sciendo

Addressing Cybersecurity Issues in ERP Systems – Emerging Trends

Liana-Elena ANICA-POPA
Bucharest University of Economic Studies, Bucharest, Romania
liana.anica@cig.ase.ro

Marinela VRÎNCIANU
Bucharest University of Economic Studies, Bucharest, Romania
marinela.vrincianu@cig.ase.ro

Irina-Bogdana PUGNA
Bucharest University of Economic Studies, Bucharest, Romania
irina.pugna@cig.ase.ro

Dana-Maria BOLDEANU
Bucharest University of Economic Studies, Bucharest, Romania
**Corresponding author, boldeanud@cig.ase.ro*

Abstract. *The integration of emerging technologies in Enterprise Resource Planning systems has the potential to enhance security, automation, decision-making, and predictive capabilities. However, this also introduces new cybersecurity challenges, as the systems may become targets for malicious attacks or data breaches. Understanding the nexus between organizational systems, artificial intelligence (AI), and cyber-security requirements, offers new insights for the modern business environment. Our study begins with an exploration of recent cases of AI-enhanced cybersecurity tools implemented within organizational information systems, as these currently stand. This research landscape is our starting point for an analysis of the impact of these tools on different types of systems, of the cyber risks reported in recent literature, and the configuration of cyber-security solutions tailored after current vulnerabilities of the business environment. We also identify trends and gaps in the existing research that suggest possible new topics for further investigation.*

Keywords: Cybersecurity, ERP Systems, Artificial Intelligence, Information Systems, Intelligence Augmentation

Introduction

Over the past few decades, ERP systems have evolved with the emergence of new technologies, incorporating advanced features, and significantly influencing global business operations. The integration of emerging technologies into future ERP systems presages disruptive elements such as artificial intelligence, the Internet of Things (IoT), big data, blockchain technology, and omnichannel strategy. Key determinants of success in ERP implementation include management support, adept project team, resilient IT infrastructure, effective communication, skilled workforce, thorough training and education, and rigorous monitoring and evaluation (Costa, et al., 2020; Vargas et al., 2020; Al-Amin et al., 2023). Additionally, cybersecurity emerges as perhaps the foremost challenge for future iterations of ERP.

The necessity of revolutionizing cybersecurity for ERP systems through the integration of AI technologies is evident, driven by the swift advancement of digital, mobile, and cloud

DOI: 10.2478/picbe-2024-0108

technologies, as well as the proliferation of IoT and remote tools. These developments have fundamentally altered the way both businesses and consumers engage with technology, resulting in a significant expansion of the digital attack surface. Cybersecurity Ventures Report (eSentire,2023) forecasts that the global annual cost of cybercrime will soar to $10.5 trillion by 2025. Moreover, SAP (2024) reports that in 2021, the number of IoT devices worldwide surpassed 10 billion, with projections indicating an exponential growth trajectory, surpassing 30 billion by 2025. With so many devices becoming integrated into businesses' IoT networks, contributing data to a centralized ERP system, the vulnerability to security threats is substantial. Onapsis (2024) reports that over 17,000 SAP and Oracle ERP applications on the internet have been identified as exposed; many of these are operated by some of the world's largest governmental and commercial organizations.

This study examines the most recent insights regarding the integration of Artificial Intelligence technologies into cybersecurity solutions integrated into ERP or other organizational systems. More specifically, we aim to answer the following research questions:

RQ1: *What is the current research landscape of AI-enhanced cybersecurity tools integrated in organizational systems?*

RQ2: *What are the main types of systems and technologies revealed by the recent studies related to AI-empowered cybersecurity features?*

RQ3: *How are cybersecurity risks currently addressed with the help of AI-enhanced cybersecurity solutions within organizational information systems?*

RQ4: *What are the emerging research trends and gaps related to AI-enhanced cybersecurity of organizational systems?*

In this paper, we examine the nexus between various organizational information systems and the realms of cybersecurity and artificial intelligence through a Structured Literature Review (SLR). Through this, we provide a comprehensive examination of research focused on integrating artificial intelligence-enhanced cybersecurity tools into organizational management systems. The basis of our investigation into this relationship is a review of publications indexed in the *Web of Science* database.

The remainder of this article is organized as follows. The next section outlines our research methodology. Section III includes an overview of Artificial Intelligence-based cybersecurity solutions integrated with organizational information systems such as ERPs, as reported in recent literature, and then we move on to the results and analysis of our findings. The paper ends with our conclusions, reflections, limits and directions for further investigation.

Methodology

The purpose of this paper, then, is to identify the main areas of interest and emerging trends outlined in scientific research on the issue of AI-enhanced cybersecurity of organizational information systems.

To answer our specific research questions, we conducted an SLR. According to Becheikh *et al.* (2006), the main purpose of this method is "*to identify key scientific contributions in a field ... its results are often descriptively presented and discussed*".

As a first phase, we reviewed approaches to AI-improved cyber-security solutions adopted within ERP systems as they have been addressed in the recent literature. The research methodology involved, in the second phase, the use of keyword-co-occurrence network mapping techniques. This paper is a preliminary study for broader research dedicated to organizational systems and cyber-

security concepts, based on AI technologies. The need for a preliminary study is motivated by the limited literature covering the collision of these topics of cyber-security, AI, and ERP Systems.

We used data visualization techniques and cluster analysis to investigate the main research directions, using Web of Science (WoS) resources. The keywords used to search for articles within WoS were: “ERP System*", "Information System*", "IT System*", “cyber*security*”, “Artificial Intelligence”, selecting papers published between 2016-2024. The query expression is the following: *(("ERP System*") or ("Information System*") or ("IT System*")) AND (“cyber*security*”) AND (“Artificial Intelligence”) (Topic) and 2024 or 2023 or 2022 or 2021 or 2020 or 2019 or 2018 or 2017 or 2016 (Publication Years)*.

This resulted in 38 articles, used to generate VOSviewer maps meant to emphasize the papers’ keywords. The WoS reporting tools were also leveraged to obtain the identified research areas, WoS papers’ categories and new topics, such as sustainability goals, found in the recent literature, generated the conceptual triad Organizational Systems - Cybersecurity - Artificial Intelligence.

We observed correlations between the keywords that refer to different types of organizational information systems with those across the "cybersecurity" and "artificial intelligence" spectrums, and examined the extent to which cyber-security tools integrating AI are implemented in organizations' activity management systems. We also identified possible research gaps and new topics brought to researchers ‘attention related to the key concepts of the investigation.

Literature review

In recent years, the integration of Artificial Intelligence (AI) with cybersecurity tools has emerged as a critical approach to bolstering organizational security against evolving threats. Jada and Mayayise (2023) note the positive way that AI is contributing to cyber-security at the organizational level, through automation, analysis, predicting threats, managing vulnerabilities, improving hardware and infrastructure security, and other aspects of the decision-making process.

The integration of ERP systems with AI technologies represents a significant advance in enhancing organizational efficiency and decision-making capabilities. Implementing robust cybersecurity protocols has been identified as crucial for the successful integration of AI technologies at the level of the organizational system (Aldoseri et al., 2024).

According to the business literature (Morisson, 2024) there is a growing trend towards integrating AI technologies into ERP systems to leverage the vast amounts of data that is generated by these systems, and to extract actionable insights for strategic decision-making (Bawa, 2023). Yathiraju (2022) concludes that overcoming the challenges of integrating AI into cloud-based ERP systems lead to clear benefits for improving work efficiency and increasing cyber-security.

A common point of analysis can be identified in the articles of Dawson et al. (2019), Pawlicki et al. (2018, 2021) and Poulsen et al. (2020) which both shed light on the intersection of cybersecurity with emerging technologies, such as the Industrial Internet of Things (IIoT), virtual labs, granular computing, value sensing robots, and handling missing data in cybersecurity applications. They emphasize the growing importance of developing frameworks and implementations to address cybersecurity challenges in these innovative domains.

Organizations are recognizing the potential for improved decision-making, operational efficiency (Alrfai et al., 2023), predictive analytics (Gatti et al., 2023), and cost savings, by leveraging AI within their ERP environments (Maia et al., 2023). This integration not only enhances business processes but also provides a competitive edge in several industries (Michailidi et al., 2021).

In conclusion, while there is considerable research covering AI-driven cybersecurity for organizational systems in general, the potential of AI in safeguarding ERP systems is much less fully explored. The existing literature, that addresses organizational systems in general, raises new difficulties: how to keep pace with rapidly changing technologies (in terms of both opportunities and security risks), how to create adaptable and autonomous systems capable of quickly identifying and responding to emerging cyber threats in real-time (Lohn, et al.,2023; Kholidi, 2021;Zhao, et al.,2020), how to develop AI-enhanced cybersecurity solutions capable of detecting and mitigating threats across multiple domains and interconnected networks (Zeadalli, et al.,2020; Maurya, 2023), how to gain insights to comprehend the rationale behind AI-based security decisions (Hamon, et al.,2022), and how to address the legal and ethical implications of AI in cybersecurity while ensuring regulatory compliance (Lee, 2021;Formosa, et al.,2021). Ramanpreet et al., (2023) highlights prospects for future research in emerging cybersecurity domains, cutting-edge AI techniques, data structuring, and the establishment of novel frameworks to effectively integrate AI-driven cybersecurity amidst the contemporary landscape of digital evolution and multifaceted crises.

Addressing these research trends and gaps will be vital for enhancing the effectiveness and reliability of AI-enhanced cybersecurity in organizational systems.

Results and discussions

1. The general research landscape

From the information extracted from the WoS, we initially obtained a general image of keywords utilized by researchers in their papers (Figure 1.). In this network visualization, the size of the label and the frame of an item is determined by its weight (the higher the weight of an item, the larger its label and frame). Figure 1. indicates that "cybersecurity" and "artificial Intelligence" appear with the largest frames, and the line between them is also stronger, indicating a high number of publications in which the two terms occur together. Starting from this concept map, we conducted a deeper investigation, searching for other major topics and more details about their research goals.

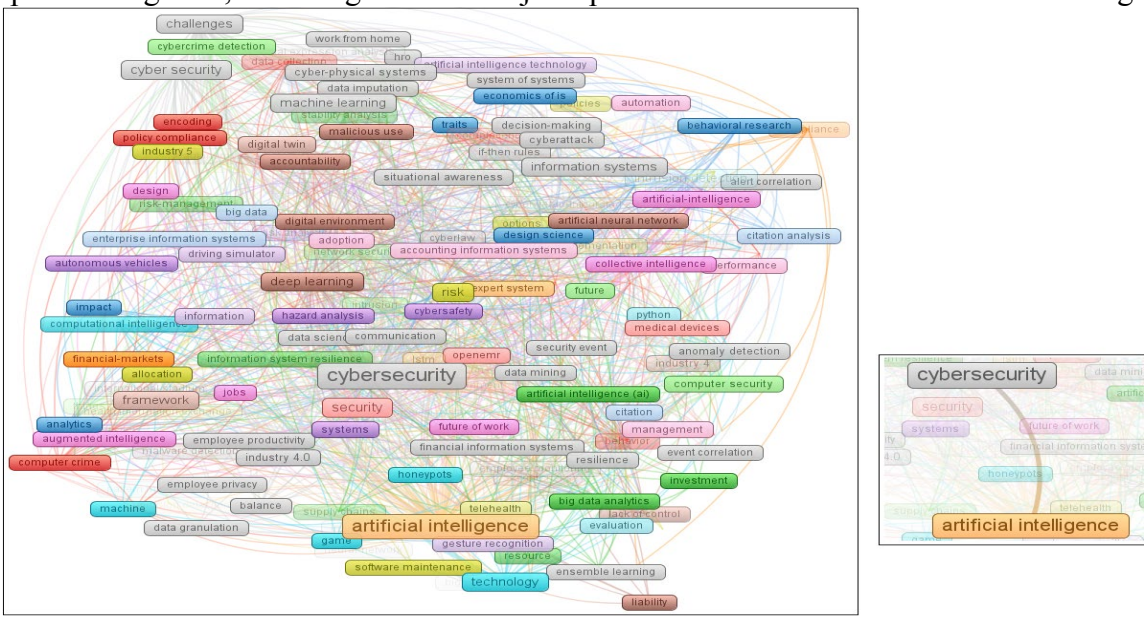

Figure 1. The keywords map (*VOSviewer*)

Source: Authors' research using VOSviewer.

The keyword map supports the ideas identified in specialized literature. Information Systems design and capabilities, Cybersecurity and Artificial Intelligence are considered among required technologies in the process of organizations 'digital transformation, along with Internet of Things, Virtual Reality, Machine Learning, Big Data (Michailidi, et al., 2021).

Conducting a keywords density analysis, we observe in figure below (Figure 2), some clusters of system types addressed in the papers: "accounting information systems", "financial information systems", "health information systems", the general concept of "information systems", and more technical constructions such as "cyber physical systems".

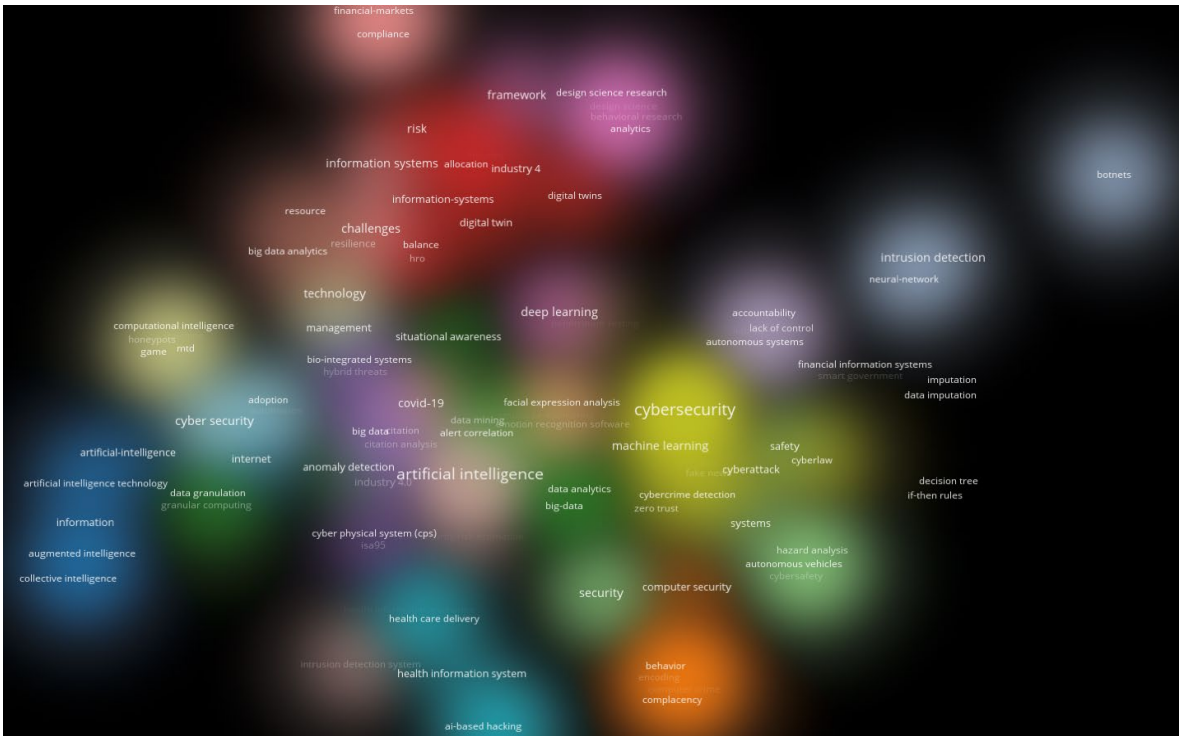

Figure 2. The clusters density analysis

Source: Authors' research using VOSviewer.

There are five core themes of cybersecurity research (Singh et al., 2022): (a) artificial intelligence in cybersecurity, (b) platform security, grids, and networks (c) algorithms and methods, (d) optimization and modelling, and (e) cybersecurity management. In the analysis of AI-based security systems, special attention is paid to the security areas towards which IT applications are oriented and to the events that trigger security risks. Most of the applications currently on the market are in the areas of malware identification and classification, intrusion detection and cybercrime prevention (Sen et al., 2022). The research is also oriented towards the establishment of conceptual and methodological frameworks. For instance, Gupta et al. (2021) advances a framework depicting the relationships among AI, information systems, and supply chain disruption. They detached from the information systems the supply chain component and emphasized the role of its infrastructure and AI-based tools for data acquisition, processing, and self-training capabilities in decreasing the impact of supply chain disruption while ensuring cybersecurity of the geographically suitable supply chains. Systematization is being tried at the level of security event correlation models in terms of their representation in AI-based monitoring

systems, introducing the following categories: rule-based, semantic, graphical and machine learning based-models (Levshun and Kotenko, 2023).

2. Co-occurrence links analysis - Types of Systems and Technologies, Cybersecurity and Artificial Intelligence (RQ2)

The keyword "systems of systems", visible in the upper part of Figure 1 (with the grey label) inspired us to conduct an in-depth analysis of advances in AI-based cybersecurity reported in relation with different types of systems spotted in the keyword maps.

As a general note, "Information Systems" is a frequently encountered keyword in the generated views. It covers large and diverse categories of management and operational systems, including ERP; however, the latter type of system was not explicitly mentioned as a keyword in papers resulting from our search.

This very concept - "systems of systems" - suggests an unprecedented level of complexity generated by the increasing degree of interconnectivity between systems, people, devices, and networks, from decision-making to business and individual operational levels. Tagarev, et al. (2019) explore the cybersecurity theme throughout five structured areas: communications, information systems and networks; cyber-physical systems; bio-integrated systems; cognitive processes; and drones (remotely controlled or autonomous) – and in so doing, analyzing AI reinforcements, vulnerabilities to cyber threats, and proposing a cybersecurity-centered multi- and interdisciplinary future research directions.

At the *industrial companies* (Figure 3, left side) level, another type of system investigated was the *Manufacturing Executive System* (Alem, et al., 2019). The authors consider cybersecurity an "urgent" objective for the industrial information systems and therefore focus their efforts on adapting an Intrusion Detection System to monitor industrial systems against illegitimate access and detect abnormal activities, proposing a hybrid intrusion detection solution based on the International Society of Automation 95 standard and neural networks. In terms of "information systems security", "data collection" in a system modelling framework (Figure 3), Pawlicki, et al. (2021) discuss the approaches to be used in ensuring cybersecurity for intelligent information systems. They also emphasize the critical role that data quality plays on the integration of artificial intelligence features and how missing data could affect systems' models and their effectiveness in real-world processes.

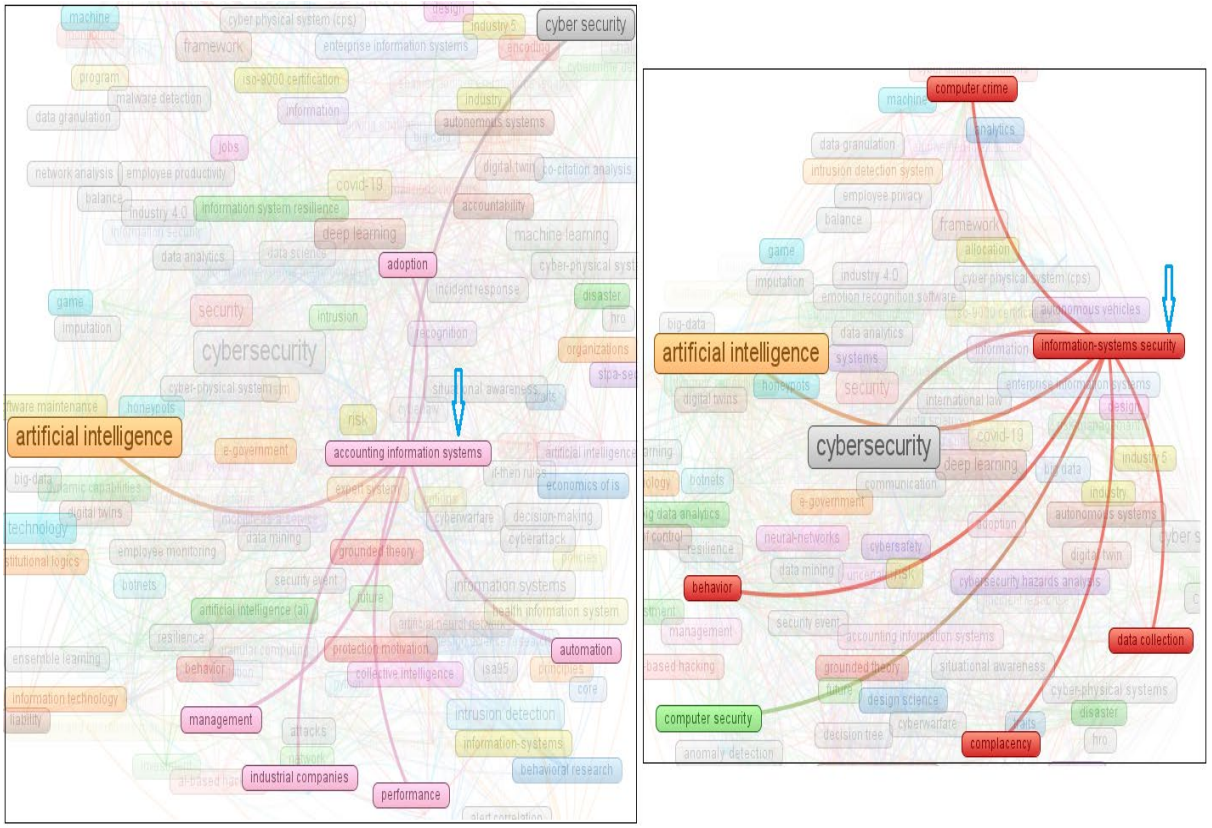

Figure 3. The nexus between system types, Cybersecurity and Artificial Intelligence
Source: Authors' research using VOSviewer.

To better adapt the design of cybersecurity tools to human behaviors, computer user security complacency ("complacency" - a red keyword in Figure 3) was investigated by Stafford (2022). Three constructs were advanced: 1) inherent complacency, due to user negligence regarding cyber-attacks; 2) platform complacency, induced by protective workplace technology implementations; and 3) social complacency, fueled by the comfort provided by guidance received from trusted individuals within personal and workplace networks. But when some hospitals faced cybersecurity incidents during the pandemic, 57.00% of hospital managers, hospital workers, and healthcare providers in China surveyed in a study ranked cybersecurity as the top challenge for health information systems (Ye, 2021).

Related to automotive-specific information systems design, scholars have investigated the application of a variety of methods to map safety and security hazards and mitigation requirements and actions in the urban mobility services area (Lee and Madnick, 2021). Two approaches - the *Cybersafety method*, based on System Theoretic Process Analysis (STPA and STPA-Sec) and *Combined Harm Analysis of Safety and Security for Information Systems* (CHASSIS) have been applied to over-the-air software updates feature in Mobility-as-a-Service (MaaS) and Internet of Vehicles (IoV) use cases. The analysis of the results also highlights a concern for the development of methodological frameworks in the area of information systems design (Figure 4). For instance, Cui et al. (2023) proposes a skeleton-based framework for designing future gesture-based in-air interfaces for In-Vehicle Information System (IVIS), contributing to the improvement of cybersecurity.

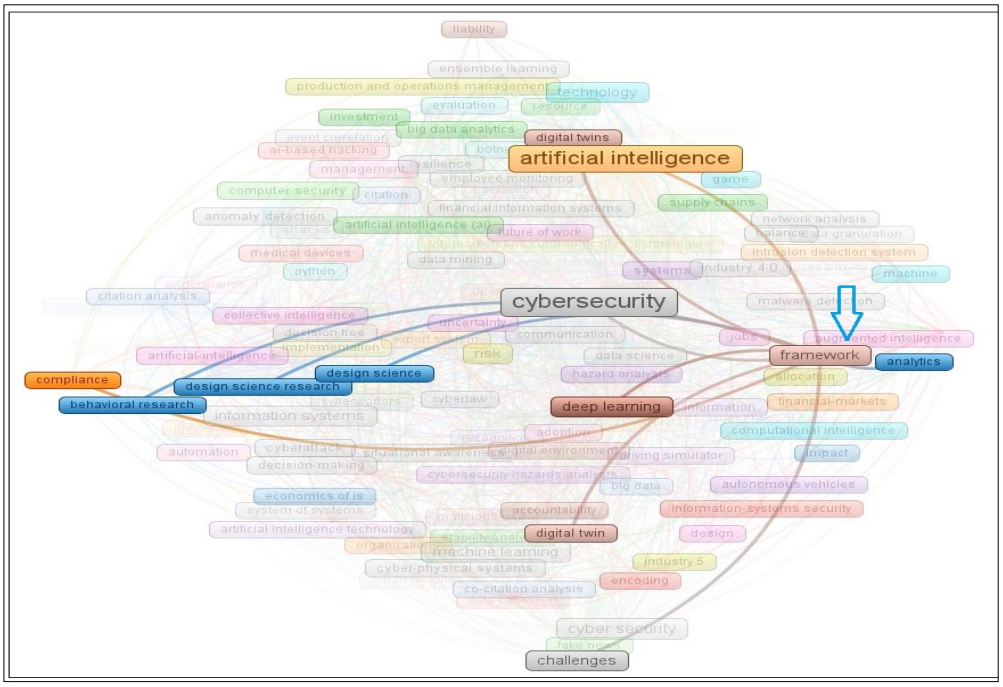

Figure 4. A view of keywords from the system design research area

Source: Authors' research using VOSviewer.

The accuracy and performance levels, recorded in intrusion detection systems by applying, as resulted in Figure 5, *deep learning algorithms* (such as multi-layer perceptron and long-short-term-memory) are better than those obtained by developments based on traditional non-DNN neural network algorithms - random forest and decision tree (Larriva-Novo, et al., 2021). By using International Society of Automation 95 standard and *artificial neural network* (Figure 5, right side), Alem, et al. (2019) modify and complete an Industrial Intrusion Detection System to cope with cyberattacks within the Open Interconnection layers of information and operational technologies.

New and emerging technologies such as AI, the IIoT, and 5G have also been explored by cybersecurity researchers within information systems generated in a virtual lab (Dawson, et al., 2019). Pawlicki, et al. (2019) introduces Granular Computing (GrC) technology, applied to enhance intrusion detection, to reduce computing costs and to better the network traffic classification in real-life traffic analysis.

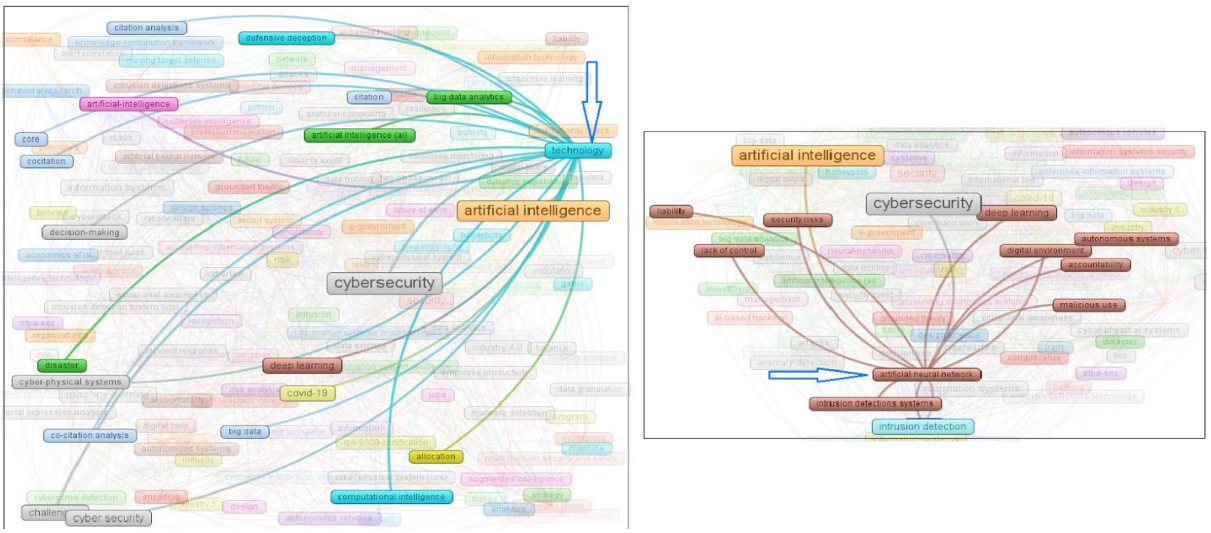

Figure 5. Mapping the technology-related keywords

Source: Authors' research using VOSviewer.

Machine learning models are also used for the early detection of behavioral anomalies and cyberattacks and to mitigate the risk exposures of information systems designed for managing large sports events such as the Olympic Games or the FIFA World Cup (Wan, et al., 2022). The researchers propose an AI-based cyber-physical system (AI-CPS) aiming at ensuring business and critical-data confidentiality, a robust warning and security breach alert mechanism, and delivering common countermeasures to attenuate the consequences. It was demonstrated that AI-CPS can improve network cybersecurity and enhance live data streaming, reducing costs and enhancing accuracy, prediction, and efficiency compared with existing methods. Much research is focused on the use of Deep Learning models and algorithms, to ensure cybersecurity of information systems. Samtani et al. (2023) contribute to Deep Learning for cybersecurity, specifically for identifying emerging threats from Dark Web for Cyber Threat Intelligence (CTI). Mohan et al. (2022) undertook a survey focusing on Defensive Deception tactics deployed using Deep Learning and Machine Learning algorithms. Defensive Deception tactics include thinking like an attacker and determining the best strategy to counter most common attack strategies. The research undertaken by Tran et al. (2022) in Vietnam, points out that there are a few emerging technologies with the potential to improve medical services in that country. The authors consider that AI-based decision-support systems could be integrated with digital health systems in hospitals to provide superior care at low cost. As in the previously mentioned cases, implementing these AI-based technologies requires an understanding of local government requirements and regulations, such as technology specifications, cybersecurity, data sharing protocols, and interoperability. Mogollón-Gutiérrez et al. (2023) presents a new perspective, using AI to ensure cybersecurity by studying network traffic. For this purpose, an overall model for the classification of cyber-attacks was built.

3. Risks and Cybersecurity solutions view (RQ3)

As a consequence of advances in information and communication technologies, organizations are now facing new challenges in the form of cybersecurity risks that are partly caused by these technologies.

According to Kumar and Mallipeddi (2022), unprecedented technological evolution has led to the adoption of Industry 5.0, generating the so-called "smartification" of modern enterprises. An

AI-enhanced cybersecurity solution leverages high-learning capabilities, detecting more effective malicious attacks, thereby responding to the urgency of safety and privacy concerns (Wan, et al., 2022). AI is also integrated in tools for generating autonomous penetration tests for extensive and decentralized information systems, to create an appropriate communication channel and a supportive feature for risk assessment reporting (François, et al., 2021).

The relation Risk-Artificial Intelligence was presented bidirectionally by Tagarev, et al., (2019). They discuss threats such as mixtures of natural language processing, ontologies and machine learning techniques harnessed to generate more legitimate-looking and deceptive malicious messages with reduced effort, time, and resources. AI techniques, like Machine Learning and Deep Learning, have been used in cyberattacks, emphasizing the need for AI-reinforced methods to counter and flag constant threats. Moreover, Aurucci (2018) warns that AI increasingly used in cyber defense may generate new *risks*, pointing out to these emerging security risks may hinder a wider harnessing of AI in cyber space, and the need to define an appropriate legislative framework to prevent and mitigate these harmful effects, whether intended or not, of AI-based technologies.

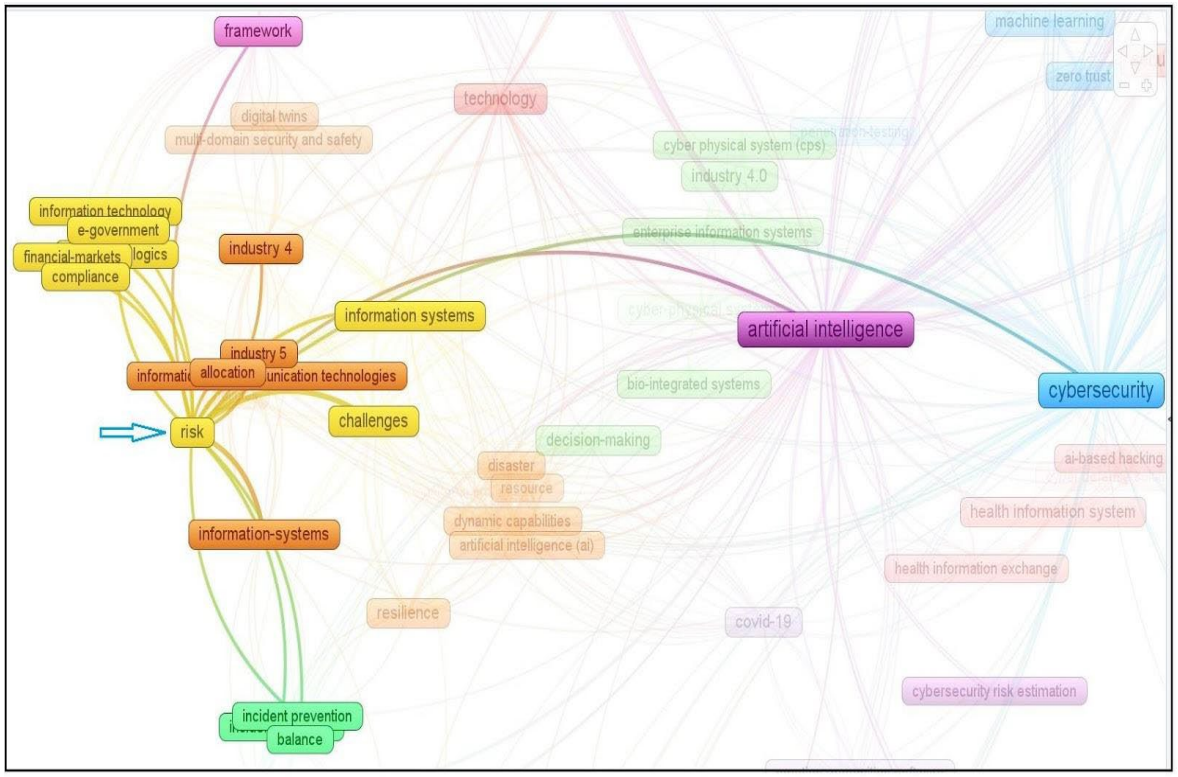

Figure 6. "Risk" co-occurrences keyword network

Source: Authors' research using VOSviewer.

As responses to "challenges" and "compliance" issues (Figure 6), during the pandemic, AI and emotion recognition tools have been used to record and control employees' activity within the information system of a simulated company in the financial services field. This was motivated by the need for monitoring remote work of users - employees and employers - and ensuring a proper cybersecurity work climate. The results were used as a teaching case, providing staff and students with useful insights regarding monitoring (Sipior, 2021).

Jain, et al. (2021) discuss the *Intelligence Augmentation (IA)* of information systems resulting from a design approach that mixes human and Artificial Intelligence, identifying as the main "rapidly emerging research areas", cybersecurity, privacy, counterterrorism, and healthcare information systems ("health information systems" or "his", "open-source electronic medical record", or "openemr" (Figure 7). According to Sarcevic et al. (2022) transparency is a major limit for implementations of black-box intelligent systems in high-risk areas such as cybersecurity, considering the growing complexity of machine learning models. We also noted the recent development of security risk assessment tools in the field of AI-based cybersecurity. For example, Gatti et al. (2023) proposes an expert system for the automatic assessment of cyber risks. This computes a risk score using available information and vulnerability assessment tools, public databases, leaks from the Dark Web, and AI-driven techniques to determine risks even. In the assessment of security risks, it is necessary to have a deep knowledge of the attack strategies and tools used by potential adversaries. He et al. (2023) proposes a new optimized ethical hacking method, based on AI and specially adapted for health information systems. Their purpose is to enable researchers and practitioners to identify the points and methods of action more effectively in potential cyberattacks.

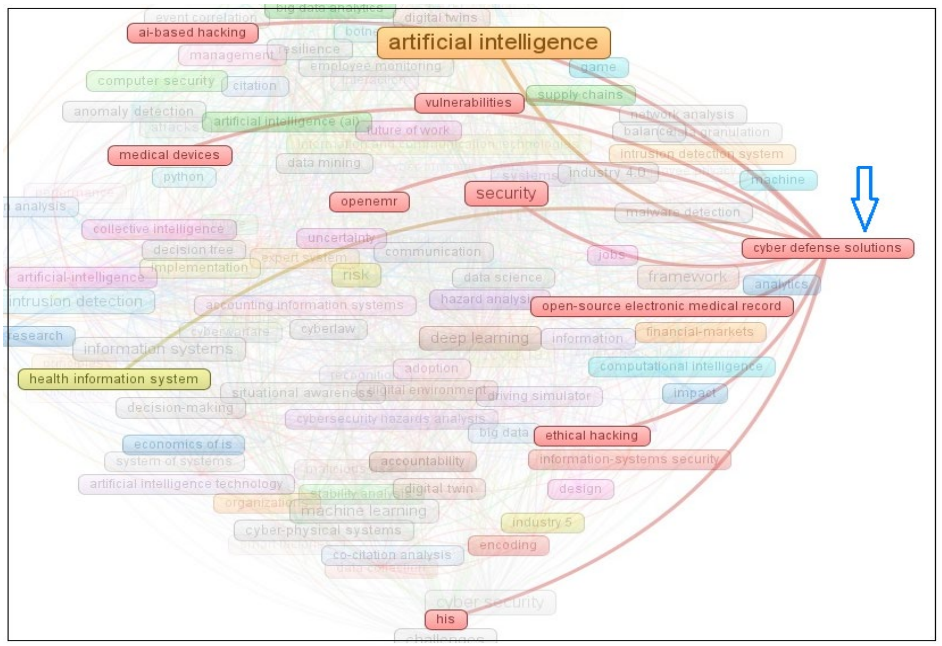

Figure 7. Observing cybersecurity-inspired research approaches

Source: Authors' research using VOSviewer.

Covering the Cybersecurity, AI, intrusion detection, and prevention systems areas, the study of Indre and Lemnaru (2016) provides a solution able to detect network intrusions and botnet communications with a precision of 98.4%, helping to understand, detect and prevent malicious connections using applied concepts of machine learning.

One of the concerns regarding security risks identified relates to the architecture of security systems. Hosney et al. (2022) analyse Zero Trust Architecture (ZTA) for designing and implementing secure IT systems. With ZTA each access from or to any asset must be assessed, following organization standard guidelines that impose a high burden on IT security and system

administrators to track and validate each control. Using Classification Algorithms in Machine Learning, the authors explore an alternative solution that helps maintain the same level of security with less human intervention. Butler et al. (2023) considers that IT artifacts pose risks and can harm individuals, different groups and organizations, but also society in general. The authors consider this issue a largely unexplored topic in Information Systems research. Regulators and opinion leaders have expressed concern about such risks, particularly those related to artificial intelligence, cybersecurity, privacy, and the market dominance of digital platforms. Addressing cybersecurity and user safety aspects, Poulsen, et al. (2020) investigates the implications for cybersecurity in codes of conduct concerning both healthcare professionals and designers of health information systems. They examine the case of social robots used for assisting LGBTIQ+ aged people, analysing how such cyber-physical health information systems can learn from experience and then act autonomously. Knowing that LGBTIQ+ elders prioritize values of acceptance, confidentiality, privacy, and personhood, the system cybersecurity, and the user safety are seen to be pivotal factors in elaborating new codes of conduct for both care robots and caregivers in such a delicate domain of AI-empowered products.

Recent studies also examine the current international legal frameworks that concern the balancing of a state-sponsored cyber-attacks as either an act of war or as a simple crime (Mottaleb and Canan, 2021). They point out the need for scientific research combining knowledge and good practices from the convergence zone of the fields of information systems, artificial intelligence, and comparative law, to analyse, understand and mitigate cyberattacks on states' political or business infrastructures that violate national and international laws' sovereignty and self-determination principles.

4. Trends and gaps identified in the current literature (RQ4)

One of the main trends noticed in the specialized literature is the use of Machine Learning algorithms and Deep Learning models, AI (allowing the development of automated security systems capable of tasks such as natural language processing, biometric/behavioral authentication), and threat detection. Unfortunately, the same technology is used by threat actors to design sophisticated attacks aimed at evading security protocols.

Also, as organizations rely on cloud services, ensuring robust security measures becomes essential for storing data and safely performing various operations. There is a diversification of targets in cyberattacks, not only governments and large corporations showing interest for attackers, but also educational, health organizations, and smaller businesses. The expansion of various IoT devices has created new attack opportunities, being susceptible to exploitation by malicious actors to initiate widespread distributed denial-of-service (DDoS) attacks. The proliferation of 5G networks offers unprecedented connectivity, especially with the Internet of Things (IoT), exposing these devices to vulnerabilities induced by external or internal threats. Ransomware attacks are a significant threat that tends to become a trend, especially for industries that rely on specific software systems. Recent incidents, such as attacks on healthcare facilities, make this topic of particular importance in research related to cybersecurity measures. Another trend is related to the development of research dedicated to the 5G architecture to identify and address potential security gaps. Adoption of Zero Trust Architecture (ZTA) and Zero Trust Security Models will expand, as organizations become aware of the limitations of traditional security models. Developments of AI-based cyber-physical systems (AI-CPS) become more and more of interest to scholars, due to their capability of ensuring data confidentiality, improving network cybersecurity, and enhancing live

data streaming, to reduce costs and optimize accuracy, prediction, and efficiency compared to other existing methods (Wan, et al., 2022).

Among the in-trend system types identified in our triadic field of research, AIS (Alrfai et al., 2023), financial administration IT systems (Ospina Diaz et al., 2023), Manufacturing Executive Systems (Alem, et al., 2019), In-Vehicle Information Systems (Cui et al., 2023), and especially starting with the pandemic, Health Information Systems (He et al., 2023; Ye, 2021) can be noted. Recent studies discuss systems *Intelligence Augmentation* (Jain, et al., 2021) supported by AI-powered features aimed at ensuring cybersecurity, privacy, and counterterrorism. In the "smartification" era (Kumar and Mallipeddi, 2022), AI has been used to more effectively identify and assess the cyber risks and cybervulnerability (Gatti et al., 2023), the methods of action in potential cyberattacks (He et al., 2023), but also in cybersecurity-centered organizational learning processes (Sipior, 2021).

The concept of "system of systems" emphasizes the idea of increasing interconnectivity and complexity of organizational systems, networks, devices and people, a context in which AI-based monitoring systems are considered crucial to prevent cyber-crime and ensure cyber-security (Sen et al., 2022; Levshun and Kotenko, 2023).

There are efforts focused also on finding more appropriate methodologies, like *Cyber-safety* (STPA and STPA-Sec) or *CHASSIS* frameworks, to be used for developing a more complete information lifecycle analysis and delivering consistent considerations for cyber-safety, effective risk mitigation measures and cyber-security tool development (Lee and Madnick, 2021).

However, scholars have addressed the entire information systems of an organization rather than simply limiting their research to ERP systems. Some business reports (Forbes, 2023) cover the adoption of AI-based cyber-security tools within ERP systems, in contrast, the specialized literature, as revealed by the search process in the WoS database, there are fewer articles focused on this triadic topic. Therefore, *a literature gap* becomes evident concerning this category of systems - ERP - in relation with AI-empowered cybersecurity tools.

Conclusion

Generally, an information system combines hardware and software components, empowering the organization's personnel to work with and to share information for functional purposes. Designing information system cybersecurity tools requires intelligence, understanding, and instruction, to offer protection in terms of confidentiality, authentication, non-repudiation, and reputation control, and to successfully manage information within a wide range of computer and router networks and devices (Wan, et al., 2022). In this context, we considered the convergence of ERP systems and AI, a critical topic for organizations interested in ensuring robust cybersecurity measures put in place to protect sensitive ERP data and AI-driven processes.

We addressed all our four research questions in the previous section.

Aiming at the identification of recent trends and gaps, our research was limited to the period 2016-2024, selecting only papers whose results included correlations related to all three main concepts targeted: cyber security, ensured by AI technology integrations within the organizational information systems / ERP systems.

Due to the unprecedented level of complexity and interconnectivity between systems, people, devices and networks, a cybersecurity-centered multi- and interdisciplinary future research orientation is considered a priority (Tagarev, et al., 2019). We estimate that Intelligence Augmentation of information systems in general and, to fill the gap identified in the literature, of

ERPs in particular, oriented towards ensuring their cyber security, represents a future research area of increased interest for both business and healthcare organizations. Moreover, cyber-risk mitigation, counterterrorism tools and procedures, and data privacy constitute rapidly emerging research areas. Addressing system cyber-security issues, related to the safety of both companies and users in the context of AI integration, could also be the focus of future research.

References

Alem, S., Espes, D., Martin, E., Nana, L.,v De Lamotte, F. (2019). A hybrid intrusion detection system in industry 4.0 based on ISA95 standard. In 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA) (pp. 1-8). IEEE. https://doi.org/10.1109/AICCSA47632.2019.9035260

Alrfai, M. N., Alqudah, H., Lutfi, A., Al-Kofahi, M., Alrawad, M., Almaiah, M. (2023). The influence of artificial intelligence on the AISs efficiency: Moderating effect of the cyber security, *Cogent Social Sciences*, 9(2). https://doi.org/10.1080/23311886.2023.2243719

Aurucci, P. (2018). Applications and Security Risks of Artificial Intelligence for Cyber Security in Digital Environment. In *Intelligent Environments 2018*, 23 (pp. 308-317). IOS Press. https://doi.org/10.3233/978-1-61499-874-7-308

Aldoseri, A., Al-Khalifa, K.N., Hamouda, A.M. (2024). Methodological Approach to Assessing the Current State of Organizations for AI-Based Digital Transformation. Appl. Syst. Innov. 2024, 7, 14. https://doi.org/ 10.3390/asi7010014

Bawa, S. S. (2023). How Business can use ERP and AI to become Intelligent Enterprise. *International Journal of Innovative Science and Research Technology*, 8(2), 1186–1189. https://doi.org/10.5281/zenodo.7688737

Butler, T., Gozman, D., & Lyytinen, K. (2023). The regulation of and through information technology: Towards a conceptual ontology for IS research. *Journal of Information Technology*, 38(2), 86-107. https://doi.org/10.1177/02683962231181147

Cui C, Shen G, Wang Y, Xu Y, Du H, Zhang W, Kong X. (2023). Impact of In-Air Gestures on In-Car Task's Diver Distraction. *Electronics*, 12(7):1626. https://doi.org/10.3390/electronics12071626

Costa, C., Aparicio, M., & Raposo, J. (2020). Determinants of the management learning performance in ERP context. *Heliyon*, 6. https://doi.org/10.1016/j.heliyon.2020.e03689.

Dawson, M., Martinez, F. G. and Taveras, P. (2019). Framework for the development of virtual labs for industrial internet of things and hyperconnected systems. In 2019 IEEE Learning With MOOCS(LWMOOCS) (pp.196-198), IEEE https://doi.org/10.1109/ lwmoocs47620.2019.8939660

François, M., Arduin, P. E., Merad, M. (2021). Artificial Intelligence & Cybersecurity: A Preliminary Study of Automated Pentesting with Offensive Artificial Intelligence. In: Saad, I., Rosenthal-Sabroux, C., Gargouri, F., Arduin, P. E. (eds) Information and Knowledge Systems. Digital Technologies, Artificial Intelligence and Decision Making. ICIKS 2021. *Lecture Notes in Business Information Processing*, vol 425. Springer, Cham. https://doi.org/10.1007/978-3-030-85977-0_10

eSentire(2023). 2023 Official Cybercrime Report by Cybersecurity Ventures. Retrieved from: https://www.esentire.com/resources/library/2023-official-cybercrime-report

Forbes (2023). Navigating The Future Of Generative AI And ERP Cybersecurity. Retrieved from: https://www.forbes.com/sites/forbestechcouncil/2023/10/30/navigating-the-future-of-generative-ai-and-erp-cybersecurity/?sh=c1c5ac93303b

Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Comput. Secur.*, 109, 102382. https://doi.org/10.1016/J.COSE.2021.102382.

Gatti, G., Basile, C. and Perboli, G. (2023). An expert system for automatic cyber risk assessment and its AI-based improvements, 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC), Torino, Italy, 2023, 1434-1440, https://doi.org/10.1109/COMPSAC57700.2023.00220.

Gupta, S., Modgil, S., Meissonier, R. and Dwivedi, Y. K. (2021). Artificial Intelligence and Information System Resilience to Cope With Supply Chain Disruption. *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2021.3116770.

He, Y., Zamani, E., Kun, N.,Yevseyeva, I. & Cunjin, L. (2022). AI-based Ethical Hacking for Health Information Systems (HIS): a simulation study (Preprint). *Journal of Medical Internet Research*. 25. https://doi.org/10.2196/41748

Hamon, R., Junklewitz, H., Sanchez, I., Malgieri, G., & Hert, P. (2022). Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making. *IEEE Computational Intelligence Magazine*, 17, 72-85. https://doi.org/10.1109/MCI.2021.3129960.

Hosney, E.S., Halim I.T.A. and Yousef, A. H. (2022). An Artificial Intelligence Approach for Deploying Zero Trust Architecture (ZTA). *2022 5th International Conference on Computing and Informatics (ICCI)*, New Cairo, Cairo, Egypt, pp. 343-350, https://doi.org/10.1109/ICCI54321.2022.9756117.

Indre, I. and Lemnaru, C. (2016). Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things. In *2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP)* (pp. 175-182). IEEE.

Jain, H., Padmanabhan, B., Pavlou, P.A., Raghu, T.S. (2021). Editorial for the special section on humans, algorithms, and augmented intelligence: The future of work, organizations, and society. *Information Systems Research*, 32(3), 675-687. https://doi.org/10.1287/isre.2021.1046

Jada Irshaad, Mayayise Thembekile O. (2023). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review, Data and Information Management, 100063, ISSN 2543-9251, https://doi.org/10.1016/j.dim.2023.100063.

Kholidy, H. (2021). Autonomous mitigation of cyber risks in the Cyber-Physical Systems. *Future Gener. Comput. Syst.*, 115, 171-187. https://doi.org/10.1016/j.future.2020.09.002.

Kumar, S. and Mallipeddi, R.R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions, Production and Operations Management, Production and Operations Management Society, vol. 31(12), pp. 4488-4500, December. https://doi.org/10.1111/poms.13859.

Larriva-Novo, X., Vega-Barbas, M., Villagrá, V., Berrocal, J. (2021). Análisis comparativo y evaluación de la aplicación de técnicas deep learning a datasets de ciberseguridad. *DYNA-Ingeniería e Industria*, 96(5), 528-533. https://doi.org/10.6036/10007

Lee, S. (2021). AI-Based CYBERSECURITY: Benefits and Limitations. *Journal of Instrumentation*, 6, 18-28. https://doi.org/10.22471/AI.2021.6.1.18.

Lee, C.W. and Madnick, S. (2021). Cybersafety approach to cybersecurity analysis and mitigation for mobility-as-a-service and internet of vehicles. *Electronics*, 10(10), 1220. https://doi.org/10.3390/electronics10101220

Levshun Diana and Kotenko Igor (2023). A survey on artificial intelligence techniques for security event correlation: models, challenges, and opportunities. Artif. Intell. Rev. 56, 8 (Aug 2023), 8547–8590. https://doi.org/10.1007/s10462-022-10381-4

Lohn, A., Knack, A., Burke, A., & Jackson, K. (2023). Autonomous Cyber Defense. . https://doi.org/10.51593/2022ca007

Levshun, D., Kotenko, I. (2023). A survey on artificial intelligence techniques for security event correlation: models, challenges, and opportunities. *Artificial Intelligence Review,* 56, 8547–8590. https://doi.org/10.1007/s10462-022-10381-4

Michailidi, E., Michailidis, H., Tavoultzidou, S., Papatsimouli, M., Fragulis, G. F. (2021). Digital Transformation of Small Greek Companies During the Covid-19 Pandemic. In 2021 International Conference on Decision Aid Sciences and Application (DASA), Sakheer, Bahrain, 2021 (pp. 1103-1108). *IEEE*. https://doi.org/10.1109/DASA53625.2021.9682410

Maurya, R. (2023). Analyzing the Role of AI in Cyber Security Threat Detection & Prevention. *International Journal for Research in Applied Science and Engineering Technology*. https://doi.org/10.22214/ijraset.2023.56510.\

Mottaleb, A. & Canan, M. (2021). Analyzing the Cyberattacks Sponsored by State-Actors Under the Contemporary Global Political and Legal Frameworks. In ICCWS 2021 16th International Conference on Cyber Warfare and Security (p. 223-230). Academic Conferences Limited.

Mohan, P. V., Dixit, S., Gyaneshwar, A., Chadha, U., Srinivasan, K., Seo, J.T. (2022). Leveraging Computational Intelligence Techniques for Defensive Deception: A Review, Recent Advances, Open Problems and Future Directions. *Sensors (Basel)*. Mar 11, 22(6), 2194. https://doi.org/ 10.3390/s22062194.

Maia, E., Wannous, S., Dias, T., Praça, I., Faria, A. (2022). Holistic Security and Safety for Factories of the Future. Sensors. 22(24):9915. https://doi.org/10.3390/s22249915

Mogollón-Gutiérrez, J.C., Núñez, S., Vegas, M.A., Lindo, A.C. (2023). A novel ensemble learning system for cyberattack classification, Intelligent Automation & Soft Computing, vol. 37, no.2, pp. 1691–1709 . https://doi.org/10.32604/iasc.2023.039255

Morrison, Christina (2024). *AI in ERP: The Next Wave of Intelligent ERP Systems, ERP Technologies*, posted on Jan 23, 2024. Retrieve from: https://www.top10erp.org/blog/ai-in-erp

Murugesan, S. (2022). The AI-Cybersecurity Nexus: The Good and the Evil. in IT Professional, vol. 24, no. 5, pp. 4-8, 1 Sept.-Oct. 2022, https://doi.org/10.1109/MITP.2022.3205529.

Ospina Díaz, M.R., Vera Osorio, S.P. & Zambrano Ospina, K.J. (2023). Sistemas de Información de Administración Financiera (SIAF) en la gobernanza pública inteligente: una exploración del caso colombiano, Opera. 34 (nov. 2023), 31–55. https://doi.org/10.18601/16578651.n34.03.

Onapsis (2024). ERP Applications Under Fire: How cyberattackers target the crown jewels. Retrieved from: https://onapsis.com/resources/reports/erp-applications-under-fire-report/

Pawlicki, M., Choraś, M. and Kozik, R. (2019). Recent granular computing implementations and its feasibility in cybersecurity domain. In Proceedings of the 13th International Conference on Availability, *Reliability and Security* (ARES 2018) (pp. 1-6).

Pawlicki, M., Choraś, M., Kozik, R., Hołubowicz, W. (2021). Missing and Incomplete Data Handling in Cybersecurity Applications. In: Nguyen, N.T., Chittayasothorn, S., Niyato, D., Trawiński, B. (eds) Intelligent Information and Database Systems. ACIIDS 2021. *Lecture Notes in Computer Science*, 12672 (pp. 413-426). *Springer*, Cham. https://doi.org/10.1007/978-3-030-73280-6_33

Poulsen, A., Fosch-Villaronga, E., and Burmeister, O. K. (2020). Cybersecurity, value sensing robots for LGBTIQ+ elderly, and the need for revised codes of conduct. *Australasian Journal of Information Systems*, 24. https://doi.org/10.3127/ajis.v24i0.2789

Ramanpreet, K., Dušan, G., Tomaž K. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions, *Information Fusion*, Volume 97, 2023, 101804, ISSN 1566-2535, https://doi.org/10.1016/j.inffus.2023.101804

SAP(2024). What is Internet of Things? (IoT). Retrieved from: https://www.sap.com/products/artificial-intelligence/what-is-iot.html

Sen, R., Heim, G., and Zhu, Q. (2022). Artificial Intelligence and Machine Learning in Cybersecurity: Applications, Challenges, and Opportunities for MIS Academics. *Communications of the Association for Information Systems*, 51, https://doi.org/10.17705/1CAIS.05109

Samtani, S., Zhu, H., Padmanabhan, B., Chai, Y., Chen, H. & Nunamaker Jr., J. F. (2023). Deep Learning for Information Systems Research, *Journal of Management Information Systems*, 40:1, 271-301

Sarcevic, A., Pintar, D., Vranic, M., Krajna, A. (2022). Cybersecurity Knowledge Extraction Using XAI. *Applied Sciences*.12, 8669. https://doi.org/10.3390/app12178669

Sipior, J. (2021). Monitoring Remote Employees at FinPro. Communications of the Association for Information Systems, 49(1), 14, 304-320. https://doi.org/10.17705/1CAIS.04912

Singh, N., Krishnaswamy, V. and Zhang, J. (2022). Intellectual structure of cybersecurity research in enterprise information systems. *Enterprise Information Systems*. 17. 1-25. https://doi.org/10.1080/17517575.2022.2025545.

Stafford, T. F. (2022). Platform-Dependent Computer Security Complacency: The Unrecognized Insider Threat. *IEEE Transactions on Engineering Management*, 69(6), 3814-3825. https://doi.org/10.1109/TEM.2021.3058344

Tagarev, T., Stoianov, N. and Sharkov, G. (2019). Integrative approach to understand vulnerabilities and enhance the security of cyber-bio-cognitive-physical systems. In Cruz, T. and Simoes, P., Proceedings of the 18th European Conference on Cyber Warfare and Security (ECCWS 2019, Coimbra, Portugal), (pp. 492-500). Academic Conferences International Limited.

Tran, D. M., Thwaites, C.L., Van Nuil, J.I., McKnight, J., Luu, A. P., Paton, C. (2022), Vietnam ICU Translational Applications Laboratory (VITAL). Digital Health Policy and Programs for Hospital Care in Vietnam: Scoping Review. *Journal of Medical Internet Research*, 2022 Feb 9;24(2), e32392. https://doi.org/10.2196/32392

Vargas, M., & Comuzzi, M. (2020). A multi-dimensional model of Enterprise Resource Planning critical success factors. *Enterprise Information Systems*, 14, 38-57. https://doi.org/10.1080/17517575.2019.1678072.

Wan, B., Xu, C., Mahapatra, R. P., Selvaraj, P. (2022). Understanding the cyber-physical system in international stadiums for security in the network from cyber-attacks and adversaries using AI.*Wireless Personal Communications*, 127(2), 1207-1224. https://doi.org/10.1007/s11277-021-08573-2

Ye, J. (2021). Health information system's responses to COVID-19 pandemic in China: a national cross-sectional study. *Applied Clinical Informatics*, 12(02), 399-406. https://doi.org/10.1055/s-0041-1728770

Yathiraju, Nikhitha (2022). Investigating the use of an Artificial Intelligence Model in an ERP Cloud-Based System, *International Journal of Electrical*, Electronics and Computers (IJECC), Vol-7, Issue-2, March - April 2022, Pages 1-26, 10.22161/eec.72.1

Zhao, F., Zhang, H., Peng, J., Zhuang, X., & Na, S. (2020). A semi-self-taught network intrusion detection system. *Neural Computing and Applications*, 1-11. https://doi.org/10.1007/s00521-020-04914-7.

Zeadally, S., Adi, E., Baig, Z., & Khan, I. (2020). Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. *IEEE Access*, 8, 23817-23837. https://doi.org/10.1109/ACCESS.2020.2968045.