Traditional cloud computing architectures route data through wide area networks to centralized servers, often located far from end devices. Even with high speed connectivity, this process typically introduces delays that range from tens to hundreds of milliseconds, which can disrupt real time services such as autonomous driving, industrial automation, or telemedicine. Edge computing mitigates this limitation by processing data closer to the source, reducing the physical distance and network hops required. Khan et al. identify latency reduction as

one of the primary motivators for deploying edge systems, showing that local computation can achieve response times in the single digit millisecond range for critical workloads [8]. This responsiveness allows edge based applications to make split second decisions that would be impossible with a purely cloud dependent model.

However, the superior latency performance of edge computing comes with trade offs. Local devices and gateways often have constrained computational capacity compared to large scale cloud infrastructures. As Khan et al. emphasize, hybrid architectures offer the most effective compromise [8]. This balance allows organizations to maintain real time responsiveness without sacrificing analytical depth or scalability. In this way, edge and cloud computing function as complementary components of a unified ecosystem. The edge provides immediate action, while the cloud delivers global insight. Together, they create the low latency, high performance backbone required for intelligent, connected technologies. Yet as computation becomes more distributed, this same architecture raises new questions about where data is processed, who controls it, and how privacy can be preserved.

V. EDGE COMPUTING VS. CLOUD COMPUTING: PRIVACY

Privacy concerns in computing structure vary drastically between cloud computing and edge computing, largely due to where and how data is processed, stored, and transmitted. In traditional cloud computing, user data is sent to centralized data centers operated by third-party providers for storage and use. This model allows for high scalability and accessibility but creates notable privacy and security risks. Users have to rely on the service provider to ensure their data is protected, which introduces vulnerabilities such as unauthorized access, data breaches, and loss of data ownership. The main privacy issues in cloud computing stem from data centralization. Since multiple users share the same physical infrastructure, malicious users or compromised virtual machines can exploit system vulnerabilities to gain unauthorized access to sensitive information. Parikh et al. name several common threats, including data theft, malware injection, and communication interception between users and cloud servers [6]. These risks are compounded by the fact that organizations often lack direct visibility or control over their cloud provider's internal operations. Even with encryption and access control measures, data privacy in the cloud depends heavily on the integrity and compliance of the service provider, making it difficult for users to fully ensure data confidentiality.

To address these vulnerabilities, various security frameworks have been proposed, such as monitoring tools, network segmentation, and encryption protocols. However, the inherent dependency on a centralized service model remains a concern. Cloud providers store massive amounts of data across networks, which makes them targets for cyberattacks. Issues like inefficient authorization systems, weak authorization mechanisms, and inadequate service level agreements contribute to ongoing privacy challenges. The weaknesses have prompted researchers and engineers to explore alternative

computing options, namely edge and fog computing, that bring computation and storage closer to data sources.

In edge computing, privacy protection is enhanced by minimizing how much data leaves the device or local environment. Instead of transmitting raw information to distant cloud servers, edge systems process it locally, either on the device itself or on nearby gateways. According to Parikh et al., this approach reduces latency, network congestion, and exposure to external threats [6]. By filtering data before sending it to the cloud, edge computing effectively limits the amount of sensitive information that travels over the network, strengthening privacy.

Despite these advantages, edge computing introduces its own privacy and security challenges. Each device or edge node can become a potential vulnerability point if not properly secured. The paper highlights issues such as weak credential protection, insecure communication protocols, and limited visibility across distributed networks. Attacks like eavesdropping, denial of service (DoS), and data tampering remain significant threats. Ensuring consistent updates, data recovery, and intrusion detection across numerous devices can be difficult, especially in large scale Internet of Things (IoT) deployments. Because edge environments are more decentralized than the cloud, maintaining uniform privacy standards requires stronger coordination between hardware and software security measures.

Both standards present a trade off between convenience and control. Cloud computing offers powerful centralized resources but at the cost of data ownership and user trust, whereas edge computing enhances privacy and responsiveness but introduces the challenges of coordinating and securing a decentralized network. As Parikh et al. conclude, "the future of secure computing lies in blending the strengths of both models, leveraging computational efficiency of the cloud while adopting the localized privacy safeguards of edge computing" [6]. Research in this area continues to focus on developing encryption techniques, intrusion detection systems, and user behavior profiling to ensure that emerging architectures can provide both performance and privacy in a rapidly growing digital ecosystem.

VI. EDGE COMPUTING VS. CLOUD COMPUTING: SCALABILITY

Scalability is a major strength of both Edge Computing and Cloud Computing. Both methods of computing work similarly, allowing for resources to be easily scalable. Edge Computing allows for quick scalability and distribution of workload across multiple edge nodes [2]. However, Edge Computing has limited resources for computation and also requires that an Edge Computing center be in a specific geographic location that is close to the data source and on the edge of the network. If there is no Edge Computing center in this specific area, an Edge Computing center will need to be built. This can be a costly process, especially in areas that are hard to reach and build in [2]. Cloud Computing allows access to vast resources located in large data centers. Similarly

to Edge Computing, Cloud Computing will automatically scale up or down depending on what the tenant needs. Unlike Edge Computing, Cloud Computing relies on massive data centers, meaning Cloud Computing has higher scalability potential. Cloud Computing also allows for automatic distribution of workloads across multiple nodes, but at a significantly larger scale then Edge Computing [2].

Big Data Analysis is one of the primary uses of Edge and Cloud Computing [5]. Cloud Computing can scale to a tremendous extent, allowing for enormous amounts of data to be processed and stored in data centers. There are enough hardware resources located in data centers that can automatically scale to handle data sets of any size. Edge Computing, due to hardware limitations, does not have the ability to scale up resources to handle the large amounts of data collected from data sources. In this situation, Edge Computing is useful for collecting and quickly processing data close to the data source. However, the Edge Computing center then needs to pass on this data to data centers where Cloud Computing can handle the Big Data Analysis [5].

VII. Integrating Cloud Computing and Edge Computing Together

Cloud and edge computing can be complimentary techniques, used together in a hybrid approach. Based on specific requirements, tasks are split up using either technique to best suit a task's needs. Cloud offers a multitude of virtual services that do not need to be handled physically, while edge computing offers a more hands on approach in handling data through things such as local servers and data centers that the company themselves handle. Of course, companies are complex, made up of many different specific needs, in which adopting both techniques is beneficial. Computer science and engineering researcher, Vamsi Krishna Rao states, "This synergy enables real-time data processing and analysis at the network edge while leveraging the scalability and flexibility of cloud resources. Recent studies indicate that this approach can improve data processing efficiency by up to 50%, a remarkable advancement in fields requiring rapid decision-making and data analysis" [5]. Not only are tech companies using these two strategies but also healthcare, government agencies, schools, and universities.

Companies are using both strategies based on specific needs. Tesla uses edge computing in car sensors, as real time data is mandatory for quick response times in emergency braking, blindspot detection, and back up cameras. Data is stored locally, processed, and used in real time, providing safety and security in Tesla vehicles. Cloud computing is used in storing massive amounts of driving data, to be analyzed and used for updating navigation maps, updating vehicle software remotely, and updating Tesla's Autopilot system.

Not only is this concept being applied in tech environments but are also being used in non tech dominated spaces such as healthcare. Strict privacy rules in the healthcare industry provide a need for edge computing services. Storing patient data such as MRI scans, vital signs, background and personal information need to be stored locally, on private company servers. Edge computing is useful for short term and quick data usage, while cloud computing is needed for storing long term patient tracking, which takes up enormous amounts of storage.

Companies and industries, of all different types, use both cloud and edge computing's advantages to mitigate each other's downsides. Using both strategies' useful techniques to handle the cons of the other, are needed for a company's success in data handling, privacy, and financials. Newer technologies involving Edge as a Service (EaaS), provide a cloud based solution to edge computing using edge nodes to store data. The EaaS approach offers on demand cloud resources that are stored closer to home, similar to edge computing. Companies such as Amazon, Microsoft, and Google, provide rentable hardware that a client would pay for, without having to own and maintain it. Technologies like Edge as a Service, may finally bridge the gap between cloud and edge computing.

Although hybrid integration of both edge and cloud computing is a popular technique, it comes with its downsides. Cons to a hybrid approach include complexity of system setup, which involves needs for skillful labor to maintain such systems. Skillful labor and maintenance leads to an overall increase in spending and expenses for a company, but also purchasing hardware and online services as well. Complexity of a hybrid system may lead to higher threats to cyber attacks as there are more attack surfaces, or entry points for hackers. Data synchronization, network issues, and scaling are potential issues with hybrid systems. Ultimately, deciding whether to use an edge, cloud or hybrid approach, is up to a company and their specific needs and constraints. Each provides advantages, as well as drawbacks, which users must weigh in on, based on what can be handled in the most efficient manner.

VIII. Conclusion

Cloud computing and edge computing offer their pros and cons, each fulfilling specific needs. Edge excels in latency and privacy, while cloud performs better in scalability and processing power. These two processes show that neither one is superior to the other in every aspect of handling data, but rather using both for their positive contributions, provides the best performance even with its drawbacks. Whether one wants to store and process large/long term data on a virtual server using a cloud approach, or storing data locally for more private and faster data handling is up to the specific user to decide, although choosing one over the other is not the only choice. Technologies such as Microsoft's Azure Data Box Edge, provide a hybrid approach, offering cloud based services at an edge computing level. With new technologies, cloud vs edge computing may not be a need for discussion as the two distinct computing approaches may converge into one simple solution.

References

[1] @articlevarghese2017edge, title=Edge-as-a-service: Towards distributed cloud architectures, author=Varghese, Blesson and Wang, Nan and

Li, Jianyu and Nikolopoulos, Dimitrios S, journal=arXiv preprint arXiv:1710.10090, year=2017

[2] @articlegeorge2023edge, title=Edge computing and the future of cloud computing: A survey of industry perspectives and predictions, author=George, A Shaji and George, AS Hovan and Baskar, T, journal=Partners Universal International Research Journal, volume=2, number=2, pages=19–44, year=2023

[3] @articlekhan2019edge, title=Edge computing: A survey, author=Khan, Wazir Zada and Ahmed, Ejaz and Hakak, Saqib and Yaqoob, Ibrar and Ahmed, Arif, journal=Future Generation Computer Systems, volume=97, pages=219–235, year=2019, publisher=Elsevier

[4] @articleshi2016edge, title=Edge computing: Vision and challenges, author=Shi, Weisong and Cao, Jie and Zhang, Quan and Li, Youhuizi and Xu, Lanyu, journal=IEEE internet of things journal, volume=3, number=5, pages=637–646, year=2016, publisher=IEEE

[5] @articlebajic2019edge, title=EDGE COMPUTING VS. CLOUD COMPUTING: CHALLENGES AND OPPORTUNITIES IN INDUSTRY 4.0., author=Bajic, Bojana and Cosic, Ilija and Katalinic, Branko and Moraca, Slobodan and Lazarevic, Milovan and Rikalovic, Aleksandar, journal=Annals of DAAAM & Proceedings, volume=30, year=2019

[6] @articleparikh2019security, title=Security and privacy issues in cloud, fog and edge computing, author=Parikh, Shalin and Dave, Dharmin and Patel, Reema and Doshi, Nishant, journal=Procedia Computer Science, volume=160, pages=734–739, year=2019, publisher=Elsevier

[7] @articleshi2016edge, title=Edge Computing: Vision and Challenges, author=Weisong, Shi and Jie, Cao and Quan, Zhang and Youhuizi, Li and Lanyu, Xu, journal=IEEE Internet of Things Journal, volume=3, number=5, pages=637–646, year=2016, publisher=IEEE

[8] @articlekhan2019survey,, title=Edge Computing: A Survey, author=Wazir Zada, Khan and Ejaz, Ahmed and Saqib, Hakak and Ibrar, Yaqoob and Athanasios, Vasilakos, journal=Future Generation Computer Systems, volume=97, pages=219–235, year=2019, publisher=Elsevier