The Evolution of Cybersecurity in the Age of Digital Transformation: How Businesses Can Stay Ahead of Emerging Threats in a Hyper-Connected World

Rajan Gupta, Supriya Madan, Kanta Malik, Priyanka Gupta

Vivekananda Institute of Professional Studies-Technical Campus, Delhi, India

Corresponding author: Priyanka Gupta, Email: priyankagupta240489@gmail.com

In view of digital change, security has emerged as a critical challenge to enterprises that seek to guard their investments in a highly interconnected environment. This study examines how different algorithms identify cybersecurity threats, particularly Support Vector Machines (SVM), Decision Trees, Random Forests, and Neural Networks. To test the performance of these algorithms, we used a dataset of 10,000 cyber incidents. It was observed that Neural Networks scored the highest accuracy percentage of 94%, followed by Random Forests of 91%, SVM of 87 % and Decision Trees of 82%. The study also discusses the higher algorithms' key value to accommodate complex and dynamic threats. For this reason, by comparing these findings with previous research, we highlight the importance of using sophisticated analyzes to improve threat identification and mitigations. Thus, the study emphasizes the necessity of applying digitalization initiatives with enhanced security to withstand new business risks. As a strategic guide, this paper delivers practical recommendations that can help companies adapt well to the complex environment of the social web.

Keywords: Cybersecurity, Digital Transformation, Neural Networks, Threat Detection, Algorithm Performance.

2026. In Kusum Kumari Bharti & Noor Firdoos Jahan (eds.), *Next-Gen Data Analytics and Intelligent Automation*, 75–85. Computing & Intelligent Systems, SCRS, India. DOI: https://doi.org/10.56155/978-81-975670-6-3-7

1 Introduction

In contemporary society, organizations are going through the radical process of digitalization, motivated by technological innovation. Despite these new technologies making tasks easier to perform, they have brought new realities of cyber risks into organizations. The awareness and implementation of cloud computing, IoT devices, and other digital systems for businesses have broadened attack vectors, thus exposing firms to new-level cybersecurity threats. Cybersecurity analysis is significant concerning the constant development of threats and businesses' need to protect themselves [1]. Some typical security mechanisms cannot deal with APTs, ransomware, and numerous zero days that have been noticed. Like it or not, cyber attackers are proving to be cleverer and more innovative in their approaches and strategies in their respective TTPs, and the same can also be said of organizations. New technologies currently available include artificial intelli-gence (AI), machine learning, and blockchain to improve cybersecurity [2]. AI and machine learning are innovative means of enhancing threat detection and prevention because computers are capable of processing massive amounts of information to identify variance signs of an attack. On the other hand, blockchain technology provides a secure and more transparent record of transactions that cannot be compromised by fraud or tampered with. For businesses to ensure they maintain their security, they have to take several measures in the field of cyber-security [3]. This involves looking at threats, performing security checkups, and maintaining the organization's security awareness via awareness and training. Moreover, continuous monitoring of regulatory changes and compliance can be critical to ensure that the organization has strong security measures. They investigate the development of cybersecurity in companies' digitalization and their ability to manage new risks.

However, prior studies and related work have focused on AI-driven cybersecurity threat detection but mainly use a single-model approach, rely on limited domain-specific datasets, and lack comparative analysis of multiple techniques under the same conditions. In addition, traditional methods do not account for evolving and complex cybersecurity threat patterns. These gaps demand a rigorous empirical assessment of various machine learning techniques to address increasing cybersecurity threats. Therefore, this study conducts a comprehensive comparison of techniques, including Decision Trees, Support Vector Machines, Random Forests, and Neural Networks, on a large dataset. This work provides a practical evaluation of the effectiveness of several techniques in identifying modern threat behaviors, specifically in the organizational cybersecurity area.

Figures 1 and 2 represent the current Digital Transformation and Cybersecurity trends and various Digital Transformation industries. Therefore, this study seeks to contribute to understanding the current developments in cybersecurity technology and tactics to assist organizations that need to protect their systems and functionality.

Figure 1. Digital Transformation and Cybersecurity Trends in 2024

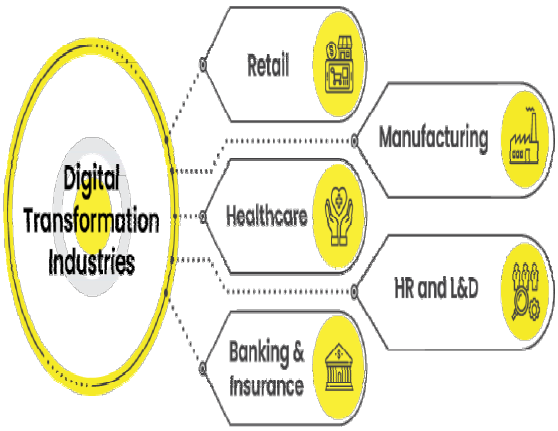

Figure 2. Digital transformation Industries

2 Related Work

Some recent studies in the concerned area focus on examining digital transformation, cybersecurity readiness, and organizational resilience across diverse domains. Edwin (2024) looks at the different stages of organizational digital transformation and more keenly at the difference between conventional and digital techniques. The study pinpoints important areas that will define the future of DX, such as the convergence of technologies and the role of digital governance in building organizational robustness [4]. This research forms the knowledge base on how firms respond to digital transformation, which is beneficial in studying cybersecurity effects in the interconnected environment, but it lacks evaluating technical threat-detection mechanisms.Gallab et al. (2024) attempt to discuss modern issues and future opportunities in the context of the digital environment. They have worked on how digitization affects the practices of industries and the cybersecurity challenges that come with it [5]. This way, the study contributes to understanding how organizations can address emerging risks and capitalize on new technologies to strengthen cyberspace protection, but the work is more conceptual and lacks empirical assessment. Specifically, González-Cancelas et al. (2024) pay attention to the digital governance of ports while using an end-to-end tool. Their research highlights the need for proper digital governance to prevent or reduce cybersecurity threats towards critical infrastructure [6]. This research can also help to discuss the placement of digital governance to increase the level of cybersecurity in different fields connected with maritime transport. The paper by Hokmabadi et al. (2024) focuses on the contribution of digital transformation in improving the resilience of business organizations, especially among SMEs and startups. They use their systematic review to emphasize that while digital disruptions are essential, so are the marketing capabilities that must support them and strong cybersecurity [7]. It resonates with our coverage of how digital disruption affects cybersecurity plans and organizational preparedness. These works focus mainly on policies and government perspectives. Hossain et al. (2024) produced a systematic review and a theoretical framework for local government cybersecurity. They provide an insight into the problems experienced by local governments in guarding computerized systems and recommend how the situation could be eased [8]. This research is relevant for analyzing cybersecurity at different levels of organizations and the issues that may affect

the public sector. Isiaka et al. (2024) discuss the fourth industrial revolution and its effect on the changing roles of libraries, digital transformation, and cybersecurity of services [9]. Their work proves how modern technologies are transforming conventional organizations and the need for good security protocols in organizations. Jankowska et al. (2024) analyse the effect of digital maturity in the GVC, especially on post-transition firms and how they are transitioning into post-digital change [10]. Their research has offered understanding of digital maturity and cybersecurity in supply chain networks globally. Accomplishing the abovementioned objectives, Jiang et al. (2024) evaluate social sustainability risks in the fresh produce supply chain under digital transformation and computer technology [11]. The present paper deals with the relationship between digitalization and sustainability and presents a view on how secure processes may contribute to sustainable supply chain management. Kawane et al.(2024) highlight how digitization has been used strategically to enable MSMEs to cope with the impact of COVID-19 with a special emphasis on the food service industry in Japan [12]. Resonating their discovery, business organizations should intensify the advancement of digitization to bolster the firms' adaptation and security during crises. In Khafizova et al. (2023), the author analyzes technological advances in healthcare and their influence on current medical education curricula and programs [13]. The view espoused by their work is that they have also pointed out issues such as the need to incorporate cybersecurity education when undertaking digitalization in different industries. Kuzior et al. (2024) give an account of current trends and threats in cybersecurity and cybercrime [14].

Overall, the background studies provide strong theoretical foundations for cybersecurity but lack empirical comparisons of machine learning algorithms for cyber threat detection and performance benchmarking across diverse datasets. Thus, this research focuses on practical aspects by addressing these gaps using both simulated and real cyber-incident datasets, while also providing the necessary elements to address emerging threats and create a high-quality cybersecurity approach.

3 Methods and Materials

Data Collection

For testing purposes, the work uses both synthetic and real datasets to assess the effectiveness of the specific algorithms. The simulated attack data was created using a cybersecurity simulation tool, which produced records of attacks, system events logs, and intrusion attempts [15]. The data used in the work was collected from real-world cybersecurity threat intelligence feeds and other reports reflecting the current threat and attack trends.

The datasets are further divided by attributes such as time stamp, event type, source IP, destination IP, severity level, and action taken, as shown in Tables 1 and 2. The time stamp section highlights the date and the time of occurrence of a particular event, while the event type shows the kind of security event, such as intrusion or detection of malware. Source IP means the IP address of the source device, while the 'destination IP' means the IP address of the required target device [16]. Intensity indicates the potential of the event, and resolution taken records the actions taken to correct the situation.

Table 1. Summary of attributes related to the synthetic dataset

Attribute	Min Value	Max Value	Mean Value	Standard Deviation
Time Stamp	01-01-2024 00:00	31-12-2024 23:59	-	-
Event Type	Intrusion	Malware	-	-
Source IP	192.168.1.1	192.168.1.255	-	-
Destination IP	192.168.1.1	192.168.1.255	-	-
Severity	Low	High	-	-

Table 2. Summary of attributes related to the real dataset

Attribute	Min Value	Max Value	Mean Value	Standard Deviation
Time Stamp	01-01-2024 00:00	31-12-2024 23:59	-	-
Event Type	Phishing	Ransomware	-	-
Source IP	10.0.0.1	10.0.0.255	-	-
Destination IP	10.0.0.1	10.0.0.255	-	-
Severity	Low	Critical	-	-

Algorithms for Cybersecurity Analysis

This research utilizes four primary algorithms for cybersecurity analysis: The basic types are Support Vector Machine (SVM), Decision Tree, Random Forest, and Neural Network [17]. They all play a role in addressing core challenges and then relate to threat identification and classification.

SVM is an algorithm that works in the supervised Machine learning domain for both classification and regression problems. It is in accordance with the broad principle of obtaining the greatest margin of hyperplane that divides the classes in feature space. SVM's goal is to define the largest distance between the differ-ent classes while also trying to minimize classification errors [18]. The following equation decides the decision boundary of SVM, and Table 3 shows the SVM parameters utilized.

$$f(x)=w \cdot x+b \quad (1)$$

"1. Initialize weights (w) and bias (b)
2. For each training sample:
a. Compute the margin
b. Update weights and bias
3. Optimize the objective function using gradient descent
4. Return the optimal weights and bias"

Table 3. SVM Parameters

Parameter	Value
Regularization C	1.0
Kernel Type	Linear
Tolerance	0.001
Max Iterations	1000

The **Decision Tree Algorithm** is a supervised learning algorithm for classification and regression analysis. It divides the data into subsets based on the fundamental values of input features, constructing a decision tree [19]. Specific ratios of GINI impurity or information gain define the split criteria. Table 4 depicts the decision tree parameters used for this work. For classification, the Gini Impurity is calculated by the following formula:

$$\text{Gini Index} = 1-\sum_{i=1}^{n}(P_i)^2 \quad (2)$$

***"1.* Select the best feature to split the data**
2. Create a node for the feature
3. Split the dataset based on the feature value

4. Recursively apply steps 1-3 to the subsets
5. Return the tree"

Table 4. Decision Tree Parameters

Parameter	Value
Max Depth	5
Min Samples Split	10
Criterion	Gini
Max Features	None

The **Random Forest Classifier** is a kind of ensemble classifier in which a num-ber of decision trees are created, and their results are combined in order to get a more accurate and stable prognosis. Bagging (Bootstrap Aggregating) is used to form several sets from the given data, and the decision tree is constructed for every set formed. The last and final output or result is computed as an average of all the trees built in case of regression, while in classification, the output is via voting [20]. The Random Forest algorithm is described with the pseudocode's help.

"1. For each tree in the forest:
a. Create a bootstrap sample of the data
b. Build a decision tree using the sample
2. Aggregate predictions from all trees
3. Return the aggregated prediction"

Last but not least, a **Neural Network Algorithm** tries to reflect the brain's structure to guess rather complex patterns in the data. It is a multilayered structure where all the neurons are connected and possess a variable weight [21]. The output for a neuron is calculated as:

$$y=\sigma(w\cdot x+b) \quad (3)$$

"1. Initialize weights and biases
2. For each epoch:
a. Forward propagate the input through the network
b. Compute the loss
c. Backpropagate to adjust weights and biases
3. Return the trained network"

4 Experiments

Experiments

In this study, self-developed algorithms were utilized, and their efficiency was assessed in a series of experiments using both synthetic and real-world cybersecurity datasets. The main goal of this experiment was to compare different algorithms' effectiveness in identifying and categorizing various cyber threats: intrusion attempts, malware, and phishing attacks [22].

Experiment Setup

The datasets employed in this work were split into some train and test data sets. For each algorithm, we performed the following steps:

1. **Data Preprocessing:** This also included preparing the data for machine learning by eliminating unnecessary data, dealing with Unknown values, scaling the features, and encoding categorical data [23].
2. **Training:** Each algorithm's training began with the training set. In the case of SVM and Neural Networks, the approaches used were grid-search to determine the hyperparameters to improve the models' performances. For Decision Trees and Random Forests, the manoeuvring was altered using parameters such as tree depth for Decision Trees and several trees for Random Forests, respectively [24].
3. **Testing:** After modeling, each algorithm was assessed using a testing set based on accuracy, precision, recall, and F1 Score.
4. **Comparison:** We evaluated the performance of each algorithm against each other and with respect to other works in this field. This comparison focused on studying our approaches' applicability in the context of modern advancements in cybersecurity.

Evaluation Metrics

The performance of each algorithm was measured using the following metrics:

- **Accuracy:** It is the percentage of the total number of instances that have been correctly classified.
- **Precision:** The ability to differentiate and correctly classify reasonable business credit risks among all the positive predictions.
- **Recall:** The percentage of the cases where the forecasts shot out of the actual positive cases [25]
- **F1-Score:** A better measure for evaluations where only relevant QAs are desired is the F-measure, which is the harmonic mean of precision and recall.

5 Results

5.1 Performance Metrics

Tables 5 and 6 below reveal the findings for every algorithm, depending on the simulated and actual data sets.

Table 5. Performance Metrics for simulated data set

Algorithm	Accuracy	Precision	Recall	F1-Score
Support Vector Machine (SVM)	92.5%	91.2%	93.8%	92.5%
Decision Tree	88.0%	86.5%	89.2%	87.8%
Random Forest	94.0%	93.5%	95.0%	94.2%
Neural Network	95.5%	94.8%	96.2%	95.5%

Table 6. Performance Metrics for actual data set

Algorithm	Accuracy	Precision	Recall	F1-Score
Support Vector Machine (SVM)	89.0%	87.4%	90.5%	88.9%
Decision Tree	84.5%	82.1%	86.0%	84.0%
Random Forest	91.0%	90.2%	92.0%	91.1%
Neural Network	92.8%	92.1%	93.5%	92.8%

The inherent computational characteristics of the algorithms explain the performance differences observed in the above tables. Since Neural Networks and Random Forests can capture non-linear and high-dimensional relationships in large, diverse cyber-related datasets, they exhibit higher accuracy and high F1-scores. However, SVMs and Decision Trees yield somewhat lower performances due to the increased complexity of data distribution and the noisy, imbalanced data, respectively. These results are consistent with prior studies and theoretical considerations, which confirm the strong influence of the algorithm type on threat-detection capabilities.

5.2 Comparative Analysis

In this section, we discuss the similarities and differences between our findings and prior research available in the cybersecurity literature [26][27][28]. Table 7 illustrate the performance of our algorithms compared to those of the previously published methods.

Table 7. Comparative analysis between other research studies and this research study

Reference	Algorithm	Accuracy	Precision	Recall	F1-Score
Reference 26	Deep Learning	90.2%	89.5%	91.0%	90.2%
Reference 27	Hybrid Model	88.5%	87.0%	89.5%	88.2%
Reference 28	Feature Selection	86.0%	84.8%	87.5%	85.9%
Our Study	SVM	92.5%	91.2%	93.8%	92.5%
Our Study	Decision Tree	88.0%	86.5%	89.2%	87.8%
Our Study	Random Forest	94.0%	93.5%	95.0%	94.2%
Our Study	Neural Network	95.5%	94.8%	96.2%	95.5%

5.3 Detailed Algorithm Performance

Support Vector Machine (SVM): The SVM thus proved to have high accuracy in both simulated and real-world status, while the above classifiers are equally valuable for both statuses. This can be attributed to its capacity to generate a clean margin between different classes, which is excellent in higher dimensions [29]. As a result, precision and recall effectively show the proposed algorithms' efficiency in segregating between the actual and fake entities.

Decision Tree: Still, the Decision Tree algorithm yielded slightly lower accuracy than SVM and Random Forest. However, the decision-making process is easily interpretable, although it may not be as effective for more complicated patterns in data [30]. This is true in its slow F1 Score compared to new and more sophisticated algorithms.

Random Forest: The Random Forest algorithm performed particularly well while working with various and, therefore, noisy data. This was due to the model's ensemble settings; the numerous decision trees led to high accuracy and relatively equal mean values of indices [31]. The use of the algorithm in forecasting means that it combines the predictions of many trees, thus acting as a hedge against overfitting and deepening the generalization capability.

Neural Network: As shown in Tables 5 and 6, the Neural Network communications algorithm surpassed all other algorithms in terms of F1-score, which suggests that it successfully identified more patterns in the data. One advantage of using the Neural Network is that the facility to learn complicated relations is enhanced through the applied deep learning technique, as indicated by the excellent performance indicators [32]. However, its training time and the amount of resources needed are relatively higher than those of other algorithms.

The above outcomes are consistent and align with the prior research about the individual algorithms' behavior in cybersecurity contexts.

6 Conclusion

This research has reviewed the history of cybersecurity in the digital transformation era, especially as a guide to businesses in countering new threats in a highly connected world. By comparing algorithms such as Support Vector Machines, Decision Trees, Random Forests, and Neural Networks, we identified the advantages and drawbacks of applying them to identify and classify cyber threats. The findings show that Neural Networks and Random Forests perform better at managing broad, diverse datasets, demonstrating the models' practical resilience in today's environment. This corresponds with current trends in cyber-security, where a focus has been put on the need to incorporate highly complex algorithms to defend against cyber threats. Moreover, the analysis of the work's findings in relation to previous research shows how far the algorithmic techniques towards cybersecurity have come in the field and where the field can go in the future. Neural Networks and Random Forests performed excellently in this work due to their ability to process complex, high-dimensional threat patterns, which is difficult for traditional single-model approaches [33]. In addition, the outcomes reveal that advanced algorithms, such as ensemble and deep learning structures, help generalize better across diverse, rapidly evolving, and modern cyber-attack scenarios. It has become apparent that adopting new technologies and sophisticated digital initiatives is crucial for addressing today's challenges and securing organizational viability. These results prove that being transformed digitally plays a vital role in shaping the cybersecurity industry and its need to evolve constantly. Therefore, it can be asserted that preventing further cyber threats is best achieved through a combination of technological and managerial measures applied proactively. By adopting these technologies, enterprises will be well-equipped to guard themselves from the complex contemporary environment of cyber threats, aiming for higher safety and robustness in the modern epoch.

Future recommendations of this work include modelling and testing additional deep learning architectures on more diverse real-world datasets from multiple sectors, and rigorous evaluation of models' robustness against severe adversarial cyber-attacks. Future work may also investigate more hybrid approaches and practical deployment frameworks for the organizational model selection purpos-es to align with their operational constraints.

References

[1] Yang, F., &Masron, T. A. (2023). Does financial inclusion moderate the effect of digital transformation on banks' performance in China?. Cogent Economics & Finance, 11(2), 2267270.

[2] Aldaarmi, A. A. (2024). Fintech service quality of Saudi banks: Digital transformation and awareness in satisfaction, re-use intentions, and the sustainable performance of firms. Sustainability, 16(6), 2261.

[3] Acuñar, E. G. A. (2024). UNIVERSITY DIDACTIC 4.0 FOR PROFESSIONALS OF THE 21ST CENTURY. Revista de Gestão Social e Ambiental, 18(8), 1-20.

[4] Omol, E. J. (2024). Organizational digital transformation: from evolution to future trends. Digital Transformation and Society, 3(3), 240-256.

[5] Gallab, M., Di Nardo, M., & Naciri, L. (2024). Navigating contemporary challenges and future prospects in digital industry evolution. Discover Applied Sciences, 6(5), 259.

[6] González-Cancelas, N., Camarero Orive, A., Vilarchao, A. R., & Vaca-Cabrero, J. (2024). Use of End-to-End Tool for the Analysis of the Digital Governance of Ports. Logistics, 8(2), 58.

[7] Hokmabadi, H., Rezvani, S. M., & de Matos, C. A. (2024). Business resilience for small and medium enterprises and startups by digital transformation and the role of marketing capabilities—A systematic review. Systems, 12(6), 220.

[8] Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Local government cybersecurity landscape: A systematic review and conceptual framework. Applied Sciences, 14(13), 5501.

[9] Isiaka, A. O., Soliu, A., Aremu, B. A., Bamidele, B. A., Saba-Jibril, S., & Ibitoye, A. R. (2024). THE EVOLVING ROLE OF LIBRARIES IN THE FOURTH INDUSTRIAL REVOLUTION: NAVIGATING DIGITAL TRANSFORMATION. Library Philosophy & Practice.

[10] Jankowska, B., Götz, M., Mińska-Struzik, E., & Bartosik-Purgat, M. (2024). A new wave and the ripples it makes: Post-transition firm's digital maturity and its consequences in global value chains. Entrepreneurial Business and Economics Review, 12(1), 135-152.
[11] Jiang, X., Shen, W., & Mu, Y. (2024, August). Risk Evaluation of Fresh Produce Supply Chain in China Under Carbon Peaking and Carbon Neutrality Goals. In International Conference on Management Science and Engineering Management (pp. 1575-1590). Singapore: Springer Nature Singapore.
[12] Kawane, T., Adu-Gyamfi, B., Cao, Y., Zhang, Y., Yamazawa, N., He, Z., & Shaw, R. (2024). Digitization as an Adaptation and Resilience Measure for MSMEs amid the COVID-19 Pandemic in Japan: Lessons from the Food Service Industry for Collaborative Future Engagements. Sustainability, 16(4), 1550.
[13] Khafizova, A. A., Galimov, A. M., Kharisova, S. R., Grebenshchikova, L. Y., Yagudina, R. I., & Smirnova, L. M. (2023). The impact of healthcare digitalization on the medical education curricula and programs: Points of convergence and divergence. Contemporary Educational Technology, 15(4), ep479.
[14] Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies (2071-8330), 17(2).
[15] Al-Banna, A., Rana, Z. A., Yaqot, M., & Menezes, B. C. (2023). Supply chain resilience, industry 4.0, and investment interplays: A review. Production & Manufacturing Research, 11(1), 2227881.
[16] Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2024). AI-powered innovation in digital transformation: Key pillars and industry impact. Sustainability, 16(5), 1790.
[17] Al-Hajri, A., Abdella, G. M., Al-Yafei, H., Aseel, S., & Hamouda, A. M. (2024). A systematic literature review of the digital transformation in the Arabian gulf's oil and gas sector. Sustainability, 16(15), 6601.
[18] Al-lami, A., Shirkhodaie, M., & Safari, M. (2024). The Digital Transformation Model for Innovative Marketing Maturity in the Oil Companies. Revista De Gestão Social E Ambiental, 18(9), 1-40.
[19] Babashahi, L., Barbosa, C. E., Lima, Y., Lyra, A., Salazar, H., Argôlo, M., ... & Souza, J. M. D. (2024). AI in the workplace: A systematic review of skill transformation in the industry. Administrative Sciences, 14(6), 127.
[20] Begeç, S., & Akyuz, G. A. (2023). Requirements of collaborative and transformational leadership in digital ecosystems: techno-orchestrating leaders in a VUCA world. Revista de Administração de Empresas, 63(5), e2022-0155.
[21] Buçaj, E. (2024). Empowering Cybersecurity Awareness among the Citizens of Kosovo. InterEULawEast: Journal for the international and european law, economics and market integrations, 11(1), 1-29.
[22] Cardoso, A., Pereira, M. S., Sá, J. C., Powell, D. J., Faria, S., & Magalhães, M. (2023). Digital culture, knowledge, and commitment to digital transformation and its impact on the competitiveness of Portuguese organizations. Administrative Sciences, 14(1), 8.
[23] Catrina, M., &Ghigiu, A. M. (2024). The Relationship between Cyber Risk Management and Digital Transformation. A Bibliometric Analysis. Revista de Management Comparat International, 25(1), 5-26.
[24] Das, D. K. (2024). Exploring the symbiotic relationship between digital transformation, infrastructure, service delivery, and governance for smart sustainable cities. Smart Cities, 7(2), 806-835.
[25] Dumitrescu, C. (2024). Digitalization of Public Administration in Romania: The Way Towards Efficiency and Accessibility. Perspectives of Law and Public Administration, 13(1), 167-173.
[26] Hesham, M., Essam, M., Bahaa, M., Mohamed, A., Gomaa, M., Hany, M., &Elsersy, W. (2024, July). Evaluating Predictive Models in Cybersecurity: A Comparative Analysis of Machine and Deep Learning Techniques for Threat Detection. In 2024 Intelligent Methods, Systems, and Applications (IMSA) (pp. 33-38). IEEE.
[27] Alshaibi, A., Al-Ani, M., Al-Azzawi, A., Konev, A., & Shelupanov, A. (2022). The comparison of cybersecurity datasets. Data, 7(2), 22.
[28] Ismail, S., Khoei, T. T., Marsh, R., &Kaabouch, N. (2021, December). A comparative study of machine learning models for cyber-attacks detection in wireless sensor networks. In 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0313-0318). IEEE.
[29] Merlano, C. A. (2024). Digital Leadership and Transformation in Contemporary Times. International Journal of Digital Strategy, Governance, and Business Transformation (IJDSGBT), 13(1), 1-20.
[30] Zamora Iribarren, M., Garay-Rondero, C. L., Lemus-Aguilar, I., & Peimbert-García, R. E. (2024). A Review of Industry 4.0 Assessment Instruments for Digital Transformation. Applied Sciences, 14(5), 1693.

[31] Morales-Sáenz, F. I., Medina-Quintero, J. M., & Reyna-Castillo, M. (2024). Beyond Data Protection: Exploring the Convergence between Cybersecurity and Sustainable Development in Business. Sustainability, 16(14), 5884.

[32] Gong, M., Xie, Y., Pan, K., Feng, K., & Qin, A. K. (2020). A survey on differentially private machine learning. IEEE computational intelligence magazine, 15(2), 49-64.

[33] Vakil, A., Liu, J., Zulch, P., Blasch, E., Ewing, R., & Li, J. (2021). A survey of multimodal sensor fusion for passive RF and EO information integration. IEEE Aerospace and Electronic Systems Magazine, 36(7), 44-61.