Journal of computer science and software applications
https://www.mfacademia.org/index.php/jcssa
ISSN:2377–0430
Vol. 5, No. 4, 2025

Cloud Computing: A Review of Evolution, Challenges, and Emerging Trends

Nathaniel Brooks[1], Corinna Vance[2], Dorian Ames[3]
[1]University of North Florida, Jacksonville, Florida, USA
[2]University of North Florida, Jacksonville, Florida, USA
[3]University of North Florida, Jacksonville, Florida, USA
*Corresponding Author: Nathaniel Brooks, nathaniel.brooks@unf.edu

Abstract:

With the continuous evolution of information technology, cloud computing has emerged as one of the core driving forces supporting the development of the global digital economy. As a service-oriented model for resource sharing and delivery, cloud computing has significantly transformed the construction and application of traditional IT infrastructures by providing scalable, elastic, and on-demand computing, storage, and networking resources. This paper systematically reviews the development history and fundamental theories of cloud computing, and provides a detailed analysis of the key technologies underpinning its evolution, including virtualization, containerization, microservices, serverless computing, edge computing, and software-defined networking. Moreover, it outlines the typical applications of cloud computing across various fields such as big data processing, artificial intelligence, the Internet of Things, financial services, healthcare, and education and research. The paper also examines the challenges cloud computing faces in areas such as data security, privacy protection, standardization, resource optimization, and service reliability. In addition, based on current technological trends, it explores future directions for cloud computing, including cloud-native architectures, AI-driven resource scheduling, green and sustainable cloud computing, multi-cloud and hybrid cloud management, and the potential integration of quantum computing with cloud services. By systematically reviewing existing literature and practical cases, this paper aims to provide researchers and industry practitioners with a comprehensive and in-depth reference to better understand the evolution of cloud computing technologies and identify future development opportunities.

Keywords:

Cloud Computing; Data Privacy and Security; Cloud-Native Architecture; Green Computing

1. Introduction

1.1 Research Background

With the accelerated global process of informatization, traditional IT infrastructures have revealed numerous limitations in resource utilization, scalability, flexibility, and cost control. Faced with the rapidly increasing volume of data and computational demands, enterprises and organizations are urgently seeking a computing paradigm capable of swiftly responding to business changes and optimizing resource allocation effectively. Cloud computing, as an emerging IT service delivery and usage model, has rapidly become a vital pillar in the field of information technology by offering on-demand self-service, resource pooling, rapid elasticity, and measurable services.

As early as the 1960s, computer scientist John McCarthy predicted that computing might someday become a public utility, much like electricity and water. However, the modern concept of cloud computing only began to gain widespread recognition and application after Amazon launched its Elastic Compute Cloud (EC2) service in 2006. Since then, major technology giants such as Google, Microsoft, and IBM have entered the cloud computing market, driving rapid technological advancement and continuous innovation in business models.

1.2 Definition and Core Characteristics of Cloud Computing

Cloud computing is not a single technology but rather a convergence of multiple technologies and concepts. According to the National Institute of Standards and Technology (NIST), cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is characterized by five essential features:

On-demand Self-Service: Users can automatically provision computing resources as needed without requiring human interaction.Broad Network Access: Resources are accessible over the network via standard mechanisms across heterogeneous platforms.Resource Pooling: Resources are pooled to serve multiple consumers using a multi-tenant model, with dynamic assignment according to demand.Rapid Elasticity: Resources can be elastically provisioned and released to scale rapidly outward or inward commensurate with demand.Measured Service: Resource usage is monitored, controlled, and reported, providing transparency for both the provider and consumer.

Cloud computing is commonly classified into three service models:

Infrastructure as a Service (IaaS): Provision of virtualized computing resources, such as Amazon EC2 and Google Compute Engine.Platform as a Service (PaaS): Provision of platforms for application development and deployment, such as Google App Engine and Microsoft Azure.Software as a Service (SaaS): Delivery of software applications over the Internet, such as Salesforce and Microsoft 365.Depending on the deployment model, cloud computing can be categorized into public cloud, private cloud, hybrid cloud, and multi-cloud, catering to diverse needs for resource control, security, and cost optimization.

1.3 Drivers of Cloud Computing Evolution

The rapid advancement of cloud computing technologies is underpinned by the maturity and innovation of several foundational technologies. Virtualization technology has broken the traditional boundaries of physical resources, enabling dynamic resource allocation and management. The adoption of containerization and microservices architectures has enhanced application flexibility and portability. Emerging paradigms such as edge computing and serverless computing have further expanded the boundaries of cloud computing applications, meeting the needs for low latency and high real-time responsiveness.

Meanwhile, with the rise of artificial intelligence (AI), big data analytics, and the Internet of Things (IoT), cloud computing has become an indispensable infrastructure platform for these emerging fields. By leveraging cloud computing, enterprises and organizations can not only reduce IT operational costs but also enhance business agility and innovation capabilities, driving the deepening of digital transformation.

1.4 Current Challenges and Issues

Despite its strong vitality and broad application prospects, cloud computing still faces numerous challenges in practice. Data privacy and security concerns have drawn widespread attention. Ensuring the protection of user data and regulatory compliance in a shared resource environment remains a critical issue for both service providers and users. In addition, resource scheduling and interoperability in multi-cloud and hybrid cloud environments have increased system complexity and management difficulties. Furthermore, deficiencies in cloud service outage handling and disaster recovery capabilities pose potential threats to business continuity.

In terms of sustainable development, the growing energy consumption of data centers has become increasingly prominent, making green cloud computing an important direction for future advancement. Maximizing energy efficiency while meeting performance demands is an urgent issue that the industry needs to address.

1.5 Research Motivation and Paper Organization

In recent years, research on cloud computing has deepened, and the number of related review articles has steadily increased. However, existing reviews often focus on specific subfields, such as virtualization, container technologies, or edge computing, lacking a comprehensive study that systematically outlines the development trajectory and future trends of cloud computing from a holistic perspective. Therefore, this paper aims to provide a systematic review covering core technologies, major applications, key challenges, and future development directions in cloud computing, offering valuable references and insights for researchers and practitioners in the field.

The structure of the paper is arranged as follows:

Section 2 introduces the architecture and service models of cloud computing, outlining the technical framework;
Section 3 explores the key technologies driving the development of cloud computing;
Section 4 analyzes case studies of cloud computing applications in major fields;
Section 5 systematically discusses challenges in cloud security and privacy protection;
Section 6 summarizes the major technical and management issues currently faced by cloud computing;
Section 7 envisions the future development trends of cloud computing;
Section 8 concludes the paper and provides recommendations for future research

Through systematic organization and analysis of the above content, this paper strives to present a comprehensive overview of the cloud computing field and promote subsequent research and innovation.

2. Cloud Computing Architecture and Service Models

As a novel paradigm for computing and resource management, cloud computing’ s architecture and service models form the core framework supporting its entire ecosystem. Understanding the internal structure and external service delivery methods of cloud computing is essential for grasping its developmental trajectory and application characteristics.

From an architectural perspective, cloud computing primarily comprises three fundamental resource layers: compute, storage, and network. These resources are logically abstracted and dynamically allocated through virtualization technologies. Compute resources are typically supported by large-scale server clusters employing distributed architectures to ensure high availability and elastic scalability. Storage resources include block storage, object storage, and file storage in various forms, catering to diverse data access needs across different application scenarios. In terms of networking, cloud platforms leverage software-defined networking (SDN) and high-speed interconnection technologies to enable efficient communication and flexible configuration among resource nodes. Built atop these foundational resources, the management and orchestration layer performs unified resource scheduling and monitoring, while providing essential services such as security management, identity authentication, and access control to ensure system stability and data security.

The service models of cloud computing are generally categorized into three types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).IaaS, as the foundational service model, primarily offers users virtualized compute, storage, and network resources. Users can flexibly configure operating systems, middleware, and applications according to their needs, achieving comprehensive control over the infrastructure. Representative IaaS providers include Amazon EC2, Google Compute Engine, and Microsoft Azure Virtual Machines.

PaaS builds upon IaaS by further abstracting the underlying infrastructure, providing developers with application hosting platforms that simplify the development, testing, and deployment processes. Through PaaS, developers can focus on application logic and innovation without concerning themselves with hardware and operating system management. Typical PaaS platforms include Google App Engine and Microsoft Azure App Service.

SaaS, the highest layer of cloud services, delivers application software directly to end-users, typically accessed via web browsers or client applications without the need for local installation and maintenance. Common SaaS products include Salesforce CRM, Microsoft 365, and Google Workspace.In terms of deployment models, cloud computing can be divided into four types based on differences in resource control and usage scenarios: public cloud, private cloud, hybrid cloud, and multi-cloud.Public cloud is operated by third-party service providers and offers resources to multiple tenants on a pay-as-you-go basis, providing high scalability and cost-effectiveness, making it suitable for large-scale general applications.

Private cloud is built and managed internally by a single organization, with resources exclusively used by that organization, meeting strict requirements for data security, compliance, and performance.Hybrid cloud combines the advantages of both public and private clouds by appropriately distributing workloads, achieving flexible deployment and risk mitigation.Multi-cloud strategies involve using services from multiple different public cloud providers simultaneously to avoid dependency on a single platform and to optimize resource allocation according to specific business needs.Key components supporting the efficient operation of cloud computing also include virtualization and containerization technologies.Virtualization abstracts physical resources into multiple logical units, enabling efficient resource utilization and flexible scheduling.Container technologies, such as Docker and Kubernetes, further enhance the ease of application deployment and migration, fostering the development of microservices architectures.

Moreover, with the rise of edge computing, cloud platforms are increasingly integrating edge nodes into their architectural design. By offloading part of the compute and storage tasks to the network edge, platforms can reduce latency and improve real-time responsiveness. This distributed architecture that coordinates core and edge resources is becoming a defining feature of next-generation cloud computing.

Overall, the architecture and service models of cloud computing are continuously evolving and optimizing, aiming to provide users with more efficient, flexible, and secure computing resources and application services. Understanding this architecture lays a foundational basis for further discussions on key technologies, application scenarios, and future trends in cloud computing.

3. Key Enabling Technologies

The rapid transition of cloud computing from a conceptual model to widespread practical application within just over a decade has been driven by the continuous evolution and integration of several core technologies. These key enabling technologies not only provide the foundational support for the performance, stability, and scalability of cloud platforms but also promote the diversification of cloud service models and application forms. Today, virtualization, containerization, microservices architecture, serverless computing, edge computing, and software-defined networking have become indispensable components of modern cloud computing platforms.

Virtualization is one of the foundational pillars of cloud computing. By running multiple isolated virtual machines (VMs) on a single physical server, virtualization achieves logical abstraction of resources and resource isolation in multi-tenant environments, significantly improving resource utilization and deployment flexibility. Common virtualization solutions include full and paravirtualization technologies based on hypervisors, such as KVM, Xen, and VMware ESXi. These solutions allow operating systems to run independently within virtual machines, supporting dynamic migration, elastic scaling, and load balancing, thus providing technical support for the construction of large-scale cloud data centers. With further technological advancements, hardware-assisted virtualization (e.g., Intel VT-x and AMD-V) has substantially enhanced the runtime efficiency of virtual machines, reducing virtualization overhead.

Although virtualization provides effective means for resource isolation and management, its heavyweight architecture limits deployment efficiency and portability. The rise of containerization has effectively addressed these limitations. Unlike VMs, containers run multiple isolated user spaces by sharing the host kernel, offering advantages such as lightweight operation, fast startup, and low resource overhead. The introduction of Docker standardized container building, distribution, and deployment, greatly simplifying development and operations processes. Container orchestration systems such as Kubernetes further automate container cluster management, including load scheduling, elastic scaling, service discovery, and rolling updates. By adopting containerization, developers can package applications together with their runtime environments, enabling "build once, run anywhere," thus significantly improving software delivery efficiency and system maintainability.

With the proliferation of containerization, microservices architecture has gradually replaced traditional monolithic applications and become the mainstream paradigm for cloud-native application development. Microservices decompose complex applications into a set of small, autonomous service modules, each developed and deployed around a specific business function. Services interact through lightweight communication protocols such as HTTP or gRPC. This architecture enhances system scalability and fault tolerance while allowing different service components to adopt heterogeneous languages and technology stacks. To better manage the complex inter-service communication, service mesh technologies such as Istio have emerged, offering features such as traffic control, service governance, security authentication, and observability, further strengthening the operational capabilities of microservices.

Serverless computing represents a further evolution of cloud service models. Its core idea is to completely offload infrastructure management responsibilities from developers, allowing the cloud platform to handle resource allocation, scaling, and maintenance automatically. Developers need only focus on implementing business logic, which is packaged into functions and uploaded to the platform for on-demand invocation and automatic billing. Representative serverless platforms include AWS Lambda, Azure Functions, and Google Cloud Functions. Serverless architectures are particularly well-suited for event-driven tasks and bursty workloads, such as image processing, data analytics, and IoT message handling. While achieving high elasticity and low costs, serverless computing also imposes higher requirements on platform cold start times, state management mechanisms, and scheduling strategies.

As the Internet of Things (IoT) and edge intelligence advance, the centralized architecture of traditional cloud computing has increasingly revealed bottlenecks in latency and real-time responsiveness. Edge computing complements cloud computing by deploying compute resources at edge nodes close to data sources, enabling local data processing and rapid feedback. Edge computing not only reduces data transmission latency and bandwidth consumption but also enhances privacy protection, making it suitable for scenarios requiring high timeliness, such as smart manufacturing, autonomous driving, and telemedicine. Leading cloud service

providers have launched edge computing platforms, such as AWS Greengrass and Microsoft Azure IoT Edge, offering unified management and development support through hybrid architectures that deeply integrate cloud and edge resources.
In terms of network architecture, Software-Defined Networking (SDN) and Network Function Virtualization (NFV) are becoming critical technologies for dynamic network resource management in cloud environments. SDN separates the control plane from the data plane, enabling centralized control and flexible orchestration of network paths, significantly improving network programmability and visibility. NFV virtualizes traditional hardware network functions (e.g., firewalls, load balancers, intrusion detection systems) and runs them as software on general-purpose servers, enabling on-demand deployment and elastic scaling of network services. The combination of SDN and NFV provides cloud platforms with greater flexibility and automation in complex networking environments.

Moreover, as cloud infrastructures continue to expand in scale, intelligent resource scheduling and operations have emerged as new research focuses. By leveraging artificial intelligence (AI) and machine learning (ML) technologies, cloud platforms can achieve predictive resource allocation, fault self-healing, and energy optimization. For instance, Google's DeepMind successfully deployed an AI system in its data centers, achieving over a 40% reduction in cooling energy consumption, demonstrating the immense potential of intelligent technologies in green cloud computing.In summary, the development of cloud computing is inseparable from the continuous advancement and integration of these key technologies. They not only build the technical foundation of modern cloud platforms but also lay a solid groundwork for future intelligent, efficient, and sustainable cloud computing paradigms. A deep understanding of these technologies is crucial for advancing next-generation cloud architecture design and cross-disciplinary innovative applications.

4. Application Scenarios and Case Studies of Cloud Computing

With its powerful computing capabilities, elastic resource management, and flexible service models, cloud computing has been widely integrated into various industries, becoming an important engine driving digital transformation. Different sectors have constructed diverse application scenarios based on their specific characteristics and needs using cloud computing platforms, significantly improving business efficiency and innovation capabilities. Through specific case studies, a more intuitive understanding of the value and challenges of cloud computing in practical applications can be achieved.

In the field of big data processing, cloud computing platforms provide unprecedented support for data storage, management, and analysis. Traditional data centers are limited by storage capacity and computing power, making it difficult to cope with the explosive growth of data. Cloud computing enables large-scale data processing through distributed storage and elastic computing resources. Solutions represented by big data frameworks such as Hadoop and Spark, combined with the elastic scalability of cloud platforms, achieve rapid processing and analysis of massive data volumes. Services such as Amazon’s Elastic MapReduce (EMR) and Google Cloud’s BigQuery are exemplary cloud-based big data processing solutions. Enterprises can utilize these services to achieve data mining, real-time analytics, and business intelligence applications, thereby enhancing decision-making and value extraction.

In the field of artificial intelligence and machine learning, cloud computing also serves as a foundational support platform. AI model training typically requires very high computational resources, and traditional on-premises deployment methods are costly and lack scalability. Cloud service providers have launched managed services specifically designed for machine learning, such as AWS SageMaker, Google Cloud AI Platform, and Microsoft Azure Machine Learning. These platforms not only offer high-performance computing resources like GPUs and TPUs but also integrate full-process support including data preprocessing, model training, automatic tuning, and deployment, significantly lowering the barriers to AI development and application. Through cloud resources, developers can quickly build various AI applications such as natural language processing, computer vision, and recommendation systems, achieving seamless integration from development to production.

The Internet of Things (IoT), serving as a bridge between the physical and digital worlds, naturally aligns with the data collection and processing needs of cloud computing. IoT devices are typically widely distributed, numerous, and generate data at a high rate and in diverse forms, which traditional IT infrastructures struggle to support in terms of real-time processing and scalability. Cloud computing platforms, by providing massive storage, real-time stream processing, and edge computing support, offer a reliable foundation for IoT system construction. Services such as AWS IoT Core, Microsoft Azure IoT Hub, and Google Cloud IoT Core manage millions of device connections, enabling data collection, analysis, and command delivery, and are widely used in smart manufacturing, smart cities, and smart homes. For example, General Electric (GE) launched its Predix platform, based on cloud computing architecture, to provide data analytics and predictive maintenance services for Industrial IoT (IIoT) devices, improving operational efficiency and production safety.

In the financial services sector, cloud computing is accelerating the digitalization of banks, insurance companies, and securities firms. Financial operations demand extremely high standards for data security, compliance, and availability. Cloud platforms meet these needs by providing encrypted storage, disaster recovery solutions, and compliance support. Financial institutions leverage cloud computing to modernize core systems, enhancing service agility and customer experience. For instance, Goldman Sachs partnered with AWS to launch a financial cloud platform supporting large-scale data analysis and risk management, while J.P. Morgan adopted a multi-cloud architecture to optimize trading platform performance and stability. Furthermore, FinTech companies heavily rely on cloud-native technologies to rapidly innovate, introducing new services such as mobile payments, robo-advisory, and blockchain finance, reshaping the traditional financial landscape.

The healthcare sector has also undergone profound transformations with the assistance of cloud computing. Healthcare data—including electronic health records (EHRs), imaging data, and genomic data—are large in volume and highly sensitive, and traditional storage and processing methods struggle to support the demands of precision medicine. Cloud computing platforms provide healthcare institutions with elastic storage and high-performance computing support while ensuring data privacy and security through strict compliance certifications such as HIPAA. Applications such as medical imaging analysis, telemedicine, and personalized treatment recommendations are becoming increasingly widespread. For example, the Philips HealthSuite platform, built on AWS cloud services, supports storage, sharing, and intelligent analysis of healthcare data, helping doctors make more informed clinical decisions. During the COVID-19 pandemic, cloud computing also supported large-scale remote consultations and vaccine development data analysis, demonstrating its critical role during public health crises.

The education and research sectors have likewise benefited from the democratization of resources brought by cloud computing. Traditional education resources face issues such as regional disparities and high access barriers. Cloud computing, through the construction of online education platforms and virtual laboratories, breaks time and space limitations, expanding the coverage of high-quality educational resources. Major Massive Open Online Course (MOOC) platforms such as Coursera and edX rely on cloud computing infrastructures to support millions of simultaneous learners and interactions worldwide. In scientific research, the high-performance computing (HPC) services provided by cloud platforms make complex scientific computing and large-scale simulations more accessible. CERN (European Organization for Nuclear Research) extensively uses OpenStack-based private cloud environments for data processing in particle physics research, demonstrating the significant value of cloud computing in fundamental scientific research.

At the case study level, leading cloud service providers are continuously innovating and expanding the boundaries of cloud applications. Amazon AWS, as the world's leading public cloud platform, offers more than 200 fully-featured services across computing, storage, databases, AI, IoT, and edge computing, supporting renowned clients such as Netflix, Airbnb, and NASA. Microsoft Azure, by deeply integrating with the Windows ecosystem and offering hybrid cloud capabilities, serves a wide range of industries including government, healthcare, and manufacturing. Google Cloud, leveraging its technological strengths in big data and artificial intelligence, has become the preferred platform for AI and analytics applications. IBM Cloud, by strengthening its support for hybrid cloud and enterprise-grade applications, holds a significant position in highly regulated industries such as finance and healthcare. Major cloud service providers are also actively expanding their multi-cloud and edge computing capabilities, pushing cloud services towards higher efficiency, greater intelligence, and more distributed architectures.

Overall, cloud computing has evolved from its initial role of IT resource outsourcing into a key driving force for innovation and transformation across industries. Whether improving operational efficiency, accelerating product innovation, or supporting the exploration of emerging business models, cloud computing plays an indispensable role. In the future, as technology continues to mature and application demands grow, cloud computing is expected to unleash its potential in even more fields, further shaping the industrial landscape and social structures of the digital economy era.

5. Security and Privacy Issues in Cloud Computing

With the widespread adoption of cloud computing, as data and services migrate from traditional on-premises environments to third-party hosted cloud platforms, security and privacy issues have become particularly prominent. While users enjoy the convenience and efficiency brought by cloud computing, they also face multiple challenges such as data breaches, service interruptions, identity theft, and compliance risks. Security has become one of the core issues determining whether cloud computing can continue to develop healthily, and it merits systematic analysis and discussion from multiple perspectives.

First, data privacy protection is a critical element of the cloud computing security system. Due to the multi-tenant nature of cloud computing, large amounts of sensitive data are stored centrally in the cloud, significantly increasing the risks of data breaches, unauthorized access, and malicious tampering. Traditional access control and encryption techniques remain important in cloud environments but must be optimized according to cloud-specific characteristics. Encryption technologies play a fundamental role in data protection, including encryption of data at rest, in transit, and in use (such as homomorphic encryption and trusted execution environments, TEE). Additionally, fine-grained access control mechanisms, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), dynamically adjust permissions based on user identity and context, enhancing data access security.

Identity and Access Management (IAM) is a critical means of ensuring secure access to cloud resources. In the cloud environment, traditional perimeter-based security models are gradually being replaced by identity-centric security concepts. Strong identity authentication (such as Multi-Factor Authentication, MFA), the principle of least privilege, and Single Sign-On (SSO) mechanisms have become fundamental requirements for building secure access systems. Cloud service providers typically offer built-in IAM services, such as AWS IAM, Azure Active Directory, and Google Cloud Identity, to help users centrally manage accounts and permissions, reducing security incidents caused by authentication vulnerabilities.

Compliance issues are particularly complex in cloud computing. Different countries and regions have varying legal and regulatory requirements for data protection and privacy, such as the General Data Protection Regulation (GDPR) in the European Union, the Health Insurance Portability and Accountability Act (HIPAA) in the United States, and the California Consumer Privacy Act (CCPA). Cloud service users must ensure that their operations comply with applicable compliance standards when using cloud resources, covering aspects such as data storage location, data transmission, access control, audit logs, and incident response. In response, major cloud service providers have obtained international certifications such as ISO 27001, SOC 2, and FedRAMP to demonstrate their platforms’ compliance and security. Meanwhile, users must adopt the Shared Responsibility Model, clearly delineating responsibilities between themselves and cloud providers in terms of security and compliance.

Cloud computing environments also face various types of security threats. Distributed Denial of Service (DDoS) attacks are among the most common threats, where attackers overload target services with malicious traffic, disrupting normal user access. To resist DDoS attacks, cloud platforms typically deploy distributed defense systems, combining traffic scrubbing, rate limiting, and dynamic scaling mechanisms to enhance system resilience. Data breach incidents are another major threat, often caused by misconfigurations, malicious attacks, or insider errors. To reduce the risk of breaches, cloud platforms and users should implement end-to-end encryption, multi-layered defense strategies, and continuous monitoring mechanisms.

The threat posed by malicious insiders is also a significant concern in cloud environments. Given the highly centralized and virtualized nature of cloud computing, insiders who abuse their privileges can cause severe damage to systems and data. Therefore, it is necessary to refine privilege segmentation, implement multi-level approval processes, strengthen auditing and monitoring, and introduce behavior analytics systems to promptly detect and contain abnormal operations.

Cloud service outages are another major threat affecting business continuity. Natural disasters, hardware failures, or software defects can all cause cloud service unavailability. To enhance system reliability, cloud platforms typically adopt multi-region deployment, automatic failover, and backup and recovery mechanisms to ensure rapid switchover and recovery in the event of localized failures. Users should also follow redundancy and disaster recovery design principles when building cloud-based applications to avoid severe impacts from single points of failure.

In the process of addressing security threats and privacy protection challenges, the Zero Trust Architecture (ZTA) concept has gained widespread acceptance. The zero trust model assumes that any network environment is potentially insecure and no longer automatically trusts any internal or external request. Instead, it dynamically evaluates the security of each access request through continuous verification, the principle of least privilege, and micro-segmentation strategies. Google’s BeyondCorp model is a notable example of zero trust practices, shifting access control from traditional perimeter defense to dynamic authorization based on users, devices, and contexts, thereby providing security assurance for large-scale distributed cloud environments.

Beyond traditional security techniques, artificial intelligence (AI) and machine learning (ML) are increasingly applied to cloud security. By analyzing large-scale logs and behavioral data through machine learning models, it is possible to achieve anomaly detection, threat prediction, and automated response. For example, security service platforms such as AWS GuardDuty and Azure Security Center use intelligent analysis technologies to identify potential threats and generate response recommendations, improving the efficiency and responsiveness of Security Operations Centers (SOCs). The introduction of AI technology makes cloud security defense more proactive, intelligent, and real-time.

Looking to the future, as cloud computing architectures continue to evolve and new application scenarios emerge, cloud security will become more dynamic, intelligent, and systematized. The proliferation of multi-cloud and hybrid cloud environments will bring more complex security management challenges, requiring unified security strategies and tool support across platforms. The massive integration of edge computing and IoT devices will expand the attack surface, driving deeper development of end-to-end security protection mechanisms. Privacy-Enhancing Computation technologies, such as Secure Multi-Party Computation (SMPC), Differential Privacy, and Federated Learning, are expected to maximize the utilization of data value while protecting privacy.

In summary, cloud computing security and privacy issues involve multiple dimensions, including technology, management, and law. They require joint collaboration among cloud service providers, users, and regulatory agencies to build a comprehensive, dynamic, and sustainable security assurance system. Only by effectively addressing security and privacy challenges can cloud computing better support the development of the digital society and gain users’ trust and widespread adoption.

6. Current Challenges

Although cloud computing technologies have made significant progress across multiple fields and have become critical infrastructure supporting the development of the digital economy, they still face a series of urgent challenges in large-scale application and continuous evolution. These challenges involve not only technical aspects but also management, economic, standardization, and legal dimensions, directly affecting the stability, reliability, and sustainable development of cloud computing.

First, resource management and optimization remain major factors restricting the improvement of cloud computing efficiency. Cloud platforms are generally composed of large-scale distributed data centers, and how to achieve efficient resource utilization and dynamic scheduling while meeting performance demands has always been a core challenge in system design. Existing resource scheduling strategies, such as load balancing and priority management methods, often struggle to balance fairness, efficiency, and cost control when faced with heterogeneous resource environments and complex application requirements. Especially in multi-tenant environments, competition for resources among different users may lead to resource fragmentation and imbalanced utilization, increasing operational complexity and energy consumption. With the widespread adoption of high-load applications such as artificial intelligence and big data analytics, there is a higher demand for real-time resource awareness and intelligent optimization, driving the development of machine learning-based adaptive resource management technologies. However, their stability and interpretability in large-scale production environments still require further validation and improvement.

Second, cost control has become an unavoidable issue in enterprise cloud adoption processes. Although the pay-as-you-go model of cloud computing theoretically reduces initial investments, in practice, resource waste, service dependency, and complex pricing structures often lead many enterprises to experience "cloud bill inflation" over long-term operations. Common causes of cost overruns include excessive resource reservation, failure to timely release idle resources, and opaque service billing details. Moreover, the implementation of multi-cloud and hybrid cloud strategies, while enhancing business flexibility and risk diversification, also further increases the complexity of cost management. How to optimize resource utilization, formulate reasonable procurement and deployment strategies, and introduce cost visualization and optimization tools has become key to achieving economically efficient operation in cloud environments.

Standardization and interoperability issues also hinder the development of the cloud computing ecosystem. Differences in technical implementations, interface specifications, and data formats among different cloud service providers create high technical barriers and costs for application migration and integration across platforms. The lack of unified standards not only increases users' risk of vendor lock-in but also limits the flexible orchestration and comprehensive utilization of cross-cloud resources. Although industry initiatives such as the Open Cloud Computing Interface (OCCI) and the Distributed Management Task Force (DMTF) have proposed standardization efforts, in practice, cloud providers often maintain the uniqueness of their ecosystems for competitive reasons, leading to slow progress in standard adoption. In the future, how to promote interface standardization, data format unification, and service interoperability amid competition and collaboration will be key to enhancing the overall usability and flexibility of cloud computing.

Improving service reliability and disaster recovery capabilities remains challenging. Although mainstream cloud service platforms generally adopt multi-region and multi-availability zone architectures to enhance system fault tolerance and high availability, cloud service outages still occasionally occur under extreme conditions. Cloud service failures may be caused by hardware failures, software bugs, configuration errors, or external attacks, posing serious threats to the business continuity of organizations relying on cloud platforms. To address this, cloud users should incorporate multi-level redundancy, cross-region deployment, and automatic failover mechanisms into system design, while preparing backup recovery and emergency response plans. Cloud service providers must continuously improve their monitoring and early warning systems, fault isolation and recovery capabilities, and enhance the availability assurance of underlying infrastructure and software stacks. Transparent incident reporting and clear responsibility delineation mechanisms are also necessary to strengthen user trust and promote the healthy development of the industry.

Security and privacy protection issues are becoming more complex in multi-cloud and edge computing environments. Multi-cloud deployments involve data flows and access control across different platforms, increasing the potential attack surface and complicating security management. Edge computing, by deploying compute resources at the network edge, improves application real-time performance but also faces challenges such as poor physical security, limited resources, and difficulty in updates at edge nodes, necessitating adjustments in protection and monitoring strategies. Traditional centralized security control strategies are increasingly inadequate for distributed environments, driving the development of new security technologies such as zero trust architecture, privacy-enhancing computation, and end-to-end encryption. However, these emerging technologies still face issues related to performance overhead, application scenario adaptation, and standardization in actual deployment, requiring continuous deepening and refinement through theoretical research and engineering practice.

Environmental sustainability issues are attracting growing attention. As high-energy-consuming infrastructures, cloud data centers demand substantial electricity and cooling systems, resulting in significant carbon emission pressures. With the global emphasis on green development and carbon neutrality goals, the cloud computing industry is also facing transformation requirements. Although some cloud service providers have begun to introduce renewable energy, improve data center energy efficiency design, and adopt intelligent energy optimization strategies, overall, the green transformation of cloud computing is still at an early stage. How to minimize energy consumption and environmental impact while ensuring service performance and scalability will become a key issue for the sustainable development of cloud computing in the future.

In summary, cloud computing currently faces many challenges in areas such as resource optimization, cost control, standard interoperability, service reliability, security and privacy, and environmental sustainability. The existence of these challenges not only affects user experience and trust but also constrains the further expansion of cloud computing to larger scales and broader fields. Only through continuous technological innovation, standard promotion, management optimization, and ecosystem collaboration can these constraints be effectively overcome, propelling cloud computing toward a smarter, more efficient, and sustainable new stage.

7. Future Development Trends of Cloud Computing

With continuous technological evolution and growing application demands, cloud computing is undergoing an accelerated transformation from traditional infrastructure services toward more intelligent, automated, and sustainable models. Looking ahead, cloud computing will exhibit a series of new development trends in architecture, service models, intelligence levels, and sustainability, profoundly influencing the global technology industry and the development pattern of the digital economy.

First, cloud-native technologies will become a core driving force behind the evolution of cloud computing. Cloud-native is not merely about deploying applications onto cloud platforms but emphasizes designing applications from the outset to fully leverage the elasticity, distributed nature, and automation features of cloud computing. Architectures based on containers, microservices, service meshes, and declarative APIs can significantly enhance scalability, maintainability, and rapid delivery capabilities. Kubernetes, as the de facto standard for container orchestration, has become fundamental infrastructure for modern cloud-native application development and operations. In the future, as the cloud-native concept continues to deepen, more lightweight orchestration systems and microservice governance tools optimized for multi-cloud and edge environments will emerge. At the same time, operations models such as GitOps, based on declarative configuration and automated deployment, will further proliferate, driving DevOps toward greater efficiency and intelligence.

Serverless computing, as an important innovation in cloud service models, will continue to expand its application scope and technical boundaries. By completely entrusting resource management and elastic scaling to cloud platforms, serverless architectures enable developers to focus solely on business logic, greatly improving development efficiency and application responsiveness. Currently, serverless is mainly applied to event-driven tasks and short-duration computing scenarios. However, as platform capabilities strengthen and ecosystems mature, serverless will gradually support long-lifecycle applications, stateful computing, and complex workflow orchestration. The deep integration of Function-as-a-Service (FaaS) and Backend-as-a-Service (BaaS) will further simplify the application development process, driving cloud computing toward higher levels of abstraction. Additionally, ongoing research and optimization will address challenges such as cold start latency, resource isolation, and observability in serverless environments.

Intelligent cloud platforms empowered by artificial intelligence will become a major evolutionary direction for cloud computing. Leveraging machine learning and deep learning technologies, cloud platforms will achieve more intelligent automated decision-making and adaptive adjustments in resource scheduling, load balancing, energy efficiency optimization, security protection, and fault prediction. Intelligent clouds will not only dynamically sense resource states and application demands for optimal configuration but also conduct trend forecasting and proactive adjustments based on historical data and real-time monitoring, significantly improving system stability and energy efficiency. For example, AI-driven operations platforms (AIOps) can automatically detect faults, analyze root causes, and provide repair suggestions, greatly reducing manual operation and maintenance costs. In the future, with the development of large models and self-supervised learning technologies, intelligent clouds will possess stronger self-learning and self-optimization capabilities, driving cloud platforms from passive reactive management to proactive intelligent autonomy.

Green cloud computing and sustainable development will become major strategic directions for the future of cloud computing. As high-energy-consuming facilities, cloud data centers face significant scrutiny regarding their energy efficiency and carbon emissions. In response to global carbon neutrality goals, cloud service providers are accelerating the adoption of renewable energy, optimizing cooling systems, and improving hardware energy efficiency designs. Additionally, intelligent scheduling and energy optimization algorithms enable data centers to dynamically adjust resource usage according to workloads, maximizing energy efficiency. In the future, green cloud computing will extend beyond data center energy consumption to encompass cloud application lifecycle management, carbon footprint tracking, and green development methodologies, promoting a fully sustainable cloud ecosystem. For instance, Google Cloud has committed to achieving carbon neutrality and operating entirely on renewable energy, setting an industry benchmark for green transformation. With tightening regulatory policies and increasing environmental awareness among users, green cloud computing will evolve from corporate social responsibility into a key component of market competitiveness.

Multi-cloud and hybrid cloud strategies will further deepen and become more widespread in the future. Due to differences among cloud platforms in service capabilities, geographical coverage, pricing structures, and compliance support, more enterprises are adopting multi-cloud strategies to enhance business flexibility, diversify supplier risks, and optimize costs. Hybrid cloud models integrate private and public cloud resources, supporting local storage of sensitive data and elastic expansion of public resources, meeting dual demands for security and agility across industries. In the future, as cross-cloud management and orchestration tools continue to mature, the deployment and operational complexity of multi-cloud and hybrid cloud environments will significantly decrease. For example, platforms such as Anthos, Azure Arc, and VMware Tanzu enable unified resource views and policy management, improving operational efficiency and consistency in multi-cloud environments. Additionally, cloud-neutral services and portable application architectures will further promote the free flow and dynamic optimization of cloud resources.

Edge computing and cloud-edge collaboration will become important complements and extensions of cloud computing architectures. With the proliferation of 5G communications, IoT, and intelligent terminals, massive amounts of data are generated at the network edge, creating strong demands for low-latency, local processing, and privacy protection. Edge computing, by performing preprocessing and preliminary analysis near data sources, significantly reduces data transmission latency and alleviates the load on core clouds. In the future, edge computing will integrate more closely with cloud platforms, forming multi-level, distributed computing and storage architectures. Cloud platforms will provide unified orchestration, data synchronization, and security management services for cloud-edge resources, supporting the rapid development and deployment of edge intelligent applications. Typical application scenarios include autonomous driving, industrial IoT, smart cities, and telemedicine, all of which demand high timeliness and reliability.

Privacy-Enhancing Computation technologies will play an important role in future cloud computing. Faced with increasingly stringent data privacy regulations and growing demands for user privacy protection, traditional encryption and access control measures are no longer sufficient to support data analysis and applications while preserving privacy. Technologies such as Secure Multi-Party Computation (SMPC), homomorphic encryption, federated learning, and differential privacy offer feasible solutions for computing and model training without exposing raw data. In the future, privacy-enhancing computation will be deeply integrated into cloud platform services, extending privacy protection from the application layer to the infrastructure layer, supporting cross-organization and cross-region data collaboration and intelligent application development, and balancing the value of data utilization with privacy protection needs.

Finally, the integration of quantum computing and cloud computing is expected to trigger a new wave of technological revolution. Quantum computing, with its superior processing capabilities in specific problem domains compared to classical computers, is considered one of the most disruptive future technologies. However, due to the high cost and technical complexity of quantum computers, they are unlikely to be widely accessible to end users in the short term. Providing Quantum Computing as a Service (QCaaS) via cloud platforms has become an important pathway for promoting quantum technology applications. Companies such as IBM, Google, and Amazon have already opened quantum computing resources on their cloud platforms, supporting algorithm development and testing for research institutions and enterprise users. In the future, as quantum hardware and algorithm technologies advance, cloud-based quantum computing is expected to demonstrate tremendous potential in areas such as cryptography, optimization problems, materials simulation, and artificial intelligence, forming complementary and synergistic relationships with traditional cloud computing.

In summary, future cloud computing will continue to evolve in multiple directions, including cloud-native technologies, serverless architectures, intelligent platforms, green sustainability, multi-cloud and hybrid strategies, cloud-edge collaboration, privacy protection, and quantum computing. These trends will collectively drive the transformation of cloud computing from basic infrastructure services to intelligent service systems, becoming a core force supporting the development of digital societies and intelligent economies. Facing future opportunities and challenges, cloud platforms must continuously innovate and upgrade themselves, and users must actively adapt to technological changes to maintain a competitive edge and fully unleash the potential of cloud computing.

8. Conclusion and Outlook

As a major transformative force in the field of information technology, cloud computing has evolved from its initial role as a resource outsourcing and Infrastructure as a Service (IaaS) model to become a core platform supporting the global digital economy and the construction of an intelligent society. This paper systematically reviewed the fundamental concepts, architecture, and service models of cloud computing, and provided a detailed analysis of the key technologies driving its evolution, including virtualization, containerization, microservices, serverless computing, edge computing, and software-defined networking. In addition, through real-world case studies, we discussed the extensive applications of cloud computing across multiple domains such as big data processing, artificial intelligence, the Internet of Things, financial services, healthcare, and education and research. We also deeply examined the current challenges cloud computing faces in resource optimization, cost control, standard interoperability, security and privacy protection, and sustainable development. Finally, based on the current development trends, we explored future directions for cloud computing, including cloud-native architectures, intelligent services, green and sustainable development, multi-cloud and hybrid deployment, cloud-edge collaboration, and quantum computing.

Overall, the continued development of cloud computing not only depends on the continuous breakthroughs and improvements in underlying technologies but also requires synergy in management models, standard-setting, ecosystem collaboration, and policy guidance. In the future, cloud computing will place greater emphasis on intelligence and automation, leveraging artificial intelligence, big data analytics, and machine learning to enable intelligent decision-making and adaptive optimization in resource scheduling, system operations, and security protection. At the same time, cloud platforms will continue to evolve toward decentralization and distribution, with edge computing and multi-cloud environments becoming important complements to mainstream architectures, supporting increasingly diverse and dynamic application needs.

In terms of security and privacy protection, as data scales and application complexity continue to grow, the threats facing cloud computing will become more diverse and concealed. In the future, zero trust security architectures, privacy-enhancing computation, and end-to-end encryption will become critical approaches to building trusted cloud platforms. Cloud service providers and users must jointly promote the dynamization, intelligence, and standardization of security protection systems to ensure the security and compliance of data and services in an ever-changing threat environment.

Environmental sustainability has become an important indicator of cloud computing's future competitiveness. In the face of global energy shortages and carbon neutrality pressures, green cloud computing is not only a manifestation of social responsibility but also an essential part of economic efficiency and brand value. By adopting renewable energy, optimizing data center design, and introducing intelligent energy management and carbon emission tracking mechanisms, cloud service providers can achieve sustainable development goals while offering users green and trustworthy cloud services.

Quantum computing, as a potentially disruptive technology, is expected to open new application fields and computing paradigms when combined with cloud computing in the future. Although quantum computing is still in the experimental and exploratory stage, the opening and popularization of cloud-based quantum computing platforms allow research institutions and enterprises to explore new methods for solving complex problems beyond traditional computing resources, fostering interdisciplinary innovation and breakthroughs.

Looking forward, cloud computing will no longer be merely an IT resource provision platform but will become the foundational infrastructure for intelligent society operations and the core engine of innovation ecosystems. To achieve this goal, academia, industry, and government must strengthen collaboration to jointly promote the development of key technologies, the establishment of standard systems, and the expansion of application scenarios. At the same time, users must continuously enhance their understanding of cloud computing architectures, service models, and security and privacy risks to fully unlock cloud computing’s potential in digital transformation and intelligent innovation.

In conclusion, as a revolutionary information technology that profoundly changes the world, cloud computing will continue to evolve, expand its boundaries, reshape industrial structures, and drive the socio-economic transition toward a more intelligent, greener, and more sustainable future. Through continuous innovation and open collaboration, cloud computing is poised to play an even more critical and far-reaching role in the future technological landscape.

References

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, 2011.

[2] M. Armbrust et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[3] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616, 2009.

[4] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: Towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2009.

[5] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions," Future Generation Computer Systems, vol. 79, pp. 849–861, 2018.

[6] T. Erl, R. Puttini, and Z. Mahmood, Cloud Computing: Concepts, Technology & Architecture. Upper Saddle River, NJ: Prentice Hall, 2013.

[7] D. Bernstein, "Containers and cloud: From LXC to Docker to Kubernetes," IEEE Cloud Computing, vol. 1, no. 3, pp. 81–84, 2014.

[8] M. Fowler and J. Lewis, "Microservices: A definition of this new architectural term," 2014. [Online]. Available: https://martinfowler.com/articles/microservices.html

[9] G. Adzic and R. Chatley, "Serverless computing: Economic and architectural impact," in Proc. ACM SIGPLAN International Workshop on Serverless Computing (WoSC), 2017, pp. 1–6.

[10] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016.

[11] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Communications and Mobile Computing, vol. 13, no. 18, pp. 1587–1611, 2013.

[12] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," Future Generation Computer Systems, vol. 56, pp. 684–700, 2016.

[13] X. Xu, "From cloud computing to cloud manufacturing," Robotics and Computer-Integrated Manufacturing, vol. 28, no. 1, pp. 75–86, 2012.

[14] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proc. ACM Workshop on Mobile Cloud Computing, 2012, pp. 13–16.

[15] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," ACM SIGCOMM Computer Communication Review, vol. 44, no. 5, pp. 27–32, 2014.

[16] P. Patel, A. Pathak, and R. Buyya, "Resource management and scheduling in multi-cloud computing environments: A taxonomy and survey," ACM Computing Surveys, vol. 50, no. 2, pp. 1–37, 2017.

[17] S. Singh and I. Chana, "Cloud security issues and challenges: A survey," International Journal of Computer Applications, vol. 90, no. 14, pp. 20–27, 2014.

[18] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," Information Sciences, vol. 305, pp. 357–383, 2015.

[19] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," The Journal of Supercomputing, vol. 63, no. 2, pp. 561–592, 2013.

[20] D. Catteddu and G. Hogben, Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA, 2009.

[21] A. Shahrad et al., "Serverless in the wild: Characterizing and optimizing the serverless workload at a large cloud provider," in Proc. USENIX Annual Technical Conference, 2020, pp. 205–218.

[22] H. Jin, S. Ibrahim, T. Bell, W. Gao, D. Huang, and S. Wu, "Cloud types and services," Handbook on Data Centers, Springer, 2015, pp. 335–355.

[23] T. Taleb, M. Corici, A. Nakao, and H. Flinck, "Mobile edge computing potential in making cities smarter," IEEE Communications Magazine, vol. 55, no. 3, pp. 38–43, 2017.

[24] L. Columbus, "Roundup of cloud computing forecasts and market estimates, 2021," Forbes, 2021.

[25] J. Dean and L. A. Barroso, "The tail at scale," Communications of the ACM, vol. 56, no. 2, pp. 74–80, 2013.

[26] H. Peng, Z. Zhang, and B. Liu, "A survey on cloud resource allocation techniques," Proceedings of the International Conference on Cloud Computing and Big Data, 2019.

[27] R. H. Deng, L. Wang, and B. Liu, "Privacy-preserving edge computing in the internet of things," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4920–4934, 2019.

[28] A. Ghosh, A. Bose, and P. Saha, "Cloud computing: Security issues and research challenges," International Journal of Computer Science and Information Technologies, vol. 3, no. 3, pp. 3874–3876, 2012.

[29] K. Hwang and Z. Xu, Distributed and Cloud Computing: From Parallel Processing to the Internet of Things. Morgan Kaufmann, 2012.

[30] D. Sirohi, P. Agrawal, and S. Mehfuz, "A review on serverless computing," International Journal of Cloud Applications and Computing, vol. 11, no. 1, pp. 60–75, 2021.

[31] A. Singh, M. Pathak, and K. Kumar, "An overview of multi-cloud computing: Taxonomy and challenges," International Journal of Computer Applications, vol. 182, no. 4, pp. 34–39, 2018.

[32] J. Kaur and K. Chatterjee, "Security issues in cloud computing: A survey," International Journal of Computer Applications, vol. 67, no. 3, pp. 19–22, 2013.

[33] T. Loukides, "What is DevOps?" O’Reilly Media, 2012.

[34] K. Salah, K. Habib, and S. Zeadally, "Security and privacy challenges in cloud computing environments," Future Generation Computer Systems, vol. 97, pp. 27–42, 2019.

[35] Y. Sverdlik, "Google’s data centers consume 50% less energy than the industry average," Data Center Knowledge, 2016.

[36] A. G. Ganek and T. A. Corbi, "The dawning of the autonomic computing era," IBM Systems Journal, vol. 42, no. 1, pp. 5–18, 2003.

[37] Lu, S., Liu, Z., Liu, T., and Zhou, W., "Scaling-up medical vision-and-language representation learning with federated learning," Engineering Applications of Artificial Intelligence, vol. 126, 107037, 2023.

[38] Liu, Z., Wu, M., Peng, B., Liu, Y., Peng, Q., and Zou, C., "Calibration learning for few-shot novel product description," in Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval, 2023, pp. 1864–1868.

[39] S. Lloyd et al., "Quantum computing for solving linear systems of equations," Physical Review Letters, vol. 103, no. 4, 2009.

[40] IBM Quantum, "IBM Quantum Services," 2024. [Online]. Available: https://quantum-computing.