World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Advancements in critical technology: An exploration in cloud computing, IoT, and Cyber-Physical systems

Brian Akashaba [1,*], Harriet Norah Nakayenga [1], Evans Twineamatsiko [2], Ivan Zimbe [1], Iga Daniel Ssetimba [1] and Jimmy Kinyonyi Bagonza [3]

[1] *Department of Computer Science, Maharishi International University, Iowa, USA.*
[2] *Department of Business Administration, Maharishi International University, Iowa, USA.*
[3] *Department of Computer Science, Makerere University, Kampala, Uganda.*

World Journal of Advanced Research and Reviews, 2024, 24(03), 3125-3130

Publication history: Received on 23 November 2024; revised on 28 December 2024; accepted on 30 December 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.24.3.4030

Abstract

This paper explores the latest advancements in critical technology areas such as cloud computing, the Internet of Things (IoT), and cyber-physical systems. It provides a comprehensive review of current trends, technological challenges, and future opportunities, emphasizing the potential impact of these technologies on modern industries and infrastructure.

Cloud computing offers a flexible framework in which data and resources are spread across different locations and can be accessed from various industrial environments. This technology has revolutionized the way resources such as data, services, and applications are used, stored, and shared in industrial applications. Over the past decade, industries have rapidly embraced cloud computing due to its advantages of enhanced accessibility, cost reduction, and improved performance. Moreover, the integration of cloud computing has led to significant advancements in the field of the Internet of Things (IoT). However, this quick shift to the cloud has also introduced various security concerns and challenges. Traditional security solutions are not always suitable or effective for cloud-based systems (Amit Kumar Tyagi, 2021).

In recent years, cyber-physical systems (CPS) have been to many vital areas, including medical devices, smart cars, industrial systems, energy grid, etc. As these systems increasingly rely on Internet, ensuring their security requirements, which are different from those of ordinary information technology systems, has become an important research topic.

Keywords: Cloud Computing; IoT; Cyber-physical systems; Technological Advancements

1. Introduction

The rapid development of critical technologies has revolutionized various sectors, including communication, data management, and automation. These advancements have fostered innovation, improved efficiency, and facilitated global connectivity. This paper examines three key areas of technological progress: cloud computing, the Internet of Things (IoT), and cyber-security systems. We will explore the current state of these technologies, analyze their applications and implications, and discuss the challenges and opportunities that lie ahead.

* Corresponding author: Brian Akashaba

1.1. Cloud Computing

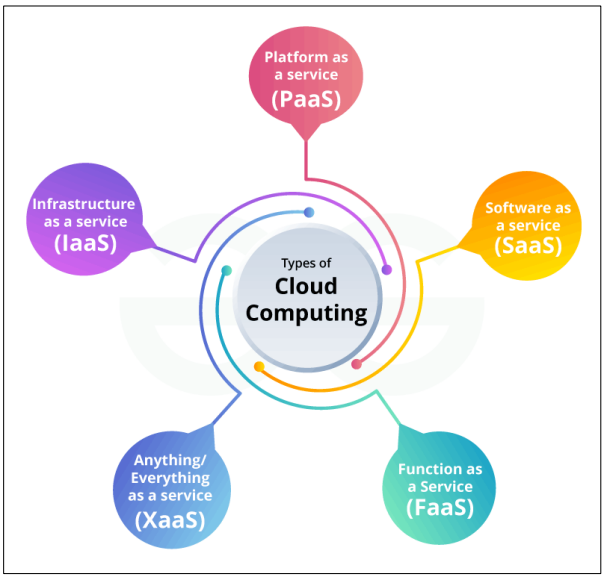

Figure 1 Types of cloud computing (Cloud based services)

Cloud computing refers to the on-demand delivery of IT resources such as servers, storage, databases, software, and networking over the internet. This model eliminates the need for physical infrastructure investment and allows for scalability based on an organization's needs. Cloud computing offers several advantages, including:

- **Cost-effectiveness:** Reduced hardware and software maintenance costs.
- **Scalability:** Easy scaling of resources up or down as needed.
- **Increased Agility:** Faster deployment of applications and services.
- **Improved Accessibility:** Access to resources from anywhere with an internet connection.

However, cloud computing also presents some challenges:

- **Security Concerns:** Data breaches and unauthorized access remain risks.
- **Vendor Lock-in:** Dependence on a specific cloud service provider can limit flexibility.
- **Latency Issues:** Network latency can affect performance for geographically dispersed users.

1.2. The Internet of Things (IoT)

The IoT refers to the network of physical devices embedded with sensors and software that collect and exchange data. These devices can range from wearables and smart home appliances to industrial sensors and connected vehicles. The growth of IoT has significant implications for various sectors, including:

- **Smart Cities:** Improved traffic management, resource optimization, and public safety.
- **Industrial Automation:** Enhanced efficiency and predictive maintenance in manufacturing.
- **Connected Healthcare:** Remote patient monitoring and personalized healthcare solutions.

However, the widespread adoption of IoT also raises concerns about:

- **Security Vulnerabilities:** Increased attack surface for cyber-attacks due to the large number of connected devices.
- **Data Privacy Concerns:** The need for robust data security protocols to protect user privacy.
- **Interoperability Challenges:** The need for standardization to ensure seamless communication between various IoT devices.

1.3. Cyber-Physical Systems (CPS)

Cyber-physical systems (CPS) are integrations of physical components and computational resources that work together to monitor and control physical processes. CPS are becoming increasingly prevalent in various applications, including:

- **Smart Grids:** Efficient management of energy distribution and consumption.
- **Autonomous Vehicles:** Improved safety and efficiency in transportation systems.
- **Advanced Robotics:** Enhanced capabilities and precision in industrial automation.

The rapid evolution of CPS also presents some challenges:

- **System Complexity:** The need for robust design and integration between physical and cyber components.
- **Real-Time Requirements:** Critical need for timely and reliable data processing for system operation.
- **Security Concerns:** The potential for cyber-attacks to disrupt physical processes.

2. Advancements in Critical Technology

2.1. Cloud Computing

- **AI/ML.** One of the most trending technologies that are close to cloud computing is Artificial Intelligence and Machine Learning. They are cost-effective technologies as they require high computational power and storage for the collection of data and training. Major advancements that will grow in this sector in the upcoming years are self-automation, self-learning, personalized cloud, high data security, and privacy. Many cloud service provider companies such as Amazon**,** Google**,** IBM, etc are investing a lot in artificial intelligence and machine learning. Amazon's AWS Deep Lens camera and Google Lens are two such examples of their products based on machine learning (Wang, J, 2024).
- **Data Security.** When it comes to data security, no business or organization wants to compromise. Security of the organization's data is a top priority. Threats such as data leaks, data deletion, and unauthorized amendments to the data need to be minimized. Certain steps can be taken to minimize the losses and ensure high data security (Namasudra, Suyel., 2024).
- **Multi and Hybrid Cloud Deployment.** The use of multi-cloud and hybrid solutions is increasing. Many organizations like banks, insurance companies, etc are using hybrid cloud service that offers a combination of both private and public clouds to store their data.
  Now, businesses are dividing their workload among multiple cloud service providers to control their data and resources as well as utilize the strength of each cloud service provider. The use of multi-cloud minimizes the potential risks and failure points and provides cost-effectiveness. In multi-cloud, you can choose a particular service of a particular cloud service provider that meets your requirements instead of deploying your entire application on that cloud. This will also ignite the cloud service providers to embed new services.
- **Low Code and No Code Cloud Solutions.** Those days are gone when users need to write hundreds of lines of code to create applications and solve real-world problems and have deep technical knowledge. Businesses can create applications and make use of AI and its subdomains with low-code and no-code cloud solutions. These solutions can help in the development of websites, apps, services, etc without having any technical knowledge. This helps in reducing the time and cost involved to create these solutions. These solutions increase product development speed and result in a smaller number of errors. Tools such as Figma and Zoho enable users to design and develop websites, apps, and services without any computing infrastructure and coding knowledge involved.
- **Edge Computing.** Edge computing includes storage of data, data processing, and data analytics which is done geographically nearer to the source. It means that the computation and storage of data are brought closer to the source sensors and devices. It provides many benefits like reduced latency, enhanced efficiency, increased privacy, security, and a high rate of data transmission. It works in real-time and processes data that is not bounded by time.
  As the use of 5G is increasing, it is easy to achieve fast processing and reduced latency. Also, many telecom and IT organizations are uniting, resulting in the rise in edge computing. With the rise in IoT devices, edge computing will play a huge role in providing real-time data and data analysis.
- **Kubernetes and Docker.** Kubernetes is an open-source orchestration platform where scaling, management, and deployment of applications is done automatically. It provides automation to the cloud network users. Organizations can choose a particular Kubernetes platform based on their requirements. Docker is a platform where developers can package applications and can deploy them anywhere in the form of containers. Kubernetes and Docker are among the trending and evolving technologies in cloud computing. They are an open-source platform that manages services and workloads from a single location while running applications from a single source. They provide scalability and efficiency to many large-scale deployments. As the use of cloud computing services is increasing, Kubernetes and Docker play a major role in managing cloud deployments of cloud users and organizations.

- **Serverless Architecture/Computing.** Serverless computing is a methodology that provides backend services on a per-user basis. There is no need for developers to manage the servers while running their code. Code execution is managed by the cloud service provider. Cloud users will pay as per the pay-as-you-go format which means that users will only pay when their code runs instead for a fixed server. There is no need to purchase the servers as a third party will manage the cost for you. This will help in reducing infrastructure costs and will enhance scalability.
  This trend can be automatically scaled as per its demand. Serverless architecture offers many advantages such as no requirement for system administration, low cost and liability, easy management of operations, and enhanced user experience even in case of no internet.
- **DevSecOps.** Cloud computing provides many benefits to its customers in managing their data but along with that, many security issues are sometimes faced by the users. Risks involving network invasion, Denial of Service (DoS) attacks, issues in virtualization, unauthorized use of data, etc. This can be minimized with the help of DevSecOps.
  DevSecOps is an integration of security with the ongoing development process. It embeds many processes in its workflow to ensure secure task automation. Many cloud service providers provide various tools and services to help businesses apply DevSecOps methods. It will provide all the required security to provide a secure system to the users.

2.2. The Internet of Things (IoT)

There is a wide range of work to be done on IoT (Internet of Things) to further its development and maximize its potential. Here are some key areas where work is ongoing or needed:

- **Security**: IoT devices are often vulnerable to cyber-attacks. Developing robust security measures and standards for IoT is crucial to protect data and privacy.
- **Interoperability**: IoT devices from different manufacturers often don't work seamlessly together. Efforts are underway to establish common communication protocols and standards to enhance interoperability.
- **Scalability**: IoT networks must be able to handle the increasing number of connected devices. Scaling IoT infrastructure, both in terms of hardware and software, is essential.
- **Low-Power Devices**: Creating more efficient and longer-lasting power sources for IoT devices, especially those in remote or inaccessible locations, is a priority (Tao, Fei, 2014).
- **Data Management**: IoT generates vast amounts of data. Developing efficient data storage, processing, and analytics solutions is essential to extract meaningful insights (Bedi, Guneet, et al 2018).
- **Edge Computing**: Processing data closer to the source (at the edge) rather than sending it all to centralized servers can reduce latency and improve IoT system efficiency.
- **Privacy**: Addressing concerns around the privacy of individuals in IoT ecosystems is crucial. Implementing robust privacy policies and practices is essential.
- **User-Friendly Interfaces**: Creating intuitive user interfaces and experiences for controlling and interacting with IoT devices is important for widespread adoption.
- **AI Integration**: Combining IoT with artificial intelligence can enhance its capabilities, but this integration needs further exploration and development (Aldhaheri, Alyazia et al, 2024).
- **Standardization**: Developing and adhering to industry standards is vital for the growth and maturity of IoT technologies.
- **Healthcare**: In the healthcare sector, there's a need for improved IoT-based remote patient monitoring and healthcare management solutions.(Li, Chunyan, et al, 2024)
- **Agriculture**: Enhancing IoT applications in agriculture for precision farming, crop monitoring, and sustainable practices.
- **Smart Cities**: Expanding IoT applications for more efficient urban planning, traffic management, and resource utilization in smart cities. These are just a few areas where work is needed in the IoT field. IoT is a rapidly evolving technology, and ongoing research, innovation, and collaboration are essential to unlock its full potential and address its challenges effectively (Albreem, Mahmoud AM, et al. 2017).

2.3. Cyber-Physical Systems (CPS)

CPSs are used as the new generation of embedded control system that can monitor and control the physical world. Many applications like energy, transportation and healthcare are being increasingly dependent on CPSs. It depends on the technology being used as a very relevant and symbolic CPS is the Supervisory Control and Data Acquisition system (Thomas, Mini S.,et al 2004) , wearable and Implantable Medical Devices.

- **Industrial Control Systems (ICS):** ICS (or SCADA or distributed control systems) is the control system that enhances the control and production while monitoring different industries such as the nuclear plants, water and sewage systems, and irrigation systems. In ICS, we have different controllers such as PLC (Programmable Logic Controller). This device has variety of capabilities that can collaborate to reach a number of desired results. Sensors and actuators are being used to connect this device to the physical world. Both the wireless and wired communication capacities are configured in this system that can be used based on the nature of surroundings. Further, it can monitor and control the operations in a control Centre by connecting it to PC systems.
- **Smart Grid Systems**: Although power grid is being used for decades, smart grid is the next generation grid for generating electricity with advanced functionalities. At local level, it is economically and environmentally feasible by allowing the consumer to have better control over their usage of energy. While at the national level, it enhances the control over emission, global load balancing and saves the energy.
- **Medical Devices**: Cyber and physical capabilities have been incorporated to improvise medical devices with an aim to deliver better health care services. These medical devices are designed to serve the patients by being implanted inside the patient's body or worn by them in the form of wearable devices. Such devices are smart and they have wireless capabilities to communicate with other devices. This communication is being provided by programmer, require for updating and reconfiguring the devices. Wearable device is more helpful in tracking minor activities of patients.
- **Smart Vehicles**: Smart Vehicles are vehicles that are more environmentally friendly, more fuel-efficient, safer, and have improved usability and convenience. Through depending on a number of 50–70 networked computers, called Electronic Control Units (ECUs), these developments were made possible. ECUs (Bird, et al 2005)are responsible for monitoring and regulating different functions such as engine emission control, brake control, entertainment (radio and multimedia players) and comfort features (cruise control and opening and closing of windows). Such innovations are most needed technology in current era scenario (i.e., to reduce traffic congestion, accidents, etc., over the road/region) (Amit Kumar Tyagi,et al 2021).

3. Challenges and Opportunities

The advancements in critical technologies discussed in this paper present both challenges and opportunities. Here's a closer look at some key points:

3.1.1. Challenges

- **Security Concerns:** Securing data, devices, and systems across all these technologies remains a top priority. Continuous innovation in cyber security solutions is essential to mitigate evolving threats.
- **Privacy Concerns:** Data privacy regulations and user trust are paramount considerations for businesses deploying these technologies.
- **Interoperability:** Ensuring seamless communication and data exchange between different technologies and platforms requires standardization efforts.
- **Scalability and Sustainability:** Managing the increasing volume of data generated by these technologies while ensuring energy efficiency is crucial.
- **Ethical Considerations:** The potential impact of these technologies on jobs, automation, and societal behavior needs careful consideration (T. Dillon, et al 2010).

3.1.2. Opportunities

- **Enhanced Efficiency and Productivity:** These technologies offer significant potential to optimize processes, streamline workflows, and improve overall efficiency.
- **Innovation and New Business Models:** The integration of these technologies can lead to the development of innovative solutions and disruptive business models across various industries.
- **Improved Decision Making:** Real-time data insights gleaned from these technologies can empower better decision-making at individual and organizational levels.
- **Global Connectivity and Collaboration:** These advancements can facilitate seamless communication and collaboration across geographical boundaries.
- **Improved Quality of Life:** The applications of these technologies can potentially improve healthcare delivery, resource management, and overall quality of life

4. Conclusion

Advancements in these critical technologies present significant opportunities for innovation and efficiency, but also pose challenges related to security, scalability, and interoperability.

The rapid evolution of cloud computing, IoT, and cyber-physical systems is reshaping the technological landscape. These advancements offer immense opportunities for innovation, efficiency, and global connectivity. However, addressing the associated challenges related to security, privacy, interoperability, scalability, and ethical considerations is crucial for the responsible and sustainable development of these technologies. As researchers, practitioners, and stakeholders, we must work collaboratively to maximize the positive impact of these advancements while mitigating potential risks. By fostering open communication, investing in robust security solutions, and prioritizing ethical considerations, we can ensure that these critical technologies contribute to a brighter and more connected future.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Bedi, Guneet, et al. "Review of Internet of Things (IoT) in electric power and energy systems." IEEE Internet of Things Journal 5.2 (2018): 847-870.

[2] Albreem, Mahmoud AM, et al. "Green internet of things (IoT): An overview." 2017 IEEE 4th International Conference on Smart Instrumentation, Measurement and Application (ICSIMA). IEEE, 2017.

[3] Tao, Fei, et al. "CCIoT-CMfg: cloud computing and internet of Things based cloud manufacturing service system." IEEE Transactions on Industrial Informatics 10.2 (2014): 1435-1442.

[4] T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges," 2010 24th IEEE International Conference on Advanced Information Networking and Applications, Perth, WA, Australia, 2010, pp. 27-33, doi: 10.1109/AINA.2010.187.

[5] Wang, J., Lu, T., Li, L., & Huang, D. (2024). Enhancing Personalized Search with AI: A Hybrid Approach Integrating Deep Learning and Cloud Computing. Journal of Computer Technology and Applied Mathematics, 1(4), 89–99. https://doi.org/10.5281/zenodo.13998900

[6] Namasudra, Suyel. "Data access control in the cloud computing environment for bioinformatics." In Research Anthology on Bioinformatics, Genomics, and Computational Biology, pp. 553-565. IGI Global, 2024.

[7] Morchid, Abdennabi, Rachid El Alami, Aeshah A. Raezah, and Yassine Sabbar. "Applications of internet of things (IoT) and sensors technology to increase food security and agricultural Sustainability: Benefits and challenges." Ain Shams Engineering Journal 15, no. 3 (2024): 102509.

[8] Li, Chunyan, Jiaji Wang, Shuihua Wang, and Yudong Zhang. "A review of IoT applications in healthcare." Neurocomputing 565 (2024): 127017.

[9] Aldhaheri, Alyazia, Fatima Alwahedi, Mohamed Amine Ferrag, and Ammar Battah. "Deep learning for cyber threat detection in IoT networks: A review." Internet of Things and Cyber-Physical Systems 4 (2024): 110-128.

[10] Thomas, Mini S., Parmod Kumar, and Vinay K. Chandna. "Design, development, and commissioning of a supervisory control and data acquisition (SCADA) laboratory for research and training." IEEE Transactions on power systems 19, no. 3 (2004): 1582-1588.

[11] Amit Kumar Tyagi, N. Sreenath, Cyber Physical Systems: Analyses, challenges and possible solutions, Internet of Things and Cyber-Physical Systems, Volume 1, 2021, Pages 22-33, ISSN 2667-3452, https://doi.org/10.1016/j.iotcps.2021.12.002.(https://www.sciencedirect.com/science/article/pii/S2667345221000055)

[12] Bird, Gary, Michael Christensen, Daniel Lutz, and P. Scandura. "Use of integrated vehicle health management in the field of commercial aviation." In Proceedings of NASA ISHEM Forum, pp. 7-10. 2005.

[13] Shekhar, Aishwarya & Aleem, Abdul. (2024). Improving Energy Efficiency through Green Cloud Computing in IoT Networks. 10.1109/IC2PCT60090.2024.10486633.