

Digital Preservation and Data Integrity: A Case Study

Normashidayu Abu Bakar, Universiti Teknologi MARA, Malaysia
Nordiana Mohd Nordin, Universiti Teknologi MARA, Malaysia
Mudiana Mukhsin, Universiti Teknologi MARA, Malaysia
Maslina Abdul Aziz, Universiti Teknologi MARA, Malaysia
Nor Diana Ahmad, Universiti Teknologi MARA, Malaysia

The Kyoto Conference on Arts, Media & Culture 2023
Official Conference Proceedings

Abstract

This study investigated the data integrity affected by digital preservation in archival institutions. Digital preservation is a broad term that includes everything that needs to be done to keep digital materials accessible even if the media fails or technology changes. The objectives of this study are to identify the factors that influence digital preservation, to examine the benefits of digital preservation in archival institutions, to measure the extent of digital preservation among members of archival institutions and to assess the data integrity of digital preservation. The advent of digital storage has profoundly altered our surroundings. Data is growing in size, usage and demand. Analysis was done using Atlas ti. Based on the findings, it was found that, in terms of skills, the respondents highlighted that it is associated with knowledge about cloud storage, experiences, and training that would enhance their digital preservation knowledge. In terms of the benefits of digital preservation, it can help in permanent digital preservation, and it is associated with complete data security. Thus, both will make the documents easy to retrieve. Besides, the important aspect is the types of data associated with the measurement of data integrity. Both are important elements in the preservation process in underpinning data integrity. Other findings include the types of data, that are associated with the measurement of data integrity and both are vital elements in the preservation process. The interview was conducted by semi-structured interviews and guided by a conceptual framework.

Keywords: Data Integrity, Digital Preservation, Archival Institutions, Cloud Storage, Data Authenticity

iafor

The International Academic Forum
www.iafor.org

Introduction

Digital preservation is a broad term that includes everything that needs to be done to keep digital materials accessible, even if the media fails or technology changes. These could be records made as part of an organization's day-to-day work, things made to be digital from the start, or the results of digitization projects. Possibly more than ever before, the digital world has necessitated that archivists develop new solutions briefly, borrow theories and methods from other fields, and interact with disciplines that have not been archivists' traditional professionals. This has resulted in a nearly existential conversation about what archives do and the development of new methodologies, funding options, methods of organizational cooperation, and ways of thinking. It has always been a struggle for libraries, archives, museums, and research organizations across the world to maintain access to vast and ever-expanding digital archives and collections (Corrado & Moulaison 2014). Because of their fragility, digital materials require extra attention to remain usable. Sadly, at many institutions, a large amount of data that was born digital is stored in an insecure digital environment.

Historically, there has been a shifting relationship between the repository and the person who created the materials. According to Duranti (2007), records that have been separated from their initial place can be preserved in archives because they meet three fundamental criteria: transparency in preserving records, confidentiality and consistency. Archives are impartial and even-handed experts who seem to be a person or organisation to the people who will use records to do their job or request for their task to be completed. Security means that the records can't be deliberately or inadvertently changed, and stability means that the contextual factors of the documents are recognized and defined in the archive.

Currently, archivists recognize that to "sell" their needs and objectives for records operations, they must establish persuasive theoretical solutions and learn how to implement them in practice (International Council on Archive, 2008). Two main variables contribute to digitalization in the archive institution: application and human factor characteristics. For the sake of archival preservation, the data must be kept in immaculate condition so that it may be accessed by the public when needed. To guarantee that digital preservation is accessible, trustworthy, and used for future generations, archival institutions must ensure that the integrity of preservation is maintained. This study, concerns data loss, manipulation, and data breaches. A record's authenticity is enhanced as it moves from the site of origin to the preservation location.

The methodology used in this research is a target population is a group of individuals from the same sample group. The target population for this study is mainly focused on the individuals involved directly with the archival institution and the digitization of the archival materials. The only group of individuals are chosen since the individuals have knowledge and experience in relating to the archival materials that have been digitized and stored in the cloud storage. So, they would most like to give the most accurate response and feedback regarding the cloud storage for the archival materials. Semi-structured interview questions were constructed to answer the following research objectives and questions.

Research Objectives

- To identify the factors that influence digital preservation
- To examine the benefits of digital preservation in archival institutions
- To measure the extent of digital preservation among members of archival institutions

- To assess the data integrity of digital preservation in archival institutions

Research Questions

- What are the factors that influence digital preservation?
- What are the benefits of digital preservation in an archival institution?
- To what extent of knowledge of archivists in digital preservation?
- What is the data integrity of archival institutions?

Conceptual Framework

The DPCM model was utilized to help diagnose the essential elements of long-term digital preservation initiatives. This model is used to assist in identifying long-term and permanent digital assets as well as to help organizations analyze the software development maturity and suggest essential practices necessary to increase that process's capabilities (Carnegie Mellon University 1990). TRAC's audit criteria and ISO 16363's approved best practices for functional digital preservation repositories form the basis of this standard. It is based on the ISO 14721 (2003) applicable standards. Each of the ISO-mentioned standards' digital preservation criteria is broken down into fifteen distinct components, each with its maturity measurements.

The DPCM model identifies additional elements of digital preservation as three interrelated contexts, namely: digital preservation infrastructure (policies and strategies; governance; collaboration; technical expertise and designated community; and trustworthy digital preservation repositories; and digital preservation systems (electronic records survey, ingest, archival storage; media or device renewal; integrity, security; preservation metadata and access) (Carnegie Mellon University 1990). Understanding the variables contributing to successful digital resource preservation in academic libraries requires all these components.

Tools factor

- The hardware and software

Individual factor

- Behaviour
- Skills
- Knowledge

Digital Preservation

- Data Migration
- Cloud Storage

Data Integrity

- Data storage
- Data loss
- Data corruption

Figure 1: The DCPM Model

The framework structure shows that factors affecting the reliability of data integrity are the tools and individual factors. The tools factor consists of the application software related to the computer used in the archival institution and other places. There may be many applications available that can be used to communicate and to go through the operations of the archival institutions in preserving the digital archives that have practical value to the community used. Unfortunately, threats to preserving the digital archives have been found, including errors (K.

Hashizume, 2013). This will affect the integrity of the information and hence affect the integrity of its values.

Literature Review

Tools Factor

Many phases of technological advancement can occur during attempts to access digital materials in an archive; this means faulty files might go overlooked till it is too late, resulting in the loss of valuable data. Aside from operational failures, there is still the potential for natural disasters, including fires and flooding, that could damage the archives collection. We also have to deal with the risk of tampering with the software system. Several of these issues may go undetected for an extended period before they can be finally discovered. The "2011 Data Breach Investigations Report" reported that hacking and malware are the common causes of data breaches, with 50% hacking and 49% malware (Sultan Aldossary, 2016).

Malware/Malicious

This malware comes from the user who used it before (W. A. Jansen, 2011). If the image is returned without properly cleaning it, sensitive data could be leaked (K. Hashizume, 2013). Malicious insiders are those authorized to manage the data, such as those authorized to manage the data. For example, database administrators or employees of the company offering cloud services (CSA, 2013). Malicious insiders are the people who are authorized to manage the data, such as database administrators or employees of the company offering cloud services (Sultan Aldossary, 2016). Obsolete computer hardware and software threaten the integrity of digital records unless careful measures are taken to ensure their usage over time.

To maintain the dependability and safety of digital records, clear and consistent mechanisms must be utilised to monitor the integrity of the content, context, and structure of every digital item. As a result of hardware and software upgrades, digital preservation typically necessitates the transfer of data from one format or configuration to the next. Because of this, the cost of transferring data (refreshing) or building and maintaining data (emulation) to accommodate outmoded data, can be prohibitive for some organizations (ICST, 2002; Lavoie & Dempsey, 2004; Navarrette, 2009). On the other hand, research on long-term digital preservation costs is littered with studies that fail to provide reliable and comprehensive data. Researchers imply that digital records are vulnerable to loss and destruction due to the fragility of the magnetic and optical media on which they are stored and the unexpected failure of the reading and writing equipment on which they are used (Sambo, Urhefe, and Ejitagha, 2017).

Individual Factor

Individual users often have limited knowledge about appropriate archival tools or necessary techniques for management and preservation (Debra A. Bowen, 2018). The staff needs to know a lot about how to use ICT tools. As stated by Jain and Mnjama 2016, most archivists and records managers lack technical knowledge when dealing with the challenges of ensuring digital records are kept for a long time. This means that archivists are unable to decide whether to keep digital records and ways to do it. These (theoretical) recommendations by archives are implemented in two ways: on the level of policies and strategies and on the level of practical solutions where time for planning is limited. Insufficient financing is frequently

stated as the primary reason for the lack of coordination between the two, as evidenced by the following report. Electronic documents in archive institutions have not received the attention they need because of a lack of funding. Policy and strategy are excellent, but unless they are implemented, they have little value (O'Shea, 1997). It necessitates substantial resources, compliant organisations, committed management and suitably trained people, implementation is likely the most challenging aspect of digital preservation to complete.

Sometimes, archivists feel that they are expected to provide answers and solutions to situations beyond their ability. The most challenging part of implementation is that it necessitates a significant investment of time and money, as well as the involvement of a large number of people, all of whom must be trained to the highest standards (O'Shea, 1997). According to Farelo and Morris (2006), African countries are plagued by a shortage of skilled workers, which is made worse by the "brain drain" phenomenon, in which experts leave the continent for the developed world in quest of better opportunities. ICT infrastructure is critical to the success of electronic government efforts, according to IRMT (2009). Government and agency IT departments must employ qualified employees and apply the best network and system management practices. This platform will serve as the foundation for future electronic government and records initiatives to prevent electronic records from being lost or corrupted.

It is correct to say that government agencies must adhere to digital record standards and functional requirements to ensure that ICT systems consistently create digital records and secure their integrity and trustworthiness by adhering to digital records standards (IRMT, 2009).

I. The behaviour

Individual users often have limited knowledge about appropriate archival tools or necessary techniques for management and preservation (Donghee Sinn, 2016).

II. The skills

Hosting data in the cloud introduces new security challenges. Firstly, data owners would worry their data could be misused or accessed by unauthorized users. Extensive research has been done on this security issue of data hosting (Sneha T., 2018).

III. The extended knowledge

The organizational preservation of digital records is like the "Tower of Babel" due to the multitude of choices, lack of knowledge about what to preserve, or what is the new business processes in digital societies.

IV. How skilled staff can be obtained?

When it comes to serving the public, archive institutions must comprehend and manage changes in their environments to adapt service delivery in the future while still meeting the mission of their organizations (O'Shea, 1997).

Digital Preservation

Preserving valuable data for future generations is a primary goal of digital preservation. Digital preservation, according to Hedstrom (1997: 190), is the "planning, resource allocation, and deployment of preservation systems and approaches essential to guarantee that digital information of permanent preservation is accessible and useable." In contrast, the

American Library Association (ALA) (2007) describes digital preservation as a mix of preservation techniques. This study defines digital preservation as a set of techniques and activities that attempt to preserve and access digital assets for as long as necessary. It is by preserving them either in their original state or a more persistent one while ensuring their authenticity and integrity. Digital preservation of personal information studies and argues that personal digital preservation should be addressed with personal, social, and technological factors (Copeland, A.J., 2011). Archives successfully protect the authenticity of records removed from their original context because they fulfil three essential criteria: transparency of records preservation, security and stability. In today's digital age, organizations are increasingly vulnerable to a variety of security risks, including those posed by the use of information systems such as viruses and hacking tools.

Those who participated in the survey were asked to state whether or not they have adopted any security measures at their respective places of employment (Kofi Koranteng, 2018). Digital reservation is a broad term that includes everything that must be done to keep digital materials accessible even if the media fails or technology changes. These could be records made as part of an organization's day-to-day work, things made to be digital from the start, or the results of digitization projects. Possibly more than ever before, the digital world has necessitated that archivists develop new solutions briefly, borrow theories and methods from other fields, and interact with disciplines that have not been archivists' traditional friends.

Data Migration

Cloud computing is facing a lot of issues. Those issues are listed as the following: data loss, data breaches, malicious insiders, insecure interfaces and APIs, account or Service hijacking, data location, and denial of Service (William Allen, 2016). It is possible to migrate data every two to three years, but it will demand a sizeable financial commitment, continual human attention, and employee training. The ability to analyze and recommend the best new formats, the time to design and evaluate migrating pilot projects and the ability to form and refine migration processes are all necessary for a successful digital migration project. In addition, the file is vulnerable to corruption as it is being re-converted. Over time, formatting can change, and data can be lost. A weird depiction of a document with no way to recover the actual data might be caused by a machine, software, or human mistake. Ensuring the long-term preservation of electronic records requires the development of best practices and methods (Siew Lin et al., 2003). The transmission of digital information inside the OAIS intends to preserve it. This type of transfer is distinct from others in that it emphasises the preservation of a comprehensive information substance that needs to be preserved. It views the new archived execution of the information as a substitute for the old and understands that sole control over all transfer elements inhabits the OAIS (CCDS, 2012).

Data Integrity

Integrity means that any unauthorized entities cannot change actual data. Also, users storing data over cloud storage have no longer extended physical possession of data; it makes data integrity protection a challenging task. It is necessary to develop a system that should protect user privacy and data integrity. Overall, the system preserves user privacy and integrity while sharing data in a cloud environment and facilitates a secure way of sharing data on the cloud server (Manoj Shantaram Tore & S.K.Sonkar, 2015). In the field of information systems and information technology (IS/IT), input (data) – process – output (information) are well-acknowledged concepts (O'Brien 2000; Oz 2002). The English word data represents the Latin

term datum's singular and plural variants. O'Brien (2000) defines data as 'raw facts or observations, often regarding physical events or commercial operations. Information has integrity if it is secured in terms of its accuracy, completeness, timeliness, validity, and manner of processing (ITGI 2004; Carlson 2001; NIST 800-12 Handbook 1995). An original state is what the IT Governance Institute (ITGI 2004:22) defines as "integrity." According to this definition, information integrity refers to how accurately a representation of the condition or subject matter is portrayed. Bovee et al. (2003) explain the four parts of integrity, which is a part of how information is made, in terms of accuracy, completeness, consistency and existence.

Data Storage

It happens when hardware, software, storage media or file formats do not last long enough to provide long-term access to digital information. Organizations can now afford to store unlimited amounts of data (Debra A. Bowen, 2018).

Data Loss

However, due to improper long-term preservation techniques, most cannot afford data loss. There are many possibilities of losing data due to a malicious attack and sometimes to server crashes or unintentional deletion by the provider without backups. Catastrophic events like an earthquake and fires could be the causes of loss (William Allen, 2016).

Data Breach

Cloud computing is facing a lot of issues. Those issues are listed as the following: data loss, data breaches, malicious insiders, insecure interfaces and APIs, account or Service hijacking, data location, and denial of Service. Any breach of this cloud environment would expose all users' and organizations' data to be unclosed. It was reported "2011 Data Breach Investigations Report" that hacking and malware are the common causes of data breaches, with 50% hacking and 49% malware (William Allen, 2016).

Data Manipulation

Data integrity could help get lost data or notify if there is data manipulation. In many cases, data could be altered intentionally or accidentally. Also, many administrative errors could cause loss of data, such as getting or restoring incorrect backups (IJACSA, 2023).

Reliability of Records

A record's reliability and usability must be evaluated in addition to its legitimacy and integrity. These characteristics are critical when archivists decide how to preserve and appraise a collection. Usability refers to the extent to which future end users can view and interact with saved material in terms of accessing, displaying, and accurately interpreting the data in the long-term preservation of digital records (Mason, 2007). While the reliability of a record as a factual statement is reflected by its trustworthiness, the opposite is true. To determine the validity of a record, it is necessary to examine its form, and the degree of control exercised over its development (Roeder et al., 2008).

Thus, the digital record must be accurate, factual, and reliable in any administrative or corporate context. (ISO 15489-1, 2001). For a record to be considered usable, it must be easy to locate, retrieve, and use. Preserving an electronic record necessitates knowing its specific qualities, which can be found by identifying, authenticating, and extracting its essential metadata, according to the IRMT (2009). As they put it, "In what format was a digital product created and stored?" would be answered by the identification procedure. Is this a digital picture? Documents created with Microsoft Word 2000 must be checked to see if a copy exists in an MS Word 2007 or an MS Word 2000 document, for example. The vulnerabilities that digital information faces and possible solutions face are well documented in the academic and professional literature (Zsuzsanna, 2014).

Research Methods

This type of research is a quantitative approach. It uses data collection techniques through interviews and semi-structured questionnaires. The presentation of the results of the data analysis using Atlas. ti. version 22.1.0. Interviews were conducted with the staff at the digital department on the issues related to data integrity and digital preservation. The interview was conducted using phenomenological analysis. Interpretative phenomenological analysis (IPA) explores how participants make clear sense of their personal and social world. The main currency for an IPA study is the meanings particular experiences, events, and states hold for participants (Smith & Osborn, 1997). According to Smith et al. (2009), it is advised to choose between 3 and 10 for studies based on interpretative phenomenological analysis, but indicate that the appropriate sample size depends on some factors specific to the study concerned, including the level of study for student work (undergraduate, postgraduate). Three staff from the ten Archives Management Divisions in the Digital Archives section have been chosen. Interviews are one way to learn more about a person's experiences or feelings about a thing, organization, culture, or space (Nixon 2018). Interviews are a great way to find out more about what happened to a participant.

Findings

There were three participants involved in the interview. They were from the Digital Archives section. The first respondent was knowledgeable from different backgrounds in IT, archives and management. The Second respondent was an IT expert, and the third was an IT assistant. The questions were answered accordingly based on their knowledge and experiences.

Extend Knowledge of Digital Preservation

These skills are one of the factors the data integrity in archival institutions based on the previous research. Hence, the respondents were participants to explain how the knowledge took place in executing the digital preservation process in archival institutions. I asked for their experiences and skills from their job scope. From this, I can identify the extent of their knowledge of digital preservation.

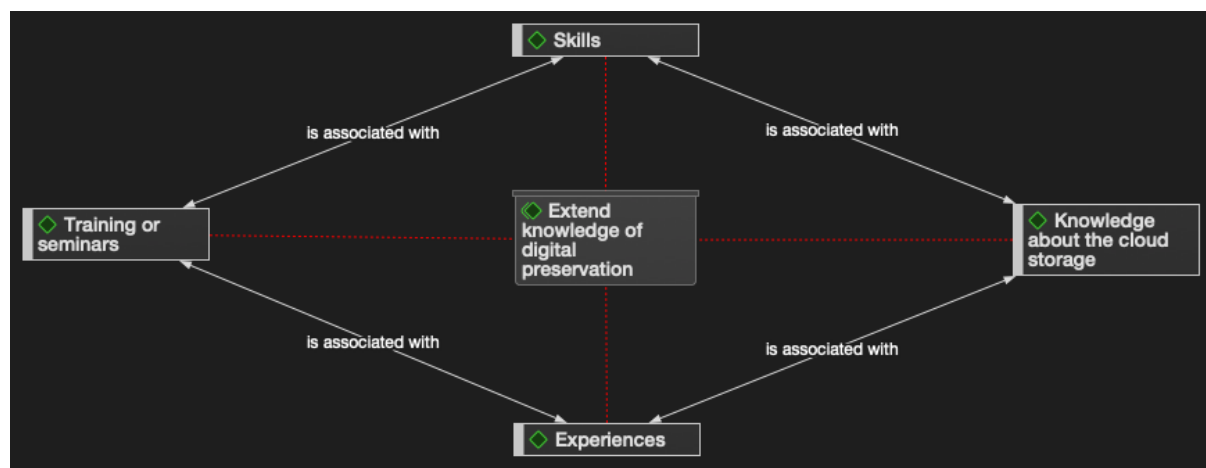


Figure 2: The extent of knowledge from the experts in archival institutions

In terms of skills, the respondents highlighted that skills are associated with knowledge about cloud storage, experiences, training and seminar that would enhance digital preservation knowledge.

Benefits of Digital Preservation

The benefits of digital preservation in archival institutions are being identified as if it influences the data integrity of digital materials transferred. The experts participated in answering the questions.

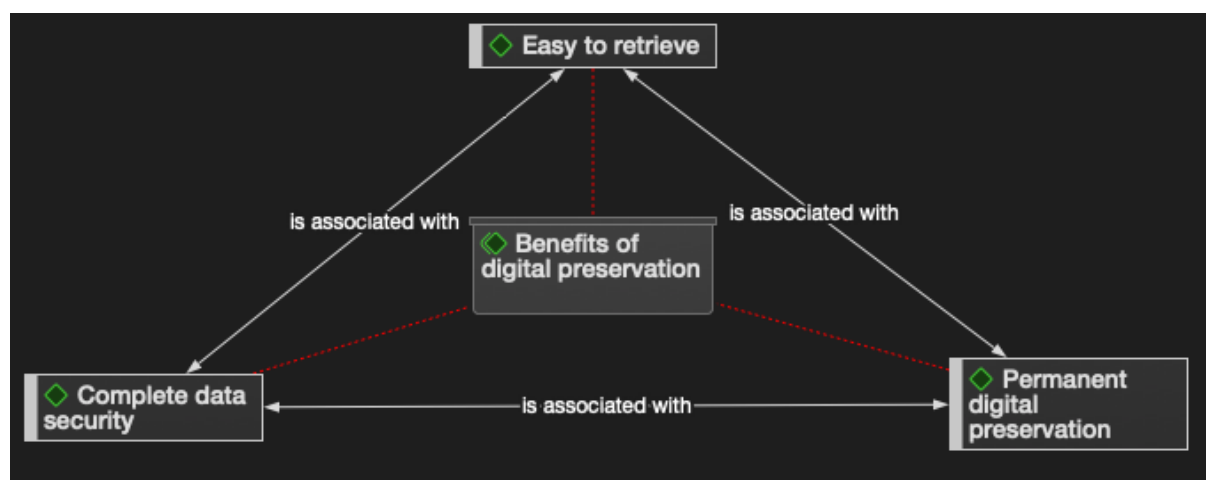


Figure 3: Data preservation benefits digital materials' data integrity

In terms of the benefits of digital preservation, it can help in permanent digital preservation, and it is associated with complete data security thus both make the documents easy to retrieve.

Identifying Data Integrity

The questions were asked about the data integrity in the archival institutions. It is one of the critical points in this research since I wanted to discover how to determine data integrity for digital preservation. The respondents answered based on their experiences handling the data before the materials were transferred into the repository. The important aspect is the types of data, that are associated with the measurement of data integrity and both are important

elements in the preservation process in underpinning data integrity. The preservation process is associated with the types of data and the measurement of data integrity.

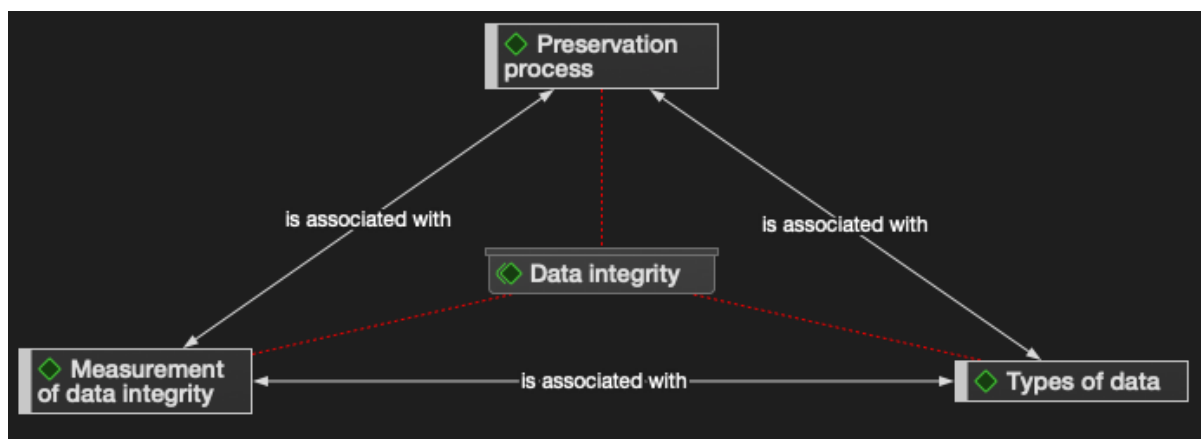


Figure 4: The data integrity in archival institutions

Factors of Digital Preservation

The respondents were asked about the factors that digital preservation influenced the data integrity of archival materials. The elements associated with the factors are adequate storage with a proper allocation, and adequate storage that are associated with the systems and tools for digital preservation. These elements are associated with collaboration and partnership. There are also constraints of digital preservation that are associated with storage equipment. All the elements are factors of digital preservation that are retrieved from the interviews.

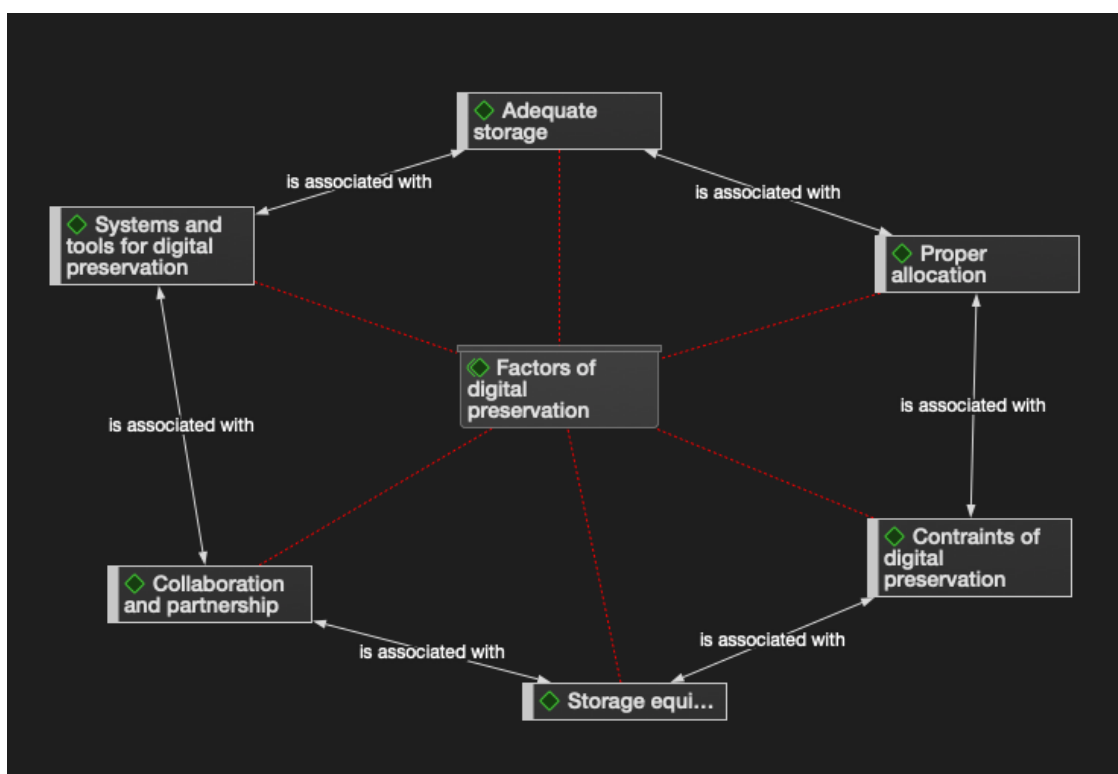


Figure 5: Factors that influenced the data integrity by digital preservation

Discussion and Recommendation

The archive system is indeed for long-term storage. So, even if they want to create their system, they can't. If they use government funding, they have to use the existing system. But still using the same system, it will be obsolete as well. So, it has to be balanced with the available funding. It supports the literature review from the proper allocation by Hedstrom (1997) where sustainable digital preservation necessitates wise use of available resources. People tend to start organizing their digital content when something important happens, like when their inbox is full, they run out of storage space, they buy a new computer, or they plan to do a spring clean-up (Williams et al., 2008). But as digital storage gets cheaper and bigger, it happens less often that a disk is full, so people don't have to get rid of their digital files as often or as often as they used to (Jones, 2007). The finding supports the literature review since the National Archives will be provided with adequate storage by request from IT. They also have a cloud repository internally. The literature review stated that it has been found that the threats to preserving digital archives include malware such as viruses and errors (K. Hashizume, 2013). This will affect the integrity of the information and hence affect the integrity of its values. However, the National Archives of Malaysia never faced any issues regarding the virus only the error issues. The corruption happens before the materials are transferred to the archive, not within the preservation state. Simply stated, data is only as permanent as the hardware or software that gives it life. It seems that technological obsolescence represents a far greater threat to the preservation of digital archives than does media longevity Betts (1999). This is associated with the findings that the software and hardware influence the data integrity of archives.

The Benefits of Digital Preservation in Archival Institutions

For a record to be considered usable, it must be easy to locate, retrieve, and use. Preserving an electronic record necessitates knowing its specific qualities, which can be found by identifying, authenticating, and extracting its essential metadata. This literature review supports this finding that the AMS can read everything in the formats that have been migrated. Meaning that there is no problem for us to open the format that has been migrated later. So, no issues back to PDF. It is easy to retrieve by digital preservation. From the literature review, Stephens (2010) suggests that archivists, record managers, and other information management specialists need to reinvent their professional practices to ensure the permanent or long-term preservation of electronic records. From the finding, this supports the benefits stated by the respondent that AMS application, the duty part is the active preservation, which is permanent preservation.

The Data Integrity by Digital Preservation in Archival Institutions

Ensuring the long-term preservation of electronic records requires the development of best practices and methods (Siew Lin et al., 2003). The transmission of digital information inside the to preserve it. This reflects the finding that AMS is developed using a framework that we have recognized and have the recognition from the International that we use the Open Archival Information System (OAIS). For integrity, the National Archives cannot identify that the document is authentic. What AMS can do here, we can identify the records or content of materials transferred from agencies that are public offices, not composed or not corrupt, and how the data authenticity is a forensic part. What AMS can do here, it able to identify the records or content of materials transferred from agencies that are public offices.

Conclusion

This paper identified several factors that contribute to successful digital preservation and concludes that these factors may affect the long-term viability of data integrity through digital preservation efforts in the archives. These include the benefits of digital preservation, the factors of digital preservation that influence data integrity, the data integrity and the extended knowledge of archivists in archival institutions. Archivists use cloud computing to store their digital documents. As each archive stated, creating copies of their documents was adequate for maintaining long-term access and preservation of those records. Ensuring that documents and archives can be accessed and used in the future, will go a long way toward the goal of achievement. Management in these institutions needs also to benchmark with other institutions in terms of good governance, implementation of policies, and building proper infrastructures through collaborative and partnership efforts. This study, therefore, recommends a multi-pronged approach to digital preservation including the enactment of preservation policies, proper allocation of resources, more collaboration, and improved technology infrastructure to address software and hardware obsolescence. Archives or archivists do not have ultimate control over the authenticity of a document. An item-by-item inspection is impossible given the volume of documents produced each year and the widespread occurrence of inadequate archives. Authenticity, on the other hand, remains unverifiable.

References

- Adu, Kofi & Adjei, Emmanuel. (2018). The phenomenon of data loss and cyber security issues in Ghana. *Foresight*. 20. 00-00. 10.1108/FS-08-2017-0043.
- Aldossary, S., & Allen, W. (2016). Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions. *International Journal of Advanced Computer Science and Applications*, 7(4). doi:10.14569/ijacsa.2016.070464
- Allen, William, et al. (2016). Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions. Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions. 7(2016) 4, 2016
www.ijacsa.thesai.org
- Allinson, Julie. (2006). OAIS as a reference model for repositories: an evaluation.
- Betts, M. (1999), "Businesses worry about long-term data losses", *Computerworld*, Vol. 33 No. 38, pp. 22-4.
- Bovee M, Srivastava RP, Mak B (2003). A conceptual framework and belief-function approach to assessing overall information quality. *International Journal of Intelligent Systems* 18: 51–74.
- Bowen, S. A. (2018). Mission and Vision. University of South Carolina.
<https://doi.org/10.1002/9781119010722.iesc0111>
- Carlson, T. (2001). Information security management: understanding ISO 17799. Lucent Technologies Worldwide Services. [Online]. Available
http://www.netbotz.com/library/ISO_17799.pdf (Accessed 1 February 2023).
- Copeland, A.J. (2011). "Analysis of public library users' digital preservation practices", *Journal of American Society for Information Science and Technology*, Vol. 62 No. 7, pp. 1288-1300.
- Corrado, E.M. and Moulaison, H.L. (2014). *Digital preservation for libraries, archives, and museums*. Lanham, MD.
- CSA, "The Notorious Nine Cloud Computing Top Threats in 2013," *The Notorious Nine Cloud Computing Top Threats in 2013*. pdf.
- David O. Stephens, *Records Management: Making the Transition from Paper to Electronic*. Lenexa, Kansas. ARMA International, 2007. xvii, 292 pp. ISBN 978 1 93 1786 29 4
- "Definitions of Digital Preservation", American Library Association, February 21, 2008.
<http://www.ala.org/alcts/resources/preserv/defdigpres0408> (Accessed October 3, 2023). Document ID: 21609b50-bc60-46e4-848e-dc5fdabdb128
- Donghee Sinn and You-Seung Kim (2016). "Development of a Collecting Policy for No Gun Ri Digital Archive," *Journal of Korean Society of Archives and Records Management* 16(3): 1-30. (Korean journal, written in Korean)

- Farelo, M & Morris, C. (2006). The Status of e-government in South Africa. ST Africa Conference, Pretoria, South Africa.
<http://researchspa.csir.co.za/DSPACE/bitstream>(Accessed on 22 November, 2013).
- Hashizume, K., D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,” *Journal of Internet Services and Applications*, vol. 4, no. 1, pp. 1–13, 2013.
- Hedstrom, M. (1997). Digital preservation: a time bomb for digital libraries. *Computers and the Humanities*, 31: 189–202. Hockx-Yu, H. 2006. Digital preservation in the context of institutional repositories. *Electronic Library and Information Management Journal*, 5: 32-40. modern organizations. Hershey: IGI Global.
- International Council on Archives, *Principles and Functional Requirements for Electronic Office Environments*, Module 2 – Guidelines and Functional Requirements for Electronic Records Management Systems, International Council on Archives, 2008, p. 13.
- International Records Management Trust. 2009. E-Records readiness assessment tool. http://irmt.org/documentsbuilding_integrityIRMT_project_proposal.pdf. (Accessed 30 May 2013).
- InterPARES, Authenticity Task Force Report, in *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*, 2002, available at http://www.interpares.org/book/interpares_book_d_part1.pdf (accessed October 2014), p.2. ISO 15489:2001 *Information and Documentation – Records Management – Part 1*, International Organization for Standardization, 2001, p. 7.
- Jain, P & Mnjama, N. (2016). Managing knowledge resources and records in modern organizations. Hershey: IGI Global.
- Jayapandian N A , Md Zubair Rahman A M J. (2018). Secure Deduplication for Cloud Jones, W. (2007), “Personal information management”, *Annual Review of Information Science and Technology*, Vol. 41 No. 1, pp. 453-504.
- Kiss, Zsuzsanna. (2014). Job search time: the indicator of employability. *Quest Journals, Journal of Research in Business and Management*. 2. 1-9.
- Lavoie, B & Dempsey, L. 2004. Thirteen ways of looking at digital preservation. *D-Lib Magazine*, 10:7-8.
- Management Journal, 26 (2),170-184, Retrieved from <https://doi.org/10.1108/RMJ-07-2015-0028> Mason, S. 2007. Authentic digital records: laying the foundation for evidence.
- M. S. T. (2015). A Cloud Storage System For Sharing Data Securely With Privacy Preservation And Fraud Detection. *International Journal Of Research In Engineering And Technology*, 04(08), 52–55. [https://Doi.Org/10.15623/Ijret.2015.0408010](https://doi.org/10.15623/Ijret.2015.0408010)

- NIST 800-12 Handbook. (1995). An introduction to computer security. National Institute of Standards and Technology. USA: US Department of Commerce.
- Nixon, E., Scullion, R. And Hearn, R. (2018). “Her majesty the student: organization higher education and the narcissistic (dis) satisfactions of the student-consumer”, *Studies in Higher Education*, Vol. 43 No. 6, pp. 927-943.
- O'Brien, J.A. 2000. Introduction to information systems: essentials for the Internetworked enterprise (9th ed). USA: McGraw-Hill Companies.
- O’Shea, G. (1997). *Research Issues in Australian Approaches to Policy Development*. 7. 5455 *Research findings - objectives, importance and techniques*.
- Oz, E. 2002. Management information systems (3rd ed). Canada: Course Technology Thomson Learning.
- Research Paper Topic Ideas & Suggestion for Students. (2021, August 25). <https://www.myresearchtopics.com/guide/research-findings> Reference Model for an Open Archival Information System (OAIS). (2012).
- Roeder, J., Eppard, P., Underwood, W. and Lauriault, T. 2008. Authenticity, reliability and accuracy of digital records in the artistic, scientific and governmental sectors. [Online].
- Sambo, A. S., Urhefe, E. A., & Ejitagha, S. (2017). A Survey of Digital Preservation Challenges in Nigerian Libraries: Librarians’ Perspectives. *International Journal of Digital Curation*, 12(1), 117–128. <https://doi.org/10.2218/ijdc.v12i1.426>
- Siew Lin, L., Ramaiah, C. K., & Kuan Wal, P. (2003). Problems in the preservation of electronic records. *Library Review*, 52(3), 117–125. <https://doi.org/10.1108/00242530310465924>
- Smith, J. A., Flowers, P., & Larkin, M. (2009). *Interpretative phenomenological analysis: Theory, method and research*. Los Angeles, CA: SAGE
- Smith, J.A., Flowers, P. and Osborn, M. (1997). ‘Interpretative phenomenological analysis and health psychology’, in L. Yardley (ed.), *Material Discourses and Health*. London: Routledge, pp. 68–91.
- Sneha Tripathi, (2018). "Digital preservation: some underlying issues for long-term preservation", *Library Hi Tech News*, 35(2),8-12, <https://doi.org/10.1108/LHTN09-2017-0067>
- TGI. 2004. *Managing enterprise information integrity: security, control and audit issues*. USA: IT Governance Institute.
- W. A. Jansen, “Cloud hooks: Security and privacy issues in cloud computing,” in *System Sciences (HICSS), 2011 44th Hawaii International Conference*. IEEE, 2011, pp. 1–10.

Williams, P., Dean, K., Rowland, I. and John, J.L. (2008). “Digital lives: report of interviews with the creators of personal digital collections”, *Ariadne*, Vol. 55, available at: www.ariadne.ac.uk/issue55/williams-et-al (accessed September 20, 2023).

Contact email: ndiana@uitm.edu.my