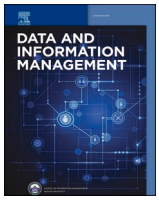
8 (2024) 100063

Contents lists available at ScienceDirect

Data and Information Management

journal homepage: www.journals.elsevier.com/data-and-information-management



The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review

Irshaad Jada, Thembekile O. Mayayise *

Information Systems Division, School of Business Sciences, University of the Witwatersrand, Private Bag 3, Wits, 2050, South Africa

ARTICLE INFO

Keywords:
Cyber security
Artificial intelligence
Machine learning
SLR

ABSTRACT

As digital transformation continues to advance, organisations are becoming increasingly aware of the benefits that modern technologies offer. However, with greater technology adoption comes a higher risk of cyber security threats and attacks. Therefore, there is a need for more advanced measures to protect against constantly evolving threats. One potential solution is the use of Artificial Intelligence (AI). The aim of this research paper was to conduct a systematic literature review (SLR) to assess the impact of AI-based technologies on organisational cyber security and determine their effectiveness compared to traditional cyber security approaches. The PRISMA flow diagram was used to guide the review process. Peer-reviewed articles from 2018 to 2023 were included from EBSCO Host, Google Scholar, Science Direct, ProQuest & SCOPUS and 73 remaining articles were synthesised.

The results revealed that AI can impact cybersecurity throughout it's entire life cycle, yielding benefits like automation, threat intelligence, and improved cyber defense. Nevertheless, it also brings challenges like adversarial attacks and the need for high-quality data, which could lead to the inefficiency of AI. These results affirm the positive influence of AI on cybersecurity, enhancing effectiveness and resilience. These findings provide a solid foundation for further research in the field of organisational cybersecurity. These results can help organisations make informed decisions on AI implementations by offering an impartial view of its impacts.

1. Introduction

The technological revolution has led to the quick development and acceptance of new and improved technologies. However, this has also resulted in a rapid evolution of cyber-related threats and attacks, as noted by Cucu (Cucu, GAVRIOLOAIA, BOLOGA, & CAZACU, 2019) and the National Academies of Sciences (National Academies of Sciences et al., 2019). These attacks are becoming more frequent, numerous, and impactful. To counteract these constantly evolving threats, it is necessary to have advanced and secure cyber security measures and protective mechanisms (Wiafe et al., 2020).

Cyber security safeguards internet-facing information and communication systems against malicious attacks and threats (Li & Liu, 2021). The Fourth Industrial Revolution and the Industrial Internet of Things (IIoT) have expanded the scope of cyber security from network and application security to infrastructure, cloud, and information security, making it multi-dimensional (Yu & Guo, 2019). Cyber security encompasses various interrelated components and technologies in cyberspace rather than just being limited to system security. In an organisational context, cyber security involves protecting all relevant cyberspace dimensions simultaneously (Li & Liu, 2021).

The concept of "Artificial Intelligence" emerged in 1956 and has since evolved into practical solutions used across various fields, as highlighted by Alom (Alom et al., 2018). Machine Learning's role in cybersecurity dates to the 1990s with the development of anomaly detection systems (ADS) and intrusion detection systems (IDS) (Joseph, Laskov, Roli, Tygar, & Nelson, 2013), though progress was hindered by data and computing limitations, as noted by (Qiu, Wu, Ding, Xu, & Feng, 2016). Today, AI is integral to cybersecurity, transcending corporate jargon (Kaplan & Haenlein, 2019) (Abbas, Ahmed, Shah, Omar, & Park, 2019). It can simulate human intelligence and behaviours, resulting in automation in cyber security beyond human capability, which can detect a security breach in a network within seconds (Zhang et al., 2021). The COVID-19 pandemic accelerated digital transformation, making businesses dependent on technologies like AI, Machine learning (ML), and Big Data. However, this led to a surge in cybercrimes, endangering individuals and established organisations. Eian (Eian, Yong, Li, Qi, & Fatima, 2020) predicts cybercrimes could cost $10.5

* Corresponding author.
E-mail addresses: 1817161@students.wits.ac.za (I. Jada), Thembekile.Mayayise@wits.ac.za (T.O. Mayayise).

https://doi.org/10.1016/j.dim.2023.100063
Received 29 June 2023; Received in revised form 15 December 2023; Accepted 16 December 2023
Available online 25 December 2023

trillion by 2025. Due to their reliance on these technologies, businesses face operational and continuity risks. The use of AI in cybersecurity is worth exploring so that organisations can understand the capabilities of AI in the cybersecurity space for the benefit of their organisation.

Advancements in Data Science and Computer Science have led to the emergence of ML, the most prominent type of AI in organisational cyber security (Scott & Kyobe, 2021). Machine Learning involves a machine's ability to learn and adapt through experience. It is deemed a subset of AI, and it focuses on the implementation of certain types of systems which can learn from historical data to identify patterns and make decisions independently (Wazid, Das, Chamola, & Park, 2022).

The vast amounts of data generated by organisations provide opportunities for a wide range of ML applications in cyberspace, including threat intelligence, anomaly detection, and automation of cybersecurity-related tasks (Huang & Rust, 2018). This relationship between AI and cyber security is called cyber-AI (Abbas et al., 2019). This study aims to look at the impact of AI on cyber-security from an organisational perspective.

1.1. Problem statement

The implementation of AI, specifically ML solutions in cyber security, can be traced back to the late 1980's, when the first anomaly detection system (ADS) was implemented (Joseph et al., 2013). This was superseded by developing an intrusion detection system (IDS) in the 1990's. Due to the lack of structured and clean data, coupled with limitations of computing power, its progression was delayed for a while (Qiu et al., 2016). Today, AI has since grown to revolutionise the capabilities of modern-day technologies in cyber security (Lo et al., 2020, p. pp129). According to (Kaplan & Haenlein, 2019), implementing AI-driven solutions in organisational cyber security has become more of a necessity.

As digital transformation has advanced steadily in recent years, there has been a growing reliance on the Internet and Information and Communication Technologies (ICTs) (Eian et al., 2020). This has led businesses to recognise the immense potential and significance of modern technologies like AI, ML, and Big Data (Almeida, Santos, & Monteiro, 2020). However, the widespread adoption of ICTs has also resulted in an increase in cybercrimes, threats, and vulnerabilities that target both individuals and established organisations (Zhang et al., 2021). Since February 2020, there has been a significant surge in cyber-related crimes and given the dependence of organisations on these technologies, cyber threats and attacks can have dire consequences on their operations and business continuity (Almeida et al., 2020).

In the past few years, research has been carried out to assess how AI affects various technological environments. Malatji (Malatji, Marnewick, & von Solms, 2018) conducted a comprehensive examination of AI's effect on the human aspects of cybersecurity within enterprises. In a similar study, Malatji et al. (Malatji et al., 2018) conducted a systematic literature review, primarily aiming to examine the influence of AI on the human aspect of information and cybersecurity. The findings suggested that AI presently enhances human abilities and predicted a potential transformation as AI evolves toward autonomy. Their review spanned publications from 2008 to 2018 and specifically examined a maximum of 12 articles per journal. The distinction between their research and the present study lies in the focus area where the current study delves into the broader impact of AI on organisational cybersecurity without restricting it to the human dimension alone. Additionally, it encompasses more recent literature, and there is no predetermined limit on the number of articles to be synthesised per journal.

In another comparable investigation conducted by De Azambuja et al. (De Azambuja et al., 2023), their emphasis was on identifying pertinent literature related to artificial intelligence-driven cyber-attacks to evaluate the features of such attacks for devising cybersecurity measures. The distinction between their research and the present study lies in their focal point. Their literature review, confined to just two databases, resulted in the synthesis of fewer than 30 articles. In contrast, our current study utilises five databases, adopting a more expansive approach to scrutinise the overall impact of AI on organisational cybersecurity. Our objective is to unveil both the positive and negative impact of AI, making this study more encompassing.

Harnessing AI's evolving capabilities can be a significant advantage for enterprises in safeguarding against cyber-attacks. Considering that the study by (Malatji et al., 2018) was conducted five years ago, it is worth revisiting the literature sources in line with the advancements in the use of AI in cybersecurity hence, this study was undertaken.

Overall, the studies which have been done to date to ascertain the impact of AI on Cybersecurity are quite scant, owing to the rapid advancements in ICT, and this paper aims to help narrow the gap.

This study aims to evaluate the impact of AI-driven technologies on organisational cybersecurity, including their positive and negative effects, and to determine the effectiveness of Cyber-AI compared to traditional cybersecurity measures.

The **main research** question that this study seeks to address is:

What is the impact of Artificial Intelligence on organisational cybersecurity?

The following **secondary research** questions will be considered in answering the primary research question:

1. What is the positive impact of AI on cyber security from an organisational perspective?
2. What is the negative impact of AI on cyber security from an organisational perspective?
3. How does the use of AI differ from traditional, non-AI-driven means of organisational cyber security?

The remainder of this paper is arranged in the following manner: Section 2 covers the research method, Section 3 discusses the results, and the study concludes in Section 4.

2. Research method

This study followed a structured process for conducting a systematic literature review, which entails planning, selection/searching and extraction and execution (Lo et al., 2020, p. pp129; Okoli, 2015; Page et al., 2021). The scope of the literature included searching for scholarly literature from the following database sources: ScienceDirect, EBSCOhost, SCOPUS and ProQuest because they were deemed to contain multi-disciplinary sources of which AI forms part (Zhang et al., 2021). Google Scholar was also used to search for other relevant sources which could be used to enhance this study. However, most of the articles identified in Google Scholar were identified as duplicates and were removed.

Table 1
Inclusion and Exclusion criteria.

Included	Excluded
Studies that focus on the Impact of AI on Cyber Security in an organisational setting	Studies that do not focus on the Impact of AI on Cyber Security in an organisational setting
Literature published in English only	Non-English written articles
Peer-reviewed journal articles, Books and conference proceedings whose content appears in any of the following database sources: Science Direct, EBSCOhost, ProQuest, Google Scholar, SCOPUS	Non-peer-reviewed literature sources
Open-access literature sources	Not subscribed to by the institution affiliated/Sources with restricted access
Literature sources published between 2018 and 2023	Studies published before 2018

2.1. Inclusion & exclusion criteria

Table 1 details the inclusion criteria adhered to in identifying relevant studies for this study. The formulation of the inclusion and exclusion criteria was informed by the research questions and objectives of this study and covered in Table 1.

Only peer-reviewed literature from conference proceedings, journal articles and book chapters, written in English, published since 2018–2023 and were available for full access through the researcher's institution's subscription, were included in this study.

2.2. Search terms

In searching for the relevant sources in the selected databases, flexible and relevant keywords and Boolean operators were used to formulate search strings. The keywords combination was in such a manner that focused on the research questions. Table 2 contains the keywords and database strings used in the selected sources.

The search strings for EBSCOhost & Science Direct to search for relevant information were the same. However, for ProQuest the initial search strings were the same as those used for EBSCOhost and Science Direct databases but yielded an excessive number of sources, and the search string and the search string had to be refined to what has been included in Table 2, which resulted in a reasonable number of search results. SCOPUS also yielded a high number of sources with the initial search string, and the sources which were considered were open-access sources which met the search criteria.

The entire SLR was further guided by using the Preferred Reporting Items for Systematic Reviews and Meta-analysis (PRISMA) flow diagram, whose steps are explained in section 2.3. The literature search was conducted between November 2022 and September 2023.

2.3. PRISMA flow diagram

The PRISMA flow diagram depicted in Fig. 1 was used in this study to systematically review the selected literature, using the selected keywords and database strings included in Table 2. It consists of four distinct stages, i.e., Identification, screening, eligibility, and synthesis, which also covers the reporting aspect. The identification stage focuses on identifying relevant literature sources in the chosen databases, especially the open-access sources. In this stage, the search results yielded 19234 combined results. In the screening phase, the articles were screened for any potential duplicates, and this brought down the number of records to 1814 records. Out of these records, a further 1752 were removed based on the abstract and keywords review and those with access restrictions, which resulted in 73 articles remaining. Those were the only remaining articles which were synthesised and reported on. These articles were then imported to the Mendeley referencing tool for sorting and analysis.

Table 2
Keywords and Database Search string.

Database	Search String/Query
EBSCOhost & ScienceDirect	("Organisations" OR "Enterprise") AND ("Cyber security" OR "Computer security" OR "System Security") AND ("Artificial Intelligence" OR "Machine learning" AND ("Impact" OR "Effect")
ProQuest	((SU.exact("Artificial intelligence") OR SU.exact("machine learning") AND SU.exact("cyber security"))
Google Scholar	("Organisation" OR "Enterprise") AND ("Cyber security" OR "Computer security" OR "System Security") AND ("Artificial Intelligence" OR "Machine learning" AND ("Impact" OR "Effect")
SCOPUS	(Artificial Intelligence OR Machine learning") AND ("Cyber Security" OR "Information Security") AND ("Impact" OR "Effect")

2.4. Bias

In preserving academic rigour and minimising bias, the following biases were identified during the review, i.e., selection, reporting and competing Bias. Selection bias, which can be interpreted as not selecting all the relevant literature for the study (Hernán, Hernández-Díaz, & Robins, 2004), was addressed by selecting four multidisciplinary database sources. According to (Drucker, Fleming, & Chan, 2016), reporting bias equates to the selective reporting of findings; the researchers followed the steps set out in the PRISMA flow diagram, especially when it came to the identification of the articles which were eligible for reporting. Competing Bias may arise when research is funded and connected to a certain organisation (Drucker et al., 2016). To address this, the researchers declare that there is no conflict of interest or association with a particular organisation as this study is concerned.

2.5. Data analysis

Considering the qualitative nature of the study, a thematic analysis of the data was conducted to provide a rich, descriptive representation of the data gathered (Clarke, Braun, & Hayfield, 2015). This data analysis approach allowed for a phased and structured data analysis. According to (Peel, 2020), the first step in conducting thematic analysis requires that the researchers familiarise themselves with the data. This was achieved by sorting and categorising the data of the included articles. The initial codes were created through the observation of recurring patterns, which resulted in themes which were created, and the findings were then presented in a meaningful manner. The findings can be linked back to the original research questions.

2.5.1. Coding strategy

Coding is an essential aspect of qualitative research, as it helps analyze and interpret data extracted in relation to research questions. Coding entails categorising concepts and identifying recurring patterns and themes within the data through an iterative process (Creswell, 2015). In this review, a hybrid coding strategy combining both inductive and deductive approaches was employed (Azungah, 2018). Inductive coding involves deriving codes directly from the reviewed data, while deductive coding utilises predefined codes from previous research. This hybrid approach allowed for a flexible data analysis focusing on the impact of AI on organisational cybersecurity. While some literature already had predefined themes on this topic, enabling the deductive establishment of themes, the rigorous evaluation of the literature led to the emergence of additional themes and concepts, which required an inductive coding approach.

3. Results

The outcome of the literature search and review resulted in a total of 73 articles remaining for detailed synthesis in line with the stated research questions. Fig. 2 shows the breakdown of the synthesised articles, highlighting that most of the synthesised sources were 55 journal articles and 18 conference papers, which is a good indication that peer-reviewed sources were consulted to reach certain conclusions in this study.

Fig. 3 depicts the distribution of the synthesised articles per year. In terms of the distribution of the research articles based on the scope of our study, which covers 2018–2023, it is evident that studies on the impact of AI on organisational cybersecurity started gradually in 2019, where only 1 study was found in relation to this study.

From 2020 to 2021, there was a gradual increase from 8 articles to 13 articles; in 2022, there was a sharp increase where the number of publications more than doubled to 28. In 2023, the number of relevant articles found was 23, which seems like a decline; however, considering that at the time of writing of this article, a few months remained before year-end, the number is more likely to increase. The picture portrayed in

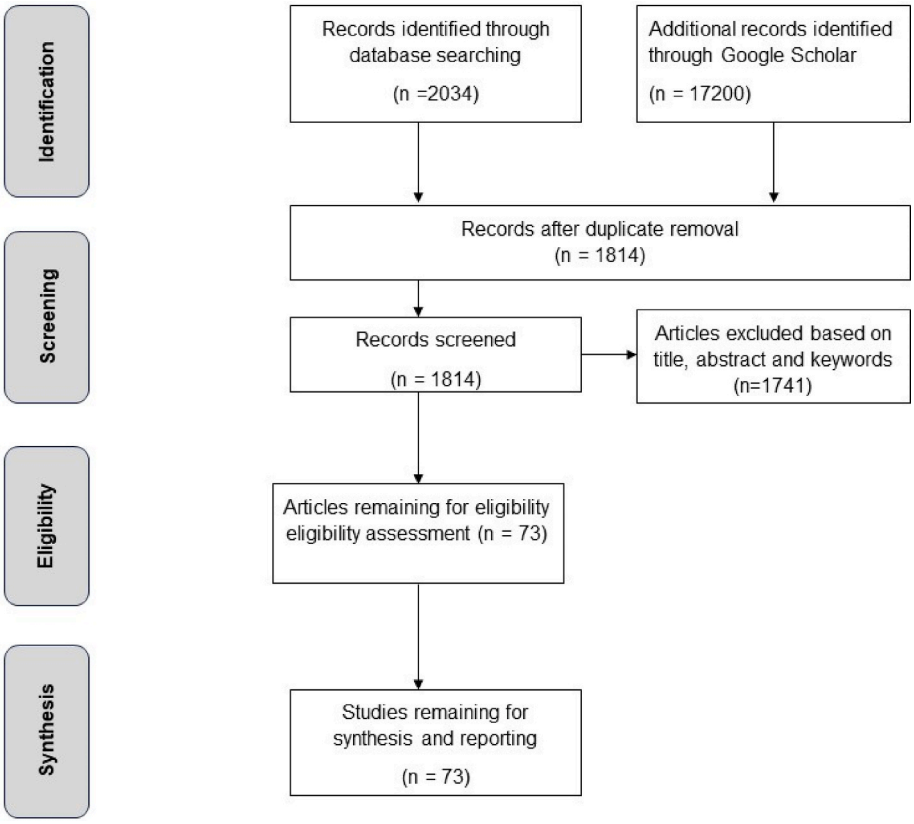


Fig. 1. Adapted PRISMA flow diagram (Page et al., 2021) (Selçuk, 2019).

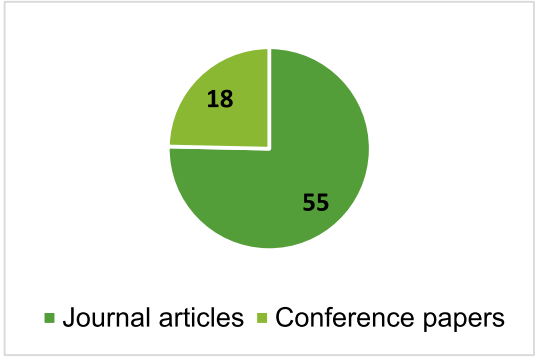


Fig. 2. Breakdown of articles synthesised.

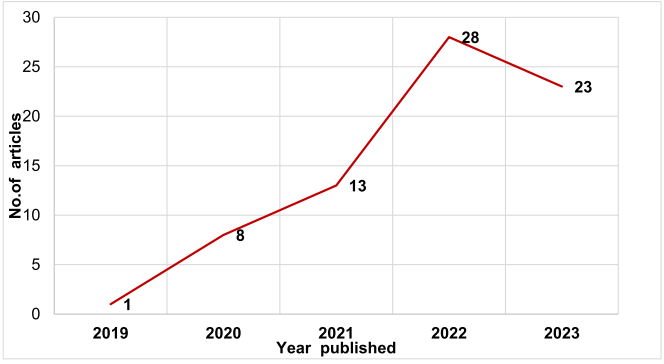


Fig. 3. Article distribution.

Fig. 3 shows a growing interest by scholarly researchers in understanding the impact of AI on organisational cybersecurity, which could be due to the ongoing advancements in the use of AI and relevant techniques in Organisational cybersecurity.

The schematic depiction of the findings is in Fig. 4, and Tables 3–5 summarise the sub-themes identified in relation to research questions one, two and three, respectively. The impact is centred around the impact of AI on cybersecurity from an organisational perspective, which is the main theme explained in relation to the stated research questions.

Fig. 4 presents a visual representation of the research findings. It displays the results related to Q1, which are grouped together, and separately showcases the findings for Q2 and Q3. Given that 73 articles were analysed, this summary highlights some of the sub-themes regarding the positive or negative influence of AI on Cybersecurity from an organisational standpoint and how AI compares to the traditional approaches. Table 3 outlines the sub-themes derived from multiple sources as individual entries, while findings that were less common but unique are consolidated under the "other" category.

AI's most significant influence lies in the realm of vulnerability management, especially in intrusion detection. It also plays a crucial role in bolstering the security of organisational networks and systems against cyber threats. The positive effects of AI on cybersecurity encompass various facets, including predicting cyber incidents and aiding in data recovery, ultimately contributing to an organisation's competitive edge. These overarching themes are presented in Table 3. These themes underscore certain trends in the prevalent applications of AI, including intrusion detection, improved security measures, and the identification of malicious software.

Table 4 provides an overview of the findings related to research question 2, which examines the adverse effects of AI on cybersecurity from an organisational standpoint. According to the results, most of the identified negative consequences were categorised as unique and under the "other" category. Additionally, the literature highlighted the

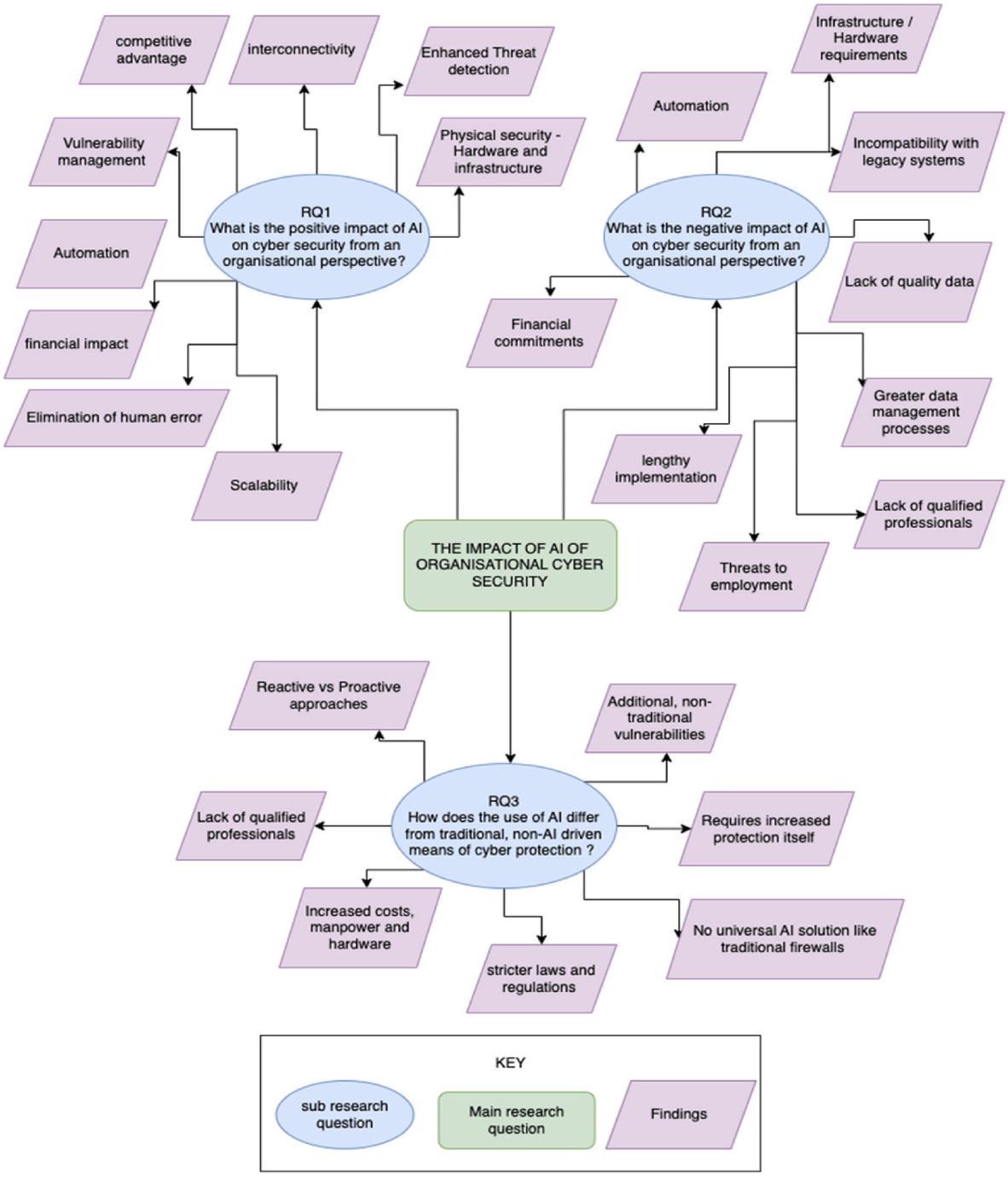


Fig. 4. Thematic map.

worrisome issue of AI systems being vulnerable to exploitation, which poses a significant detriment to organisational cybersecurity.

A shortage of skilled individuals and the absence of effective AI techniques for generating predictive explanations are perceived as factors that have a detrimental effect on organisations' cybersecurity. Additionally, adversarial attacks are recognised as contributors to cybersecurity challenges, as hackers persistently endeavour to deploy deceptive tactics that can outsmart security systems. Table 5 provides a concise overview of AI's performance compared to traditional non-AI methods, and it pertains to the study's third research question.

Based on the results of the experiments conducted in some of the literature reviewed, comparing AI and non-AI approaches, it became clear that AI-based methods outperformed the other methods in terms of their effectiveness and precision, offering increased security and improved capabilities for detecting intrusions.

3.1. Discussion

The literature review results are presented in this section to comprehensively discuss the overall effects of AI-based solutions on organisational cybersecurity. This analysis considers both the positive and negative impacts. Furthermore, to gain a complete understanding of the overall impact, a comparison between AI and traditional methods of cyber protection was necessary for a broader view. Hence, this review also examines the differences between AI and traditional, non-AI approaches to organisational cybersecurity.

Table 3
Summary of results-positive impact of AI on cybersecurity.

Sub-Themes	No of articles	Sources
Intrusion Detection	16	(Gupta, Sabitha, & Punhani, 2019; Haider, Khan, Rehman, Ur Rahman, & Kim, 2020; Joseph, Elmalech, & Hajaj, 2023; Keshk et al., 2023; Ma, Dhot, & Raza, 2023; Macas & Wu, 2020; Maia et al., 2022; Mogollón-Gutiérrez, Núñez, Vegas, & Lindo, 2023; Nagy et al., 2023; Ndichu, Ban, Takahashi, & Inoue, 2023; Redino et al., 2022; Sivamohan & Sridhar, 2023; Sowmya & Mary Anita, 2023; Thapa, Liu, Kc, Gokaraju, & Roy, 2020; Thapa et al., 2020, 2020; The, Luong, Nguyen, & Hoang, 2023)
Enhanced Protection	12	(Ahamed et al., 2022; Alhayani, Mohammed, Chaloob, & Ahmed, 2021; Chakraborty, Mitra, Mittal, & Young, 2022; Dias, Oliveira, Sousa, Praça, & Sousa, 2022; Ghandour, 2021; Jadav et al., 2023; Krichen, 2023; Naik, Mehta, Yagnik, & Shah, 2022; Ogundokun et al., 2021; Raimundo & Rosário, 2021; Sun & Bai, 2022; Truong, Diep, & Zelinka, 2020)
Other	8	(Agrawal, Hazratifard, Elmiligi, & Gebali, 2023; Aliyari, 2021; Angelopoulos et al., 2019; Ariffin & Maskat, 2021; Dawson, 2021; Kant & Johannsen, 2022; Pearce, Tan, Ahmad, Karri, & Dolan-Gavitt, 2023; Trim & Lee, 2022)
Malware detection	5	(Al-Khshali & Ilyas, 2023; Bhandari, Lyth, Shalaginov, & Grønli, 2023; Jo, Cho, & Moon, 2023; Kumar, Sharma, Vachhani, & Yadav, 2022; Ullah et al., 2022)
Attack prevention	4	(AL-Hawamleh, 2023; Chaithanya & Brahmananda, 2022; Massaro, Gargaro, Dipierro, Galiano, & Buonopane, 2020; Mhlanga, 2020)
Anomaly Detection	3	(Ha et al., 2022; Kaymakci, Wenninger, & Sauer, 2021; Krishnan, Jain, Aldweesh, Prabu, & Buyya, 2023)
Improved threat intelligence	2	(Kaur, Gabrijelčič, & Klobučar, 2023; Siddaway, 2014)

Table 4
Summary of results- negative impact of AI on cybersecurity.

Sub-Themes	No of articles	Sources
Other	14	(Alalwan, 2022; Brison, Wimmer, & Rebman, 2022; Dawson, 2021; Diallo & Patras, 2021; Ghandour, 2021; Lim, 2022; Muller, Pizzi, & Williams, 2022; Musbahi, Syed, Le Feuvre, Cobb, & Jones, 2021; Nagy et al., 2023; Ozturk, Ekmekcioglu, Cetin, Arief, & Hernandez-Castro, 2023; Prazeres, Costa, Santos, & Rabadão, 2023; Rawindaran, Jayal, & Prakash, 2021; Shroff, Walambe, Singh, & Kotecha, 2022; Sun & Bai, 2022)
AI systems can be exploited	5	(AL-Dosari, Fetais, & Kucukvar, 2022; Fritsch, Jaber, & Yazidi, 2022; Tetaly & Kulkarni, 2022; Truong et al., 2020; Zeadally, Adi, Baig, & Khan, 2020)
Adversarial attacks	4	(Dawson, 2021; Lim, 2022; Lu & Thing, 2022; Patil et al., 2021; Reilly, O'Shaughnessy, & Thorpe, 2023)
Lack of predictive explanations	4	(Capuano, Fenza, Loia, & Stanzione, 2022; Lu & Thing, 2022; Martin, 2021; Sharma, Birnbach, & Martinovic, 2023)
AI Skills shortage	2	(Dawson, 2021; Lim, 2022)

3.1.1. *The positive impact of AI on organisational cyber security*

To evaluate the overall influence of AI on organisational cybersecurity, this review focuses on the question: "What is the positive impact of AI on cybersecurity from an organisational perspective?" Existing research indicates that the rise of cyber threats and attacks has compelled organisations to adopt AI-based technologies for safeguarding their digital assets. While the initial driver for this adoption is necessary to implement AI in organisational settings, and its application to cyber protection results in significant competitive advantages to organisations (Dawson, 2021). Moreover, it is believed to bring a revolutionary change in modern-day cyber protection and its scope (Dawson, 2021). Table 3 presents a condensed overview of the underlying subtopics derived from the literature analysis related to the beneficial effects of utilizing AI in the context of malware detection (Al-Khshali & Ilyas, 2023; Bhandari et al., 2023; Kumar et al., 2022; Ullah et al., 2022), as well as in identifying other network or system intrusion incidents (Ha et al., 2022; Kaymakci et al., 2021; Krishnan et al., 2023). Additionally, AI's favourable influence extends to the realm of cybersecurity administration, streamlining operational procedures and enhancing overall convenience (Angelopoulos et al., 2019; Ariffin & Maskat, 2021).

Table 5
Summary of Results- How AI compares to the traditional approaches.

Sub-Themes	No.of articles	Sources
Enhanced performance	9	[38,67,27,82, 50,56,55,59,80]
Enhanced intrusion detection	2	(Keshk et al., 2023; Sivamohan & Sridhar, 2023)
Improved accuracy	2	(Mogollón-Gutiérrez et al., 2023; The et al., 2023)
Improved security	2	(Agrawal et al., 2023; Jadav et al., 2023)

By considering humans as the weakest link in the security chain, introducing AI-driven task automation is seen to address the vulnerabilities associated with human error in the workforce (Hansen & Bøgh, 2021). This is of utmost importance because, according to Alhayani et al. (Alhayani et al., 2021), human error is the primary cause of cybersecurity breaches. Whether it is a decision-based mistake, a skill-related oversight, or an error in task execution, intentional or not, eliminating the potential for human error is the initial step in establishing a well-protected cyber environment. This objective is achievable through improved threat detection methods, where using unsupervised machine learning intrusion detection systems (IDS) enables the identification of even the smallest threats or attacks before they happen. In the past, this task would take hours, but with AI, it can be done efficiently in seconds (Zhang et al., 2021).

This automation extends to vulnerability management and decision-making, where a specific branch of AI, Neural networks and Natural Language Processing (NLP), aids in the management and prioritisation of both known and unknown threats. It achieves this by analysing existing threats, newly discovered threats, false positives, network behaviour baselines, systems, and servers (Zhan, 2021). Through the identification of data patterns and the detection of abnormal behaviour, the system can identify potential risks (De Azambuja et al., 2023). Consequently, this automation enables organisations to adopt a proactive approach to recognising, anticipating, and addressing familiar and unfamiliar threats (Aliyari, 2021) rather than relying solely on reactive measures following a cyber breach. As stated by (Hariyanti, Djunaidy, & Siahaan, 2021), the automation of cybersecurity tasks reduces the need for human intervention, minimises human interaction, and subsequently reduces the potential for human error throughout the entire security life cycle.

In terms of organisational cybersecurity, it's not just about advanced software and protective solutions. The safeguarding of physical security and vital hardware and infrastructure components is crucial for an organisation to achieve comprehensive and mature cyber protection (Aliyari, 2021). The multifaceted nature of artificial intelligence (AI) can have a positive impact on the security of hardware and infrastructure by optimising and monitoring data centres, servers, and processors responsible for this protection (Angelopoulos et al., 2019). AI-powered solutions employ machine learning techniques to monitor aspects such

as hardware temperature, cooling systems, power consumption, and power backups. By analysing this data along with historical information, these solutions enhance hardware performance and overall infrastructure efficiency. Moreover, AI implementation helps to minimise the financial burden of hardware and infrastructure maintenance costs necessary for protecting an organisation. It achieves this by intelligently notifying organisations about scheduled maintenance or predicting potential failures of specific hardware components, enabling proactive replacement before a complete breakdown occurs. Ultimately, integrating AI technologies with hardware and infrastructure maintenance can provide financial savings for organisations and reduce the overall power consumption of hardware components (Kaplan & Haenlein, 2019).

Another positive impact of the use of cyber-AI prominent in the literature reviewed was the scalability and interconnectivity of AI solutions at a more advanced level (Ahamed et al., 2022). Network protection by means of AI-driven network analysis systems (NAS) and network protection systems (NPS) can guarantee the safety and availability of computer networks within an organisation, not just for a single computer but for an entire computer network system simultaneously (Zhan, 2021). These AI solutions can be deployed at each stage of the security life cycle, thus allowing for a more complete, well-rounded, and interconnected solution (Raimundo & Rosário, 2021).

3.1.2. The negative impact of AI on organisational cyber security

Although AI implementation in organisational cyber security is recognised for its ability to achieve efficiencies beyond human capabilities, there are several drawbacks associated with its adoption, particularly at the organisational level. Table 4 provides a condensed overview of the limitations it encompasses. The increased adoption of AI has led to an uptick in adversarial attacks, raising the threat of cyberattacks. The existence or absence of relevant regulations and standards can impede AI adoption within an organisation. These negative effects hinder or defer the widespread acceptance of AI solutions as a mainstream cybersecurity approach.

According to current literature, one of the main obstacles to the widespread adoption of AI in the cyber realm is its impact on infrastructure and hardware requirements. To effectively implement AI-driven solutions at the organisational level, significant computational power, processing capabilities, and memory are necessary (Dawson, 2021). Furthermore, larger and more advanced AI models demand modern central processing units (CPUs) that can perform ten times faster than traditional processors, resulting in substantial implementation costs (Wilkins, 2018). Another challenge lies in the compatibility issues caused by the continued use of outdated systems, programming languages, and overall technological infrastructure in many organisations. These legacy systems fail to adequately support the requirements of AI and machine learning (ML) techniques. For instance, the analysis of vast amounts of complex data, a critical step in successful AI and ML deployment, is hindered by the lack of scalability offered by legacy databases and obsolete systems. In essence, implementing AI solutions in organisations is not a simple task, as it often necessitates a complete overhaul of the technological infrastructure (Arasada, 2021).

The literature consistently highlights a recurring theme of insufficient availability of high-quality, error-free & cleaned data. AI solutions rely on extensive datasets for training models and achieving accurate results. As a result, obtaining a large quantity of data is essential for training AI models effectively (Sun & Bai, 2022). Moreover, implementing a cyber-AI solution necessitates a more complex organisational data management process due to the diverse volumes and types of data stored, the speed at which data is accumulated, the need to maintain data confidentiality, and the constant requirement for additional data (Raimundo & Rosário, 2021). This aspect is particularly crucial because the intelligence of AI solutions relies solely on the quality of the datasets used to train the models.

There is no universal cyber-AI solution that fits all situations, as most AI systems need to be customized for specific organisations in some way (Cucu et al., 2019). Although some solutions can be put into practice relatively quickly, it has been observed that the time required to implement most Cyber-AI solutions at an organisational level negatively affects their adoption. This delay can be attributed to the inherent complexity of modern AI itself, and even the simplest AI solution may take months or even years to fully implement within an organisation (Attaran & Deb, 2018). This extended implementation period is mainly due to hardware restructuring, acquiring the necessary data for training and testing the models, and allowing sufficient time for the models to comprehend and learn the unique networking and behavioural patterns specific to the organisation (Kaplan & Haenlein, 2019).

Besides the long implementation time, it was discovered that implementing Cyber-AI presents a challenge due to its multidisciplinary nature, requiring a range of specialised professionals such as data scientists, data analysts, AI experts, machine learning specialists, developers, cybersecurity specialists, and project managers, each with different levels of technical expertise (Attaran & Deb, 2018).Arasada (Arasada, 2021) also notes that this extensive requirement for skilled personnel poses a difficulty for organisations, given the current shortage of qualified and experienced professionals in these specialised fields who can effectively implement and manage cyber-AI solutions at an organisational level. Moreover, organisations often face significant financial burdens in recruiting these scarce professionals (Attaran & Deb, 2018; Dawson, 2021; Lim, 2022). On the other hand, the introduction of cyber-AI solutions brings automation to the organisation, which threatens many cyber-related jobs due to its ability to offer faster, more accurate, and reliable cybersecurity solutions (Lim, 2022). Although it is unlikely that AI will completely replace the need for human employees, (Kaplan & Haenlein, 2019) explains that its introduction to the cybersecurity domain alone poses a threat to certain roles, jobs, and tasks related to cybersecurity, as they may become obsolete with the implementation of cyber-AI solutions.

Exploiting AI systems gives hackers the autonomy to utilise AI-based attacks that can evade AI-based protective measures (AL-Dosari et al., 2022; Tetaly & Kulkarni, 2022), potentially resulting in privacy breaches. These AI-driven attacks have the capability to evolve faster than the protective tools themselves, thanks to a technique called neural fuzzing. Neural fuzzing employs neural networks to identify vulnerabilities in target systems, allowing attackers to learn from existing AI protective tools (Agrawal et al., 2023; Zhan, 2021). The unreliability of generative AI is also a concern in some organisations due to the high number of false positives.

3.1.3. How does the use of AI differ from traditional, non-AI-driven means of organisational cyber security?

To fully gauge the impact of AI on organisational cyber security, it was determined that a comparison needed to be made between traditional cyber security approaches and AI-driven approaches. Whilst there is limited literature that directly explores the difference between AI and traditional, non-AI driven means of cyber protection, it was found that in addition, a traditional reactive approach to cyber security, where the aim is to wait for an attack and then neutralise it, AI enables a proactive approach to not only reacting but anticipating and dealing with a breach (Raimundo & Rosário, 2021). This is made possible through AI-driven threat intelligence and prediction that can learn from past experiences and data available to recognise anomalous behaviours (Zhan, 2021). AI methods have demonstrated superior performance in contrast to alternative methods, as evidenced by several studies (Diallo & Patras, 2021; Haider et al., 2020; Massaro et al., 2020). In the conducted experiments, AI solutions have consistently outperformed other approaches in intrusion detection (Keshk et al., 2023; Selçuk, 2019) due to their enhanced precision (Mogollón-Gutiérrez et al., 2023; The et al., 2023) and heightened security capabilities (Agrawal et al., 2023; Jadav et al., 2023).

However, compared to traditional approaches, the interrelated

nature of AI with other protective components is seen to bring about additional, non-traditional vulnerabilities in the security chain (Angelopoulos et al., 2019). According to Mohammed (Mohammed, 2020), if any interrelated component of an AI system is compromised, it is likely that the entire system will be compromised. For example, if the training data sets used to train the models are compromised, it may affect the outcome of the 'learning results', and thus, the entire model may not perform as intended. Therefore, although AI provides greater protection, AI systems require increased protection throughout the security development lifecycle as opposed to traditional approaches (Hariyanti et al., 2021).

Additionally, it was found that the difference between these two approaches also stems from the fact that there is no one-size-fits-all solution like traditional firewalls, anti-virus software or antimalware software (Cucu et al., 2019). Each AI solution must be tailored to a specific organisation using organisational-specific internal and external data (Raimundo & Rosário, 2021). This requires not only a greater financial and manpower commitment but also a greater hardware and infrastructure commitment to implement compared to traditional approaches. It was evident that whilst traditional network security tools such as firewalls and anti-virus software are universal, they are seen today as border-based protection (Zhan, 2021). AI-driven network analysis systems (NAS) have substituted these traditional network protection mechanisms as it is simply much faster and more efficient compared to the traditional approaches (Aliyari, 2021).

Lastly, the implementation of AI solutions at an organisational level is subject to stricter laws and regulations as compared to traditional cyber security approaches. Whilst AI is mainly used for defensive purposes in organisational cyber security, certain governments and regulatory bodies have regulated high-risk AI applications to ensure the responsible use of such a powerful technology (Rawindaran et al., 2021).

3.2. Limitations of the study

This study provides valuable insights into AI's impact on organisational cybersecurity, but it has limitations. It takes a broad view of Cyber-AI's influence on organisations, overlooking variations among organisation types, sizes, sectors, and regions, which can yield different effects. It doesn't delve into specific AI tools, limiting our understanding of their diverse impacts. Time constraints restricted the literature search to four databases, potentially excluding relevant materials from other sources. Additionally, the inclusion/exclusion criteria narrowed down the selection of pertinent literature, focusing on English publications between 2018 and 2023.

3.3. Recommendations for future research

This study concentrated on examining how AI influences organisational cybersecurity. Future research endeavours may direct attention toward investigating the specific impact of AI on distinct types of institutions, such as those in financial, manufacturing, healthcare, educational, critical infrastructure, and government sectors. A more targeted exploration of these areas could yield deeper insights, aiding in the optimal utilisation of AI for enhanced cybersecurity. Additionally, it would facilitate the development of measures to mitigate potential malicious exploits where AI tools are employed with harmful intentions, specifically targeting certain institutions. Comparative analyses could also be conducted to evaluate the effects of AI usage on cybersecurity within organisational types in specific countries. Furthermore, forthcoming studies might dissect the impact of AI on cybersecurity, examining its repercussions on the confidentiality, integrity, and availability of information within organisations.

It's worth noting that most of the existing literature in this field has concentrated on large, well-established organisations, so there is a need for more attention on small and medium-sized enterprises (SMEs). Furthermore, the impacts of AI on cybersecurity identified in this review are broad and not specific to any AI-powered cybersecurity solution. Therefore, future research could explore the effects of specific AI solutions and tools on an organisation's cybersecurity.

Cucu (Cucu et al., 2019) reports a significant rise in sophisticated cyber-attacks, prompting the adoption of AI algorithms for detecting unusual behaviour and analysing extensive data sets. This shift poses a challenge to static, non-AI approaches, urging the adaptation of existing technologies to address evolving threats. Prospective research ought to examine the effectiveness of AI-driven and unconventional AI approaches in cybersecurity. It is crucial to explore how non-AI methods can be adjusted to address upcoming cybersecurity threats. Additionally, emphasis should be placed on incorporating the human factor, as certain attacks may still occur due to human error or insufficient awareness of specific threats (AL-Hawamleh, 2023).

When artificial intelligence is employed to compromise organizational cybersecurity, it can lead to significant financial losses. Further research could explore the financial implications of AI on organisational cybersecurity, particularly focusing on the impact of cyber-attacks that result in data losses. This investigation would aim to determine the recovery period and the associated costs involved in recovering from such security breaches.

Given the absence of standardized regulations for AI utilisation across countries, prospective research can delve into diverse legal frameworks that effectively oversee the application of AI in cybersecurity within different nations. These studies have the potential to mitigate the risk of malicious AI usage in organisations by contributing to the establishment of more comprehensive and effective regulatory measures.

One prevalent issue associated with machine learning models is their dependence on precise datasets for making accurate predictions. Consequently, there is a need for research to develop improved approaches for identifying errors in datasets (Wazid et al., 2022).

The existing literature highlights a growing interest in employing artificial intelligence (AI) for cybersecurity, sparking ongoing discussions about the efficacy of AI methods in fortifying cybersecurity across various domains. Particularly, research emphasis has been placed on utilizing AI for intrusion detection (Maia et al., 2022; Redino et al., 2022; Sivamohan & Sridhar, 2023; Sowmya & Mary Anita, 2023; Sowmya and Mary Anita, 2023, 2023), as well as for enhancing protection and identifying malware (Al-Khshali & Ilyas, 2023; Kumar et al., 2022; Ullah et al., 2022). Earlier studies also delved into the potential exploitation of AI systems and their utilisation in launching adversarial attacks (AL-Dosari et al., 2022; Fritsch et al., 2022; Tetaly & Kulkarni, 2022; Truong et al., 2020). Given the dual nature of AI—capable of being used for both positive and malicious purposes—there is a need to scrutinise governance issues concerning the use of AI for cybersecurity within organisations. Future research endeavours should delve into these governance aspects and their implications.

4. Conclusion

As technology adoption within organisations grows, the occurrence of cyber threats and attacks also rises. Existing literature indicates a pressing requirement for enhanced and secure methods of organisational cyber security using AI-driven solutions to safeguard against constantly evolving threats. Hence, the objective of this research was to assess the overall influence of AI-driven solutions on organisational cyber security. This study examined the advantages and disadvantages of implementing AI-based cyber solutions in organisations and compared their effectiveness to conventional cyber security approaches.

Through this literature review, it was discovered that the utilisation of AI-powered solutions affects the cyber security of organisations throughout the entire security life cycle. On the positive side, AI contributes to organisational cyber security by automating processes, analysing, and predicting threats, improving hardware and infrastructure

security, managing vulnerabilities, aiding decision-making, and overall enhancing the robustness and resilience of system security. Conversely, there are negative implications of AI on organisational cyber security. These include significant data requirements, the need for skilled professionals, hardware and infrastructure demands, challenges in implementation, and the potential threat it poses to cybersecurity-related job positions. Additionally, since hackers themselves utilise AI for attacks, certain attacks have become resistant to AI-based protective measures. While AI enables a proactive approach to cyber security, it also introduces additional vulnerabilities that need to be considered before implementing it at an organisational level. Factors such as the absence of universal AI-based solutions and the need for stricter regulations compared to traditional cybersecurity approaches should be considered.

In summary, despite some disadvantages, incorporating AI solutions into organisational cybersecurity has a predominantly beneficial effect. Essentially, AI usage offers an effective, advanced, and heightened level of cyber protection. This outcome theoretically establishes a foundation for future studies, which can delve into specific factors like organisational size and type and assess the impact of AI. From a practical standpoint, these findings can assist organisations in making better-informed choices regarding AI solutions by providing an unbiased evaluation of the associated impacts.

Declaration of generative AI in scientific writing

During the preparation of this work, the author(s) used ChatGPT to improve the readability, Grammar and conciseness of certain parts of the article. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

APPENDIX A

Findings to
Q1: What is the positive impact of AI on cyber security from an organisational perspective?
Q2 What is the negative impact of AI on cyber security from an organisational perspective?

Authors	Year	Type of Study	Finding positive/negative impact of AI	Document Type
Gupta S.; Sabitha A.S.; Punhani R.	2019	Qualitative	AI will be able to offer solutions that automate the detection of external threats in a machine-readable format, enhancing data precision and efficiency within the distinctive framework of each intelligent organisation.	Article
Haider A.; Khan M.A.; Rehman A.; Ur Rahman M.; Kim H.S.	2020	Experiment	A Real-Time Sequential Deep Extreme Learning Machine-based intrusion detection model outperforms traditional intrusion detection algorithms. However, a smart intrusion detection system fuelled by data can leverage the capabilities of artificial intelligence (AI), with a particular focus on machine learning (ML) methodologies.	Article
Massaro A.; Gargaro M.; Dipierro G.; Galiano A.M.; Buonopane S.	2020	Experiment	AI techniques have the potential to enhance cybersecurity by preventing cyberattacks. The XGBoost-based AI algorithms are the most effective and precise approach for thwarting cyberattacks as they have a remarkable capability to categorise and recognise distinctive patterns within the most significant traffic log variables.	Article
Thapa N.; Liu Z.; Kc D.B.; Gokaraju B.; Roy K.	2020	Experiment	Machine learning (ML) and deep learning (DL) approaches complement each other effectively in creating a robust network intrusion detection system.	Article
Macas M.; Wu C.	2020	Qualitative	AI and deep learning represent crucial methods for bolstering cybersecurity. Deep learning approaches have proven to be effective in the realm of network intrusion detection.	Conference paper
Mhlanga D.	2020	Qualitative	AI systems are employed to defend financial institutions from cybersecurity threats and also shape wealth management by utilizing bot advisors to offer automated financial planning services such as tax planning, insurance guidance, health advice, and investment recommendations.	Article
Truong T.C.; Diep Q.B.; Zelinka I.	2020	Qualitative	Artificial intelligence has the potential to create more robust security defense systems for safeguarding the organization, but it can also be harnessed by malicious entities to inflict greater damage.	Article
Zeadally S.; Adi E.; Baig Z.; Khan I.A.	2020	Qualitative	Artificial intelligence and cryptography hold great potential in the realm of cybersecurity administration. Specifically, machine learning within AI can enhance an organization's capacity to identify system breaches. Nevertheless, AI methodologies can also be exploited to compromise passwords. Additionally, the presence of spam and malware bots can have detrimental effects on network operations.	Article
Angelopoulos, Angelos; Michailidis, Emmanouel T.; Nomikos, Nikolaos; Trakadas, Panagiotis; Hatziefremidis, Antonis; Voliotis, Stamatis; Zahariadis, Theodore	2020	Qualitative	In IIoT, increased connectivity heightens cybersecurity risks, including threats like Stuxnet. Machine learning offers three key defenses: fault detection, issue prediction, and cyberattack prevention.	Article
Diallo A.F.; Patras P.	2021	Experiment	Artificial intelligence encounters fresh cybersecurity challenges as network traffic volumes surge. The AI-based ACID (Adaptive Clustering-based Intrusion Detection) model outperformed other	Conference paper

(continued on next page)

(*continued*)

Authors	Year	Type of Study	Finding positive/negative impact of AI	Document Type
			state-of-the-art clustering techniques and network intrusion detection methods regarding accuracy and efficiency.	
Ogundokun R.O.; Awotunde J.B.; Sadiku P.; Adeniyi E.A.; Abiodun M.; Dauda O.I.	2021	Experiment	Machine learning techniques strenghts vary when it comes to ensuring cyber security.K-Nearest Neighbor (PSO + KNN) is better than PSO + Decision Tree (PSO + DT)	Conference paper
Patil S.; Varadarajan V.; Walimbe D.; Gulechha S.; Shenoy S.; Raina A.; Kotecha K.	2021	Experiment	Machine learning methods used to identify malware are susceptible to adversarial attacks and exhibit a degree of fragility. While ensemble methods prove effective in malware detection, it is advisable to incorporate adversarial training for enhanced robustness.	Article
Ariffin N.H.M.; Maskat R.	2021	Qualitative	AI offers new prospects for cybersecurity organisations prioritizing cognitive intelligence or IQ-related AI skills, highlighting its industry-transforming impact.	Article
Ghandour A.	2021	Qualitative	Artificial Intelligence, specifically using Deep Learning (DL) and Machine Learning (ML), is crucial in enhancing cybersecurity by focusing on secure transaction processing and actively identifying and thwarting financial fraud. However, it could lead to privacy breaches.	Article
Kaymakci C.; Wenninger S.; Sauer A.	2021	Qualitative	Unsupervised AI models like LSTM-based Autoencoders (AE) are a superior choice for industrial companies detecting malicious energy consumption anomalies compared to traditional non-AI methods.	Conference paper
Musbahi O.; Syed L.; Le Feuvre P.; Cobb J.; Jones G.	2021	Qualitative	The use of AI in healthcare organisations raises concerns about cybersecurity	Article
Raimundo, Ricardo; Rosário, Albérico	2021	Qualitative	AI has evolved to implement a multi-stage strategy in cybersecurity, where it's used across the entire security process, enhancing reliability and trustworthiness, especially in E-Commerce applications, including digital signatures and cryptography.	Article
Dawson, Maurice	2021	Qualitative	AI provides a competitive advantage for organisations, but a shortage of skilled AI, data science, and cybersecurity professionals poses a significant implementation challenge, especially when combining these fields. The automation enabled by AI in cybersecurity is eliminating some jobs, raising workforce concerns. However, there has been a 10% increase in organisations adopting cyber-AI solutions post-COVID-19.	Article
Aliyari, M.	2021	Qualitative	AI is used to recover data after cyberattacks, and machine learning helps enhance information security by allowing self-aware machines to independently monitor system health and make predictions.	Article
Li, Guangjun; Sharma, Preetpal; Pan, Lei; Rajasegarar, Sutharshan; Karmakar, Chandan; Patterson, Nicholas	2021	Qualitative & Quantitative	Deep learning surpasses traditional machine learning by efficiently handling unstructured data, but it requires more training time, resulting in superior accuracy.	Article
Alhayani, Bilal; Jasim Mohammed, Husam; Zeghaiton Chaloob, Ibrahim; Saleh Ahmed, Jehan	2021	Quantitative	AI technologies, including neural networks, intelligent agents, and expert systems, are vital for enhancing information security and reducing the impact of cyberattacks in organizational and government cybersecurity initiatives.	Article
Rawindaran, Nisha; Jayal, Ambikesh; Link to external site, this link will open in a new window; Prakash, Edmond	2021	Quantitative & Qualitative	Laws such as GDPR and ISO standards, along with factors like BREXIT, significantly impact the integration of machine learning solutions in organisations. The adoption of machine learning for cybersecurity in SMEs is hindered by cost factors, while their vulnerability to cyberattacks is rising due to limited expertise and funding.	Article
Chakraborty T.; Mitra S.; Mittal S.; Young M.	2022	Qualitative	The AI-Adaptive-PoW framework safeguards the client-server architecture against DDoS attacks.	Article
Ahamed F.; Farid F.; Suleiman B.; Jan Z.; Wahsheh L.A.; Shahrestani S.	2022	Experiment	AI-based multimodal biometric authentication outperforms traditional single-modal methods with higher accuracy and lower error rates.	Article
Brison R.; Wimmer H.; Rebman C.M., Jr.	2022	Experiment	The progress in AI has led to a rise in cybersecurity attacks carried out by botnets in recent times, underscoring its impact on the threat landscape.	Article
Catak F.O.; Kuzlu M.; Catak E.; Cali U.; Guler O.	2022	Experiment	The mitigation approach can protect DL-based channel estimation models from adversarial attacks within NextG networks.	Article
Ha D.T.; Hoang N.X.; Hoang N.V.; Du N.H.; Huong T.T.; Tran K.P.	2022	Experiment	An explainable artificial intelligence solution is an enhancer in assisting industrial anomaly detection	Conference paper
Le T.-T.-H.; Kim H.; Kang H.; Kim H.	2022	Experiment	Interpreting outcomes from some DNNs is challenging, but a combined AI approach with Decision Trees, Random Forests, Explainable AI, and SHAP effectively clarifies results. This could help experts to quickly refine and validate their judgments because the outcomes are much clearer.	Article
Lu Z.; Thing V.L.L.	2022	Experiment	AI methods often lack clear predictive explanations, posing risks to lives and assets. However, PhilaeX, an AI model using heuristics, outperforms models like LIME and SHAP in explaining various classifiers.	Conference paper
Lu Z.; Thing V.L.L.	2022	Experiment	Various AI models have shortcomings in terms of their ability to provide explanations in adversarial malware detection	Conference paper

(*continued on next page*)

(*continued*)

Authors	Year	Type of Study	Finding positive/negative impact of AI	Document Type
Maia E.; Sousa N.; Oliveira N.; Wannous S.; Sousa O.; Praça I.	2022	Experiment	SMS-I's AI-powered Intelligent Dashboard helps leaders thoroughly analyze breaches and asset compromises, providing proactive threat insights for effective network protection.	Article
Muller N.M.; Pizzi K.; Williams J.	2022	Experiment	AI techniques has some weaknesses when it comes to the detection of audio deepfakes.	Conference paper
Redino C.; Nandakumar D.; Schiller R.; Choi K.; Rahman A.; Bowen E.; Shaha A.; Nehila J.; Weeks M.	2022	Experiment	Deep learning techniques are effective in detecting cyber anomalies	Conference paper
Shroff J.; Walambe R.; Singh S.K.; Kotecha K.	2022	Experiment	Cyber attackers are now using advanced AI tools, like generative models, to create synthetic attacks that can trick conventional detection methods. Additionally, there's a shortage of well-developed and trained models capable of effectively detecting both standard Distributed Denial of Service (DDoS) attacks and adversarial attacks.	Article
Ullah F.; Alsirhani A.; Alshahrani M.M.; Alomari A.; Naeem H.; Shah S.A.	2022	Experiment	AI ensemble models are effective,accurate in malware detection and classification.	Article
Alalwan J.A.A.	2022	Qualitative	AI-based cybersecurity has negative effects spanning regulations, ethics, trust, bias, data quality, workforce, and costs.	Article
AL-Dosari K.; Fetais N.; Kucukvar M.	2022	Qualitative	AAI enhances cybersecurity but can be exploited, posing a security risk in banking as AI tools have vulnerabilities.	Article
Capuano N.; Fenza G.; Loia V.; Stanzione C.	2022	Qualitative	Explainability of AI could result in improving cybersecurity practices whilst leaving the system vulnerable to attacks	Article
Chaithanya B.N.; Brahmananda S.H.	2022	Qualitative	Utilizing AI-based methods for safeguarding organizational data can proactively avert potential future ransomware attacks.	Article
Dias T.; Oliveira N.; Sousa N.; Praça I.; Sousa O.	2022	Qualitative	Hybrid model Artificial intelligence methods provide better and more long-lasting security.	Conference paper
Fritsch L.; Jaber A.; Yazidi A.	2022	Qualitative	Artificial intelligence and machine learning methods are gaining popularity in cyberattacks due to their effectiveness in concealing malicious software.	Conference paper
Kant D.; Johannsen A.	2022	Qualitative	AI offers critical security capabilities such as data protection, fraud detection, malware and intrusion detection, risk assessment in networks, user/machine behavior analysis, and security automation in SMEs. Nonetheless, AI can also be employed for more effective cyberattacks.	Conference paper
Martin T.	2022	Qualitative	There is a lack of collaboration between AI machines and humans due to lack of explainability among other reasons.	Article
Sewak M.; Sahay S.K.; Rathore H.	2022	Qualitative	Deep reinforcement learning is being applied in a variety of ways, enabling numerous innovative uses within the realm of threat defense.	Conference paper
Tetaly M.; Kulkarni P.	2022	Qualitative	The manipulation or theft of data is possible when AI is employed for routine tasks, as they can be vulnerable to hacking	Conference paper
Trim P.R.J.; Lee Y.-I.	2022	Qualitative	Machine learning and artificial intelligence enhance the way cybersecurity is administered within an enterprise.	Article
Sun, Hongbin; Bai, Shizhen	2022	Qualitative	AI enhances organizational data security through customized strategies using AI-powered Information Security Management Platforms (ISMPs) and improves precision by utilizing enterprise-specific data for training. This AI-driven approach reduces human labor, saves time, and enhances overall security. Nevertheless, the adoption of AI systems may face challenges due to the dependence on high-quality data.	Article
Binny, Naik; Ashir, Mehta; Hiteshri, Yagnik; Manan, Shah	2022	Qualitative	Fuzzy neural networks, a form of machine learning, have the potential to develop a robust cybersecurity system for Industry 4.0	Article
Lim, Ernest	2022	Qualitative	A shortage of in-house cyber-AI skills leads organisations to turn to external AI solutions, which can present difficulties. Unattended AI systems, lacking internal control, may result in unforeseen financial setbacks. Despite their apparent self-sufficiency, unsupervised AI demands guidance to match an organization's objectives.	Article
Kumar, Rajesh; Sharma, Siddharth; Vachhani, Chirag; Yadav, Nitish	2022	Quantitative	Artificial intelligence has resulted in a higher prevalence of machine learning in the realm of malware examination and the identification of network irregularities.	Article
Agrawal V.; Hazratifard M.; Elmiligi H.; Gebali F.	2023	Experiment	AI-based technologies provide improved security and user convenience for authentication compared to facial recognition biometrics.	Article
Al-Khshali H.H.; Ilyas M.	2023	Experiment	Utilizing AI-driven techniques to distinguish between benign and malicious files demonstrated the superior accuracy of the AI approach in yielding results.	Article
Bhandari G.; Lyth A.; Shalaginov A.; Grønli T.-M.	2023	Experiment	The use of AI-ML methods significantly enhances the precision and efficiency of detecting malware attacks in smart environments.	Article
Jadav D.; Jadav N.K.; Gupta R.; Tanwar S.; Alfarraj O.; Tolba A.; Raboaca M.S.; Marina V.	2023	Experiment	AI and Blockchain techniques surpass traditional methods in safeguarding patient data with greater accuracy.	Article
Jo J.; Cho J.; Moon J.	2023	Experiment	Explainable AI models are most effective in malware detection	Article
Joseph O.; Elmalech A.; Hajaj C.	2023	Experiment	ML algorithms can detect various types of cyberattacks(Parallel Covert Data Transmission Channels in Video Conferencing) using statiscal models.	Article

(*continued on next page*)

(*continued*)

Authors	Year	Type of Study	Finding positive/negative impact of AI	Document Type
Keshk M.; Koroniotis N.; Pham N.; Moustafa N.; Turnbull B.; Zomaya A.Y.	2023	Experiment	An explainable deep learning Intrusion detection framework in the Internet of Things networks succeeds in detecting cyberattacks with accuracy and efficiency and outperforms similar techniques	Article
Mogollón-Gutiérrez Ó.; Núñez J.C.S.; Vegas M.Á.; Lindo A.C.	2023	Experiment	Ensemble models in AI demonstrate superior accuracy and effectiveness when analyzing network traffic compared to other cutting-edge techniques.	Article
Nagy N.; Aljabri M.; Shaahid A.; Ahmed A.A.; Alnasser F.; Almakramy L.; Alhadab M.; Alfaddagh S.	2023	Experiment	Artificial intelligence (AI)-based techniques such as machine learning (ML) and deep learning (DL) have proven to be effective in detecting phishing attacks. However, Sequential machine learning techniques are time-consuming and not effective in the timely detection of phishing scams.	Article
Ndichu S.; Ban T.; Takahashi T.; Inoue D.	2023	Experiment	Ensemble AI techniques are more effective in intrusion analysis with the low rates of false positives.	Article
Ozturk O.S.; Ekmekcioglu E.; Cetin O.; Arief B.; Hernandez-Castro J.	2023	Experiment	AI models, including static code analysers like ChatGPT, have their constraints, particularly in vulnerability assessments where they tend to produce more false positives. Nevertheless, they possess significantly more potential compared to conventional static code analysers.	Conference paper
Pearce H.; Tan B.; Ahmad B.; Karri R.; Dolan-Gavitt B.	2023	Experiment	AI-based models seem promising at repairing cybersecurity bugs in a code; however these models need to be evaluated and refined for effectiveness	Conference paper
Prazeres N.; Costa R.L.D.C.; Santos L.; Rabadão C.	2023	Experiment	Machine learning-based solutions have high potential for cybersecurity, but there are still challenges related to training and generalisation, which may impose constraints on the architecture.	Article
Reilly C.; O'Shaughnessy S.; Thorpe C.	2023	Experiment	Deep learning techniques for malware detection are susceptible to adversarial attacks, which also undermine image based classification. However, the training of deep learning models with generative adversarial network-generated data improves their robustness to adversarial attacks.	Conference paper
Sharma Y.; Birnbach S.; Martinovic I.	2023	Experiment	Machine learning and network analysis methods have demonstrated significant shortcomings due to their perceived monolithic nature and lack of interpretability, rendering the explanation of network analysis and malware detection challenging.	Conference paper
Sivamohan S.; Sridhar S.S.	2023	Experiment	Ensemble AI methods, such as the Bidirectional Long Short-Term Memory Explainable Artificial Intelligence framework (BiLSTM-XAI), have demonstrated significantly improved accuracy in detecting intrusions.	Article
Thi T.-T.T.; Luong D.-T.; Nguyen H.-D.; Hoang T.-M.	2023	Experiment	Ensemble AI models that incorporate deep neural networks and heuristic algorithms enhance the accuracy of intrusion detection.	Article
AL-Hawamleh A.M.	2023	Qualitative	The utilisation of two-factor authentication, backend security measures, and the application of artificial intelligence can effectively deter hacking attempts.	Article
Kaur R.; Gabrijelčič D.; Klobučar T.	2023	Qualitative	AI boosts cybersecurity by automating tasks, speeding up threat detection and response, and enhancing precision to strengthen defenses against various security threats and cyberattacks.	Article
Krichen M.	2023	Qualitative	Artificial intelligence can enhance security and reliability by effectively countering attacks on smart contracts.	Article
Krishnan P.; Jain K.; Aldweesh A.; Prabu P.; Buyya R.	2023	Qualitative	A data streaming analytics framework with machine learning for anomaly detection outperforms prior SDN-based open stack solutions.	Article
Ma K.W.F.; Dhot T.; Raza M.	2023	Qualitative	Artificial intelligence techniques have the potential to assist in identifying, thwarting, and controlling cybersecurity risks, and they can also be harnessed for the mitigation of Authorized Push Payment fraud.	Article
Sowmya T.; Mary Anita E.A.	2023	Qualitative	AI-based intrusion detection techniques improve accuracy and attack classification	Article

APPENDIX B

Findings to Q3: How does the use of AI differ from traditional, non-AI-driven means of organisational cyber security?

Authors	Year	How does AI use differ from traditional means
Haider A.; Khan M.A.; Rehman A.; Ur Rahman M.; Kim H.S.	2020	A Real-Time Sequential Deep Extreme Learning Machine-based intrusion detection model outperforms traditional intrusion detection algorithms.
Diallo A.F.; Patras P.	2021	The AI-based ACID (Adaptive Clustering-based Intrusion Detection model outperformed other state-of-the-art clustering techniques and network intrusion detection methods regarding accuracy and efficiency.

(*continued on next page*)

(*continued*)

Authors	Year	How does AI use differ from traditional means
Patil S.; Varadarajan V.; Walimbe D.; Gulechha S.; Shenoy S.; Raina A.; Kotecha K.	2021	Ensemble methods prove effective in malware detection
Kaymakci C.; Wenninger S.; Sauer A.	2021	Unsupervised AI models like LSTM-based Autoencoders (AE) are a superior choice for industrial companies detecting malicious energy consumption anomalies compared to traditional non-AI methods.
Li, Guangjun; Sharma, Preetpal; Pan, Lei; Rajasegarar, Sutharshan; Karmakar, Chandan; Patterson, Nicholas	2021	Deep learning surpasses traditional machine learning by efficiently handling unstructured data, but it requires more training time, resulting in superior accuracy.
Le T.-T.-H.; Kim H.; Kang H.; Kim H.	2022	Interpreting outcomes from some DNNs is challenging, but combining AI with Decision Trees, Random Forests, Explainable AI, and SHAP effectively clarifies results.
Shroff J.; Walambe R.; Singh S.K.; Kotecha K.	2022	Advanced AI tools used to trick conventional detection models
Agrawal V.; Hazratifard M.; Elmiligi H.; Gebali F.	2023	AI-based technologies provide improved security and user convenience for authentication compared to facial recognition biometrics.
Jadav D.; Jadav N.K.; Gupta R.; Tanwar S.; Alfarraj O.; Tolba A.; Raboaca M.S.; Marina V.	2023	AI and Blockchain techniques surpass traditional methods in safeguarding patient data with greater accuracy.
Keshk M.; Koroniotis N.; Pham N.; Moustafa N.; Turnbull B.; Zomaya A.Y.	2023	An explainable deep learning Intrusion detection framework in the Internet of Things networks succeeds in detecting cyberattacks with accuracy and efficiency and outperforms similar techniques
Mogollón-Gutiérrez Ó.; Núñez J.C.S.; Vegas M.Á.; Lindo A.C.	2023	Ensemble models in AI demonstrate superior accuracy and effectiveness when analyzing network traffic compared to other cutting-edge techniques.
Ozturk O.S.; Ekmekcioglu E.; Cetin O.; Arief B.; Hernandez-Castro J.	2023	AI models, including static code analyzers like ChatGPT, have their constraints, particularly in vulnerability assessments where they tend to produce more false positives. Nevertheless, they possess significantly more potential compared to conventional static code analyzers.
Sivamohan S.; Sridhar S.S.	2023	Ensemble AI methods, such as the Bidirectional Long Short-Term Memory Explainable Artificial Intelligence framework (BiLSTM-XAI), have demonstrated significantly improved accuracy in detecting intrusions.
Thi T.-T.T.; Luong D.-T.; Nguyen H.-D.; Hoang T.-M.	2023	Ensemble AI models that incorporate deep neural networks and heuristic algorithms enhance the accuracy of intrusion detection.
Krishnan P.; Jain K.; Aldweesh A.; Prabu P.; Buyya R.	2023	A data streaming analytics framework with machine learning for anomaly detection outperforms prior SDN-based open stack solutions.

References

Abbas, N. N., Ahmed, T., Shah, S. H. U., Omar, M., & Park, H. W. (2019). Investigating the applications of artificial intelligence in cyber security. *Scientometrics, 121*(2), 1189–1211.

Agrawal, V., Hazratifard, M., Elmiligi, H., & Gebali, F. (2023). Electrocardiogram (ECG)-Based user Authentication using deep learning algorithms. *Diagnostics, 13*(3). https://doi.org/10.3390/diagnostics13030439

Ahamed, F., Farid, F., Suleiman, B., Jan, Z., Wahsheh, L. A., & Shahrestani, S. (2022). An intelligent Multimodal Biometric Authentication model for Personalised healthcare services. *Future Internet, 14*(8). https://doi.org/10.3390/fi14080222

AL-Dosari, K., Fetais, N., & Kucukvar, M. (2022). *Artificial intelligence and cyber defense system for Banking Industry: A qualitative study of AI applications and challenges. Cybernetics and systems*. https://doi.org/10.1080/01969722.2022.2112539

AL-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. *International Journal of Advanced Computer Science and Applications, 14*(2), 801–809. https://doi.org/10.14569/IJACSA.2023.0140292

Al-Khshali, H. H., & Ilyas, M. (2023). Impact of portable executable Header features on malware detection accuracy. *Computers, Materials & Continua, 74*(1), 153–178. https://doi.org/10.32604/cmc.2023.032182

Alalwan, J. A. A. (2022). Roles and challenges of AI-based cybersecurity: A Case study. *Jordan Journal of Business Administration, 18*(3), 437–456. https://doi.org/10.35516/jjba.v18i3.196

Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. *Materials Today: Proceedings*.

Aliyari, M. (2021). Securing Industrial infrastructure against cyber-attacks using machine learning and artificial intelligence at the Age of industry 4.0. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12*(11), 6581–6594.

Almeida, F., Santos, J. D., & Monteiro, J. A. (2020). The challenges and opportunities in the digitalization of companies in a post-COVID-19 World. *IEEE Engineering Management Review, 48*(3), 97–103.

Alom, M. Z., Taha, T. M., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, M. S., … Asari, V. K. (2018). *The history began from alexnet: A comprehensive survey on deep learning approaches*. arXiv preprint arXiv:1803.01164.

Angelopoulos, A., Michailidis, E. T., Nomikos, N., Trakadas, P., Hatziefremidis, A., Voliotis, S., et al. (2019). Tackling faults in the industry 4.0 era—a survey of machine-learning solutions and key aspects. *Sensors, 20*(1), 109.

Arasada, S. (2021). These four challenges in adopting machine learning can lower your ROI and sabotage success. Forbes https://www.forbes.com/sites/forbestechcouncil/2021/08/31/these-four-challenges-in-adopting-machine-learning-can-lower-your-roi-and-sabotage-success/?sh=2818cdf47c4a.

Ariffin, N. H. M., & Maskat, R. (2021). A proposal of ethical competence model for cyber security organization. *Indonesian Journal of Electrical Engineering and Computer Science, 24*(3), 1711–1717. https://doi.org/10.11591/ijeecs.v24.i3.pp1711-1717

Attaran, M., & Deb, P. (2018). Machine learning: The new'big thing'for competitive advantage. *International Journal of Knowledge Engineering and Data Mining, 5*(4), 277–305.

Azungah, T. (2018). Qualitative research: Deductive and inductive approaches to data analysis. *Qualitative Research Journal, 18*(4), 383–400.

Bhandari, G., Lyth, A., Shalaginov, A., & Grønli, T.-M. (2023). Distributed deep neural-network-based middleware for cyber-attacks detection in smart IoT ecosystem: A novel framework and performance evaluation approach. *Electronics (Switzerland), 12*(2). https://doi.org/10.3390/electronics12020298

Brison, R., Wimmer, H., & Rebman, C. M. (2022). Botnet intrusion detection: A modern architecture to defend a virtual private cloud. *Issues in Information Systems, 23*(3), 114–127. https://doi.org/10.48009/3_iis_2022_110

Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in CyberSecurity: A survey. *IEEE Access, 10*, 93575–93600. https://doi.org/10.1109/ACCESS.2022.3204171

Chaithanya, B. N., & Brahmananda, S. H. (2022). AI-Enhanced defense against ransomware within the organization's architecture. *Journal of Cyber Security and Mobility, 11*(4), 621–654. https://doi.org/10.13052/jcsm2245-1439.1146

Chakraborty, T., Mitra, S., Mittal, S., & Young, M. (2022). AI_Adaptive_POW: An AI assisted Proof of Work (POW) framework for DDoS defense. *Software Impacts, 13*. https://doi.org/10.1016/j.simpa.2022.100335

Clarke, V., Braun, V., & Hayfield, N. (2015). Thematic analysis. *Qualitative psychology: A practical guide to research methods, 3*, 222–248.

Creswell, J. W. (2015). *Revisiting mixed methods and advancing scientific practices*.

Cucu, C., Gavrioloaia, G., Bologa, R., & Cazacu, M. (2019). *Current technologies and trends in cybersecurity and the impact of artificial intelligence* (Vol. 2). eLearning & Software for Education.

Dawson, M. (2021). Cybersecurity impacts for artificial intelligence use within industry 4.0. *Scientific Bulletin, 26*(1), 24–31.

De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. *Electronics, 12*(8), 1920. https://doi.org/10.3390/electronics12081920

Diallo, A. F., & Patras, P. (2021). Adaptive clustering-based malicious traffic classification at the network edge. *Proceedings - IEEE INFOCOM, 2021-May*. https://doi.org/10.1109/INFOCOM42981.2021.9488690

Dias, T., Oliveira, N., Sousa, N., Praça, I., & Sousa, O. (2022). A hybrid approach for an interpretable and explainable intrusion detection system. In *Lecture notes in networks and systems, 418 LNNS*. https://doi.org/10.1007/978-3-030-96308-8_96

Drucker, A. M., Fleming, P., & Chan, A. W. (2016). Research techniques made simple: Assessing risk of bias in systematic reviews. *Journal of Investigative Dermatology, 136*(11), e109–e114.

Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H., & Fatima, Z. (2020). *Cyber-attacks in the era of COVID-19 and possible solution domains*.

Fritsch, L., Jaber, A., & Yazidi, A. (2022). An overview of artificial intelligence used in malware. In *Communications in computer and information science, 1650 CCIS*. https://doi.org/10.1007/978-3-031-17030-0_4

Ghandour, A. (2021). Opportunities and challenges of artificial intelligence in banking: Systematic literature review. *TEM Journal, 10*(4), 1581–1587. https://doi.org/10.18421/TEM104-12

Gupta, S., Sabitha, A. S., & Punhani, R. (2019). Cyber security threat intelligence using data mining techniques and artificial intelligence. *International Journal of Recent*

Technology and Engineering, 8(3), 6133–6140. https://doi.org/10.35940/ijrte.C5675.098319
Ha, D. T., Hoang, N. X., Hoang, N. V., Du, N. H., Huong, T. T., & Tran, K. P. (2022). Explainable anomaly detection for industrial control system cybersecurity. *IFAC-PapersOnLine, 55*(10), 1183–1188. https://doi.org/10.1016/j.ifacol.2022.09.550
Haider, A., Khan, M. A., Rehman, A., Ur Rahman, M., & Kim, H. S. (2020). A real-time sequential deep extreme learning machine cybersecurity intrusion detection system. *Computers, Materials & Continua, 66*(2), 1785–1798. https://doi.org/10.32604/cmc.2020.013910
Hansen, E. B., & Bøgh, S. (2021). Artificial intelligence and internet of things in small and medium-sized enterprises: A survey. *Journal of Manufacturing Systems, 58*, 362–372.
Hariyanti, E., Djunaidy, A., & Siahaan, D. (2021). Information security vulnerability prediction based on business process model using machine learning approach. *Computers & Security, 110*, Article 102422.
Hernán, M. A., Hernández-Díaz, S., & Robins, J. M. (2004). A structural approach to selection bias. *Epidemiology*, 615–625.
Huang, M. H., & Rust, R. T. (2018). Artificial intelligence in service. *Journal of Service Research, 21*(2), 155–172.
Jadav, D., Jadav, N. K., Gupta, R., Tanwar, S., Alfarraj, O., Tolba, A., et al. (2023). A trustworthy healthcare management framework using amalgamation of AI and blockchain network. *Mathematics, 11*(3). https://doi.org/10.3390/math11030637
Jo, J., Cho, J., & Moon, J. (2023). A malware detection and extraction method for the related information using the ViT attention mechanism on android operating system. *Applied Sciences, 13*(11). https://doi.org/10.3390/app13116839
National Academies of Sciences. (2019). Engineering, and medicine, intelligence community studies board, computer science and telecommunications board, & division on engineering and physical Sciences. In A. Johnson, & E. Grumbling (Eds.), *Implications of artificial intelligence for cybersecurity: Proceedings of a workshop*. National Academies Press. https://doi.org/10.17226/25488.
Joseph, O., Elmalech, A., & Hajaj, C. (2023). Detecting parallel covert data transmission channels in video conferencing using machine learning. *Electronics (Switzerland), 12*(5). https://doi.org/10.3390/electronics12051091
Joseph, A. D., Laskov, P., Roli, F., Tygar, J. D., & Nelson, B. (2013). Machine learning methods for computer security (Dagstuhl Perspectives Workshop 12371). In *Dagstuhl manifestos (Vol. 3, No. 1). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik*.
Kant, D., & Johannsen, A. (2022). Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs). *IS and T International Symposium on Electronic Imaging Science and Technology, 34*(3). https://doi.org/10.2352/EI.2022.34.3.MOBMU-387
Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons, 62*(1), 15–25.
Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*. https://doi.org/10.1016/j.inffus.2023.101804
Kaymakci, C., Wenninger, S., & Sauer, A. (2021). Energy anomaly detection in industrial applications with long short-term memory-based autoencoders. *Procedia CIRP, 104*, 182–187. https://doi.org/10.1016/j.procir.2021.11.031
Keshk, M., Koroniotis, N., Pham, N., Moustafa, N., Turnbull, B., & Zomaya, A. Y. (2023). *An explainable deep learning-enabled intrusion detection framework in IoT networks* (Vol. 639). Information Sciences. https://doi.org/10.1016/j.ins.2023.119000
Krichen, M. (2023). Strengthening the security of smart contracts through the power of artificial intelligence. *Computers, 12*(5). https://doi.org/10.3390/computers12050107
Krishnan, P., Jain, K., Aldweesh, A., Prabu, P., & Buyya, R. (2023). OpenStackDP: A scalable network security framework for SDN-based OpenStack cloud infrastructure. *Journal of Cloud Computing, 12*(1). https://doi.org/10.1186/s13677-023-00406-w
Kumar, R., Sharma, S., Vachhani, C., & Yadav, N. (2022). What changed in the cyber-security after COVID-19? *Computers & Security, 120*, Article 102821.
Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176–8186.
Lim, E. (2022). B2B artificial intelligence transactions: A framework for assessing commercial liability. *Singapore Journal of Legal Studies*, 46–74.
Lo, C. K. (2020). Systematic reviews on flipped learning in various education contexts. In O. Zawacki-Richter, M. Kerres, S. Bedenlier, M. Bond, & K. Buntins (Eds.), *Systematic reviews in educational research* (pp. pp129–143). Springer.
Lu, Z., & Thing, V. L. L. (2022). *"How does it detect A malicious app?" Explaining the predictions of AI-based malware detector. Proceedings - 2022 IEEE 8th International conference on Big data security on cloud, IEEE International conference on high performance and Smart computing, and IEEE International conference on intelligent data and security* (pp. 194–199). BigDataSecurity/HPSC/IDS 2022. https://doi.org/10.1109/BigDataSecurityHPSCIDS54978, 2022.00045.
Macas, M., & Wu, C. (2020). Review: Deep learning methods for cybersecurity and intrusion detection systems. In *Proceedings - 2020 IEEE Latin-American conference on communications*. https://doi.org/10.1109/LATINCOM50620.2020.9282324. LATINCOM 2020.
Ma, K. W. F., Dhot, T., & Raza, M. (2023). Considerations for using artificial intelligence to manage authorized push payment (APP) scams. In *IEEE engineering management review*. https://doi.org/10.1109/EMR.2023.3288432
Maia, E., Sousa, N., Oliveira, N., Wannous, S., Sousa, O., & Praça, I. (2022). SMS-I: Intelligent security for cyber–physical systems. *Information, 13*(9). https://doi.org/10.3390/info13090403
Malatji, M., Marnewick, A., & von Solms, S. (2018). The impact of artificial intelligence on the human aspects of information and cybersecurity. In *Haisa* (pp. 158–169).
Martin, T. (2021). On the need for collaborative intelligence in cybersecurity. *CEUR Workshop Proceedings, 3125*, 100–112.
Massaro, A., Gargaro, M., Dipierro, G., Galiano, A. M., & Buonopane, S. (2020). Prototype cross-platform oriented on cybersecurity, virtual connectivity, big data and artificial intelligence control. *IEEE Access, 8*, 197939–197954. https://doi.org/10.1109/ACCESS.2020.3034399
Mhlanga, D. (2020). Industry 4.0 in finance: The impact of artificial intelligence (ai) on digital financial inclusion. *International Journal of Financial Studies, 8*(3), 1–14. https://doi.org/10.3390/ijfs8030045
Mogollón-Gutiérrez, Ó., Núñez, J. C. S., Vegas, M.Á., & Lindo, A. C. (2023). A novel ensemble learning system for cyberattack classification. *Intelligent Automation and Soft Computing, 37*(2), 1691–1709. https://doi.org/10.32604/iasc.2023.039255
Mohammed, I. A. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. *Artificial Intelligence, 7*(9).
Muller, N. M., Pizzi, K., & Williams, J. (2022). Human perception of audio deepfakes. In *DDAM 2022 - proceedings of the 1st international workshop on deepfake detection for audio multimedia* (pp. 85–91). https://doi.org/10.1145/3552466.3556531
Musbahi, O., Syed, L., Le Feuvre, P., Cobb, J., & Jones, G. (2021). Public patient views of artificial intelligence in healthcare: A nominal group technique study. *Digital Health, 7*. https://doi.org/10.1177/20552076211063682
Nagy, N., Aljabri, M., Shaahid, A., Ahmed, A. A., Alnasser, F., Almakramy, L., et al. (2023). Phishing URLs detection using sequential and parallel ML techniques: Comparative analysis. *Sensors, 23*(7). https://doi.org/10.3390/s23073467
Naik, B., Mehta, A., Yagnik, H., & Shah, M. (2022). The impacts of artificial intelligence techniques in augmentation of cybersecurity: A comprehensive review. *Complex & Intelligent Systems, 8*(2), 1763–1780.
Ndichu, S., Ban, T., Takahashi, T., & Inoue, D. (2023). AI-assisted security alert data analysis with imbalanced learning methods. *Applied Sciences, 13*(3). https://doi.org/10.3390/app13031977
Ogundokun, R. O., Awotunde, J. B., Sadiku, P., Adeniyi, E. A., Abiodun, M., & Dauda, O. I. (2021). An enhanced intrusion detection system using particle swarm optimization feature extraction technique. *Procedia Computer Science, 193*, 504–512. https://doi.org/10.1016/j.procs.2021.10.052
Okoli, C. (2015). A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems, 37*(43), 879–910.
Ozturk, O. S., Ekmekcioglu, E., Cetin, O., Arief, B., & Hernandez-Castro, J. (2023). New tricks to old codes: Can AI chatbots replace static code analysis tools? *ACM International Conference Proceeding Series, 13*. https://doi.org/10.1145/3590777.3590780. –18.
Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *International Journal of Surgery, 88*, Article 105906.
Patil, S., Varadarajan, V., Walimbe, D., Gulechha, S., Shenoy, S., Raina, A., et al. (2021). Improving the robustness of ai-based malware detection using adversarial machine learning. *Algorithms, 14*(10). https://doi.org/10.3390/a14100297
Pearce, H., Tan, B., Ahmad, B., Karri, R., & Dolan-Gavitt, B. (2023). Examining zero-shot vulnerability repair with large language models. *Proceedings - IEEE Symposium on Security and Privacy*. https://doi.org/10.1109/SP46215.2023.10179420, 2023-May, 2339–2356.
Peel, K. L. (2020). A beginner's guide to applied educational research using thematic analysis. *Practical Assessment, Research and Evaluation, 25*(1), 2.
Prazeres, N., Costa, R. L. D. C., Santos, L., & Rabadão, C. (2023). Engineering the application of machine learning in an IDS based on IoT traffic flow. *Intelligent Systems with Applications, 17*. https://doi.org/10.1016/j.iswa.2023.200189
Qiu, J., Wu, Q., Ding, G., Xu, Y., & Feng, S. (2016). A survey of machine learning for big data processing. *EURASIP Journal on Advances in Signal Processing, 2016*(1), 1–16.
Raimundo, R., & Rosário, A. (2021). The impact of artificial intelligence on data system security: A literature review. *Sensors, 21*(21), 7029.
Rawindaran, N. R., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers, 10*(11), 150.
Redino, C., Nandakumar, D., Schiller, R., Choi, K., Rahman, A., Bowen, E., et al. (2022). Zero day threat detection using graph and flow based security telemetry. *3rd IEEE 2022 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS, 2022*, 655–662. https://doi.org/10.1109/ICCCIS56430.2022.10037596
Reilly, C., O'Shaughnessy, S., & Thorpe, C. (2023). Robustness of image-based malware classification models trained with generative adversarial networks. *ACM International Conference Proceeding Series*, 92–99. https://doi.org/10.1145/3590777.3590792
Scott, J., & Kyobe, M. (2021). Trends in cybersecurity management issues related to human behaviour and machine learning. In *2021 international conference on electrical, computer and energy technologies (ICECET)* (pp. 1–8). IEEE.
Selçuk, A. A. (2019). A guide for systematic reviews: Prisma. *Turkish Archives of otorhinolaryngology, 57*(1), 57.
Sharma, Y., Birnbach, S., & Martinovic, I. (2023). RADAR: A TTP-based extensible, explainable, and effective system for network traffic analysis and malware detection. *ACM International Conference Proceeding Series*, 159–166. https://doi.org/10.1145/3590777.3590804
Shroff, J., Walambe, R., Singh, S. K., & Kotecha, K. (2022). Enhanced security against volumetric DDoS attacks using adversarial machine learning. *Wireless Communications and Mobile Computing, 2022*. https://doi.org/10.1155/2022/5757164
Siddaway, A. P. (2014). What is a systematic literature review and how do I do one? *Political Science*, pp1–13.
Sivamohan, S., & Sridhar, S. S. (2023). An optimized model for network intrusion detection systems in industry 4.0 using XAI based Bi-LSTM framework. *Neural Computing & Applications, 35*(15), 11459–11475. https://doi.org/10.1007/s00521-023-08319-0

Sowmya, T., & Mary Anita, E. A. (2023). A comprehensive review of AI-based intrusion detection system. *Measurement: Sensors, 28*. https://doi.org/10.1016/j.measen.2023.100827

Sun, H., & Bai, S. (2022). *Enterprise information security management using internet of Things combined with artificial intelligence technology*. Computational Intelligence and Neuroscience, 2022.

Tetaly, M., & Kulkarni, P. (2022). Artificial intelligence in cyber security - a threat or a solution. *AIP Conference Proceedings, 2519*. https://doi.org/10.1063/5.0109664

Thapa, N., Liu, Z., Kc, D. B., Gokaraju, B., & Roy, K. (2020). Comparison of machine learning and deep learning models for network intrusion detection systems. *Future Internet, 12*(10), 1–16. https://doi.org/10.3390/fi12100167

The, T.-T. T., Luong, D.-T., Nguyen, H.-D., & Hoang, T.-M. (2023). A study on heuristic algorithms combined with LR on a DNN-based IDS model to detect IoT attacks. *Mendel, 29*(1), 62–70. https://doi.org/10.13164/mendel.2023.1.062

Trim, P. R. J., & Lee, Y.-I. (2022). Combining sociocultural intelligence with artificial intelligence to increase organizational cyber security provision through enhanced resilience. *Big Data and Cognitive Computing, 6*(4). https://doi.org/10.3390/bdcc6040110

Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. *Symmetry, 12*(3). https://doi.org/10.3390/sym12030410

Ullah, F., Alsirhani, A., Alshahrani, M. M., Alomari, A., Naeem, H., & Shah, S. A. (2022). Explainable malware detection system using transformers-based transfer learning and multi-model visual representation. *Sensors, 22*(18). https://doi.org/10.3390/s22186766

Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. In *ICT express* (pp. 313–321). Korean Institute of Communication Sciences. https://doi.org/10.1016/j.icte.2022.04.007. Vol. 8, Issue 3.

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. *IEEE Access, 8*, 146598–146612.

Wilkins, J. (2018). Is artificial intelligence a help or hindrance? *Network Security, 2018*(5), 18–19.

Yu, X., & Guo, H. (2019). A survey on IIoT security. In *2019 IEEE VTS Asia Pacific wireless communications symposium (APWCS)* (pp. 1–5).

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access, 8*, 23817–23837. https://doi.org/10.1109/ACCESS.2020.2968045

Zhan, K. (2021). Design of computer network security defense system based on artificial intelligence and neural network. *Journal of Intelligent and Fuzzy Systems, 113*. https://doi.org/10.3233/JIFS-189794

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., … Choo, K. K. R. (2021). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1–25.