Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(RESEARCH ARTICLE)

Check for updates

Compliance and Governance issues in Cloud Computing and AI: USA and Africa

Adebola Folorunso [1], Olufunbi Babalola [2], Chineme Edger Nwatu [3,*] and Urenna Ukonne [4]

[1] *School of Business, Technology and Health Care Administration Capella University, Minneapolis, MN, USA 55402.*
[2] *Carnegie Mellon University, 5000 Forbes Avenue Pittsburgh, PA 15213.*
[3] *Western Illinois University School of Computer Sciences Stripes Hall 44, 1 University Circle Macomb IL 61455-1390 US.*
[4] *Harrisburg University of Science &Technology, Systems Engineering 326 Market Street Harrisburg, PA 17101 USA.*

Global Journal of Engineering and Technology Advances, 2024, 21(02), 127–138

Publication history: Received on 07 October 2024; revised on 19 November 2024; accepted on 21 November 2024

Article DOI: https://doi.org/10.30574/gjeta.2024.21.2.0213

Abstract

The rapid expansion of cloud computing and artificial intelligence (AI) has driven transformative change across various industries, presenting both opportunities and challenges in the realms of compliance and governance. This review examines the distinctive and overlapping compliance and governance issues faced by the United States (USA) and African countries in managing cloud computing and AI technologies. In the USA, compliance frameworks such as the California Consumer Privacy Act (CCPA), HIPAA, and the NIST AI Risk Management Framework provide regulatory infrastructure, emphasizing data privacy, sovereignty, and AI ethics. In contrast, African nations, led by South Africa's Protection of Personal Information Act (POPIA) and regional initiatives like those promoted by the African Union, are developing data protection and AI governance structures within diverse and resource-constrained environments. Key compliance concerns include data privacy, sovereignty, and cross-border data transfers, with the USA focusing on sectoral regulations and Africa on emerging continent-wide data frameworks. Governance challenges differ across regions, especially in data ownership, AI ethics, and risk management; in the USA, well-established risk management frameworks enable more consistent cybersecurity practices, whereas African nations often face hurdles related to limited infrastructure and varying regulatory standards. This comparative analysis underscores the importance of harmonized policies, highlighting the need for collaborative, cross-regional initiatives to mitigate regulatory disparities and foster secure data flows. Ultimately, this review advocates for adaptive, flexible frameworks that incorporate ethical AI guidelines and global best practices, which are essential for supporting sustainable cloud and AI adoption across the USA and Africa. Through proactive compliance strategies and enhanced governance mechanisms, these regions can effectively navigate the challenges of a technology-driven global landscape while promoting innovation and protecting stakeholder interests.

Keywords: Cloud Computing; Artificial intelligence. USA; Africa

1. Introduction

Cloud computing and artificial intelligence (AI) have transformed industries worldwide, enabling increased data accessibility, real-time analytics, and innovative solutions across sectors such as finance, healthcare, and government (Akter *et al*., 2022; Kanungo, 2020). In the USA, cloud adoption has been robust, driven by technological advances, a strong digital infrastructure, and a regulatory environment that balances innovation with compliance. Major cloud providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud dominate the market, offering scalable solutions that support AI applications in sectors from retail to healthcare (Dhanaraj *et al*., 2021; Sharma *et al*., 2022). Africa, while still developing its digital infrastructure, has also seen significant growth in cloud computing and AI adoption. With an emerging tech ecosystem and mobile-first innovations, African countries are increasingly utilizing cloud platforms to enhance business operations, healthcare, and educational services. Yet, cloud and AI adoption across

* Corresponding author: Chineme Edgar Nwatu

Africa often face infrastructure and regulatory challenges, alongside issues related to data sovereignty and cross-border data flows.

The accelerated adoption of cloud and AI across both regions highlights the importance of comprehensive compliance and governance frameworks (Kumar, 2022). These frameworks ensure that cloud technologies and AI systems operate within secure, ethical, and lawful boundaries. For instance, data breaches and misuse of AI can compromise user trust and lead to substantial legal penalties. Compliance frameworks, therefore, play a critical role in safeguarding user data, promoting accountability, and maintaining regulatory alignment (de Almeida *et al*., 2021). Governance frameworks, on the other hand, establish clear roles, responsibilities, and oversight mechanisms to ensure that cloud computing and AI applications operate transparently and, in the public's, best interest. Together, compliance and governance frameworks support secure, ethical AI and cloud usage, addressing concerns around data privacy, transparency, and fairness (Chang, 2021).

While both the USA and African nations acknowledge the necessity of these frameworks, their regulatory approaches reveal key differences shaped by distinct socio-economic and technological landscapes. The USA, for instance, has adopted a sectoral approach to regulation, with specific laws governing data privacy in healthcare (HIPAA) and consumer protection (CCPA) (Mulgund *et al*., 2021). Additionally, the USA's regulatory bodies, such as the Federal Trade Commission (FTC) and the National Institute of Standards and Technology (NIST), provide industry guidelines and compliance frameworks that promote data security and AI ethics. In contrast, African countries have started adopting data protection laws, such as South Africa's Protection of Personal Information Act (POPIA) and Kenya's Data Protection Act, aiming to protect personal data while encouraging tech adoption. However, regulatory enforcement can vary widely across the continent, often due to resource constraints and differing legislative priorities (Preston *et al*., 2020). This creates complexities in ensuring consistent compliance, especially as cloud platforms and AI applications gain traction across borders.

Another difference in regulatory approaches lies in data sovereignty and localization policies. The USA's relatively open stance on data flow aligns with its globalized tech sector, although concerns about cross-border data transfers and data security have led to increased scrutiny (Chang *et al*., 2020). In Africa, the demand for data sovereignty is stronger, as governments prioritize protecting citizens' data within national borders. This emphasis on data localization presents both challenges and opportunities for cloud providers and AI developers, who must adapt to diverse regulatory requirements across multiple jurisdictions.

The USA and Africa represent two distinct approaches to cloud computing and AI regulation, shaped by their unique challenges and growth trajectories. As cloud and AI adoption continue to expand, the importance of compliance and governance frameworks cannot be overstated. These frameworks provide a foundation for secure, ethical, and transparent technology adoption, fostering trust and innovation in the digital ecosystem. The following sections will delve into specific elements of compliance and governance, examining how these frameworks can be adapted to address the regulatory landscapes and technological needs in both the USA and Africa.

2. Compliance Issues in Cloud Computing and AI

As organizations increasingly adopt cloud computing and artificial intelligence (AI), compliance with data privacy and protection laws becomes critical to safeguard user information and uphold trust. In both the USA and Africa, compliance challenges arise from varied legal frameworks, data sovereignty requirements, and the rapid evolution of AI technologies.

In the USA, data privacy is governed by a patchwork of laws and regulations. The California Consumer Privacy Act (CCPA) is one of the most comprehensive state-level privacy laws, granting consumers rights to understand how their personal data is collected, used, and shared by businesses (Determann and Tam, 2020). It mandates that companies disclose their data practices and allows consumers to opt out of the sale of their personal information. Additionally, sector-specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), impose strict standards for protecting sensitive health information. HIPAA requires healthcare providers and their business associates to implement safeguards to secure patient data, ensuring privacy and confidentiality.

In Africa, the landscape of data protection is evolving rapidly, with various nations adopting their own regulations. South Africa's Protection of Personal Information Act (POPIA) serves as a significant benchmark, aiming to promote the responsible processing of personal data and enhancing individuals' privacy rights (Nyoni *et al*., 2020; Netshakhuma, 2022). Other countries, such as Kenya and Nigeria, are also developing data protection laws, reflecting a growing recognition of the importance of safeguarding personal information. However, challenges arise due to varying

enforcement levels across countries, leading to inconsistencies in compliance. Furthermore, cross-border data transfer issues complicate compliance efforts, as organizations must navigate different legal requirements when moving data across national boundaries. The level of data protection infrastructure varies significantly, impacting the ability to enforce compliance effectively.

Data sovereignty refers to the idea that data is subject to the laws and regulations of the country in which it is located (Vatanparast, 2020). In the USA, there is no overarching federal data sovereignty policy; instead, state-level regulations can impose specific requirements. For instance, certain states may have laws dictating how data must be stored or managed. However, federal initiatives focus on ensuring national security and protecting sensitive information held by government entities. Conversely, in Africa, data localization efforts are gaining traction, driven by the African Union's emphasis on digital sovereignty. Many African nations are advocating for data residency requirements that mandate data generated within their borders to be stored locally. This movement reflects a desire to control data flows and protect citizens' privacy, but it also poses challenges for cloud service providers who must adapt their infrastructure to comply with these regulations. Balancing international data flow with local regulatory demands is a significant hurdle, as companies must ensure compliance while maintaining operational efficiency.

As AI technologies proliferate, establishing compliance standards specifically tailored to AI applications becomes increasingly important. In the USA, initiatives like the National Institute of Standards and Technology (NIST) AI Risk Management Framework aim to provide guidelines for managing AI risks. This framework emphasizes the need for transparency, accountability, and ethical considerations in AI development and deployment. Emerging AI accountability frameworks are also being discussed to address potential biases and ensure fairness in AI systems (Oyeniran *et al*., 2022). In Africa, the development of AI policies is still in its nascent stages. Several countries are beginning to draft their own frameworks, while pan-African organizations are working towards creating unified standards for AI governance. These efforts aim to address the ethical implications of AI technologies, ensuring that they are deployed in a manner that is transparent and equitable. However, establishing clear guidelines on AI transparency, fairness, and accountability presents challenges. Diverse cultural contexts and varying levels of technological maturity across African nations complicate the creation of a cohesive regulatory framework.

Compliance issues in cloud computing and AI present complex challenges in both the USA and Africa. The need for robust data privacy and protection laws, clear data sovereignty and residency requirements, and well-defined AI-specific compliance standards is paramount. Organizations must navigate a dynamic regulatory landscape that varies significantly between regions, and they must be proactive in developing and implementing compliance strategies that address these challenges (Lescrauwaet *et al*., 2022). As cloud computing and AI continue to evolve, the importance of effective compliance measures will only grow, demanding ongoing collaboration between governments, industry stakeholders, and technology providers to create a secure and trustworthy digital ecosystem.

2.1. Governance Issues in Cloud Computing and AI

As cloud computing and artificial intelligence (AI) continue to revolutionize various sectors, effective governance is essential to ensure the ethical, secure, and responsible use of these technologies as explain on figure 1 (Ahmad *et al*., 2022; Mökander, 2023). Governance issues encompass data ownership, risk management, security standards, and ethical considerations, presenting distinct challenges in both the USA and Africa.

In the USA, data governance is primarily characterized by corporate control and user rights. Organizations emphasize the importance of maintaining ownership over the data they generate, often implementing stringent data sharing practices with third parties. Regulatory frameworks, such as the California Consumer Privacy Act (CCPA), mandate that companies disclose their data handling practices to users, ensuring transparency and providing individuals with rights over their personal information. However, as organizations increasingly leverage third-party cloud services, questions arise regarding data ownership, especially in multi-tenant environments where multiple clients share the same infrastructure. The complexities of data ownership are further compounded by the existence of cross-border data flows, necessitating clear governance frameworks that delineate responsibilities and rights among various stakeholders (Carter *et al*., 2021).

In Africa, governance frameworks for data management are still evolving, particularly in the context of partnerships with multinational corporations and foreign cloud providers. Emerging regulations, such as South Africa's Protection of Personal Information Act (POPIA), aim to address data governance concerns by promoting responsible data processing practices. However, the continent faces challenges in establishing consistent data governance policies, especially in regions with varying regulatory landscapes (Bernier *et al*., 2022). The lack of a unified approach complicates data ownership issues, particularly when data crosses national borders or when organizations collaborate with foreign

entities. Defining ownership rights in multi-tenant and cross-border environments remains a significant challenge that necessitates robust governance structures.

Risk management and cybersecurity are paramount in both the USA and Africa, particularly as organizations increasingly rely on cloud computing (Abioye *et al*., 2021). In the USA, regulatory requirements such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Federal Risk and Authorization Management Program (FedRAMP) outline stringent security standards for cloud service providers. These frameworks are designed to ensure that organizations implement robust cybersecurity measures to protect sensitive data and maintain operational integrity. However, the rapid evolution of cyber threats poses ongoing challenges, requiring organizations to remain vigilant and continuously update their security protocols. In Africa, cybersecurity challenges are amplified by the lack of resources and infrastructure in many regions. While initiatives like Smart Africa aim to enhance cybersecurity awareness and establish security standards across the continent, organizations often struggle to address the complexities of securing multi-cloud environments. Limited financial and technical resources hinder the implementation of comprehensive cybersecurity measures, leaving organizations vulnerable to cyber threats (Uddin *et al*., 2020). As more businesses adopt cloud solutions, the need for region-specific governance frameworks that address these challenges becomes increasingly critical.

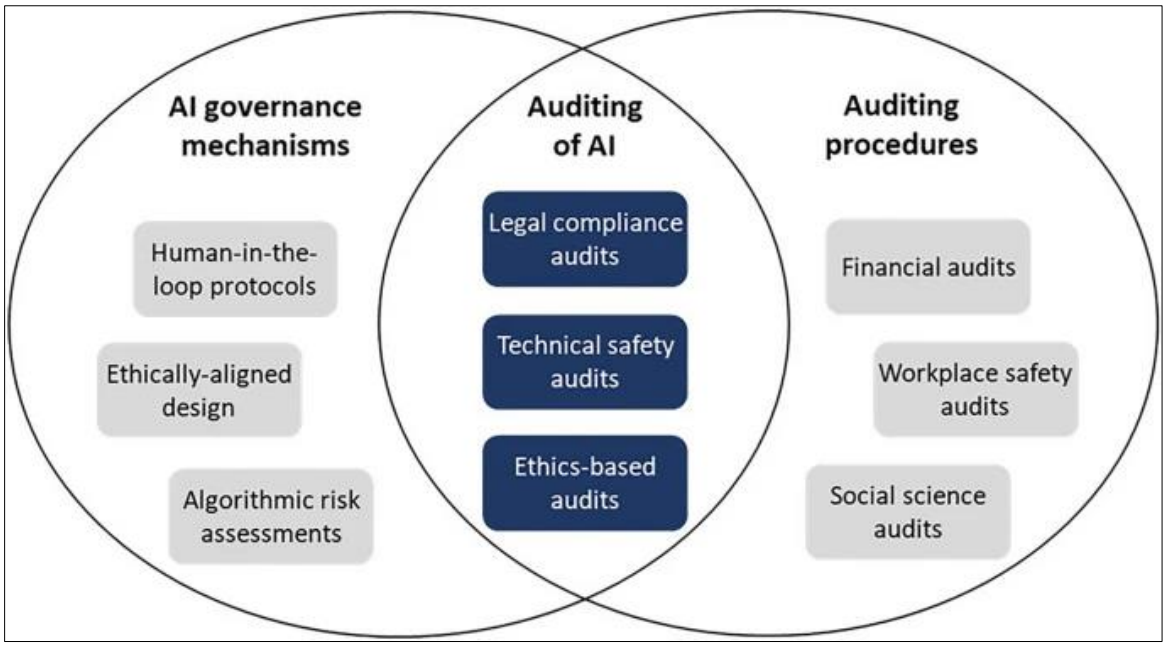

Figure 1 A schematic overview of how auditing of AI relates to previous work on AI governance (Mökander, 2023)

The ethical use of AI is a growing concern in both the USA and Africa, with an emphasis on transparency, bias minimization, and accountability. In the USA, initiatives like the Blueprint for an AI Bill of Rights focus on establishing policies that promote ethical AI practices (Saveliev and Zhurenkov, 2021). These efforts underscore the importance of transparency in AI algorithms, ensuring that users understand how their data is used and how decisions are made. However, the rapid deployment of AI technologies raises concerns about inherent biases in algorithms and their potential impact on marginalized communities. In Africa, emerging ethical AI initiatives reflect the continent's commitment to responsible AI development. The African Union has proposed guidelines aimed at promoting ethical AI practices that align with local values and priorities (Gaffley *et al*., 2022). These initiatives are crucial for ensuring that AI technologies contribute to the continent's socio-economic development without perpetuating existing inequalities. However, balancing AI ethics with economic development goals presents challenges. As countries strive to harness AI for growth, they must ensure that ethical considerations are not overshadowed by economic imperatives (Feijóo *et al*., 2020). Aligning local ethical standards with global best practices is essential for fostering responsible AI governance across the continent.

Governance issues in cloud computing and AI present significant challenges and opportunities in both the USA and Africa. As organizations navigate the complexities of data ownership, risk management, and ethical AI practices, the need for robust governance frameworks becomes increasingly apparent. By addressing these issues through collaboration and the development of comprehensive policies, stakeholders can ensure the responsible use of cloud computing and AI technologies, ultimately fostering trust and driving innovation in the digital age (Jelovac *et al*., 2022).

2.2. Comparative Analysis of Regulatory Approaches to Cloud Governance and Compliance in the USA and Africa

The evolution of cloud computing and artificial intelligence (AI) has necessitated robust regulatory frameworks to ensure data governance and compliance (Shah and Konda, 2022). This comparative analysis explores the differences and similarities in regulatory approaches between the USA and African countries, the impact of international regulations on local cloud governance in Africa, and the examination of collaborative initiatives aimed at bridging compliance gaps.

The regulatory landscape in the USA is characterized by a decentralized approach, where multiple layers of federal and state regulations govern cloud computing and data privacy (Kushwaha *et al*., 2020). Major regulations, such as the California Consumer Privacy Act (CCPA) and the Health Insurance Portability and Accountability Act (HIPAA), provide specific frameworks for data protection. The emphasis in the USA is on corporate responsibility, consumer rights, and the protection of sensitive information, but the regulatory patchwork can create challenges for businesses operating across different states. In contrast, many African nations are in various stages of developing comprehensive regulatory frameworks for cloud governance (Shibambu and Marutha, 2022). While South Africa's Protection of Personal Information Act (POPIA) is a significant step toward enhancing data protection, other countries on the continent lack similar robust regulations. However, a common trend among African countries is the increasing focus on establishing national data protection laws, reflecting a collective recognition of the importance of governance in the digital age. Despite the differences in regulatory maturity, both regions share a commitment to protecting data privacy and fostering secure cloud environments.

International regulations, particularly those emerging from the European Union, such as the General Data Protection Regulation (GDPR), have far-reaching implications for local governance and compliance efforts in Africa as explain in figure 2 (Makulilo, 2021; Georgiadis and Poels, 2022). As African nations seek to engage in international trade and partnerships, aligning their regulations with global standards becomes essential. The GDPR sets a high bar for data protection, compelling many African countries to enhance their data privacy frameworks to facilitate cross-border data flows. For instance, organizations in Africa that wish to collaborate with European entities must adhere to GDPR standards, which can lead to improved data governance practices locally. However, the challenge lies in adapting these international regulations to local contexts. Many African countries face resource constraints and varying levels of technological infrastructure, which can impede their ability to implement stringent compliance measures. Thus, while international regulations serve as a benchmark for data governance, there is a pressing need for tailored approaches that consider the socio-economic realities of individual African nations (Ebrahim *et al*., 2020; Jernite *et al*., 2022).

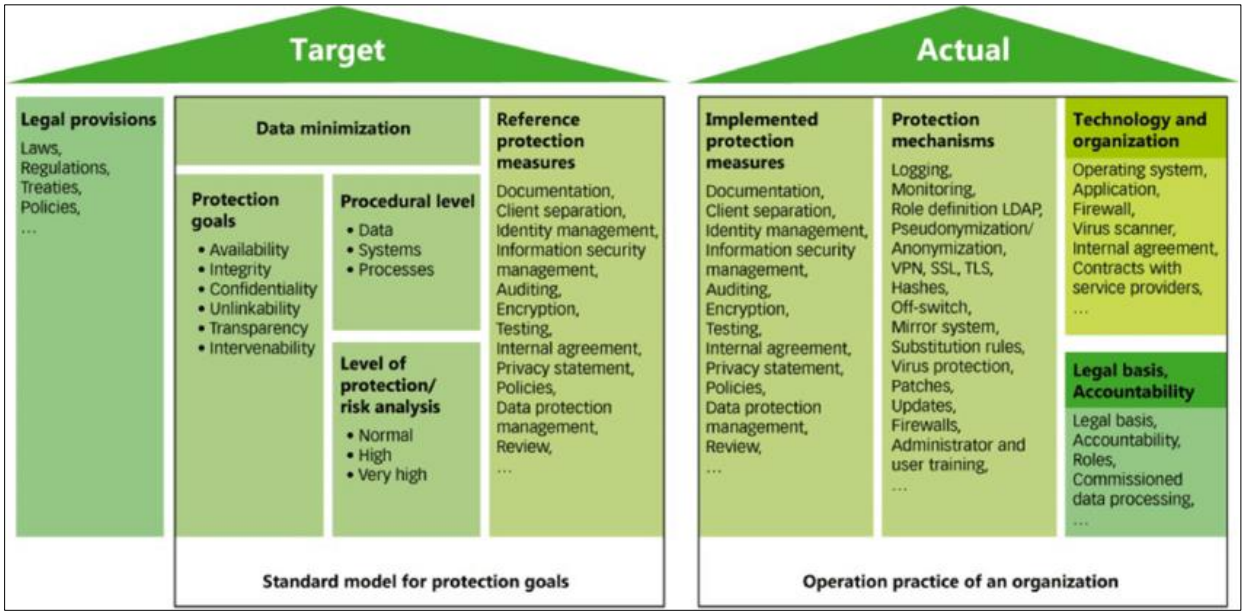

Figure 2 An Impact Assessment Procedure for Data Protection Under the European General Data Protection Regulation (Georgiadis and Poels, 2022)

To address the complexities of compliance and governance in a globalized digital economy, collaborative initiatives play a crucial role. Frameworks for international data transfer, such as the Privacy Shield Framework between the USA and the European Union, aim to facilitate secure data exchanges while ensuring compliance with respective regulations (Bradford *et al*., 2020). Similar initiatives can be developed to strengthen ties between the USA and African countries, fostering an environment where secure data transfers can occur without compromising local governance. Additionally, regional organizations in Africa, such as the African Union, are working to harmonize data protection regulations across member states. This effort seeks to create a unified framework that not only aligns with international standards but also promotes consistency in compliance practices. Collaborative partnerships between public and private sectors can further enhance these initiatives, as they provide the resources and expertise necessary to strengthen cloud governance across the continent. Moreover, knowledge-sharing platforms and workshops can facilitate dialogue between regulators, industry stakeholders, and international partners, promoting best practices and innovative solutions for compliance challenges. Such initiatives can bridge the gap between regulatory requirements and operational capabilities, empowering African nations to develop more effective governance frameworks that protect data privacy while encouraging technological advancement (Abbott and Snidal, 2021).

The comparative analysis of regulatory approaches to cloud governance and compliance reveals significant differences and similarities between the USA and African countries. While the USA exhibits a decentralized regulatory landscape, African nations are gradually building their frameworks in response to the increasing importance of data protection. The impact of international regulations, particularly those from the EU, underscores the need for African countries to adapt their local governance efforts to align with global standards (Coenen *et al*., 2021). Collaborative initiatives aimed at bridging compliance gaps are essential for fostering secure cloud environments and ensuring that both regions can navigate the complexities of a rapidly evolving digital landscape. By leveraging shared experiences and insights, stakeholders can work together to create comprehensive frameworks that promote data governance and compliance across borders (Pisa *et al*., 2020).

2.3. Recommendations for Enhanced Compliance and Governance in Cloud Computing

As cloud computing continues to evolve, the need for robust compliance and governance frameworks becomes increasingly critical (Abdulsalam and Hedabou, 2021). This presents recommendations aimed at enhancing compliance and governance in cloud computing for both the USA and Africa. These recommendations focus on fostering alignment between regulatory bodies, improving infrastructure, and ensuring that local contexts are considered in the development of compliance standards.

One of the primary challenges in the USA is the fragmented regulatory landscape, where federal and state-level compliance policies can differ significantly (Kanda *et al*., 2022). To enhance compliance, it is essential to promote alignment between these regulations. This can be achieved through the establishment of a federal framework that provides baseline compliance requirements while allowing states the flexibility to address specific local concerns. Collaborative efforts among state regulators, industry stakeholders, and federal agencies can facilitate dialogue and lead to the development of coherent policies that reduce confusion for organizations operating in multiple jurisdictions. This alignment will not only streamline compliance efforts but also foster a more secure and efficient cloud environment across the nation. With the increasing globalization of cloud services, fostering secure cross-border data transfer frameworks is vital. The USA should engage in diplomatic discussions and collaborations with African nations to develop agreements that facilitate the safe exchange of data across borders (Ayodele, 2021). Such frameworks can address concerns related to data privacy and security while ensuring compliance with local regulations. By promoting these frameworks, the USA can enhance its cloud operations and support African nations in their efforts to build strong data protection laws (Prinsloo and Kaliisa, 2022). This mutual cooperation will strengthen both regions' capacities to manage and secure cloud data while enabling innovation and economic growth.

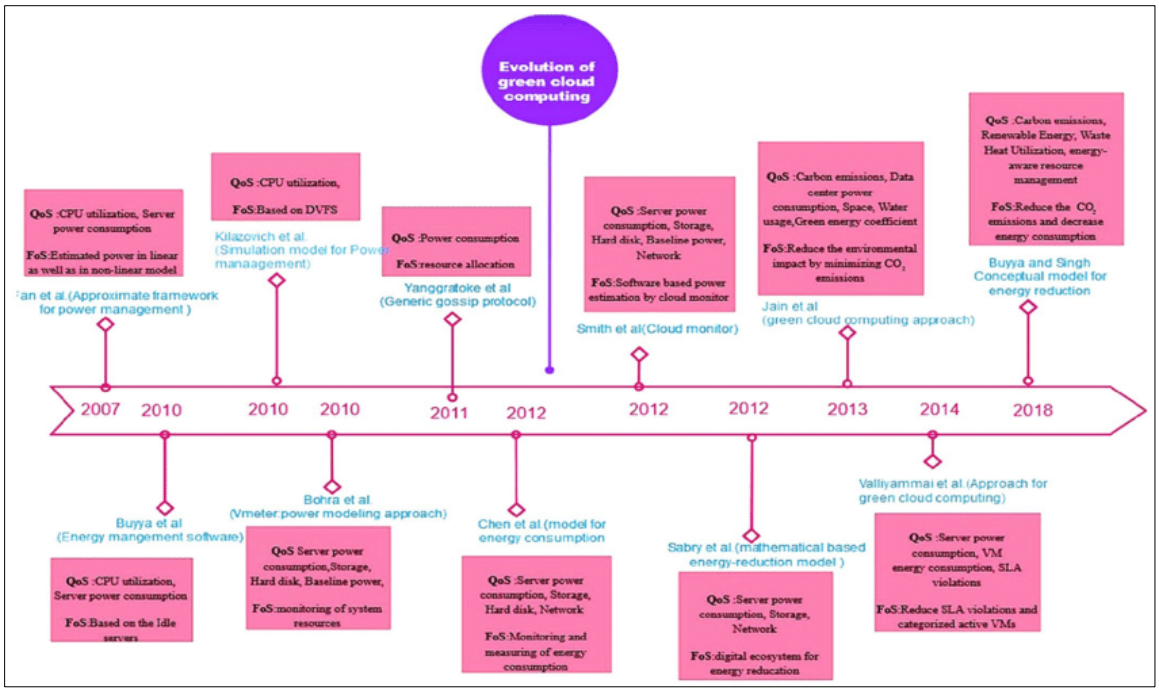

Figure 3 Green cloud computing's evolution (Bharany *et al*., 2022)

African nations face challenges related to regulatory diversity, which can hinder effective cloud governance and compliance. To address this issue, it is essential to build stronger pan-African regulations that establish unified compliance standards across the continent. The African Union can play a pivotal role in coordinating efforts to develop harmonized regulations that consider the unique socio-economic contexts of member states. By creating a consistent regulatory environment, African countries can enhance their attractiveness to foreign investments and facilitate smoother cloud operations for businesses operating across borders (Ismail and Masud, 2020). Public-private partnerships (PPPs) can significantly enhance cloud infrastructure and compliance capabilities in Africa as figure 2 showing the evolution of green cloud computing (Bharany *et al*., 2022). By fostering collaborations between government agencies and private sector players, African nations can leverage resources, expertise, and technology to build robust cloud infrastructures that meet compliance requirements. These partnerships can also drive innovation by enabling the sharing of best practices and developing tailored solutions to address local compliance challenges. Additionally, collaborative efforts can enhance capacity building and knowledge transfer, equipping local stakeholders with the necessary skills to navigate the complexities of cloud governance and compliance (Bozkurt *et al*., 2020; Rahman *et al*., 2021). Africa can benefit from leveraging international best practices in cloud compliance and governance while adapting them to local contexts. By studying successful frameworks and regulations from countries like the USA, African nations can identify relevant strategies that align with their unique circumstances. This approach will ensure that the compliance frameworks developed are both effective and culturally appropriate. Additionally, engaging with international organizations and regulatory bodies can provide valuable insights into emerging trends and challenges, allowing African countries to remain agile in their compliance efforts (Ogedengbe *et al*., 2023).

Enhancing compliance and governance in cloud computing requires a concerted effort from both the USA and African nations. By aligning federal and state-level policies in the USA and promoting cross-border data transfer frameworks, the USA can create a more coherent regulatory environment (Kuzio *et al*., 2022). Meanwhile, Africa can strengthen its compliance efforts by building pan-African regulations, fostering public-private partnerships, and leveraging international best practices. Together, these recommendations can lead to more effective cloud governance, ensuring that both regions can navigate the complexities of the digital landscape while promoting innovation and economic growth.

2.4. Future Directions in Compliance and Governance for AI and Cloud Computing

The rapid evolution of cloud computing and artificial intelligence (AI) technologies necessitates continuous adaptation of compliance and governance frameworks (Khadka, 22022). In both the USA and Africa, the regulatory landscape is undergoing significant transformations to address the unique challenges posed by these advanced technologies. This

explores the future directions of compliance and governance in the context of evolving regulations, the impact of emerging technologies, and the critical need for international collaboration.

As AI and cloud computing technologies advance, regulatory frameworks must evolve to ensure that they adequately address the complexities introduced by these innovations (Machireddy *et al*., 2021). In the USA, recent discussions around federal AI regulations indicate a move toward a more structured approach that balances innovation with accountability. Initiatives such as the National AI Initiative and the proposed AI Bill of Rights signal a shift toward establishing clear guidelines on ethical AI use, data privacy, and accountability measures (Lane, 2022). These efforts aim to create an environment conducive to innovation while safeguarding public interest. In Africa, the regulatory landscape is also changing as governments recognize the need to create a supportive framework for cloud computing and AI. The African Union is taking steps to unify data protection laws across member states, which is crucial for enhancing compliance and governance in a region characterized by regulatory diversity. Additionally, many African nations are in the process of developing national AI strategies that align with international best practices, ensuring that they are equipped to harness the benefits of these technologies responsibly (Sey and Mudongo, 2021; Wakunuma *et al*., 2022).

The rapid development of emerging technologies, such as blockchain, the Internet of Things (IoT), and advanced data analytics, will have a profound impact on compliance and governance practices. Blockchain technology, for instance, has the potential to enhance transparency and traceability in data management, making it easier to establish accountability and comply with regulatory requirements (Feng *et al*., 2020). Smart contracts could automate compliance processes, reducing the burden on organizations and increasing efficiency. Similarly, IoT devices generate vast amounts of data that raise new compliance challenges, particularly concerning data privacy and security. As organizations adopt IoT technologies, they must develop robust governance frameworks that account for the complexities of managing data across interconnected devices. This includes addressing issues related to data ownership, consent management, and cross-border data flow, ensuring that compliance efforts keep pace with technological advancements. Moreover, the integration of AI into compliance and governance practices can lead to more efficient monitoring and reporting mechanisms (Mökander *et al*., 2022). AI-driven analytics can help organizations identify compliance risks in real-time, allowing for proactive risk management and informed decision-making. However, organizations must also navigate the ethical implications of AI, ensuring that algorithms are transparent, fair, and accountable.

As the regulatory landscape evolves and technologies advance, the importance of international collaboration cannot be overstated (Schmitt, 2022). Establishing cohesive global standards for cloud computing and AI will be essential to facilitate secure and compliant cross-border data flows (Triolo *et al*., 2020). International collaboration can lead to the development of frameworks that address the challenges posed by varying national regulations, ensuring that organizations can operate seamlessly across jurisdictions. Initiatives such as the OECD's Recommendation on Artificial Intelligence and the Global Privacy Assembly's discussions on data protection highlight the growing recognition of the need for coordinated efforts among countries. These collaborative frameworks can help align regulatory approaches, share best practices, and address compliance gaps that may arise from differing national policies. In Africa, engaging with international partners can also provide valuable insights and resources to support the development of robust compliance frameworks. Leveraging expertise from more developed regulatory environments can empower African nations to craft effective regulations that are contextually relevant and adaptive to emerging technologies (Atiase *et al*., 2020; Peter, 2021).

The future of compliance and governance in AI and cloud computing is marked by an evolving regulatory landscape, the impact of emerging technologies, and the need for international collaboration. As both the USA and Africa navigate these changes, proactive measures must be taken to ensure that regulatory frameworks are not only responsive to technological advancements but also promote ethical practices and safeguard public interests. By fostering collaboration and sharing best practices, nations can work together to establish cohesive global standards that facilitate innovation while addressing the complexities of compliance and governance in an increasingly interconnected digital landscape (Haider and Ivanov, 2022; Dawodu *et al*., 2023).

3. Conclusion

In summary, compliance and governance challenges in cloud computing and AI present significant obstacles for both the USA and African nations. In the USA, regulatory frameworks are often fragmented, leading to inconsistencies in data protection and accountability. Conversely, African countries face hurdles related to developing comprehensive legal frameworks that can effectively manage the rapid growth of cloud and AI technologies, while also addressing issues of data sovereignty and infrastructure limitations. Both regions must navigate the complexities of cross-border data flows

and ensure that their regulatory approaches align with the global standards increasingly shaping the technology landscape.

The importance of proactive policy frameworks cannot be overstated. Such frameworks are essential for promoting responsible cloud and AI adoption by providing clear guidelines that protect consumer rights and foster innovation. By establishing robust compliance and governance structures, organizations can mitigate risks associated with data privacy and security while enhancing trust among users. Policymakers must engage stakeholders from various sectors, including technology, law, and ethics, to create a collaborative environment that supports sustainable development.

Building resilient and adaptable compliance systems is critical for supporting future growth in cloud computing and AI. As these technologies continue to evolve, regulatory frameworks must also be dynamic, able to accommodate emerging trends and challenges. Continuous dialogue between governments, industry leaders, and civil society is essential to ensure that compliance systems remain relevant and effective. By investing in adaptable governance structures, both the USA and African nations can harness the transformative potential of cloud computing and AI while safeguarding public interests and fostering innovation in an increasingly digital world.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abbott, K.W. and Snidal, D., 2021. Strengthening international regulation through transnational new governance: Overcoming the orchestration deficit. In *The spectrum of international institutions* (pp. 95-139). Routledge.

[2] Abdulsalam, Y.S. and Hedabou, M., 2021. Security and privacy in cloud computing: technical review. *Future Internet*, *14*(1), p.11.

[3] Abioye, T.E., Arogundade, O.T., Misra, S., Adesemowo, K. and Damaševičius, R., 2021. Cloud-based business process security risk management: a systematic review, taxonomy, and future directions. *Computers*, *10*(12), p.160.

[4] Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J. and Al-Fuqaha, A., 2022. Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. *Computer Science Review*, *43*, p.100452.

[5] Akter, S., Michael, K., Uddin, M.R., McCarthy, G. and Rahman, M., 2022. Transforming business using digital innovations: The application of AI, blockchain, cloud and data analytics. *Annals of Operations Research*, pp.1-33.

[6] Atiase, V.Y., Kolade, O. and Liedong, T.A., 2020. The emergence and strategy of tech hubs in Africa: Implications for knowledge production and value creation. *Technological Forecasting and Social Change*, *161*, p.120307.

[7] Ayodele, O., 2021. The digital transformation of diplomacy: Implications for the African Union and continental diplomacy. *South African Journal of International Affairs*, *28*(3), pp.379-401.

[8] Bernier, A., Molnár-Gábor, F. and Knoppers, B.M., 2022. The international data governance landscape. *Journal of Law and the Biosciences*, *9*(1), p.lsac005.

[9] Bharany, S., Sharma, S., Khalaf, O.I., Abdulsahib, G.M., Al Humaimeedy, A.S., Aldhyani, T.H., Maashi, M. and Alkahtani, H., 2022. A systematic survey on energy-efficient techniques in sustainable cloud computing. *Sustainability*, *14*(10), p.6256.

[10] Bognár, F. and Benedek, P., 2021. A Novel Risk Assessment Methodology—A Case Study of the PRISM Methodology in a Compliance Management Sensitive Sector. *Acta Polytechnica Hungarica*, *18*(7), pp.89-108.

[11] Bozkurt, A., Jung, I., Xiao, J., Vladimirschi, V., Schuwer, R., Egorov, G., Lambert, S., Al-Freih, M., Pete, J., Olcott Jr, D. and Rodes, V., 2020. A global outlook to the interruption of education due to COVID-19 pandemic: Navigating in a time of uncertainty and crisis. *Asian Journal of Distance Education*, *15*(1), pp.1-126.

[12] Bradford, L., Aboy, M. and Liddell, K., 2020. International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an 'adequate'level of protection. *Journal of Law and the Biosciences*, *7*(1), p.lsaa055.

[13] Carter, T.R., Benzie, M., Campiglio, E., Carlsen, H., Fronzek, S., Hildén, M., Reyer, C.P. and West, C., 2021. A conceptual framework for cross-border impacts of climate change. *Global Environmental Change*, *69*, p.102307.

[14] Chang, V., 2021. An ethical framework for big data and smart cities. *Technological Forecasting and Social Change*, *165*, p.120559.

[15] Chang, Y., Iakovou, E. and Shi, W., 2020. Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities. *International Journal of Production Research*, *58*(7), pp.2082-2099.

[16] Coenen, J., Bager, S., Meyfroidt, P., Newig, J. and Challies, E., 2021. Environmental governance of China's belt and road initiative. *Environmental Policy and Governance*, *31*(1), pp.3-17.

[17] Dawodu, S.O., Omotosho, A., Akindote, O.J., Adegbite, A.O. and Ewuga, S.K., 2023. Cybersecurity risk assessment in banking: methodologies and best practices. *Computer Science & IT Research Journal*, *4*(3), pp.220-243.

[18] de Almeida, P.G.R., dos Santos, C.D. and Farias, J.S., 2021. Artificial intelligence regulation: a framework for governance. *Ethics and Information Technology*, *23*(3), pp.505-525.

[19] Determann, L. and Tam, J., 2020. The California Privacy Rights Act of 2020: A broad and complex data processing regulation that applies to businesses worldwide. *Journal of Data Protection & Privacy*, *4*(1), pp.7-21.

[20] Dhanaraj, R.K., Jena, S.R., Yadav, A.K. and Rajasekar, V., 2021. Mastering Disruptive Technologies: Applications of Cloud Computing, IoT, Blockchain, Artificial Intelligence & Machine Learning Techniques. HP Hamilton Limited, UK.

[21] Ebrahim, S.H., Zhuo, J., Gozzer, E., Ahmed, Q.A., Imtiaz, R., Ahmed, Y., Doumbia, S., Rahman, N.M., Elachola, H., Wilder-Smith, A. and Memish, Z.A., 2020. All hands on deck: a synchronized whole-of-world approach for COVID-19 mitigation. *International Journal of Infectious Diseases*, *98*, pp.208-215.

[22] Feijóo, C., Kwon, Y., Bauer, J.M., Bohlin, E., Howell, B., Jain, R., Potgieter, P., Vu, K., Whalley, J. and Xia, J., 2020. Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy. *Telecommunications Policy*, *44*(6), p.101988.

[23] Feng, H., Wang, X., Duan, Y., Zhang, J. and Zhang, X., 2020. Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges. *Journal of cleaner production*, *260*, p.121031.

[24] Gaffley, M., Adams, R. and Shyllon, O., 2022. Artificial intelligence. African insight. A research summary of the ethical and human rights implications of AI in Africa.

[25] Georgiadis, G. and Poels, G., 2022. Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review. *Computer Law & Security Review*, *44*, p.105640.

[26] Haider, I. and Ivanov, A., 2022. Telecommunication Networks and Regional Connectivity: A Comparative Analysis. *Journal of Regional Connectivity and Development*, *1*(1), pp.44-53.

[27] Ismail, N.A. and Masud, M.M., 2020. Prospects and challenges in improving e-commerce connectivity in Malaysia. *E-commerce Connectivity in ASEAN*, *78*.

[28] Jelovac, D., Ljubojević, Č. and Ljubojević, L., 2022. HPC in business: the impact of corporate digital responsibility on building digital trust and responsible corporate digital governance. *Digital Policy, Regulation and Governance*, *24*(6), pp.485-497.

[29] Jernite, Y., Nguyen, H., Biderman, S., Rogers, A., Masoud, M., Danchev, V., Tan, S., Luccioni, A.S., Subramani, N., Johnson, I. and Dupont, G., 2022, June. Data governance in the age of large-scale data-driven language technology. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (pp. 2206-2222).

[30] Kanda, W., Zanatta, H., Magnusson, T., Hjelm, O. and Larsson, M., 2022. Policy coherence in a fragmented context: the case of biogas systems in Brazil. *Energy Research & Social Science*, *87*, p.102454.

[31] Kanungo, S., 2020. REVOLUTIONIZING DATA PROCESSING: ADVANCED CLOUD COMPUTING AND AI SYNERGY FOR IOT INNOVATION. *International Research Journal of Modernization in Engineering Technology and Science*, *2*, pp.1032-1040.

[32] Khadka, P., 2022. AI-Enhanced Cloud Computing: A Comprehensive Review of Techniques, Challenges, and Future Directions in Resource Management, Fault Tolerance, and Security Automation. *International Journal of Applied Machine Learning and Computational Intelligence*, *12*(11), pp.1-10.

[33] Kumar, B., 2022. Challenges and Solutions for Integrating AI with Multi-Cloud Architectures. *International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068*, *1*(1), pp.71-77.

[34] Kushwaha, N., Roguski, P. and Watson, B.W., 2020, May. Up in the air: Ensuring government data sovereignty in the cloud. In *2020 12th International Conference on Cyber Conflict (CyCon)* (Vol. 1300, pp. 43-61). IEEE.

[35] Kuzio, J., Ahmadi, M., Kim, K.C., Migaud, M.R., Wang, Y.F. and Bullock, J., 2022. Building better global data governance. *Data & Policy*, *4*, p.e25.

[36] Lane, L., 2022. Clarifying human rights standards through artificial intelligence initiatives. *International & Comparative Law Quarterly*, *71*(4), pp.915-944.

[37] Lescrauwaet, L., Wagner, H., Yoon, C. and Shukla, S., 2022. Adaptive legal frameworks and economic dynamics in emerging tech-nologies: Navigating the intersection for responsible innovation. *Law and Economics*, *16*(3), pp.202-220.

[38] Machireddy, J.R., Rachakatla, S.K. and Ravichandran, P., 2021. Leveraging AI and Machine Learning for Data-Driven Business Strategy: A Comprehensive Framework for Analytics Integration. *African Journal of Artificial Intelligence and Sustainable Development*, *1*(2), pp.12-150.

[39] Makulilo, A.B., 2021. The long arm of GDPR in Africa: reflection on data privacy law reform and practice in Mauritius. In *The Right to Privacy Revisited* (pp. 121-150). Routledge.

[40] Mökander, J., 2023. Auditing of AI: Legal, ethical and technical approaches. *Digital Society*, *2*(3), p.49.

[41] Mökander, J., Axente, M., Casolari, F. and Floridi, L., 2022. Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI regulation. *Minds and Machines*, *32*(2), pp.241-268.

[42] Mulgund, P., Mulgund, B.P., Sharman, R. and Singh, R., 2021. The implications of the California Consumer Privacy Act (CCPA) on healthcare organizations: Lessons learned from early compliance experiences. *Health Policy and Technology*, *10*(3), p.100543.

[43] Netshakhuma, N.S., 2022. Implementation of Protection of Personal Information Act No. 4 of 2013 of South Africa by Comparing Universities of Venda and Witwatersrand. In *Handbook of Research on the Global View of Open Access and Scholarly Communications* (pp. 148-164). IGI Global.

[44] Nyoni, P., Velempini, M. and Mavetera, N., 2020. Emerging internet technologies and the regulation of user privacy. *The African Journal of Information Systems*, *13*(1), p.1.

[45] Ogedengbe, D.E., James, O.O., Afolabi, J.O.A., Olatoye, F.O. and Eboigbe, E.O., 2023. Human resources in the era of the fourth industrial revolution (4ir): Strategies and innovations in the global south. *Engineering Science & Technology Journal*, *4*(5), pp.308-322.

[46] Oyeniran, C.O., Adewusi, A.O., Adeleke, A.G., Akwawa, L.A. and Azubuko, C.F., 2022. Ethical AI: Addressing bias in machine learning models and software applications. *Computer Science & IT Research Journal*, *3*(3), pp.115-126.

[47] Peter, C., 2021. Social innovation for sustainable urban developmental transitions in Sub-Saharan Africa: Leveraging economic ecosystems and the entrepreneurial state. *Sustainability*, *13*(13), p.7360.

[48] Pisa, M., Dixon, P., Ndulu, B. and Nwankwo, U., 2020. Governing data for development: trends, challenges, and opportunities. *CGD Policy Paper*, *190*, pp.1-61.

[49] Preston, C., Dias, M.F., Peña, J., Pombo, M.L. and Porrás, A., 2020. Addressing the challenges of regulatory systems strengthening in small states. *BMJ Global Health*, *5*(2), p.e001912.

[50] Prinsloo, P. and Kaliisa, R., 2022. Data privacy on the African continent: Opportunities, challenges and implications for learning analytics. *British Journal of Educational Technology*, *53*(4), pp.894-913.

[51] Rahman, F., Putri, G., Wulandari, D., Pratama, D. and Permadi, E., 2021. Auditing in the Digital Era: Challenges and Opportunities for Auditor. *Golden Ratio of Auditing Research*, *1*(2), pp.86-98.

[52] Saveliev, A. and Zhurenkov, D., 2021. Artificial intelligence and social responsibility: the case of the artificial intelligence strategies in the United States, Russia, and China. *Kybernetes*, *50*(3), pp.656-675.

[53] Schmitt, L., 2022. Mapping global AI governance: a nascent regime in a fragmented landscape. *AI and Ethics*, *2*(2), pp.303-314.

[54] Sey, A. and Mudongo, O., 2021. Case studies on AI skills capacity building and AI in workforce development in Africa. *Research ICT Africa*.

[55] Shah, V. and Konda, S.R., 2022. Cloud Computing in Healthcare: Opportunities, Risks, and Compliance. *Revista Espanola de Documentacion Cientifica*, *16*(3), pp.50-71.

[56] Sharma, U., Bairagee, D., Singh, N. and Jain, N., 2022. Computational Cloud Infrastructure for Patient Care. In *Bioinformatics Tools and Big Data Analytics for Patient Care* (pp. 105-131). Chapman and Hall/CRC.

[57] Shibambu, A. and Marutha, N.S., 2022. A framework for management of digital records on the cloud in the public sector of South Africa. *Information Discovery and Delivery*, *50*(2), pp.165-175.

[58] Triolo, P., Allison, K., Brown, C. and Broderick, K., 2020. The digital silk road: expanding China's digital footprint. *Eurasia Group*, *8*, pp.1-13.

[59] Uddin, M.H., Ali, M.H. and Hassan, M.K., 2020. Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*, *22*(4), pp.239-309.

[60] Vatanparast, R., 2020. Data governance and the elasticity of sovereignty. *Brook. J. Int'l L.*, *46*, p.1.

[61] Wakunuma, K., Ogoh, G., Eke, D.O. and Akintoye, S., 2022, May. Responsible AI, SDGS, and AI governance in Africa. In *2022 IST-Africa Conference (IST-Africa)* (pp. 1-13). IEEE.