

Streamlining Compliance and Governance with AI in Cloud-based Programs

Drijesh Patel

Program Manager

Abstract

Cloud-based programs offer numerous advantages to businesses and governments, including cost reduction, scalability, and on-demand services. Software as a Service (SaaS) is a prominent cloud computing model, providing potential cost-savings and improved cost control. Cloud-based programs enable efficient resource provisioning, auto-scaling, and dynamic resource acquisition and release, leading to increased profitability and reduced reliance on on-site IT infrastructure. However, adopting cloud-based programs comes with challenges related to security and compliance.

This article explores the advantages and differences of cloud-based programs compared to traditional software. It highlights the benefits of using AI in cloud-based programs to improve governance and compliance by streamlining processes and automating tasks. AI can enhance energy efficiency in cloud-based programs and significantly contribute to cost savings. However, it also introduces potential security risks and the need for robust security solutions to protect data in cloud-based eHealth systems.

The article emphasizes best practices for ensuring security in cloud-based programs, such as role-based access, encryption, and data monitoring. It discusses the potential risks of using AI for security and the importance of developing governance practices specific to AI applications. Moreover, it explores the benefits of AI for compliance and governance in cloud-based programs, such as risk management, scalability, and improved efficiency. The article underscores the long-term benefits of using AI in compliance and governance, including the enhancement of corporate governance and expertise in AI risks over time.

In conclusion, cloud-based programs coupled with AI present opportunities to revolutionize various industries by providing cost-effective, scalable, and secure solutions for compliance and governance needs. However, adopting AI in these programs requires careful consideration of security measures and adherence to specific AI governance practices to ensure the responsible and beneficial deployment of AI technologies.

Keywords: AI in Compliance, Governance and Security, Cloud Computing

Overview of Cloud-based Programs

What are the advantages of using cloud-based programs?

Cloud computing presents many advantages to businesses and governments, such as its distributed nature, scalability, and on-demand services [1]. Cost reduction is also one of the major benefits of cloud

computing, as it helps to reduce servicing costs [2]. This is especially true when it comes to Software as a Service (SaaS), which presents a new service delivery model in which a service provider delivers electronic services over the web to many users on a pay-per-use or period basis [3]. SaaS could result in potential cost-savings and better cost control by outsourcing the local control, installation and development of software [3]. Cloud-based programs can help SaaS providers minimize their payments, as well as enable efficient resource provisioning [2]. Moreover, such programs allow for the leasing of both resources and software as services [2]. Auto-scaling is also a major advantage of cloud-based programs, as it allows the addition or removal of resources on the fly, ensuring that the software system can handle unexpected spikes in workload and provide an optimal user experience, leading to increased profit for the cloud application owner [2]. Additionally, cloud elasticity allows for the automatic acquisition and release of resources, so that users only pay for what they consume [2]. Cloud-based programs also enable scalability and flexibility for businesses, as well as reducing the need for on-site IT infrastructure and maintenance [4]. Furthermore, such programs allow for access to data and applications from anywhere with an internet connection, facilitating distributed manufacturing, and enabling integration of information exchange between companies [4].

How do cloud-based programs differ from traditional software?

Cloud-based programs differ significantly from traditional software in terms of management and delivery [5][6]. Cloud-based design and manufacturing (CBDM) is a new paradigm for product design and manufacturing [6]. It is a business model which incorporates the use of cloud computing to reduce costs and increase efficiency [5]. CBDM, which is also known as Cloud Manufacturing, is distinct from traditional paradigms such as web- and agent-based technologies [6]. DMCloud is a prototype system developed at Georgia Tech for CBDM [6]. It helps organizations to shift computing costs to operational expenses [6]. In addition, the fundamentals of CBDM are highlighted in the chapter [6]. Furthermore, cloud-based programs require different testing techniques, QoS standards, and requirements compared to traditional software [5]. Testing as a service (TaaS) is a new business opportunity, challenge, and demand in cloud-based programs [5]. TaaS introduces new underlying issues, challenges, and emergent needs compared to traditional software testing [5]. It has distinct features and requires different techniques compared to conventional software testing services [5]. Safety and reliability are important considerations for cloud computing environment due to the threat of DDoS attacks [7]. DDoS attacks target the resources of cloud computing services, decreasing their ability to provide optimal network infrastructure usage [7]. Thus, methodologies for preventing or stopping DDoS attacks are quite different in cloud computing compared to traditional networks [7]. Cloud computing environment requires practical defense mechanisms against different types of DDoS attacks [7].

What are the security challenges associated with cloud-based programs?

Security is another concern associated with cloud-based applications and programs [8]. The threat of data breaches, hacking, and misuse of information is a real concern [8]. Organizations often lack knowledge about the shared security responsibility in cloud migration, which can lead to poorly secured data [8]. Additionally, users and enterprises are reluctant to trust sensitive data to cloud environments, which has led to the development of private clouds as a response [9]. Data security is a critical issue in cloud-based applications [9], however, the text does not provide specific details about the security challenges associated with cloud-based programs [8]. In healthcare, there are security challenges associated with

cloud-based programs, such as the implementation of appropriate security architecture, and the lack of knowledge of the shared security responsibility [8]. The security of critical electronic health records (EHRs) is a challenge associated with cloud-based programs in healthcare [8]. Security challenges also arise due to APIs, which can be exposed, broken, or hacked [8]. To stay ahead of such threats, updating cloud-driven apps frequently is necessary [8]. Furthermore, user access to cloud-based apps needs to be protected with a complete balance of protection, and security transfer needs to be managed regularly [8]. Moreover, simple and effective authentication is necessary for secure user access to mobile apps, EMR, or e-health programs [8]. Unfortunately, there is no process or mechanism for attribute revocation in cloud-based programs, and security access control issues can arise [8]. To ensure better security, certificates need to be trusted and issued from a certified hosting platform [8]. All these security challenges associated with cloud-based programs highlight the need for appropriate security solutions to be developed and maintained to protect data security in cloud-based eHealth systems [8].

AI in Cloud-based Programs

How can AI be used to improve the governance and compliance of cloud-based programs?

AI is increasingly being utilized to improve the governance and compliance of cloud-based programs. AI technology has been used to facilitate tax compliance and monitor governmental policies [10]. Cloud-based e-governance has become a reality due to the availability of IT infrastructure and government advisors' perspectives [10]. AI can also be used to calculate taxes, detect tax evasion, and improve the compliance process [10]. It can lead to significant improvements in the control environment, as well as business process improvements [11]. AI developers are also utilizing structured access, which is an emerging paradigm for the safe deployment of AI in cloud-based programs [11][12]. This is most effective when implemented through cloud-based AI services, rather than disseminating AI software that runs locally on users' hardware [12]. This allows AI developers to control how the AI system is used, and protect against unauthorized modifications to the system's design [12]. AI-powered packaged analytics can also be used to gain better oversight over financial spend in cloud-based programs [13]. AI can detect patterns of noncompliance in cloud-based programs, as well as be used to disrupt noncompliance [13].

What are the benefits of using AI in cloud-based programs?

AI algorithms have been used to improve energy efficiency in cloud-based programs [14]. AI calculation service provided by a cloud service can increase energy efficiency by providing intelligent control [14]. This enables users to run AI programs in the cloud and control air conditioners remotely from home [14]. Not only can this reduce air conditioner costs and prices by increasing energy efficiency, but also allows users to alter the AI programs in the cloud any time for better control performance without altering the control hardware [14]. The proposed system in the test bed reduced the power consumption by up to 22.5% [14]. AI techniques can be integrated and reassembled to develop cloud-based AI for split-type air conditioners, resulting in an energy-saving ratio higher than 22.5% [14]. AI can be developed on cloud-based platforms with minimum hardware costs and lead to energy savings [14]. Economic incentives can also increase the adoption of technologies that improve AC energy efficiency [14]. The energy-saving effect of cloud-based AI is expected to increase with the use of VSDs, and fuzzy + PID and MPCs are methodologies that can result in higher energy-saving ratios compared to other techniques [14]. AI techniques like ANN, DMS, fuzzy, GA, MAS, ML, MPC, RBR, RNN, and SNN can be evaluated for their energy saving effects, and the use of AI can result in obtaining EER and CSPF [14]. AI can improve energy

efficiency of split-type air conditioners, and provide dynamic control responses [14]. The energy-saving effect of AI is proven through analyzing the relationship between compressor rotational speed and indoor temperature variation, and AI can save a similar amount of energy as mentioned in the literature [14]. Cloud-based AI has better control responses compared to PID control in simulated climate conditions for late spring [14], and the final stable control can reduce the indoor air temperature drop-down slope to zero [15]. AI-based improvements can achieve higher benefits at lower costs compared to previous hardware modifications [14], and effectively use an MPC to save energy [15]. Thus, using AI for indoor temperature control can result in a higher slope, indicating little energy used by the air conditioner, and the use of AI is critical in saving energy, as observed through control models [15]. It has been shown that AI can increase EER and CSPF [15], and can improve energy efficiency in cloud-based programs [14].

What are the potential risks associated with using AI in cloud-based programs?

While cloud-based programs offer convenience and cost-effectiveness, they come with certain risks that must be addressed. For instance, testing as a service (TaaS) can be a double-edged sword [16], as it accelerates the AI lifecycle and enables collaboration and reuse of AI components. However, it also raises the question of security, privacy, and trust [15]. Additionally, the cloud-based design and manufacturing-related software and services may raise the risk of data breaches. To address these risks, a combination of cloud-based and on-premises AI is used to manage the Learning Factory [17], which is a shared workspace where safety risks exist. Furthermore, the use of IoT-based cloud and AI-based applications in such environments can be an effective solution [18], as it provides solutions to problems such as data analysis and visualization of UAV collected data [19]. Moreover, cloud-based systems are increasingly being used to store data from tablets and laptops [20], which can be linked to cloud robotics artificial intelligence systems. In light of these potential risks, it is important to consider the use of accounting software features and the impact they have on financial errors, as well as the use of Internet-related technologies such as AI, big data, cloud, and blockchain [21]. All this is essential for identifying those at risk of “sight-threatening” diseases, such as obesity, and developing AI-based intervention programs [22].

Streamlining Compliance and Governance

What are some strategies for streamlining compliance and governance in cloud-based programs?

Implementing cloud-based solutions can be a great way to streamline compliance and governance. Cloud-based providers only need to make changes to legislation once, and those changes will be applicable to all customers, making it easier to keep up with regulations and policies [23]. This also frees up vendors to focus on innovating new functionality that can benefit customers, as they do not need to worry about making changes to comply with regulations with every new release [23]. Additionally, cloud-based solutions make it easier to keep track of compliance and governance, as the updates are made automatically for all users. This helps ensure that all customers are up to date with the latest changes and can remain compliant with policy and regulations. Furthermore, cloud-based solutions are more secure than on-premises solutions. Cloud solutions are managed and maintained by professionals, which helps to ensure that the system is secure and compliant with the latest regulations. This also helps to reduce the risk of data breaches and unauthorized access to customer data. By streamlining compliance and governance with cloud-based solutions, businesses are able to benefit from improved security, improved compliance, and improved customer service.

How can AI be used to automate compliance and governance tasks?

AI has penetrated into financial services and can be used to automate compliance and governance tasks. For instance, AI can be used to collect and correlate information on bank transfers and identify behavioural characteristics of financial crimes including money laundering, as well as extracting entities of interest from evidentiary documents [24]. AI can also screen known criminals and forecast the likelihood of money laundering, detect suspicious transactions and provide risk scores for such transactions and streamline KYC/CDD processes, reducing compliance costs [24]. Additionally, AI can be used to optimize capital on peer-to-peer (p2p) platforms, helping more firms to come to the market to offer services [24]. AI technology is not only used in financial services, but also in RegTech or SupTech solutions to detect, prevent and control financial crime [24]. However, effective data governance needs to be established to protect individual rights and societal safety while using AI for compliance and governance tasks [24]. More detailed rules need to be developed to certify good algorithms and good platforms to strengthen ex ante and increase ex post protection of individuals who use robo-advisers [24], as current governance practices have evolved from more traditional financial applications and modeling frameworks, and frequently involve complex review flows and rely heavily on manual steps [25]. Therefore, the proposed framework aims to enable potential solution opportunities through increased automation and the integration of monitoring, management, and mitigation capabilities, providing improved capabilities to manage model risk during deployment [25].

What are the benefits of automating compliance and governance tasks?

Automating compliance and governance tasks offers a number of potential benefits. As organizations increasingly rely on data and technology, the need for compliance and governance processes has become even more critical [26]. Automation of these processes can help organizations to efficiently comply with external regulations and internal governance policies by streamlining the collection of evidence and documentation [27]. Automation also allows for data reconciliation at the supply chain level [28]. Organizations can use automated processes to identify and mitigate risks [29]. The President's e-government task force identified four broad areas of transformation: customer service, policymaking, program administration, and compliance [30]. Automation can help to streamline and automate processes such as record-keeping, filing, tax payment, and auditing, reducing compliance and administration costs [31][32]. Blockchain technology can also be used to automate governance tasks, such as risk management and compliance [33]. In addition, automation can help to streamline the process of handling cases and ensure compliance with EU rules [34]. By automating compliance and governance tasks, organizations can benefit from improved data accuracy, increased efficiency, and cost savings.

Security Considerations in Cloud-based Programs

What are some best practices for ensuring security in cloud-based programs?

Cloud-based programs are convenient and efficient, but it is essential to ensure that security measures are in place to protect data. Cloud service providers must take responsibility for implementing the appropriate mechanisms to guarantee the safety and privacy of their clients' data [35]. They should secure the platform and network, and guarantee that the service offered is always available [35]. Additionally, they must be compliant with various certifications and third-party requirements [35]. The security measures that should be considered include role-based access, network security mechanisms, data encryption, digital signatures, and access monitoring [35]. Furthermore, they must ensure that the databases are secure, and deploy

authentication systems to prevent unauthorized access [35]. Privacy and confidentiality terms are also key for EHR security [35]. Additional security measures include network secure protocols to prevent external attacks, as well as data logging and monitoring tools to improve security [35]. Moreover, it is important to confirm that the provider operates in the country where the service will be offered [35]. Additionally, health care providers must be aware of security mechanisms before migrating EHRs to the Cloud, and build a relationship of trust with the Cloud service provider [35]. Lastly, patients must be kept informed about their data and how it is being managed [35]. All of these steps are necessary for best practices in ensuring security in cloud-based programs.

How can AI be used to improve security in cloud-based programs?

AI technology is an ideal tool for enhancing the security of cloud-based programs. AI-powered algorithms can be used to apply tree-based hashing to the authentication process, which makes it difficult for malicious actors to gain access [8]. AI can also be used to guarantee user privacy by displaying random action keys, which are only visible to the user, in secure data connections [8]. AI can also be used to analyze data and detect fraudulent attacks [8]. In addition, AI can be used to incorporate system design controls for each process [8], allowing administrators to keep closer tabs on suspicious activity within their networks. AI can also be used to identify and mitigate threats that may arise from external sources. AI-powered algorithms can be used to monitor the network for suspicious activities, such as unauthorized access or data breaches. For example, AI can be used to detect malicious code and malware. AI-powered algorithms can also be used to monitor the cloud environment for malicious activity, such as unauthorized access or data breaches. AI can also be used to detect potential threats and alert administrators to take corrective action. By incorporating AI into the security of cloud-based programs, administrators can feel more confident in the security of their networks.

What are the potential risks of using AI for security in cloud-based programs?

AI is increasingly being used in the security of cloud-based programs. [8] This is due to the range of benefits it can bring to data storage, collaborative Artificial Intelligence (AI) and machine learning applications. [36] In order to protect the data from unauthorized access, it is essential to implement suitable security measures. [37] This includes deploying security models, serverless architectures, and high-performance virtual machines to ensure that all components are secure at an acceptable level of risk. [38] In addition, it is important to identify potential IP addresses found in the Viewstate and V15, as well as potential path traversal risks and treat them using security Controls. [39] Such measures are necessary to protect against potential IoT attacks. [40] It is also important to monitor changes to software solutions on a regular basis in order to identify vulnerabilities and weaknesses. [41] Furthermore, the use of encryption is essential in order to protect the data and prevent privacy and security issues. [42] Finally, a cloud-based IoT platform permits customers and programs to use AI and machine intelligence to enhance horizontal drilling and increase security. [43]

Benefits of AI for Compliance and Governance

What are the advantages of using AI for compliance and governance in cloud-based programs?

Artificial Intelligence (AI) is a powerful mechanism for compliance and governance in cloud-based programs. AI can be used to construct a model for risk management and governance programs, to ensure compliance with normative standards [22]. The use of Big Data and AI can bring various benefits, such

as technical standards, compliance assurance, and data security and privacy [44]. Cloud-based storage and processing can be used to meet government privacy and other requirements [45]. AI can also be used for complying with government regulations such as customs, while providing scalability [46]. AI can help in minimizing the time and costs associated with approving a system for use by a federal government [37]. AI can also be used to augment the data governance structures that take advantage of cloud-based computing [47]. Moreover, AI can be used for the calculation of expected benefits and for shaping corporate practices to enable compliance [48]. AI can also be used as an added functionality to existing cloud-based services as well as to ensure compliance with new governance and compliance regulations [49]. Therefore, AI is a useful tool for cloud-based programs that can help in saving time and money, while ensuring compliance with the required regulations.

How does AI improve the efficiency of compliance and governance tasks?

AI is increasingly being used to improve the efficiency of compliance and governance tasks, particularly in terms of corporate social responsibility (CSR) [50]. In this regard, the European Union's Draft European AI Regulation (DEAR) is of particular importance. DEAR requires organizations engaging in "high-risk AI" to implement organization-level governance for data and quality management procedures and ongoing monitoring, including transparency and provision of information for users across the AI lifecycle [51]. In this way, DEAR provides the regulatory impetus needed for organizations to ascribe budget and costs for ethical implementation requirements [51]. However, there is a risk that DEAR could invoke a "tick-box" compliance culture, rather than espousing a digital ethics culture across the AI lifecycle and digital society [50]. Nonetheless, DEAR still offers a significant improvement for AI governance, affording organizations the opportunity to find and create risk management, governance, and oversight solutions provided they achieve conformity [50]. As such, the key to success is in embedding trust into practical ethical data and AI governance tools, as this will become a pivotal method of competitive advantage [51]. High-risk AI operators must also decide the method/technical solution to achieve compliance under DEAR guidance [51], and AI can incentivize reform in CSR governance for socially responsible investments (SRIs) [50].

What are the potential long-term benefits of using AI for compliance and governance?

In addition to safety and reliability, long-term benefits can be derived from using AI for compliance and governance. AI can be used to improve corporate governance by selecting goods and services that are in the public interest [52]. Furthermore, customers are sometimes willing to pay more for ethical standards in non-AI industries [52]. This shift towards private messaging platforms, such as Snapchat and WhatsApp, is an example of how users prioritize certain technology uses [52]. AI users may also be willing to pay more for products with higher ethical standards [52]. The use of AI in compliance and governance could result in rejecting certain uses and prioritizing others [52]. Building expertise in AI risks over time is a potential long-term benefit of using AI for compliance and governance [53]. Pre-existing corporate structures can build expertise in AI risks as the field of AI corporate governance matures, standards are published, and regulations enter into force [53]. AI governance functions can be built into pre-existing structures for compliance and risk management [53]. As AI technology advances, businesses may benefit from improved methods of compliance and governance.

References

1. Wong, J., Wang, X., Li, H., Chan, G. *A review of cloud-based bim technology in the construction sector.* (n.d.) Retrieved June 5, 2023, from espace.curtin.edu.au/handle/20.500.11937/50359
2. Jamshidi, P., Ahmad, A., Pahl, C. *Autonomic resource provisioning for cloud-based software.* (n.d.) Retrieved June 5, 2023, from dl.acm.org/doi/abs/10.1145/2593929.2593940
3. Janssen, M., Joha, A. (n.d.) Retrieved June 5, 2023, from aisel.aisnet.org/ecis2011/80/
4. Helo, P., Suorsa, M., Hao, Y., Anussornnitisarn, P. *Toward a cloud-based manufacturing execution system for distributed manufacturing.* (n.d.) Retrieved June 5, 2023, from www.sciencedirect.com/science/article/pii/S0166361514000311
5. Gao, J., Bai, X., Tsai, W., Uehara, T. *Testing as a Service (TaaS) on Clouds.* (n.d.) Retrieved June 5, 2023, from ieeexplore.ieee.org/abstract/document/6525524/
6. Wu, D., Rosen, D., Schaefer, D. *Cloud-Based Design and Manufacturing: Status and Promise.* (n.d.) Retrieved June 5, 2023, from link.springer.com/chapter/10.1007/978-3-319-07398-9_1
7. Darwish, M., Ouda, A., Capretz, L. *Cloud-based DDoS attacks and defenses.* (n.d.) Retrieved June 5, 2023, from ieeexplore.ieee.org/abstract/document/6636342/
8. Sivan, R., Zukarnain, Z. *Security and privacy in cloud-based e-health system.* (n.d.) Retrieved June 5, 2023, from www.mdpi.com/2073-8994/13/5/742
9. Fylaktopoulos, G., Goumas, G., Skolarikis, M. *An overview of platforms for cloud based development.* (n.d.) Retrieved June 5, 2023, from link.springer.com/article/10.1186/s40064-016-1688-5
10. Kumar, R., Kathuria, S., Malholtra, R. *Role of Cloud Computing in Goods and Services Tax(GST) and Future Application.* (n.d.) Retrieved June 5, 2023, from ieeexplore.ieee.org/abstract/document/10104597/
11. Role, B., Need, B., Monitoring, S., Industry, B. *Harnessing Artificial Intelligence to Deliver Real-Time Intelligence.* (n.d.) Retrieved June 5, 2023, from www.oversight.com
12. Moll, J., Yigitbasioglu, O. *The role of internet-related technologies in shaping the work of accountants: New directions for accounting research.* (n.d.) Retrieved June 5, 2023, from www.sciencedirect.com/science/article/pii/S0890838919300459
13. Shevlane, T. *Computer Science > Artificial Intelligence.* (n.d.) Retrieved June 5, 2023, from arxiv.org/abs/2201.05159
14. Lee, D., Tsai, F. *Energies | Free Full-Text | Air Conditioning Energy Saving from Cloud-Based Artificial Intelligence: Case Study of a Split-Type Air Conditioner.* (n.d.) Retrieved June 5, 2023, from www.mdpi.com/694168
15. Wu, D., Terpenney, J., Schaefer, D. *Digital design and manufacturing on the cloud: A review of software and services—RETRACTED.* (n.d.) Retrieved June 5, 2023, from www.cambridge.org
16. Hummer, W., Muthusamy, V., Rausch, T. *Modelops: Cloud-based lifecycle management for reliable and trusted ai.* (n.d.) Retrieved June 5, 2023, from ieeexplore.ieee.org/abstract/document/8790192/
17. Balakreshnan, B., Richards, G., Nanda, G., Mao, H. *PPE compliance detection using artificial intelligence in learning factories.* (n.d.) Retrieved June 5, 2023, from www.sciencedirect.com/science/article/pii/S2351978920310556
18. Junaid, M., Shaikh, A., Hassan, M., Alghamdi, A., Rajab, K. *Smart agriculture cloud using AI based techniques.* (n.d.) Retrieved June 5, 2023, from www.mdpi.com/1235728
19. Ampatzidis, Y., Partel, V., Costa, L. *[HTML][HTML] Agroviz: Cloud-based application to process, analyze and visualize UAV-collected data for precision agriculture applications utilizing artificial*

- intelligence*. (n.d.) Retrieved June 5, 2023, from www.sciencedirect.com/science/article/pii/S0168169920304695
20. Bogue, R. *Cloud robotics: a review of technologies, developments and applications*. (n.d.) Retrieved June 5, 2023, from www.emerald.com
21. Ionescu, L. *Big data, blockchain, and artificial intelligence in cloud-based accounting information systems*. (n.d.) Retrieved June 5, 2023, from www.ceeol.com/search/article-detail?id=816594
22. Marshall, T., Lambert, S. *Cloud-based intelligent accounting applications: accounting task automation using IBM watson cognitive computing*. (n.d.) Retrieved June 5, 2023, from publications.aaahq.org/jeta/article-abstract/15/1/199/9251
23. Woodward, D. *How businesses can find the streamlined path to delivering software updates*. (n.d.) Retrieved June 5, 2023, from www.emerald.com
24. Lee, J. *Access to Finance for Artificial Intelligence Regulation in the Financial Services Industry*. (n.d.) Retrieved June 5, 2023, from link.springer.com/article/10.1007/s40804-020-00200-0
25. Kurshan, E., Shen, H., Chen, J. *Towards self-regulating AI: challenges and opportunities of AI model governance in financial services*. (n.d.) Retrieved June 5, 2023, from dl.acm.org/doi/abs/10.1145/3383455.3422564
26. Miasayedava, L., McBride, K., Tuhtan, J. *Automated environmental compliance monitoring of rivers with IoT and open government data*. (n.d.) Retrieved June 5, 2023, from www.sciencedirect.com/science/article/pii/S0301479721023458
27. Panian, Z. *[PDF][PDF] Some practical experiences in data governance*. (n.d.) Retrieved June 5, 2023, from citeseerx.ist.psu.edu
28. Bharosa, N., Janssen, M., van Wijk, R., de Winne, N. *Tapping into existing information flows: The transformation to compliance by design in business-to-government information exchange*. (n.d.) Retrieved June 5, 2023, from www.sciencedirect.com/science/article/pii/S0740624X12001475
29. Cachalia, M. *[BOOK][B] The Use of Blockchain Technology to Improve Transfer-Pricing Compliance and Administration in South Africa*. (n.d.) Retrieved June 5, 2023, from search.proquest.com
30. Evans, D., Yen, D. *E-government: An analysis for implementation: Framework for understanding cultural and social impact*. (n.d.) Retrieved June 5, 2023, from www.sciencedirect.com/science/article/pii/S0740624X05000547
31. Dzurandin, A., Mălăescu, I. *The current state and future direction of IT audit: Challenges and opportunities*. (n.d.) Retrieved June 5, 2023, from publications.aaahq.org/jis/article-abstract/30/1/7/1103
32. Kakebayashi, M. *The Potential of Central Bank Digital Currency for Transforming Public Finance: A Focus on VAT Systems*. (n.d.) Retrieved June 5, 2023, from papers.ssrn.com/sol3/papers.cfm?abstract_id=4449562
33. Kumari, A., Tanwar, S., Tyagi, S., Kumar, N. *Verification and validation techniques for streaming big data analytics in internet of things environment*. (n.d.) Retrieved June 5, 2023, from ietresearch.onlinelibrary.wiley.com
34. Tallberg, J. *[BOOK][B] European governance and supranational institutions: making states comply*. (n.d.) Retrieved June 5, 2023, from books.google.com

35. JPC Rodrigues, J., de la Torre, I., Fernández, G. *Journal of Medical Internet Research - Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems*. (n.d.) Retrieved June 5, 2023, from www.jmir.org/2013/8/e186/
36. Gaurav, A., Psannis, K., Peraković, D. *Security of cloud-based medical internet of things (miots): A survey*. (n.d.) Retrieved June 5, 2023, from www.igi-global.com
37. Robertson, J., Fossaceca, J. *A cloud-based computing framework for artificial intelligence innovation in support of multidomain operations*. (n.d.) Retrieved June 5, 2023, from ieeexplore.ieee.org/document/9497678/
38. Mishra, S., Sharma, S., Alowaidi, M. *RETRACTED ARTICLE: Analysis of security issues of cloud-based web applications*. (n.d.) Retrieved June 5, 2023, from link.springer.com/article/10.1007/s12652-020-02370-8
39. Ahmad, W., Rasool, A., Javed, A., Baker, T., Jalil, Z. *[HTML][HTML] Cyber security in iot-based cloud computing: A comprehensive survey*. (n.d.) Retrieved June 5, 2023, from www.mdpi.com/article/10.3390/electronics11010016
40. Butpheng, C., Yeh, K., Xiong, H. *[HTML][HTML] Security and privacy in IoT-cloud-based e-health systems—A comprehensive review*. (n.d.) Retrieved June 5, 2023, from www.mdpi.com/772394
41. Vijayakumar, K., Arun, C. *Automated risk identification using NLP in cloud based development environments*. (n.d.) Retrieved June 5, 2023, from link.springer.com/article/10.1007/s12652-017-0503-7
42. Alam, T. *Cloud-based IoT applications and their roles in smart cities*. (n.d.) Retrieved June 5, 2023, from www.mdpi.com/1275770
43. Lian, J. *Critical factors for cloud based e-invoice service adoption in Taiwan: An empirical study*. (n.d.) Retrieved June 5, 2023, from www.sciencedirect.com/science/article/pii/S0268401214001042
44. Al Batayneh, R., Taleb, N., Said, R. *IT governance framework and smart services integration for future development of Dubai infrastructure utilizing AI and big data, its reflection on the citizens standard of* (n.d.) Retrieved June 5, 2023, from link.springer.com/chapter/10.1007/978-3-030-76346-6_22
45. Atieh, A. *The next generation cloud technologies: a review on distributed cloud, fog and edge computing and their opportunities and challenges*. (n.d.) Retrieved June 5, 2023, from researchberg.com/index.php/rrst/article/view/18
46. Hartley, J., Sawaya, W., Dobrzykowski, D. *Exploring blockchain adoption intentions in the supply chain: Perspectives from innovation diffusion and institutional theory*. (n.d.) Retrieved June 5, 2023, from www.emerald.com
47. Ngiam, K., Khor, W. *Big data and machine learning algorithms for health-care delivery*. (n.d.) Retrieved June 5, 2023, from www.sciencedirect.com/science/article/pii/S1470204519301494
48. Renda, A. *[BOOK][B] Artificial Intelligence. Ethics, governance and policy challenges*. (n.d.) Retrieved June 5, 2023, from www.ceeol.com/search/book-detail?id=829907
49. Treleaven, P., Barnett, J., Knight, A., Serrano, W. *Real estate data marketplace*. (n.d.) Retrieved June 5, 2023, from link.springer.com/article/10.1007/s43681-021-00053-4
50. Elliott, K., Price, R., Shaw, P., Spiliotopoulos, T., Ng, M. *Towards an Equitable Digital Society: Artificial Intelligence (AI) and Corporate Digital Responsibility (CDR)*. (n.d.) Retrieved June 5, 2023, from link.springer.com/article/10.1007/s12115-021-00594-8

51. Filgueiras, F. *New Pythias of public administration: ambiguity and choice in AI systems as challenges for governance*. (n.d.) Retrieved June 5, 2023, from link.springer.com/article/10.1007/s00146-021-01201-4
52. Cihon, P., Schuett, J., Baum, S. *Information | Free Full-Text | Corporate Governance of Artificial Intelligence in the Public Interest*. (n.d.) Retrieved June 5, 2023, from www.mdpi.com/2078-2489/12/7/275
53. Ulnicane, I., Knight, W., Leach, T., Stahl, B. *Framing governance for a contested emerging technology: insights from AI policy | Policy and Society | Oxford Academic*. (n.d.) Retrieved June 5, 2023, from academic.oup.com