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

Implementing Data Loss Prevention (DLP)

Firoz Mohammed Ozman *

Solutions Architect, Anecca Ideas Corp, Toronto, Canada.

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(02), 2427-2436

Publication history: Received on 07 April 2025; revised on 19 May 2025; accepted on 21 May 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.2.0792

Abstract

The aim of the research is to critically evaluate the challenges and opportunities associated with Data Loss Prevention (DLP) adoption procedures, and to propose different solutions and strategies for implementing and improving the performance of DLP, while examining its maturity within a business context. Businesses demonstrate significant growth through cloud-based services and digital transformation, but also face data security challenges that have become increasingly complex. The foundation of insider threat, both intentional and unintentional, encompasses significant causes associated with data theft, posing a substantial challenge for organizations to effectively navigate and implement various measures related to Data Loss Prevention (DLP). The research study directly contributes to the growing body of knowledge about the critical challenge of data security management, particularly in the implementation of Data Loss Prevention (DLP) solutions within large-scale business environments. The research aimed to fill the gap by proposing a practical and comprehensive approach, along with a sophisticated framework, for enhancing Data Loss Prevention (DLP) implementation and adoption.

Keywords: Data Loss Prevention (DLP); Insider Threat; Cloud-based Services; Implementation Challenges; Machine Learning; Artificial Intelligence

1. Introduction

Data loss prevention (DLP) is considered one of the most significant strategies for businesses to approach and secure sensitive information, given the era of growing cyber threats. With the rapid evolution of cloud adoption and digital data, companies are facing unprecedented risks, considering the increasing prevalence of data breaches and data leakage. The situation can progress to legal liability, financial loss, and reputational damage. The integration of data loss prevention technology is specifically designed to identify, monitor, and prevent unauthorized transmission of sensitive information across various storage systems and networks (Guha et al., 2021). This type of Technology plays a significant role in mitigating insider threats, unintentional data leakage, and targeted cyberattacks. Apart from that, potential advancements in the area of machine learning and artificial intelligence contribute directly to the creation of data loss prevention solutions, enabling the effective prevention and prediction of data breaches by successfully analyzing user behaviour and identifying anomalies (Gupta & Kush, 2021). Despite significant business advancements, persistent challenges persist when implementing and adopting a Data Loss Prevention (DLP) strategy for large-scale environment management (Arslan, 2021).

1.1. Problem statement

Businesses demonstrate significant growth through cloud-based services and digital transformation, but face data security challenges that have become increasingly complex (Ozman, 2024). The foundation of insider threat, encompassing both intentional and unintentional causes, is associated with significant data theft, posing a substantial challenge for organizations to effectively navigate and implement measures related to Data Loss Prevention (DLP)

* Corresponding author: Firoz Mohammed Ozman

(Moudni & Ziyati, 2023). Even though Data Loss Prevention (DLP) solutions have the potential to provide a radical mechanism for safeguarding sensitive data, their integration and deployment correspond to acknowledging larger environments associated with obstacles in navigation, such as resistance to adoption, operational complexity, and high implementation costs (Arslan, 2021). Apart from that, there has been a significant margin of limitation when it comes to creating standardized models to critically assess maturity and guidance associated with Data Loss Prevention (DLP), considering the integration of appropriate strategies (Alsubaie et al., 2021). In this regard, all identify the challenges for the motivated composition of increasing cyber-attack sophistication by simply targeting Software-as-a-Service (SaaS) applications (Omodara, 2022). Hence, it has become one of the most pressing requirements of research to directly address the issue by proposing a suitable model for enhancing Data Loss Prevention (DLP) performance and adoption.

1.2. Research aim

The research aims to critically evaluate the challenges and opportunities associated with Data Loss Prevention (DLP) adoption procedures, proposing different solutions and strategies for implementation and performance improvement of DLP while examining maturity within a business context.

1.3. Research objectives

- To critically evaluate organizational challenges experienced when it comes to the deployment and adoption of Data Loss Prevention (DLP) solutions.
- To directly determine the solution's strategy and framework for critically navigating the effectiveness and maturity of Data Loss Prevention (DLP)
- To critically analyze a suitable framework for the enhancement of Business Insider's trust management to reduce data leakage risk

1.4. Significance of the study

The research study directly contributes to the growing body of knowledge about the critical challenge of data security management, particularly in the implementation of Data Loss Prevention (DLP) solutions within large-scale business environments. It provides valuable knowledge regarding the assessment of Data Loss Prevention strategy maturity and effectiveness, helping organizations navigate data protection measures for improvement while identifying gaps (Alsuwaie et al., 2021). By successfully determining insider threat calculation procedures that leverage deep learning modelling, a significant potential for information loss prevention can be acknowledged, as evidenced by the research of Guha et al. (2021). This study provides a critical bridge between practical applications and theoretical knowledge. The research offers actionable recommendations for business organizations to approach safeguarding opportunities related to sensitive information while ensuring compliance with data protection regulations. The research study holds the potential to assist various cybersecurity experts, IT professionals, and policymakers in developing a suitable, sophisticated framework for mitigating the risk of data leakage and enhancing business resilience against sophisticated cyberattacks.

1.5. Research Gap

While existing research navigates different variations when it comes to the technology of Data loss prevention (DLP), the research navigates standardized models by simply evaluating maturity associated with Data loss prevention (DLP) to optimize data protection strategy successfully. Apart from that, the strategic integration of insider threat trust calculation, along with the AI-driven mechanism, contributes to the process of evaluation within the current research setting. The gap critically represents a significant research requirement to focus on the framework of holistic Data Loss Prevention (DLP) implementation, considering the mitigation of business challenges within a threat management and Technology advancement context, particularly in a cloud-based environment. The research aimed to fill the gap by proposing a practical and comprehensive approach, along with a sophisticated framework, for enhancing Data Loss Prevention (DLP) implementation and adoption.

2. Literature review

2.1. DLP Adoption and Implementation Challenges

The strategic adoption of data loss prevention technology is considered one of the most significant aspects in navigating contemporary data security challenges. In this regard, it has been identified that Data Loss Prevention (DLP) encompasses a comprehensive mechanism for monitoring, determining, and preventing unauthorized data access and data leakage, as well as data transfer. Despite the situation, organizations face significant challenges when it comes to

Data Loss Prevention (DLP) adoption and major deployment procedures. Arslan (2021) discusses the significant complexity associated with organizational experience within large-scale environments, where Data loss prevention solutions struggle with scalability when it comes to maintaining integration with existing infrastructure. Other important challenges include the need for initial investment costs to disrupt existing operations and technical limitations when managing large volumes of data across various business platforms. Furthermore, Moudni and Ziyati (2023) highlight the significant difficulty in the insider threat mitigation process, which is another effective challenge in focusing on data leakage prevention. The situation presents unique resistance for different data law prevention technologies to navigate dependency on suspicious activity detection and anomaly behaviour evaluation for the prevention of data breaches.

2.2. DLP Maturity Models and Performance Assessment

Table 1 Key Aspects and Importance of DLP Maturity Models in Organizational Data Security

Aspect	Description	Importance
DLP Maturity Models	Frameworks are used to assess and guide the adoption of DLP technologies within organizations, typically including stages such as awareness, integration, and optimization.	Helps organizations assess their readiness for DLP implementation, set benchmarks, and track progress toward a more secure data environment.
Stages of Maturity	Stages often include initial awareness, technology implementation, continuous monitoring, and optimization for advanced threat protection.	Provides organizations with a roadmap for improving DLP systems, moving from reactive measures to proactive, predictive security.
Performance Assessment	Involves evaluating the effectiveness of DLP solutions by measuring incident detection rates, prevention efficiency, and system scalability.	Helps in measuring the effectiveness of DLP systems, identifying weaknesses, and ensuring continuous improvement of the data security infrastructure.
Forecasting and Analytics	Use of predictive analytics to forecast data security incidents based on historical trends, improving DLP performance.	Forecasting assists in predicting future data leakage events, enabling more proactive and timely measures to prevent breaches.

2.3. Technological Advancements in DLP

Table 2 Emerging Technologies and Their Advancements in Data Loss Prevention (DLP) Systems

Technology	Description	Advancement
Machine Learning (ML)	Machine learning algorithms are used to identify patterns and anomalies in data access and transmission, improving the detection of suspicious activity (Gupta and Kush, 2021).	Enhances DLP systems by allowing them to detect subtle data leakage patterns, reducing false positives, and improving accuracy.
Artificial Intelligence (AI)	AI-driven DLP solutions use cognitive computing to analyze large data volumes, enabling intelligent threat detection and decision-making.	AI algorithms allow for real-time data monitoring, automated responses to potential threats, and predictive analytics to forecast breaches (Guha et al., 2021).
Deep Learning	Deep learning models, particularly in document and file analysis, are used to detect and prevent data loss in multi-page or complex digital documents (Guha et al., 2021).	Deep learning models can learn complex data patterns, improving the accuracy of DLP systems for document-level security and preventing leaks that traditional systems might miss.
Predictive Analytics	Predictive analytics uses historical data to forecast potential data leakage events, enabling proactive responses before incidents occur.	Combines historical data analysis and forecasting to improve decision-making and prioritize potential security risks, enhancing overall DLP effectiveness.
Cloud-Native DLP	DLP systems designed specifically for cloud environments protect data stored in SaaS	Cloud-native DLP solutions are scalable, flexible, and designed to address unique cloud

	applications and cloud platforms, ensuring remote data security.	vulnerabilities, providing more robust protection for cloud-hosted sensitive data (Omodara, 2022).

2.4. Cloud Security and DLP for SaaS Applications

Concerning high-speed adoption procedures considered in cloud services and Software-as-a-Service (SaaS) applications, challenges are considered to be focused on data host security within the remote location Management process. The research study by Omodara (2022) has highlighted significant vulnerability when it comes to software as a service application of integration by different cyber criminals due to the large base of user data utilization and storage of sensitive information. Productional solutions of Data Loss Prevention (DLP) were found to be not appropriate for cloud environments, and this is the main reason why organizations are transforming into cloud-native solutions of data loss prevention to become better suited for the protection and monitoring of data.

3. Material and methods

The systematic approach used in conducting the literature review, along with the resultant steps, including search strategies, inclusion and exclusion criteria, a time horizon for the reviewed studies, and the use of the PRISMA framework to ensure transparency and reproducibility, is explained in this section.

3.1. Search strategy

A qualitative study is used with different keywords to apply Boolean Operators. Across nine databases, including Scopus, PubMed, Google Scholar, and IEEE Xplore, among others, a literature search was conducted. Articles about data loss prevention, DLP implementation, information security, data protection, and sensitive data were identified with keywords like 'DLP', 'DLP implementation', 'information security', 'data protection' and 'sensitive data'. To obtain comprehensive coverage, Boolean operators (AND, OR) were utilized to refine searches. The results were narrowed down using advanced search filters, such as publication date and peer-reviewed status, and categorized by subject categories. To capture practical insights into DLP implementation, grey literature, including white papers and technical reports, was also considered.

3.2. Exclusion and inclusion criteria

The inclusion criteria for the review were:

- The pieces are peer-reviewed in reputable journals or conferences.
- Studies in the design, implementation or evaluation of DLP systems.
- Articles published in English.
- Research on issues, strategies, or applications of DLP implementation specifically.

Exclusion criteria included:

- Articles unrelated to DLP, but still quite relevant.
- Those studies are purely theoretical frameworks and have no practical experience.
- Duplicates across databases.
- Non-English publications.

Table 3 Inclusion and Exclusion Criteria

Criteria	Inclusion	Exclusion
Peer Reviewed	Peer-reviewed articles published in reputable journals or conferences	Articles not subjected to peer review
Focus	Studies focusing on the design, implementation, or evaluation of DLP systems	Articles not directly related to DLP
Language	Published in English	Non-English publications
Content	Research addressing challenges, strategies, or case studies related to DLP	Studies focusing solely on theoretical frameworks without practical insights

Duplicates	N/A	Duplicates across databases

(Source: Self-Developed)

3.3. Time Horizon

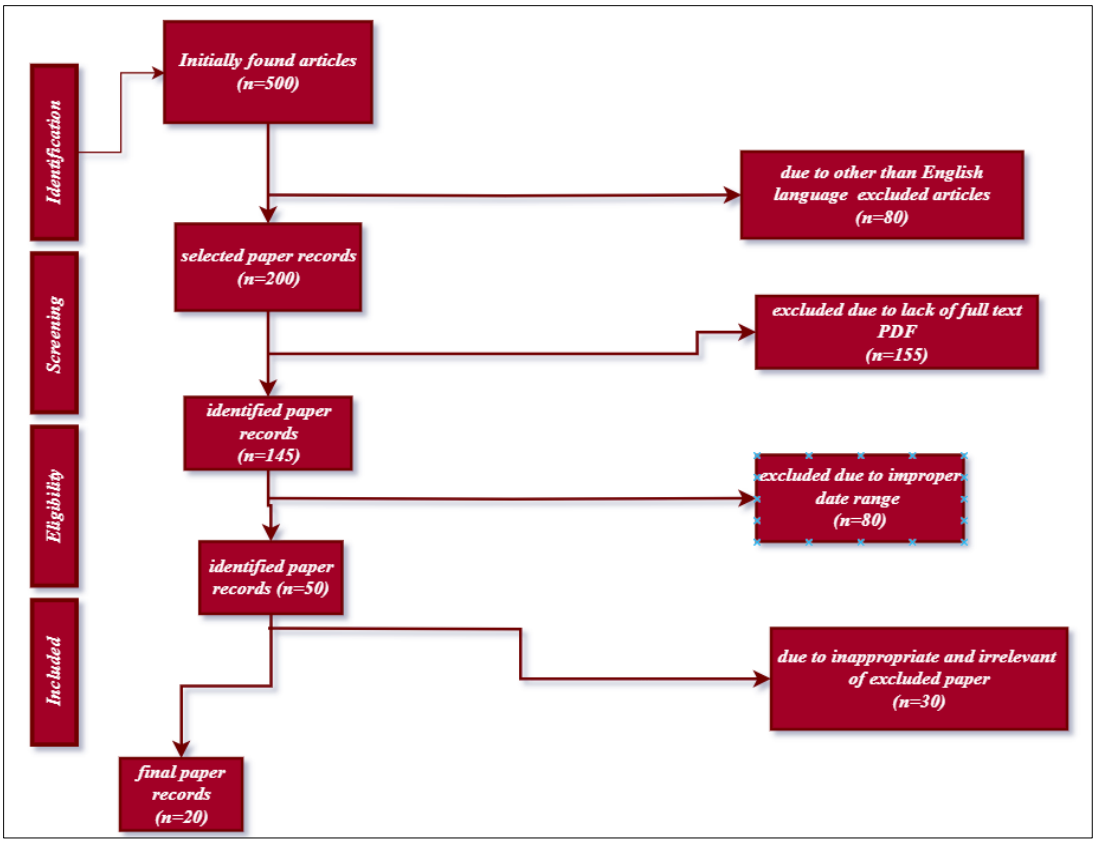
Studies published between 2020 and 2025 were reviewed. This timeframe enables tracking the response of DLP technologies to escalating cybersecurity threats and the expansion of cloud computing and remote working environments. The chosen period allows the review to be confined to both fundamental research and emerging work in DLP systems.

3.4. Prisma

The researcher used the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework and methodological rigour to ensure transparency. The PRISMA flow diagram outlines the selection process:

- ***Identification:*** Initial database searches yielded 500 articles.
- ***Screening:*** A total of 100 relevant articles from the pool were then reviewed for their abstracts and titles.
- ***Eligibility:*** A total of 50 eligible studies were identified through a full-text review.
- ***Inclusion:*** A total of 20 articles were selected for detailed analysis after application of the inclusion and exclusion criteria.

The PRISMA framework facilitated a systematic, reproducible, and unbiased review process, thereby strengthening the credibility of the findings.



(Source: Self-Developed)

Figure 1 PRISMA Framework

4. Results and discussion

4.1. Challenges experienced by businesses in the deployment and adoption of DLP

The adoption and deployment of data law prevention systems represent significant challenges, as per the knowledge gained from a systematic literature review, which revealed that organizations are particularly focused on increasing the complexity of the landscape, considering the large scale of operation in the digital environment. According to a systematic literature review, it has been found that integration complexity is a significant challenge, particularly considering the existing infrastructure setup of the business system, which is not sufficiently compatible with the new DLP technology solution (Turobova et al., 2021). Multiple businesses have struggled with data loss prevention solutions in terms of workflow without resulting in any disruption. Another significant challenge in this matter, as revealed by the systematic review, is insider threat, as multiple data leakages are occurring from business-trusted employees who appear to have authorized access to company-sensitive information (El Moudni & Niyati, 2023). Although the Data Loss Prevention system is specifically designed for data protection, it can also strike a balance between employee productivity and security by preventing challenges associated with strict policies, which could lead to business workflow bottlenecks (Gupta & Kush, 2021). Apart from that, organizations also face the challenge of high investment costs associated with new software implementation and training, making it highly challenging for small companies to adopt DLP solutions (Arslan, 2021). Finally, the challenge of managing data across a large cloud environment creates a unique set of resistance to consulting implementations of DLP, for example, cloud-native infrastructure alignment with on-premise solutions (Omodara, 2022).

4.2. Framework for Effectiveness and Maturity of Data Loss Prevention (DLP)

One of the most significant frameworks is a critical analysis of the maturity and effectiveness of data loss prevention systems, evaluating different factors such as response efficiency, detection ability, and scalability. The integration of a maturity model, acknowledged by Alsuwaie et al. (2021), employs a multi-dimensional approach that critically evaluates the initial awareness of continuous optimization, Technology deployment, and policy formation. Another significant component in the framework is the detection capability, which refers to the system's ability to identify potential data breaches, enabling swift and accurate measures to neutralize the threat. Finally, scalable and effective data loss prevention solutions incorporate the growing landscape of data volume management to address complex network activity (Gupta & Kush, 2021). The framework critically evaluates business maturity by identifying potential gaps and providing recommendations to transition from reactive measures to a proactive business strategy. Apart from that, regular performance evaluation is another substantial component of the framework, based on real-world performance metrics, to integrate the frequency of data breaches with employee compliance management and provide support for navigating DLP strategy towards maximum impact.

4.3. A solutions strategy for insider trust management and the reduction of data leakage risk

Effective management fosters insider trust, which is crucial for mitigating data leakage risk within a business. One of the most significant strategies is dynamic access control mitigation at the business level, which needs to be calculated in real-time. El Moudni and Ziyati (2023) propose a model that critically navigates the assessment of sensitive data, which is not only granted for user evaluation but also acknowledged as one of the most considered factors, such as access requests and user behaviour patterns. This approach facilitates the identification of anomalous behaviour to promote a security awareness culture, enabling employees to understand the consequences associated with data leakage directly. Apart from that, integrating a machine learning model is another potential strategy for enhancing accuracy, while detecting unusual activity and excessive patterns improves response time.

5. Conclusion

Data Loss Prevention (DLP) is based on the CIA triad and offers two key tools: strategies and technologies. Developers will need to deploy these strategies and technologies to ensure that sensitive data is not accessed, shared, or leaked outside the organization. Firstly, developers should categorize sensitive information, such as financial data, intellectual property, or personal information. They utilize DLP tools that can monitor and control data flow across endpoints, emails, cloud services, and networks. Security data should be trained to employees on data security practices and strictly adhered to regulatory standards. Moreover, Data Loss Prevention ensures data integrity by controlling edits and preventing overwriting.

As a result of this systematic literature review, the critical importance of implementing robust 'Data Loss Prevention (DLP)' systems to protect sensitive information is highlighted. It is found that DLP technologies have progressed

significantly, but they also present challenges related to scalability, integration with existing systems, and compliance. The review highlights the need to consider all these factors, including technological, organizational, and human factors, to ensure the success of DLP systems. Additionally, the literature shows an increasing momentum for incorporating machine learning and artificial intelligence into DLP solutions for real-time threat detection and adaptive responses.

Regulatory compliance, as well as DLP strategies aligned with organizational goals, were identified as central themes. While such developments have been made, there are still gaps in dealing with insider threats, securing the cloud, and controlling the influx of an increasing volume of sensitive data. This review synthesizes existing insights from diverse studies to provide a comprehensive understanding of the current status of DLP implementation. It provides firms with a foundation for advancing their data protection strategy and reducing risks by identifying best practices and potential research areas.

Recommendations

Based on the findings of this review, several recommendations can guide organizations in implementing effective DLP systems:

- ***Adopt a Holistic Approach:*** DLP solutions can deliver best practices in a small, embedded way within an organization's broader cybersecurity strategy, as they are both complementary and aligned with regulatory requirements and organizational objectives (Guha et al., 2021).
- ***Leverage Advanced Technologies:*** Machine learning and artificial intelligence can further enhance DLP's detection capabilities and platforms, enabling proactive responses to emerging threats.
- ***Focus on User Awareness:*** Data Loss Protection is essential to a culture of data security and user compliance with DLP policies; comprehensive training programs are key to achieving this objective (Arslan, 2021).
- ***Prioritize Cloud Security:*** As more companies rely on cloud services, sensitive data presents unique challenges that require addressing through DLP strategies.
- ***Continuous Monitoring and Updates:*** DLP systems across organizations should be regularly updated to see whether they are effective, and policies and technologies updated to keep up with the ever-evolving threats.

If implemented, these recommendations will help organizations build more effective data protection frameworks, mitigate risks, and protect sensitive information in the increasingly complex digital landscape.

References

[1] Alhindi, H., Traore, I. and Woungang, I. (2021). Preventing data leak through semantic analysis. Internet of Things, 14, p.100073. https://doi.org/10.1016/j.iot.2019.100073

[2] Alsuwaie, M.A., Habibnia, B., and Gladyshev, P. (2021, November). Data Leakage Prevention Adoption Model and DLP Maturity Level Assessment. In 2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC) (pp. 396-405). IEEE. https://doi.org/10.3390/jcp4020009

[3] Amit, G., Yeshooroon, A., Kiperberg, M. and Zaidenberg, N.J. (2021, January). DLP-Visor: A Hypervisor-based Data Leakage Prevention System. In ICISSP (pp. 416-423). https://doi.org/10.5220/0010221104160423

[4] Arslan, Y. (2021). DEPLOYING DATA LOSS PREVENTION PROJECTS IN BIG ENVIRONMENTS. Yönetim Bilişim Sistemleri Dergisi, 7(1), pp.61-78. https://dergipark.org.tr/en/pub/ybs/issue/63606/876190

[5] Daubner, L. and Považanec, A. (2023, August). Data loss prevention solution for Linux endpoint devices. In Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1-10). https://doi.org/10.1145/3600160.3605036

[6] DOMNIK, J. and HOLLAND, A. (2022). On data leakage prevention and machine learning. 35th Bled eConference Digital Restructuring and Human (Re) action, p.695. https://doi.org/10.18690/um.fov.4.2022

[7] El Moudni, M., & Ziyati, E. (2023, October). Data Leakage Prevention Approach Based on Insider Trust Calculation. In 2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM) (pp. 1–6). IEEE. 10.1109/WINCOM59760.2023.10322935

[8] Guha, A., Samanta, D., Banerjee, A. & Agarwal, D. (2021). A deep learning model for information loss prevention from multi-page digital documents. IEEE Access, 9, pp.80451–80465. https://ieeexplore.ieee.org/abstract/document/9443107/

[9] Gupta, I., Mittal, S., Tiwari, A., Agarwal, P. & Singh, A.K. (2022). TIDF-DLPM: Term and inverse document frequency based data leakage prevention model. arXiv preprint arXiv:2203.05367. https://arxiv.org/abs/2203.05367

[10] Gupta, K. & Kush, A. (2023). A learning oriented DLP system based on classification model. arXiv preprint arXiv:2312.13711. https://arxiv.org/abs/2312.13711

[11] Gupta, K., & Kush, A. (2021). A forecasting-based DLP approach for data security. In Data Analytics and Management: Proceedings of ICDAM (pp. 1–8). Springer Singapore. https://link.springer.com/chapter/10.1007/978-981-15-8335-3_1

[12] Herrera Montano, I., García Aranda, J.J., Ramos Diaz, J., Molina Cardín, S., De la Torre Díez, I. and Rodrigues, J.J. (2022). Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat. Cluster Computing, 25(6), pp.4289-4302. https://doi.org/10.1007/s10586-022-03668-2

[13] Herrera Montano, I., García Aranda, J.J., Ramos Diaz, J., Molina Cardín, S., De la Torre Díez, I. and Rodrigues, J.J. (2022). Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat. Cluster Computing, 25(6), pp.4289-4302. https://doi.org/10.1007/s10586-022-03668-2

[14] Jadhav, A. and Chawan, P.M. (2021). A system for detection and prevention of data leak. https://www.academia.edu/download/93567346/IRJET_V9I9178.pdf

[15] Mukati, A. and Prakash, D.S. (2022). The Role of Data Leakage Prevention System in CBDC. Indian Journal of Cryptography and Network Security, 2(2), pp.5-11. https://doi.org/10.54105/ijcns.B3604.112222

[16] Naima, A. (2023). DEVELOPING DATA LEAKAGE PREVENTION SYSTEMS. Conferencea, pp.14–23. https://conferencea.org/index.php/conferences/article/view/3008

[17] Omodara, H. (2022). Cloud Security: A survey of Information Communication Technology (ICT) and Cybersecurity professionals' perception on Data Loss Prevention (DLP) measures for Software-as-a-Service (SaaS) application-related data breaches and leakage. https://www.academia.edu/download/92532251/Cloud_Security_A_survey_of_ICT_and_Cybersecurity_professionals_perception_on_DLP_measures_for_SaaS_breaches.pdf

[18] Ozman, F.M. (2024). Security challenges and solutions using Cloud Computing. World Journal of Advanced Engineering Technology and Sciences, 13(2), pp. 738–750. https://doi.org/10.30574/wjaets.2024.13.2.0652

[19] Syarova, S., Toleva-Stoimenova, S., Kirkov, A., Petkov, S. and Traykov, K. (2024, June). Data Leakage Prevention and Detection in Digital Configurations: A Survey. In Environment. Technologies. Resources. Proceedings of the international scientific and practical conference (Vol. 2, pp. 253-258). https://doi.org/10.17770/etr2024vol2.8045

[20] Turobova, G.O.Q., Djangazova, Q.A. and Ganikhodjayeva, D.Z. (2021). Data Loss Prevention and Challenges Faced in Their Deployments. Oriental renaissance: Innovative, educational, natural and social sciences, 1(9), pp.176-182. https://cyberleninka.ru/article/n/data-loss-prevention-and-challenges-faced-in-their-deployments

[21] Victor, A., Arunkumar, G., Rajkumar, S. and Selvanambi, R. (2024). Survey on effective disposal of e-waste to prevent data leakage. Computer Assisted Methods in Engineering and Science, 31(2), pp.187-212. https://doi.org/10.24423/cames.2024.492

Appendices

Appendix 1: Systematic Literature Review Table

Topic	DOI	Authors	Codes/Themes	Key Findings	Recommendations
Data Leakage Prevention Adoption Model and DLP Maturity Level Assessment	https://doi.org/10.3390/jcp4020009	Alsuwaie, M.A., Habibnia, B., Gladyshev, P.	DLP Adoption, Maturity, Model Assessment	Found key adoption challenges and maturity level factors	Enhance DLP maturity with continuous monitoring and adaptation
Data Leakage Prevention Approach Based	https://doi.org/10.3390/jcp4020009	El Moudni, M., Ziyati, E.	Insider Trust, DLP	Proposed an insider trust calculation	Implement trust-based models to detect malicious insiders

on Insider Trust Calculation				model to prevent data leakage	
A forecasting-based DLP approach for data security	https://doi.org/10.3390/jcp4020009	Gupta, K., Kush, A.	DLP, Forecasting	A forecasting approach for proactive data leakage prevention	Use forecasting techniques for preemptive threat identification
Data Loss Prevention and Challenges Faced in Their Deployments	https://cyberleninka.ru/article/n/data-loss-prevention-and-challenges-faced-in-their-deployments	Turobova, G.O.Q., Djangazova, Q.A., Ganikhodjayeva, D.Z.	Deployment, DLP Challenges	Explores difficulties in DLP deployment and strategies to address them	Recommend adapting DLP systems to specific organization needs
Cloud Security: A survey of ICT and Cybersecurity professionals	https://www.academia.edu/download/92532251/Cloud_Security_A_survey_of_ICT_and_Cybersecurity_professionals_perception_on_DLP_measures_for_SaaS_breaches.pdf	Omodara, H.	Cloud Security, SaaS	Insights into DLP challenges related to SaaS applications	Strengthen DLP measures for cloud environments
A deep learning model for information loss prevention	https://ieeexplore.ieee.org/abstract/document/9443107/	Guha, A., Samanta, D., Banerjee, A., Agarwal, D.	Deep Learning, Information Loss	Used deep learning techniques to enhance document protection	Apply deep learning for automated data leak prevention
Deploying Data Loss Prevention Projects in Big Environments	https://dergipark.org.tr/en/pub/ybs/issue/63606/876190	Arslan, Y.	DLP Deployment, Large Scale	Challenges of deploying DLP in large-scale environments	Recommend modular DLP implementations for scalability
TIDF-DLPM: Term and inverse document frequency-based DLP model	https://arxiv.org/abs/2203.05367	Gupta, I., Mittal, S., Tiwari, A., Agarwal, P., Singh, A.K.	Term Frequency, DLP	Introduced a term frequency-based DLP model for improved security	Integrate TF-IDF models into existing DLP systems
Data loss prevention solution for Linux endpoint devices	https://doi.org/10.1145/3600160.3605036	Daubner, L., Považanec, A.	Linux, Endpoint Security	Proposes solutions for data leakage on Linux-based systems	Develop Linux-specific DLP solutions to strengthen endpoint security
Data Leakage Prevention and Detection in Digital Configurations	https://doi.org/10.17770/etr2024vol2.8045	Syarova, S., Toleva-Stoimenova, S., Kirkov, A., Petkov, S., Traykov, K.	Data Leakage Detection, Digital Systems	Survey on current DLP detection methods	Improve detection algorithms for digital configurations
Data Loss Prevention from a Malicious Insider	https://doi.org/10.18690/um.fov.4.2022	Shahzad, A., de Sousa, E.M.	Insider Threat, DLP	Discusses strategies for mitigating risks from malicious insiders	Develop adaptive insider threat detection systems

On data leakage prevention and machine learning	https://doi.org/10.24423/cames.2024.492	Domnik, J., Holland, A.	Machine Learning, DLP	Investigated the application of machine learning for DLP	Enhance DLP systems by integrating machine learning models
Survey on effective disposal of e-waste to prevent data leakage	https://www.academia.edu/download/93567346/IRJET_V9I9178.pdf	Victor, A., Arunkumar, G., Rajkumar, S., Selvanambi, R.	E-waste Disposal, Data Leakage	Focused on proper e-waste disposal techniques to prevent data leakage	Implement secure data destruction methods in e-waste disposal
A system for detection and prevention of data leak	https://doi.org/10.5220/0010221104160423	Jadhav, A., Chawan, P.M.	Detection, Prevention	Developed a system for the detection and prevention of data leaks	Improve automated detection systems for rapid response
DLP-Visor: A Hypervisor-based Data Leakage Prevention System	https://doi.org/10.54105/ijcns.B3604.112222	Amit, G., Yeshooroon, A., Kiperberg, M., Zaidenberg, N.J.	Hypervisor, Data Leakage	Explores a hypervisor-based approach to prevent data leakage	Adopt hypervisor-based solutions for improved virtual machine security
The Role of Data Leakage Prevention System in CBDC	https://arxiv.org/abs/2312.13711	Mukati, A., Prakash, D.S.	CBDC, DLP	Discussed DLP measures for Central Bank Digital Currencies (CBDC)	Implement robust DLP protocols for financial systems
A learning-oriented DLP system based on classification model	https://doi.org/10.1016/j.iot.2019.100073	Gupta, K., Kush, A.	Classification Model, DLP	Introduced a classification-based DLP system for effective prevention	Enhance classification models for better leakage prediction
Preventing data leak through semantic analysis	https://doi.org/10.1007/s10586-022-03668-2	Alhindi, H., Traore, I., Woungang, I.	Semantic Analysis, Data Leak	Applied semantic analysis for preventing data leaks	Integrate semantic techniques into existing DLP systems
Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat	https://doi.org/10.1007/s10586-022-03668-2	Herrera Montano, I., García Aranda, J.J., Ramos Diaz, J., Molina Cardín, S., De la Torre Díez, I., Rodrigues, J.J.	Insider Threat, DLP	Survey on DLP techniques to counter insider threats	Prioritize insider threat mitigation methods in DLP systems
Developing Data Leakage Prevention Systems	https://conferencea.org/index.php/conferences/article/view/3008	Naima, A.	DLP System Development	Explores the process of developing effective DLP systems	Implement a modular DLP architecture that can adapt to evolving threats