INSTITUTO
UNIVERSITÁRIO
DE LISBOA

The Impact of Artificial Intelligence on the Testing Instrument Industry and its Countermeasures

Qiu Zhili

Master in Business Administration

Supervisors:

PhD Renato Jorge Lopes da Costa, Assistant Professor with Aggregation

ISCTE - Instituto Universitário de Lisboa

MSc António Ângelo Machado Matos Pereira, Invited Lecturer

ISCTE - Instituto Universitário de Lisboa

September 2024

BUSINESS
SCHOOL

Department of Marketing, Strategy and Operations

The Impact of Artificial Intelligence on the Testing Instrument Industry and its Countermeasures

Qiu Zhili

Master in Business Administration

Supervisors:

PhD Renato Jorge Lopes da Costa, Assistant Professor with Aggregation

ISCTE - Instituto Universitário de Lisboa

MSc António Ângelo Machado Matos Pereira, Invited Lecturer

ISCTE - Instituto Universitário de Lisboa

September 2024

Acknowledgement

I am eternally grateful to the supervisors of this PhD work, PhD Renato Jorge Lopes da Costa, and the MSc António Ângelo Machado Matos Pereira, for the time and effort given designing, proposing, evaluate, and correcting this thesis. Their specializations in artificial intelligence and testing instruments are invaluable in helping me navigate through the details of my work.

In addition, I would like to thank my family for their boundless love, support, and patience that they have been providing all the time while I was following this path of learning. Their support has been the driving force that has kept me going throughout the process.

I also acknowledge and thank my friends and all the colleagues who provided me with motivation, ideas, and stimulating discussions that deepened my ideas and views on the materials being discussed.

Extra thanks to ISCTE-IUL's faculty and employees for the knowledge-creating context in which the school facilitates learning and development.

Resumo

Esta revisão sistemática da literatura examina cuidadosamente como a inteligência artificial (IA) impacta grandemente a indústria de instrumentos de teste e as estratégias para mitigar essas repercussões. Ao empregar uma metodologia robusta, a investigação inclui o exame minucioso de bases de dados notáveis como *Scopus* e *Web of Science*. Seguindo o método PRISMA como princípio orientador, os artigos são selecionados e excluídos com precisão. A revisão revela avanços significativos das aplicações de IA em instrumentos de teste, destacando simultaneamente as oportunidades e desafios que essas tecnologias apresentam. O estudo identifica ainda domínios-chave e clusters em IA e instrumentos de teste, como abordagens de aprendizado de máquina, avanços de aprendizado profundo e estruturas de redes neurais. Além disso, fornece informações sobre os principais argumentos dentro do domínio. Os debates discutem principalmente as implicações éticas associadas à IA e a precisão dos instrumentos de teste alimentados por IA, enfatizando a exigência de que os seres humanos tenham supervisão identificada pela análise bibliométrica dos principais autores, revistas proeminentes e pontos geográficos de pesquisa na área. Também identifica as publicações mais citadas, autores influentes e palavras-chave predominantes. Este estudo acrescenta valor ao corpo de conhecimento existente, apresentando uma exploração e avaliação aprofundadas da investigação atual neste domínio. O artigo oferece uma análise extensiva de como a IA afeta a indústria de instrumentos de teste e apresenta caminhos potenciais para exploração futura.

Keywords: Inteligência Artificial, Instrumentos de Teste, Contramedidas, Revisão Sistemática da Literatura

JEL Classification:

M000 Administração de Empresas e Economia Empresarial; Marketing; Contabilidade; Economia do Pessoal: Geral

O330 Mudança Tecnológica: Escolhas e Consequências; Processos de Difusão

Abstract

This systematic literature review carefully examines how artificial intelligence (AI) greatly impacts the testing instrument industry and strategies to mitigate these repercussions. By employing a sturdy methodology, the investigation includes the thorough examination of notable databases such as Scopus and Web of Science. By following the PRISMA method as a guiding principle, papers are selected and excluded with precision. The review unearths significant advancements of AI applications in testing instruments, simultaneously highlighting the opportunities and challenges these technologies present. The study further identifies key domains and clusters in AI and testing instruments, like machine learning approaches, deep learning advancements and neural network frameworks. In addition, it provides insight into pertaining to the key arguments within the domain. The debates primarily discuss the ethical implications associated with AI and the precision of testing instruments powered by AI, emphasizing the requirement for humans to have oversight identified by the bibliometric analysis of leading authors, prominent journals and geographical hotspots of research in the field. It also identifies the most cited publications, influential authors and prevalent keywords. This study adds value to the existing body of knowledge by presenting a thorough exploration and evaluation of the current research in this field. The paper offers an extensive analysis of how AI impacts the testing instrument industry and puts forward potential avenues for future exploration.

Keywords: Artificial Intelligence, Testing Instruments, Countermeasures, Systematic Literature Review.

JEL Classification:

M000 Business Administration and Business Economics; Marketing; Accounting; Personnel Economics: General

O330 Technological Change: Choices and Consequences; Diffusion Processes

Contents

Glossary List

Accountability: The obligation to answer for responsibilities or actions, often associated with ensuring ethical behavior and adherence to standards.

Algorithmic Bias: The systematic and unfair distortion of data or algorithmic systems, leading to discriminatory outcomes.

Artificial Intelligence (AI): The field of computer science focused on creating systems that can perform tasks that typically require human intelligence.

Assurance: The act of giving confidence or certainty regarding the quality or reliability of something.

Bayesian Probability: A mathematical method for calculating the probability of an event based on prior knowledge or beliefs.

Bias Mitigation: Efforts to reduce or eliminate biases in data, algorithms, or decision-making processes.

Bibliometric: The quantitative analysis of publications, often used to evaluate research trends and impact within a particular field.

Cognition: The mental process of acquiring knowledge and understanding through thought, experience, and the senses.

Computation: The process of performing calculations using computers or mathematical algorithms.

Countermeasures: Actions or strategies taken to address or mitigate potential risks, challenges, or limitations.

Data Privacy: The protection of sensitive information from unauthorized access, use, disclosure, disruption, modification, or destruction.

Deep Learning: A subset of machine learning that uses artificial neural networks to learn and make decisions based on data.

Deep Neural Networks: A type of artificial neural network with multiple layers between the input and output layers, allowing for complex pattern recognition and learning.

Diagnostics: The identification of the nature or cause of a particular phenomenon, typically a problem or disease.

Ethical Considerations: The moral principles and values that guide decisions and actions related to the development and use of technology.

Genomics: The branch of molecular biology concerned with the structure, function, evolution, and mapping of genomes.

Information Technology: The use of computers and telecommunications equipment to store, retrieve, transmit, and manipulate data.

Logical Reasoning: The process of using rational thinking to draw conclusions or make decisions based on given premises or evidence.

Machine Learning Models: Mathematical models or algorithms that learn patterns and relationships from data to make predictions or decisions.

Machine Learning: A subset of artificial intelligence that enables systems to learn from data and improve their performance over time without being explicitly programmed.

Natural Language Processing (NLP): The field of artificial intelligence concerned with the interaction between computers and humans through natural language.

Non-Destructive Testing (NDT): A wide group of analysis techniques used in science and technology to evaluate the properties of a material, component, or system without causing damage.

Oversight: The process of supervising or monitoring the actions or operations of a system or organization to ensure compliance with regulations or standards.

Personalized Learning: Educational approaches that tailor instruction, pacing, and content to meet the individual needs of each learner.

Predictive Analysis: The process of using data, statistical algorithms, and machine learning techniques to identify the likelihood of future outcomes based on historical data.

Problem Solving: The process of finding solutions to difficult or complex issues.

Quality Control: The process of ensuring that products or services meet specified standards and customer expectations.

Risk-Based Testing: Testing approaches that prioritize tests based on the level of risk associated with specific features or functionalities.

Test Automation: The use of software to control the execution of tests and the comparison of actual outcomes with predicted outcomes.

Transparency: The quality of being easily understandable and open to scrutiny or evaluation.

1. INTRODUCTION

1.1 Context

The discipline of artificial intelligence (AI) has undergone spectacular advances in evolution for numerous years. It involves concepts in computation, cognition, information technology, which is an emerging area of knowledge. Through their various research projects and development programs, researchers and practitioners in AI have continually been working towards making machines and software intelligent as those of humans abducted in order to be sacrificed'; However, the journey in this essay has been guided by the notable authors and expert scholars.

One such luminary is John McCarthy who coined the phrase “artificial intelligence” in 1956. The work done by McCarthy paved the way for the construction of logical reasoning as well as problem solving based artificial intelligence systems. He wrote “Proposal for the Dartmouth Summer Research Project on Artificial Intelligence” that served as a roadmap of the early research in AI. Additionally, one should mention Alan Turing who is now called ‘the father of computer science’ and laid groundwork for understanding computational intelligence due to his invention called the ‘Turing machine’.

Prominent AI researcher and co-founder of Google Brain, Andrew Ng has had his works featured prominently in the present-day land space of AI. His contributions range from simple machine learning through deep learning, and his online course has revolutionised the global AI studies. For example, the path breaking works of Geoffrey Hinton, Yoshua Bengio, and Yann LeCun on deep learning have completely changed the face of the AI and paved way for improvement especially in aspects of natural language processing, computer vision and so forth.

Quality control and assurance have crucial importance in many industries such as manufacturing, health care, and materials science and include testing instruments industry. These developments include inroads of AI and automation, which it was hugely impacted. Indeed, many researchers and experts in this field seek to exploit possible advantages which AI can bring into test instruments and processes, including higher precision, greater accuracy and credibility. Ronald A. Howard is among the authors that have assisted in the development of the theories in decision making analysis. Through his work in decision analysis and Bayesian probability, Howard has significantly contributed to how organizations decide on quality control procedures and instruments.

In relation to the medical testing field, Dr. Jennifer Doudna's breakthrough research concerning CRISPR-Cas9 gene-editing system has transformed genetic testing. Indeed, her research into state-of-the-art evaluation devices in genomics and genomics diagnostics has not only provided new test gadgets but also raised ethical and legal issues concerning integration of artificial intellect in biomedicine. In addition, the use of AI in NDT is also growing popular among other authors such as Anthony J. Deese and Christopher A. Paul who are working on developing AI-based NDT methods. Their work has led to modern and more advanced material tests that are effective at testing items to be used in different fields like the aerospace, civil engineering among others.

1.2 Research Problem

Integration of artificial intelligence (AI) in domain of testing instruments have presented great chances and challenges this systematic review has demanded clear problem statement and focused research. The purpose of this research is to examine how AI may disrupt the testing instrument market and suggest preventive measures. This review discusses the need to define how AI changed the landscape for test instruments, AI limitations, and methods to handle difficulties that may arise.

There are a number of instruments for testing that are applicable in education, psychology, medical sphere, etc. The incorporation of artificial intelligence (AI) has greatly changed these instruments with a shift towards new parameters and uses. These changes however, entails questions regarding which are these changes and what implications does it present. This systematic literature review is undertaken in order to fill this information gap.

In this review, our primary focus is on addressing pivotal questions, striving to unravel the core issues and gain a comprehensive understanding of the subject matter at hand.

How has AI transformed the functionalities and applications of testing instruments in diverse fields?

What are the challenges and potential drawbacks associated with the integration of AI in testing instruments?

What are the existing countermeasures and strategies to address these challenges and maximize the benefits of AI in testing instruments?

In order to conduct such a study, we will draw reference to relevant literatures, theories, and empirical research that have provided insights into the consequences of AI in the testing instrument sector. Also, we shall review possible approaches suggested through literature as well as experts for maximizing on AI benefits but minimizing its risks. The present study is designed as a systematic literature review that synthesizes contemporary knowledge about it, which eventually, opens way for further studies and practical application.

1.3 Research Objectives and Research Questions.

The primary objective of this systematic literature review is to comprehensively investigate the impact of Artificial Intelligence (AI) on the testing instrument industry and to identify the countermeasures employed in response to these changes. The research aims to contribute to a deeper understanding of this evolving intersection between AI and testing instruments, ultimately advancing the state of knowledge in this domain.

To achieve this overarching objective, we have delineated the following research questions:

RQ1) How has the integration of AI transformed the accuracy, predictive capabilities, and automation of testing instruments in various domains, including education, psychology, and healthcare?

RQ2) What are the specific functionalities, algorithms, and machine learning methodologies employed in AI-powered testing instruments that set them apart from traditional testing methods?

RQ3) In what ways can AI-powered testing instruments adapt to user responses, provide real-time feedback, and generate comprehensive reports, ultimately enhancing the efficiency and effectiveness of testing procedures?

RQ4) What gaps and limitations exist in the current body of scholarly work regarding the impact of AI on the testing instrument industry, and how have countermeasures been addressed or proposed to address these limitations?

Through a systematic review of the literature and an analysis of existing research, this study aims to shed light on the transformation brought about by AI in the testing instrument industry and highlight areas where further investigation is warranted. Additionally, it seeks to identify strategies and countermeasures that have been implemented or recommended to harness the potential of AI in testing instruments effectively while addressing any challenges or limitations that may arise.

1.4 Thesis Structure

The structure of the thesis on AI in test instruments is based on an extensive examination of the subject matter. Section 1.0 consists of an excellent introduction that lays down necessary grounds. This section focuses on defining the main problem under study as well as its relevance. Section 1.3 provides specific research objectives and questions that shape the

direction of this work. As an addendum, Section 1.4 outlines the structure of the thesis to give readers an overview in advance. Section 2 is arranged into three parts which allow the comprehensive study on the development of AI in tests devices, features of AI as a part of the industry, and the effects of AI upon tests process. Section 3 presents the method through which the research was conducted in a well-defined manner. A new approach for measuring research trends within Section 4 is presented through bibliometric. Section 5 is for finding and their implications whereby it gives meaningful contribution towards the field. Lastly, Section 6 presents a summary of the major outcomes and also indicates the challenges encountered during preparation for this paper. The organized methodology allows exploring all AI test instruments for clarity of the research's goals and conclusions.

2. LITERATURE REVIEW

2.1 Artificial Intelligence

According to the study by Bécue et al. (2021), the use of Artificial intelligence in test automation has been a major transformation among others during this period. Among others, AI has ushered in a revolutionary era of test automation which have substituted manual testing practices with precise, expedite, and adaptable methods. Traditional test automation is, by now, well-proven in terms of its ability to improve cost and time efficiency, but the problems have intensified with growing sophistication and dynamics of modern software systems. Such barriers have necessitated the introduction of alternative means by AI thus, bringing a time machine era of test automation.

In three critical areas, Zaman et al. (2021) argue that traditional test automation faces some challenges. In the first place, since testing involves designing of test scripts and this takes computer programs understanding a lot of business users find it difficult. This is true because they understand their processes well and most likely do not have any background in computing or programming. They encounter huge problems being involved in the testing procedure because they should design test cases. For example, in SAP test automation, functional users create test cases and their limited programming skills affect their full engagement.

Liu et al. (2020), additionally state that tradition test automation has faced the challenge of secondly challenge of test maintenance. It uses object locators like ID, name, XPath and CSS to operate with UI elements. Test automation scripts can break as a result of changing UI during application's update and that's why object locator should be reusable. However, such constant manual input is needed in order to keep or change these scripts which takes away precious time. Meanwhile, test prioritization poses a challenge as determining what to test in a software application can be intricate. Normally, these adapted scenarios are chosen not

based on any specific rationale but as a result of procedural experience or educated guess. This strategy may only lead to an over-test being performed or bad spending much resources, which can equally expose the business to threats.

AI provides new ways of dealing with these problems that long are associated with test automation. For instance, in the early stages of design for test scripts by Artificial Intelligence particularly via Natural Language Processing (NLP) has resolved this problem that people with no special software skills can write test cases in English with regard to work done by Yang et al. (2019). This invention in technology not only allows less technical users like business representatives and operation managers to create test script for testing but also does not demand learning specific programming rules. With the help of these types of tools such as Opkey, AI is used to generate automated test scripts through plain English based test cases; thus, one can say that business analogy has liberally employed organization and diluted.

Self-healing technology using machine learning is a solution to AI in the area of test maintenance, as claimed by de Azambujao et al. Based on machine learning, test scripts will be able to recognize changes done in UI elements and flows, what is more these modifications can be applied automatically with no human-doing. It does so by reducing the excessive human oversight that could be associated with dealing with test scripts in such a manner test automation framework like OpKey have been provided self-healing features that automatically heal the scripts if there is a variation of locators or flow.

Focusing on the conclusion of Jagielski et al. (2018), another way to approach this issue concerning test selection is by using AI-driven automation frameworks designed specifically for testing purposes, whose potential applications might lead us toward smarter methods than those currently present today in most used tools such as UFTLib 5, etc. The testing is executed by a model which was developed very recently. The algorithms decide the minimum number of tests required for a given change, such that they cut down on manual

judgment or running all regression cases but not every single run. This approach maximizes code coverage through minimizing manual activity. To illustrate, Opkey promotes test coverage infused with risk-based testing and a difference in how they implemented through test gap analysis – the greatest changes are examined to great depths where possible and simultaneously any unnecessary over-testing is avoided. This increases the efficiency and also means avoiding potential risks associated with software upgrades.

The combination of AI and test automation has a lot of various advantages including the rapidity, flexibility, in addition to increased risk coverage. One of the AI methodologies and technologies that accelerate these procedures include use of machine learning and natural language processing as it covers all possible risks in a detailed way. By using AI for automated testing platforms, organizations become flexible enough to quickly respond to a fast-evolving climate in modern software creation (Ahanger et al., 2022). AI-assisted test automation architecture such as Opkey solves the issues of conventional test automation. Risk based testing using risk analysis allows for greater optimization, they allow non-programmers in the project to create tests without programming skills, self-healing eliminates manual test maintenance efforts. With time that AI is integrated into the automations of software, organizations aiming at maximizing their effectiveness and quality of software test will keep adapting. It is vital that this progress marking a major breakthrough towards accuracy and swiftness in test automation.

AI-Powered Testing Instrument Functionalities.

Ahmed et al. (2021) findings state that Artificial Intelligence is highly successful because it has unique and exceptional features that make it work in the testing instrument industry. The advent of AI-driven testing tools has revolutionized how examinations are conducted, bringing unprecedented accuracy, speed and flexibility. The essence of such tools incorporates complex machine learning techniques such as deep neural networks and decision

trees that make it easy to deal with overwhelming amounts of data. Indeed, these technologies can be used in a variety of sectors most distinctly in education sector where it has ushered a new era of personalized learning experience and more effective assessment system. However, Sharifi et al. (2021) argue that the success of AI-based test tools relies on the use of complex machine-learning methods. These algorithms enable these tools to detect trends, forecasts, and smoothly respond to varying conditions in continuous nature. Deep neural networks as well as many machine learning models are well equipped to process and look into complex data sets with patterns and relations invisible for the naked eye. The ability to manage huge volumes of intricate data effectively characterizes artificial intelligence assisted testing machines as distinct from their traditional counterparts.

Machine learning according to the study by Taddeo et al. (2019) has been a crucial element in boosting the prowess of the AI testing tools especially deep neural networks. Such networks aim to model the neural nodes that connect to each other just as these happen in the human brain when processing information. The use of deep learning models is vital in testing instruments based on automation of natural language understanding, image recognition, as well as predictive analyses. Educational transformation through using artificial intelligence driven testing equipment illustration. Through analysis of their performance data, these tools are capable of personalizing learning experiences to suit an individual student or a group of learners. Traditional teaching techniques are however not appropriate for the world of education, where different student learning styles exist at a rate of varied learning pace (Keleko et al., 2022). AI driven educational systems track the students' progress all along, pointing out what areas they are good at while weak in and hence give personalized learning material. For example, if the student performs well in particular subjects but not in all, the system will automatically tailor the contents to deal with the poor performance and provide

immediate guidance towards appropriate learning needs. At this point, it shows a marked departure from commonplace methods of teaching.

The testing procedure is also improved through the use of AI-enabled test tools. In healthcare, AI-driven test instruments can analyze patients' medical history along with their present symptoms to provide faster and precise diagnoses. The instruments are able to adjust themselves for changes in clinical conditions, thus producing the best diagnostics and treatment (Varian, 2018). Additionally, AI automated testing gadgets are efficient and can process massive data sets immediately. Such an efficiency simplifies the testing procedure and drains greatly of the time and the resources for accurate results. For instance, in sectors, such as material sciences where the quality and confidence are essential, intelligent testing tools speed up the assessment of different products, which ensure that the materials comply with the industry requirements and safety requirements.

In summary, AI-driven testing instruments usher in an era of accuracy and flexibility in numerous sectors including education and health care. Machine learning is what drives their outstanding functions like pattern recognition, prediction and adaptation to changing situations without any hassle. Notably, according to Oseni et al. (2021), testing tools with artificial intelligence capability have great potential to provide tailored learning opportunities, facilitate test administrations, and improve diagnostic precision in various settings. The future of these devices as the world keeps on moving forward with artificial intelligence could be full of promises as more innovations will be invented for these devices that would help to increase their precision, efficacy, and flexibility in aiding the process toward testing and assessment.

Challenges and Limitations.

There is no doubt that the use of artificial intelligence has revolutionized how instruments used for testing are precise and flexible. However, it is never perfected and it reminds of

various peculiarities. The introduction of the AI technology is rather optimistic but not cheap for both less and more material circumstances that limit its application even further. (Singhal et al., 2020). The issue of data confidentiality is one of the most important dilemmas of the AI assisted testing tools domain. Equally sensitive information that forms core to essentially all the databases used in training and learning of an AI testing tool. For instance, in the field of healthcare, AI is being used by some diagnostic testing devices and it has a challenge with regard to patients' information privacy. Beyond medical information, confidentiality becomes an essential protective factor of sensitive personal data from leakages and intrusions.

It is another serious challenge according to Bistron & Piotrowski (2021), regarding the risk of bias by AI algorithms. AI systems undergo their learning process from historical trends which may be subjected to immaterial inequalities. The algorithmic biases can be very serious in a diagnostic testing or instrument. When the AI models that are used in such instruments unintentionally reflect the biases embedded within the data, this leads to many errors in interpretations or even as some would say miscalculated diagnostics and treatment directions. Not only do these biases exist in society, but they can also affect different groups disproportionately to the extent that what is being exacerbated are already known inequities in healthcare outcomes. Thus, disrupting algorithmic bias and guaranteeing that AI-driven testing devices furnish reasonable and adaptable results is an urgent undertaking. The study by Guo & Li (2018) notes that the adoption of AI is also generally led by ethical concerns. The importance of ensuring that these tools comply with ethics and standards is great, especially for any field dealing directly with human beings such as healthcare. The dilemma of ethical concerns can arise from questions such as those regarding transparency and accountability to quandaries pertaining to the interpretation and implementation of data using AI. By merging the technological improvements with responsible conduct, there comes a situation where one needs to strike the right balance which is a question that merits attention.

Countermeasures and Strategies.

For Hamon, et al. (2020), the somewhat complicated sets of countermeasures and strategies have been presented to exploit the full potentials of AI in test instruments while simultaneously dealing with the challenges it brings up into play. These bi-level measures have been created to reduce risks, provide the facilitation of responsible AI usage and maintaining ethics during development and commissioning IT systems using artificial intelligence.

Ethical Guidelines: The creation of deeply rooted ethical codes also constituted a crest stone, one that was very crucial in portraying the significance of a responsible AI usage. Prior to the adjustment of any AI-based testing tools, these guidelines can be regarded as a foundation for both developers and users. They represent a number of ethical concepts such as equity, openness and reliability with an intention to address any possible concerns involving ethics. For the successful and ethical implementation of AI, these recommendations can be followed, or else better approaches should keep focusing on avoiding ethical breaches in AI-driven testing while upholding it as an accepted practice in society (Ansari et al., 2020).

Transparent AI Algorithms: Transparency can be considered a necessary feature of AI algorithms, and it is still one of the pillars in decision-making understanding. The supply of details on the mechanisms and approaches applied to AI models for producing conclusions is a crucial step towards recognition, as well as eradicating algorithmic biases. AI-powered testing tools can make it so that's transparent which assures in the human race that results are based on fairness and is what allows stakeholders to trust decisioning from AI.

Rigorous Data Privacy Measures: Ensuring data security becomes an ineluctable step in the realm of AI. Shielding information by strong data privacy measures, including encryption, access control and anonymizing data represent the fortification that keeps individual's private

data secure especially in learning situations. However, the compliance with stringent data protection regulations clearly assure that such required steps are observed, for instance GDPR.

Ethical Considerations in Personalized Learning: In the context of education, ethicality becomes an important aspect in personalized learning platform development as most developments involve consideration and implementation measures on data protection to ensure students' data privacy and security. These attempts are also meant to show a deliberate sacrifice of the interests of students, whilst ensuring they get customized learning experience. In this respect, technological providers of education have taken strategies like anonymization in covering student information through which they can deliver customized education with security of the data (Chakraborty et al., 2021).

Bias Mitigation: The reduction of algorithm-bias is on urgent attention. In addition, developers are increasingly implementing bias-reduction approaches that seek to reduce bias in AI models. Among these are data diversity, wherein training data is made representative to create a more inclusive model that does not exhibit bias in its predictive functionalities; the auditing of deployed models as well as constant checking and reconditioning is utilized to avoid cases of biased performances by mitigating imbalance in the testing results. Measures to combat bias are required for any AI-operated testing in order to promote fairness and equality.

Oversight and Accountability: Setting up mechanisms for monitoring and accountability is crucial in ensuring utilization of AI application-based test devices responsibly. These systems demarcate functions and obligations spanning the life cycle of such instruments, from their creation to their readiness and utilization. Thus, checks and balances mechanisms are enforced because those held accountable for possible ethical lapses or breaches have to take responsibility (Zhang & Zhang, 2023).

2.2 The testing instrument industry (present the sector)

However, the testing instrument industry in Artificial Intelligence (AI) space has seen significant transformation over the recent past, motivated by the dynamic changes taking place within this AI technology. AI is one of the leading frontiers in innovation where it has terrifically dissipated across different sectors, chiefly including the health sector related industries healthcare finance independent transport and natural language processing (Khan et al., 2023). Along with tremendous gains, the unleashed vastness of AI provides many dangers in case its systems break down or generate impure results. Therefore, strict testing needs to be a priority making sure that the AI systems are trustworthy enough in terms of credible operations, proper accuracy and safety. The demand for all-inclusive AI testing products further grows, as the level of dispersion of AI in various sectors continues to develop another solid manifestation is the significance as well as necessity for them were put within the framework of an independent industry which controls integrity and behavior packaging pertaining to modern AI solutions.

Significance of AI Testing Instruments

As Kertysova (2018) pointed out, testing tools somehow reveal the importance stage of AI industry. As AI systems learn by themselves and can make decisions in critical situations, they should be as to the point examined and evaluated lest failure or mistake is propagated further up into a severe occurrence. This need grows more important where such errors tend to have adverse effects on self-driving cars, clinical diagnosis or trading actions etc. where every step has an effect, no matter how minute it may.

Firstly, in accordance with the report published by Schwartz et al. (2022), they guarantee quality assurance as they referred to automatically fail-proof AI system behavior against any factor which is likely to contribute toward malfunctions or inferior outcomes. Another vital issue safety, especially in systems that define by possibilities with people life-styles for

example health or autonomous vehicles like the system test structures assess these systems evaluation of fundamental security including the principles to provide a reliable set of choices through emergent events. With regard to AI ethics due to biases carry over, the plans solve issues caused by various forms of tools that compute efficiency and discrimination detection, accountability and transparency as a way to detect ethical dilemmas. Furthermore, Jagielski et al. (2018) note that regulatory compliance is an important component and AI-testing instruments are helping organizations to ensure their AI system uses in line with regulations as well as other relevant compliances. Finally, these tools pursue the effectiveness of AI systems by calibrating algorithms for higher speed, precision and efficiency of resources and are, therefore, able to achieve desired output from AI applications.

The AI testing instrument industry is on a rapid growth trajectory fueled by the promising combination of certain drivers that highlight it as one whose time has come and one which shows promise. These drivers encompass a variety of facets. Initially, as referred by Siddiqi et al. (2022), the speed with which AI has spread over different sectors such as healthcare, banking, e-commerce etc., it is mainly due to their growing requirement for instruments used in testing a commodity or service. Seeing AI-based systems are in the core of daily action such organizations require to always monitor this accuracy and precision, meaning no days with no necessity for performance testing: such growing coherency is supported by an emerging need for performance testing. Moreover, the awareness of the danger posed by human mistakes made by AI is also acutely increased demand for inclusive test designing tools. It is more so in applications of safety-critical set, by virtue of a fact that the eventuality may result in total loss depending on the case; insinuating why tools for testing are vital to risk mitigation.

In addition, Akhtar et al. (2023) states that the range of control from AI over different industries had demanded strict regulations to meet the system criteria. Fulfilling all evolving

regulations needs tough tests and validation procedures, adding even more pressure in terms of testing instruments. However, ethical troubles and biases developed within AI systems have taken a strong focus by special investigations requiring testing instruments that test for problems of fairness, accountability, and transparency in the techniques. Besides these trends, optimization of AI system performance has been a key factor. Test systems have important roles to achieve the goals in correcting places where improvements are needed and for improving AI algorithms that can produce superior speed, reliability as well resource consumption. Finally, advancement of AI technologies and testing tools has made one another. As modern AI testing instruments are developed with high-quality computing abilities to be able to evaluate complicated systems produced by these new types of intelligent artificial intelligence.

Changes in the characteristics of testing instruments of artificial intellects show an evolving nature to a great extent. Positive trends include AI testing with AI, which is performed using machine-learning models that autonomously generate test cases and evaluate the performance of AI systems. Another important trend is ‘Shift Left Testing’ which proposes early testing right into the software development life cycle to identify defects and rectify them at earlier stages (Keleko et al., 2021). Explainable AI Testing is important because it helps ensure that some members of the public are called ‘unsuspecting’ or ‘victims’ and countless dollars have been spent as a result. Test automation, thanks to AI, is now on the hike and tools are being developed which can generate as well as execute test cases automatically. Moreover, this shift has led to continuous testing within the DevOps pipeline that is now part and parcel of DevOps but also to the emergence of Artificial Intelligence and other AI testing instruments in providing real-time feedback. Furthermore, there is a comparative trend towards measuring the effect of AI across different stakeholders as a result of their perspective on how AI systems shaping end-user experience, ethics and societal values. One of the main aspects,

however, that organizations should take into account in pursuing these goals is staying informed about the changes to keep up with the latest testing methodologies that are being used and keep competition at bay as AI change management will continue to develop.

As this industry celebrates ever exceeding new heights of growth and development, it faces a number of broader challenges. According to the sophisticated testing tools and methodologies, it would only be complex calculation in itself and the operation of an AI element can therefore occur because of elements intricate calculations and nerve groups of chips fired upon specifically on an AI program. Since, methods such as the means below are often large in data it is shown that a deal of focus should be given to first how exactly this will manage sensitive information and their effects on data privacy & security. While the observation and detection of potential biases in an AI system as well as the subsequent fixation has become an integral part of any given programming, their identification is extremely difficult due to non-uniform ways, through which they appear within a certain system.

The darkness or limited insight within AI models, most commonly referred to as ‘black boxes’ raises challenges when trying to explain and interpret the underlying thought process. One of the continuously complicated tasks that need to be constantly adapted is to respond to the new laws and standards, leading us into digital AI-empowered futures (Singhal et al., 2020). Moreover, with increasing adoption of AI systems as technology matures and grows in scale, scalability of test tools required to evaluate these systems efficaciously on a large scale assumes the role of an industry challenge. These challenges are critical to be addressed as the respective AI testing instrument industry is needed, which serves for further innovation and evolution alongside intrinsically advancing branch of artificial intelligence.

In spite of all stated challenges, AI testing instrument industry still has very innovative options and also bright technical future. These innovations are essential to remain on the world’s financial development and maintain relevancy amidst the growing field of AI. AI-

driven testing tools tailored for AI systems, which use AI to test the operations of an ML system have come about offering automatic development and execution of test cases and bottleneck equivalent prediction improving productivity as well as thoroughness during such tests. Over the course of recent years, one significant pattern is the enactment of clarified AI testing gadgets that react to the hiddenness of AI framework and making them noticeable and interpretative in nature so as to have a positive effect on debugging too ethical contemplations Taddeo et al. (2019). Focusing on the growing issues of bias in AI systems, ethical and bias testing instruments are to be developed which would help identifying major biases and work out means to reduce them. Continuous testing tools that are incorporated into the DevOps frameworks emerge as common digital standards, which provide real-time feedback and monitoring in AI.

Furthermore, working with domain experts during the process of developing the testing instruments guarantees that their practices and needs are catered for in specific contexts since these include the aspects such as situations related to special challenges. In addition, the development of AI testing as a service called (AI TaaS) streamlines the process of testing for organizations that lack internal expertise Ahmed et al. (2021). Finally, the manufacture of testing auditing tools having in-built regulatory festivities helps organizations to maintain compliance with continuously changing regulation standards thereby improving the compliant area. The presented innovative solutions and trends show that the industry has potential not only to change but also lay down the path for a future where AI systems could be tested and applied in different areas properly and ethically.

Summing up, the AI testing instruments sector is well set for not only constant but also significant growth and dynamism. As AI applications continue to permeate multiple industries, the need for strong testing and assurance tools will grow even more urgent. This sector is critical for asserting that AI systems are uncompromising, safe, moralistic and

compliant from the point of view of laws. With innovative solutions coming up, the discipline will be at the center of evolution in the technological arena and print human faces for all AI testing and validation.

2.3 AI on the testing instruments industry

The major revolution that came in testing instruments with the help of AI is the main cause which has led to multiple scholarly discussions and studies. The number of literary sources discussing this change is countless, with different points of view having appeared on the situation and that makes a discussion rather rich, differentiated and multidimensional. The areas that are covered by these studies, ranging from ethical concerns to security issues and the plausible preventive actions include more than enough facts proving AI impact on testing instruments well. The emerging technology of artificial intelligence had already proved itself to be revolutionary in different spheres, which has provided revolutionary features that have led innovation and high performance. The objective of this systematic literature review is to conduct a thorough analysis into a broad swath of studies that explore the major role that AI plays on testing devices Moreover, the evaluation identifies the suggested actions to be taken in order to overcome any challenges that may arise. The latter refers to the threat imminent from AI as detailed by Hu et al. (2021) among other things who broadly outline these security risks.

In addition, they examine how the risks can be reduced by employing their plans. By looking into the complexities of AI systems, they draw attract attention to complex algorithms and vast datasets that support these systems. Here, their argument indicates that although AI has potential to help uphold cybersecurity technology, the very use of such systems bears unique vulnerabilities via which malicious force can find openings and strategize their game. The elements of complexity that lie within AI systems also ensure that the loyal vulnerabilities are being precluded. There are shortages of transparency in how these systems make decisions.

Additionally, these risks demand AI algorithms to have bias in order to handle them (Hu et al., 2021) observe some mitigation strategies. The strategies of safeguarding data include a set of security protocols aimed at ensuring reliable functionality, AI algorithms that ensure secure implementation, if considered into place and the process of rigorous testing and validation is another factor to consider.

This is what Mohana Krishnan et al. (2023) suggested according to their results; they deal with this issue specifically as cybersecurity history in relation to AI. In identifying intrusion detection systems, they describe what precisely their artificial principles excellently reduce malice as an attack, for a better accuracy which serves the automatic management of security incidents and actions related to them. However, they issue a warning about the potential hazards associated with over-reliance on AI. The roadblocks include such possibilities as erroneous suspect-returns, the fact of having to defend one's self against hostile attacks and the difficulties associated with maintaining information confidentiality and privacy. The potential bias point in the formation of AI systems is one of the serious concerns, in accordance with Schwartz et al. (2022) Treating bias as a major concern, Schwartz and his colleagues (2018) argue for standards to be built for identifying it and managing partiality effectively. As they suggest that the essence of AI encompasses integrity and reliability so, securing together these elements in systems is crucial. This is also very much illustrated in the way the bias is related to context, particularly when testing tools are assessed and regarded while understanding how they help determine result authenticity. In order to curtail bias in artificial intelligence, a number of techniques are suggested. Other elements of such strategies include exploiting a multitude of training data, and likewise using metrics to ensure that fairness is maintained; furthermore, knowing how AI systems come about decisions when explainable techniques are used pertains to these strategies.

In the paper by Whelan et al. (2022), the application of AI in intrusion detection systems for maneuvered aerial vehicles is examined. They point out that machine-learning algorithms may help to boost these systems' capabilities. It is that said they emphasis on the importance of robust defense mechanisms as a means to protect against potential security hazards. The adopted countermeasures include secure communication protocols, intrusion detection algorithms implemented and data encryption. By his very nature, Zaman et al. (2019) utilize AI to detect railroad trespassing automatically. In this particular case, AI capabilities that highlight the security strengthening are discussed. AI-Based solutions are offered in various forms. The application entails using image recognition algorithms while getting predictive models into use for implementation, whereas machine learning is designed to assess pattern correlating intrusion.

The utilization of the countermeasures and camouflage when dealing with EO/IR imaging systems has been done by Livada and Perić, 2020. The attention is focused towards comprehension that there are constant contests for developing new AI technologies and strategies in reducing the risks which these advances bring. A noticeable development in the ongoing competition is, therefore, its continuous progress toward introducing newer AI algorithms and techniques. The response here is the ensuing growth of countermeasure measures seeking to provide defense against these threats. This is also reflected in what Namatherdhalaet al. (2022) have to say about AI for education and provide a comprehensive account with regard to technological progress achieved in the field of artificial intelligence especially as far as education sector is concerned. Under this light, the emphasis is on indicating that AI may indeed enhance educational outcomes but only provided that one will have to put in place strict security mechanisms to prevent such imminent dangers. The initiatives to be implemented for the purpose of enhancing the security are applying reliable data storage and transmission methods. Finally, the adoption of preserving privacy algorithms

and implementing strong authentication techniques enhances the security of information databases is realized.

Waheed et al. (2020) investigated the areas of overlap between AI, machine learning and blockchain as they relate to IoTs in terms of security. In addition, these technologies are made applicable showing the potential for improving IoT security Issues of protection against possible threats are also highlighted. Some of such countermeasures include locus use of secure communication protocols. Along with this implement blockchain authentication systems deploy machine learning techniques in order to be able to identify and react towards security incidents and all these points focusing primarily on robotics cybersecurity vulnerabilities and attacks (Yaacoub et al, 2022). A great deal of attention is given to the potential of AI to surmount the limitations that have become evident in its earlier iterations and enhance the capabilities of robotic systems. However, they highlight the importance of implementing effective measures to protect for potential threats.

A study conducted by Bonfanti (2022) focuses on the actions and reaction dynamics of the offense component and a bargaining capability defense party in AI cybersecurity. His argument is that AI has a type of potential to desynchronize this balance, and therefore requiring some new approaches on how to maintain security. Given these options of defense strategies, he suggests various ways to ensure the offence-defense equilibrium. The use of safe coding practices is one strategy implementing the methods employed secure testing and validation procedures, and the use of adversarial training methods is another strategy with these approaches that aimed at enhancing AI systems resilience. On the one hand, AI is able to deliver enhanced computing power and experience that improves action where necessary. In light of this field, the threats, countermeasures, and design principles corresponding to it are highlighted thereby dwelling deep into hardware design detail where aspects such as

generation of attacks against hardware are brought up and requirement for effective safeguards to ensure secure application as well as operation is touched.

From the adaptive learning industry, various researches have been conducted to highlight different implications of AI on education assessment tools. The article by Fengying et al. (2021), in their research, provide an elaborate exposition on the development trends, challenges and counter measures surrounding AI implementation in education sector. Thus, this study offers a close reflection of the findings of Li and Wang (2020), who sought to investigate in what ways AI can present an opportunity for adaptive learning as well as the doses it presents. These studies give clear and deep ideas on AI applications that help in improving testing practices in the educational setting through adaptive learning environments, individuality as well as all-around assessment.

Additionally, these studies do not indicate the insufficiency of countermeasures necessary to prevent misuse and improve performance. The possibility of using AI in a wide variety of situations is also highlighted by Livada and Perić (2020), as well as Namatherdhala et al. (2021), which discuss current advances concerning countermeasures towards EO/IR imaging systems and camouflage and trends on the field of education related to AI. Their results add to the characterization of AI Humanists' influence on testing tools by demonstrating the adaptability that it can give. At the same time, the article by Thomas et al. (2022) widens the frame of discussion on AI and expands its possible applications – vaccines and drugs design. However, this experiment shows us the possibilities of AI application in different sectors which are growing to new heights paving a way for its transformation in other areas like health care and pharmaceuticals. They emphasise the AI abilities in predicting drug-drug interactions, faster vaccine development and improved testing shortenings. This research, however, can be seen as a breakage in the subject of this review it continues to demonstrate how AI expresses itself over testing tools across these different fields.

There is a crucial aspect of AI and cybersecurity overlap widely discussed by many researchers. Ramadan et al. (2021) highlighted the contribution of AI to imbue cybersecurity measures with enhanced security features against infiltration consisted particularly pointed out during Covid time where onset focus was laid on digital safety. They suggest AI-based testing tools that may achieve active detection and counteract cyber threats effectively. This study is accompanied by the work of Surma, who reveals the classification of machine learning attacks thereby supplementing this research and contributing to the discussion about strengths that AI brings to demand for cybersecurity. Truong et al (2020) prepared a profound analysis of the military capabilities of AI in cybersecurity as well as introduced new testing tools and countermeasures. This study finds a comprehensive discussion of this aspect from the impact of AI and Big Data on China's international trade as they take place in crises. By illustrating an ability of AI to enhance recovery in sectors such as testing instruments amid unprecedented threats, it proves the might of AI when confronted with difficulties. According to such hypotheses, the research puts forth that AI technology is an integral tool to unite industries for testing gadgets in sophisticated conditions of large scales.

The articles by Mihoub et al. (2022) and Rugo et al. (2022) are relevant to the subject, as they address denial-of-service attack detection and countermeasures in the UAVNet era. These works helped inform the discussion of AI implementations during cybersecurity testing, with support from two novel essays. This study pinpoints, the model of use for AI to establish algorithm detection and improving on network security as well as come up with strong defense mechanism against any sort of cyber threats. The extended domains security in which different areas obtain it many from research such as Putra, (2020) covering Cognitive AI or Ansari et al. (2020), of featuring distinguished intelligence caretaker against the edge computing environment. From this analysis, these investigations shed light on the potential of AI transforming the processes involved in security across different technological platforms

such as edge computing and cognitive intelligence systems. More so, Rauti et al. (2021) contributes to the discussion of how Man in the Browser attack can occur by studying literary on IoT devices. They create a complex network of potential threats, challenges, and countermeasures that rear their heads as the interplay between AI's technology emergence into the emerging IoT field. Similarly, Chakraborty et al (2021) studies give an in-depth insight on the entire issues concerning securing the nodes of IoT. In this sense, their results reiterate one of the main messages of this review and additionally justify the significant snapshots on AI effects when it comes to test instruments based on situations that require countermeasures in both IoT as well as wider technological backgrounds.

3. METHODOLOGY

The methodological basis of this study consists in the Artificial Intelligence theoretical approach about its impact on various testing instrument industries from different areas. It draws upon relevant theories, concepts and models therein originate from the literature to describe the nature of its topic lucidly. On the contrary, theoretical concepts of machine learning, natural language processing and test automation are employed for an in-depth analysis into which direction AI affects the testing tools.

Further, the study however collates more specifically the decision-making analysis theories of Ronald A. Howard with respect to quality control procedures and instruments. The topic of the Bayesian probability framework is also highlighted when making reference to how AI acts knowledgably in all factors relating to decision-making and managing risks within the test instrument industry.

In order to reinforce this theoretical approach, empirical research and case studies are incorporated in place of providing knowledge about the applications of AI found in testing business in terms that is factual. This combination of theories is applicable when analysis in a broad sense has been exhausted after identifying counteractions together with the strategies for coping up with challenges that are present here, it seems the special emphasis is laid out at all positive aspects given by Artificial Intelligence technology adoption towards testing instruments.

We have applied the approach of systematic literature review to conduct this study. Consistently, we applied a bibliometric analysis methodology to examine the trends, patterns and influences within the scientific literature pertaining to the effects of AI on the testing instruments industry, as well as to quantify research and identify potential research gaps on the topic. According to Tranfield et al. (2003), this process of bibliometric analysis involves the quantitative examination of publication trends, citation patterns, authorship collaborations,

and key research topics within a specific field of study. It offers valuable insights into the evolution of research, identifies prominent researchers and institutions, and highlights areas for further investigation or intervention. The working of this method is aimed at accumulating a detailed and objective picture of the matter under studying with many scholarly sources. The systematic literature review process conducted in this study consists of the following steps:

1. Identification of the research scope and objectives: The lines for research and goals were outlined to guide the literary study search.

2. Literature search: This study looked at articles and studies as to how AI would influence the test tool industry; this was done by a comprehensive search in academic databases such as Scopus, IEEE Xplore and Web of Science. These keywords include artificial intelligence, as well as testing devices used in test automation and machine learning.

3. Selection of relevant literature: For the purpose of screening, the articles applicable to this research were selected based on their relevance to the objectives. The review refers to works dedicated to AI help in testing tools and its redesigning process, as well as the obstacles and limitations of integration.

4. Data extraction and analysis: The data from articles of their choice was extracted and used to identify themes, findings and recommendations that linked to different research questions. The data episodes provided structured and generalized information on the literature as a whole.

5. Evaluation of the quality and validity of the literature: The selected articles were subjected to critical review where the validity and accuracy was assessed. Authors' credibility, method rigor or systematic aspects of the research as well as its relation to their outcomes concerning research objectives were evaluated.

6. Synthesis of findings and identification of gaps: The articles were analyzed and their findings were integrated to establish common themes, trends and gaps in the literature. This enabled the identification of the main areas for further research and development of recommendations.

7. Development of countermeasures and strategies: The synthesized findings and identified gaps were used to formulate countermeasures and strategies that could be used as interventions in addressing the challenges faced by AI users to maximize their benefits. A systematic literature review methodology is used; this way, the study base will be established on existing knowledge and present a comprehensive analysis of the research topic. It helps to outline such key trends, issues and suggestions that can promote the area further and have an impact on future studies/practice.

In our study we used a mixed methods approach that included quantitative and qualitative research methods. In particular, we utilized content analysis and bibliometric analysis to achieve overall understandings regarding the effects of AI on this industry into testing instruments.

3.1 Data Sources

A wide variety of data sources were utilized to conduct a comprehensive systematic literature review. The main sources of primary data included academic databases like Scopus, Web of Science, and IEEE Explore. These databases were searched with the help of relevant keywords and filters to find scholarly articles, conference papers and other research studies. The search inclusion criteria included papers published within the past 10 years, in the English language and focused on the impacts of AI on the testing instruments industry. Apart from the academic databases, relevant industry reports, white papers and technical documents were also used as secondary data sources. These sources offered invaluable information and examples of AI integration into test instruments.

3.2 Search Strategy

A combination of keywords and filters were used in the search strategy to narrow down the results. An initial search was done with broad keywords like ‘artificial intelligence’, ‘testing instruments’, and ‘AI in test automation’, and the results were refined by additional keywords such as ‘machine learning’, ‘test scripting/test script generation automation’, ‘natural language processing’, and ‘self-healing test’. To ensure a thorough search, the keywords and search terms were also used in their variations including synonyms or related words. The search was also restricted to appropriate disciplines including computer science, engineering and automation.

3. 3 Screening and Selection Criteria

The process of screening and selection involved a two-step procedure. In the first stage, titles and abstracts of identified articles were screened for relevance to research objectives. Articles not relevant to the study like those that are more than 10 years and articles that focused on something other than AI’s influence on the testing instrument industry were not excluded. The second step involved a full-text review of the remaining articles.

In the stage of full-text review, articles were appraised for their quality pertinence and contribution to the research aims. Articles considered to meet the inclusion criteria as well as those articles that gave valuable insights and findings were chosen for an in-depth analysis and a synthesis of information.

3. 4 Data Extraction and Analysis

A systematic approach was used to analyze the selected articles. Data were extracted from the articles and structured according to research questions and topics identified in the literature. Important findings, patterns, and suggestions were identified and summarized.

After extracting the above data, they were analyzed and then synthesized to give a holistic view of how AI affects the testing instrument industry. The common ground, issues, and limitations were highlighted following the consolidation of results.

4. BIBLIOMETRIC ANALYSIS

One common quantitative method appears to be bibliometric analysis - a process where trends, data and patterns are analyzed within scientific literature. Studies on AI based test tool industry necessitated a bibliometric analysis to establish research trends and patterns. The scope of the study was concerned with publication trends, citation patterns and researchers' collaboration. The bibliometric analysis was conducted by entering the selected articles into VOS viewer or Scopus to utilize their standardized approach The information extracted using the articles retrieval focused on publication year, author's institutions, keywords and citations in order to develop charts and statistics.

Bibliometric analysis revealed that as the number of publications in the field increased, authorship patterns evolved with top researchers and institutions as well as key articles published during that time period which research topics flourished. It also provided the detection of any gaps between research that needs closing or areas where more work would be necessary. The outcomes achieved from the bibliometric analysis were subsequently combined with those of their literature review to enable greater understanding on how AI affects test instrument manufacturing and what preemptive steps need to be taken in the development process or strategies should they be incorporated.

Presentation and Discussion

Presentation

AI is an evolving technology with the capability of transforming scores of industries such as those ability of automating tasks and generating useful information from large datasets. However, amidst its potential lies a critical concern: reliability and stability, especially for AI systems, mainly utilized in critical applications like self-driving vehicles and diagnosing medical technologies - that is sometimes hard to achieve. By doing so, these

tools play the indispensable role that was pointed out by Walter et al (2021). These tools are considered the sentinel, maintaining the engineering and resilience of AI software and avoiding the worsening of the situation by developing functions or suboptimal results. In addition to that, they take up the task of identifying the loopholes in the existing security measures, mitigating biases, ensuring regulatory compliance, and improving algorithms for enhanced efficiency and effectiveness.

The rising trend of AI verification equipment repeats the immediate adoption of AI across some industries, such as healthcare, banks and e-commerce. Organizations now realize the necessity of maintaining surveillance conditions related to AI accuracy and preparedness, which creates the products and services for performance testing tools. Moreover, there is an increased awareness about the threat ensuing from AI errors as humans that has made this situation an indispensable necessity for the developers to develop appropriate testing tools, especially when it comes to life-critical applications where error is not tolerated. For Artificial Intelligence (AI) applications, the complexity and variety of them mandate the multiplex approach of testing which considers different circumstances and borderlines, to make sure all of them are evaluated rightly.

Nevertheless, along with the soaring digital advancement in testing, the industry is ripe with complex challenges. The complexity of AI procedures together with the large volumes of data requests a safe way of managing private info to ensure data protection and security. Identifying biases residing within AI systems, in addition to devising mitigating strategies, AI also face extra challenges due to multiple peculiar presentations of biases (Wang and Chung, 2022). Similarly, the AI models hard to understand, called ‘black boxes’, add to the infidelity in interpreting the AI systems’ decisions during the testing unfolds, which is also a tough job for re-creators. Addressing these stumbling blocks necessitates shared efforts of the stakeholders, such as researchers, developers, regulators and

manufacturers, to create practical test frameworks and approaches for verifying the safety and quality of 3-D printed medical devices.

In addition, the AI testing instruments business is not static but it is dynamic while it continuously evolves to circumvent the challenges. Through advanced techniques such as the AI-driven testing tools, explainable AI testing methodologies as well as test automation, the testing processes are being streamlined to make them easier, and at the same time the reliability of the AI systems is better enforced. Joint projects with domain experts and the use of AI testing as a service (AI TaaS) point out the increase in the classes' readiness and the speed of testing processes (Wazid et al., 2022). Additionally, the surveillance and auditing toolsets, which are integrated with built-in regulated conditions, are crucial for compliance with increasingly complex and dynamic regulatory requirements. With future and present AI technologies increasingly infiltrating all areas, AI testing instruments will consequently become one of the most important tools in the box for the relentless battle against AI system failure risks as well as to ensure responsible and ethical deployments of AI systems.

Discussion

AI applies to the key aspect of AI testing technology – the aim of which is to avoid safety and reliability problems and address ethical issues with AI systems in various fields. AI is making moves towards seeping into various sectors, so the demand for more effective testing solutions is bound to keep increasing. Organizations should identify the significance of the mentioned AI testing tools and invest appropriately to mitigate the risk and guarantee the implementation of AI projects' success (Wu et al., 2020). Therefore, this requires a regulating assessment of testing, which consists of the whole system review of artificial intelligence in different scenarios and conditions. An ever-changing landscape of applications of AI dictates that there should be similar changes in testing methodologies, which is also important in

making the testing process unique for different domains. This process also requires ongoing research and development in AI testing.

Extending the achievements of the AI testing apparatus industry is not a one-sided story, hence there is a need for unison efforts by the stakeholders. Increasing data privacy and security policies, identifying and addressing bias-related issues and introducing transparency concepts in artificial intelligence models are indeed major steps toward overcoming these challenges (Wazid et al., 2022). Collaboration between the scientific communities, and industrial experts is worthwhile as it gives room to establish uniform testing procedures and keep regulations. Moreover, the establishment of training and education programs is essential to ensure that personnel possess the expertise required not only to make proper use of AI testing tools and methods but also to contribute meaningfully to the generation and refinement of AI-derived insights. This working together to generate creativity will bring forward a breakthrough in the technology of AI test methods. The collective experiential grounding of all stakeholders in academia, industry and the government, will largely determine the future of AI testing, and consequently, the actualization of medically valuable AI technologies.

The next step in AI research should be the implementation of new testing methods, which not only address the issue of old challenges but also help to improve system reliability of artificial systems. It is, however, essential to do research in more advanced approaches and to innovate new original methodologies and machines to cater to the escalating complexities in AI algorithms as well as applications. Along with this, further emphasis should be laid on integrating AI testing as smoothly as possible into the general DevOps pipeline, which will help optimize the testing process and smoothly incorporate it into the overall development workflow (Walter et al., 2023). The adoption of the anticipated developments of AI and the sobering of the current issues today by the stakeholders will make the successful run of AI

safer. Through this AI testing approach, sensitivity to proactive AI testing is a critical step toward creating trust and confidence in AI technologies within many fields. Effective testing methodologies become a critical point holding in place the ability of AI to increase the innovation rate and deal with the most complicated issues of society.

In conclusion, AI testing devices are inevitably crucial tools that can harm the dependence, safety, and ethicality of AI systems through diverse applications. Undoubtedly, the industry remains a challenge but the industry keeps on innovating while collaboration is at the etymological root driving the progress of AI testing methods (Wang et al, 2022). Stakeholders would need to address these challenges and adopt future trends to ensure that the reliability and effectiveness of AI Systems will remain expected to be seen for the years to come. AI testing tools will kind of govern the development of AI tech and the ways it will be used in the future, and this explains why they are indeed an essential item in corporate plans for the adoption and deployment of AI.

5. FINAL CONSIDERATIONS

5.1 Main Conclusions

To conclude, the study explored AI's immense influence on the testing industry at critical levels. The deployment of artificial intelligence by the testing equipment industry is a change overtaking itself, bearing different consequences for distinct areas. In this investigation the influence of AI on testing devices modernization has been shown. AI markedly improves test accuracy and expands their capabilities and flexibility while optimizing test procedures. The utilization of AI technologies, in addition, has made advanced testing instruments more adaptive and capable of performing tirelessly with increasing accuracy. One of the main observations drawn from this study is that AI-based testing tools generate significant potential for the enhancement of quality assurance processes across different industries. These devices have the potential to automate repetitive tasks, analyze large volumes of data, and identify patterns that a human operator may not be able to identify. Through this, organizations will be allowed to reach and maintain a higher degree of dependability and consistency on the tests and thus will result in a better quality of the products as well as customer satisfaction.

Moreover, human resources managers can now improve and optimize the decision-making process due to the machines helping in testing employees' intellectual capacities. Organizations now are able to streamline their processes by integrating AI algorithms into the system that helps them to process data in real-time, identify trends, and make decisions based on data that will lead to the goals of the organization (Bai et al., 2022). Furthermore, these powers enable management of the company more precise and exactly formulate strategies and resources allocation for the achievement of the best business outcomes. Similarly, thanks to advanced technologies, testing can be done automatically and may admittedly change

many different spheres such as healthcare, banking and training. In health care, such as, AI-based diagnostic testing tools can help medical experts with breaking down the medical conditions and creating patient-specific treatment protocols. In the finance sphere, AI-based testing tools are becoming to evaluate the financial information, detect fraud, forecast the market, and make optimum investment strategies via them. Likewise, in the transport industry, an intelligent and convertible evaluation-system tool can enhance both safety and dependability of autonomous cars and transport systems.

5.2 Contributions of the Research

5.2.1 Contributions for Corporations

Through this study, AI companies need to steer their approach toward AI integration to account for ethical considerations, forming a clear path for success. Concludingly, these enumerated hurdles and suggested mitigations are the sources of an actionable map for corporations to move through all upcoming aspects of AI implementation. This paper presented a range of guidelines for business ethics which is perceived as a basic structure for corporations. Principals like Equity, transparency and dependability are highlighted through these standards (Basner et al., 2021), which show the significance of the issues of ethics in the AI system. Adhering to these basic values helps corporations in creating strong ethical principles which makes trust among stakeholders, and AI continues to be ethically applied. AI algorithms with high transparency requirements are possible tools for businesses to control the issue of decision-making understanding. Through explaining processes and methods secured in AI models, corporations increase transparency among consumers, thus providing the right foundation for trust-building. This will not only facilitate trust in the results of AI-based testing apparatus but also make it possible to minimize algorithmic biases where the opportunity arises which would lead to unbiased and fair decisions.

The implementation of stringent data protection rules and regulations is in par with the already existing regulations, like the General Protection Data Regulation (GDPR). For example, businesses are media owners if they create and share information online, whereas they are also media producers when they use social media to communicate directly with consumers (Barnawi et al., 2021). Encryption, access control, and anonymizing data are emphasized in order to establish barriers that prevent unwanted people accessing individual private data in the learning environments. The bias mitigation strategies encompassing data diversity and continuous auditing, which are introduced in this research, providing viable approaches for corporations to deal with algorithmic bias can be viewed as the practical measures. Given that there are substantial policy consequences of biases in AI models, especially in accurate diagnostic images and tools, these tactics become essential in ensuring the fact and fairness in AI technologies.

5.2.2 Contributions for Academia

Academically, this research contributes significantly by providing theoretical frameworks, methodological considerations and the knowledge base for the future research in the area of AI and testing instruments. Firstly, this research scrutinizes a pragmatic approach that embraces AI, decision-making theory while in flat and empirical insights (Bai et al., 2022). Here, this comprehensive methodology increases our knowledge on how artificial intelligence may be used on wide range of instruments within the industries. Through applying these theoretical grounds, scholars and scientists will be able to investigate other spheres of effectualness, ethical rules, and future perspectives of the topic.

Secondly, the methodological contribution of this research lies in the systematic literature review and bibliometric analysis. This rigorous approach not only forms a model that can be used to replicate future studies but also serves as a sign post for the AI field and ensures a high level of validity. In a systematic way, researchers are able to sort out trends and

exposing holes, and assessing quality of the literature which puts this methodological framework into a continuous process of development to expand the existing knowledge in the field (Basner et al., 2021). Furthermore, this secondary source, or systematic literature review, can be used as an in-depth stock of knowledge for academia. In the event that a research approach is amalgamated, trends and gaps are found, and the research thus presents a good study base for those who want to understand the impact of AI in the current testing instruments. The dissection of challenges, ways of response, and ethical issues deliver an in-depth image of the issue so that everyone can start a journey to the answer from vice-versa with critical thinking.

5.3 Research Limitations

While our research throws light upon the collision of AI and testing software, it is imperative to bring to light some limitations associated with the work which have a major impact on the outcomes of this investigation. These limitations allow us to draw conclusions on the context-specific nature of the research and the direction in which further exploration could be undertaken so as to address these shortcomings. Firstly, we should acknowledge that the challenges identified and the proposed solutions in this text depends on a given context and therefore may need a tailored approach to industry specifics (Bhatnagar et al., 2019). The wide versatility of the testing instruments across different industries also introduces various challenges, which may not be entirely addressed by this study. It will be key for future research works to delve into industry-specific nuances and thus provide customized measures for organizations working in more generalized verticals.

Furthermore, the research elaborates the role of AI on the testing tools in particular, emphasizing the need for responsible and ethical use in the mentioned integration process. However, such emphasis may not cover the entire breadth of AI applications across different sectors of the market. The future research could be extended to discover the more significant

effects AI has on industries besides traditional industries, this will uncover both the challenges and opportunities each domain present (Bécue et al., 2021). Lastly, the depth of the analysis presented in some thematic areas, including bias mitigation and personalized learning could be systematically expanded in future research. Although this study becomes the base on which these aspects of the human spaceflight mission will be further assessed, in-depth investigations on these particular domains could reveal the challenging details and novel solutions that will mitigate those challenges.

5.4 Suggestions for Future Research

Dynamic Assessment of AI Impact: The constant advancement of AI systems means that there is an ongoing necessity to both the constant and dynamic reviews of the assessed AI technologies effect on testing devices. The studies should continually involve such different ways as real time monitoring of actions, incorporation of latest technologies and business transformations. Such method makes sure that the guidelines and measures stay up-to-date and in-sync in the dynamic environment of this AI, helping the stakeholders to come forward in the adopting of responsible AI.

Industry-Specific Studies: While the research covered a broad general perception of the testing instrument sector, it left room for investigations on a more targeted scale of individual fields of the sector. Extensive studies on such sectors as health care, finance or transport will reveal the industry-specific challenges, questions about ethics, and activities aimed at these sectors. First and foremost, considering carefully the unique aspects of each field would be most valuable for such research. Such research would provide more granular insights, enabling businesses to introduce AI that fits each industry’s individual details and intricacies (Bhatnagar et al., 2019).

Human-AI Collaboration: Delving deeper into the mechanics of human-artificial intelligence collaboration testing instruments also represents a good point of focus for the continuation of research. Realizing AI is not a substitute replacing human inputs, but it is a tool, a way of tackling biased outcomes, and a valuable resource for decision making processes are key factors that can shape functional collaborative models. Many testing areas could be supported by this research as it could indicate the right mixture of human expertise and AI capabilities which will result in faster and ethical testing.

Longitudinal Studies: Conducting long-term studies monitoring the implement of AI strategies progress and its effects on the short-term and long-term impact of proposed solutions can be very useful in the examination of the suitability and effectiveness of a project. Implementing fair processes and assessing outcomes based on the ethical guidelines can pave the way to the continuous adaptation to any emerging biases. Longitudinal studies often give an overall picture of the change process, where the newest AI technology becomes part of the medical practice and thereby organizations may use the knowledge about reality behind the approach and modify their methods (Barnawi et al., 2021).

Ultimately, the proposed research lays the groundwork for transparent AI integration across our product lineup. The offered directions for further investigation aim to not only improve on what has already been achieved but also to make the positive influence of AI into what is known, correct, and in parallel with the interests of industries and society at large.

References

Abd-Alrazaq A, Alajlani M, Alhuwail D, Schneider J, Al-Kuwari S, Shah Z, et al. Artificial intelligence in the fight against COVID-19: scoping review. 2020;22(12)

.Ahanger, T. A., Aljumah, A., &Atiquzzaman, M. (2022). State-of-the-art survey of artificial intelligent techniques for IoT security. Computer Networks, 206, 108771.

Ahmad H, Dharmadasa I, Ullah F, Babar MA. A review on c3i systems' security: Vulnerabilities, attacks, and. 2023;55(9).

Ahmed, S., Hossain, M. F., Kaiser, M. S., Noor, M. B. T., Mahmud, M., & Chakraborty, C. (2021). Artificial intelligence and machine learning for ensuring security in smartcities.In Data-Driven Mining, Learning and Analytics for Secured Smart Cities: Trendsand Advances (pp. 23-47). Cham: Springer International Publishing.

Akhtar P, Ghouri AM, Khan HUR, Amin ul Haq M, Awan U, Zahoor N, et al. Detecting fake news and disinformation using artificial intelligence and. 2023;327(2).

Alblwi A, McAlaney J, Altuwairiqi M, Stefanidis A, Phalp KT, Ali R. Procrastination on social networks: Triggers and countermeasures. 2020;53(4).

Aldahdooh A, Hamidouche W, Fezza SA, Déforges O. Adversarial example detection for DNN models: A review and experimental. 2022;55(6).

Aldhyani THH, Alkahtani H. Artificial Intelligence Algorithm-Based Economic Denial of Sustainability. 2022;22(13).

Algarni A, Thayananthan V. Autonomous vehicles: The cybersecurity vulnerabilities and countermeasures. 2022;14(12).

Alqudaihi KS, Aslam N, Khan IU, Almuhaideb AM, Alsunaidi SJ, Ibrahim NMAR, et al. Cough sound detection and diagnosis using artificial intelligence. 2021;9.

Al-Zahrani MS, Wahsheh HAM, Alsaade FW. Secure real-time artificial intelligence system against malicious QR code. 2021;2021.

Ansari MS, Alsamhi SH, Qiao Y, Ye Y, Lee B. Security of distributed intelligence in edge computing: Threats and. 2020;

Arima A, Tsutsui M, Washio T, Baba Y, Kawai T. Solid-state nanopore platform integrated with machine learning for digital. 2020;93(1).

Bahalul Haque AKM, Bhushan B, Nawar A, Talha KR, Ayesha SJ. Attacks and countermeasures in IoT based smart healthcare applications. 2022;

Bai J, Zheng D, Jia C. Safety technology risks and countermeasures in the intelligent. 2022;2022.

Barnawi A, Chhikara P, Tekchandani R, Kumar N, Alzahrani B. Artificial intelligence-enabled Internet of Things-based system for. 2021;124.

Basner M, Dinges DF, Howard K, Moore TM, Gur RC, Mühl C, et al. Continuous and intermittent artificial gravity as a countermeasure to the. 2021;12.

Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*, *54*(5), 3849-3886.

Bhatnagar D, Som S, Khatri SK. Advance persistant threat and cyber spying-the big picture, its tools,. 2019;

Bistron, M., & Piotrowski, Z. (2021). Artificial intelligence applications in military systems and their influence on sense of security of citizens. *Electronics*, *10*(7), 871.

Blauth TF, Gstrein OJ, Zwitter A. Artificial intelligence crime: An overview of malicious use and abuse of. 2022;10.

Bonfanti ME. Artificial intelligence and the offence-defence balance in cyber security. 2022;

Cai M, Luo J. Influence of COVID-19 on manufacturing industry and corresponding. 2020;25.

Caviglione L. Trends and challenges in network covert channels countermeasures. 2021;11(4).

Chakraborty C, Rajendran SR, Rehman MH. Security of Internet of Things Nodes: Challenges, Attacks, and. 2021;

Chiba T, Sei Y, Tahara Y, Ohsuga A. A countermeasure method using poisonous data against poisoning attacks on. 2021;15(2).

Chowdhury A, Karmakar G, Kamruzzaman J, Jolfaei A, Das R. Attacks on self-driving cars and their countermeasures: A survey. 2020;8.

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.

Dennetiere S, Saad H, Vernay Y, Rault P, Martin C, Clerc B. Supporting energy transition in transmission systems: An operator's. 2019;17(3).

Doukas N, Stavroulakis P, Bardis N. Review of artificial intelligence cyber threat assessment techniques for. 2021;

Esposito S, Sgandurra D, Bella G. Protecting Voice-Controllable Devices Against Self-Issued Voice Commands. 2023;

Falahati A, Shafiee E. Improve safety and security of intelligent railway transportation system. 2022;

Fallucchi F, Coladangelo M, Giuliano R, William De Luca E. Predicting employee attrition using machine learning techniques. 2020;9(4).

Fatima A, Khan TA, Abdellatif TM, Zulfiqar S, Asif M, Safi W, et al. Impact and Research Challenges of Penetrating Testing and Vulnerability. 2023;

Fysarakis K, Lekidis A, Mavroeidis V, Lampropoulos K, Lyberopoulos G, Vidal IG-M, et al. PHOENI2X--A European Cyber Resilience Framework With. 2023;

Godakanda Arachchige PGB. Detecting Business Email Compromise and Classifying for Countermeasures. 2023;

Guo, J., & Li, B. (2018). The application of medical artificial intelligence technology in rural areas of developing countries. *Health equity*, *2*(1), 174-181.

Hammi B, Zeadally S, Khatoun R, Nebhen J. Survey on smart homes: Vulnerabilities, risks, and countermeasures. 2022;117.

Hamon, R., Junklewitz, H., & Sanchez, I. (2020). Robustness and explainability of artificial intelligence. *Publications Office of the European Union*, *207*.

Han D. IoT Security in the Era of Artificial Intelligence. 2022;

Haque AB, Bhushan B, Dhiman G. Conceptualizing smart city applications: Requirements, architecture,. 2022;39(5).

Haque MA, Haque S, Kumar K, Singh NK. A comprehensive study of cyber security attacks, classification, and. 2021;

He Q, Hu B. Research on the influencing factors of film consumption and box office. 2021;2021.

He Y, Zamani E, Yevseyeva I, Luo C. Artificial Intelligence–Based Ethical Hacking for Health Information. 2023;25.

Ho LT, Gan C, Jin S, Le B. Artificial intelligence and firm performance: Does machine intelligence. 2022;15(7).

Hu W, Chang C-H, Sengupta A, Bhunia S, Kastner R, Li H. An overview of hardware security and trust: Threats, countermeasures, and. 2020;40(6).

Hu Y, Kuang W, Qin Z, Li K, Zhang J, Gao Y, et al. Artificial intelligence security: Threats and countermeasures. 2021;55(1).

Huang TV. Unmasking Concealed 5G Privacy Identity with Machine Learning and GPU in. 2020;

Jagadeesh C, Kshirsagar PR, Sarayu G, Gouthami G, Manasa B. Artificial intelligence based Fake Job Recruitment Detection Using Machine. 2021;12.

Jagielski, M., Oprea, A., Biggio, B., Liu, C., Nita-Rotaru, C., & Li, B. (2018, May). Manipulating machine learning: Poisoning attacks and countermeasures for regression learning. In *2018 IEEE symposium on security and privacy (SP)* (pp. 19-35). IEEE.

Jinnuo Z, Goyal SB, Tesfayohanis M, Omar Y. Implementation of Artificial Intelligence Image Emotion Detection. 2022;2022.

Jo JH, Sharma PK, Sicato JCS, Park JH. Emerging technologies for sustainable smart city network security: Issues,. 2019;15(4).

Jordan SB, Fenn SL, Shannon BB. Transparency as threat at the intersection of artificial intelligence and. 2020;53(10).

Keleko, A. T., Kamsu-Foguem, B., Ngouna, R. H., & Tongne, A. (2022). Artificial intelligence and real-time predictive maintenance in industry 4.0: a bibliometric analysis. *AI and Ethics*, *2*(4), 553-577.

Keller N, Whittle RS, McHenry N, Johnston A, Duncan C, Ploutz-Snyder L, et al. Virtual Reality “exergames”: A promising countermeasure to improve. 2022;13.

Kertysova, K. (2018). Artificial intelligence and disinformation: How AI changes the way disinformation is produced, disseminated, and can be countered. *Security and Human Rights*, *29*(1-4), 55-81.

Khan, A., Malik, K. M., Ryan, J., & Saravanan, M. (2023). Battling voice spoofing: a review, comparative analysis, and generalizability evaluation of state-of-the-art voice spoofing counter measures. *Artificial Intelligence Review*, 1-54.

Khandker S, Turtiainen H, Costin A, Hämäläinen T. Cybersecurity attacks on software logic and error handling within ADS-B. 2021;58(4).

Li F, He Y, Xue Q. Progress, challenges and countermeasures of adaptive learning. 2021;24(3).

Li H, Wang H. Research on the application of artificial intelligence in education. 2020;

Lin H, Lin J, Wang F. An innovative machine learning model for supply chain management. 2022;7(4).

Liu, J., Chang, H., Forrest, J. Y. L., & Yang, B. (2020). Influence of artificial intelligence on technological innovation: Evidence from the panel data of china's manufacturing sectors. *Technological Forecasting and Social Change*, *158*, 120142.

Livada B, Perić D. EO/IR imaging systems countermeasures and camouflage: capabilities and new. 2020;11536.

Luo Q, Cao Y, Liu J, Benslimane A. Localization and navigation in autonomous driving: Threats and. 2019;26(4).

Masood M, Nawaz M, Malik KM, Javed A, Irtaza A, Malik H. Deepfakes generation and detection: State-of-the-art, open challenges,. 2023;53(4).

Matloob S, Li Y, Khan KZ. Safety measurements and risk assessment of coal mining industry using. 2021;9(3).

Mihoub A, Fredj OB, Cheikhrouhou O, Derhab A, Krichen M. Denial of service attack detection and mitigation for internet of things. 2022;98.

MohanaKrishnan M, Kumar AVS, Talukdar V, Saleh OS, Irawati ID, Latip R, et al. Artificial Intelligence in Cyber Security. 2023;

Musumeci F, Fidanci AC, Paolucci F, Cugini F, Tornatore M. Machine-learning-enabled ddos attacks detection in p4 programmable. 2022;30.

Najmi KY, AlZain MA, Masud M, Jhanjhi NZ, Al-Amri J, Baz M. A survey on security threats and countermeasures in IoT to achieve users. 2021;

Namatherdhala B, Mazher N, Sriram GK. A comprehensive overview of artificial intelligence tends in education. 2022;4(7).

Oseni, A., Moustafa, N., Janicke, H., Liu, P., Tari, Z., & Vasilakos, A. (2021). Security and privacy for artificial intelligence: Opportunities and challenges. *arXiv preprint arXiv:2102.04661*.

Pajola L, Pasa L, Conti M. Threat is in the air: Machine learning for wireless network applications. 2019;

Parisi A. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI. 2019;

Payedimarri AB, Concina D, Portinale L, Canonico M, Seys D, Vanhaecht K, et al. Prediction models for public health containment measures on COVID-19 using. 2021;18(9).

Qiu H, Ding S, Liu J, Wang L, Wang X. Applications of artificial intelligence in screening, diagnosis,. 2022;29(3).

Ramadan RA, Aboshosha BW, Alshudukhi JS, Alzahrani AJ, El-Sayed A, Dessouky MM. Cybersecurity and Countermeasures at the Time of Pandemic. 2021;2021.

Rauti S, Laato S, Pitkämäki T. Man-in-the-browser attacks against IoT devices: a study of smart homes. 2021;

Repede Ștefan E. Researching disinformation using artificial intelligence techniques: 2023;12(2).

Rugo A, Ardagna CA, Ioini NE. A security review in the UAVNet era: threats, countermeasures, and gap. 2022;55(1).

Sabir B, Ullah F, Babar MA, Gaire R. Machine learning for detecting data exfiltration: A review. 2021;54(3).

Sadiq A, Anwar M, Butt RA, Masud F, Shahzad MK, Naseem S, et al. A review of phishing attacks and countermeasures for internet of. 2021;3(5).

Schwartz R, Vassilev A, Greene K, Perine L, Burt A, Hall P. Towards a standard for identifying and managing bias in artificial. 2022;1270(10.6028).

Schwartz, R., Vassilev, A., Greene, K., Perine, L., Burt, A., & Hall, P. (2022). Towards a standard for identifying and managing bias in artificial intelligence. *NIST special publication*, *1270*(10.6028).

Seljan S, Tolj N, Dunđer I. Information Extraction from Security-Related Datasets. 2023;

Shah H, Shah S, Tanwar S, Gupta R, Kumar N. Fusion of AI techniques to tackle COVID-19 pandemic: models, incidence. 2021;

Shang W. The Intellectualized Disposal System of Cognitive Domain's Confrontation. 2023;

Sharifi, A., Ahmadi, M., & Ala, A. (2021). The impact of artificial intelligence and digital style on industry and energy post-COVID-19 pandemic. *Environmental Science and Pollution Research*, *28*, 46964-46984.

Siddiqi MA, Pak W, Siddiqi MA. A study on the psychology of social engineering-based cyberattacks and. 2022;12(12).

Singhal, V., Jain, S. S., Anand, D., Singh, A., Verma, S., Rodrigues, J. J., ... &Iwendi, C. (2020). Artificial intelligence enabled road vehicle-train collision risk assessment framework for unmanned railway level crossings. *IEEE Access*, *8*, 113790-113806.

Sun J, Cao Y, Chen QA, Mao ZM. Towards robust LiDAR-based perception in autonomous driving: General. 2020;

Surma J. Hacking machine learning: towards the comprehensive taxonomy of attacks. 2020;

Swathi V, Shereesha M, Sravya K, Kumar RA, Allala K. Influence Based Defence Against Data Poisoning Attacks In Online Learning. 2023;

Swessi D, Idoudi H. A survey on internet-of-things security: threats and emerging. 2022;124(2).

Taddeo, M., McCutcheon, T., &Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), 557-560.

Tharayil KS, Farshteindiker B, Eyal S, Hasidim N, Hershkovitz R, Houri S, et al. Sensor defense in-software (SDI): Practical software-based detection of. 2020;95.

Thomas S, Abraham A, Baldwin J, Piplani S, Petrovsky N. Artificial intelligence in vaccine and drug design. 2022;

Tlili F, Fourati LC, Ayed S, Ouni B. Investigation on vulnerabilities, threats and attacks prohibiting UAVs. 2022;129.

Truong TC, Diep QB, Zelinka I. Artificial intelligence in the cyber domain: Offense and defense. 2020;12(3).

Tsiknas K, Taketzis D, Demertzis K, Skianis C. Cyber threats to industrial IoT: a survey on attacks and countermeasures. 2021;2(1).

Varian, H. (2018). Artificial intelligence, economics, and industrial organization. In *The economics of artificial intelligence: an agenda* (pp. 399-419). University of Chicago Press.

Waheed N, He X, Ikram M, Usman M, Hashmi SS, Usman M. Security and privacy in IoT using machine learning and blockchain: Threats. 2020;53(6).

Wang C, Chen J, Yang Y, Ma X, Liu J. Poisoning attacks and countermeasures in intelligent networks: Status quo. 2022;8(2).

Wang H, Sayadi H, Dinakarrao SMP, Sasan A, Rafatirad S, Homayoun H. Enabling micro ai for securing edge devices at hardware level. 2021;11(4).

Waqas M, Tu S, Halim Z, Rehman SU, Abbas G, Abbas ZH. The role of artificial intelligence and machine learning in wireless. 2022;55(7).

Wen Y, Lu F, Liu Y, Huang X. Attacks and countermeasures on blockchains: A survey from layering. 2021;191.

Whelan J, Almehmadi A, El-Khatib K. Artificial intelligence for intrusion detection systems in unmanned aerial. 2022;99.

World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. 2021;

Xu G, Li H, Ren H, Yang K, Deng RH. Data security issues in deep learning: Attacks, countermeasures, and. 2019;57(11).

Xue M,Yuan C, Wu H, Zhang Y, Liu W. Machine learning security: Threats, countermeasures, and evaluations. 2020;8.

Yaacoub J-P, Noura H, Salman O, Chehab A. Security analysis of drones systems: Attacks, limitations, and. 2020;11.

Yaacoub J-PA, Noura HN, Salman O, Chehab A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and. 2022;

Yamin MM, Ullah M, Ullah H, Katt B, Hijji M, Muhammad K. Mapping Tools for Open Source Intelligence with Cyber Kill Chain for. 2022;10(12).

Yan Z, Wu J, Li G, Li S, Guizani M. Deep neural backdoor in semi-supervised learning: Threats and. 2021;16.

Yang Z, Chen Z, Lee K, Owens E, Boufadel MC, An C, et al. Decision support tools for oil spill response (OSR-DSTs): Approaches,.2021;167.

Yang, K. C., Varol, O., Davis, C. A., Ferrara, E., Flammini, A., & Menczer, F. (2019). Arming the public with artificial intelligence to counter social bots. *Human Behavior and Emerging Technologies*, *1*(1), 48-61.

Yue P, An J, Zhang J, Pan G, Wang S, Xiao P, et al. On the security of LEO satellite communication systems: Vulnerabilities, 2022;

Zagrouba R, Alhajri R. Machine learning based attacks detection and countermeasures in IoT. 2021;13(2).

Zaman A, Ren B, Liu X. Artificial intelligence-aided automated detection of railroad trespassing. 2019;2673(7).

Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. *Ieee Access*, *9*, 94668-94690.

Zhang J, Zhang Z-M. Ethics and governance of trustworthy medical artificial intelligence. 2023;23(1).

Zhang X, Zhang X, Liu W, Zou X, Sun M, Zhao J. Waveform level adversarial example generation for joint attacks against. 2022;116.

Zhao S. Impact of COVID 19 Pandemic and Big Data on China's International Trade: 2022;10.

Zhou J. Analysis and countermeasures of green finance development under carbon. 2022;10(2).

Zhu K, Zheng L. Based on Artificial Intelligence in the Judicial Field Operation Status. 2021;2021.

Appendices

Appendix I: Critical Appraisal of Eligible Qualitative Research

Citation	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
DuckettSJ. 2012.	N	N	N	Y	N	Y	Y	U	Y	Y
Putra SD, Sumari ADW, Ahmad AS, SutiknoS, KurniawanY.2020.	Y	Y	N	Y	N	Y	Y	Y	Y	Y
ZamanS, Alhazmi K, Aseeri MA, Ahmed MR, Khan RT, Kaiser MS, et al. 2021.	Y	N	Y	N	N	Y	N	Y	N	U
Fengying Li YH and QX.	N/A	N/A	N	N	N/A	N/A	N	Y	N/A	Y
Zhu K, Zheng L. 2021.	Y	N	Y	N	N	U	U	Y	Y	U
Hu Y, Kuang W, Qin Z, Li K, Zhang J, Gao Y, et al. 2021.	Y	N	N	Y	Y	Y	Y	N	Y	Y
%	66.66	16.66	33.33	50.0	16.66	66.66	50.0	66.66	66.66	66.66

Appendix II: Critical Appraisal of Eligible Randomized Controlled Trial

Citation	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13
Wang C, Chen J, Yang Y, Ma X, Liu J. 2022.	Y	N	U	Y	N	U	U	N	Y	N	U	U	N/A
Thomas S, Abraham A, Baldwin J, Piplani S, Petrovsky N. 2022.	Y	N	Y	N	Y	Y	Y	Y	U	Y	N	Y	Y
Bai J, Zheng D, Jia C. 2022.	Y	N	U	Y	N	U	U	N	N	N	U	N/A	Y
Xue M, Yuan C, Wu H, Zhang Y, Liu W. 2020.	Y	N	U	Y	Y	N	N	Y	N	U	N/A	U	N
Zhao S. 2022.	Y	N	U	N	N	Y	Y	Y	N	U	Y	Y	N
Yaacoub J-PA, Noura HN, Salman O, Chehab A. 2022.	Y	N	U	N	N	Y	U	Y	N	N	U	N	U
Fatima A,	Y	N	Y	Y	N	U	N/	U	Y	N	U	N	Y

Khan TA, Abdellatif TM, Zulfiqar S, Asif M, Safi W, et al. 2023.							A						
Bhatnagar D, Som S, Khatri SK. 2019.	Y	N	U	Y	N	Y	N	U	N/A	U	N	Y	N
Swessi D, Idoudi H. 2022.	Y	N	N	N	Y	N	N	U	Y	Y	N	N	N/A
Luo Q, Cao Y, Liu J, Benslimane A. 2019.	Y	N	U	U	N	N/A	U	U	N	U	N	N/A	Y
Cai M, Luo J. 2020.	Y	N	U	Y	Y	N	N/A	N	U	Y	Y	Y	N
Hu W, Chang C-H, Sengupta A, Bhunia S, Kastner R, Li H. 2020.	Y	N	U	N	U	N	N/A	U	N	Y	N	U	N/A
Surma J. 2020.	Y	N	N	Y	N	N	N	U	N	Y	Y	U	Y
Li F, He Y, Xue Q.	Y	N	U	U	U	N/A	N/A	N	N	N	Y	N	U

2021.													
Sabir B, Ullah F, Babar MA, Gaire R. 2021.	Y	N	U	U	N/A	U	N	Y	Y	Y	N	Y	Y
Doukas N, Stavroulakis P, Bardis N. 2021.	Y	N	U	N	Y	Y	N	U	U	U	N	N	U
Chakraborty C, Rajendran SR, Rehman MH. 2021.	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y	Y
Falahati A, Shafiee E. 2022.	Y	N	Y	N	U	U	N	U	N	N/A	N	U	N
Livada B, Perić D. 2020.	Y	N	Y	U	Y	Y	Y	N	U	U	N/A	Y	Y
Waheed N, He X, Ikram M, Usman M, Hashmi SS, Usman M. 2020.	N	U	N/A	N	N	U	N	U	N/A	N	N/A	N	Y
Ansari MS, Alsamhi SH, Qiao Y, Ye	Y	N	U	Y	N	N	Y	Y	N	Y	Y	Y	Y

Y, Lee B. 2020.													
Yue P, An J, Zhang J, Pan G, Wang S, Xiao P, et al. 2022.	Y	N	Y	N	N	U	U	N/A	U	N	N	U	N/A
Keller N, Whittle RS, McHenry N, Johnston A, Duncan C, Ploutz-Snyder L, et al. 2022.	Y	N	Y	Y	Y	U	N	U	U	Y	Y	Y	Y
Esposito S, Sgandurra D, Bella G. 2023.	Y	Y	N	U	N/A	N	U	N/A	N	U	U	U	N
Algarni A, Thayanantha n V. 2022.	Y	Y	Y	Y	Y	Y	N	U	Y	Y	Y	Y	N
Zhang J, Zhang Z-M. 2023.	Y	N	Y	Y	N	U	U	U	N	U	N/A	Y	N
Repede Ștefan E. 2023.	Y	Y	Y	Y	Y	Y	Y	N	Y	N	U	Y	Y
Najmi KY,	Y	N	U	N	U	N/	U	N	U	N	Y	N	U

AlZain MA, Masud M, Jhanjhi NZ, Al-Amri J, Baz M. 2021.						A							
Sadiq A, Anwar M, Butt RA, Masud F, Shahzad MK, Naseem S, et al. 2021.	Y	N	U	Y	U	U	Y	Y	Y	Y	Y	Y	Y
Namatherdhala B, Mazher N, Sriram GK. 2022.	U	N	U	N/A	N	U	N/A	U	N	Y	N	U	Y
Zhang X, Zhang X, Liu W, Zou X, Sun M, Zhao J. 2022.	Y	N	Y	Y	Y	Y	N	Y	Y	N	Y	Y	Y
Basner M, Dinges DF, Howard K, Moore TM, Gur RC, Mühl C, et	N	N	N	Y	Y	N	Y	N	N	Y	N	Y	N

al. 2021.													
Yaacoub J-P, Noura H, Salman O, Chehab A. 2020.	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Qiu H, Ding S, Liu J, Wang L, Wang X. 2022.	Y	N	U	Y	N	N	Y	N	N	U	N/A	U	N
Yamin MM, Ullah M, Ullah H, Katt B, Hijji M, Muhammad K. 2022.	Y	Y	U	N/A	N	U	N	N	N	N	U	N/A	U
Ramadan RA, Aboshosha BW, Alshudukhi JS, Alzahrani AJ, El-Sayed A, Dessouky MM. 2021.	U	N	N	N	N	Y	U	U	Y	U	N	Y	Y
Seljan S, Tolj N,	Y	N	Y	Y	Y	N	U	N/A	Y	Y	Y	N	Y

Dunđer I. 2023.													
Akhtar P, Ghouri AM, Khan HUR, Amin ul Haq M, Awan U, Zahoor N, et al. 2023.	Y	N	Y	N	Y	N	N	N	N	Y	N	Y	N
Alqudaihi KS, Aslam N, Khan IU, Almuhaideb AM, Alsunaidi SJ, Ibrahim NMAR, et al. 2021.	Y	N	N	N	Y	N	U	U	N	U	U	N	N
Fallucchi F, Coladangelo M, Giuliano R, William De Luca E. 2020.	N	U	N/A	N	U	N/A	N	U	N/A	N	U	N/A	N
Khandker S, Turtiainen H, Costin A, Hämäläinen T. 2021.	Y	Y	U	N	Y	Y	Y	Y	N	Y	N	Y	Y
Masood M,	Y	N	N	Y	N	N	U	U	N	U	N/	N	U

Nawaz M, Malik KM, Javed A, Irtaza A, Malik H. 2023.											A		
Zagrouba R, Alhajri R. 2021.	Y	Y	Y	Y	Y	Y	Y	N	U	N	N	Y	Y
Rugo A, Ardagna CA, Ioini NE. 2022.	Y	Y	Y	Y	Y	N	Y	N	N/A	Y	Y	N/A	N
Rauti S, Laato S, Pitkämäki T. 2021.	N	U	N	N	U	U	N	U	N	N	U	U	N/A
Jagadeesh C, Kshirsagar PR, Sarayu G, Gouthami G, Manasa B. 2021.	Y	N	Y	N	N	N	Y	N	N	Y	U	N	Y
Tsiknas K, Taketzis D, Demertzis K, Skianis C. 2021.	Y	Y	N	Y	N/A	Y	Y	N	Y	Y	N	Y	Y

Al-Zahrani MS, Wahsheh HAM, AlsaadeFW. 2021.	N	U	N/A	N	N/A	N	U	U	Y	N	N	U	Y
Xu G, Li H, Ren H, Yang K, Deng RH. 2019.	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y
MohanaKrishnan M, Kumar AVS, Talukdar V, Saleh OS, Irawati ID, Latip R, et al. 2023.	N	U	N	U	N/A	N	N/A	U	N	U	N/A	U	N
Parisi A. 2019.	Y	N	Y	Y	Y	N	Y	Y	N	Y	Y	Y	Y
Lin H, Lin J, Wang F. 2022.	U	N	Y	Y	N	N	N	U	N/A	N	U	N	Y
World Health Organizatio n. 2021.	Y	Y	Y	Y	N	N	Y	Y	N	U	Y	Y	Y
Payedimarri AB,	Y	N	Y	N	U	N	U	N	N	U	N	N	N

Concina D, Portinale L, Canonico M, Seys D, Vanhaecht K, et al. 2021.													
Jinnuo Z, Goyal SB, Tesfayohanis M, Omar Y. 2022.	Y	Y	Y	Y	Y	N	U	Y	N	Y	N	Y	Y
Shang W. 2023.	Y	N	U	N	U	N	U	N	Y	N	Y	N	U
Jordan SB, Fenn SL, Shannon BB. 2020.	Y	Y	Y	N	U	Y	Y	N	Y	Y	Y	N	Y
Blauth TF, Gstrein OJ, Zwitter A. 2022.	N	U	U	N	U	N	N	U	N	Y	Y	N	U
Swathi V, Shereesha M, Sravya K, Kumar RA, Allala K. 2023.	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y
He Y, Zamani E, Yevseyeva	N	U	Y	N	U	N/A	N	U	N/A	U	U	N/A	N

I, Luo C. 2023.													
Schwartz R, Vassilev A, Greene K, Perine L, Burt A, Hall P. 2022.	Y	Y	Y	Y	N	U	Y	Y	Y	N	U	Y	Y
Waqas M, Tu S, Halim Z, Rehman SU, Abbas G, Abbas ZH. 2022.	N	N	Y	N	Y	N/A	N	U	U	U	N	N	U
Abd-Alrazaq A, Alajlani M, Alhuwail D, Schneider J, Al-Kuwari S, Shah Z, et al. 2020.	N	U	N	N/A	N/A	U	N	Y	N	N	Y	N	U
Barnawi A, Chhikara P, Tekchandani R, Kumar N, Alzahrani B. 2021.	Y	N	Y	N	Y	N	N	N	Y	Y	N	Y	Y
Siddiqi MA, Pak W, Siddiqi MA.	Y	Y	Y	Y	N	U	Y	N	N	Y	Y	Y	N

2022.													
Sun J, Cao Y, Chen QA, Mao ZM. 2020.	Y	N	Y	N	U	U	Y	N/A	N	N/A	Y	N	U
Pajola L, Pasa L, Conti M. 2019.	Y	Y	Y	Y	Y	Y	N	Y	N/A	Y	N	Y	Y
Jo JH, Sharma PK, Sicato JCS, Park JH. 2019.	Y	N	Y	Y	N	N	N	N	N	Y	U	U	U
Zhou J. 2022.	Y	N	U	U	U	N	U	N/A	U	U	N	U	N/A
Bonfanti ME. 2022.	Y	N	U	N	Y	Y	N	U	N/A	N	Y	Y	N
Wang H, Sayadi H, Dinakarrao SMP, Sasan A, Rafatirad S, Homayoun H. 2021.	Y	N	U	Y	Y	Y	Y	Y	N	Y	N	Y	Y
Haque AB, Bhushan B, Dhiman G. 2022.	N	U	Y	Y	N	U	N	U	U	U	N	N	U

Aldhyani THH, Alkahtani H. 2022.	Y	N	U	Y	Y	Y	Y	Y	N	U	Y	Y	Y
Hammi B, Zeadally S, Khatoun R, Nebhen J. 2022.	N	N	U	Y	Y	U	U	U	U	N	U	N	U
Alblwi A, McAlaney J, Altuwairiqi M, Stefanidis A, Phalp KT, Ali R. 2020.	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y
Caviglione L. 2021.	Y	N	U	Y	N	N	U	U	N	N/A	N	U	U
Han D. 2022.	Y	Y	Y	Y	Y	Y	N/A	N	Y	Y	Y	Y	Y
Mihoub A, Fredj OB, Cheikhrouhou O, Derhab A, Krichen M. 2022.	N	U	N	N/A	N	N	U	Y	Y	N	Y	Y	N/A
Huang TV. 2020.	N	U	Y	Y	N/A	N/A	Y	Y	Y	Y	Y	Y	Y

Arima A, Tsutsui M, Washio T, Baba Y, Kawai T. 2020.	U	U	U	N	U	N/A	N/A	Y	U	U	U	N	Y
Fysarakis K, Lekidis A, Mavroeidis V, Lampropoulos K, Lyberopoulos G, Vidal IG-M, et al. 2023.	Y	N	Y	N	Y	N	Y	Y	Y	Y	N	Y	Y
Ho LT, Gan C, Jin S, Le B. 2022.	N	U	U	U	N	Y	U	N/A	U	N	Y	N	U
He Q, Hu B. 2021.	Y	Y	Y	N	U	U	Y	U	Y	Y	Y	Y	N
Chowdhury A, Karmakar G, Kamruzzaman J, Jolfaei A, Das R. 2020.	N	U	N	U	Y	N	N	N	N/A	U	Y	Y	N
Aldahdooh A,	Y	N	U	Y	Y	Y	Y	Y	N	N	Y	N	U

Hamidouche W, Fezza SA, Déforges O. 2022.													
Wen Y, Lu F, Liu Y, Huang X. 2021.	N	N	U	N/A	N	U	N/A	N	U	N/A	Y	Y	Y
Ahmad H, Dharmadasa I, Ullah F, Babar MA. 2023.	Y	N	Y	Y	N	N/A	Y	Y	Y	N	Y	Y	N
Haque MA, Haque S, Kumar K, Singh NK. 2021.	U	U	N	N	N/A	N/A	N	N	U	U	N/A	U	N
Zaman A, Ren B, Liu X. 2019.	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Godakanda Arachchige PGB. 2023.	N	U	N	N	N	Y	N/A	U	U	N	N	U	N
Yan Z, Wu J, Li G, Li S, Guizani M. 2021.	Y	Y	Y	Y	Y	N	N	Y	N	Y	Y	Y	Y
Matloob S,	Y	N	Y	N	N	U	N/	U	N	U	N	U	N/

Li Y, Khan KZ. 2021.							A						A
Yang Z, Chen Z, Lee K, Owens E, Boufadel MC, An C, et al. 2021.	N	U	N/A	N	N/A	N	U	N/A	N	U	N/A	N	U
Li H, Wang H. 2020.	Y	N	Y	Y	Y	Y	Y	N	U	N	N	N	Y
Truong TC, Diep QB, Zelinka I. 2020.	U	N/A	N	Y	N/A	Y	U	U	Y	N	N	N	U
Bahalul Haque AKM, Bhushan B, Nawar A, Talha KR, Ayesha SJ. 2022.	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Shah H, Shah S, Tanwar S, Gupta R, Kumar N. 2021.	U	N/A	N/A	U	N	N	Y	Y	U	U	N	Y	Y
Whelan J, Almehmadi A, El-Khatib	Y	N	Y	N	Y	Y	N	U	U	N	N	U	Y

K. 2022.													
Tlili F, Fourati LC, Ayed S, Ouni B. 2022.	Y	Y	Y	Y	N	U	N	Y	Y	Y	N	N	Y
Musumeci F, Fidanci AC, Paolucci F, Cugini F, Tornatore M. 2022.	N/A	N	N	Y	U	U	U	N	U	N/A	U	U	N
Chiba T, Sei Y, Tahara Y, Ohsuga A. 2021.	Y	N	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Tharayil KS, Farshteindiker B, Eyal S, Hasidim N, Hershkovitz R, Houri S, et al. 2020.	N	U	Y	U	N/A	U	N	N/A	U	N	N/A	U	N
Dennetiere S, Saad H, Vernay Y, Rault P, Martin C, Clerc B. 2019.	Y	N	Y	Y	Y	Y	Y	Y	N	Y	Y	U	Y

%	71.84	22.33	46.6	49.51	38.83	31.06	33.98	31.06	30.09	39.8	39.8	45.63	48.54

Appendix III: List of studies <u>included</u> following title and abstract screening

Abd-Alrazaq A, Alajlani M, Alhuwail D, Schneider J, Al-Kuwari S, Shah Z, et al. Artificial intelligence in the fight against COVID-19: scoping review. 2020;22(12).

Ahmad H, Dharmadasa I, Ullah F, Babar MA. A review on c3i systems' security: Vulnerabilities, attacks, and. 2023;55(9).

Akhtar P, Ghouri AM, Khan HUR, Amin ul Haq M, Awan U, Zahoor N, et al. Detecting fake news and disinformation using artificial intelligence and. 2023;327(2).

Al-Zahrani MS, Wahsheh HAM, Alsaade FW. Secure real-time artificial intelligence system against malicious QR code. 2021;2021.

Alblwi A, McAlaney J, Altuwairiqi M, Stefanidis A, Phalp KT, Ali R. Procrastination on social networks: Triggers and countermeasures. 2020;53(4).

Aldahdooh A, Hamidouche W, Fezza SA, Déforges O. Adversarial example detection for DNN models: A review and experimental. 2022;55(6).

Aldhyani THH, Alkahtani H. Artificial Intelligence Algorithm-Based Economic Denial of Sustainability. 2022;22(13).

Algarni A, Thayananthan V. Autonomous vehicles: The cybersecurity vulnerabilities and countermeasures. 2022;14(12).

Alqudaihi KS, Aslam N, Khan IU, Almuhaideb AM, Alsunaidi SJ, Ibrahim NMAR, et al. Cough sound detection and diagnosis using artificial intelligence. 2021;9.

Ansari MS, Alsamhi SH, Qiao Y, Ye Y, Lee B. Security of distributed intelligence in edge computing: Threats and. 2020;

Arima A, Tsutsui M, Washio T, Baba Y, Kawai T. Solid-state nanopore platform integrated with machine learning for digital. 2020;93(1).

Bahalul Haque AKM, Bhushan B, Nawar A, Talha KR, Ayesha SJ. Attacks and countermeasures in IoT based smart healthcare applications. 2022;

Bai J, Zheng D, Jia C. Safety technology risks and countermeasures in the intelligent. 2022;2022.

Barnawi A, Chhikara P, Tekchandani R, Kumar N, Alzahrani B. Artificial intelligence-enabled Internet of Things-based system for. 2021;124.

Basner M, Dinges DF, Howard K, Moore TM, Gur RC, Mühl C, et al. Continuous and intermittent artificial gravity as a countermeasure to the. 2021;12.

Bhatnagar D, Som S, Khatri SK. Advance persistant threat and cyber spying-the big picture, its tools. 2019;

Blauth TF, Gstrein OJ, Zwitter A. Artificial intelligence crime: An overview of malicious use and abuse of. 2022;10.

Bonfanti ME. Artificial intelligence and the offence-defence balance in cyber security. 2022;

Cai M, Luo J. Influence of COVID-19 on manufacturing industry and corresponding. 2020;25.

Caviglione L. Trends and challenges in network covert channels countermeasures. 2021;11(4).

Chakraborty C, Rajendran SR, Rehman MH. Security of Internet of Things Nodes: Challenges, Attacks, and. 2021;

Chiba T, Sei Y, Tahara Y, Ohsuga A. A countermeasure method using poisonous data against poisoning attacks on. 2021;15(2).

Chowdhury A, Karmakar G, Kamruzzaman J, Jolfaei A, Das R. Attacks on self-driving cars and their countermeasures: A survey. 2020;8.

Dennetiere S, Saad H, Vernay Y, Rault P, Martin C, Clerc B. Supporting energy transition in transmission systems: An operator's. 2019;17(3).

Doukas N, Stavroulakis P, Bardis N. Review of artificial intelligence cyber threat assessment techniques for. 2021;

Esposito S, Sgandurra D, Bella G. Protecting Voice-Controllable Devices Against Self-Issued Voice Commands. 2023;

Falahati A, Shafiee E. Improve safety and security of intelligent railway transportation system. 2022;

Fallucchi F, Coladangelo M, Giuliano R, William De Luca E. Predicting employee attrition using machine learning techniques. 2020;9(4).

Fatima A, Khan TA, Abdellatif TM, Zulfiqar S, Asif M, Safi W, et al. Impact and Research Challenges of Penetrating Testing and Vulnerability. 2023.

Fysarakis K, Lekidis A, Mavroeidis V, Lampropoulos K, Lyberopoulos G, Vidal IG-M, et al. PHOENI2X--A European Cyber Resilience Framework With. 2023;

Godakanda Arachchige PGB. Detecting Business Email Compromise and Classifying for Countermeasures. 2023;

Hammi B, Zeadally S, Khatoun R, Nebhen J. Survey on smart homes: Vulnerabilities, risks, and countermeasures. 2022;117.

Han D. IoT Security in the Era of Artificial Intelligence. 2022;

Haque AB, Bhushan B, Dhiman G. Conceptualizing smart city applications: Requirements, architecture. 2022;39(5).

Haque MA, Haque S, Kumar K, Singh NK. A comprehensive study of cyber security attacks, classification, and. 2021;

He Q, Hu B. Research on the influencing factors of film consumption and box office. 2021;2021.

He Y, Zamani E, Yevseyeva I, Luo C. Artificial Intelligence–Based Ethical Hacking for Health Information. 2023;25.

Ho LT, Gan C, Jin S, Le B. Artificial intelligence and firm performance: Does machine intelligence. 2022;15(7).

Hu W, Chang C-H, Sengupta A, Bhunia S, Kastner R, Li H. An overview of hardware security and trust: Threats, countermeasures, and. 2020;40(6).

Hu Y, Kuang W, Qin Z, Li K, Zhang J, Gao Y, et al. Artificial intelligence security: Threats and countermeasures. 2021;55(1).

Huang TV. Unmasking Concealed 5G Privacy Identity with Machine Learning and GPU in. 2020;

Jagadeesh C, Kshirsagar PR, Sarayu G, Gouthami G, Manasa B. Artificial intelligence based Fake Job Recruitment Detection Using Machine. 2021;12.

Jinnuo Z, Goyal SB, Tesfayohanis M, Omar Y. Implementation of Artificial Intelligence Image Emotion Detection. 2022;2022.

Jo JH, Sharma PK, Sicato JCS, Park JH. Emerging technologies for sustainable smart city network security: Issues. 2019;15(4).

Jordan SB, Fenn SL, Shannon BB. Transparency as threat at the intersection of artificial intelligence and. 2020;53(10).

Keller N, Whittle RS, McHenry N, Johnston A, Duncan C, Ploutz-Snyder L, et al. Virtual Reality “exergames”: A promising countermeasure to improve. 2022;13.

Khandker S, Turtiainen H, Costin A, Hämäläinen T. Cybersecurity attacks on software logic and error handling within ADS-B. 2021;58(4).

Li F, He Y, Xue Q. Progress, challenges and countermeasures of adaptive learning. 2021;24(3).

Li H, Wang H. Research on the application of artificial intelligence in education. 2020;

Lin H, Lin J, Wang F. An innovative machine learning model for supply chain management. 2022;7(4).

Livada B, Perić D. EO/IR imaging systems countermeasures and camouflage: capabilities and new. 2020;11536.

Luo Q, Cao Y, Liu J, Benslimane A. Localization and navigation in autonomous driving: Threats and. 2019;26(4).

Masood M, Nawaz M, Malik KM, Javed A, Irtaza A, Malik H. Deepfakes generation and detection: State-of-the-art, open challenges. 2023;53(4).

Matloob S, Li Y, Khan KZ. Safety measurements and risk assessment of coal mining industry using. 2021;9(3).

Mihoub A, Fredj OB, Cheikhrouhou O, Derhab A, Krichen M. Denial of service attack detection and mitigation for internet of things. 2022;98.

MohanaKrishnan M, Kumar AVS, Talukdar V, Saleh OS, Irawati ID, Latip R, et al. Artificial Intelligence in Cyber Security. 2023;

Musumeci F, Fidanci AC, Paolucci F, Cugini F, Tornatore M. Machine-learning-enabled ddos attacks detection in p4 programmable. 2022;30.

Najmi KY, AlZain MA, Masud M, Jhanjhi NZ, Al-Amri J, Baz M. A survey on security threats and countermeasures in IoT to achieve users. 2021;

Namatherdhala B, Mazher N, Sriram GK. A comprehensive overview of artificial intelligence tends in education. 2022;4(7).

Pajola L, Pasa L, Conti M. Threat is in the air: Machine learning for wireless network applications. 2019;

Parisi A. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI. 2019;

Payedimarri AB, Concina D, Portinale L, Canonico M, Seys D, Vanhaecht K, et al. Prediction models for public health containment measures on COVID-19 using. 2021;18(9).

Qiu H, Ding S, Liu J, Wang L, Wang X. Applications of artificial intelligence in screening, diagnosis. 2022;29(3).

Ramadan RA, Aboshosha BW, Alshudukhi JS, Alzahrani AJ, El-Sayed A, Dessouky MM. Cybersecurity and Countermeasures at the Time of Pandemic. 2021;2021.

Rauti S, Laato S, Pitkämäki T. Man-in-the-browser attacks against IoT devices: a study of smart homes. 2021;

Repede Ștefan E. Researching disinformation using artificial intelligence techniques: 2023;12(2).

Rugo A, Ardagna CA, Ioini NE. A security review in the UAVNet era: threats, countermeasures, and gap. 2022;55(1).

Sabir B, Ullah F, Babar MA, Gaire R. Machine learning for detecting data exfiltration: A review. 2021;54(3).

Sadiq A, Anwar M, Butt RA, Masud F, Shahzad MK, Naseem S, et al. A review of phishing attacks and countermeasures for internet of. 2021;3(5).

Schwartz R, Vassilev A, Greene K, Perine L, Burt A, Hall P. Towards a standard for identifying and managing bias in artificial. 2022;1270(10.6028).

Seljan S, Tolj N, Dunđer I. Information Extraction from Security-Related Datasets. 2023;

Shah H, Shah S, Tanwar S, Gupta R, Kumar N. Fusion of AI techniques to tackle COVID-19 pandemic: models, incidence. 2021;

Shang W. The Intellectualized Disposal System of Cognitive Domain's Confrontation. 2023;

Siddiqi MA, Pak W, Siddiqi MA. A study on the psychology of social engineering-based cyberattacks and. 2022;12(12).

Sun J, Cao Y, Chen QA, Mao ZM. Towards robust LiDAR-based perception in autonomous driving: General. 2020;

Surma J. Hacking machine learning: towards the comprehensive taxonomy of attacks. 2020;

Swathi V, Shereesha M, Sravya K, Kumar RA, Allala K. Influence Based Defence Against Data Poisoning Attacks In Online Learning. 2023;

Swessi D, Idoudi H. A survey on internet-of-things security: threats and emerging. 2022;124(2).

Tharayil KS, Farshteindiker B, Eyal S, Hasidim N, Hershkovitz R, Houri S, et al. Sensor defense in-software (SDI): Practical software-based detection of. 2020;95.

Thomas S, Abraham A, Baldwin J, Piplani S, Petrovsky N. Artificial intelligence in vaccine and drug design. 2022;

Tlili F, Fourati LC, Ayed S, Ouni B. Investigation on vulnerabilities, threats and attacks prohibiting UAVs. 2022;129.

Truong TC, Diep QB, Zelinka I. Artificial intelligence in the cyber domain: Offense and defense. 2020;12(3).

Tsiknas K, Taketzis D, Demertzis K, Skianis C. Cyber threats to industrial IoT: a survey on attacks and countermeasures. 2021;2(1).

Waheed N, He X, Ikram M, Usman M, Hashmi SS, Usman M. Security and privacy in IoT using machine learning and blockchain: Threats. 2020;53(6).

Wang C, Chen J, Yang Y, Ma X, Liu J. Poisoning attacks and countermeasures in intelligent networks: Status quo. 2022;8(2).

Wang H, Sayadi H, Dinakarrao SMP, Sasan A, Rafatirad S, Homayoun H. Enabling micro ai for securing edge devices at hardware level. 2021;11(4).

Waqas M, Tu S, Halim Z, Rehman SU, Abbas G, Abbas ZH. The role of artificial intelligence and machine learning in wireless. 2022;55(7).

Wen Y, Lu F, Liu Y, Huang X. Attacks and countermeasures on blockchains: A survey from layering. 2021;191.

Whelan J, Almehmadi A, El-Khatib K. Artificial intelligence for intrusion detection systems in unmanned aerial. 2022;99.

World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. 2021;

Xu G, Li H, Ren H, Yang K, Deng RH. Data security issues in deep learning: Attacks, countermeasures, and. 2019;57(11).

Xue M, Yuan C, Wu H, Zhang Y, Liu W. Machine learning security: Threats, countermeasures, and evaluations. 2020;8.

Yaacoub J-P, Noura H, Salman O, Chehab A. Security analysis of drone systems: Attacks, limitations, and. 2020;11.

Yaacoub J-PA, Noura HN, Salman O, Chehab A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and. 2022;

Yamin MM, Ullah M, Ullah H, Katt B, Hijji M, Muhammad K. Mapping Tools for Open Source Intelligence with Cyber Kill Chain for. 2022;10(12).

Yan Z, Wu J, Li G, Li S, Guizani M. Deep neural backdoor in semi-supervised learning: Threats and. 2021;16.

Yang Z, Chen Z, Lee K, Owens E, Boufadel MC, An C, et al. Decision support tools for oil spill response (OSR-DSTs): Approaches. 2021;167.

Yue P, An J, Zhang J, Pan G, Wang S, Xiao P, et al. On the security of LEO satellite communication systems: Vulnerabilities. 2022;

Zagrouba R, Alhajri R. Machine learning based attacks detection and countermeasures in IoT. 2021;13(2).

Zaman A, Ren B, Liu X. Artificial intelligence-aided automated detection of railroad trespassing. 2019;2673(7).

Zhang J, Zhang Z-M. Ethics and governance of trustworthy medical artificial intelligence. 2023;23(1).

Zhang X, Zhang X, Liu W, Zou X, Sun M, Zhao J. Waveform level adversarial example generation for joint attacks against. 2022;116.

Zhao S. Impact of COVID 19 Pandemic and Big Data on China's International Trade: 2022;10.

Zhou J. Analysis and countermeasures of green finance development under carbon. 2022;10(2).

Zhu K, Zheng L. Based on Artificial Intelligence in the Judicial Field Operation Status. 2021;2021.

Appendix IV: List of studies excluded following title and abstract screening

Abir SMAA, Islam SN, Anwar A, Mahmood AN, Oo AMT. Building resilience against COVID-19 pandemic using artificial. 2020;1(2).

Adel M, Yokoyama H, Tatsuta H, Nomura T, Ando Y, Nakamura T, et al. Early damage detection of fatigue failure for RC deck slabs under wheel. 2021;246.

Afshan Hassan 1Devendra Prasad. Gauging the Impact of Artificial Intelligence and Mathematical Modeling in Response to the COVID-19 Pandemic: A Systematic Review[Internet].Availablefrom: https://www.hindawi.com/journals/bmri/2022/7731618/

Ahmed I, Zhang Y, Jeon G, Lin W, Khosravi MR, Qi L. A blockchain-and artificial intelligence-enabled smart IoT framework for. 2022;37(9).

Ahmed S, Hossain MF, Kaiser MS, Noor MBT, Mahmud M, Chakraborty C. Artificial intelligence and machine learning for ensuring security in. 2021;

Albalawi U, Mustafa M. Current Artificial Intelligence (AI) Techniques, Challenges, and. 2022;19(10).

Aldawood H, Skinner G. Contemporary cyber security social engineering solutions, measures. 2019;10(1).

Ali A, Jadoon YK, Farid Z, Ahmad M, Abid N, Alzoubi HM, et al. The Threat of Deep Fake Technology to Trusted Identity Management. 2022;

Aljaidi M, Alsarhan A, Samara G, Alazaidah R, Almatarneh S, Khalid M, et al. NHS WannaCry Ransomware Attack: Technical Explanation of The. 2022;

Alsariera YA, Adeyemo VE, Balogun AO, Alazzawi AK. Ai meta-learners and extra-trees algorithm for the detection of phishing. 2020;8.

Alshahrani E, Alghazzawi D, Alotaibi R, Rabie O. Adversarial attacks against supervised machine learning based network. 2022;17(10).

Alsowail RA, Al-Shehari T. Techniques and countermeasures for preventing insider threats. 2022;8.

Al-Qahtani AF, Cresci S. The COVID-19 scamdemic: A survey of phishing attacks and their. 2022;16(5).

Amicone D, Cannas A, Marci A, Tortora G. A smart capsule equipped with artificial intelligence for autonomous. 2021;11(17).

Apruzzese G, Colajanni M, Ferretti L, Marchetti M. Addressing adversarial attacks against security systems based on machine. 2019;900.

Arora M, Bhardwaj I. Artificial Intelligence in Collaborative Information System. 2022;14(1).

Arshad A, Hanapi ZM, Subramaniam S, Latip R. A survey of Sybil attack countermeasures in IoT-based wireless sensor. 2021;7.

Bagaa M, Taleb T, Bernabe JB, Skarmeta A. A machine learning security framework for iot systems. 2020;8.

Barta G, Görcsi G. Risk management considerations for artificial intelligence business. 2021;21(1).

Bauer K, von Zahn M, Hinz O. Expl (AI) ned: The impact of explainable artificial intelligence on users'. 2023;

Ben Hamida S, Mrabet H, Belguith S, Alhomoud A, Jemai A. Towards securing machine learning models against membership inference. 2021;70(3).

Bendiab G, Saridou B, Barlow L, Savage N, Shiaeles S. IoT Security Frameworks and Countermeasures. 2021;

Bhutoria A. Personalized education and artificial intelligence in the United States. 2022;3.

Bill B, Melchers KG. Thou Shalt not Lie! Exploring and testing countermeasures against faking. 2023;31(1).

Bistron M, Piotrowski Z. Artificial intelligence applications in military systems and their. 2021;10(7).

Bridgelall R. Using artificial intelligence to derive a public transit risk index. 2022;24.

Bubaš G, Čižmešija A. A Critical Analysis of Students' Cheating in Online Assessment in Higher. 2023;

Butt UJ, Richardson W, Abbod M, Agbo H-M, Eghan C. The deployment of autonomous drones during the COVID-19 pandemic. 2021;

Bécue A, Praça I, Gama J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and. 2021;54(5).

Caviglione L, Comito C, Guarascio M, Manco G. Emerging challenges and perspectives in Deep Learning model security: A. 2023;

Celik I. Towards Intelligent-TPACK: An empirical study on teachers' professional. 2023;138.

Chakraborty A, Alam M, Dey V, Chattopadhyay A, Mukhopadhyay D. A survey on adversarial attacks and defences. 2021;6(1).

Chehri A, Fofana I, Yang X. Security risk modeling in smart grid critical infrastructures in the era. 2021;13(6).

Choi S, Kwon O-J, Oh H, Shin D. Method for effectiveness assessment of electronic warfare systems in. 2020;12(12).

Chu Z, Han Y, Zhao K. Botnet vulnerability intelligence clustering classification mining and. 2019;7.

Cui L, Guo L, Gao L, Cai B, Qu Y, Zhou Y, et al. A covert electricity-theft cyberattack against machine learning-based. 2021;18(11).

Danielis P, Beckmann M, Skodzik J. An ISO-compliant test procedure for technical risk analyses of IoT systems. 2020;

Das S. Artificial intelligence in highway safety. 2022;

Dash B, Ansari MF. An Effective Cybersecurity Awareness Training Model: First Defense of an. 2022;

Demertzi V, Demertzis S, Demertzis K. An Overview of Cyber Threats, Attacks and Countermeasures on the Primary. 2023;13(2).

Ding Y, Shi Y, Wang A, Wang Y, Zhang G. Block-oriented correlation power analysis with bitwise linear leakage: An. 2020;106.

Eigner O, Eresheim S, Kieseberg P, Klausner LD, Pirker M, Priebe T, et al. Towards resilient artificial intelligence: Survey and research issues. 2021;

Eshete B. Making machine learning trustworthy. 2021;373(6556).

Fang K. The development dilemma and countermeasures of strong artificial. 2020;

Floridi L, Holweg M, Taddeo M, Amaya Silva J, Mökander J, Wen Y. CapAI-A procedure for conducting conformity assessment of AI systems in. 2022;

Gao Y, Doan BG, Zhang Z, Ma S, Zhang J, Fu A, et al. Backdoor attacks and countermeasures on deep learning: A comprehensive. 2020;

Gausen A, Luk W, Guo C. Can we stop fake news? using agent-based modelling to evaluate. 2021;

Gautam V, Trivedi NK, Singh A, Mohamed HG, Noya ID, Kaur P, et al. A transfer learning-based artificial intelligence model for leaf disease. 2022;14(20).

Gilli A. Preparing for "NATO-mation": the Atlantic Alliance toward the age of. 2019;

Goldfarb A, Lindsay JR. Prediction and judgment: Why artificial intelligence increases the. 2021;46(3).

Gradoń K. Crime in the time of the plague: Fake news pandemic and the challenges to. 2020;4(2).

Gu J, Oelke D. Understanding bias in machine learning. 2019;

Gupta C, Johri I, Srinivasan K, Hu Y-C, Qaisar SM, Huang K-Y. A systematic review on machine learning and deep learning models for. 2022;22(5).

Haddaji A, Ayed S, Fourati LC. Artificial Intelligence techniques to mitigate cyber-attacks within. 2022;104.

Haigh K, Andrusenko J. Cognitive electronic warfare: an artificial intelligence approach. 2021;

Hamamoto R, Suvarna K, Yamada M, Kobayashi K, Shinkai N, Miyake M, et al. Application of artificial intelligence technology in oncology: Towards the. 2020;12(12).

Hamon R, Junklewitz H, Sanchez I. Robustness and explainability of artificial intelligence. 2020;207.

Hasan MK, Ghazal TM, Saeed RA, Pandey B, Gohel H, Eshmawi A 'a, et al. A review on security threats, vulnerabilities, and counter measures of 5G. 2022;16(5).

Hassan A, Prasad D, Rani S, Alhassan M. Gauging the impact of artificial intelligence and mathematical modeling in. 2022;2022.

Hassan F, Javed A. Voice spoofing countermeasure for synthetic speech detection. 2021;

He X, Liu X, Li P. Coordinated false data injection attacks in AGC system and its. 2020;8.

Hou Z. Research on adopting artificial intelligence technology to improve. 2021;1744.

Hu H, Pang J. Stealing machine learning models: Attacks and countermeasures for. 2021;

Huang S, Peng X, Jiang H, Luo Y, Yu S. New security challenges on machine learning inference engine: Chip cloning. 2020;

Ilahi I, Usama M, Qadir J, Janjua MU, Al-Fuqaha A, Hoang DT, et al. Challenges and countermeasures for adversarial attacks on deep. 2021;3(2).

Jaber A, Fritsch L. Towards ai-powered cybersecurity attack modeling with simulation tools: 2022;

Jamal AA, Majid A-AM, Konev A, Kosachenko T, Shelupanov A. A review on security analysis of cyber physical systems using Machine. 2023;80.

Janko V, Slapničar G, Dovgan E, Reščič N, Kolenik T, Gjoreski M, et al. Machine learning for analyzing non-countermeasure factors affecting early. 2021;18(13).

Jayalaxmi PLS, Saha R, Kumar G, Conti M, Kim T-H. Machine and Deep Learning Solutions for Intrusion Detection and Prevention. 2022;

Jiang L. A Study on the Efficiency and Countermeasures of Network-Based Autonomous. 2021;345.

Johnson J. Artificial intelligence: A threat to strategic stability. 2020;14(1).

Jones VA. Artificial intelligence enabled deepfake technology: The emergence of a. 2020;

Jovic A, Jap D, Papachristodoulou L, Heuser A. Traditional machine learning methods for side-channel analysis. 2022;

Kapadiya K, Patel U, Gupta R, Alshehri MD, Tanwar S, Sharma G, et al. Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: An. 2022;10.

Karaarslan E, Babiker M. Digital twin security threats and countermeasures: An introduction. 2021;

Keng-Yu LinORCID K-HC*. Artificial Intelligence and Information Processing: A Systematic Literature Review [Internet]. Available from: https://www.mdpi.com/2227-7390/11/11/2420

Khalaf BA, Mostafa SA, Mustapha A, Mohammed MA, Abduallah WM. Comprehensive review of artificial intelligence and statistical approaches. 2019;7.

Khan AA, Laghari AA, Rashid M, Li H, Javed AR, Gadekallu TR. Artificial intelligence and blockchain technology for secure smart grid. 2023;57.

Khan RS, Rehman IU. Spectroscopy as a tool for detection and monitoring of Coronavirus. 2020;20(7).

Kim Y, Kim J, Chang H. Design of an information security service for medical artificial. 2021;70.

Koblah D, Acharya R, Capecci D, Dizon-Paradis O, Tajik S, Ganji F, et al. A survey and perspective on artificial intelligence for security-aware. 2023;28(2).

Kong G, Zhang J. Analysis of quality problems and countermeasures in tunnel lining. 2024;

Kotenko I, Saenko I, Lauta O, Kribel A. A Proactive Protection of Smart Power Grids against Cyberattacks on. 2022;22(19).

Kreps S, McCain RM, Brundage M. All the news that's fit to fabricate: AI-generated text as a tool of media. 2022;9(1).

Krichen M, Adoni WYH, Mihoub A, Alzahrani MY, Nahhal T. Security challenges for drone communications: Possible threats, attacks. 2022;

Kuang B, Fu A, Susilo W, Yu S, Gao Y. A survey of remote attestation in Internet of Things: Attacks,. 2022;112.

Laplante P, Voas J. Zero-trust artificial intelligence? 2022;55(2).

Lefèvre L, Ligozat A-L, Trystram D, Bouveret S, Bugeau A, Combaz J, et al. Environmental assessment of projects involving AI methods. 2023;

Lei Y, Xu Y, Wang M, Zhu G, Jin Z. Origin, influence, and countermeasures of defects in perovskite solar. 2021;17(26).

Li P. Research on radar signal recognition based on automatic machine learning. 2020;32.

Li Y, Ding Q, Li K, Valtchev S, Li S, Yin L. A survey of electromagnetic influence on UAVs from an EHV power converter. 2021;10(6).

Li Z, Li H, Yin J, Li Y, Nie Z, Li X, et al. A review of spatter in laser powder bed fusion additive manufacturing: In. 2022;13(8).

Liakos KG, Georgakilas GK, Moustakidis S, Sklavos N, Plessas FC. Conventional and machine learning approaches as countermeasures against. 2020;79.

Lin M, Lin Z. Artificial intelligence ethics. 2022;2(2).

Liu J, Chang H, Forrest JY-L, Yang B. Influence of artificial intelligence on technological innovation: Evidence. 2020;158.

Liu J, Qian Y, Yang Y, Yang Z. Can artificial intelligence improve the energy efficiency of manufacturing. 2022;19(4).

Liu X. Artistic reflection on artificial intelligence digital painting. 2020;1648.

Liu Y. Research on Countermeasures of Rural Revitalization Assisted by Science. 2023;4(1).

Lv Z, Xie S. Artificial intelligence in the digital twins: State of the art,. 2022;1.

Ma P, Zhang Z, Wang J, Zhang W, Liu J, Lu Q, et al. Review on the application of metalearning in artificial intelligence. 2021;2021.

Ma Y, Xie T, Li J, Maciejewski R. Explaining vulnerabilities to adversarial machine learning through visual. 2019;26(1).

Manford D, Jahankhani H. Evaluating Countermeasures for Detecting Misinformation Attacks on Stock. 2022;

Masur PH, Reed JH, Tripathi NK. Artificial intelligence in open-radio access network. 2022;37(9).

Matsuda W, Fujimoto M, Aoyama T, Mitsunaga T. Cyber security risk assessment on industry 4.0 using ics testbed with ai. 2019;

Meocci M, Branzi V, Martini G, Arrighi R, Petrizzo I. A predictive pedestrian crash model based on artificial intelligence. 2021;11(23).

Miao Y, Chen C, Pan L, Han Q-L, Zhang J, Xiang Y. Machine learning–based cyber attacks targeting on controlled information: 2021;54(7).

Mirzaee PH, Shojafar M, Cruickshank H, Tafazolli R. Smart grid security and privacy: From conventional to machine learning. 2022;10.

Mishra S, Albarakati A, Sharma SK. Cyber Threat Intelligence for IoT Using Machine Learning. 2022;10(12).

Mohanta BK, Jena D, Satapathy U, Patnaik S. Survey on IoT security: Challenges and solution using machine learning,. 2020;11.

Mongelli M. Design of countermeasure to packet falsification in vehicle platooning by. 2021;179.

Mpatziakas A, Drosou A, Papadopoulos S, Tzovaras D. IoT threat mitigation engine empowered by artificial intelligence. 2022;203.

Naanani A. Security in Industry 4.0: Cyber-attacks and countermeasures. 2021;12(10).

Naik B, Mehta A, Yagnik H, Shah M. The impacts of artificial intelligence techniques in augmentation of. 2022;8(2).

Oeschger TM, McCloskey DS, Buchmann RM, Choubal AM, Boza JM, Mehta S, et al. Early warning diagnostics for emerging infectious diseases in developing. 2021;54(19).

Oprea A, Singhal A, Vassilev A. Poisoning Attacks Against Machine Learning: Can Machine Learning Be. 2022;55(11).

Oseni A, Moustafa N, Janicke H, Liu P, Tari Z, Vasilakos A. Security and privacy for artificial intelligence: Opportunities and. 2021;

O'Brien JT, Nelson C. Assessing the risks posed by the convergence of artificial intelligence. 2020;18(3).

Pan Q, Ma Z. Research and development of mosaic warfare. 2022;

Pan T. Study on the impact of new crown epidemic situation on China's foreign. 2020;

Park SH, Han K, Jang HY, Park JE, Lee J-G, Kim DW, et al. Methods for clinical evaluation of artificial intelligence algorithms for. 2023;306(1).

Pauling C, Gimson M, Qaid M, Kida A, Halak B. A tutorial on adversarial learning attacks and countermeasures. 2022;

Peksen MM. Artificial intelligence-based machine learning toward the solution of. 2022;4(3).

PerezSantin E, Rodríguez Solana R, González García M, García Suárez MDM, Blanco Díaz GD, Cima Cabal MD, et al. Toxicity prediction based on artificial intelligence: A multidisciplinary. 2021;11(5).

Pitropakis N, Panaousis E, Giannetsos T, Anastasiadis E, Loukas G. A taxonomy and survey of attacks against machine learning. 2019;34.

Pooyandeh M, Han K-J, Sohn I. Cybersecurity in the AI-Based metaverse: A survey. 2022;12(24).

Procopiou A, Chen TM. Explainable ai in machine/deep learning for intrusion detection in. 2021;

Pu X. Research on the Problems and Countermeasures in Network teaching of law. 2021;

Qasaimeh GM, Jaradeh HE. The impact of artificial intelligence on the effective applying of cyber. 2022;2(1).

Qiu S, Liu Q, Zhou S, Wu C. Review of artificial intelligence adversarial attack and defense. 2019;9(5).

Raheja H, Arora J, Gupta S, Gupta P, Singh A, Nagla A. Artificial Intelligence based Security Countermeasures for Internet of. 2023;

Rahimi P, Singh AK, Wang X, Prakash A. Trends and challenges in ensuring security for low-power and. 2021;

Ramirez MA, Kim S-K, Hamadi HA, Damiani E, Byon Y-J, Kim T-Y, et al. Poisoning attacks and defenses on artificial intelligence: A survey. 2022;

Rasheed J, Jamil A, Hameed AA, Al-Turjman F, Rasheed A. COVID-19 in the age of artificial intelligence: a comprehensive review. 2021;13.

Rawal A, Rawat D, Sadler BM. Recent advances in adversarial machine learning: status, challenges and. 2021;11746.

Rehman E, Haseeb-ud-Din M, Malik AJ, Khan TK, Abbasi AA, Kadry S, et al. Intrusion detection based on machine learning in the internet of things,. 2022;

Ries M. The COVID-19 infodemic: Mechanism, impact, and counter-measures—A review. 2022;14(5).

Roth HR, Xu Z, Tor-Díez C, Jacob RS, Zember J, Molto J, et al. Rapid artificial intelligence solutions in a pandemic—The COVID-19-20 Lung. 2022;82.

Saeedi S, Fong ACM, Mohanty SP, Gupta AK, Carr S. Consumer artificial intelligence mishaps and mitigation strategies. 2021;11(3).

Sanders LM, Scott RT, Yang JH, Qutub AA, Garcia Martin H, Berrios DC, et al. Biological research and self-driving labs in deep space supported by. 2023;5(3).

Sayadi H, Wang H, Miari T, Makrani HM, Aliasgari M, Rafatirad S, et al. Recent advancements in microarchitectural security: Review of machine. 2020;

Selvaganapathy S, Sadasivam S, Ravi V. A review on android malware: Attacks, countermeasures and challenges ahead. 2021;

Sepasgozar S, Karimi R, Farahzadi L, Moezzi F, Shirowzhan S, M. Ebrahimzadeh S, et al. A systematic content review of artificial intelligence and the internet of. 2020;10(9).

Shan W, Zhang S, Xu J, Lu M, Shi L, Yang J. Machine learning assisted side-channel-attack countermeasure and its. 2019;55(3).

Sharma A, Singh UK. Modelling of smart risk assessment approach for cloud computing. 2022;3(1).

Sharma E. Artificial Intelligence and Clean Air: Development of Novel Algorithms. 2022;

Sharma P, Thapa K, Dhakal P, Upadhaya MD, Adhikari S, Khanal SR. Performance of ChatGPT on USMLE: Unlocking the Potential of Large Language. 2023;

Sharma S, Verma VK. AIEMLA: artificial intelligence enabled machine learning approach for. 2021;77(12).

Shrivastwa R-R, Guilley S, Danger J-L. Multi-source fault injection detection using machine learning and sensor. 2021;

Shukla A, Ahamad S, Rao GN, Al-Asadi AJ, Gupta A, Kumbhkar M. Artificial intelligence assisted IoT data intrusion detection. 2021;

Singh S, Sharma C, Sharma S, Verma NK. Re-Learning Emotional Intelligence Through Artificial Intelligence. 2021;

Singhal V, Jain SS, Anand D, Singh A, Verma S, Rodrigues JJ, et al. Artificial intelligence enabled road vehicle-train collision risk. 2020;8.

Solano J, Lopez C, Rivera E, Castelblanco A, Tengana L, Ochoa M. Scrap: synthetically composed replay attacks vs. adversarial machine. 2020;

Szczepański M, Pawlicki M, Kozik R, Choraś M. New explainability method for BERT-based model in fake news detection. 2021;11(1).

Taddeo M, McCutcheon T, Floridi L. Trusting artificial intelligence in cybersecurity is a double-edged sword. 2019;1(12).

Tahirkheli AI, Shiraz M, Hayat B, Idrees M, Sajid A, Ullah R, et al. A survey on modern cloud computing security over smart city networks: 2021;10(15).

Tang R, Zhuo Z, Zhang C, Li L. The applications of artificial intelligence in situation assessment and. 2019;

Tao F, Akhtar MS, Jiayuan Z. The future of artificial intelligence in cybersecurity: A comprehensive. 2021;8(28).

Tariq MI, Memon NA, Ahmed S, Tayyaba S, Mushtaq MT, Mian NA, et al. A review of deep learning security and privacy defensive techniques. 2020;2020.

Tayarani M. Applications of artificial intelligence in battling against covid-19: A. 2020;

Telo J. Smart City Security Threats and Countermeasures in the Context of Emerging. 2023;6(1).

Thanh CT, Zelinka I. A survey on artificial intelligence in malware as next-generation threats. 2019;25.

Tian Z, Cui L, Liang J, Yu S. A comprehensive survey on poisoning attacks and countermeasures in machine. 2022;55(8).

Tidjon LN, Khomh F. Threat assessment in machine learning based systems. 2022;

Ukwandu E, Farah MAB, Hindy H, Brosset D, Kavallieros D, Atkinson R, et al. A review of cyber-ranges and test-beds: Current and future trends. 2020;20(24).

Velasco C. Cybercrime and Artificial Intelligence. An overview of the work of. 2022;23.

Vähäkainu P, Lehto M, Kariluoto A. Cyberattacks Against Critical Infrastructure Facilities and Corresponding. 2022;

Wall J, Krummel T. The digital surgeon: How big data, automation, and artificial intelligence. 2020;55.

Walsh DP, Ma TF, Ip HS, Zhu J. Artificial intelligence and avian influenza: using machine learning to. 2019;66(6).

Walter MJ, Barrett A, Walker DJ, Tam K. Adversarial AI testcases for maritime autonomous systems. 2023;

Wang D, Chen K, Wang W. Demystifying the Vetting Process of Voice-Controlled Skills on Markets. 2021;5(3).

Wang H, Salehi S, Sayadi H, Sasan A, Mohsenin T, Manoj PDS, et al. Evaluation of machine learning-based detection against side-channel. 2021;

Wang S, Sun Z, Chen Y. Effects of higher education institutes' artificial intelligence capability. 2023;28(5).

Wang Y, Chung SH. Artificial intelligence in safety-critical systems: a systematic review. 2022;122(2).

Wang Y, Zhang S, Chi M, Yu J. A PDCA model for disinfection supply rooms in the context of artificial. 2022;2022.

Wazid M, Das AK, Chamola V, Park Y. Uniting cyber security and machine learning: Advantages, challenges and. 2022;8(3).

Wu H, Han H, Wang X, Sun S. Research on artificial intelligence enhancing internet of things security: 2020;8.

Wu Y, Shan S. Application of artificial intelligence to social governance capabilities. 2021;2021.

Xiaoling P. Discussion on ethical dilemma caused by artificial intelligence and. 2021;

Xiaoyang H, Junzhi Z, Jingyuan F, Xiuxia Z. Effectiveness of ideological and political education reform in. 2021;40(2).

Xiong P, Buffett S, Iqbal S, Lamontagne P, Mamun M, Molyneaux H. Towards a robust and trustworthy machine learning system development: An. 2022;65.

Xu L. The dilemma and countermeasures of AI in educational application. 2020;

Xu X, Zhang J. Rethinking FPGA security in the new era of artificial intelligence. 2020;

Yamin MM, Ullah M, Ullah H, Katt B. Weaponized AI for cyber attacks. 2021;57.

Yan Y, Huang D, Yin P, Luo H, Chen J, Mao Y, et al. Artificial key fingerprints for continuous-variable quantum key. 2023;108(1).

Yang J. A Systematic Literature Review of Information Security in Chatbots [Internet]. 1st ed. TAIWAN: MBPI; 2023. Available from: https://www.mdpi.com/2076-3417/13/11/6355

Yang K, Varol O, Davis CA, Ferrara E, Flammini A, Menczer F. Arming the public with artificial intelligence to counter social bots. 2019;1(1).

Yang X, Shu L, Liu Y, Hancke GP, Ferrag MA, Huang K. Physical security and safety of iot equipment: A survey of recent advances. 2022;18(7).

Yang Z, Xia S, Feng S. Construction of a physical and medical care integrated model for the. 2022;2022.

Yeboah-Ofori A, Mouratidis H, Ismai U, Islam S, Papastergiou S. Cyber supply chain threat analysis and prediction using machine learning. 2021;

Yu X, Zhou X, Wang D, Li W, Liu X. Current Situation of Prevention and Control of New Coronavirus in China. 2022;5(1).

Zhang Y, Dai Z, Zhang L, Wang Z, Chen L, Zhou Y. Application of artificial intelligence in military: From projects view. 2020;

Zhao J, Li Q. Big Data–Artificial Intelligence Fusion Technology in Education in the. 2022;10(3).

Zhou C, Liu Q, Zeng R. Novel defense schemes for artificial intelligence deployed in edge. 2020;2020.

Zhu Y. Research on the Translation System of Spoken English Situational Dialogue. 2023;

Çakmakçı SD, Hutschenreuter H, Maeder C, Kemmerich T. A framework for intelligent DDoS attack detection and response using SIEM. 2021;

Appendix V: Qualitative Research

Study: Duckett SJ. 2012.	
Finding	suitable (C)
Illustration	all information has been well analyzed
Study: Putra SD, Sumari ADW, Ahmad AS, Sutikno S, Kurniawan Y. 2020	
Finding	suitable (C)
Illustration	all information has been well analyzed
Study: Zaman S, Alhazmi K, Aseeri MA, Ahmed MR, Khan RT, Kaiser MS, et al. 2021.	
Finding	not suitable (U)
Illustration	some data analyzed information is missing
Study: Fengying Li YH and QX.	
Finding	suitable (C)
Illustration	all information has been well analyzed
Study: Zhu K, Zheng L. 2021.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Hu Y, Kuang W, Qin Z, Li K, Zhang J, Gao Y, et al. 2021.	
Finding	suitable (C)
Illustration	all information has been well analyzed
Study: Wang C, Chen J, Yang Y, Ma X, Liu J. 2022.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed

	and is useful for this topic
Study: Thomas S, Abraham A, Baldwin J, Piplani S, Petrovsky N. 2022.	
Finding	unsuitable to be used in this research (U)
Illustration	study was not in-depth
Study: Bai J, Zheng D, Jia C. 2022.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzedand is useful for this topic
Study: Xue M, Yuan C, Wu H, Zhang Y, Liu W. 2020.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Zhao S. 2022.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: PanniyammakalJeemon 2017	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Yaacoub J-PA, Noura HN, Salman O, Chehab A. 2022.	
Finding	suitable (C)

Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Fatima A, Khan TA, Abdellatif TM, Zulfiqar S, Asif M, Safi W, et al. 2023.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Bhatnagar D, Som S, Khatri SK. 2019.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Shane Amanda 2019	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Swessi D, Idoudi H. 2022.	
Finding	unsuitable (N)
Illustration	all information has not been well analyzed
Study: Luo Q, Cao Y, Liu J, Benslimane A. 2019.	
Finding	Suitable to be used in this research (C)
Illustration	all information has been well analyzed
Study: Cai M, Luo J. 2020.	
Finding	suitable (C)

Illustration	all information has been well analyzed
Study: Hu W, Chang C-H, Sengupta A, Bhunia S, Kastner R, Li H. 2020.	
Finding	suitable (C)
Illustration	all information has been well analyzed
Study: Surma J. 2020.	
Finding	suitable (C)
Illustration	all information has been well analyzed
Study: Li F, He Y, Xue Q. 2021.	
Finding	suitable (C)
Illustration	all information has been well analyzed
Study: Sabir B, Ullah F, Babar MA, Gaire R. 2021.	
Finding	suitable (C)
Illustration	i have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Guo-Lian Ding 2015	
Finding	SUITABLE (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Doukas N, Stavroulakis P, Bardis N. 2021.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic

Study: Chakraborty C, Rajendran SR, Rehman MH. 2021	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Falahati A, Shafiee E. 2022.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Livada B, Perić D. 2020.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Waheed N, He X, Ikram M, Usman M, Hashmi SS, Usman M. 2020.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Ansari MS, Alsamhi SH, Qiao Y, Ye Y, Lee B. 2020.	
Finding	suitable (N)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Yue P, An J, Zhang J, Pan G, Wang S, Xiao P, et al. 2022.	

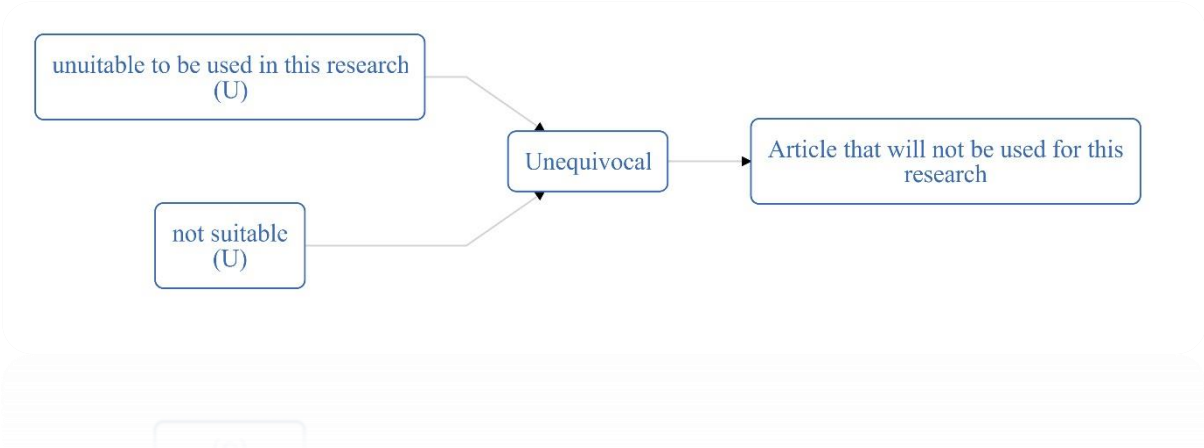
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Keller N, Whittle RS, McHenry N, Johnston A, Duncan C, Ploutz-Snyder L, et al. 2022.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzedand is useful for this topic
Study: Esposito S, Sgandurra D, Bella G. 2023	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Algarni A, Thayananthan V. 2022.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Zhang J, Zhang Z-M. 2023.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Repede Ștefan E. 2023.	
Finding	suitable (C)

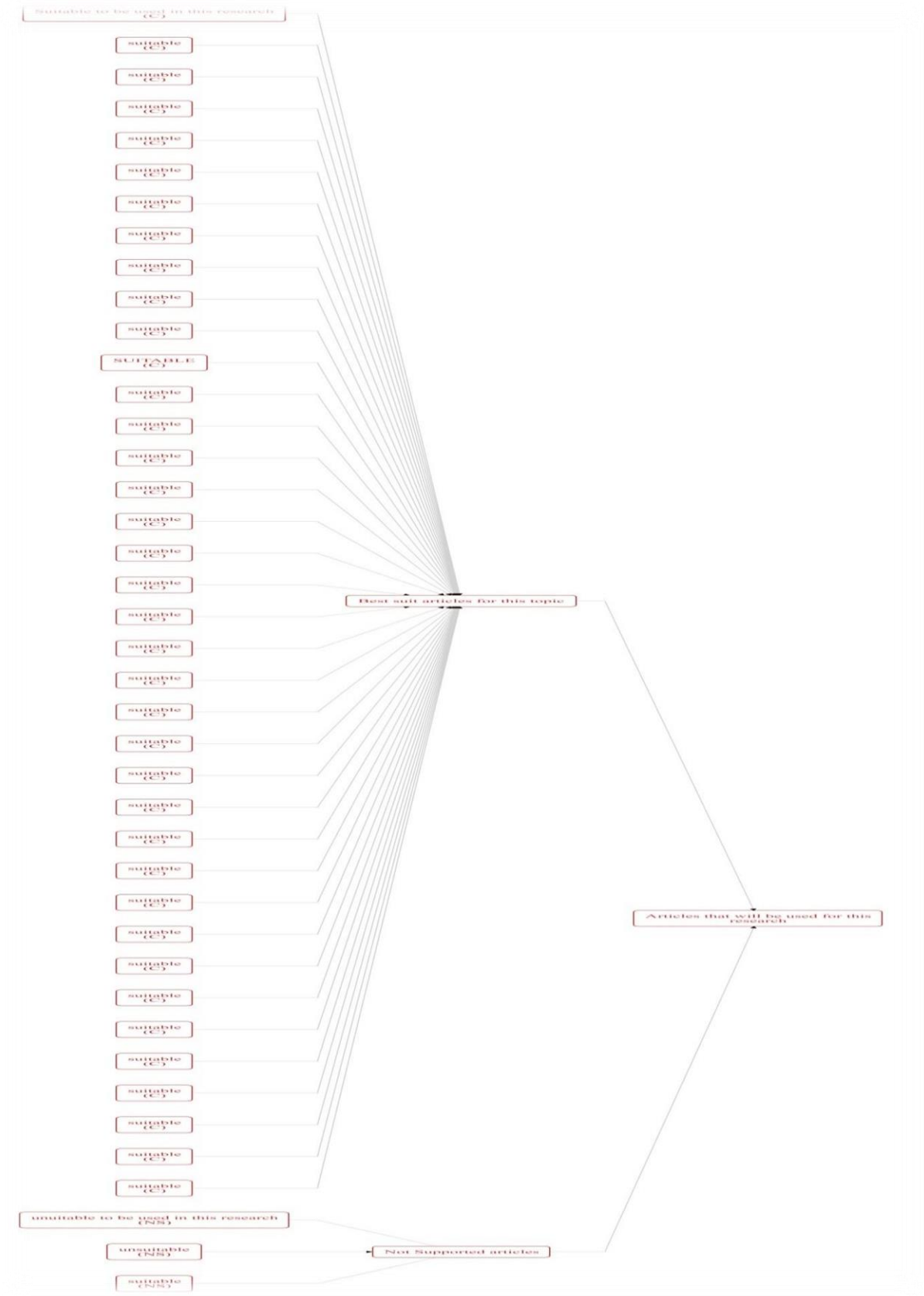
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Najmi KY, AlZain MA, Masud M, Jhanjhi NZ, Al-Amri J, Baz M. 2021	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Namatherdhala B, Mazher N, Sriram GK. 2022	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Zhang X, Zhang X, Liu W, Zou X, Sun M, Zhao J. 2022.	
Finding	unsuitable to be used in this research (N)
Illustration	some information has not been analyzed
Study: Basner M, Dinges DF, Howard K, Moore TM, Gur RC, Mühl C, et al. 2021	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Yaacoub J-P, Noura H, Salman O, Chehab A. 2020.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic

Study: Qiu H, Ding S, Liu J, Wang L, Wang X. 2022.	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic
Study: Raquel Villegas 2006	
Finding	suitable (C)
Illustration	I have checked and confirmed that all information has been well analyzed and is useful for this topic

Appendix VI: Review findings

Review findings are preferentially structured according to the phenomena of interest for reviews that include qualitative data. The meta-aggregative table has been accompanied by sufficient narrative to explain the findings and categories organized clearly under each synthesized finding. It is clear how many findings make up each category and how many categories make up each synthesized finding. Full description of the similarity of meaning informing each category and synthesized finding has been provided.




Suitable to be used in this research (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
SUITABLE (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
suitable (C)
Best suit articles for this topic
Articles that will be used for this research
unsuitable to be used in this research (NS)
unsuitable (NS)
suitable (NS)
Not Supported articles