A Comparative Review of Five Leading Document Management Systems Based on Information Security

ONYEMA EMEKA FAMOUS[1], SUNDAY ERIC ADEWUNMI[2], VICTORIA YEMI-PETERS[3]
[1, 2, 3] *Department of Computer Science, Federal University, Lokoja, Lokoja Kogi State*

Abstract- ***In today's digital and data-driven world, ensuring robust information security is crucial for all organizations irrespective of their sizes, location, and use. With an emphasis on Information Security, this paper presents a comparative review of five leading document management systems (DMS) – DocuWare, M-Files, ZohoDoc, PandaDoc, and eFileCabinet thereby reviewing their various methods of ensuring information security and using a qualitative review method based on confidentiality, integrity, availability, and compliance (CIA-C). It examines popular features that make up CIA-C and finds that PandaDoc is the most secure. Through this comparative analysis, individuals and organizations will gain a deeper understanding of the security features of these Document Management Systems (DMS) solutions which will help them make informed decisions based on their needs, making sure their choice aligns with their security requirements, with organizations having a firm foundation of trust to mitigate potential risks thereby contributing to a more secure digital environment.***

Indexed Terms- ***Availability, Confidentiality, Document management systems, Information Integrity, Privacy, security***

I. INTRODUCTION

A document basically refers to a container of information (often paper) that contains written or drawn information for a particular purpose in a structured way [1].

According to [2], an "electronic document" is an information container in electronic form, which gathers information from a variety of sources, in a number of formats, around a specific topic to meet the needs of a particular individual. This means that an individual can create an electronic document on a personal computer without creating a paper document. This electronic document can be identified, stolen, hijacked, or transferred using any form of network in an electronic manner. It can either be sent to a single person or a group of people at the same time. This is called document sharing.

A Document Management System is a system or process used to capture, track, and store electronic documents such as PDFs, word processing files, and digital images of paper-based content [3].

Security vulnerabilities are a weak point of any system at the design and implementation levels, and document management systems (DMS) are not an exception [4].

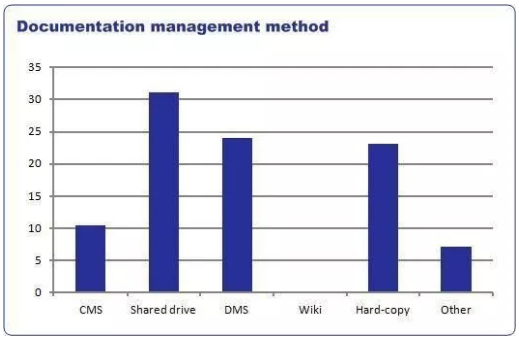

Figure 1 - Methods of Document Management [5]

With the advent of shared drives incorporated into document management systems, one may wonder the level of information security embedded on these systems especially as it relates to *confidentiality*, *integrity*, *availability and compliance*.

The aim, therefore, is to compare the level of information security implementation in these document management systems through a number of metrics and through this comparison with objectives to:

i. Identify similarities, state-of-the-art (SoTA) security techniques used in the selected document management systems.

ii. Provide users with informative decision and broaden perspectives on choosing a document management system outlined in this paper.

II. LITERATURE REVIEW

This section provides a review of the relevant literature that will inform the subsequent comparative analysis.

There are several works in the related literature comparing ease of use, features, pricing, work centric and services offered by document management systems. As regards the ease of use of various features of cloud storage systems using a multi-criteria decision analysis (MCDA), [6] compared various systems and the report showed that *SugarSync* is easier to use when compared with others such Google Drive and DropBox while as regards been a crucial factor to consider when deciding on the cloud storage platform to use and following the report of [7] in comparing the pricing of cloud storage, Google Drive stood out among DropBox, IDrive and SurgarSync with its various free service option and size of storage up to fifteen gigabyte.

To further provide information to users on the various features and services offered by these numerous storage platforms, [8] showed that in terms of manuscript management systems for scholarly publishing in Korea, systems which defined roles of authors, editors, peer reviewers, printing agencies and journal managers should be considered although no specific system was mentioned but these features makes a better system since it covers the entire process of manuscript reviewing and allows the writer to be in control. However, in the report of [8] though with a shorter free version should be considered as it has rich features which other than those mentioned above include the option of capturing the issues and tracks of journals and conferences and most importantly it is very affordable. Despite the numerous reviews on various components of storage systems, The authors in [9] were more concerned about the work centric and tuning measures of these systems. Their research addressed the flexibility and human orientation of eight different document Management systems in which four out of the eight systems compared have proper workflow features different from others. The review showed that M-Files is most supportive followed by BlueDoc, Speedy organizer and Iso Tracker. They pointed out that *M-Files* is more work centric and could fit into the daily use of most organizations in terms if document management systems.

In terms of security of these systems, the work of [10] suggested the use of SMS notification to handle unauthorized access and authentication and built a system called F-Secure. This suggestion did not however capture the limitations in cases where users' phones were out of reach or poor network reception. Compliance and certification is also a major component of information security and as such the various methodologies of document management systems should be made to support ISO 9001:2008 which include the use of suitable and strong encryption algorithms alongside other means of ensuring information security [11]. The security of any system should not just be about the codes or design methodology but a thorough one throughout the life cycle of the system. Scholars such as [12] suggested that features such as Confidentiality, Authorization, Accountability, Integrity, Authenticity and Non-repudiation to mention a few should be made to exist within the entire life cycle of the system despite the overhead cost of implementation. Any plan to increase the security of a system without considerations for training and retraining of users on best practices on threats, weakness and security vulnerabilities will not yield the required result [13].

In addition, the problem of Spam mails common in DropBox according to [14] can best be solved through the use of improved *honey encryption* which has a way of tricking the attacker into believing that he has access to valuable information only to realize that an attempt to decrypt the file is an *impossible mess.* The use of honey encryption is still a work in progress. While [15] suggested the use of a secure watermark system (SWS) due to the computational effect of encryption algorithm. With the current power of processors, computational effect should be less a factor to consider and hence the use of a strong encryption algorithm should be considered rather than a secure water mark which only identifies the document but does not secure integrity nor availability [16].

The review of related work showed that while some researchers have done noble work on comparing price, features, ease of use, work centric and workflow and others, there is currently no research that compares the information security level of document management systems in order to better inform users and guide their choice and decision making. This is what this research will focus on.

In order to perform this comparison, five (5) leading cloud storage document management systems were selected and analyzed. These document management systems include DocuWare, M-Files, eFileCabinet, PandaDoc and ZohoDoc.

2.1 DocuWare

DocuWare is a document management, Enterprise Content Management (ECM) and workflow automation software solution designed to help businesses and organizations digitize, store, manage, and process their documents and data electronically [17]. As a company, it was founded in 1988 by a German based software company owned by Jürgen Biffar and Thomas Schneck. Docuware initial aim was to just digitalize paper documents, improve document storage and retrieval and streamline business process and hence started as a standalone app and by 1992, it had grown beyond the German border to international use. In 2012, in response to the growing demand of cloud-based solutions, DocuWare introduced DocuWare cloud which offered subscription-based services and allowed users to access their documents from anywhere in the world. However, in 2019, DocuWare was acquired by Ricoh Company Ltd., which allowed DocuWare to expand its services. DocuWare has a number of features and functionalities such as Document capture which allows users to capture documents from various sources and perform OCR, document indexing by tagging each document with a metadata for easy retrieval, document Storage which provides a secure and centralized repository for storing electronic documents and files, reporting and analytics and workflow automation.

DocuWare architecture is a 3-tier architecture that includes Client Application, server component and Database. The first tier provides interface for users to interact with DocuWare and make available a Desktop app on various platforms. The server component is where integration and content services are shared from while the database handles storage and indexing using a relational database management system.

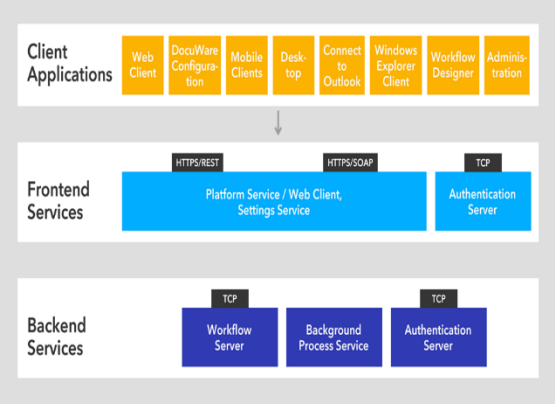

Figure 2: DocuWare Architecture [9]

DocuWare offers robust security features including user authentication, encryption and audit trails. DocuWare ensures confidentiality using a number of methods such as access control to ensure that authorized personnel can access specific documents and data by using Role based Access control (RBAC), encryption and authentication. It offers encryption for data in motion using TLS/SSL to encrypt data transmitted between the client and DocuWare server ensuring that data is secure while traversing the network and at rest (data on disk and in database) by relying on typical encryption available on RDMS. According to [9], DocuWare uses AES (Advanced Encryption Algorithm) along with symmetric keys of 1024 bits with a key size or length of 256 bits and then uses a key length of 4,096 bits to encrypt the symmetric keys and also generate a new key for each document. This is a good tackle and fortifies confidentiality.

In terms of data and files integrity, a look at their website shows that DocuWare ensures document integrity through version control and audit trails, allowing you to track changes and maintain data integrity. It used SHA-256 which generate a fixed length hash such that any change in the document will result in a different hash value allowing for the detection of data tempering.

DocuWare ensures availability by leveraging on multiple servers and IT infrastructure in case of

outages and its failover mechanisms, help minimizes downtime and ensures accessibility even in the event of hardware or software failures.

DocuWare uses consent management, encryption and data subject rights such as the right to access, rectify, or delete personal data and in compliance with regulations, it provides tools for managing data retention and deletion. DocuWare is SOC 2 certified. SOC (Service Organization Control) 2 defines the criteria for managing client data based on five trust service principles – security, availability, processing, integrity, confidentiality and privacy. While type I describes a vendor's systems and whether their design is suitable to meet relevant trust principles, type II details operational effectiveness of those system. SOC 3 on the other hand is the public declaration of SOC 2.

2.2 M-FILES

M-Files offers an innovative metadata-driven document management platform. M-Files gives midsize and enterprise businesses a leading edge. According to [18], M-Files is one of the most powerful document management software that seamlessly organizes and manages electronic documents and could be seen as one of the best DMS. It has a number of relevant features with a well-organized and intuitive dashboard. M-files been metadata-driven makes it more remarkable as observed by [19]. Metadata is described as data about data which means that descriptive data related to the context can be defined which is difficult in a traditional document management system.

M-files is compatible with major browsers with outstanding features such as robust search functionality where users can use customized search metadata to find contents, optical character recognition which makes searching possible beyond the metadata, automated workflow, versioning, electronic signature and top of it has offline access such that when internet access is restored, it synchronizes to the cloud.

M-files was founded in 1989 by its current CEO Antti Nivala as a solution to a market problem his father had uncovered with information management for his architectural engineering firm and at the moment with over 5000 customers and headquarters in Texas.

M-files prioritized information security and uses different mechanisms in achieving it. Confidentiality which is preserving authorized restrictions on access and disclosure as defined by Qadir & Quadri, (2016) is highly valuable aspect of information security. M-files ensures confidentiality by implementing robust access control and authentication mechanism using access control list (ACLs). Users can also set permissions based on user roles and responsibilities and uses document level encryption for files and encryption at rest and on transit. M-files uses AES-256 algorithm (compliant with FIPS 140-2 Standard) to protect data at rest and uses HTTPS, RPC and IPSec for data on transit [18]. M-Files supports authentication via any OAuth 2.0 compatible Identity Provider (IdP).

Integrity is also very critical in M-Files as it employs version control and audit trail functionalities whereas the version control keeps track of changes made to the document and allowing users to revert previous versions if necessary, audit trails record all activities related to documents which help to detect any unauthorized changes or tampering [19]. M-files like Docuware uses checksums and hash functions OF SHA-256 bit which generates a fixed-size hash value when data is uploaded which can be recalculated when data is retrieved in other to detect any changes or corruption in the data making it a very strong level of integrity.

M-Files prides itself with a high level of availability by minimizing system downtime both on it server and on the Azure datacenters where it is hosted. It uses a multi-server mode to create active cluster that serves as backup in case of maintenance or interruptions. The benefit of the Azure datacenter is that the network does not contain any single point of failure and potency is well monitored by additional technologies [20].

Along with many other security certifications, M-Files is both SOC 2 and SOC 3 certified, making it a step higher.

2.3 eFileCabinet

This is a top-rated document management software that meticulously organizes, secured and retrieves your documents [21]. As a leading document management system, it offers a number of features

such as file-sharing, workflow automation and full text search function and also support a number of industry specific features like compliance tools which makes it quite beneficial for the healthcare and finance industry. This means that eFileCabinet embeds a number of features that are handy to industries and can therefore seamlessly be integrated with other software platforms. Although it began as an internal product for the accounting firm where James Blaylock's worked and also the CEO, words spread quickly due to its numerous features and the demand grew. In response to this enormous demand this time not just from accounting related industry, eFileCabinet was officially founded in 2001to build upon, improve and market the software.

Depending on which version of the software you are using, eFileCabinet typically has 2-tier architectural system which comprises.

(1) Client Applications which is basically the web-based interface and desktop on premise application and (2) server infrastructure which comprises of its web servers which handle user request, database servers that stores document and metadata information about the file locations stored in database and storage servers which stores the actual documents on a network Attached device (NAS).

According to [21], eFileCabinet employs a holistic system to ensure maximum security which is a priority. As common with most document management system, eFileCabinet is no exception as it ensures confidentiality by implementing access control to ensure that only authorized users can access and use the system, encryption techniques are used to protect data by using SSL/TLS for document on transit and AES 256-bit as a standard on their data servers. While eFileCabinet did not publicly disclose the security system for maintaining document integrity, it however has version control to track changes made to your documents over time and audit trails that logs user's activities, document access, edits and deletions. Disaster recovery, redundancy and backup are done regularly to ensure data availability. It also makes use of failover systems by using multiple servers to avoid down times.

Earlier on in 2022, eFileCabinet achieves DOC 2 Type II certification set by the American Institute of Certified Public Accountants (AICPA) making it one of the few systems to be cleared of security threats by the body.

2.4 PandaDoc

PandaDoc is a complete suite document management automation software that makes the process of creating, approving and e-signing proposals, quotations, contracts etc. enabling teams to get more deals, create documents and be more predictable in their tasks [22].

PandaDoc as a DMS has a lots of built in features and allows integration with others systems. It allows for easier creation of documents, performs calculations such as taxes, automate workflows, real time tracking and auto reminders. PandaDoc also integrates with popular CRM applications such as Salesforce, HubSpot and Microsoft Dynamics, other DMS such as Google Drive and Box and productive apps such as Google Calendar and slack.

The PandaDoc architecture is multi-tiered into logical components (front-end, mid-tier, and database) each independently separated from each other on a demilitarized zone (DMZ) configuration which help to guarantee maximum protection, independence between lavers and additional securitv.

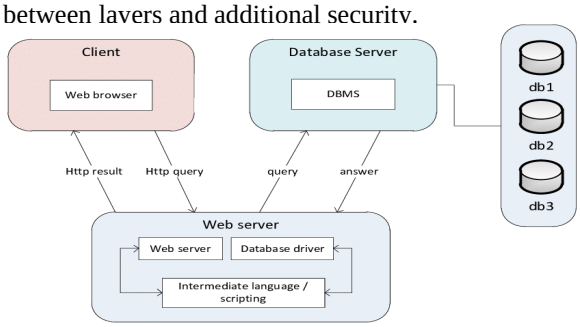

Figure 3: 3-tier Architecture [23]

PandaDoc like many other DMS ensures confidentiality through Role Based Access Control (RBAC), authentication and encryption both on transit and at rest. Using RBAC ensures that not everyone can perform the same role based on organizational demand. While using SSL/TLS for data on transit, it uses AES-256 alongside sophisticated encryption keys to protect data at rest [24].It employs the use of

standard data retention policy by allowing originations to define how long before a document is automatically deleted and document expiry within which a document can no longer be edited to safe guard the document and unauthorized use of outdated document. One amazing feature of PandaDoc is the secure collaboration which allows concerns parties to set key roles on documents without which it cannot be edited nor accessed. In other to maintain document integrity, PandaDoc stores documents alongside metadata and other activities of original files in different server locations when generating the requested documents such that metadata details will not be overwritten. The use of Amazon AWS infrastructure-as-a-service (IaaS) platform is a boost to their information availability. PandoDoc systems are monitored 24/7/365 days a year while critical alerts by these systems are escalated appropriately [21]. PandaDoc is SOC 2 Type 2 certified.

2.5 ZohoDocs

A statement from ZohoDcs defines it as an online document management system with built-in online editors to create and edit files. Like every other DMS, the general idea of ZohoDocs is that all your files can easily be accessed from any location or device. The word Zoho is actually tweaked as it comes from two - Small Office/Home Office which should be SOHO but for language reasons became known as Zoho [25].

ZohoDocs does not just allow you to create and share files but also to collaborate in real time and synchronize documents in other to keep focus on productivity. Although no mention on the kind of architecture used in ZohoDocs, it is most likely a 3-tier architecture due to its numerous app and integrations. It is offered as Software-as-a-service (SaaS).

ZohoDocs over twenty-five years of existence certainly may be a proof of great information security. ZohoDocs ensures confidentiality by a number of methods such as Access controls using password although not Role based in Nature, 2FA authentication and encryption both in motion and at rest.

Data at rest is encrypted using industry-standard AES-256. All customer data is encrypted in transit over public networks using Transport Layer Security (TLS) 1.2/1.3 with Perfect Forward Secrecy (PFS) to protect it from unauthorized disclosure or modification (Zoho, 2023). ZohoDocs currently uses in-house Key Management Service (KMS) as there are no provisions for users to upload their own keys.

With its version control policy which allows users to track changes made to document over time and the possibility to revert to the previous version if need be, audit trails through logging of activities in other to reduce the risk of document compromise, document locking to ensure that multiple users do not work on a document simultaneously and data validation to ensure the accuracy of the document and data hashing, ZohoDocs is able to protect document integrity. With adequate Load balancing helping to distribute networks on multiple network, use of multiple data centers in various countries which help to increase uptime even though no system has 100% uptime, proper failover mechanisms and proper surveillance and alerts, ZohoDocs maintains availability. ZohoDocs is SOC 2 type 2 compliant, ISO 27001, ISO 27017 and ISO 27018 certified, EU-U.S privacy shield compliant and in 2018, ZohoDocs was certified to be in compliance with General Data Protection Regulation (GDPR) which toughest privacy and security law in the world.

III. METHOD

This research used a qualitative review method in considering a number of information security metrics or features which make up for confidentiality, integrity, availability and compliance on the selected DMS. The use of qualitative research method allows us to search for primary evidence from different sources and through that draw a conclusion.

Firstly, selected document management systems were investigated from internet review websites and document management systems websites. In addition, we conducted a literature search on Google Scholar using the following search text:

1. Information security in Document management systems
2. Confidentiality, integrity and availability techniques in document management systems
3. Comparative review of document management systems

4. Encryption methods in document management systems

A total of 70 papers where collected based on the search texts above. Next, the literature obtained were filtered based on the following inclusion criteria:
"The paper employed an empirical research methodology"
"The paper should be published"
"The paper should be accessible"
"The paper should be published within the 10-year period (2013 – 2023)"

A total of 34 papers were excluded as they did not meet the criteria above.

Table 1 – Table of Database of selected paper

#	Digital Library	No of Journals/Article
1	ResearchGate	21
2	Google Scholar	9
3	ijcsma	4
4	Springer Open Access	2
TOTAL		36

The table above shows that majority of the review papers were gotten from ResearchGate which is a popular digital library and contributing 58% to the overall library followed by Google Scholar with 25%, ijcsma with 11% and Springer Open Access with 6%.

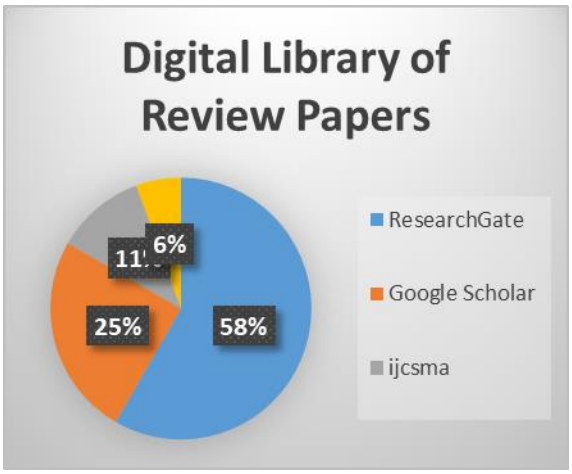

Figure 4 – Digital Library of review Papers

3.1 Analysis of Selected DMS based on Information Security Metrics

Based on information provided by the selected DMS websites, review website and research articles and close examination, we examined the selected DMS following the features that can be used to ensure information security as outlined by [26],[27] and seen in table 2 where "YES" means that the feature is available or implemented and "NO" means it was not implanted nor available.

Table 2: CIA-C elements of the selected DMS

INFORMATION SECURITY & COMPLIANCE																										
DMS	Confidentiality										Integrity					Availability						Compliance & Certification				
CIA-C Elements	Role Based	Authenticati	Encryption	Data	Secure	Data Expiry	2FA	User	Document	TLS/SSL	Hash	Version	Audit Trails	Digital	Logging	Intrusion	Regular	Multi-layer	Redundant	Load	Monitoring	SOC II Type	SOC 3	ISO	GDPR	EU-U.S.
eFile Cabinent	YES	YES	256-BIT	YES	NO	NO	YES	NO	YES	YES	SHA-2	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
M-FILES	YES	YES	256-BIT	NO	NO	YES	YES	NO	YES	YES	SHA-2	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
PandaDoc	YES	YES	256-	YES	YES	YES	YES	YES	YES	YES	SHA-	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO	YES	YES	YES

Zoho Doc	YES	YES	256-	NO	NO	NO	YES	NO	YES	YES	SHA-	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO	YES	YES	YES
Docu Ware	YES	YES	256-	YES	NO	YES	YES	NO	YES	YES	SHA-	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES

IV. RESULTS AND DISCUSSION

The result in figure. 5 revealed that PandaDoc achieved the highest CIA-C percentage score because of features such as user education, secure collaboration, Data Retention Policy, and EU-U. S security compliance.

Again, in figure 6, PandaDoc had 25 out of the 26 metrics or features for implementing CIA-C, eFileCabinet has 23 making it the second most second secured system of the five selected DMS.

The Secure hash Algorithm (SHA-2) was used in maintaining the integrity (trustworthiness, accuracy and consistency) of all systems because it offers a better security over other kinds of hashing algorithms. Features such as logging, digital signature, version control and audit trails improved the integrity of the various systems.

The availability of a system which is simply the ability to make information or documents and other related physical and logical resources accessible as needed, when needed, and where they are needed as defined by [5] was tackled using a number of attributes such as instruction detection system, regular backup, use of multi-servers etc.

User education is very important as [28] outlined that *in 2014 IBM reported that 95% of all security incidence involves human error and that most of the successful security attacks prey on the weakness of human and sabotage within the organization*. The use of weak passwords by users, use of public computers and poor firewall and other security measures are a soft target for intruders. These has promoted attacks such as spoof attack where deceptive messages are sent to unsuspecting users and then through users' action, gain access to sensitive information, MITM attack and many others. [28] Suggested that a solid information policy and constant user education should be conducted to keep users abreast of new threats and how not to fall prey. This is what PandaDoc has prioritized.

Secure collaboration which is "people's security" which basically means that security is in the hands of a group of persons or parties [29]. Secure collaboration slows down major attacks because of the variety of access level that is needed. In the case of PandaDoc, two or more users can set joint security access to a file or document instead of just an individual. This should be a model to beef up security in not just document management systems but similar systems.

The time a document should be stored, if not accessed contributes to information security. Data retention policy tells which data will be achieved, how long will it be kept and what happens at the end of retention period. Proper retention policy ensures document consistency, reliability and integrity [30].

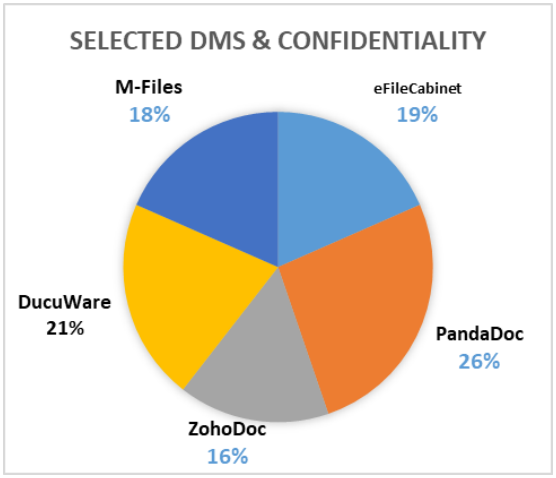

Figure 5: Information Confidentiality among selected DMS

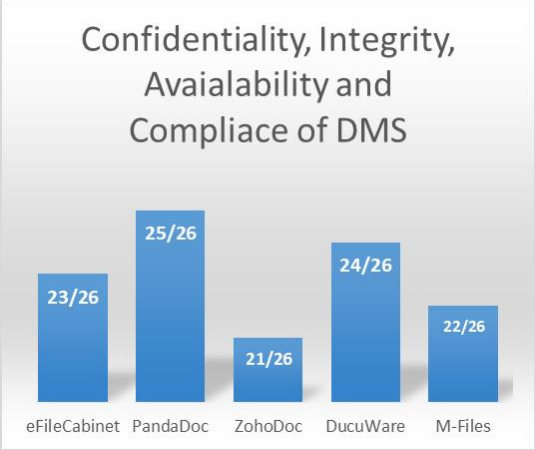

Figure 6: score Index for selected DMS

CONCLUSION

In this study, all five leading DMS compared has some level of information security although some did better than others. However, in terms of encryption techniques for data at rest and on transit, they all used the Advanced Encryption Algorithm (AES) with 256-bit and TLS/SSL respectively. This is the state-of-the-art security technique adopted by all five systems.

PandaDoc is the most secured system based on this comparative analysis haven scored more than other systems. Notwithstanding, information security is an unending task and as such will recommend for future works that a zero-knowledge security measure be undertaken by all DMS in a user related approach such that the entire life cycle of the system is secured while constant training and retraining of users and teams are regularly carried out.

REFERENCES

[1] S. Jordan, S. S. Zabukovšek, and I. S. Klančnik, "Document Management System – A Way to Digital Transformation," *Naše gospodarstvo/Our economy*, vol. 68, no. 2, pp. 43–54, 2022, doi: 10.2478/ngoe-2022-0010.

[2] H. S. Ahmad, I. M. Bazlamit, and M. D. Ayoush, "Investigation of Document Management Systems in Small Size Construction Companies in Jordan," in *Procedia Engineering*, Elsevier Ltd, 2017, pp. 3–9. doi: 10.1016/j.proeng.2017.03.101.

[3] A. A. Kayode, B. M. Lawan, I. A. Ajadi, and J. A. Lukman, "E-Government, Information and Communications Technology Support and Paperless Environment in Nigerian Public Universities: Issues and Challenges," *Journal of Technology Management and Business*, vol. 7, no. 1, 2020, doi: 10.30880/jtmb.2020.07.01.006.

[4] "Report for Market Research of Document Management Solutions - Pericent." Accessed: Aug. 25, 2023. [Online]. Available: https://www.pericent.com/resources/market-analysis-report/

[5] S. Qadir and S. M. K. Quadri, "Information Availability: An Insight into the Most Important Attribute of Information Security," *Journal of Information Security*, vol. 07, no. 03, pp. 185–194, 2016, doi: 10.4236/jis.2016.73014.

[6] V. Kostoglou, J. Papathanasiou, and D. Petkos, "A comparative analysis of cloud computing services using multicriteria decision analysis methodologies. International Journal of Information and A comparative analysis of cloud computing services using multicriteria decision analysis methodologies Jason ," vol. 7, no. April 2015, pp. 51–70, 2013.

[7] S. Yaqub, I. Sattar, N. Manzoor, and S. Ashraf, "Cloud Service Providers: A Comparative Analysis of Cloud Storage Pricing," *International Journal of Computer Applications*, vol. 162, no. 1, pp. 22–26, 2017, doi: 10.5120/ijca2017913211.

[8] S. Kim, H. Choi, N. Kim, E. K. Chung, and J. Y. Lee, "Comparative analysis of manuscript management systems for scholarly publishing," *Science Editing*, vol. 5, no. 2, pp. 124–134, 2018, doi: 10.6087/KCSE.137.

[9] L. Parra, S. Sendra, S. Ficarelli, and J. Lloret, "Comparison of Online Platforms for the Review Process of Conference Papers," *CONTENT 2013 The Fifth International Conference on Creative Content Technologies*, no. c, pp. 16–22, 2013.

[10] I. Shaikh, P. Bafna, and S. R. Lahane, "File Sharing System," *International Journal of Scientific and Research Publications*, vol. 3, no. 6, 2013.

[11] J. M. C. Hernad and C. G. Gaya, "Methodology for implementing Document Management Systems to support ISO 9001:2008 Quality

Management Systems," *Procedia Engineering*, vol. 63, pp. 29–35, 2013, doi: 10.1016/j.proeng.2013.08.225.

[12] R. K. C. Chien Hua Wu, Da Wei Wang, "A Study of Secure Document Sharing System for Electronic Medical Records," *International Journal of Engineering Research and Technology (IJERT)*, vol. 5, no. 2, 2016.

[13] Y. Turgut, "A Comparative Analysis of University Information Systems within the Scope of the A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks," *Tem*, vol. 5, no. 2, pp. 180–191, 2016, doi: 10.18421/TEM52-10.

[14] K. Latha, B. Gowsalya, and B. Kannega, "Procuring the Dropbox using honey encryption technique," *Applied Mechanics and Materials*, vol. 573, no. June 2014, pp. 523–528, 2014, doi: 10.4028/www.scientific.net/AMM.573.523.

[15] A. Odeh, S. R. Masadeh, A. Azzazi, and C. Information, "A Performance Evaluation of Common Encryption Technique with secure watermark system (SWS)," vol. 7, no. 3, pp. 31–38, 2015.

[16] N. R. Salunke, "Files Storage & Sharing Platform Using Cloud," *International Journal for Research in Applied Science and Engineering Technology*, vol. 9, no. 11, pp. 1338–1344, 2021, doi: 10.22214/ijraset.2021.38994.

[17] A. Wicaksana and T. Rachman, "What is Docuware?," Angewandte Chemie International Edition, 6(11), 951–952. [Online]. Available: https://medium.com/@arifwicaksanaa/pengertian-use-case-a7e576e1b6bf

[18] S. Peek, "M-Files Review and Pricing." [Online]. Available: https://www.business.com/reviews/m-files-dms-document-management-software/

[19] H. Asılı and O. O. Tanrıover, "Comparison of Document Management Systems by Meta Modeling and Workforce Centric Tuning Measures," *International Journal of Computer Science, Engineering and Information Technology*, vol. 4, no. 1, pp. 57–67, 2014, doi: 10.5121/ijcseit.2014.4106.

[20] "Platform Security | M-Files." Accessed: Sep. 20, 2023. [Online]. Available: https://www.m-files.com/products/platform-security/

[21] Curtis Nash, " eFileCabinet Security & Backup." Accessed: Sep. 21, 2023. [Online]. Available: https://support.efilecabinet.com/hc/en-us/articles/360037987892-FAQ-Security-Backup

[22] Laila Belali, "PandaDoc: what it is used for and main features." Accessed: Sep. 21, 2023. [Online]. Available: https://www.occamagenciadigital.com/en/blog/pandadoc-what-is-it-for-and-principal-features

[23] Jose Melo, "The 3-tier architecture | Download Scientific Diagram." Accessed: Sep. 21, 2023. [Online]. Available: https://www.researchgate.net/figure/The-3-tier-architecture_fig22_260389483

[24] "PandaDoc Security: Physical, Data, and User Security - PandaDoc." Accessed: Sep. 21, 2023. [Online]. Available: https://www.pandadoc.com/security/

[25] Zoho, "Introduction about Zoho Docs." Accessed: Jun. 14, 2023. [Online]. Available: https://www.zoho.com/docs/help/about-zoho-docs.html

[26] S. Samonas and D. Coss, "THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY".

[27] R. Brooks, "The CIA Triad and Real-World Examples," *https://blog.netwrix.com/*, 2023.

[28] P. Kwaku, D. Keddy, and E. Nii, "Importance of Information Security Education and Awareness in Ghana," *Communications on Applied Electronics*, vol. 6, no. 6, pp. 30–35, 2017, doi: 10.5120/cae2017652479.

[29] Y.-H. Chang, "Yu-Hsuan Chang. A Study of Document Sharing and Managing Behaviors in Cloud Storage. A STUDY OF DOCUMENT SHARING AND MANAGING BEHAVIORS IN CLOUD STORAGE," 2013.

[30] Edward Vesely, "The Importance of a Document Retention Policy - Lighthouse Services." Accessed: Oct. 18, 2023. [Online]. Available: https://www.lighthouse-services.com/newsletters/the-importance-of-a-document-retention-policy/