

IMPROVING DATA SECURITY IN CLOUD REPOSITORY: FUTURE CHALLENGES IN ELECTRONIC RECORDS MANAGEMENT

Abstrak. Penggunaan penyimpanan berbasis *cloud* untuk penyimpanan arsip elektronik di satu sisi mampu meningkatkan transparansi penggunaan data, namun di sisi lain menimbulkan tantangan dalam mempertahankan keaslian, akurasi dan reliabilitas yang menjadi dasar kepercayaan pengguna terhadap data yang dikelola. Tulisan ini berfokus pada upaya untuk menetapkan kebijakan keamanan data yang dilakukan oleh organisasi sebagai bagian dari proses pemanfaatan, penyimpanan, dan pengelolaan data berbasis *cloud*. Tulisan ini bertujuan untuk dapat memberikan rekomendasi atau masukan untuk kebijakan di masa mendatang, terutama pada masalah keamanan dan kepercayaan pada *cloud* sebagai tempat penyimpanan data. Penelitian ini menggunakan metode tinjauan pustaka untuk mengembangkan pemikiran kritis tentang aspek keamanan data dalam sistem penyimpanan *cloud* dan menjelaskan masalah keamanan dan kepercayaan dari data yang disimpan di *cloud*. Artikel tentang topik keamanan data dalam sistem penyimpanan *cloud* digunakan sebagai literatur utama. Selain itu, *litmaps.co* digunakan untuk memetakan sebaran artikel terkait sebagai literatur pendukung. Hasil penelitian ini menunjukkan bahwa masalah pelanggaran data menempati urutan teratas dalam kaitannya dengan keamanan data yang disimpan di *cloud*, sehingga tantangan keamanan tidak terletak pada sistem atau penyedia *cloud*, tetapi pada penguasaan kebijakan dan teknologi. Oleh karena itu, peningkatan keamanan data di penyimpanan *cloud* dan pengelolaan data *cloud* dapat dilakukan melalui pemilihan jenis *cloud* yang tepat, membuat model arsitektur keamanan data sesuai dengan kemungkinan ancaman keamanan dan menerapkan prinsip-prinsip manajemen data seperti *respect des fonds* dan *provenance*. Pemerintah dapat berperan dalam meningkatkan keamanan data dengan memberikan kebijakan privasi dan pengelolaan data *cloud* serta memfasilitasi pengembangan teknologi *blockchain* untuk meningkatkan keamanan data.

Kata Kunci: Arsip elektronik; manajemen rekod; cloud repository; keamanan data

Abstract. The use of cloud-based storage for electronic archive on one hand can increase transparency of the use of data, but on the other hand it raises challenges in maintaining authenticity, accuracy, and reliability of the data, which is the basis of user trust in the managed data. This article focuses on the efforts to establish data security policies carried out by organizations as part of the process of utilizing, storing, and managing cloud-based data. This article also aims to provide recommendations for future policies, especially on security and trust issues in using cloud as data repository. Method used in this study is a literature review with aim to develop critical thinking on data security aspects in cloud storage systems and explain security and trust issues of data stored in the cloud. In addition, *litmaps.co* is used to map the distribution of related articles as supporting literature. The finding of this study shows that the problem of data breaches ranks at the top in relation to the security of data stored in the cloud, so the security challenge does not lie with the system or cloud provider, but in the mastery of policies and technology. Therefore, improving data security in cloud storage and cloud data management can be done by choosing the suitable type of cloud, modeling data security architecture according to possible security threats and applying data management principles such as *respect des fonds* and *provenance*. Governments can play a role in improving data security by providing privacy policies and cloud data management as well as facilitating the development of blockchain technology to improve data security.

Keywords: electronic records; records management; cloud repository; data security

Achmad Fachmi^{1*}, Wira Sakinatun Najahah², Adista Nurfitri³, Taufik Asmiyanto⁴, M. Hanif Inamullah⁵
¹²³⁴⁵Departemen Ilmu Perpustakaan dan Informasi, Fakultas Ilmu Pengetahuan Budaya, Universitas Indonesia
E-mail koresponden*: achmad.fachmi90@gmail.com

Diterima: 8 Mei 2026

Direvisi: 28 Mei 2026

Disetujui: 8 Juni 2026

PENDAHULUAN

The development of information technology is currently growing rapidly and massively so every human activity cannot be separated from the use of information technology. It has the effect of an information explosion with a digital volume created every second in a digital environment. Surely

this will have a significant influence on data management in organizations, especially data storage systems. Therefore, in today's digital era, records managers must be able to adapt information technology that can support organizational activities where business processes can run more effectively and efficiently, one of which is by using cloud computing.

Because cloud-based storage is considered capable of increasing efficiency and transparency in data management. Furthermore, this effort is also in line with the objectives of the e-government program, namely efficiency, and effectiveness (Lončarić & Stančić, 2017). This condition demands the need and transparency of the use of data information. In a sense, National Institute of Standards and Technology defines it as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” Jansen and Grance (in Duranti, (2012). They said that there are four cloud architecture models, namely private cloud, public cloud, community cloud, and hybrid cloud, each of which has advantages and risks that are appropriate to be analyzed in the context of trust requirements.

Therefore, openness and transparency in the use of data information are based on user trust. So, the choice of a cloud architecture model depends on the level of how important the data is stored and the needs of the user. In utilizing printed data, users place their trust in the creator of the data manager (Duranti & Rogers, 2012). Users can assess the data used from several aspects, such as attributes in the data or performance or data management. But in digital data, this is often difficult to do. However, it is important to maintain user confidence in the authenticity and accuracy of the data they hold.

Cloud-based storage media is capable of increasing the transparency of data usage, but has challenges in maintaining the authenticity, accuracy and reliability which are the nature of users' trust in the data. The Cloud Security Alliance (CSA) (2017) has identified 12 major issues related to cloud security. Based on the results of the CSA survey, the highest ranking in terms of severity is data breaches, followed by weak identity, credentials and privileges management. According to Gartner Inc., the security challenge lies not in the system or cloud provider, but in policy and technology mastery. Policies and mastery of technology depends on the user, in this case the organizations using the cloud and users who have access to the data. As explained by Panetta (2019), almost all cases occur due to user mistakes, not due to the failure of the cloud provider to manage and control to protect data. This fact shows that the trust in the managed data will be determined by the user of the cloud storage media.

In fact, Badan Siber dan Sandi Nasional (BSSN) says in addition to the many advantages, there are also security vulnerabilities in cloud-based storage systems. There are vulnerabilities in cloud-based storage systems: 1) Threats that come from external, from the data found it is said that this problem is a problem that is increasing rapidly; 2) Threats from superhumans; the problem that occurs is that the login is done from a different place but at the same time; 3) The problem of storage space, is closely related to digital forensic investigations for digital crimes, where the authorities sometimes have difficulty retrieving data because the cloud storage area is not located in Indonesia.

In addition, Vice President of Research at Gartner Inc, Jay Heiser, a cloud expert, said that by 2022 at least 95% of cloud security failures will be user errors (Panetta, 2019). Therefore, organizations need to self-evaluate and ask “are they using the cloud safely?” and no longer ask “is the cloud safe to use?”. Currently, cloud technology has an access restriction system and log history when accessing data content. These features were created to protect trust and data security. Even though it has been systemically restricted, as Gartner Inc. reported, data abuse ranks first out of 12 major cloud security problems. Users can exploit and abuse context in data without any protection from the organization. Therefore, organizations still need to pay attention to the process of creating metadata in data management when using the cloud.

In the article entitled ‘Dampak Kejahatan Siber Terhadap Teknologi Informasi dan

Pengendalian Internal' by Lana (2021) said that there were reports on the results of cyber security monitoring in 2002 in three sectors: the government sector; 2) Infrastruktur Informasi Kritis Nasional (IIKN) sector, which is any disturbance to the information infrastructure that can disrupt the lives of many people; 3) Ekonomi Digital (Ekodig) sector, which is a form of economic activity that utilizes information technology. So, it was found that there was an increase in cybercrime in Indonesia, considering that cybercrimes can occur by breaking through judicial, territorial, and cross-border boundaries.

Therefore in digital data management, data managers must actively capture and store data for as long as necessary for the organization's business purposes (Williams, 2006). The rapid change and growth of digital data makes misuse of data by users difficult to detect. To increase user trust in the authenticity of the data, data managers can also add information in the metadata that describes the history of changes and usage of the data. This article focuses on efforts to establish data security policies in organizations as part of the cloud-based data utilization, storage and management process. This article will provide recommendations or input for future policies, especially on security issues and trust in the cloud as a data storage system.

METODE

This article uses a literature review to develop critical thinking on the data security aspect of cloud storage systems. It is important to note that a literature review is a theoretical study, references, and other scientific literature related to the culture, values, and norms that develop in the social situation under study (Sugiyono, 2018). Thus, the data collection technique is done by reviewing books, notes, and other literature related to acquired research problems. Data analysis in this study were conducted using descriptive qualitative methods to broadly explain the behavior and attitudes of a number of individuals or groups of people, as well as to understand the meaning that comes from social problems (Creswell & Creswell, 2018). The descriptive analysis process is used to describe data security aspects in cloud storage systems. The primary sources of this research come from two main articles –*Trust in digital records: An increasing cloudy legal area* by Luciana Duranti (2012) and *The cloud: challenges and issues* by Julie McLeod (2017) related to data security aspects in cloud storage systems. Furthermore, apart from searching independently, we also used www.litmaps.co to map the distribution of articles related to cloud storage systems, as a secondary source in this research.

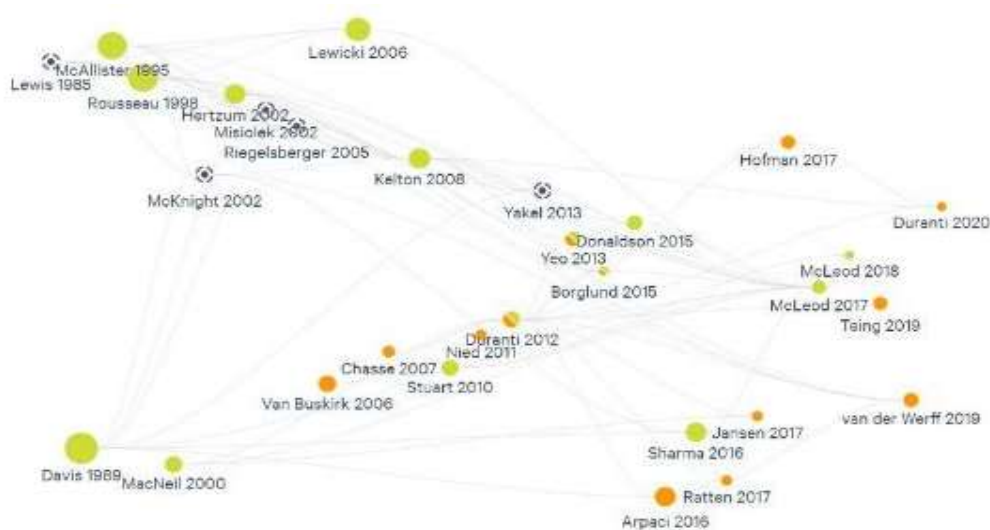


Figure 1. distribution map of articles related to cloud storage systems using www.litmaps.co

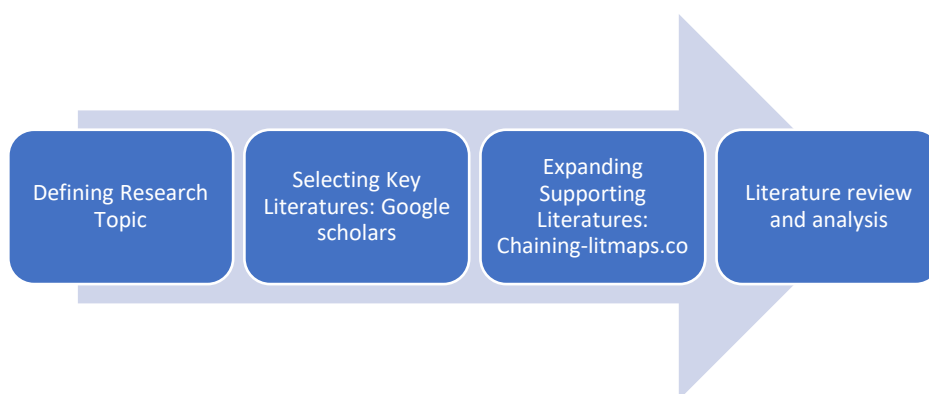


Figure 2. process diagram of literature review

HASIL DAN PEMBAHASAN

Between Traditional and Electronic Records and Data

The meaning of records is often limited to recorded information in printed form on paper and has a value for organizations or individuals. However, in fact, according to the Indonesia Archives Act No. 43 of 2009 the forms and media of recorded information as evidence of activities could be adjusted to the development of information and communication technology (Republik Indonesia, 2009). This distinction of understanding resulting a wide gap of meaning in the context of records and data. Essentially, all records are data. However, not all data are considered as a record. Especially nowadays, the emergence of digitally born records has added to the record ecosystem that has always been filled with traditional records for decades. Not to mention the records or archives in paper form which are undergoing a digitization process in order to preserve the content and provide quick access to the information stored in them. Records that have undergone a media transfer or digitization process are categorized as electronic records. Electronic records are information contained in media or electronic files that are created, received and managed by organizations or individuals as evidence of activities (Rifauddin, 2016). Electronic records or archives have been legally recognized as valid legal evidence from the issuance of Information and Electronic Transactions Act No. 11 of 2008. However, some institutions still feel the need to keep records in paper or printed form and keep the electronic copy of the records as “backup” files that can be utilized quickly using technology transmission.

Rapid development of technology allows the creation of records in the form of digital data. The data in digital form can be easily processed, managed and used for various purposes so that organizations can improve the efficiency and effectiveness of performance (Muhidin et al., 2016). This digital data can record the activities of the organization formally and legally. However, in practice, data management, both in paper and digital form, has not yet become a single entity in Indonesia. It is proven by the problem of managing and using personal data in the e-KTP (electronic Citizens’ ID Card) which is part of the private records of citizens. In some administrative processes such as making e-money, citizens are still asked to photocopy the e-KTP (Permana, 2021).

The Ministry of Home Affairs stated these kinds of problems can occur if the relevant institutions have not cooperated and coordinated with the Population and Civil Registry Office in providing services. The Department of Population and Civil Registration (Disdukcapil Kabupaten Bantul, 2013) in its official portal also stated that e-KTP cannot be photocopied because it may damage the chip inside and increase the risk of falsification of personal data. However, the two statements above cannot answer the problems that occur regarding the administrative process that requires a photocopy of the e-KTP. This problem is one of many other problems related to records and

data which indicates that there is no synchronization of understanding, implementation and policies regarding electronic records and data in Indonesia.

Different understanding of records in paper and digital form may have an impact on the principles of management, utilization and creation of rules including the use of supporting hardware and software. Therefore, data or electronic records developed in a digital environment will be related to the principle of origin, where electronic records will be closely related to the origin of the record. According to Zou (2019) “... archival principles have been developed with paper-based archival records; the provenance of electronic documents is different from the traditional way of managing provenance in paper records.” Hickerson (Zou, 2019) also stated that “...managing electronic records is considered one of the most important challenges for records in digital environments.” These challenges provide many changes to records management activities. Record users no longer have to rely on the physical presence of records managers to identify, review, and retrieve records. In fact, records do not have to be physically limited by the organizational structure and its materials no longer have to be physically limited to boxes or folders (Zhang, 2012).

Thus, it can be seen that the record representation process seems to have differences and the framework used is also different. This means that the rules in the representation of traditional records are not compatible nor suitable to be applied to electronic records and are used for online access. As said by Zhang (2012) in his research that “*general rule does not seem always applicable when archival material is digitized and represented for online access.*” It can be seen that traditional record representation activities focus on the context of records arranged in a hierarchical order, while electronic records have a purpose in the ease of access to content.

Records Management Principles

In the records business, records management is an important routine activity. Because the results of this records management activity can support the organization's business activities so that business processes can run more effectively and efficiently. Records management activities require procedures or models that are suit the needs of the organization and current development of ICTs with the aim of regulating record management techniques and stages in implementation of records management. As stated by Svård (2017) that “...there are two well-recognized principles to the theory and practice of records management, namely Life-Cycle and the Records Continuum Model.”

According to Karabinos (2015) “...the life cycle model breaks a record down into three distinct stages that distinguish records from archives. The first stage is the active stage, when records are created and actively used by the creating agency. In the second stage, the dormant stage, records are no longer of current use. The third stage is when records become archives, being stored and preserved for future use. Prior to the archival stage is the selection and appraisal process, where records are discarded or ‘advanced’ to the archival stage”. Indonesia adheres to the principle of the Life cycle model. This can be seen from the Performance Accountability Report of the National Archives of the Republic of Indonesia in 2013 that “*The Indonesian Archives (system) actually refers to an institution based on the principles, rules, and standards of archival administration practice in documents/archives in the administrative processes of government institutions and agencies within a framework of archival science which is described as a life cycle model of the North American tradition (Arsip Nasional Republik Indonesia, 2013)*”.

Meanwhile, the continuum model is a model for managing records with clear controls from the time the records are created until they are publicly accessible or published (Kennedy & Schauder, 1998). Australia, which has become an international reference in managing records, uses a continuum model approach, because it is considered the most appropriate to overcome the problems experienced in digital objects. Handayani (2019) supports this view by adding that the continuum model becomes more visible when the records created in electronic or digital form. As is known, the continuum model

approach is closely related to electronic and digital media. In line with this, President Joko Widodo during the 50th Archives Day Commemoration Night on 9 June 2021, demanded that the management of national archives should be in line with technological development –digital-based (Auliani, 2021). He said that the adaptation of digital technology must become a priority and be done immediately. Thus, the continuum model approach is a suitable choice to support developments in electronic records management in Indonesia.

Cloud Computing

Cloud computing is an organized computing system that specifically offers resources at dynamic scale, allowing all data (including emails, photos, documents and others) to be stored and shared via an unlimited number of hosted web applications. The cloud architecture has four layers, namely: hardware, software, virtualization and management. The commercial cloud architecture offers users on-demand access to the entire network of standard devices that can be accessed via the internet. In relation to records management, this system also facilitates processes for communication, backup and storage, collaboration, distribution, storage and preservation of records (Arpaci, 2016; Duranti, 2016).

Cloud, in providing its services, generally has three service models offered by cloud service providers, namely 1). Software as a Service (SaaS); a service model in the form of software such as Google Docs and Sheets and Adobe Creative Cloud. Service providers guarantee the availability and reliability of their applications, and users can focus on using these applications; 2). Platform as a Service (PaaS); a service that provides a platform for the use of its applications. This model does have a suitable security platform but not for applications built by users. Users still have to consider the applications' security; 3). Infrastructure as a Service (IaaS); a cloud service that provides servers and networks, users entrust data to service providers, so they don't need to provide hardware and do routine maintenance. The most common and well-known types of this model services are Google Drive and Dropbox (Duranti & Rogers, 2012).

The cloud architecture model that all services offer will be served on a trustworthy electronic record because Trust is complex and is at the core of the successful adoption and use of the cloud (McLeod & Gormly, 2017). Since data security and protection remain the responsibility of users/organizational management, it is necessary to increase data security in the form of risk mitigation strategies and trust in third-party service providers. As explained by Carroll & Kotzé (2011) namely: 1) Data Security, administration, and control is identifying and classifying information that can be allowed in the cloud, electronic record storage managers must have adequate skills, the need for backup schemes for data in the cloud, and cloud service providers must have acceptable interoperability standards to ensure data migration. Third parties service providers should periodically conduct audits to monitor compliance with agreed requirements; 2) Logical Access, is classifying access rights for managers and providing access restrictions and controls to prevent, detect and take action against security breaches. In addition, it is necessary to filter user profiles based on roles and classification of access rights following existing security policies within the organization; 3) Network Security, is to exercise control at the network level to create a system, prevent illegal access and prevent data loss or loss; 4) Physical security, it is by providing data encryption control and using a VPN (Virtual Private Network) when accessing data in the cloud that it aims to provide secure and private access by changing the connection path through the server and hiding the data exchange; 5) Compliance, ensures that the organization undergoes external audits and security certifications and complies with the law implemented in the policy. In addition to the ISO/IEC 27001 – Information security management systems requirements in clause 8, which is operational, the organization will be required to comply with annex A.12.3 Back-up data and A.17.2 Redundancy (The International Organization for Standardization, 2013); and 6) Virtualization, in addition to carrying out technical

security, providing socialization to users related to security in order to increase awareness of the risks of virtualization.

Along with the development of ICTs, many organizations have been using the cloud to store their documents. Ease of access and storage capacity is one of the reasons why many organizations decided to store their documents in the cloud. This is indicated by the increasing sales of cloud-related IT infrastructure in 2015, with total sales of one-third of their overall IT infrastructure sales revenue, International Data Corporation, in McLeod and Gormly (2017). In 2019, the Indonesian Minister of Education and Culture also encouraged the storage of their institutions' data, in this case electronic records, on cloud storage to adapt to the development of ICTs. This was done to facilitate data access as well as to support system efficiency and effectivity (Alim, 2019).

Data Retention Policy on Security and Trust

Trust in records relies on four types of related knowledge about the creator or maintainer of records: reputation, past performance, competence, and assurance of confidence in future performance. Meanwhile, in another sense, trust can be defined as user confidence in the applications and services offered by cloud service providers. Thus, making trust depends on the privacy and security properties of the chosen deployment model on the technology that ensures confidence in future performance. The stricter the security and privacy policies followed by the cloud service provider, the higher the level of user acceptance of the cloud (Arpaci, 2016).

Meanwhile, in archival science, data or electronic records can be considered trustworthy because they are influenced by three aspects, namely: 1) Records first must be seen to be accurate, which means the level of accuracy of the truth is high and far from error; 2) 'Reliability is another of the main dimensions of trustworthiness from an archival science perspective' record as a description of human activity and is a real fact, so that reliability here is the belief in records that can maintain facts. To achieve reliability records must have three main characteristics as: Completeness at point of creation, Consistency and Objectivity (Naturalness); 3) Furthermore, Authenticity is truly original records with real quality. For records to be considered authentic, records must be created by individuals who are represented as creators. There are two necessary preconditions for authenticity: identity (archival bond) and integrity of the record (completeness after creation) (Lemieux, 2017).

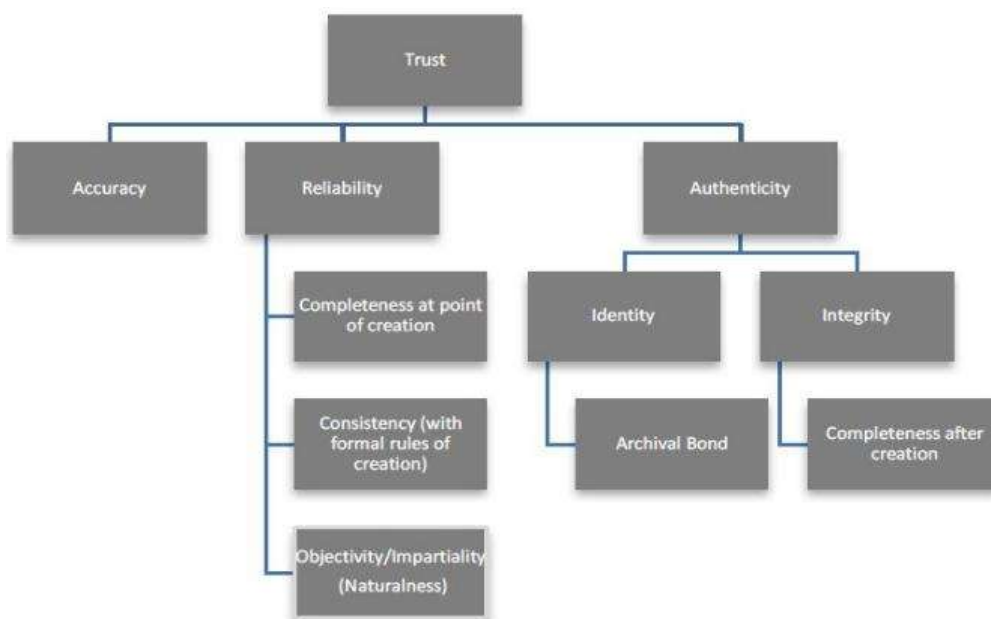


Figure 3. A taxonomy of key archival concepts and their relationship to trust (Lemieux, 2017).

In Werff's research (2019) *entitled Building consumer trust in the cloud: an Experimental analysis of the cloud trust label approach*, cloud storage systems can provide an effective way to communicate trust to consumers. The research shows that trust labels containing positive information can have a positive impact on trust while trust labels containing negative information can also have a negative impact on trust.

One of the methods to build and foster trust in digital environment is to build knowledge-based trust, even without any prior experience of interaction between parties in the business. In the context of information systems, efforts to build trust without a history of interaction tend to focus on third-party information (e.g., recommendation systems) or heuristic cues (e.g., web design). By providing objective information about the cloud service, it provides an opportunity to form knowledge-based trust (van der Werff et al., 2019). Thus, from the very beginning, users' trust can be gained with an agreement that clarifies the status and conditions regarding the cooperation in using the cloud.

Challenges and Solutions for Data Managers

The use of the cloud as part of a data management system in an organization will cause some changes to individual users and to the organization. At the level of individual users, the boundaries between data creators and users become not clear (Duranti, 2016). Cloud allows each individual user to communicate and collaborate flexibly. If a data is uploaded to a cloud system, other users can use the data and modify it into new data. This can blur the line between data users and data creators if rules and restrictions regarding maintaining data content and context are not applied.

Meanwhile, at the institutional level, data in printed form is managed and transferred according to the frequency of usage and its value, so that institution can limit the data access. However, the use of the cloud allows access from multiple devices making duplication and storing location out of control. To solve this problem, some institutions decide to provide special hardware for their internal use. Nevertheless, this will not necessarily work. Survey results show that more than half of the Y Generation workers are willing to violate company policies that prohibit carrying and accessing data via personal hardware if it interferes with their personal and professional computing and social networking activities (Duranti, 2016).

The challenge in using cloud systems can also be caused by the large volume of digital data that needs to be managed in various online platforms used by the institution. To overcome this problem, cloud system providers offered automatic deletion of data with certain categories and times. However, the deletion applies only to the institution's repository system and not on the provider's server. This causes data that should have been deleted, can still be found through other search alternatives outside the institutional repository. The amount of digital data that can be managed by the cloud system makes frequency of its usage even greater. Massive use of cloud systems is also along with user expectations that the data provided in the cloud is trusted and authentic. On those challenges, data managers are expected to be capable to maintain the accuracy, reliability and efficiency of retrieval of authentic data sources in the cloud.

It is clear that security concerns have played an essential role in using the cloud as a repository. Users relying on third parties to store their electronic archives may look terrible. Moreover, security problems such as phishing, botnet, and data loss seriously threaten organizations. In addition, the multi-lease model and the pooled computing resources in cloud computing have introduced new challenges that require new techniques to overcome (Kuyoro et al., 2011). This is undoubtedly one of the dangers or harmful impacts that can occur in the use of the cloud. Therefore, it is necessary to increase data security in the cloud repository.

In addition, Carroll & Kotzé (2011) say that the proper safety and protection of business data and systems remain the responsibility of the organization's management, regardless of whether the

data and systems are hosted in the cloud. If this is not done, it will have implications for data security risks such as the risk of data leakage leading to confidentiality and privacy risks, lack of control over hosted data and applications, concerns, risk of data integrity damage, and non-compliance with management policies resulting in hacking and misuse access. For this reason, transparency about who uses information and data stored in the cloud, why, and for what purpose can be shown in the history log to show accountability. Because this is part of good governance and communication. Similarly, organizations must ensure that cloud service providers safeguard the data and information they create and store (McLeod & Gormly, 2017).

There are several considerations and alternative solutions that can be applied by data managers. First, before utilizing cloud services, data managers must consider the type of cloud to be implemented. Types of cloud services can be divided into three, namely private, public, and hybrid. Private cloud is a type of cloud that can be used for internal purposes in an institution. The advantage of a private cloud is that it allows institutions to have a self-service, elastic and scalable model of IT infrastructure and services that can be scaled according to the needs and capabilities of the agency (Priyam, 2018). The possibility of using data architecture models, IT infrastructure and services independently, makes private clouds able to improve their security quality compared to other types of clouds. However, compared to the other two types, private cloud requires a higher cost.

Public cloud offers “one for all” services with a paid subscription and storage system”. As a result, institutions cannot adapt only to the specific types of services required. Although it costs much less than a private cloud, this system often charges unexpected fees for its services (Ali, 2019). When a public cloud's main server experiences problems and users lose data, the service providers often will not take responsibility on this risk. The sheer scale of public cloud users makes recovering lost data difficult for providers to facilitate. With limited funds, institutions can also choose a hybrid cloud. This cloud system combines private and public clouds. In a hybrid cloud system, sensitive and confidential data can be secured using a private system, while public data can use a public system. This system will bring financial benefits as well as security for the data managed by the agency.

An alternative solution that can be chosen by data managers in cloud systems is to build a security architecture system according to the possibility of hacking threats on the cloud system used (Gonzales et al., 2017). Data managers need to carry out risk assessments that may be obtained when utilizing cloud computing. Through proper risk assessment, it is possible to create a suitable data architecture to ward off threats that may occur.

In managing data in government institutions, Duranti (2016) states that it is impossible for archival institutions under the auspices of the government to protect material that can be accounted for as evidence and reliable sources. This happens if the government continues to implement a policy of restricting data access, even though the use of cloud systems aims to increase public trust through data transparency. The use of cloud systems that can no longer be restricted in today's era requires the active role of the government to create policies that protect data privacy and security in cloud systems through data protection and management laws as a legal protection (Hofman et al., 2017). The existence of legal protection regarding data and management in the cloud system is an alternative solution that can be provided by the government. This can have a positive impact on public trust in data managed by institutions.

Data managers can continue to maintain the principles that have been applied to printed data such as *respect des fonds* and *provenance* in their application in cloud systems. This application is one of the efforts to authenticate data control, so that the data found will not be lost or disconnected from the previous information chain. Thus, the data can be proven at a certain time and still considered authentic. In order to maintain user trust in the managed data, it is necessary to pay attention to reliability, accuracy and authenticity (Duranti & Rogers, 2012).

Efforts to maintain trust and security in digital data in the cloud continue to this day. One of the

latest findings regarding the breakthrough development of data privacy and security in the cloud is by utilizing the blockchain system (Hofman et al., 2017). Blockchain is a recording system that is carried out on an algorithm to verify every transaction made. In another explanation Blockchain is a distributed data transaction base, where the storage area is commonly referred to as scattered records and works together to store encrypted data as a unit or block and connected/chained to one another (Lemieux, 2016).

Blockchain technology, when adapted for data and records management systems, can play a role in better protecting private and vital data managed by cloud systems such as data related to identity, data ownership, and other personal data. So, it can be seen in general that blockchain technology can help with record authentication problems, because of the distributed system model. By using blockchain, because by using blockchain electronic record that have been authenticated and stored cannot be re-engineered to get solutions from original record (Fachmi & Mayesti, 2022). In addition, blockchain is also a digital data storage solution with a low-cost validation mechanism, but blockchain cannot guarantee data reliability from the start and has limitations as a reliable long-term data maintenance solution.(Lemieux, 2016).

From the explanation, it can be seen that both are virtual data storage places that have important points related to trust instruments (reliability, accuracy, and authenticity) for electronic records. This of course cannot be separated from their respective characteristics, if the cloud repository is centralized while the blockchain is decentralized, both can be an option for data managers depending on the needs of each organization.

SIMPULAN

Cloud-based storage is considered capable of increasing efficiency, effectiveness, and transparency in data management, of course, this is in accordance with the concept used by e-government, which is effective and efficient. This is a product of technological developments that provide convenience and solutions for humans. But keep in mind that convenience and solutions always go hand in hand with problems and challenges related to trust (authentication, accuracy, and reliability) of users over the managed data. Therefore, it is necessary to increase the security of digital data in the storage system and data management in the form of a cloud, which can be done by choosing the type of cloud that suits the needs and capabilities of the agency in managing data. Certainly, private cloud infrastructure is a good choice for organizations. Because the data owned will be managed by the organization, and private cloud services provide excellent control over the cloud infrastructure to increase security, compliance, transparency, and resilience. However, organizations should note that private cloud services require a large budget, IT personnel, and skilled experts to manage and operate.

Furthermore, the organization can build a data security architecture model that fits the hacking threat that may occur on the cloud system that is used. Either use the highest type of Cloud Services, Platform as a Service (PaaS), if the organization's readiness is proper, or use the most basic type of Infrastructure as a Service (IaaS) if the organization's still growing up. This can be done with information about threats that may occur in the cloud system, by conducting an assessment through the data manager This process is used to maintain data management by applying data management principles such as respect des fonds and provenance. On a broader scale, government can play a role in providing legal protection regarding privacy policies and data management in the cloud. In addition, adequate risk mitigation strategies need to be developed and followed to ensure security risk mitigation and data protection from risks such as phishing, botnets, data loss, leaks leading to confidentiality and privacy risks, loss of control over data, risk of data integrity damage, and non-compliance with management policies resulting in hacking and illegal access. In the future, the

government and agencies can also develop decentralized data storage technology and are currently developing namely blockchain technology. So that it can be used and become another choice of virtual storage for digital data managers, to increase data security and user confidence in data management.

DAFTAR RUJUKAN

- Ali, I. (2019, July 24). *Public Atau Private? Pengguna Cloud Wajib Tahu!* | Pricebook. Pricebook.Co.Id. <https://www.pricebook.co.id/article/news/9334/pengguna-cloud-storage-wajib-tahu>
- Alim, M. (2019, February 25). *Mendikbud Dorong Penyimpanan Arsip Lewat Cloud*. Jurnas.Com. <https://www.jurnas.com/artikel/48781/Mendikbud-Dorong-Penyimpanan-Arsip-Lewat-Cloud/>
- Arpaci, I. (2016). Understanding and predicting students' intention to use mobile cloud storage services. *Computers in Human Behavior*, 58, 150–157. <https://doi.org/10.1016/J.CHB.2015.12.067>
- Arsip Nasional Republik Indonesia. (2013). *Laporan Akuntabilitas Kinerja Instansi Pemerintah Arsip Nasional Republik Indonesia Tahun 2013*. <https://anri.go.id/download/laporan-akuntabilitas-kinerja-arsip-nasional-republik-indonesia-tahun-2013-1573667317>
- Auliani, P. A. (2021, June 9). *Jokowi: Tinggalkan Cara Lama Kelola Arsip Halaman all - Kompas.com*. Kompas.Com. <https://nasional.kompas.com/read/2021/06/09/21442311/jokowi-tinggalkan-cara-lama-kelola-arsip?page=all>
- Carroll, M., Van Der Merwe, A., & Kotzé, P. (2011). Secure cloud computing: Benefits, risks and controls. In *2011 Information Security for South Africa*. <https://doi.org/10.1109/ISSA.2011.6027519>
- Cloud Security Alliance. (2017). *Top Threats to Cloud Computing Plus: Industry Insights*. Cloudsecurityalliance.Org. <https://cloudsecurityalliance.org/artifacts/top-threats-cloud-computing-plus-industry-insights/>
- Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* - John W. Creswell, J. David Creswell - Google Books. In *SAGE Publications, Inc.*
- Disdukcapil Kabupaten Bantul. (2013, June 27). *E- KTP BOLEH DI FOTOCOPY ATAU TIDAK ??? – Disdukcapil*. Disdukcapil.Bantulkab.Go.Id. <https://disdukcapil.bantulkab.go.id/berita/58-e-ktp-boleh-di-fotocopy-atau-tidak>
- Duranti, L. (2016). Digital Records and Archives in the Commercial Cloud. In *Regulating the Cloud*. <https://doi.org/10.7551/mitpress/9780262029407.003.0007>
- Duranti, L., & Rogers, C. (2012). Trust in digital records: An increasingly cloudy legal area. *Computer Law & Security Review*, 28(5), 522–531. <https://doi.org/10.1016/J.CLSR.2012.07.009>
- Fachmi, A., & Mayesti, N. (2022). Tinjauan literatur argumentatif tentang kepemilikan data arsip digital non-fungible token (NFT) pada teknologi blockchain. *Berkala Ilmu Perpustakaan Dan Informasi*, 18(1), 144–158. <https://doi.org/10.22146/bip.v18i1.3989>
- Gonzales, D., Kaplan, J. M., Saltzman, E., Winkelman, Z., & Woods, D. (2017). Cloud-Trust-a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds. *IEEE TRANSACTIONS ON CLOUD COMPUTING*, 5(3). <https://doi.org/10.1109/TCC.2015.2415794>
- Handayani, T. (2019). Jadwal Retensi Arsip di Era Undang-Undang Republik Indonesia Nomor 43 Tahun 2009 tentang Kearsipan. *Anuva*, 3(4).
- Hofman, D., Duranti, L., How, E., Loong Keoh, S., & Mi Mi Aung, K. (2017). Trust in the balance: Data protection laws as tools for privacy and security in the cloud. *Algorithms*, 10(47). <https://doi.org/10.3390/a10020047>
- Karabinos, M. J. (2015). The shadow continuum : testing the records continuum model through the Djogdja Documenten and the migrated archives [Institute for History, Faculty of Humanities, Leiden University]. In *The shadow continuum*. <https://hdl.handle.net/1887/33293>
- Kennedy, J., & Schauder, C. (1998). The records life cycle model and the records Continuum Model. In *Records Management* (pp. 9–12). Addison Wesley Longman Australia.
- Kuyoro, S. O., Bikunle, F., & Awodele, O. (2011). Cloud Computing Security Issues and Challenges. *Kuyoro S. O., Ibikunle F. & Awodele O. International Journal of Computer Networks (IJCN)*, 03(5), 247–255. [http://eprints.lmu.edu.ng/1390/1/Cloud Computing Security Issues and](http://eprints.lmu.edu.ng/1390/1/Cloud%20Computing%20Security%20Issues%20and)

Challenges.pdf

- Lana, A. (2021). Dampak Kejahatan Siber Terhadap Teknologi Informasi Dan Pengendalian Internal. *Journal of Economics, Social and Education*, 1(3), 1–13. <https://jiesp.ppak-atmajaya.com/ojsjiesp/index.php/JIESP/article/view/5>
- Lemieux, V. L. (2016). Blockchain for recordkeeping: Help or hype? *SSHRC Knowledge Competition, Canada*, October. https://www.researchgate.net/publication/309414276_Blockchain_for_Recordkeeping_Help_or_Hype
- Lemieux, V. L. (2017). Blockchain and distributed ledgers as trusted recordkeeping systems. *FTC*. https://www.researchgate.net/profile/Victoria-Lemieux/publication/317433591_Blockchain_and_Distributed_Ledgers_as_Trusted_Recordkeeping_Systems_An_Archival_Theoretic_Evaluation_Framework/links/593aa6450f7e9b3317f4d860/Blockchain-and-Distributed-Ledgers-as
- Lončarić, K., & Stančić, H. (2017). Reaching computational trust: requirements for implementing trusted e-government. *Tehnički in Vsebinski Problemi Klasičnega in Elektronskega Arhiviranja. Digitalno in Digitalizirano. Arhivsko Gradivo Včeraj, Danes in Jutri [Elektronski Vir] : Zbornik Mednarodne Konference*, 97, 25. <https://www.bib.irb.hr/870193>
- McLeod, J., & Gormly, B. (2017). Using the cloud for records storage: issues of trust. *Archival Science*, 17, 349–370. <https://doi.org/10.1007/s10502-017-9280-5>
- Muhidin, S. A., Winata, H., & Santoso, B. (2016). Pengelolaan arsip digital. *JPBM (Jurnal Pendidikan Bisnis Dan Manajemen)*, 2(3), 178–183. <http://journal2.um.ac.id/index.php/jpbm/article/view/1708>
- Panetta, K. (2019, October 10). *Is The Cloud Secure?* Gartner.Com. <https://www.gartner.com/smarterwithgartner/is-the-cloud-secure>
- Permana, R. H. (2021, March 3). *Viral Keluhan Netizen Diminta Fotokopi e-KTP, Ini Penjelasan Kemendagri*. DetikNews. <https://news.detik.com/berita/d-5480894/viral-keluhan-netizen-diminta-fotokopi-e-ktp-ini-penjelasan-kemendagri>
- Priyam, P. (2018). *Cloud Security Automation* (1st ed.). Packt Publishing.
- Republik Indonesia. (2009). *Undang-Undang Republik Indonesia Nomor 43 Tahun 2009 Tentang Kearsipan*.
- Rifauddin, M. (2016). Pengelolaan Arsip Elektronik Berbasis Teknologi. *Khazanah Al- Hikmah Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan*, 4(2). <https://doi.org/https://doi.org/10.24252/kah.v4i27>
- Sugiyono. (2018). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D* (26th ed.). Alfabeta.
- Svård, P. (2017). Enterprise content management, records management and information culture amidst E-government development. In *Enterprise Content Management, Records Management and Information Culture Amidst E-Government Development*.
- The International Organization for Standardization. (2013). ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls. In *ISO.org [Online]* (Vol. 2013).
- van der Werff, L., Fox, G., Masevic, I., Emeakaroha, V. C., Morrison, J. P., & Lynn, T. (2019). Building consumer trust in the cloud: an experimental analysis of the cloud trust label approach. *Journal of Cloud Computing*, 8(1). <https://doi.org/10.1186/s13677-019-0129-8>
- Williams, C. (2006). Managing Archives: Foundations, Principles and Practice. In *Managing Archives: Foundations, Principles and Practice*. <https://doi.org/10.1533/9781780630892>
- Zhang, J. (2012). Archival Representation in the Digital Age. *Journal of Archival Organization*, 10(1), 45–68. <https://doi.org/10.1080/15332748.2012.677671>
- Zou, Q. (2019). *The representation of archival descriptions: An ontological approach* [McGill University]. <https://escholarship.mcgill.ca/concern/theses/rr172245f>