World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Systematic literature review on 'secure document management systems (DMS)'

Firoz Mohammed Ozman *

Solutions Architect, Enterprise Architecture, Anecca Ideas Corp, Toronto, Canada.

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(01), 1460-1469

Publication history: Received on 12 February 2025; revised on 23 March 2025; accepted on 26 March 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.1.0146

Abstract

This study has explored the implementation optimization in designing a secure document management system that addresses the challenges of individual transformation and operational efficiency. This systematic literature review describes secure Document Management Systems (DMS) architecture, challenges, and best practices. The systematic literature review methodology, guided by the PRISMA framework, is used in this review. Among them, 20 peer-reviewed articles were analyzed to investigate the advancement of DMS. It outlines advancements in security features and the gaps identified in the peer-reviewed literature using a PRISMA-guided methodology. Findings identify critical strategies for increasing DMS reliability and user trust.

The study has effectively highlighted the importance of adaptable and scalable systems directly allied with an organization's digital maturity. The research has focused on understanding the role of DMS in enabling digital transformation while enhancing operational efficiency and ensuring resonance against cyber security risks. The findings have provided actionable insights into how the organization aims to implement future-ready DMS to meet the solutions and the demand of rapidly digitizing. This systematic literature review describes secure Document Management Systems (DMS) architecture, challenges, and best practices. It outlines advancements in security features and the gaps identified in the peer-reviewed literature using a PRISMA-guided methodology. Findings identify critical strategies for increasing DMS reliability and user trust.

Keywords: Secure; DMS; Document; Collaboration; Management; Encryption; Compliance

1. Introduction

The increasing form of digitalization in the organizational operation has significantly transformed the document management system by making it one of the most famous tools in today's business landscape. A secure document management system plays an important role in storing, retrieving, and sharing critical information in the dynamic business world, ensuring the integrity and accessibility of the documents. The organization today is handling an increasing volume of sensitive data, with the need for security measures in DMS, has become more pressing. The traditional paper-based method is not applicable as it leads to specific manual errors and risks of physical damage and inefficiency. The change of digitalization and its transformation in every organization has led to the adoption of cloud-based an, advanced digital system where it focuses on implementing security features like multi-factor authentication encryption and security cloud storage.

Integrating artificial intelligence data mining and cloud computing has effectively transformed DMS while enhancing its efficiency and security (Xing, 2024). Digital documents' security is a critical concern, particularly with the rise of cybercrime, which has consequently focused on seeking solutions with offerings like encryption and secure cloud storage (Syamsuddin and Yunianta, 2022). However, this systematic literature review has focused on evaluating the

* Corresponding author: Firoz Mohammed Ozman

impact of secure data management systems in today's world while ensuring the safety of sensitive documents in the evolving technological landscape.

1.1. Problem Statement

The problem statement that has been focused on in this SLR is that although DMS provides numerous benefits with the ongoing concerns related to cyber-attack vulnerability, it includes data breaches and unauthorized access (Ikuomola et al., 2022). Moreover, integrating various security protocols within the existing system makes every organization unit's implementation challenging. This research will focus on understanding the problem related to DMS with the emerging technology that makes it difficult for organizations to adopt per the change in digital transformation.

Therefore, understanding the limitations of the current DM's solutions and identifying the factors focused on influencing their security is essential for improving their reliability and effectiveness in securing sensitive documents.

1.2. Research Aim

The primary aim of the research is to explore the design and implementation of secure document management systems and identify strategies for enhancing the organization's security system.

Objectives

- To understand the current landscape, delete the secure DMS and analyze the security protocols implemented within this system.
- To explore the challenges and limitations related to the existing DMS.
- To investigate the role of emerging technologies concerning the enhancement of DMS security.
- To provide a Framework for designing and implementing a secure DMS that is directly aligned with the dynamic business world and digital transformation.

1.3. Significance

The study's primary significance addresses the growing concern about data security within the document management system. This research is beneficial as it focuses on handling sensitive data of business and government institutions, where it is important to implement robust security measures to protect the documents from cyber threats (Ikuomola et al., 2022). By effectively investigating the role of emerging technology in enhancing DMS security, this research will focus on providing valuable insight while designing the security system that supports the digital transformation of the companies. Additionally, the findings will assist in improving the organization's efficiency while directly streamlining the document management process to maintain a high level of security.

1.4. Research Gap

The main research gap focused on this research is the evaluation of DMS's functionality, performance, and usability. Further, integrating emerging technology to enhance security has not been adopted adequately or explored. Earlier in the past research, only the security challenges have been focused on DMS, but it has not examined the role of technology in improving these security issues. To reduce this research, the SLR will focus on exploring how this technology can be effectively implemented in the context of digital transformation efforts in organizations.

2. Literature Review

2.1. Overview of Secure Document Management Systems

Digital management related to documents has become one of the core elements of modern organizations, providing advantages in terms of efficiency, accessibility, and collaboration. However, in terms of security, digital documents have remained one of the most pressing concerns for the organization as it faces increasing cyber threats. A document management system is a software solution that allows organizations to track and manage in-store shared electronic documents. Over the years, this system has evolved as per the organization's changing needs, along with understanding and integrated modes of stated technology such as artificial intelligence cloud computing to improve document accessibility and management efficiency (Javed et al., 2024). The secure DMS have ensured that the documents remain confidential and only accessible to authorized individuals. With the increasing rise of digitalization, secure DMS has become essential for industries like finance, healthcare and government, where protecting sensitive data is paramount.

With the rise of digitalization and secure DMS, it has become essential for industries to implement protection against sensitive data. As organizations have evolved towards digital document management, the main emphasis has shifted from simply storing and managing documents to securing them against unauthorized access.

2.2. Security Protocols in Document Management Systems

The document's security is fundamental in DMS as the organization implements various security protocols, including multi-factor authorization access control and encryption integrated into DMS for protecting sensitive information (Jordan et al., 2022). With the help of an encryption technique, it ensures the document remains unreadable concerning unauthorized access. In contrast, the access control mechanism tends to restrict user permission based on the roles within the organization.

Research by Mikl et al. (2021) has highlighted the importance of rule-based access control in effectively managing the user's excess of the document. This system ensures that individuals and those with appropriate authorization focus on accessing certain documents or performing specific actions that reduce the risk of internal data breaches. Moreover, the use of multi-factor authentication is another level of security that requires the user to help them with additional forms of verification set, including the one-time password for regular credential updates. Despite these security measures, vulnerability has remained one of the challenging factors of DMS, particularly with the rise of cyber-attacks. Improving continuously and ensuring that acids are secured to protocols to stay ahead while evolving threats is important.

2.3. Challenges and Limitations of Existing DMS

DMS has offered a range of security features but does not offer them without issues. One of the primary issues is the scalability of this system, which allows the organization to grow and accumulate more data. It has become difficult for DMS to handle large volumes of data without compromising security (Logeshwaran, 2022). It has been observed that Day In has struggled to scale effectively, leading to issues such as slow document retrieval and difficulty in managing the large data set.

Another major challenge is implementing DMS with other organizational systems. For example, integrating DMS with existing enterprise resources planning solutions or custom relationship management is very complex (Zabukovšek et al., 2023). It mainly requires custom solutions and increases the system's potential vulnerability.

2.4. Role of Emerging Technologies in DMS Security and Current Design

The emerging technology in DMS security has played an important role, as cloud computing has allowed organizations to store documents in a secure and flexible environment while making document management more cost-effective (Mikl et al., 2021). However, using cloud-based DMS has caused concerns about data privacy and security.

This approach has offered the benefits of cloud storage, which is currently used by most organizations while ensuring critical documents are kept in a secure environment. Data mining techniques have effectively been applied to improve document retrieval and management. By analyzing the last data set, these techniques focus on identifying the patterns and trends related to the organization and optimizing and accessing the security protocols.

2.5. Theory: Information security control theory

The information security control theory has mainly focused on understanding the presentation of security measures, which are the information assets concerning unauthorized access and destruction. It has effectively implemented security controls such as access control authentication mechanisms and encryption, which are essential for safeguarding the digital documents within the DMS. The theory has advocated and helped understand the technical and security approach, ensuring comprehensive protection. It has also highlighted the importance of continuous monitoring risk assessment along with the help of regulatory frameworks that would address the emerging security threat. Active security management has effectively supported the theory to mitigate vulnerabilities and ensure data integrity.

3. Methodology

This systematic literature review adopts an appropriate methodology to investigate all Secure Document Management Systems (DMS) aspects. It is divided into four subsections: search strategy, inclusion and exclusion criteria, time horizon, and the PRISMA framework.

3.1. Search strategy

The qualitative strategy has been adopted, and different keywords have been used to apply Boolean operators. In order to maximize the retrieval of high-quality and relevant literature from known academic sources, a search strategy was developed to search the IEEEXplore, SpringerLink, PubMed, Scopus, and Web of Science. Some example keywords found were 'secure document management systems,' 'DMS security challenges,' 'DMS best practices,' and 'data protection in DMS,' and these were used with the Boolean operators (AND, OR) to refine results. Searches were restricted to peer-reviewed journal articles, conference papers, and high-impact publications to impose academic priorities. The technical report was included to pick up on practical realizations of DMS.

3.2. Exclusion and inclusion criteria

Inclusion and exclusion criteria were defined to ensure relevance and quality.

- Articles were included if they:
- Secure DMS or its implementation focused.
- Discussed security challenges, security solutions, and DMS new technologies.
- Were published in English.
- Within the defined time horizon, the publication dates.

Articles were excluded if they:

- Lacked peer review.
- It is solely focused on non-secure or legacy DMS systems.
- They were opinion pieces or editorials with no 'empirical evidence.'
- Based on pilot searches, inclusion and exclusion criteria were iteratively refined to reconcile with the study purpose.

Table 1 Exclusion and Inclusion Criteria

Criteria	Inclusion	Exclusion
Focus	Secure DMS or their implementation	Non-secure or legacy DMS systems
Content	Security challenges, solutions, or emerging technologies in DMS	Opinion pieces or editorials with no empirical evidence
Peer Reviewed	Articles subjected to peer review	Articles lacking peer review
Language	Published in English	Non-English publications
Publication Date	Within the defined time horizon	Outside the defined time horizon

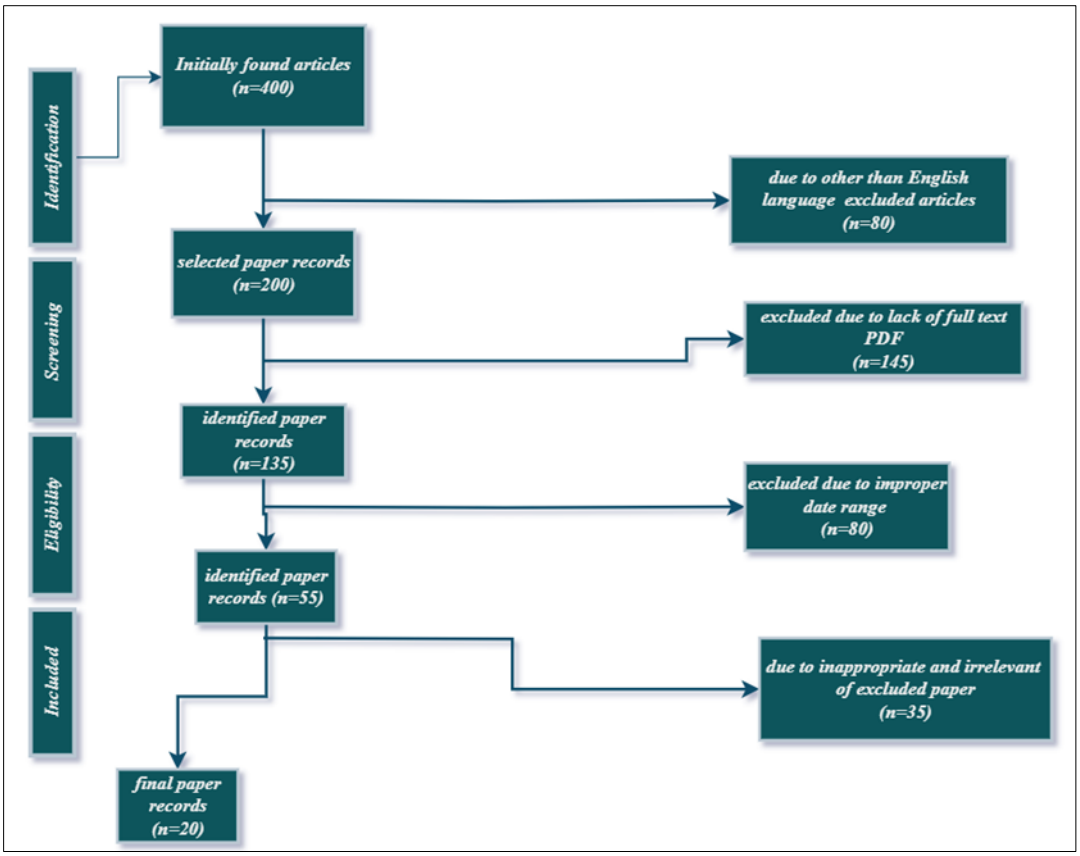
(Source: Self-Developed)

3.3. Time Horizon

A review of the literature published over the last five years was conducted to capture developments in secure DMS technology and practices. The timing balances the need for historical context with a focus on current development. Only studies older than five years were included if they provided seminal insights into the foundational concepts of secure DMS.

3.4. Prisma

In order to enhance translucence and reproducibility, the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework was used. The PRISMA flow diagram documented the process, including identification, screening, eligibility, and inclusion of studies. Based on database searches, initial records were identified in the first 400. Two hundred records were screened based on titles and abstracts, leaving 55 full-text articles to assess for eligibility after duplicate removal. Twenty studies were included in the qualitative synthesis. The PRISMA framework ensured a systematic approach to avoid bias and raise the review's credibility.



(Source: Self-Developed)

Figure 1 PRISMA Framework

4. Result and Analysis

4.1. Security Mechanisms in DMS

The results from the literature review and the above study for the secure document management system are directly linked with the result objective, emphasizing the advance in various spheres. With integrating security mechanisms that include rule-based access control, blockchain technology and encryption have effectively emerged as cornerstones for the secure DMS. For instance, Ikuomola et al. (2022) have focused on the effectiveness of the cloud-based system, which has enhanced encryption to safeguard sensitive information systems. Similarly, Xing (2024) highlights the role of recommendation in ensuring an algorithm while effectively ensuring secure access to documents and minimizing the risk of authorized access.

Concerning blockchain technology, data integrity and transparency are the significant aspects that have evolved as a privacy-preserving system for data management (Azbeg et al., 2022). With a secure DMS, it is scalable and focuses on the organization's growing demand. It has been observed that advanced communication management techniques have been supported by ultra-dense cloud systems and ensure proper scalability without compromising the security factor. Zabukovšek et al. (2023) have argued that DMS has the organization of digital maturity, which is important for the successful implementation of digital transformation that effectively highlights the need for using adaptable systems to integrate new technology.

4.2. Enhancing Operational Efficiency

Operational efficiency is one of the key factors that has evolved from the articles, which observed that it is driven by automation and intelligence systems focused on DMS. The determining technique has been important in optimizing the document workflow by enabling the less information system and its retrieval. Buctuanon et al. (2021) have effectively emphasized the application of rule-based pattern recognition, which has improved document classification in cloud-based DMS. Additionally, machine learning algorithms and artificial intelligence have facilitated predictive analytics while ensuring more accurate and faster document retrieval (Mikl et al., 2021). Compliance with the regulatory

framework, such as GDPR, effectively focuses on implementing modern DMS. The usability features in the system, like DocManS, have effectively aligned with the legal requirement while improving the user experience.

4.3. Addressing Emerging Cyber Threats

The articles indicate that cyber threats are required for protective measures in DMS design. Alouffi et al. (2021) have focused on the importance of layered security strategies with physical control and technical administration. Additionally, these systems have integrated DMS files, enhancing the overall residence of the document and its management infrastructure. Security DMS played an important role in enabling digital transformation. Zabukovšek et al. (2023) have effectively imposed upon managing the DMS life cycle to ensure the alignment with organizational goals. These findings have effectively demonstrated that DMS improves the document's security and catalyzes broad organizational changes.

Overall, the implementation of security has not only provided various benefits to the organization but has also incorporated advanced security systems and scalability features, which address the critical need for efficient and secure document management. These systems are directly connected with organizational goals and the regulatory environment while ensuring resilience against cyber threats.

5. Conclusion

This systematic literature review illustrates the advancements and open issues in secure Document Management Systems. Advanced security features, such as encryption, role-based access control, and audit trails, have been part of DMS for many years and significantly enhance its capability to protect sensitive information. However, vulnerabilities persist due to new cybersecurity threats, rapidly changing technology, and the complexity of user adoption. Many organizations depend on DMS to handle critical documents, and DMS systems must address the complete spectrum of security and usability issues.

A DMS offers a secure means for the safe storage, access, and collaboration of sensitive information. Data at rest and in transit are protected using encryption; no unauthorized access is permitted. A classic role-based access control provides document access for accredited users, and audit trails track activities for responsibility. It is integrated with multi-factor authentication (MFA) to provide extra security. Along with automatic backups, disaster recovery tools, and compliance with things like GDPR or HIPAA, secure DMS solutions are those.

This review finds that DMS could benefit from integrating cutting-edge technologies such as blockchain and artificial intelligence (AI) to increase its security and scalability. However, despite these efforts, gaps were identified in current research on user-centred design, compliance with the evolving regulatory framework and how to prevent insider threats. User education and engagement are rate-limiting steps for bridging the gaps and creating trust in DMS security protocols. In today's modern world, document management has found secure DMS to play an integral role in technical progress as it must also be implemented in the practical aspect of the job. Organizations can build DMS that are robust and reliable with future security demands by considering both technical vulnerabilities and human-centric challenges. The artifacts laid a robust foundation for further research and practical developments in the field.

Recommendations

Based on the findings of this review, several recommendations are proposed to enhance the security and effectiveness of Document Management Systems (DMS):

- ***Adoption of Advanced Technologies:*** Organisations should integrate blockchain and AI for tamper-proof data storage, real-time threat detection, and anomaly analysis.
- ***User-Centric Design:*** Developers should focus on creating user-friendly interfaces and training programs that ease compliance with security protocols. By enhancing user awareness, people can reduce the chance of human error, which is one of DMS's common vulnerabilities (Javed et al., 2024).
- ***Regulatory Compliance:*** Since DMS is such an integral part of an organization's information management, organizations must ensure that the DMS they use adheres to global data protection standards like the GDPR, HIPAA, and ISO 27001. People must audit regularly and update control and security policies to comply with continually changing regulations (Mikl et al., 2021).
- ***Comprehensive Monitoring and Incident Response:*** Advanced logging and monitoring tools help detect and mitigate threats in real-time. Incident response plans should be regularly updated and tested to address emerging risks (Jordan et al., 2022).

If an organization implements these recommendations, it will increase the security, dependability, and trustworthiness of its DMS so that it can meet today's and future problems.

References

[1] Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D.E.A., Bajaj, M., Blazek, V. and Prokop, L. (2024). Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. Results in engineering, p.102647. https://doi.org/10.1016/j.rineng.2024.102647

[2] Al Mamun, A., Azam, S. & Gritti, C. (2022). Blockchain-based electronic health records management: a comprehensive review and future research direction. IEEE Access, 10, pp.5768–5789. https://ieeexplore.ieee.org/abstract/document/9673752/

[3] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H. and Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. Ieee Access, 9, pp.57792-57807. https://ieeexplore.ieee.org/abstract/document/9404177/

[4] Alsoufi, M.A., Razak, S., Siraj, M.M., Nafea, I., Ghaleb, F.A., Saeed, F. & Nasser, M. (2021). Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review. Applied Sciences, 11(18), p.8383. https://doi.org/10.3390/app11188383

[5] Azbeg, K., Ouchetto, O. and Andaloussi, S.J. (2022). Access control and privacy-preserving blockchain-based system for disease management. IEEE Transactions on Computational Social Systems, 10(4), pp.1515-1527. https://ieeexplore.ieee.org/abstract/document/9819963/

[6] Buctuanon, M. M., Gadiane, J. L. A., Margallo, F. A., and Lucero, P. R. (2021). Incorporating Rule-based Pattern Recognition Approach for Document Structure Classification on Cloud-based Document Management System. Mindanao Journal of Science and Technology, 19(2).https://mjst.ustp.edu.ph/index.php/mjst/article/download/999/189

[7] Ikuomola Aderonke Justina, Oyekan, E.A. & Orogbemi, Olutomisin M (2022). A Secured Cloud-Based Electronic Document Management System. International Journal of Innovative Research and Development. [online] doi: https://doi.org/10.24940/ijird/2022/v11/i12/dec22010.

[8] Iqbal, N., Jamil, F., Ahmad, S. and Kim, D. (2021). A novel blockchain-based integrity and reliable veterinary clinic information management system using predictive analytics for the provisioning of quality health services. Ieee Access, 9, pp.8069-8098. https://ieeexplore.ieee.org/abstract/document/9314077/

[9] Javed, M. A., Alam, M., Alam, M. A., Islam, R., and Ahsan, M. N. (2024). Design and Implementation of Enterprise Office Automation System Based on Web Service Framework and Data Mining Techniques. Journal of Data Analysis and Information Processing, 12(4), 523-543. https://doi.org/10.4236/jdaip.2024.124028

[10] Jordan, S., Zabukovšek, S.S. and Klančnik, I.Š. (2022). Document Management System – A Way to Digital Transformation. Our Economy Journal of Contemporary Issues in Economics and Business, [online] 68(2), pp.43–54. Doi:.

[11] Logeshwaran, J. (2022). The control and communication management for ultra dense cloud system using fast Fouranlultra-gorithm. ICTACT Journesoa n Data Science and Machine Learning, 3(2), 281–284. https://www.researchgate.net/profile/Jaganathan-Logeshwaran/publication/363332677_The_control_and_communication_management_for_ultra_dense_cloud_system_using_fast_Fourier_algorithm/links/63180e2961e4553b956eaa70/The-control-and-communication-management-for-ultra-dense-cloud-system-using-fast-Fourier-algorithm.pdf

[12] Mikl, J., Herold, D. M., Ćwiklicki, M., and Kummer, S. (2021). The impact of digital logistics start-ups on incumbent firms: a business model perspective. The International Journal of Logistics Management, 32(4), 1461-1480. https://doi.org/10.1108/IJLM-04-2020-0155

[13] Ng, K.K., Chen, C.H., Lee, C.K., Jiao, J.R. and Yang, Z.X. (2021). A systematic literature review on intelligent automation: Aligning concepts from theory, practice, and future perspectives. Advanced Engineering Informatics, 47, p.101246. https://doi.org/10.1016/j.aei.2021.101246

[14] Syamsuddin, I., and Yunianta, A. (2022). Design and usability assessment of DocManS: A document management system with security and social media features. International Journal of Advanced and Applied Sciences, 9(1).https://doi.org/10.21833/ijaas.2022.01.007

[15] Tariq, U., Ahmed, I., Bashir, A.K. & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review. Sensors, 23(8), p.4117. https://doi.org/10.3390/s23084117

[16] Votto, A.M., Valecha, R., Najafirad, P. and Rao, H.R. (2021). Artificial intelligence in tactical human resource management: A systematic literature review. International Journal of Information Management Data Insights, 1(2), p.100047. https://doi.org/10.1016/j.jjimei.2021.100047

[17] Wang, T., Zhang, Y., Qi, S., Zhao, R., Xia, Z. & Weng, J. (2024). Security and privacy on generative data in aigc: A survey. ACM Computing Surveys, 57(4), pp.1–34. https://doi.org/10.1145/3703626

[18] Xing, L. (2024). Research on secure Official Document Management and Intelligent Information Retrieval System based on recommendation algorithms. International Journal of Intelligent Networks. [online] doi:https://doi.org/10.1016/j.ijin.2024.02.003.

[19] Zabukovšek, S.S., Jordan, S. and Bobek, S. (2023). Managing Document Management Systems' Life Cycle in Relation to an Organization's Maturity for Digital Transformation. Sustainability, [online] 15(21), pp.15212–15212. doi:https://doi.org/10.3390/su152115212 .

[20] Zubaydi, H.D., Varga, P. and Molnár, S. (2023). Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: A systematic literature review. Sensors, 23(2), p.788. https://doi.org/10.3390/s23020788

Appendix

- Systematic Literature Review Table

Topic	**DOI**	**Authors**	**Codes/Themes**	**Key Findings**	**Recommendations**
Enterprise Office Automation System	https://doi.org/10.4236/jdaip.2024.124028	Javed, M. A., Alam, M., Alam, M. A., Islam, R., Ahsan, M. N.	Web service framework, Data mining techniques	Web service frameworks enhance office automation, improve productivity and decision-making.	Implement robust data mining models for efficient system performance.
Impact of Digital Logistics Start-ups	https://doi.org/10.1108/IJLM-04-2020-0155	Mikl, J., Herold, D. M., Ćwiklicki, M., Kummer, S.	Business models, Digital logistics, Incumbent firms	Digital start-ups disrupt traditional logistics, reshaping business models.	Established firms should adopt digital innovations to remain competitive.
Cloud-based Electronic Document Management System	https://doi.org/10.24940/ijird/2022/v11/i12/dec22010 .	Ikuomola Aderonke Justina, Oyekan, E.A., Orogbemi, Olutomisin M.	Cloud computing, Security, Document management	Cloud systems offer improved access, storage, and security for document management.	Further improve security protocols and enhance user interfaces.
Document Management System and Digital Transformation	https://doi.org/10.2478/ngoe-2022-0010 .	Jordan, S., Zabukovšek, S.S., Klančnik, I.Š.	Digital transformation, Document management	Effective document management is crucial for digital transformation in organizations.	Focus on scalability and adaptability for evolving digital needs.
Secure Official Document Management and Intelligent Information Retrieval	https://doi.org/10.1016/j.ijin.2024.02.003 .	Xing, L.	Secure document management, Intelligent retrieval	Intelligent systems can enhance the retrieval and security of official documents using recommendation algorithms.	Develop intelligent retrieval algorithms to improve document access speed and accuracy.
Pattern Recognition for	https://mjst.ustp.edu.ph/index.php/mjst/articl	Buctuanon, M. M., Gadiane, J. L. A.,	Rule-based pattern recognition,	Rule-based patterns aid in efficient document	Incorporate advanced machine learning models to

Document Classification	e/download/999/189	Margallo, F. A., Lucero, P. R.	Cloud-based system	classification in cloud-based systems.	enhance classification accuracy.
Document Management Systems' Life Cycle in Organizations	https://doi.org/10.3390/su152115212 .	Zabukovšek, S.S., Jordan, S., Bobek, S.	Document lifecycle, Organizational maturity	Managing document systems' life cycle is essential for digital transformation in mature organizations.	Prioritize lifecycle management in organizations' digital transformation strategies.
Cloud System Control and Communication Management	https://www.researchgate.net/profile/Jaganathan-Logeshwaran/publication/363332677_The_control_and_communication_management_for_ultra_dense_cloud_system_using_fast_Fourier_algorithm/links/63180e2961e4553b956eaa70/The-control-and-communication-management-for-ultra-dense-cloud-system-using-fast-Fourier-algorithm.pdf	Logeshwaran, J.	Cloud systems, Communication management, Fast Fourier	Fast Fourier algorithms improve control and communication management in ultra-dense cloud systems.	Optimize algorithms for real-time performance in cloud management.
Design and Usability of DocManS: A Document Management System	https://doi.org/10.21833/ijaas.2022.01.007	Syamsuddin, I., Yunianta, A.	Security, Usability, Social media features	The design of DocManS offers strong security and integrates social media for efficient document management.	Improve user training and the integration of social media features for broader use.
Artificial Intelligence in Human Resource Management	https://doi.org/10.1016/j.jjimei.2021.100047	Votto, A.M., Valecha, R., Najafirad, P., Rao, H.R.	Artificial intelligence, Human resource management	AI enhances HR processes, improving efficiency and decision-making.	Incorporate more AI-driven tools for talent management and prediction models.
Cloud Computing Security: Threats and Mitigation Strategies	https://ieeexplore.ieee.org/abstract/document/9404177/	Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., Ayaz, M.	Cloud computing security, Threat mitigation	Security threats in cloud computing demand continuous updates to security measures and frameworks.	Strengthen encryption and continuous monitoring systems.
Intelligent Automation in Industry	https://doi.org/10.1016/j.aei.2021.101246	Ng, K.K., Chen, C.H., Lee, C.K., Jiao, J.R., Yang, Z.X.	Intelligent automation, Industry applications	Intelligent automation streamlines operations but requires alignment	Establish clear frameworks for implementing automation in industry.

				between theory and practical use.	
Blockchain-based Electronic Health Records Management	https://ieeexplore.ieee.org/abstract/document/9673752/	Al Mamun, A., Azam, S., Gritti, C.	Blockchain, Electronic health records	Blockchain ensures secure and transparent management of health records.	Focus on scalability and integration with existing health IT systems.
Anomaly-based Intrusion Detection in IoT using Deep Learning	https://doi.org/10.3390/app11188383	Alsoufi, M.A., Razak, S., Siraj, M.M., Nafea, I., Ghaleb, F.A., Saeed, F., Nasser, M.	Intrusion detection, IoT, Deep learning	Deep learning models provide high accuracy in detecting intrusions in IoT networks.	Enhance deep learning models for better real-time detection capabilities.
Blockchain for Security in IoT Systems	https://doi.org/10.3390/s23020788	Zubaydi, H.D., Varga, P., Molnár, S.	Blockchain, IoT security, Privacy	Blockchain provides strong security measures for IoT devices, addressing privacy and integrity concerns.	Integrate blockchain with IoT devices for real-time security applications.
Blockchain-based Veterinary Clinic Information Management	https://ieeexplore.ieee.org/abstract/document/9314077/	Iqbal, N., Jamil, F., Ahmad, S., Kim, D.	Blockchain, Veterinary information management	Blockchain ensures integrity and reliability in managing veterinary clinic information.	Extend blockchain applications to other healthcare sectors for better information management.
Security and Privacy on Generative Data in AIGC	https://doi.org/10.1145/3703626	Wang, T., Zhang, Y., Qi, S., Zhao, R., Xia, Z., Weng, J.	Generative data, AI-generated content, Security	Generative AI models pose significant privacy and security risks related to content generation.	Develop frameworks for secure and privacy-preserving generative AI systems.
Cybersecurity in Modern Power Systems	https://doi.org/10.1016/j.rineng.2024.102647	Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D.E.A., Bajaj, M., Blazek, V., Prokop, L.	Cybersecurity, Power systems, Resilience	Power systems face growing cybersecurity risks, requiring proactive defense strategies.	Implement comprehensive cybersecurity measures to ensure power system resilience.
Blockchain for Disease Management	https://ieeexplore.ieee.org/abstract/document/9819963/	Azbeg, K., Ouchetto, O., Andaloussi, S.J.	Blockchain, Disease management, Privacy	Blockchain enhances privacy and access control in disease management systems.	Expand blockchain applications to include all aspects of healthcare management.
Critical Cybersecurity Analysis for IoT	https://doi.org/10.3390/s23084117	Tariq, U., Ahmed, I., Bashir, A.K., Shaukat, K.	IoT cybersecurity, Future research	IoT faces increasing cybersecurity challenges due to its vulnerability and rapid expansion.	Design resilient IoT security frameworks based on advanced encryption techniques.