ISBN: 978-628-96613-3-0. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2026.1.1.700

Deep Learning Based Intelligent System for Data Automation in a Private Security Company

Elvis Chacón-Pajuelo[1]; José Iglesias-Reyes[2]; Rosalynn Ornella Flores-Castañeda[3]
[1,2,3] Facultad de Ingeniería y Arquitectura, Universidad César Vallejo, Perú, *echaconpa@ucvvirtual.edu.pe, jiglesiasr@ucvvirtual.edu.pe, rfloresc@ucv.edu.pe*

Abstract*–Nowadays, the advance of digitalization and the growing need to optimize processes have driven companies to look for innovative solutions to improve their operational efficiency. In this context, the following study aimed to implement an intelligent system based on Deep Learning to automate data processes within the company, focusing on improving efficiency, accuracy and optimization of operational tasks. The research used a pre-experimental design, with quantitative approach and applied character, analyzing a population of 1,400 records of human management data, such as attendance, task and customers. Data collection was carried out through direct observation and documentary analysis, while the system development was based on the Crystal-Clear agile methodology, allowing specific adaptations to the company's operational needs. The results showed significant improvements: information access time was reduced from 29.90 seconds to 15.77 seconds, accuracy in identifying sensitive data increased from 58.70% to 91.43%, and automation efficiency increased from 28.67% to 95.67%. Statistical tests confirmed the relevance of these results. The system optimized processes and reduced manual intervention and highlighted the importance of customized intelligent solutions to improve organizational performance. These findings highlight the potential of Deep Learning-based systems to transform data-sensitive sectors such as private security.

***Keywords*-- Deep Learning; data automation; predictive modelling; neural networks; PRISMA; data security**

I. Introduction

Today, the biggest challenge facing all institutions in this digital era is the rapid growth of data from various sources and in different formats. However, in traditional data processing, the main shortcomings are speed, accuracy and the ability to extract valuable information from complex data sets [1]. Likewise, the absence of a comprehensive strategy to automate worsens the problem because it exposes companies to many threats, from information loss to unauthorized access and malicious manipulation.

Over time, data management has been crucial around the world and new methods of protection have been developed. However, data is vulnerable to attacks because traditional methods are no longer effective. Experiments have shown the high efficiency of this approach in addressing various challenges in categorizing sensitive data and its contribution to data management and protection worldwide has been significant [2].

In this context, it is very important for organizations in various sectors to implement cutting-edge solutions based on cutting-edge technologies such as Deep Learning (DL), to face these challenges and maintain their competitiveness in the market in which they are located [3]. In this sense, the evolution of artificial intelligence (AI) is creating new opportunities in different areas, and Machine Learning (ML) plays a vital role in this process [4]. Similarly, the integration of DL and rule-based systems in a decision support system for smart devices enables visual inspection in production [5]

Additionally, some algorithms have been suggested to fuse sensor data based on DL models which are fed by suboptimal networks, where stacked auto-encoder fusion and clustering protocols optimize the performance of data fusion in wireless sensor networks [6]. In addition, tools such as NeuroCAD automate the assessment of producibility using voxelization and DL methods based on CAD files, making it possible to evaluate abstract and production-relevant geometric properties [7].

At this point, data has become essential in the digitization process of companies [8]. Where, the use of AI in data analysis offers companies the possibility to automate procedures, optimize decision making in real time and provide tailored experiences [8].

Therefore, implementing an intelligent DL-based system for data automation will not only boost efficiency in operations, but also foster economic growth, job generation, and entrepreneurship by freeing up resources and refining strategic decision making. This innovative solution will enable institutions to overcome current constraints and optimize the use of the potential of existing data.

The objective is to implement an intelligent system based on Deep Learning to automate data processes within the company, focusing on improving efficiency, accuracy and optimization of operational tasks.

II. LITERATURE REVIEW

Blockchain technology has had a remarkable impact on the financial sector in recent years. This is not only due to its outstanding ability to efficiently manage cryptocurrency accounts, but also to its possible implementation in key aspects of finance, such as trust management, data governance and process automation. According to [9], the technology in question excels in the processes of data governance and automation of financial systems, this because it ensures trust through consensus mechanisms and digital signatures. These particularities make Blockchain an extremely useful asset to address regulatory and operational challenges in the sector. In short, these technologies will play a central role in the financial system to ensure transparency, confidentiality and efficiency of all its procedures.

In the current era, the use of new computer technologies for toxicity analysis has gained relevance thanks to their efficiency and accuracy that are more key than conventional studies. As mentioned by [10], the development of a new way of analyzing information based on trained models is a great technological advance that allows obtaining more valid results that can be molded based on parameter modifications, which leads to a greater contribution to research. In view of this, trained models, thanks to learning platforms, provide security and quality to the users who employ them. Therefore, in the development of the research they carried out, models such as Vertex AI, Azure, among others, stood out, which provided great reliability in the results. Thus, the use of a new technology provides an optimization in the accuracy and score analysis and modeling of information, which leaves aside the conventional methods and provides a new way of doing things.

Continuing, according to [11], who conducted research on the use of ML technology in the digital marketing sector where their objective was to analyze the behavior of their customers to provide them with recommendations based on information received and processed using artificial intelligence algorithms. That is why, for the development of the research they used a methodology based on decision algorithms, which, through tree-based decisions, were able to classify the data with a perfect 100% accuracy by using the Naïve Bayes classification. Finally, based on exact numbers, the algorithm gave an accuracy result of 97.175% with a margin of error of 0.028%, which demonstrated its high accuracy in classifying data in this research. As a synthesis, the combination of these three AI-driven ML algorithms proved to be an effective strategy to improve digital marketing tactics in the food retail industry, thus reducing time and expenses.

According to [12], the objective of this research was to use the proposed ML models, such as Multilayer Perceptron, Decision Tree and Support Vector Machine, to categorize data as anomaly or non-anomaly based on 5G Open Access Radio Architecture (O-RAN) data sets with various key performance indicators. The methodology that underpinned this research was the development of a strategy to classify anomalous situations by using the t-Distributed Stochastic Neighbor Embedding (tSNE) technique on datasets containing various key performance indicators. As a result, an accuracy of over 90% was achieved in all use cases analyzed. In summary, this study was able to demonstrate that the detection of faults in 5G O-RAN networks, were thanks to the use of ML algorithms, which could be evidenced in an efficient way that its performance is optimal for future research in other environments.

According to [13], the main objective of this study was to face the challenge of effectively managing large amounts of data, with the guarantee of preserving high levels of security, accuracy and availability. In the study, the abilities of the Intelligent Document Management System (IDMS) to integrate the collection and processing of medical billing information, Aadhaar ID cards and PAN ID cards could be evidenced. Additionally, two different perspectives were employed: Using Easy OCR and a mixed strategy that merged natural language processing through regular patterns and optical character identification, the effectiveness of the system in handling such documents was enhanced. As a result, the findings indicated that the proposed hybrid approach (NLPCV) achieved a superior accuracy of 97% for hospital bills, 71% for Aadhaar cards and 78% for PAN cards. To conclude, this integrated AI-based approach enabled the creation of a highly effective intelligent document management system.

In a study by [14], an intelligent management system was developed which aimed to improve the management of sand factories. This system used DL for automatic sand detection and Edge Computing for local data processing, which improved both the quality and efficiency of operations compared to traditional methods. The results of the study indicated an accuracy of 98% in the identification and a response time of 0.022 seconds, which highlights the great effectiveness of the implemented system.

On the other hand, [15] reposed as an objective to examine the great importance of using data-driven DL technology to improve reliability, quality and management of distribution networks. The findings highlighted the application and progress of mixed approaches that merge Deep Learning with other strategies in order to refine and enhance the structure of such systems. In summary, the analysis provided an updated view about the role of Deep Learning in power distribution automation, highlighting its increasing importance in this industry.

Similarly, [16], unveiled a hybrid random deep neural network (HDRaNN) specially developed to identify cyber-attacks in the Industrial Internet of Things (IIoT). The goal was set to create and implement robust security systems for IIoT networks using deep learning and massive data evaluation. The methodology in choice fused a random deep neural network with a multilayer perceptron and dropout regularization. Consequently, the suggested method categorized 16 different varieties of cyber-attacks with 98% and 99% accuracy on DS2OS and UNSW-NB15 datasets, respectively, evidencing superior performance to other DL grounded methods. In conclusion, this research proposed an effective hybrid neural network for detecting cyber-attacks in IIoT environments.

According to [17], in research on IoT system for dropout prediction using ML and socioeconomic data, they developed an IoT framework for predicting dropout using machine learning techniques, including Decision Tree, Logistic Regression, SVM, KNN, Multilayer Perceptron, and DL. Its objective was to address the problem of student dropout that negatively impacts social, economic, political and academic issues, especially in underdeveloped nations. The methodology automated the prediction to obtain data that is difficult for humans to access. The system achieved 99.34% accuracy, 99.34% F1 score, 100% completeness and 98.69% accuracy using Decision Tree. In summary, this IoT system was shown to be a viable tool for universities to identify students at risk of dropping out.

In research by [18], a DL model was created to reliably quantify occlusions in dentinal tubules, this to replace the manual evaluation techniques that had been performed. Data augmentation techniques were used to enhance learning, reaching a total of 10700 images belonging to five classes, which were used to train the neural network. The proposed convolutional neural network (CNN) was able to classify the degree of occlusion into five categories with an accuracy of 90.24%. In summary, this architecture proved to be a highly effective alternative for the automatic and objective classification of segmented images of dentinal tubules.

III. METHODOLOGY

The research was developed as an applied study with quantitative approach and pre-experimental design, evaluating the impact of an intelligent system based on Deep Learning for data automation in a company. The population consisted of 1400 data records related to human management, selected by census sampling. Data were collected using the direct observation technique and structured record cards designed to measure key indicators such as efficiency, accuracy and optimization. For data analysis, statistical tools such as SPSS and Excel were used to perform descriptive and inferential analyses.

A) Case development

For the development of the intelligent system based on Deep Learning, the Crystal Clear agile methodology was adopted, which focuses on small, flexible teams and iterative deliveries of functional software. This approach allowed constant feedback and adjustments during the development cycle, ensuring that the solutions were aligned with the specific requirements of the private security company.

1. Planning:

During this stage, we started with the project scope and mission statements, in order to distinguish the functional requirements and thus define the objectives. Table I defines the functional requirements of the system as such

TABLE I
SYSTEM REQUIREMENTS

REQUIREMENT	DESCRIPTION
RF1: LoginA	The administrator must log in with a username and password.
RF2: LoginP	Staff must log in with an e-mail address and password.
RF3: Registration of Personal	The administrator can register new operational staff members in the system.
RF4: Personnel Modification	The administrator can modify personnel information such as personal data and unit assignments.
RF5: Personnel Elimination	The administrator can delete personnel records that are no longer part of the company.
RF6: Assign Unit to a Staff	The administrator can assign personnel to a specific unit in the system.
RF7: Register dates SUCAMEC	The administrator can record and update the dates related to issuance and expiration.
RF8: Display Personal Card	The administrator can display a detailed

	personnel file with data.
RF9: Display SUCAMEC Card	The administrator can visualize data related to the course or SUCAMEC card.
RF10: User Registration	The administrator can register new users in the system with different roles, such as administrators or operational staff.
RF11: Modify Users	The administrator can modify user information.
RF12: Delete users	The administrator can delete users.
RF13: Register units	The administrator can register new operating units to which personnel will be assigned.
RF14: Modify Units	The administrator can modify the information of the operating units.
RF15: Delete Units	The administrator can delete units that are no longer needed.
RF16: View Card Units	The administrator can display a card with the unit information.
RF17: Registrar Tareaje	The administrator can record staff attendance.
RF18: Modify Task	The administrator can modify the records to update.
RF19: Exporting Harassment	The administrator can export the task records.
RF20: Dashboard	The administrator can access a dashboard that displays statistics on attendance, staffing, and other key metrics.
RF21: Password recovery	Users can recover their passwords through a secure reset process.
RF22: Dashboard Predictions	The system should display a dashboard with predictions based on attendance history.

2. *Design:*

In this next stage, the design was made according to business logic, which could be deduced from the requirements.

Fig. 1 presents the system architecture based on the MVC pattern, highlighting the separation between business logic, user interface and flow control to ensure scalability and maintainability.

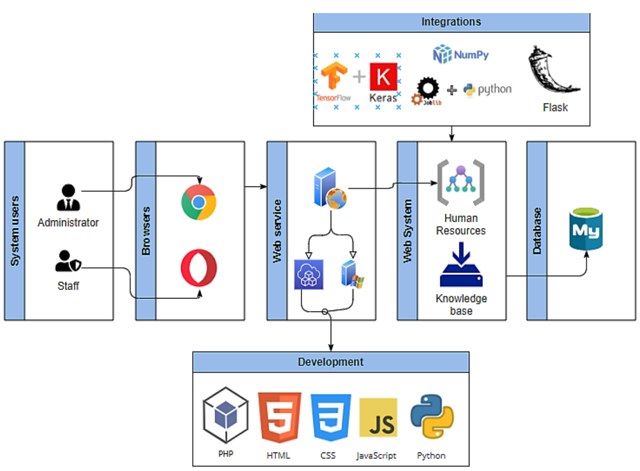

Fig. 1 System architecture

3. *Development:*

The development phase focused on the modular implementation of the system, following the proposed design and ensuring the integration of components through unit testing. Deep Learning models were trained with real data, ensuring their accuracy and adaptability to the operating environment.

III. RESULTS

This section details the results obtained from the research regarding the dimensions of "efficiency (EF)" with the information access time indicator (TA), "precision (PR)" with the sensitive data identification rate indicator (TD) and "optimization (OP)" with the data automation efficiency (EA), showing the effects of the intelligent system based on Deep Learning.

A. *Descriptive analysis:*

The following descriptive analysis evaluates the results by indicator.

Table II shows the improvement in information access time, reducing the mean from 29.90 seconds in the pre-test to 15.77 seconds in the post-test, evidencing greater speed and consistency after the implementation of the system.

TABLE II
DESCRIPTIVE MEASUREMENT OF I1-TA

	N	Minimum	Maximum	Media	Standard deviation
Pre-test(sg)	30	26,00	34,00	29,9000	1,76850
Post-test(sg)	30	14,00	18,00	15,7667	1,22287

Table III shows an increase in the accuracy of sensitive data identification, with an improvement from a mean of 58.70% in the pre-test to 91.43% in the post-test, reflecting greater reliability in data handling after implementation of the system.

TABLE III
DESCRIPTIVE MEASUREMENT OF I2-TD

	N	**Minimum**	**Maximum**	**Media**	**Standard deviation**
Pre-test (%)	30	,50	,67	,5870	,05174
Post-test(%)	30	,87	,98	,9143	,02738

Table IV evidence a significant improvement in automation efficiency, increasing the average from 28.67% in the pre-test to 95.67% in the post-test, demonstrating an optimized capability after system implementation.

TABLE IV
DESCRIPTIVE MEASUREMENT OF I3-EA

	N	Minimum	Maximum	Media	Standard deviation
Pre-test(%)	30	,20	,40	,2867	,07761
Post-test(%)	30	,90	1,00	,9567	,05040

B. *Inferential analysis:*

The following is the inferential analysis that complements the descriptive findings, allowing us to evaluate the significance of the results obtained after the implementation of the intelligent system based on DL.

Normality test:

- H_0: The TA indicator data are arranged in the normal way.
- H_1: The TA indicator data are not available in the normal way.

Table V presents the results of the Shapiro-Wilk normality test for information access time, showing normality in the pre-test with a significance value of .198 and absence of normality in the post-test with a significance value of .001, reflecting significant changes after implementation.

TABLE V
NORMALITY TEST I1-TA

	Shapiro-Wilk		
	Statistics	gl	Sig.
Pre-test(sg)	,953	30	,198
Post-test(sg)	,868	30	,001

Table VI shows the results of the Shapiro-Wilk normality test for the sensitive data identification rate. In the pre-test, the significance value of .050 indicates a possible marginal normality, while in the post-test, with a significance value of .405, the null hypothesis is accepted, suggesting that the data are normally distributed.

TABLE VI
NORMALITY TEST I2-TD

	Shapiro-Wilk		
	Statistics	gl	Sig.
Pre-test(%)	,930	30	,050
Post-test(%)	,965	30	,405

Table VII presents the results of the Shapiro-Wilk normality test for data automation efficiency. In both pre-test and post-test, the significance values are less than .001, leading to accept the alternative hypothesis (H_1) and reject the null hypothesis (H_0), indicating that the data do not follow a normal distribution in either scenario.

TABLE VII
NORMALITY TEST I3-EA

	Shapiro-Wilk		
	Statistics	gl	Sig.
Pre-test(%)	,803	30	<,001
Post-test(%)	,632	30	<,001

C. *Hypothesis testing:*

The sample data do not have a normal distribution; therefore, the Wilcoxon signed-rank test will be applied, which is a non-parametric test to contrast the mean between two related samples.

- H_0: There is no significant difference in the information access time (TA) before and after the implementation of the intelligent system based on Deep Learning.
- H_1: There is a significant difference in the information access time (TA) before and after the implementation of the intelligent system based on Deep Learning.

Table VIII shows that all 30 data are in the negative range, with an average of 15.50 and a sum total of 465.00, indicating that the post-test values are consistently lower than the pre-test values, suggesting a reduction in information access time after

TABLE VIII
RANK I1-TA

		N	Average Range	Sum of ranks
Post-Test(sg) - Pre-Test(sg)	Negative Ranges	30[a]	15,50	465,00
	Positive ranges	0[b]	,00	,00
	Ties	0[c]		
	Total	30		
a. Post-Test(sg) < Pre-Test(sg)				
b. Post-Test(sg) > Pre-Test(sg)				
c. Post-Test(sg) = Pre-Test(sg)				

Table IX presents the statistical results of the Wilcoxon test to contrast the differences between the pre-test and post-test.

TABLE IX
CONFRONTATION STASTICS I1-TA

Test statistic[a]	
	Post-test(sg) - Pre-test(sg)
Z	-4,796[b]
Asymp. Sig (two-tailed)	<,001
a. Wilcoxon signed-rank test	
b. It is based on positive ranges.	

- H_0: No significant difference in information access time (TD) before and after the implementation of the intelligent system based on Deep Learning.
- H_1: There is a significant difference in the rate of identification of sensitive data (TD) before and after the implementation of the intelligent system based on Deep Learning.

Table X shows that all 30 data are in the positive range, with an average of 15.50 and a sum of 465.00, indicating that the post-test values are consistently higher than the pre-test values, suggesting an improvement in the rate of identification of sensitive data after implementation of the system.

TABLE X
RANK I2-TD

		N	Average Range	Sum of ranks
Post-test(%) - Pre-test(%)	Negative Ranges	0[a]	,00	,00
	Positive ranges	30[b]	15,50	465,00
	Ties	0[c]		
	Total	30		
a. Post-test(%) < Pre-test(%)				
b. Post-test(%) > Pre-test(%)				
c. Post-test(%) = Pre-test(%)				

Table XI presents the statistical results of the Wilcoxon test for the identification rate of sensitive data.

TABLE XI
CONFRONTATION STASTICS I2-TD

Test statistic[a]	
	Post-test(%) - Pre-test(%)
Z	-4,784[b]
Asymp. Sig (two-tailed)	<,001
a. Wilcoxon signed-rank test	
b. It is based on negative ranges.	

- H_0: No significant difference in data automation (DA) efficiency before and after implementation of the intelligent system based on Deep Learning.
- H_1: There is a significant difference in data automation (DA) efficiency before and after the implementation of the intelligent system based on Deep Learning.

Table XII shows that all 30 data are in the positive range, with an average of 15.50 and a sum of 465.00, indicating that the post-test values are consistently higher than the pre-test values, suggesting an improvement in data automation efficiency after implementation of the system.

TABLE XII
RANK I3-EA

		N	Average Range	Sum of ranks
Post-test(%) - Pre-test(%)	Negative Ranges	0[a]	,00	,00
	Positive ranges	30[b]	15,50	465,00
	Ties	0[c]		
	Total	30		
a. Post-test(%) < Pre-test(%)				
b. Post-test(%) > Pre-test(%)				
c. Post-test(%) = Pre-test(%)				

Similarly, Table XIII presents the statistical results of the Wilcoxon test for data automation efficiency.

TABLE XIII
CONFRONTATION STASTICS I3-EA

Test statistic[a]	
	Post-test(%) - Pre-test(%)
Z	-4,872[b]
Asymp. Sig (two-tailed)	<,001
a. Wilcoxon signed-rank test	
b. It is based on negative ranges.	

IV. DISCUSSION

Data automation theory points out that operational efficiency is significantly optimized when intelligent systems, such as those based on machine learning, are implemented to reduce time and resources used in key processes. According to [17], IoT systems and machine learning significantly improve prediction and decision making, and [14] showed that the use of Deep Learning can reduce processing time by 98%. In this study, the results showed that the average information access time decreased from 29.90 seconds in the pre-test to 15.77 seconds in the post-test, validating the positive impact of automation. Compared to the findings of [14], the reduction obtained in this case was higher, which can be attributed to the customized design of the algorithms adapted to the specific security environment, where the conditions and requirements differed significantly from the cases studied by the authors mentioned above. Furthermore, in comparison with [17], the results confirm that a strategic and contextualized approach to Deep Learning can maximize operational efficiency in specific sectors. This reflects that the implementation of technologies tailored to the needs of the business context not only improves access times, but also enhances overall business performance in a competitive and dynamic industry.

On the other hand, according to [12], deep learning has demonstrated its effectiveness in analyzing complex patterns in large volumes of data, allowing the identification of critical information with an accuracy of over 90% [10] also highlighted that intensive training of models in specific environments improves the adaptive capacity of intelligent systems. In this study, the results revealed an increase in the accuracy of sensitive data identification, with a significant improvement from 58.70% in the pre-test to 91.43% in the post-test, evidencing the positive impact of the implemented system. Comparing these results with those of [12], there are coincidences in the increase in accuracy, although in this case this percentage is exceeded, possibly due to the customization and adjustment of the model to the particular needs of the security company. Furthermore, while [10] emphasize the importance of advanced training, this study validates the relevance of adapting Deep Learning models to the operational context to maximize their performance. In conclusion, the accuracy achieved reflects not only the effectiveness of the applied technology, but also the importance of customizing intelligent systems according to industry requirements.

Similarly, according to [19], intelligent systems can significantly increase the efficiency in process automation, facilitating the management of large volumes of data and improving the speed and accuracy in the execution of repetitive tasks. In this study, the results reflected an increase in automation efficiency, from 28.67% in the pre-test to 95.67% in the post-test. These findings agree with those reported by [20], who observed substantial improvements when adapting automated systems to specific contexts. However, this study outperforms those results by customizing the Deep Learning model for the needs of a security company, an approach that highlights the importance of adjusting the technology to the characteristics of the operating environment. Unlike previous studies that applied more generalist models, this work demonstrates that a targeted approach maximizes efficiency, reducing human intervention and improving the consistency of results. In summary, the results obtained validate that a system based on Deep Learning significantly optimizes key processes, consolidating itself as a strategic tool in highly demanding business environments.

Finally, according to [8], advanced automation systems allow significantly reducing human intervention, improving efficiency and optimizing strategic decision making in demanding operational environments. Similarly, [21] emphasize that data automation based on deep neural networks ensures high accuracy in the classification and processing of critical information, which is essential in sectors that handle large volumes of sensitive data. In this study, the implementation of the Deep Learning system achieved outstanding results in the indicators evaluated: a reduction in the average time to access information from 29.90 to 15.77 seconds, an increase in the accuracy of identification of sensitive data from 58.70% to 91.43%, and an optimization of key processes with an increase in efficiency from 28.67% to 95.67%. These findings are in line with those of [21], ho highlighted the positive impact of customized solutions in specific contexts. However, this study exceeds those results by adjusting the algorithms to the needs of the security sector, which allowed maximizing the operational efficiency and ensuring the adaptability of the system. This demonstrated that the implementation of a Deep Learning-based system not only demonstrates its ability to transform data management processes, but also underscores the importance of customizing these technologies to maximize their impact in specialized sectors such as private security.

V. CONCLUSION

The implementation of an intelligent system based on Deep Learning in a private security company allowed to significantly automate internal processes, overcoming the limitations of traditional methods. This breakthrough resulted in improved access time to information and greater accuracy in identifying sensitive data, optimizing data management and contributing to more efficient strategic decisions. In addition, the system improved the automation of repetitive tasks, reducing manual intervention and increasing the consistency of operations. The customization of the model made it possible to adapt to the particularities of the environment, maximizing operational efficiency and reliability of results, optimizing resources and improving productivity. The findings demonstrate that advanced technologies such as Deep Learning are crucial to optimize key processes and increase competitiveness in critical sectors, consolidating themselves as strategic tools in data management and security.

For future research, it is suggested to focus on exploring the integration of complementary technologies, such as Machine Learning, Deep Learning and Artificial Intelligence (AI), to further improve the accuracy and adaptability of intelligent systems in dynamic environments. In addition, it would be valuable to investigate the application of these systems in other sectors beyond private security, such as healthcare or finance, to evaluate their effectiveness in managing sensitive data in different contexts. Another interesting field of study is the optimization of technological infrastructure, considering aspects such as cloud computing and data decentralization, to improve scalability and efficiency in the implementation of intelligent systems. It is also suggested to investigate the impact of data automation on strategic decision making at the organizational level, with a focus on long-term cost-benefit analysis.

REFERENCES

[1] A. Mumuni y F. Mumuni, «Automated data processing and feature engineering for deep learning and big data applications: A survey», *Journal of Information and Intelligence*, ene. 2024, doi: 10.1016/J.JIIXD.2024.01.002.

[2] M. Li, J. Liu, y Y. Yang, «Automated Identification of Sensitive Financial Data Based on the Topic Analysis», *Future Internet*, vol. 16, n.o 2, p. 55, feb. 2024, doi: 10.3390/fi16020055.

[3] Q. Liu et al., «A collaborative deep learning microservice for backdoor defenses in Industrial IoT networks», Ad Hoc Networks, vol. 124, p. 102727, ene. 2022, doi: 10.1016/J.ADHOC.2021.102727.

[4] H. Bangui, M. Ge, y B. Buhnova, «Deep-Learning based Reputation Model for Indirect Trust Management», Procedia Comput Sci, vol. 220, pp. 405-412, 2023, doi: https://doi.org/10.1016/j.procs.2023.03.052.

[5] A. Sulich, L. Sołoducho-Pelc, y S. Grzesiak, «Artificial Intelligence and Sustainable Development in Business Management Context – Bibliometric Review», Procedia Comput Sci, vol. 225, pp. 3727-3735, 2023, doi: https://doi.org/10.1016/j.procs.2023.10.368.

[6] M. Anshari, M. Syafrudin, A. B. Y. Tan, N. L. Fitriyani, y Y. Alas, «Optimisation of Knowledge Management (KM) with Machine Learning (ML) Enabled», INFORMATION, vol. 14, n.o 1, 2023, doi: 10.3390/info14010035.

[7] R. G. C. Schönhof y M. Fechter, «Towards automated Capability Assessment leveraging Deep Learning», Procedia CIRP, vol. 91, pp. 433-438, ene. 2020, doi: 10.1016/J.PROCIR.2020.02.195.

[8] J. Guaña-Moya, N. Salgado-Reyes, y C. Escobar-Terán, «Computing and data science using deep learning[La informática y la ciencia de datos utilizando Deep learning]», RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, vol. 2022, n.o E49, pp. 116-127, abr. 2022.

[9] H. Chen, N. Wei, L. Wang, W. Mubarak, M. A. Albahar, y Z. A. Shaikh, «The Role of Blockchain in Finance Beyond Cryptocurrency: Trust, Data Management, and Automation», IEEE Access, vol. 12, pp. 64861-64885, ene. 2024, doi: 10.1109/ACCESS.2024.3395918.

[10] X. Xiao, T. X. Trinh, Z. Gerelkhuu, E. Ha, y T. H. Yoon, «Automated machine learning in nanotoxicity assessment: A comparative study of predictive model performance», Comput Struct Biotechnol J, vol. 25, pp. 9-19, dic. 2024, doi: 10.1016/j.csbj.2024.02.003.

[11] C. Yaiprasert y A. N. Hidayanto, «AI-driven ensemble three machine learning to enhance digital marketing strategies in the food delivery business», Intelligent Systems with Applications, vol. 18, p. 200235, 2023, doi: https://doi.org/10.1016/j.iswa.2023.200235.

[12] P. V. A. Alves et al., «Machine Learning Applied to Anomaly Detection on 5G O-RAN Architecture», Procedia Comput Sci, vol. 222, pp. 81-93, 2023, doi: https://doi.org/10.1016/j.procs.2023.08.146.

[13] M. Pandey, M. Arora, S. Arora, C. Goyal, V. K. Gera, y H. Yadav, «AI-based Integrated Approach for the Development of Intelligent Document Management System (IDMS)», Procedia Comput Sci, vol. 230, pp. 725-736, 2023, doi: https://doi.org/10.1016/j.procs.2023.12.127.

[14] B. Li et al., «Construction of a Smart Supply Chain for Sand Factory Using the Edge-Computing-Based Deep Learning Algorithm», Sci Program, vol. 2022, 2022, doi: 10.1155/2022/9607755.

[15] M. Jafari, A. Kavousi-Fard, M. Dabbaghjamanesh, y M. Karimi, «A Survey on Deep Learning Role in Distribution Automation System: A New Collaborative Learning-to-Learning (L2L) Concept», IEEE ACCESS, vol. 10, pp. 81220-81238, 2022, doi: 10.1109/ACCESS.2022.3195053.

[16] Z. E. Huma et al., «A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things», IEEE Access, vol. 9, pp. 55595-55605, 2021, doi: 10.1109/ACCESS.2021.3071766.

[17] F. A. D. Freitas et al., «IoT System for School Dropout Prediction Using Machine Learning Techniques Based on Socioeconomic Data», Electronics (Basel), vol. 9, n.o 10, 2020, doi: 10.3390/electronics9101613.

[18] A. Duru, İ. R. Karaş, F. Karayürek, y A. Gülses, «A Deep Learning Approach for Classification of Dentinal Tubule Occlusions», Applied Artificial Intelligence, vol. 36, n.o 1, 2022, doi: 10.1080/08839514.2022.2094446.

[19] J. de Godoy, K. Otrel-Cass, y K. H. Toft, «Transformations of trust in society: A systematic review of how access to big data in energy systems challenges Scandinavian culture», Energy and AI, vol. 5, p. 100079, sep. 2021, doi: 10.1016/J.EGYAI.2021.100079.

[20] A. S. Camanho, M. C. Silva, F. S. Piran, y D. P. Lacerda, «A literature review of economic efficiency assessments using Data Envelopment Analysis», Eur J Oper Res, vol. 315, n.o 1, pp. 1-18, may 2024, doi: 10.1016/J.EJOR.2023.07.027.

[21] H. M. Soliman, D. Sovilj, G. Salmon, M. Rao, y N. Mayya, «RANK: AI-Assisted End-to-End Architecture for Detecting Persistent Attacks in Enterprise Networks», *IEEE Trans Dependable Secure Comput*, 2023, doi: 10.1109/TDSC.2023.3338136.