Balancing Security and Information Management in the Digital Workplace

Rabah Scharif [1], Ossama Embarak[2,*]

[1]Applied Engineering Department, Institute of Applied Technology, UAE

[2]Higher Colleges of Technology (HCT), UAE

Email: rabah.scharif@aths.ac.ae; oembarak@hct.ac.ae

Abstract

As the digital workplace becomes more prevalent, organizations are faced with the challenge of balancing security and information management. On one hand, there is a need to protect sensitive data and prevent cyberattacks, while on the other hand, organizations must enable employees to collaborate and share information effectively. Machine learning (ML) is a promising technology that can help organizations address this challenge. By analyzing data patterns and identifying potential security threats, ML algorithms can enhance security measures and mitigate risks. At the same time, ML can also facilitate information management by automating routine tasks and improving the accuracy of data analysis. In this paper, we explore the role of ML in balancing security and information management in the digital workplace. We propose a hybrid ML model that integrates autoencoder and convolutional subnetworks in unified architecture to help capturing and security threats in the digital workplace, without compromising the information management tasks. We also present a case study of a real-world implementation of ML in a digital workplace setting, highlighting the benefits and limitations of this approach. Our findings suggest that ML can be a valuable tool for achieving a balance between security and information management in the digital workplace, but its successful implementation requires careful consideration of organizational context and stakeholder needs.

Keywords: Security; Risks; Digital data; Machine Learning

1. Introduction

As the digital workplace continues to evolve, organizations face the challenge of balancing security and information management. On the one hand, they need to protect sensitive data and intellectual property, comply with regulations, and prevent cyber-attacks [1]. On the other hand, they need to enable employees to work collaboratively, share information, and access the resources they need to be productive. Achieving a balance between security and information management requires a holistic approach that considers the entire organization's needs, including people, processes, and technology.

Machine learning (ML) is a technology that has the potential to help organizations balance security and information management in the digital workplace. By analyzing data patterns and identifying potential security threats, ML algorithms can enhance security measures and mitigate risks. At the same time, ML can also facilitate information management by automating routine tasks and improving the accuracy of data analysis [2-4]. However, implementing ML systems in the digital workplace requires careful consideration of organizational context and stakeholder needs. Organizations must involve employees, IT professionals, and data privacy experts in the development and implementation of ML systems to ensure that they meet the needs of all stakeholders and comply with relevant regulations.

Doi : https://doi.org/10.54216/JCIM.110201
Received: November 18, 2022 Revised: January 02, 2023 Accepted: March 02, 2023

This paper explores the potential of ML to address the challenge of balancing security and information management in the digital workplace. We include a real-world case study that highlights the benefits and limitations of ML for balancing security and information management in the digital workplace. We hybrid ML model, which combines autoencoder and convolution subnetworks, as a valuable tool for achieving a balance between security and information management in the digital workplace, but its successful implementation requires a holistic approach that considers the broader organizational context [5-6]. By providing a comprehensive analysis of the potential of ML for balancing security and information management in the digital workplace, our paper contributes to a deeper understanding of this critical issue and provides valuable insights for organizations seeking to enhance their security and information management practices in the digital age.

The next section is the related work studies. Then section 3 has the proposed solution and section 4 has the experemental analysis. The last section is the conclusion ast section 5.

2. Related Work

The literature on ML for balancing security and information management in the digital workplace is rapidly evolving, reflecting the growing importance of this topic in modern organizations. Many studies have focused on the use of ML for cybersecurity, such as detecting anomalies and predicting potential threats. The authors of [5] discussed the importance of balancing integration and flexibility in e-business architectures to effectively manage business transformation. They argued that traditional approaches to e-business architecture do not adequately address the dynamic nature of modern business environments and proposed a framework that incorporates a modular, service-oriented approach to support agile and flexible business processes. The authors of [6] proposed a framework for developing effective digital business strategies. The paper argues that the rapid pace of technological change, coupled with the increasing importance of digital channels in business, requires a new approach to strategy development that incorporates both traditional business strategy concepts and emerging digital technologies. The proposed framework included three components: digital assets, digital capabilities, and digital infrastructures. The paper also discusses the implications of the framework for strategic decision-making and provides insights into how organizations can leverage digital technologies to create competitive advantage. The authors of [8] examined the potential benefits of digital transformation for Germany's industrial sector. The paper argues that digital technologies such as the cloud, the IoT, and Big Data analytics have the potential to drive significant improvements in productivity, efficiency, and innovation. They discussed the number of case studies from German companies that have successfully implemented digital transformation initiatives, highlighting the benefits that these initiatives have delivered. They also addressed some of the challenges that companies may face in implementing digital transformation, such as concerns around data privacy and security. The authors of [12] investigated the impact of digital transformation on the automotive industry. The paper presents findings from a case study of a German automotive manufacturer that underwent a digital transformation initiative. They discussed the various components of the initiative, including the use of Big Data analytics, cloud computing, and mobile technologies. The authors of [14] presented a comprehensive review of the literature on the topic and provide insights into the potential implications of robotics for various industries, including manufacturing, healthcare, and transportation. They also discussed the ethical and societal implications of robotics and digital transformation, such as the potential displacement of human workers and the need for new forms of social protection. The authors of [16] discussed the various components of digital transformation, including the IoT, cloud computing, and Big Data analytics, and highlights the potential benefits and challenges associated with each. They also provided a comprehensive overview of the state of digital transformation in various industries, including manufacturing, healthcare, and energy. They argued that the successful adoption of digital technologies will require significant changes in organizational culture and mindset, as well as new skills and competencies. The authors of [19] presented a framework for developing an Information System (IS) strategic plan using the IT Balanced Scorecard (BSC). They argued that the combination of these two frameworks can help organizations align their IS strategy with their overall business strategy, while also ensuring that the IS strategy is aligned with the needs of the organization's stakeholders. They provided a step-by-step guide for developing an IS strategic plan using the framework, including the identification of strategic objectives, the development of performance measures, and the establishment of an implementation plan. The authors of [23] argued that Information Systems (IS) research should incorporate more philosophical perspectives in order to address the complex ethical and social issues raised by digital transformation. The paper suggests that IS research should move beyond technical considerations and instead focus on the ethical and social implications of digital transformation. They argued that a philosophical approach can help to provide a more holistic understanding of the impact of digital transformation on society and can help to identify potential solutions to the challenges posed by the digital era. The paper also discusses the need for IS research to engage with values such

Doi : https://doi.org/10.54216/JCIM.110201
Received: November 18, 2022 Revised: January 02, 2023 Accepted: March 02, 2023

as ethics, justice, and responsibility in order to ensure that digital transformation is aligned with the needs of society. Overall, the paper offers a valuable perspective on the role of philosophy in IS research and the importance of considering ethical and social issues in the context of digital transformation. The authors of [25] presented a framework for structuring digital transformation efforts within organizations. The framework consists of six action fields: "strategy and governance," "processes and organization," "culture and leadership," "skills and capabilities," "technology and infrastructure," and "business models and ecosystems." The paper applies this framework to the case of ZEISS, a global technology company, to illustrate how it can be used to structure and guide digital transformation initiatives. The authors provide specific examples of how ZEISS has addressed each of the action fields in its digital transformation efforts and highlight the importance of aligning these efforts with the organization's overall strategy and goals. The paper concludes by emphasizing the need for organizations to view digital transformation as an ongoing process rather than a one-time event, and to continually adapt and evolve their approach in response to changing business environments and technologies.

3. Proposed Solution

This section presents a comprehensive framework for the implementation of ML systems in the digital workplace. We propose a specific solution that combines auto-encoders (AE) for dimensional reduction and convolutions for classification. AEs are applied as an unsupervised learning algorithm to reduce the dimensionality of large data sets. By compressing the data into a smaller feature space, auto-encoders can improve the efficiency and accuracy of subsequent classification tasks.

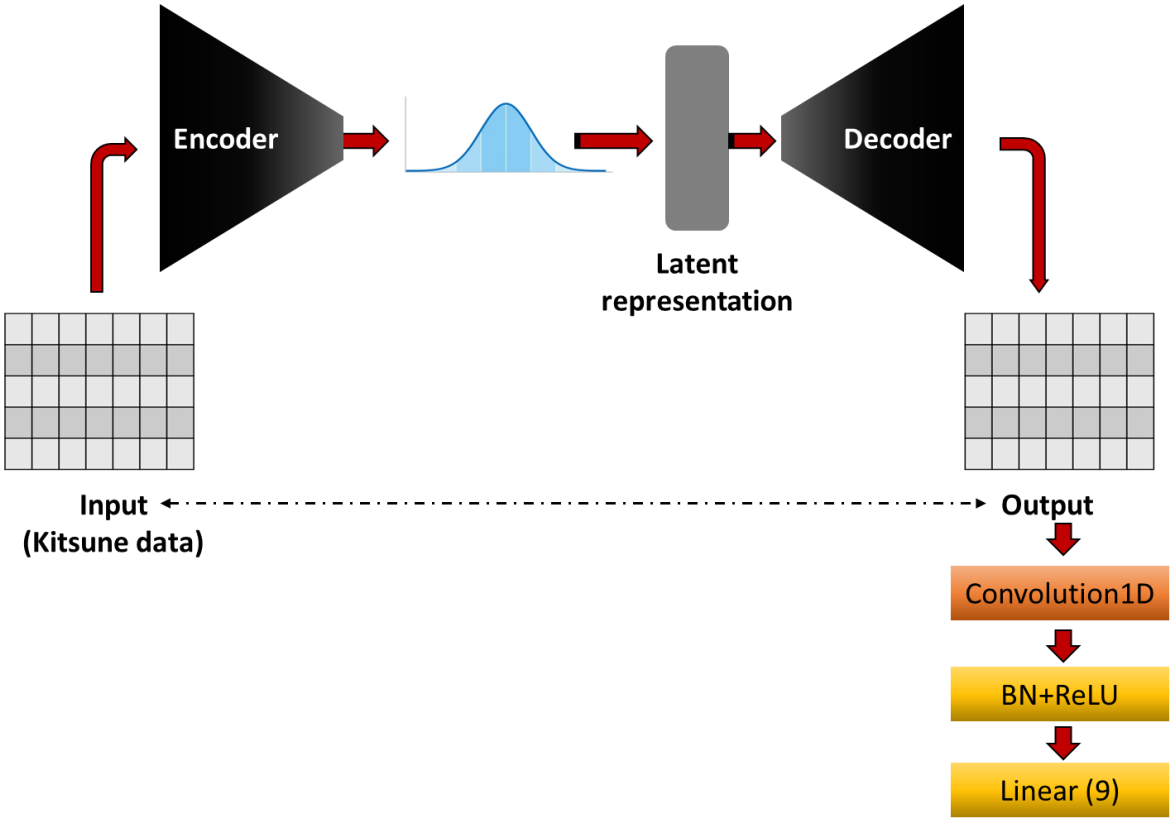

Figure 1: Illustration of the proposed ML model for detecting security attacks in digital world.

In the context of security data in the digital world, AEs can be used to reduce the dimensionality of large data sets and identify patterns that are relevant for security purposes. The motivation to use AEs for security data is their ability to

Doi : https://doi.org/10.54216/JCIM.110201
Received: November 18, 2022 Revised: January 02, 2023 Accepted: March 02, 2023

identify anomalies or outliers in the data. AEs trained on network traffic data can identify unusual patterns of communication that may indicate a cyber-attack. By reducing the dimensionality of large data sets, AEs can reduce the computational cost of subsequent tasks, such as classification or clustering. This can be especially important in real-time security applications where speed is critical. Given input $x = (x_1, x_2, \dots, x_n)$, AE first reduces this input to a latent representation composed of multiple hidden layers $a = (a_1, a_2, \dots, a_m)$. latent representations are then processed to generate $x = (x'_1, x'_2, \dots, x'_n)$. Let j be the counter parameter for the neurons in the current layer l, and i be the counter parameter for the neurons in the previous hidden layer l−1. The output of a neuron in the hidden layer can be represented by the following formula.

$$a_j^{(l)} = f\left(z_j^{(l)}\right) = sigmoid\left(\sum_{i=1}^{n} W_{ji}^{(l-1)}.a_i^{(l-1)} + b_j^{(l-1)}\right) \quad (1)$$

where W and b denote the learning parameters optimized thru backpropagation, by optimizing the objective function J given as below:

$$J(W, b; \hat{x}, x) = \frac{1}{k}\sum_{i=1}^{k}\left(\frac{1}{2}||\hat{x} - x|\,|^2\right) + \frac{1}{\lambda}\sum_{l=1}^{ls-1}\sum_{j=1}^{m}\sum_{i=1}^{n}\left(W_{ji}^{(l)}\right)^2 \quad (2)$$

The symbol λ denotes a parameter selected as a regularization factor for all parameters in a distinct layer. To enforce a sparsity restraint on the hidden units, one policy is to augment an extra factor to the objective function throughout training to punish the Jensen–Shannon divergence between a normal variable and a required sparsity average:

$$\widehat{\rho_j} = \frac{1}{k}\sum_{i=1}^{k}\left[a_j^{(i)}\left(x^{(i)}\right)\right] \quad (3)$$

It is important to note that the effectiveness of AE for security data depends on the quality and quantity of the data available. Auto-encoders are most effective when trained on large, diverse data sets that represent a wide range of potential security scenarios. The reduced features from AE are then passed to a set of convolutional layers to extract the sophisticated representations via many kernels, that are responsible for generating fine-grained feature maps. The convolutional procedure is formulated as follows:

$$Conv_{x,y} = A(\sum_{i}^{n.m} W_i \cdot s_i + bias), \quad (4)$$

with h being computed as follows:

$$A(x) = max(0, x) \quad (5)$$

The output of convolutional layers is then flattened and passed to linear layers, at which the final output is computed. By the end of this subnetwork, the cross-entropy function is used to measure the loss during the training iterations:

$$L = -\frac{1}{N}\sum_{i=1}^{N}\sum_{c=1}^{C} L_{y_i \in C_c} log P_{model}[y_i \in C_c], \quad (6)$$

where c and N denote the number of classes and samples, respectively.

4. Experimental Analysis

This section discusses the implementation setups and the experimental details of our study. Then, we delve into the discussion of the results of the conducted experiments. Determining the optimal set of metrics for evaluating performance is an important step in our experimental design. We choose the below metrics to evaluate the performance of ML methods.

$$\boldsymbol{Accuracy\ (A)} = \frac{\boldsymbol{TP + TN}}{\boldsymbol{TP + TN + FP + FN}} \times \mathbf{100} \quad (1)$$

$$\boldsymbol{Precision\ (P)} = \frac{\boldsymbol{TP}}{\boldsymbol{TP + FP}} \times \mathbf{100}, \quad (8)$$

$$\boldsymbol{Recall\ (R)} = \frac{\boldsymbol{TP}}{\boldsymbol{TP + FN}} \times \mathbf{100}, \quad (9)$$

Doi : https://doi.org/10.54216/JCIM.110201
Received: November 18, 2022 Revised: January 02, 2023 Accepted: March 02, 2023

$$\boldsymbol{F1-score\ (F1) = 2 * \frac{P * R}{P + R}}, \qquad (10)$$

More, the kitsune dataset [20] is used as a case study for security data for training and evaluation of ML approaches considered in this study. The data contains nine classes of network attacks, where the distribution of samples per each class is provided in Table I. Each sampel in the dataset is composed of a total of 115 features.

Table 1 Summary of features of the kitsune dataset

Figure 2: Illustration of the distribution of 115 features from kitsune dataset

Attack Type	Attack Name	Tool	Violation	Vector	#Packets	Time[min.]
Recon	OS Scan Fuzzing	Nmap Sfuzz	C C	1 3	1,697,851 2,244,139	52.2 85.5

Doi : https://doi.org/10.54216/JCIM.110201
Received: November 18, 2022 Revised: January 02, 2023 Accepted: March 02, 2023

Man in the Middle	Vicleo Injection ARP MitMm Ac.rive Wiretap	Video Jack Etterc.ap Raspberry PI 3B	C,I C C	1 1 2	2,472,401 2,504,267 4,554,925	33.4 28.2 95.6
Deniol of Service	SSDP Flood SYN DoS SSL Renegotiation	Saddam Hping3 THC	A A A	1 1 1	4,077,266 2,771,276 6,084,492	40.8 52.8 65.6
Botnet Malware	Mirai	Telnet	C,I	X	764,137	118.9

Table 1: correlation between th first twenty feature of from kitsune dataset

	X2	**X3**	**X4**	**X5**	**X6**	**X7**	**X8**	**X9**	**X10**	**X11**	**X12**	**X13**	**X14**	**X15**	**X16**	**X17**	**X18**	**X19**	**X20**
X2	1.00	0.43	-0.74	1.00	0.43	-0.72	1.00	0.43	-0.63	1.00	0.43	-0.55	1.00	0.43	-0.74	1.00	0.43	-0.74	1.00
X3	0.43	1.00	-0.71	0.43	1.00	-0.70	0.43	1.00	-0.61	0.43	1.00	-0.50	0.43	1.00	-0.72	0.43	1.00	-0.71	0.43
X4	-0.74	-0.71	1.00	-0.74	-0.72	0.99	-0.74	-0.72	0.88	-0.75	-0.72	0.78	-0.75	-0.72	1.00	-0.74	-0.72	1.00	-0.74
X5	1.00	0.43	-0.74	1.00	0.43	-0.72	1.00	0.43	-0.63	1.00	0.43	-0.55	1.00	0.43	-0.75	1.00	0.43	-0.74	1.00
X6	0.43	1.00	-0.72	0.43	1.00	-0.70	0.44	1.00	-0.61	0.44	1.00	-0.50	0.44	1.00	-0.72	0.43	1.00	-0.72	0.43
X7	-0.72	-0.70	0.99	-0.72	-0.70	1.00	-0.72	-0.70	0.92	-0.73	-0.70	0.84	-0.73	-0.70	0.98	-0.72	-0.70	0.99	-0.72
X8	1.00	0.43	-0.74	1.00	0.44	-0.72	1.00	0.44	-0.63	1.00	0.44	-0.55	1.00	0.44	-0.75	1.00	0.43	-0.74	1.00
X9	0.43	1.00	-0.72	0.43	1.00	-0.70	0.44	1.00	-0.61	0.44	1.00	-0.50	0.44	1.00	-0.72	0.43	1.00	-0.72	0.43
X10	-0.63	-0.61	0.88	-0.63	-0.61	0.92	-0.63	-0.61	1.00	-0.64	-0.61	0.98	-0.64	-0.61	0.86	-0.63	-0.61	0.88	-0.63
X11	1.00	0.43	-0.75	1.00	0.44	-0.73	1.00	0.44	-0.64	1.00	0.44	-0.56	1.00	0.44	-0.75	1.00	0.43	-0.75	1.00
X12	0.43	1.00	-0.72	0.43	1.00	-0.70	0.44	1.00	-0.61	0.44	1.00	-0.50	0.44	1.00	-0.72	0.43	1.00	-0.72	0.43
X13	-0.55	-0.50	0.78	-0.55	-0.50	0.84	-0.55	-0.50	0.98	-0.56	-0.50	1.00	-0.56	-0.50	0.77	-0.55	-0.50	0.78	-0.56

Doi : https://doi.org/10.54216/JCIM.110201
Received: November 18, 2022 Revised: January 02, 2023 Accepted: March 02, 2023

X14	1.00	0.43	-0.75	1.00	0.44	-0.73	1.00	0.44	-0.64	1.00	0.44	-0.56	1.00	0.44	-0.75	1.00	0.43	-0.75	1.00
X15	0.43	1.00	-0.72	0.43	1.00	-0.70	0.44	1.00	-0.61	0.44	1.00	-0.50	0.44	1.00	-0.72	0.43	1.00	-0.72	0.43
X16	-0.74	-0.72	1.00	-0.75	-0.72	0.98	-0.75	-0.72	0.86	-0.75	-0.72	0.77	-0.75	-0.72	1.00	-0.74	-0.72	1.00	-0.75
X17	1.00	0.43	-0.74	1.00	0.43	-0.72	1.00	0.43	-0.63	1.00	0.43	-0.55	1.00	0.43	-0.74	1.00	0.43	-0.74	1.00
X18	0.43	1.00	-0.72	0.43	1.00	-0.70	0.43	1.00	-0.61	0.43	1.00	-0.50	0.43	1.00	-0.72	0.43	1.00	-0.72	0.43
X19	-0.74	-0.71	1.00	-0.74	-0.72	0.99	-0.74	-0.72	0.88	-0.75	-0.72	0.78	-0.75	-0.72	1.00	-0.74	-0.72	1.00	-0.74
X20	1.00	0.43	-0.74	1.00	0.43	-0.72	1.00	0.43	-0.63	1.00	0.43	-0.56	1.00	0.43	-0.75	1.00	0.43	-0.74	1.00

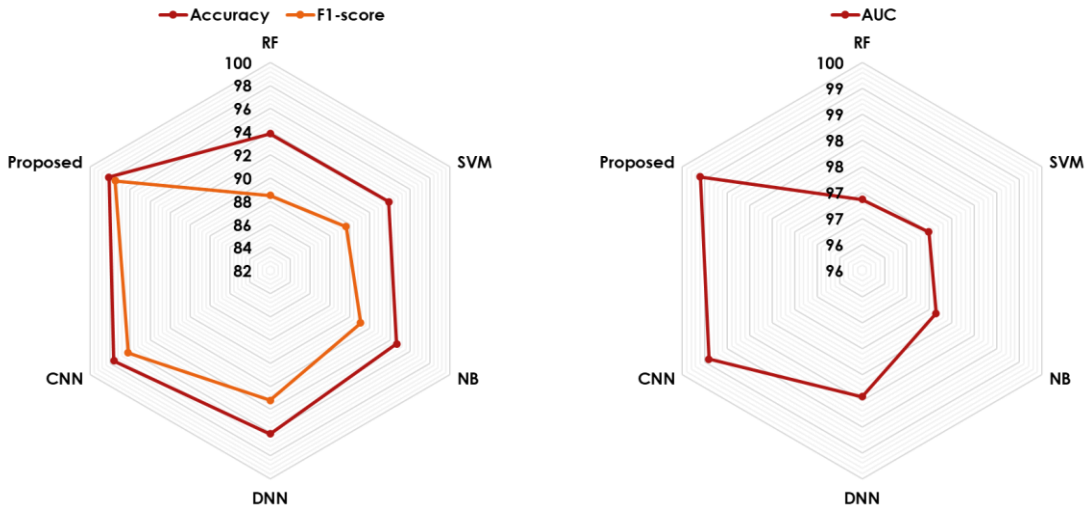

Figure 3: comparison between our model and cutting-edge ML method for threat detection.

At this part of the experiments, we includes empirical comparisons, in which the proposed system is compared against the state of the art under fair conditions. The results of those experiments are displayed in Figure 2. As sown, the results in the left part of the figure focus on accuracy and f1-score, while the right part focus on AUC metric. It is notable that the support vector machine and naïve biase are attaining the lowest possible detection performance (Accuracy: 92%-94%, F1-score: 88%-92%) among the other competing baselines. Comparatively, the standard three-layer DNN and three-layer CNN model is attaining better performance improvements (Accuracy:94%-95% , F1-score: 93%-95%). Remrkably, it could be noted that the proposed system can significantly surpass (Accuracy: 96%-98%) the previous methods across different metrics. These findings can be further validated by a significance test, in which paired t-test is used to measure the statistical difference between the prediction of different methods on confidence intervals of 95% (See Table 2). It could be note that the p-value for each experimental test is bellow the significance threshold excpect for comparison with CNN. This, in turn, reflect the competitive ability of our model in detecting the security threats.

Doi : https://doi.org/10.54216/JCIM.110201
Received: November 18, 2022 Revised: January 02, 2023 Accepted: March 02, 2023

Table 2. The results of paired t-test on our comparison experiments (p-value threshold: 0.05)

Proposed vs RF	Proposed vs SVM	Proposed vs NB	Proposed vs DNN	Proposed vs CNN
4.25E-07	9.20E-05	9.33E-03	3.96E-08	1.39E-01

5. Conclusion

This paper examines the potential of ML to balance security and information management in the digital workplace by proposing an intelligent ML for discovering cybersecurity threats, such as the ability to detect anomalies and predict potential threats. We have also discussed some of the challenges and limitations of ML, including the need for high-quality data, the risk of bias and ethical considerations, and the potential for over-reliance on technology. Our case study of a real-world implementation of ML in a digital workplace setting has shown that while our model can deliver significant benefits, its success depends on careful consideration of organizational context and stakeholder needs. It is essential to involve employees, IT professionals, and data privacy experts in the development and implementation of ML systems to ensure that they meet the needs of all stakeholders and comply with relevant regulations.

References

[1] Ilvonen, Ilona, Stefan Thalmann, Markus Manhart, and Christian Sillaber. "Reconciling digital transformation and knowledge protection: a research agenda." *Knowledge Management Research & Practice* 16, no. 2 (2018): 235-244.

[2] Peppard, Joe, and John Ward. *The strategic management of information systems: Building a digital strategy*. John Wiley & Sons, 2016.

[3] Casalino, Nunzio, Ireneusz Żuchowski, Nikos Labrinos, Ángel Luis Munoz Nieto, and Jose Antonio Martín. "Digital strategies and organizational performances of SMEs in the age of Coronavirus: balancing digital transformation with an effective business resilience." *Queen Mary School of Law Legal Studies Research* Paper Forthcoming (2019).

[4] Vial, Gregory. "Understanding digital transformation: A review and a research agenda." *The journal of strategic information systems* 28, no. 2 (2019): 118-144.

[5] `, Subodh, and Rajhans Mishra. "Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges." *Enterprise Information Systems* 15, no. 4 (2021): 565-584.

[6] M. Alhamad, T. Dillon, and E. Chang, "A trust-evaluation metric for cloud applications," *International Journal of Machine Learning and Computing*, vol. 1, no. 4, pp. 416–421, Oct. 2018

[7] Klein, Vinícius Barreto, and José Leomar Todesco. "COVID-19 crisis and SMEs responses: The role of digital transformation." *Knowledge and Process Management* 28, no. 2 (2021): 117-133.

[8] Kraus, Sascha, Francesco Schiavone, Anna Pluzhnikova, and Anna Chiara Invernizzi. "Digital transformation in healthcare: Analyzing the current state-of-research." *Journal of Business Research* 123 (2021): 557-567.

[9] Pittaway, Jeffrey J., and Ali Reza Montazemi. "Know-how to lead digital transformation: The case of local governments." *Government Information Quarterly 37*, no. 4 (2020): 101474.

[10] Piccinini, Everlin, Andre Hanelt, Robert Gregory, and Lutz Kolbe. "Transforming industrial business: the impact of digital transformation on automotive organizations." (2015).

[11] Berghaus, Sabine, and Andrea Back. "Disentangling the fuzzy front end of digital transformation: Activities and approaches." *Association for Information Systems*, 2017.

[12] Kaivo-Oja, Jari, Steffen Roth, and Leo Westerlund. "Futures of robotics. Human work in digital transformation." *International Journal of Technology Management* 73, no. 4 (2017): 176-205.

[13] Boneva, Miroslava. "Challenges related to the digital transformation of business companies." In *Innovation Management, Entrepreneurship and Sustainability (IMES 2018)*, pp. 101-114. Vysoká škola ekonomická v Praze, 2018.

[14] Berger, Roland. "The digital transformation of industry." *The study commissioned by the Federation of German Industries (BDI), Munich (www. rolandberger. com/publications/publication_pdf/roland_berger_ digital transformation of industry 20150315. pdf)* (2015).

[15] Nambisan, Satish, Mike Wright, and Maryann Feldman. "The digital transformation of innovation and entrepreneurship: Progress, challenges and key themes." *Research Policy* 48, no. 8 (2019): 103773.

Doi : https://doi.org/10.54216/JCIM.110201
Received: November 18, 2022 Revised: January 02, 2023 Accepted: March 02, 2023

[16] Dwivedi, Yogesh K., D. Laurie Hughes, Crispin Coombs, Ioanna Constantiou, Yanqing Duan, John S. Edwards, Babita Gupta et al. "Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life." *International journal of information management* 55 (2020): 102211.

[17] Setiawan, Awan, and Erwin Yulianto. "Information System Strategic Planning Using IT Balanced Scorecard In Ward & Peppard Framework Model." *International Journal of Engineering and Technology (IJET)* 9, no. 3 (2017): 1864-1872.

[18] Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: an ensemble of autoencoders for online network intrusion detection. arXiv preprint arXiv:1802.09089.

[19] Sabherwal, R., R. Hirschheim, and T. Goles. "Information Systems—Business Strategy Alignment The dynamics of alignment: insights from a punctuated equilibrium model." *Strategic information management* 311 (11).

[20] He, Qile, Maureen Meadows, Duncan Angwin, Emanuel Gomes, and John Child. "Strategic alliance research in the era of digital transformation: Perspectives on future research." *British Journal of Management* 31, no. 3 (2020): 589-617.

[21] Borangiu, Theodor, Damien Trentesaux, André Thomas, Paulo Leitão, and Jose Barata. "Digital transformation of manufacturing through cloud services and resource virtualization." *Computers in Industry* 108 (2019): 150-162.

[22] Tallon, Paul P., Ronald V. Ramirez, and James E. Short. "The information artifact in IT governance: Toward a theory of information governance." *Journal of Management Information Systems* 30, no. 3 (2013): 141-178.

[23] Rowe, Frantz. "Being critical is good, but better with philosophy! From digital transformation and values to the future of IS research." *European Journal of Information Systems* 27, no. 3 (2018): 380-393.

Doi : https://doi.org/10.54216/JCIM.110201
Received: November 18, 2022 Revised: January 02, 2023 Accepted: March 02, 2023