Estudiante Law Journal

Volume 7 Number 3, October, 2025: Pp 634-646
Faculty of Law, Universitas Negeri Gorontalo, City of Gorontalo, Indonesia
https://ejurnal.ung.ac.id/index.php/eslaw/index

Cloud Computing: A Threat or a Boon for Government Administration in the Digital Age?

Chami Yassine

Abu Dhabi University, Uni Emirat Arab

Email: prof.yassine@yahoo.com

Abstract: The implementation of cloud computing in government administration in the digital era presents both opportunities and challenges. This technology offers a range of benefits, including enhanced operational efficiency, cost savings, improved inter-agency collaboration, and the provision of public services in a faster and more transparent manner. Cloud computing enables centralized data management and real-time access to information, thereby supporting digital government (e-government) initiatives. However, its application also introduces risks related to data security and the privacy of highly sensitive information, such as citizens' personal data and critical information pertaining to government policies. Dependence on third-party cloud service providers exacerbates the threat to data sovereignty and increases the risk of unauthorized access. This study aims to explore the benefits and challenges faced by governments in implementing cloud computing and to identify mitigation measures that can be adopted to ensure robust data protection. The methodology employed in this study is normative, involving an analysis based on literature, legal regulations, and policies related to cloud computing and data protection in the public sector. The study examines the regulations, policies, and best practices implemented by several countries in managing government data stored in the cloud. The findings reveal that although cloud computing offers efficiency and ease in data management, challenges related to data security, privacy, and dependence on cloud service providers must be addressed with clear policies and stringent security systems. With appropriate policy implementation, cloud computing can be a boon for government administration; however, if not managed carefully, it may pose a threat to public data security.

Keywords : Cloud Computing; Government Administration; Data Security

How to cite (Chicago Style) :

Chami Yassine . "Cloud Computing: A Threat or a Boon for Government Administration in the Digital Age?". *Estudiante Law Journal*, 7 (3) (October, 2025): 634-646. https://doi.org/10.33756/eslaj.v7i3.31089

1. Introduction

In this rapidly evolving digital era, information and communication technology (ICT) has permeated nearly every aspect of life from the business sector to government. One technology that has become increasingly popular and widely adopted across various sectors, including the public sector, is cloud computing. Cloud computing offers numerous advantages in terms of efficiency, flexibility, and lower costs in managing IT infrastructure. For government administration, the implementation of cloud computing opens up significant opportunities to enhance the quality of public services, transparency, and data management efficiency. However, behind the ease and benefits it offers lie several challenges and potential threats that must be carefully considered, particularly with regard to security, data privacy, and reliance on third-party service providers.[1] In this context, the question arises: Is cloud computing a threat or rather a boon for government administration in the digital age?

The implementation of cloud computing in government has the potential to significantly transform the way data and information are managed. In the past, many government agencies were hampered by expensive and complex technological infrastructures. However, with cloud computing, governments can access centralized computing resources available on the Internet without the need to build and maintain their own data centers. This technology offers high flexibility, as services such as data storage, software applications, and data processing can be accessed on demand. Such flexibility is undoubtedly advantageous for government administration, which increasingly faces demands for prompt, transparent, and accountable public service.

One of the primary advantages of cloud computing is its ability to reduce operational costs. By eliminating the need to invest in hardware infrastructure, software, and data center maintenance, governments can reallocate funds to other, higher-priority needs. For example, budgets previously used to purchase servers and hire IT staff for maintenance can instead be directed toward improving the quality of public services or developing more user-friendly applications for the community. Furthermore, cloud computing allows government agencies easier access to centralized data in real time, which supports more effective collaboration among various departments and stakeholders.[2]

Cloud computing also supports the concept of digital government (e-government), wherein administrative processes can be conducted online more efficiently and with a

[1] Dwina Satrinia, Syifa Nurgaida Yutia, and Iik Muhamad Malik Matin, "Analisis Keamanan Dan Kenyamanan Pada Cloud Computing," *Journal of Informatics and Communication Technology (JICT)* 4, no. 1 (July 20, 2022): 85–91, https://doi.org/10.52661/j_ict.v4i1.111.

[2] Mulyawa Safwandy Nugraha and Hendi Rochimat, "Efektivitas Penerapan Sistem Informasi Manajemen Pendidikan Berbasis Cloud Dalam Meningkatkan Efisiensi Administrasi Sekolah Menengah," *Jurnal Global Ilmiah* 2, no. 4 (January 28, 2025), https://doi.org/10.55324/jgi.v2i4.175.

higher degree of transparency. For instance, through cloud-based systems, citizens can easily access information on public services, submit document requests digitally, and monitor the status of their applications. This undoubtedly accelerates bureaucratic processes that have long been perceived as slow and inefficient. Additionally, cloud computing facilitates the use of big data and analytics, enabling data gathered from various government sectors to be analyzed in order to formulate more targeted, evidence-based policies.

Despite the many benefits offered by cloud computing, it is undeniable that there are potential threats that governments must consider, particularly regarding security and data privacy issues. One of the primary concerns in implementing cloud computing is the dependency on cloud service providers. In many cases, governments opt to use cloud services provided by large corporations, meaning that highly sensitive data may be stored overseas or managed by third parties whose privacy policies differ from those of the state. This situation opens up the possibility of data misuse by irresponsible parties or even foreign governments, thereby posing risks to national security and the confidentiality of public information.[3]

In addition, cyberattacks that could compromise the security of government data represent a risk that must be guarded against. Although cloud service providers generally employ sophisticated security systems, threats to these systems persist. Hacking or Distributed Denial of Service (DDoS) attacks can disrupt public services and even result in the theft of sensitive government data. Therefore, it is imperative for governments to select trustworthy cloud service providers that adhere to high security standards and to ensure that privacy and data protection policies comply with the relevant national regulations.

Beyond security concerns, the implementation of cloud computing in the public sector also raises challenges related to regulations and policies. In some countries, there is concern about the loss of control over government data stored in the cloud. Some argue that utilizing cloud services provided by foreign companies may undermine data sovereignty and national privacy. For example, a cloud service provider based in another country might be legally obliged to hand over data stored on its servers if requested by its own government, which could create issues regarding the protection of citizens' personal data.[4]

---

[3] Selvisah Pitriyani and Rayyan Firdaus, "Pengembangan Data Base Terdistribusi Untuk Aplikasi Cloud Computing," *Innovative: Journal Of Social Science Research* 4, no. 3 (June 25, 2024): 15905–17, https://doi.org/10.31004/innovative.v4i3.12437.

[4] Zulkarnaim Masyhur, Adhy Rizaldy, and Patmayanti Kartini, "Studi Literatur Keamanan Dan Privasi Data Sistem Cloud Computing Pada Platform Google Drive," *Journal Software, Hardware and Information Technology* 1, no. 2 (June 30, 2021): 31–38, https://doi.org/10.24252/shift.v1i2.15.

Furthermore, governments must ensure that the adoption of cloud computing does not exacerbate the digital divide within society. Although cloud computing facilitates easier access to public services, challenges arise if the community lacks adequate Internet access or the necessary skills to use this technology. Thus, it is important for governments to ensure inclusivity in the adoption of cloud technology so that all segments of society including those in remote areas can benefit from its implementation in governance.

In addressing these challenges, governments need to develop appropriate policies to mitigate the risks associated with cloud computing. One key measure is to establish clear regulations regarding the protection of personal data, including requirements for cloud service providers to adhere to stringent security and privacy standards. Governments should also enact regulations governing the use of cloud computing by government agencies, including limitations on data storage locations and restrictions on third-party access.[5]

Overall, the implementation of cloud computing in government administration in this digital era can either be a boon or a threat, depending on how governments utilize this technology and manage the associated risks. If implemented wisely and supported by clear policies and rigorous oversight, cloud computing can offer substantial benefits to both governments and society. However, if its risks are not taken seriously, potential threats to data security and privacy could undermine both the stability of governance and public trust. Therefore, it is crucial for governments to continuously educate themselves and the public about the benefits and risks of cloud computing, and to ensure that this technology is employed for the public good in a safe, transparent, and accountable manner.

2. Method

The research method used in this research is the normative method, in which researchers will analyze and examine the application of cloud computing in government administration based on applicable laws, policies, and norms. This research focuses on understanding the legal, ethical, and regulatory aspects related to the use of cloud computing by government agencies. The data collected are legal documents, regulations, and literature related to cloud technology, which are then analyzed to assess their suitability and potential impact on government policies. The results of the research are expected to provide recommendations for improving cloud computing policies and regulations in government.[6]

[5] Aprillia Sakinah et al., "Analisis Kerentanan: Memanfaatkan Kerentanan dan Pengaruh Keamanan Siber pada Cloud Computing," *Jurnal SITECH : Sistem Informasi dan Teknologi* 7, no. 2 (2024): 95–102, https://doi.org/10.24176/sitech.v7i2.13370.

[6] Zainuddin Ali, *Metode Penelitian Hukum* (Sinar Grafika, 2021).

3. Data Security and Privacy in Cloud Computing Implementation in Government

Amid a rapid digital transformation, information technology plays a crucial role in enhancing the performance of the public sector, notably through the implementation of cloud computing. Cloud computing enables the efficient storage and processing of data without the need to manage large-scale physical infrastructures, thereby allowing governments to handle data more effectively, transparently, and swiftly. However, despite the myriad benefits this technology offers, significant challenges remain particularly regarding the security and privacy of data managed through cloud systems. When highly sensitive data is managed outside the traditional government infrastructure, questions about who controls the data, how it is protected, and how it might be accessed or misused become exceedingly important.[7]

Governments bear a profound responsibility for protecting sensitive data related to their citizens. This data encompasses personal information, financial records, health details, and information pertaining to government policies that can affect large segments of the population. If such data falls into the wrong hands or is exposed as a result of a cyberattack, the consequences can severely undermine public trust in the government. Therefore, it is imperative that governments establish clear and stringent policies on personal data protection and ensure that any data stored in the cloud is secure from both external and internal threats. One of the most frequently cited concerns is the risk of cyberattacks. Although major cloud service providers generally offer robust security, the continually evolving nature of cyber threats remains a risk that must be carefully managed. A successful breach could expose sensitive data and compromise the integrity of the information stored in cloud systems.

Another significant concern is the dependence on cloud service providers. Many governments opt to use cloud services from large technology companies that may have servers distributed across multiple regions worldwide. Consequently, data stored in the cloud might reside on servers located outside the country and subject to foreign jurisdictions. In such cases, the data may be governed by legal frameworks that differ from those in the country where the data is intended to be protected, raising issues of data sovereignty and privacy. For example, if a nation requires access to sensitive data stored by a cloud provider, it might compel the company to hand over the requested data, thereby risking the confidentiality of the information and the privacy of its citizens while deepening dependence on foreign entities that may not adhere to national data protection standards.[8]

---

[7] Aditya Yoga Arisandy et al., "Adopsi Cloud Computing Dalam Perencanaan Dan Pengembangan Bisnis Usaha Kecil Menengah (UKM)," *Economics And Business Management Journal (EBMJ)* 3, no. 01 (April 4, 2024): 20–29.

[8] Doni El Rezen Purba, Albert Alfredo S, and Juniarta Simamora Simamora, "Penyimpanan Digital dan Dokumen Online Berbasis Teknologi Informasi untuk Mendukung Kegiatan Administrasi Pemerintahan

It is important to note, however, that despite this reliance on third parties, cloud computing can also offer advantages in terms of redundancy and data security. Data stored in the cloud is not confined to a single server or data center; rather, it is often distributed across multiple locations and safeguarded by layers of encryption and sophisticated security systems. This means that even if the physical servers are damaged or affected by a natural disaster, the data can still be recovered and remain secure. Moreover, cloud service providers typically maintain professional, round-the-clock security teams dedicated to detecting and preventing threats to their systems. In some cases, cloud infrastructure is even more secure than traditional data centers managed by government agencies, as many cloud providers employ cutting-edge technologies and rigorous security protocols.[9]

Nevertheless, reliance on cloud providers does not absolve governments of their responsibility for data security. Even though cloud providers may possess state-of-the-art security tools and systems, the ultimate responsibility lies with the government to ensure that stored and managed data complies with all applicable regulations and policies. Governments must therefore select reputable cloud service providers that adhere to security standards equivalent to those mandated by national policies and have a proven track record in preserving data privacy and integrity. One critical measure is to ensure that these providers meet clearly defined and detailed service requirements regarding security standards, data storage, and protection against potential breaches.[10]

Furthermore, the use of cloud computing necessitates strict data management policies, particularly concerning data access and control. In many government agencies, data is stored and accessed by various departments or entities, which can complicate data management and oversight since access to sensitive data must be restricted solely to authorized personnel. Employing multi-factor authentication systems and role-based access control is essential in this regard. By using multi-factor authentication, governments can ensure that only duly authorized users gain access to specific data. Additionally, real-time monitoring and reporting of data access activities must be implemented to detect any unauthorized access or suspicious behavior promptly.

Data security and privacy in cloud computing are also intrinsically linked to data recovery and business continuity. Although cloud data is stored on third-party servers,

---

Desa Baja Dolok Kecamatan Sipispis," *ULEAD : Jurnal E-Pengabdian*, July 21, 2021, 33–37, https://doi.org/10.54367/ulead.v1i1.1358.

[9] Wiradharma Sampurna Putra, "Penerapan Penyimpanan Protokol Notaris Dengan Metode Cloud Computing System," *Unes Journal of Swara Justisia* 8, no. 1 (April 17, 2024): 113–32, https://doi.org/10.31933/ujsj.v8i1.482.

[10] Sayuthi Sayuthi and M. Rizal Yahya, "Pengaruh Business Intelligence Dan Cloud Computing Terhadap Keamanan Sistem Informasi (studi Pada Bumn Di Provinsi Aceh)," *JURNAL ILMIAH MAHASISWA EKONOMI ISLAM* 5, no. 2 (December 31, 2023): 212–43, https://doi.org/10.24815/jimeki.v5i2.29266.

governments must ensure that it can be swiftly restored in the event of a disaster or system failure. Thus, it is vital for governments to develop a comprehensive disaster recovery plan that guarantees data remains accessible or can be recovered during emergencies. This requirement also extends to maintaining backup storage that is always available, ensuring that data is neither lost nor compromised in times of crisis.[11]

Continuous and rigorous oversight of both cloud service providers and the use of cloud technologies by government agencies is essential. Governments should conduct regular audits to ensure that data stored in the cloud is consistently well-protected and that all practices conform to established policies. Periodic assessments of security systems, data protection measures, and compliance with regulatory standards are crucial in preventing any breaches. Additionally, it is imperative that policies on personal data protection and data security are updated regularly in response to technological advancements and the growing potential for external threats.

Another challenge that warrants attention is the interoperability among various cloud platforms used by different government agencies. Many entities employ different cloud providers for diverse needs, whether for data storage, application processing, or other services, which creates challenges for data exchange between agencies using disparate systems. Therefore, establishing technical standards that ensure data across various cloud platforms can be accessed and exchanged both easily and securely is of utmost importance.[12]

In summary, while cloud computing offers substantial benefits in enhancing efficiency, transparency, and accessibility within government administration, issues related to data security and privacy remain primary challenges. Governments must ensure that data stored in the cloud is shielded from external threats and that citizens' privacy is rigorously protected. This objective can be achieved through stringent oversight, clear policy frameworks, and close collaboration with cloud service providers who adhere to high security standards. With the appropriate measures in place, cloud computing can deliver significant benefits to both government and society, yet ensuring data security and privacy must always remain a top priority in every technological implementation.[13]

---

[11] Jesline Arsjad, Sinta Dewi Rosadi, and Rika Ratna Permata, "Pengaturan dan Tanggung Jawab Penyedia Jasa Layanan Komputasi Awan (Cloud Computing) atas Penyimpanan Data Pribadi Pengguna dari Kebocoran Data Elektronik," *Jurnal Ilmu Hukum Kyadiren* 2, no. 1 (July 30, 2020): 97–106, https://doi.org/10.46924/jihk.v2i1.136.

[12] Zuhairlan Zainul and Nurul Habib Romadhan, "Cloud Storage Sebagai Pengganti Arsip Manual Dalam Penunjang Aktifitas Sehari-Hari," *Kohesi: Jurnal Sains Dan Teknologi* 1, no. 6 (October 18, 2023): 20–30, https://doi.org/10.3785/kjst.v1i6.405.

[13] Sopian Aji et al., "Pengembangan Sistem Informasi Anggaran Desa Berbasis Cloud Computing Untuk Meningkatkan Transparansi Dan Akuntabilitas Pengelolaan Keuangan Desa Bumiharja," *TEMATIK* 10, no. 2 (December 17, 2023): 258–63.

4. Cloud Computing as an Efficiency Solution for Government Administration in the Digital Era

The implementation of cloud computing in government administration represents a significant advancement with the potential to deliver substantial benefits in operational efficiency, transparency, and improved public services. In today's digital era where the demand for rapid and accurate data access is increasingly urgent cloud computing offers a highly relevant solution for governments to streamline administrative processes, reduce operational costs, and accelerate service delivery to the public. By leveraging cloud technology, governments can manage and store data more efficiently while providing services that are both transparent and responsive.[14]

One of the primary benefits of adopting cloud computing in the public sector is the ease of data management. Previously, many government agencies managed data through disparate systems scattered across various departments, often resulting in inefficiencies in maintenance, updates, and access. With cloud computing, data can be stored centrally on internet-connected cloud servers, enabling agencies to access information in real time and in a more organized manner. This streamlined data management not only boosts internal productivity but also minimizes the risk of errors arising from data duplication or loss due to human error or system failures.

Additionally, cloud computing supports the concept of digital government or e-government which emphasizes the use of information technology to enhance public service quality. By utilizing cloud services, various government applications that involve interaction with the public can be accessed more easily, irrespective of time or location. For instance, citizens can submit documents or service requests online through cloud-based platforms, eliminating the need to visit government offices in person. Moreover, data accumulated via cloud computing can be analyzed more readily, assisting governments in making evidence-based decisions that are more responsive to community needs.[15]

Another significant advantage of cloud computing is the reduction in operational costs. Governments, like many other organizations, often face budgetary challenges, particularly when it comes to procuring expensive IT infrastructure and maintaining data centers. Cloud computing eliminates the need to purchase and maintain costly physical servers, as well as the expenses associated with hardware and software upkeep. Instead, governments pay only for the services they use through flexible, cost-effective pay-as-

[14] PRATAMA SATRIYA, "Pemanfaatan Teknologi Sistem Komputasi Awan Dalam Perlindungan Data Pribadi Di Indonesia," Skripsi (UNIVERSITAS LAMPUNG: FAKULTAS HUKUM, August 4, 2023), https://digilib.unila.ac.id/75206/.

[15] Edy Rakhmat et al., "Pemanfaatan Aplikasi Owncloud Pada Sistem Keamanan Cloud Computing," *Jurnal Sistem Informasi Dan Informatika (Simika)* 4, no. 2 (August 25, 2021): 146–55, https://doi.org/10.47080/simika.v4i2.1454.

you-go or subscription models. Consequently, funds previously allocated to IT infrastructure can be redirected towards developing other public services such as improvements in education, healthcare, and other critical infrastructures that directly benefit the community.[16]

Cloud computing also enables improved collaboration among government agencies. In traditional systems, collaboration between departments or agencies was often hindered by data access issues stemming from isolated, unconnected systems. With cloud computing, data and applications used by various departments can be accessed seamlessly from a single platform, facilitating more effective and efficient cooperation. This capability is particularly important given the increasingly complex nature of governmental tasks that require cross-sector collaboration from ministries to local governments. For example, during disaster response or national health programs, inter-agency collaboration is crucial for consolidating information and formulating appropriate policies. Cloud computing allows the involved agencies to access information simultaneously and work together more swiftly in responding to urgent situations.[17]

The use of cloud computing also facilitates the implementation of transparency and accountability in government. A common public complaint is the lack of transparency in data management and public service delivery. With cloud computing, government-managed data can be easily accessed by the public, enabling citizens to monitor administrative processes and provide feedback. Moreover, cloud-based platforms make it possible to implement electronic reporting systems that allow citizens to file complaints or report issues more conveniently and to track the progress of their submissions in real time. This not only enhances transparency but also empowers governments to improve public service delivery by giving citizens a greater voice in the decision-making process.

An important aspect of using cloud computing in government is its ability to address scalability challenges. In the public sector, workloads can fluctuate due to various factors such as election cycles, the implementation of new policies, or crises that demand rapid responses. Cloud computing enables governments to scale their service capacity up or down as needed without making significant investments in infrastructure. This flexibility allows governments to adapt quickly to changing circumstances while continuing to provide optimal services to the public. For instance, during a natural disaster, a

[16] Tobi Haryadi, "Perlindungan Data Pribadi Dalam Cloud Computing: Perspektif Hukum," *Disiplin : Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda* 30, no. 4 (December 28, 2024): 163–70, https://doi.org/10.46839/disiplin.v30i4.141.

[17] Jesline Arsjad, Sinta Dewi Rosadi, and Rika Ratna Permata, "Cloud Computing Service Provider Arrangements and Responsibilities for Storage of User's Personal Data From Electronic Data Leaks," *Jurnal Ilmu Hukum Kyadiren* 2, no. 1 (2020): 97–106, https://doi.org/10.46924/jihk.v2i1.136.

government can rapidly increase the capacity of its cloud systems to manage a surge in data and service requests without disrupting other operations.[18]

Furthermore, cloud computing enhances mobility and flexibility for government employees. Often, government officials are required to work from various locations, including off-site assignments. With cloud computing, the necessary data and applications can be accessed from any internet-connected device, enabling employees to work from anywhere at any time. This increased flexibility is particularly beneficial in emergency situations or when officials need to perform tasks in the field, thereby boosting overall productivity.[19]

However, despite its many benefits, the implementation of cloud computing in government is not without challenges. One of the most significant concerns is data security and privacy. Governments must ensure that data stored in the cloud is well protected against hacking or unauthorized access, which could severely undermine public trust. Moreover, clear and stringent regulations regarding the protection of personal data must be enforced to prevent the misuse of sensitive information that could harm citizens. Thus, while cloud computing can enhance efficiency, appropriate security measures must be implemented to safeguard data integrity and privacy.

Governments must also ensure that the deployment of cloud computing does not exacerbate the digital divide. Although cloud computing can simplify access to public services, many regions still lack adequate internet infrastructure. Therefore, it is crucial that the adoption of this technology does not widen the gap between urban and rural areas or among socioeconomically disadvantaged groups. One viable solution is to improve internet access nationwide, ensuring that all segments of society can benefit from cloud computing.[20]

In summary, cloud computing offers an excellent solution for enhancing the operational efficiency of government, expediting public service delivery, and reducing operational costs. Moreover, it supports the development of a digital government that is more transparent, accountable, and responsive to public needs. With its ability to efficiently store and manage data, facilitate inter-agency collaboration, and provide faster, more accurate services, cloud computing can play a crucial role in modernizing government

[18] Erni Ermawati et al., "Pelatihan Manajemen Arsip Digital dengan Teknologi Cloud Computing Google Drive Pada Desa Karangtengah Cibadak Sukabumi," *Jurnal Abdimas Teknologi Informatika dan Komputer* 1, no. 2 (August 2, 2024): 110–17.

[19] Betharia Wahyu Rizdawaty and Hindayati Mustafidah, "Faktor-Faktor yang Mempengaruhi Adopsi Cloud oleh Instansi Pemerintah: Tinjauan Pustaka Sistematis," *Sainteks* 18, no. 2 (February 12, 2022): 95, https://doi.org/10.30595/sainteks.v18i2.10573.

[20] Jelita Ritonga, "Implementasi Cloud Computing Pada Sistem Informasi Manajemen Pelayanan Kantor Desa Ulumamis Situnggaling Berbasis Website" (skripsi, UIN Sumatera Utara Medan, 2024), http://repository.uinsu.ac.id/23841/.

administration.[21] However, to maximize these benefits, governments must implement appropriate policies to address challenges such as data security, privacy, and the digital divide. With careful and strategic planning, cloud computing can serve as a key driver in creating a more efficient and responsive government in the digital age.

5. Conclusion

The implementation of cloud computing in government administration offers numerous advantages, such as enhanced operational efficiency, transparency, and improved quality of public services. By managing data centrally, cloud computing facilitates easier access and collaboration among government agencies. This technology also supports digital governance, enabling citizens to access public services quickly and accurately. However, challenges related to data security and privacy must be addressed by ensuring that cloud service providers adhere to high standards. Overall, cloud computing can be an effective solution for modernizing government administration, provided that it is implemented with appropriate policies and maintains digital inclusivity.

References:

Aji, Sopian, Dany Pratmanto, Rousyati Rousyati, Melly Agustin, Tasya Desti Setiawan, Afida Nurul Yasmin, and Andri Miftahul Akhyar. "Pengembangan Sistem Informasi Anggaran Desa Berbasis Cloud Computing Untuk Meningkatkan Transparansi Dan Akuntabilitas Pengelolaan Keuangan Desa Bumiharja." *TEMATIK* 10, no. 2 (December 17, 2023): 258–63.

Ali, Zainuddin. *Metode Penelitian Hukum*. Sinar Grafika, 2021.

Arisandy, Aditya Yoga, Sherly Della Permatasari, Shoqibatul Izaroh, Rusdi Hidayat, and Maharani Ikaningtyas. "Adopsi Cloud Computing Dalam Perencanaan Dan Pengembangan Bisnis Usaha Kecil Menengah (UKM)." *Economics And Business Management Journal (EBMJ)* 3, no. 01 (April 4, 2024): 20–29.

Arsjad, Jesline, Sinta Dewi Rosadi, and Rika Ratna Permata. "Cloud Computing Service Provider Arrangements and Responsibilities for Storage of User's Personal Data From Electronic Data Leaks." *Jurnal Ilmu Hukum Kyadiren* 2, no. 1 (2020): 97–106. https://doi.org/10.46924/jihk.v2i1.136.

———. "Pengaturan dan Tanggung Jawab Penyedia Jasa Layanan Komputasi Awan (Cloud Computing) atas Penyimpanan Data Pribadi Pengguna dari Kebocoran Data Elektronik." *Jurnal Ilmu Hukum Kyadiren* 2, no. 1 (July 30, 2020): 97–106. https://doi.org/10.46924/jihk.v2i1.136.

Ermawati, Erni, Ramdhan Saepul Rohman, Renny Oktapiani, and Dasya Arief Firmansah. "Pelatihan Manajemen Arsip Digital dengan Teknologi Cloud Computing Google Drive Pada Desa Karangtengah Cibadak Sukabumi." *Jurnal Abdimas Teknologi Informatika dan Komputer* 1, no. 2 (August 2, 2024): 110–17.

[21] Haryadi, "Perlindungan Data Pribadi Dalam Cloud Computing."

Haryadi, Tobi. "Perlindungan Data Pribadi Dalam Cloud Computing: Perspektif Hukum." *Disiplin : Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda* 30, no. 4 (December 28, 2024): 163–70. https://doi.org/10.46839/disiplin.v30i4.141.

Masyhur, Zulkarnaim, Adhy Rizaldy, and Patmayanti Kartini. "Studi Literatur Keamanan Dan Privasi Data Sistem Cloud Computing Pada Platform Google Drive." *Journal Software, Hardware and Information Technology* 1, no. 2 (June 30, 2021): 31–38. https://doi.org/10.24252/shift.v1i2.15.

Nugraha, Mulyawa Safwandy, and Hendi Rochimat. "Efektivitas Penerapan Sistem Informasi Manajemen Pendidikan Berbasis Cloud Dalam Meningkatkan Efisiensi Administrasi Sekolah Menengah." *Jurnal Global Ilmiah* 2, no. 4 (January 28, 2025). https://doi.org/10.55324/jgi.v2i4.175.

Pitriyani, Selvisah, and Rayyan Firdaus. "Pengembangan Data Base Terdistribusi Untuk Aplikasi Cloud Computing." *Innovative: Journal Of Social Science Research* 4, no. 3 (June 25, 2024): 15905–17. https://doi.org/10.31004/innovative.v4i3.12437.

Purba, Doni El Rezen, Albert Alfredo S, and Juniarta Simamora Simamora. "Penyimpanan Digital dan Dokumen Online Berbasis Teknologi Informasi untuk Mendukung Kegiatan Administrasi Pemerintahan Desa Baja Dolok Kecamatan Sipispis." *ULEAD : Jurnal E-Pengabdian*, July 21, 2021, 33–37. https://doi.org/10.54367/ulead.v1i1.1358.

Putra, Wiradharma Sampurna. "Penerapan Penyimpanan Protokol Notaris Dengan Metode Cloud Computing System." *Unes Journal of Swara Justisia* 8, no. 1 (April 17, 2024): 113–32. https://doi.org/10.31933/ujsj.v8i1.482.

Rakhmat, Edy, Saleh Dwiyatno, Sulistiyon Sulistiyon, Agus Irawan, and Ferli Setiawan. "Pemanfaatan Aplikasi Owncloud Pada Sistem Keamanan Cloud Computing." *Jurnal Sistem Informasi Dan Informatika (Simika)* 4, no. 2 (August 25, 2021): 146–55. https://doi.org/10.47080/simika.v4i2.1454.

Ritonga, Jelita. "Implementasi Cloud Computing Pada Sistem Informasi Manajemen Pelayanan Kantor Desa Ulumamis Situnggaling Berbasis Website." Skripsi, UIN Sumatera Utara Medan, 2024. http://repository.uinsu.ac.id/23841/.

Rizdawaty, Betharia Wahyu, and Hindayati Mustafidah. "Faktor-Faktor yang Mempengaruhi Adopsi Cloud oleh Instansi Pemerintah: Tinjauan Pustaka Sistematis." *Sainteks* 18, no. 2 (February 12, 2022): 95. https://doi.org/10.30595/sainteks.v18i2.10573.

Sakinah, Aprillia, Sangkot Khofipah, Pesah Sifrah Tripena, Maria Anjelina Dewi Karoko, and Fauziyah Fauziyah. "Analisis Kerentanan: Memanfaatkan Kerentanan dan Pengaruh Keamanan Siber pada Cloud Computing." *Jurnal SITECH : Sistem Informasi dan Teknologi* 7, no. 2 (2024): 95–102. https://doi.org/10.24176/sitech.v7i2.13370.

Satrinia, Dwina, Syifa Nurgaida Yutia, and Iik Muhamad Malik Matin. "Analisis Keamanan Dan Kenyamanan Pada Cloud Computing." *Journal of Informatics and Communication Technology (JICT)* 4, no. 1 (July 20, 2022): 85–91. https://doi.org/10.52661/j_ict.v4i1.111.

SATRIYA, PRATAMA. “Pemanfaatan Teknologi Sistem Komputasi Awan Dalam Perlindungan Data Pribadi Di Indonesia.” Skripsi. UNIVERSITAS LAMPUNG: FAKULTAS HUKUM, August 4, 2023. https://digilib.unila.ac.id/75206/.

Sayuthi, Sayuthi, and M. Rizal Yahya. “Pengaruh Business Intelligence Dan Cloud Computing Terhadap Keamanan Sistem Informasi (studi Pada Bumn Di Provinsi Aceh).” *JURNAL ILMIAH MAHASISWA EKONOMI ISLAM* 5, no. 2 (December 31, 2023): 212–43. https://doi.org/10.24815/jimeki.v5i2.29266.

Zainul, Zuhairlan, and Nurul Habib Romadhan. “Cloud Storage Sebagai Pengganti Arsip Manual Dalam Penunjang Aktifitas Sehari-Hari.” *Kohesi: Jurnal Sains Dan Teknologi* 1, no. 6 (October 18, 2023): 20–30. https://doi.org/10.3785/kjst.v1i6.405.