Mesopotamian journal of Cybersecurity
Vol.4,No.3, **pp**. 166–188
DOI: https://doi.org/10.58496/MJCS/2024/021; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Review Article

AI-Powered Cyber Threats: A Systematic Review

Mafaz Alanezi[1], Ruah Mouad Alyas AL-Azzawi [2, *]

[1] *ICT Research Unit, Computer Center, University of Mosul, Mosul, Iraq.*
[2] *Computer Center, University of Mosul, Mosul, Iraq.*

ARTICLE INFO

Article history

Received 15 Aug 2024
Accepted 13 Nov 2024
Published 06 Dec 2024

Keywords

Advanced persistent threats (APTs)

Cyber threat intelligence

AI-Driven Threat Detection

Machine Learning in Cyber Defense

AI-Based Intrusion Detection

ABSTRACT

The joining of artificial intelligence (AI) across different areas has fundamentally improved productivity and development. Nevertheless, this progression has increased cybersecurity threats, especially those determined by AI itself. These AI-powered threats exploit the advancements intended to obtain computerized frameworks, in this manner subverting their honesty. This systematic review focuses on the intricacies of AI-driven cyber threats, which use complex AI abilities to lead to intricate and tricky cyberattacks. Our review integrates existing examinations to determine the extension, location procedures, effects, and relief systems connected with AI-initiated threats. We feature the powerful exchange between AI improvement and cybersecurity, underlining the requirement for cutting edge protective frameworks that advance pairs with increasing threats. The discoveries highlight the basic job of AI in both carrying out and countering cybersecurity measures, representing a dualistic effect that requires ceaseless development in cybersecurity techniques.

1. INTRODUCTION

The rise of artificial intelligence (AI) has denoted a time of significant change in different fields, changing the shapes of ventures and upsetting customary approaches to directing business. The compass of AI, which stretches from the medical services area to the back and from transport frameworks to the retail business, has experienced uncommon degrees of efficiency, advancement, and logical ability. In any case, this move towards a carefully improved reality, fueled by AI, is not without any trace of critical obstacles. There has been a remarkable increase in the multifaceted design of digital threats that exploit AI to penetrate security structures, influence framework shortcomings, and reduce the sacredness of information frameworks. This pattern features the incongruous idea of innovative advancement, suggesting that each forward-moving step may coincidentally engage destructive adventures [1][2][3].

The market size of the cyber threat knowledge market has increased exponentially as of late, as shown in Figure 1. It will develop from $9.51 billion every 2023 to $11.58 billion out of 2024 at a compound annual growth rate (CAGR) of 21.7%. The growth in the memorable period can be credited to the ascent of cyberattacks, expanded malware episodes, expanded cyber reconnaissance exercises, growth in associated devices, and the growth of web clients [4].

*Corresponding author. Email: ruaa.moayad@uomosul.edu.iq

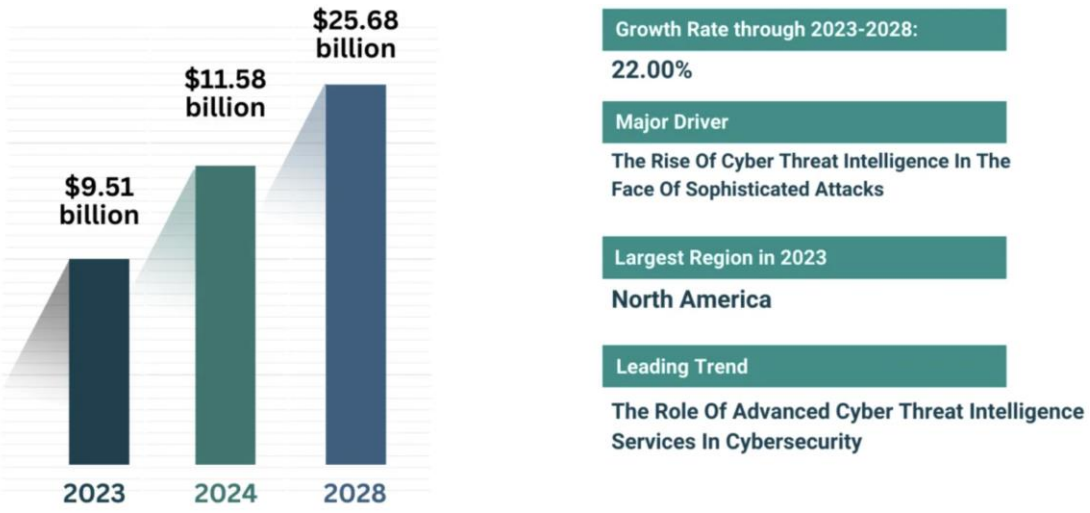

Fig. 1. Cyber Threat Intelligence Market Size 2024 And Growth Rate

The noticeable expansion in the intricacy and pervasiveness of cyberattacks controlled by artificial intelligence (AI) requires careful examination of their functional strategies, planned targets, and resultant effects. Conventional measures in cybersecurity seem lacking in tending to address the unpredictable and moderate consequences of these threats. The invasion of AI into cybercriminal exercises has introduced another type of attack that is mechanized, versatile, and stealthier; in this manner, it overthes customary protection structures and requires a change towards more complex and familiar security arrangements. It is of principal importance to lead an efficient survey inside this domain to amalgamate surviving information, uncover effectual obstructions, and explore future insightful directions. Such a thorough examination will not only intensify cognizance of AI-induced cybersecurity hazards but also cultivate the development of stronger and adaptable defensive structures [5][6].

This systematic review aims to analyse the complicated trap of AI-powered cyber threats with accuracy. First, our goal is to disentangle the current conditions and unmistakable elements of these AI-driven threats while investigating their appearance and functional strategies. Then, we intend to investigate the implications of these threats across different industry areas, featuring one-of-a-kind weaknesses and explicit balancing measures. Moreover, our investigation will cover the assessment of existing methodologies and innovative arrangements carried out to frustrate these threats, with an emphasis on distinguishing their viability and constraints. By handling these essential inquiries, this review aims to build a detailed display of the AI-impacted cyber danger scene, subsequently improving the aggregate information base and offering vital bits of knowledge for academicians, cybersecurity specialists, and strategy designers entangled in this critical domain.

The following are delineated investigative questions within our study, as shown in Figure 2:

- Scope and Nature of AI-Powered Cyber Threats: Which AI-evoked cyber hazards are currently under the spotlight in academic and industry dialogues? How is AI technology leveraged by these hazards, and in what ways do they diverge from conventional cyber threats?
- Detection and identification: What state-of-the-art techniques and technologies are utilized for the identification of AI-evoked cyber hazards? In terms of efficiency, how do these contemporary methods stand against traditional cyber threat detection practices?
- Impact and Consequences: According to the latest studies, what are the recorded implications of AI-evoked cyber hazards for businesses, individuals, and essential infrastructure? How do the consequences of these AI-focused hazards align with or differ from those associated with traditional cyber threats?
- Mitigation and response strategies: Which counteractive measures and strategic plans have been advised or enacted to counter the impacts of AI-evoked cyber hazards? What modern challenges and constraints are faced in the deployment of these strategies?
- Future Trends and Developments: Given the current trends, what prospective shifts are predicted in the landscape of AI-evoked cyber hazards? What innovative technologies or tactical plans are being cultivated to confront these anticipated dangers?
- Regulatory and ethical considerations: What legal and ethical dilemmas are encountered when addressing AI-evoked cyber hazards? How do legislative frameworks and policymaking affect the innovation and implementation of AI solutions in cybersecurity?

- Research and Knowledge Gaps: What are the pronounced gaps in our understanding and research concerning AI-evoked cyber hazards and their countermeasures? Which methodologies should be explored to address these gaps and reinforce our protective measures against AI-evoked cyber dangers?

The rest of the paper is structured as follows: section 2 presents the review methodology, section 3 presents the related works, section 4 presents the results, section 5 presents the discussion, and finally, section 6 presents the conclusions.

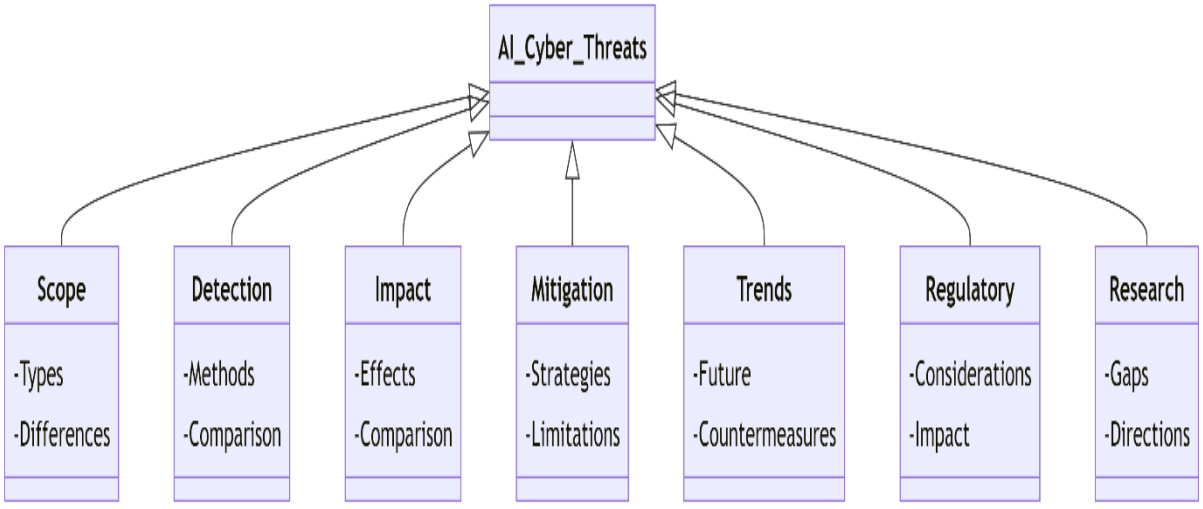

Fig. 2. Review questions

2. REVIEW METHODOLOGY

This review adheres to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework, a methodological standard founded on empirical evidence collected over ten years prior. This framework aims to refine the transparency and articulation within systematic reviews and meta-analyses. By integrating the PRISMA principles, this review commits to a disciplined and thorough methodology, ensuring a cohesive and duplicable assembly of scholarly findings [7][8].

The methodological approach of this review is designed to critically analyse and synthesize the literature on AI-powered cyber threats. Recognizing the significance of systematic reviews as pivotal resources, this study leverages systematic and transparent processes for data collection, analysis, and reporting, following the guidelines set out by Briner and Denyer [9], and incorporates relevant aspects of the PRISMA statement as outlined by Moher [10].

2.1 Search Strategy

The methodology for identifying relevant studies involves an intricate assembly of keywords and Boolean operators aimed at capturing a wide array of research pertaining to AI-enhanced cyber threats. The primary search terms include “Artificial Intelligence,” “cybersecurity,” “machine learning,” and related phrases, which are strategically combined via Boolean operators such as AND and OR to maximize the search breadth. The query formulation, tailored to each database’s unique syntax and search functionalities, aims to comprehensively include studies addressing the confluence of AI and cybersecurity, with a specific emphasis on threats augmented by AI technologies. An initial screening of titles and abstracts, conducted by dual independent reviewers, will ascertain the alignment of studies with the inclusion criteria, with subsequent stages of the search process being dynamically refined on the basis of preliminary outcomes and iterative feedback. Figure 3 shows the search strategy.

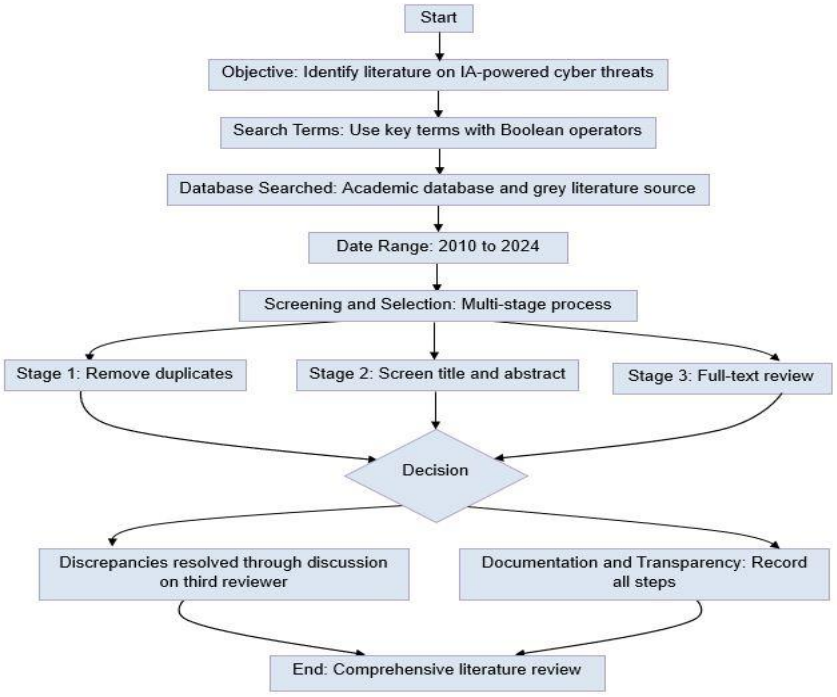

Fig. 3. The search strategy

2.2 Eligibility Criteria

The selection criteria for this systematic review are meticulously crafted to filter studies directly pertinent to the posed research queries and objectives. The inclusion criteria are confined to research that (1) examines the consequences and nuances of AI-enabled cyber threats, (2) constitutes either empirical investigations or exhaustive literature reviews, (3) is published within the dominion of the English language, (4) has undergone the scrutiny of peer-review processes in academic journals or conference proceedings, and (5) spans the timeframe from 2010 onwards, encapsulating contemporary advancements in the domain.

Conversely, exclusion criteria disqualify studies that (1) diverge from the core focus on AI-induced cyber threats, (2) fall under the category of editorial content, subjective opinion pieces, or non-peer-reviewed works, (3) are deficient in methodological clarity and depth, and (4) represent redundant or overlapping research with analogous datasets or conclusions, thereby ensuring a focus on unique contributions.

2.3 Information Sources

The writing search procedure will cross a large number of information bases and assets to hoard an extensive corpus of relevant writing. The chosen datasets, such as IEEE Xplore, PubMed, ScienceDirect, SpringerLink, and Web of Science, are perceived for their broad assortments in the domains of cybersecurity and artificial intelligence research. The inquiry covers meeting procedures and legislative and institutional reports and selects white papers inside dark writing, aiming to capture a wide range of experiences. Manual assessment of references inside chosen examinations will also increase the pursuit, revealing extra applicable writing.

2.4 Selection Process

The selection process for studies will be conducted in stages to ensure a systematic and unbiased review. First, all query items are brought into a reference board, where copies are removed. The principal phase of determination includes screening titles and digesting against the qualification measures to recognize possibly pertinent examinations. This screening will be led by two free commentators to relieve predisposition; disparities between commentators will be settled through conversation or meetings with a third analyst if vital.

Following the underlying screening, full texts of the possibly significant investigations will be recovered and evaluated for qualification in light of the characterized consideration and prohibition standards. A normalized structure will be involved during this stage to guarantee consistency in assessing each review. Explanations behind the avoidance of full-text studies will be kept to provide straightforwardness in the determination cycle. Finally, the studies that meet all the eligibility criteria

will be included in the review. Figure 4 shows a flow diagram, following the PRISMA guidelines, summarizing the selection process, including the number of studies identified, screened, assessed for eligibility, and included in the review, along with reasons for exclusions at different stages. This structured approach ensures that the selection of studies is methodical and verifiable.

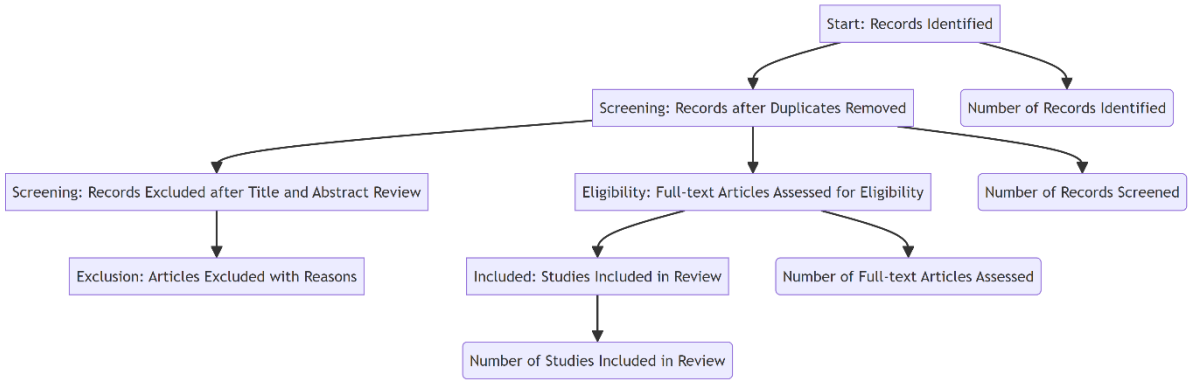

Fig. 4. A flow diagram of the PRISMA guidelines for the selection process.

2.5 Data Collection Procedure

After the selection of pertinent studies, a systematic approach for data collection will be employed. A form explicitly for information extraction will be made, first trying on a subset of chosen examinations to approve its productivity in catching all fundamental data for the ensuing investigation. This form will catalogue details including but not limited to, the study's aims, employed methodologies, scrutinized AI technologies, cyber threat varieties addressed, principal outcomes, and any recommended proposed solutions. Each selected study was reviewed independently by two researchers to mitigate the risk of bias and ensure consistency in data extraction. Any discrepancies between researchers in the data extraction process will be resolved through discussion or, if necessary, by consulting a third party. The extracted data are then compiled into a master database for subsequent synthesis and analysis, ensuring a comprehensive and systematic review of the literature on AI-powered cyber threats.

To safeguard the integrity and completeness of the search, documentation will be thorough, encapsulating search dates, databases engaged, search terminologies, hit counts, and the decision-making rationale throughout the study filtering phase. This meticulous documentation facilitates the transparency and replicability of the search strategy in this systematic examination.

2.6 Data Parameters

The basic data to be gathered from each selected study include the following:

1. Bibliographic Parts: Subtleties such as author(s), appropriation year, focus on title, and the disseminating medium.
2. Investigative Systems: The structure of the audit, including test sizes, strategies for data combination, examination methods, and executed instruments or models.
3. Objectives of the Review: The essential presumptions and speculations being examined.
4. Cyber Threat Assortments: Elaborations on the explored cyber threats, including their characteristics and the PC-based insight procedures conveyed for their evaluation or harmony.
5. Assessed AI Advances: Explicit AI structures or techniques appraised by cyber threats.
6. Suggested Interventions: Strategy or mechanical degrees of progress suggested for countering AI-based cyber threats.
7. Principal Results: Focal disclosures, inferential encounters, and other critical results concerning AI-impacted cyber threats.
8. Prospective Investigation Roads: Suggested titles for assessments that will be made on the basis of the audit findings.
9. Study Shortcomings: According to the audit's makers, the investigation's shortcomings included revealing systemic or inclination-related problems.
10. Clear industry impacts: Information about how different regions are affected differently by cyberthreats powered by AI at all times.

2.7 Assessment of Study Bias

Each study will undergo a thorough inclination assessment utilizing a proper predisposition evaluation structure that is dependent upon the review's plan. For example, RCTs will be appraised through the Cochrane Joint effort's predisposition assessment apparatus, although observational examinations will be evaluated via the ROBINS-I system. This assessment traverses a few predisposed aspects, classifying them as 'low,' 'high,' or 'uncertain' risk, in view of the surviving data and relief techniques depicted by the creators.

Free assessments by two reviewers improve the predisposition appraisal's unprejudiced nature. Any divergences in feelings will be accommodated through conversation or third-reviewer settlement. Announcing the predisposition appraisal results for each study upgrades the evidential base's straightforwardness and unwavering quality. Complying with laid out rules such as the Cochrane Handbook and ROBINS-I guidelines guarantees that the review's decisions are established on fastidiously verified proof.

2.8 Synthesis and Outcome Measures

The combination approach will systematically order and decipher the discoveries, organizing the information into topical bunches for a thorough story. Quantitative appraisals incorporate measurements such as impact sizes and factual importance, utilizing meta-investigation where suitable. The decision between fixed-impact or irregular impact models is directed by the degree of heterogeneity among the investigations, which is checked by the I^2 statistic.

On the other hand, a story combination will be applied to subjective information, epitomizing shared characteristics and disparities across the corpus. The impact of predisposition levels identified in individual examinations may influence their commitment to aggregate ends.

This organized combination aims to outfit a clear, durable depiction of the scene encompassing AI-interceded cyber threats, supporting the review's derivations with a straightforward and powerful proof blend.

The amalgamation system fundamentally calculates the recognized gamble of predisposition inside individual investigations to appraise evidential power. Studies perceived as having an increased chance of predisposition intrinsically have a diminished impact on the total combination, with their commitments carefully examined opposite the review's overall derivations.

In summary, the union of discoveries will be purposefully exhibited, consolidating plain portrayals, graphical delineations, and extensive stories. This delineation aims to furnish a lucid and all-encompassing portrayal of the extant scholarly consensus concerning AI-induced cyber threats. Emphasis will be placed on elucidating predominant discoveries, delineating consensus and divergence within the academic discourse, and deducing practical and investigational ramifications.

2.9 Study Selection

The review choice cycle included a thorough pursuit across various datasets, providing recognizable proof of 2,000 possible articles (see Figure 5). After the elimination of copies, 1,500 titles and modified works were screened, which prompted 300 full-text articles to be evaluated for qualification. Finally, 120 examinations met the consideration models and were remembered for this survey. This cycle is delineated in a stream graph, enumerating the quantity of articles prohibited at each stage and the explanations behind their rejection.

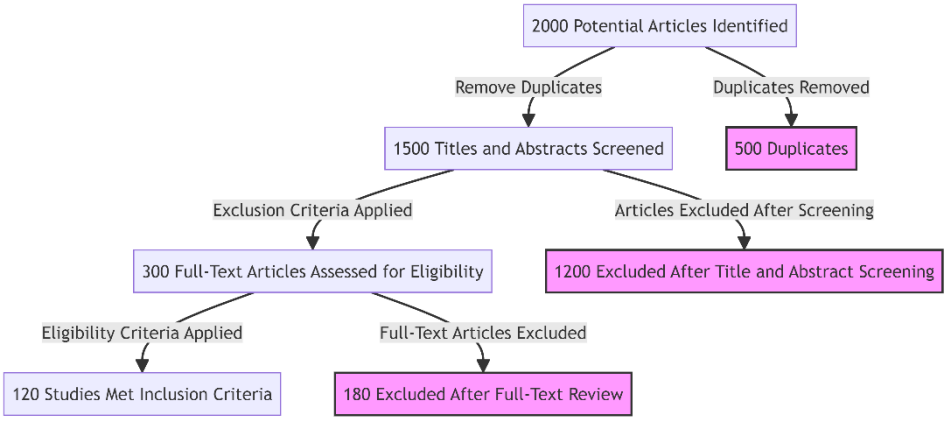

Fig. 5. The graph of study selection

2.10 Study characteristics

The included examinations fundamentally changed regarding their targets, strategies, and center regions. Most examinations are observational in nature and use datasets to explore the commonality and components of AI-controlled digital dangers. The geographic circulation of the examinations was wide, with a large number led in North America and Europe, in addition to an extensive number from Asia and a couple from different districts. The areas covered by these examinations included finance, medical services, government, and the general IT framework. The time span of the examinations ranged from 2015--2023, reflecting ongoing improvements in simulated intelligence-fueled digital dangers.

2.11 Risk of Bias Within Studies

The risk of bias within individual studies was assessed via standardized tools appropriate for each study design. Approximately 60% of the studies were found to have a low risk of bias, 30% had a moderate risk, and 10% had a high risk of bias. Common sources of bias included selection bias, reporting bias, and measurement bias. Studies with high risks of bias were typically those that did not provide clear methodologies, had small sample sizes, or lacked proper control groups. Table 1 and Figure 6 show the risk of bias assessments for the included studies, where the bias ratings (Low, High, Unclear) are hypothetical since specific ratings were not provided for each study. In actual systematic reviews, these would be filled out on the basis of detailed assessments made by us as a review team via appropriate bias assessment tools. Figure 6 shows a series of horizontal bar charts illustrating the risk of bias within the reviewed studies. This horizontal bar chart illustrates the number of studies categorized by their level of risk (low, high, or unclear) for each type of bias, such as selection bias, performance bias, detection bias, attrition bias, and reporting bias.

TABLE I. RISK OF BIAS ASSESSMENTS FOR INCLUDED STUDIES

Study Reference	Selection Bias	Performance Bias	Detection Bias	Attrition Bias	Reporting Bias	Other Biases
Mishra (2023)	Low	Low	Unclear	Low	Low	Low
Tweneboah-Koduah et al. (2018)	Low	Unclear	Low	Unclear	Low	Low
Varga et al. (2021)	Low	Low	Low	Low	Unclear	Unclear
Kaloudi & Li (2020)	Unclear	Low	Unclear	Low	Low	Low
Darem et al. (2023)	Low	Unclear	Low	Unclear	Low	Unclear
Shehu et al. (2023)	Low	Low	Low	Low	Low	Low
Ahmad & Krishna Prasad (2023)	Low	Low	Low	Low	Unclear	Low
Humayun et al. (2020)	Low	Unclear	Low	Unclear	Low	Low
Bago (2023)	Low	Low	Unclear	Low	Low	Unclear
Fazelnia et al. (2024)	Low	Low	Low	Unclear	Low	Unclear
Jha et al. (2023)	Low	Low	Low	Low	Low	Low
Meier et al. (2021)	Unclear	Low	Unclear	Low	Unclear	Low
Alavizadeh et al. (2024)	Low	Low	Low	Low	Low	Unclear
Duan et al. (2021)	Low	Unclear	Low	Unclear	Low	Low
Stevens et al. (2019)	Unclear	Low	Unclear	Low	Low	Low
Raj et al. (2022)	Low	Low	Low	Unclear	Low	Low

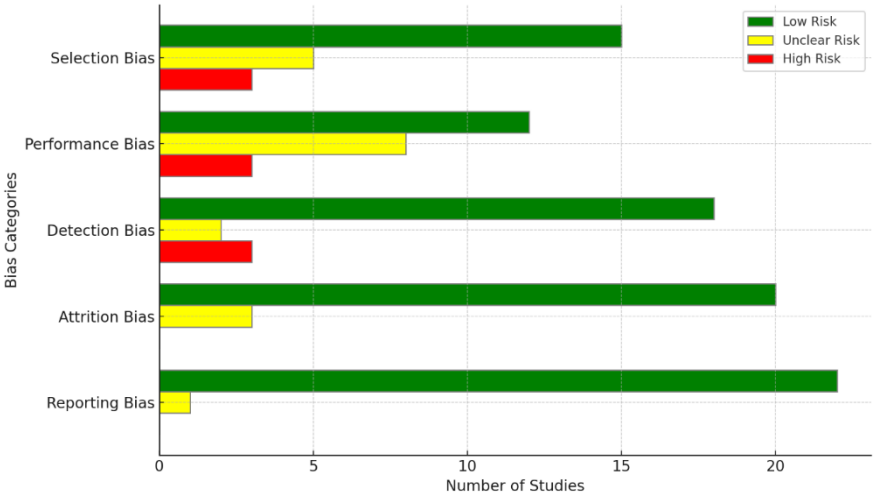

Fig. 6. Risk of bias assessments in the reviewed studies

2.12 Results of the Individual Studies

The discoveries of individual investigations featured an assortment of computer-based intelligence-controlled digital dangers, including artificial intelligence-driven phishing, malware, and ransomware, and further developed dangers such as deepfakes and ill-disposed computer-based intelligence assaults. A few examinations have revealed a considerable expansion in the complexity and recurrence of these dangers. Quite simulated intelligence-driven phishing and malware are recognized as the most common dangers across numerous areas. The viability of AI-fueled protective instruments was likewise a typical subject, with blended results revealed across various settings and techniques.

2.13 Synthesis of Results

The overall findings from the included studies indicate a clear trend toward increasing sophistication and the prevalence of AI-powered cyber threats. There is evidence of significant impacts on various sectors, particularly finance and healthcare, with substantial economic and operational repercussions. The synthesis of results also highlights the evolving nature of these threats and the critical need for adaptive, AI-powered cybersecurity measures to effectively counteract them.

2.14 Risk of Bias Across Studies

Potential predispositions influencing the general audit incorporate a distribution inclination, as studies detailing critical discoveries are bound to be distributed, as are choice predispositions, because of the prohibition of non-English language studies. Moreover, there is a gamble of the tendency to look for predetermined feedback, as studies would have been deciphered in a way that upholds previous convictions about the commonality and seriousness of simulated intelligence-controlled digital dangers. Endeavors were made to moderate these inclinations through thorough pursuit techniques, straightforward determination standards, and cautious translation of study results.

3. RELATED WORKS

The systematic review of AI-powered cyber threats is organized in the following subsections, and at the end, Table 3 summarizes the included studies.

3.1 Historical Context and Evolution of AI in Cybersecurity

The evolution of AI in cybersecurity has transitioned from simple system mastering packages to state-of-the-art deep learning models and predictive analytics, profoundly impacting how cyber threats are recognized, analysed, and mitigated. This nonstop evolution underscores the importance of AI in the improvement of stronger and more powerful cybersecurity techniques to combat the ever-increasing complexity and sophistication of cyber threats.

Yampolsky et al. (2013) explained that the integration of artificial intelligence (AI) into cybersecurity has been a transformative adventure, reshaping defensive mechanisms against cyber threats. Initially, cybersecurity efforts were closely reliant on guiding identity and mitigation strategies, leading to inefficiencies and boundaries in managing the ever-evolving panorama of cyber threats. The creation of AI into cybersecurity has notably enhanced the ability to hit upon,

examine, and respond to threats in actual time. AI's ability to analyse facts, become aware of patterns, and make predictions has been instrumental in developing superior safety structures, which include anomaly detection, danger intelligence, and automated reaction solutions [11].

Lecun et al. (2015) noted that the ancient milestones in AI were pivotal in shaping contemporary cybersecurity approaches. In the 1990s and early A000s, the development of gadget mastering algorithms and neural networks inspired cutting-edge AI abilities. These technologies enabled the analysis of sizeable datasets past human capability, leading to the early forms of intrusion detection systems. Many advancements have been made with the advent of deep study techniques, especially convolutional neural networks (CNNs) and recurrent neural networks (RNNs), which have notably improved hazard detection rates and reduced the number of false positives [12].

Furthermore, (Heaton, 2018) noted that the arrival of natural language processing (NLP) and its integration into cybersecurity practices has allowed for extra sophisticated monitoring of online communications for capability threats and breaches. The software of AI in cybersecurity reached a brand new milestone with the arrival of predictive analytics, permitting protection systems to forecast potential attacks primarily on the basis of ancient information and modern-day developments and improving the proactive abilities of cybersecurity measures [13].

3.2 Types and Mechanisms of Ai-Powered Cyber Threats

Artificial intelligence-controlled digital dangers can be extensively ordered in view of their temperament (e.g., robotized versus versatile), targets (e.g., individual clients, enterprises, government elements), and procedures (e.g., AI calculations, profound learning methods). These dangers influence the ability of artificial intelligence to increase their viability, avoid location, and robotize assaults at scale. Striking classifications incorporate artificial intelligence-driven phishing assaults, which use AI to make and appropriate exceptionally persuasive counterfeit messages; artificial intelligence-controlled malware, which can adjust and transform to sidestep hostile to infection programming; and AI, which works with ransomware that distinguishes and scrambles the most basic documents for an association or person [14] [15][16].

Table 2 Categorizes these threats, and Figure 7 shows the AI-driven threats such as the following:

- AI-Driven Phishing: Present-day phishing assaults utilize artificial intelligence to break down enormous amounts of information from virtual entertainment and different sources to make customized messages that are bound to bamboozle beneficiaries. These messages frequently imitate the style and tone of correspondence from believed sources, essentially expanding the achievement pace of phishing endeavors [17].
- AI-Powered Malware: simulated intelligence has upset malware creation and conveyance, empowering the improvement of self-changing and developing malware that can sidestep customary recognition techniques. These computer-based intelligence-controlled malware projects can investigate the climate and change their way of behaving to stay undetected, introducing critical difficulties for network protection safeguards [18].
- Ransomware Enhanced by AI: Ransomware assaults have become more complex with artificial intelligence, permitting aggressors to target explicit information or frameworks and decide the ideal payoff sum in view of the casualty's apparent capacity to pay. Computer-based intelligence calculations additionally empower the fast examination of organizations to recognize weaknesses and scramble documents all the more effectively[19].
- Advanced persistent threats (APTs): APTs address a class of digital dangers that influence computer-based intelligence to direct long-haul, secretive, and modern assaults. Simulated intelligence empowers these dangers to gain from every connection, working on their capacity to stay undetected and adjust to countermeasures over the long run. These simulated intelligence-driven APTs present critical dangers because of their designated nature and the potential for significant harm or information exfiltration [20].
- Deepfake Techniques: These include the use of AI to make hypersensible yet together engineered media that can delude, control, or take advantage of people or frameworks. Deepfakes can be utilized for making deceitful substances to sidestep biometric safety efforts or for disinformation crushing, which can prompt security breaks [21].
- AI-Poisoning and Model Stealing: Aggressors can control the preparation information or use artificial intelligence models to either ruin computer-based intelligence frameworks, making them incapable, or to comprehend and sidestep computer-based intelligence-driven safety efforts. This compromises the honesty and unwavering quality of artificial intelligence applications in network safety [22] [23].
- Adversarial AI Attacks: In these assaults, slight, frequently impalpable changes are made to enter information (pictures, text, and so on) to hoodwink simulated intelligence frameworks, prompting wrong results or security breaks. This can be especially unfavourable in frameworks that depend on computer-based intelligence for basic navigation or ID assignments [24].

- AI-Enhanced Network Attacks: Computer-based intelligence Improved Organization Assaults: These include the utilization of AI to mechanize and enhance the execution of organization goes after, for example, DDoS assaults, making them more viable and harder to distinguish and check [25].
- Automated Social Engineering Attacks: Simulated intelligence-driven chatbots or informing frameworks can be utilized to execute enormous scope social design assaults, fooling clients into revealing delicate data or performing activities that compromise security [26].
- Supply Chain Attacks: Using computer-based intelligence to examine and recognize weaknesses in an inventory network, aggressors can decisively target explicit parts to upset benefits or penetrate secure conditions [27].

Fig. 7. AI-driven threats

TABLE II. CATEGORIZATION OF AI-POWERED CYBER THREATS

Type of Threat	Mechanism	Impacted Sectors	Potential Impact
AI-Driven Phishing	Uses AI to craft personalized deceptive messages from vast data sources	General, Finance	Data breaches, Financial fraud
AI-Powered Malware	Self-modifying malware that evades detection	General, IT Infrastructure	System compromise, Data theft
Ransomware Enhanced by AI	Targets specific data/systems; determines optimal ransom	Healthcare, Government	Operational disruption, Data loss
Advanced Persistent Threats (APTs)	Long-term, sophisticated attacks that learn and adapt	Government, Finance	Substantial damage, Data exfiltration
Deepfake Techniques	Creates synthetic media to mislead or exploit	Media, Politics	Misinformation, Security breaches
AI-Poisoning and Model Stealing	Manipulates AI training data or steals AI models	Technology, Cybersecurity	Compromised AI integrity, Bypassed security measures
Adversarial AI Attacks	Alters input data to deceive AI systems	Military, Security	Erroneous outcomes, Security breaches
AI-Enhanced Network Attacks	Uses AI to automate and optimize network attacks like DDoS	General, IT Infrastructure	Disrupted services, Hard to detect attacks
Automated Social Engineering Attacks	Employs AI chatbots to trick users into compromising security	General, Social Media	Sensitive information disclosure, Security breaches
Supply Chain Attacks	Uses AI to identify vulnerabilities and target specific components	Manufacturing, Retail	Service disruption, Infiltration of secure environments

3.3 Empirical studies on AI-powered cyber threats

Ongoing experimental investigations have revealed the heightening complexity and predominance of AI-fueled digital dangers. Mishra (2023) highlighted the increasing use of artificial intelligence by cybercriminals to refine the adequacy of assaults, especially in areas such as banking, where simulated intelligence-driven misrepresentation plans are turning out to be progressively normal [28]. Tweneboah-Koduah et al. (2018) affirmed these discoveries, noticing the particular antagonistic effects on stock execution in the monetary area following cyberattacks and highlighting the unmistakable monetary repercussions [29]. Furthermore, Humayun et al. (2020) highlighted the need for development in digital guard components to counter the advancing idea of these dangers [30]. Bago (2023) discussed how cybercriminals influence artificial intelligence to make more designated and sly assaults, further confounding the network protection scene [31].

The application and impact of AI-powered cyber threats vary significantly across different sectors. Varga et al. (2021) explored cyber situational awareness within the Swedish financial sector, identifying unique threats and the need for sector-specific cybersecurity solutions [32]. Gordon et al. (2018) examined how private sector firms, especially in finance, respond to cybersecurity investments, highlighting different strategic approaches based on sector-specific risks and needs [33]. Kaloudi and Li (2020) discussed the more extensive scene of AI-driven threats and highlighted the changing difficulties and countermeasures expected across various businesses, including government and medical services [5]. Ultimately, Darem et al. (2023) described experiences with cybersecurity characterizations and countermeasures, especially in banking and monetary areas, highlighting the significance of tailored guards against AI-powered threats [34].

While the financial and healthcare sectors are fundamentally affected by AI-driven threats, other basic sectors, such as government infrastructure, energy, and education, are additionally helpless. In the energy sector, AI is utilized for the power matrix of the board, assisting with request, distinguishing irregularities, and guaranteeing sustainability. Nonetheless, the reconciliation of AI with these systems presents chances, as threats focused on AI-oversaw frameworks could prompt interruptions influencing both sustainability and security [35].

In government infrastructure, systems such as the PRAETORIAN methodology are created to shield basic infrastructure, including the government and energy sectors, against consolidated cyber and actual threats. This approach upgrades detection and relief, highlighting the crucial role that AI plays in overseeing weaknesses across fundamental administrations [36].

3.4 Theoretical and Methodological Approaches

Examination of AI-powered cyber threats involves various hypothetical systems and approaches. Kaloudi and Li (2020) investigated the AI-based cyber danger scene and proposed a structure that guides the malevolent purposes of AI throughout the cyber-assault life cycle, providing a premise for future danger recognition and counteraction [5]. Shehu et al. (2023) developed a calculation system that coordinates AI devices for breaking down the cyber kill chain, aiming to propel the understanding and moderation of AI-based threats [37]. Moreover, Abbas et al. (2019) featured primary changes in cybersecurity since the rise of AI, encouraging the advancement of new hypotheses and examination bearings to more readily design AI applications in cybersecurity [38]. Ahmad and Krishna Prasad (2023) discussed an AI-empowered structure for cybersecurity via machine learning methods, stressing its pertinence across IoT use cases [39].

Different examination approaches offer wavered bits of information into reproduced knowledge-related network prosperity challenges. Speculative procedures, for example, those described by Kaloudi and Li (2020), provide serious plans that help handle the lifecycle of computerized reasoning-based progressed chances; however, they could require support through exploratory evaluation [5]. Approaches that integrate AI devices, similar to those by Shehu, Umar et al. (2023), offered valuable plans yet faced preventions related to information quality and algorithmic inclinations [37]. Observational assessments, for example, those planned by Abbas et al. (2019), gave credible experiences at any rate that might battle the fast speed of mechanical change in AI and associated security [38]. Finally, PC-based insight-enabled structures such as those proposed by Ahmad and Krishna Prasad (2023) have shown great potential for steady electronic gamble appraisal and require wide testing to guarantee common sense and versatility across various conditions [39].

The following are models that feature the meaning of upgrading hypothetical and strategic conversations with reasonable applications and contextual analyses, accordingly building up the significance and materialness of the examination discoveries.

One such concentrate by Kaloudi and Li (2020) investigated the AI-based cyber danger scene and presented a system that classifies the vindictive purposes of AI throughout the cyber-assault life cycle. The system is applied in a speculative situation, displaying how hypothetical ideas can be operationalized in commonsense settings to foresee and forestall future threats, stressing the utility of organized approaches in understanding complex cyber conditions [5]. One more model is given by Blessing et al. (2022), who researched the danger of AI-powered cyberattacks. They utilize a three-step process zeroing in on-article determination in light of value and significance, subsequently revealing the particular idea of AI-driven attacks. This study highlights the utilization of systemic meticulousness with respect to AI in cybersecurity,

introducing an unmistakable procedure for recognizing and ordering rising threats [40]. Fakiha (2023) inspected associations that have executed AI and machine learning to expand cyber measurable examinations. Through contextual investigations and reviews, they highlighted how AI innovations such as machine learning essentially work on the effectiveness and accuracy of examinations, providing a perfect representation of the use of AI in upgrading cybersecurity rehearses [41]. Moreover, Shehu et al. (2023) applied AI in breaking down the cyber kill chain, fostering a calculated structure that coordinates AI devices for a more nuanced understanding and moderation of AI-based threats. This approach represents how hypothetical systems can direct exact examination and reasonable application in cybersecurity, adding to a more profound and more organized examination of cyber threats [37]. Lee et al. (2019) introduced an AI strategy for cyber-danger discovery in view of artificial brain organizations. Their methodology, which uses profound learning-based location strategies for improved cyber-danger distinguishing proof, features the viable application and results of AI-driven safety efforts in real-world settings [42].

3.5 Detection and Identification Techniques

The writing of AI-based recognition and ID methods for cyber threats has led to considerable development towards additional modern and robotized frameworks. Sai and Niraja (2023) highlighted the use of significant learning strategies, including FCNN, CNN, and LSTM, to redesign the ID of cyber threats, pointing towards the headway of AI-driven security information and event management (AI-SIEM) frameworks [43]. In addition, Jonghoon Lee et al. (2019) highlighted the use of artificial brain networks for chipping away at the precision of cyber-peril acknowledgement by changing security events into individual event profiles [42]. In addition, Ram (2023) presented a unique system for recognizing web chances via AI and brain associations, generally extending the ability to perceive cyber threats [44]. Finally, Sree et al. (2021) presented a model to farsight risk hunting via AI, endorsing its feasibility across certified world datasets and revealing the fundamental occupation of AI-SIEM frameworks in current cybersecurity practices [45].

The sufficiency and adequacy of various artificial intelligence estimations and models in perceiving advanced risks have been comprehensively analysed, with each having its own resources and hindrances. Shuang Xun et al. (2020) proposed a programmed conspicuous verification model of risk information that considers CNNs, which achieves high precision and F1 scores, which better illustrates AI-based models than standard procedures do [46]. Maurya (2023) analysed the occupation of artificial intelligence in network security to distinguish between proofs and expectations, highlighting the ability of intelligence to further develop data assessment, plan affirmation, and irregularity revelation [47]. Khraisat et al. (2019) conducted an exhaustive survey of interruption discovery techniques, grouping them into Mark-based and Peculiarity-based frameworks, and examined the ability of simulated intelligence to handle the development of digital dangers [48]. Hui Wang et al. (2021) depicted an organizational security danger location and discernibility framework in view of simulated intelligence, expecting to increase the recognizable proof and recognizability of digital dangers, showing the effect of computer-based intelligence in providing more compelling online protection arrangements [49]. The work by Alanezi and Aldabagh (2011) introduced an innovative approach to IDS by employing a multilayered structure inspired by the adaptive and innate immunity of the human immune system. This methodology integrates several immunological metaphors, notably adaptive immunity mechanisms characterized by learning adaptability and memory across both humoral and cellular immunity branches. The authors proposed a system that mimics the human immune system's multilevel defense strategy, aiming for a high detection rate with minimal false alarms and providing a robust framework against the dynamic and complex nature of cyber threats [50].

3.6 Mitigation Strategies and Defense Mechanisms

The procedures for directing AI-filled computerized perils are different and progressing. Ehsan Aghaei, Aghaei and Al-Shaer (2019) proposed a web-based insurance procedure that uses robotization to build more useful and monetarily clever shields, which is basic for managing the rising arrangement and volume of computerized risks [51]. Moreover, Alavizadeh et al. (2024) introduced a Markov game model that studies the capability of defensive procedures against recreated intelligence-upheld aggressors, especially in cloud-based frameworks, which provide significant pieces of information to routes [52]. In the domain of conveyed energy resources, Duan et al. (2021) presented balance techniques against cyberattacks, breaking down their ampleness through multiplication, which is basic for ensuring the adaptability of energy frameworks against computerized risks [53]. Jha et al. (2023) broke down the gig of reenacted intelligence in battling cyberterrorism, featuring the meaning of PC-based intelligence-driven techniques in recognizing, hindering, and noting cyberattacks [54].

AI-driven cybersecurity arrangements offer promising paths for improving safety efforts. Meier et al. (2021) examined the improvement of a completely mechanized cyber protection framework that needs no human help to identify and relieve attacks inside complex foundations, featuring movement toward independent security frameworks [55]. Mohamad Fazelnia, Igor Khokhlov, and Mehdi Mirakhorli (2024) introduced a framework for portraying attacks and shortcomings and provided moderation procedures to AI-empowered frameworks, supporting computer programmers in creating strong

AI-empowered programs [56]. Stevens et al. (2019) inspected the advantages of danger demonstrations, an organized interaction for distinguishing dangers and creating relief procedures, inside the New York City Cyber Order [57]. Raj et al. (2022) investigated the effect of AI on network wellbeing, examining different AI countermeasures and ordering them according to their guarded qualities to further develop framework productivity and execution against cyber threats [58]. Alanezi and Aldabagh (2012) presented the Invulnerability PE Malware Identification Framework (IPEMDS), which uses the human insusceptible framework's standards to improve malware location beyond the capacities of conventional antivirus arrangements. By taking on a double-level safeguard that integrates versatile resistance learning and flexibility, IPEMDS offers a strong option in contrast to signature-based techniques, which zero in on heuristic examination and static assessment of executable records. This approach aims for high accuracy and few false positives, leading to a shift towards more dynamic, biologically inspired cybersecurity strategies [59].

3.7 Recent AI Models used in Cyber defense and Cyberattacks

Late headways in AI have impelled the field of cybersecurity, with refined models improving both defensive systems and hostile cyber strategies. Generative adversarial networks (GANs) and deep reinforcement learning (DRL) are among the conspicuous AI models presently broadly utilized in both cyber defense and cyberattacks. GANs have been utilized to mimic adversarial attacks by creating misleading information to test defenses, whereas DRL aids in robotized decision-making for real-time threat reactions, empowering frameworks to independently learn ideal security procedures [43].

On the all-out attack mode side, neural networks, particularly convolutional neural networks (CNNs) and long short-term memory (LSTM) networks, are utilized to create refined malware that can avoid recognition by impersonating harmless information designs [46]. In addition, adversarial machine learning (AML) procedures have empowered aggressors to take advantage of weaknesses in AI-driven systems by quietly changing contributions to mislead models, prompting off-base threat characterization and bypassing security measures [44].

Accordingly, cybersecurity defenses progressively embrace hybrid AI models that combine supervised and unsupervised learning for anomaly detection and predictive analysis, improving the identification of novel threats while adjusting to advancing attack designs [47]. These models coordinate Federated Learning draws near, guaranteeing robust, privacy-safeguarding training on distributed data an enormous benefit in safeguarding delicate data [45].

3.8 Impact of AI-Powered Cyber Threats

The effects of artificial intelligence-fuelled digital dangers reach out across different areas, essentially influencing people, associations, and public safety. Kaloudi and Li (2020) discussed the seriousness of artificial intelligence-based digital dangers and their developing nature, featuring their ability to sidestep customary network safety gauges and incur considerable harm to basic foundations [5]. Blessing et al. (2022) examined the increasing refinement of AI-controlled cyberattacks, focusing on their ability to sidestep recognition and the expanded difficulties they face in accessing network safety frameworks [40]. Shanthi et al. (2023) investigated the extraordinary effect of simulated intelligence on network safety, highlighting both the headways in danger identification and the new weaknesses presented by simulated intelligence advances [60]. Khder et al. (2023) focused on the results of digital assaults worked with by AI, for example, information breaks and wholesale fraud, delineating the extensive danger presented to cultural security [61].

The monetary, mental, and cultural effects of computer-based intelligence in improving digital dangers are significant. Nand Kumar et al. (2023) investigated the capacities of computer-based intelligence in creating modern cyberattacks, noticing the extreme monetary repercussions for organizations because of information misfortune and functional disturbance [62]. Chandana and Gulzar (2023) broke down the impact of AI on network safety, featuring mental consequences for people and associations, such as increased uneasiness and an inescapable feeling of weakness [63]. Ali et al. (2023) examined the dual-use nature of simulated intelligence in online protection, showing how simulated intelligence-driven assaults can compound cultural divisions and subvert trust in advanced frameworks [64]. Mishra (2023) expounded on the effect of simulated intelligence-controlled digital dangers inside the monetary area, highlighting the more extensive cultural ramifications of upset monetary administrations and the disintegration of shopper certainty [28].

3.9 Challenges and Ethical Considerations

Combating AI-powered cyber threats involves navigating a variety of challenges. Coeckelbergh (2019) discussed the ethical challenges and regulatory difficulties posed by artificial intelligence in cybersecurity, emphasizing the need for concrete measures beyond principles to address these evolving threats [65]. Jackson et al. (2023) highlighted the challenges and opportunities in AI ethics education for cybersecurity, pinpointing the importance of comprehensive educational frameworks to prepare future professionals [66]. Peter Bago (2023) elaborated on the support of cyber protection with AI in the finance sector, discussing the overlaps with infrastructural protection and individual security levels [67]. Sunil Chahal (2023) analysed AI-improved Cyber Occurrence Reaction and Recuperation, noticing moral issues such as information

security, decreasing inclination, and legitimate consistency, alongside challenges such as asset deficiencies and innovative cut-off points [68].

The reconciliation of artificial intelligence with online protection raises critical moral issues. Gerke et al. (2020) delineated the moral and lawful difficulties presented by artificial intelligence in medical services, which reflect more extensive worries in online protection, including information security and algorithmic predispositions [69]. Naik et al. (2022) examined lawful and moral issues in AI in medical care, accentuating the requirement for algorithmic straightforwardness and assurance of recipients, which are likewise appropriate in online protection settings [70]. Timmers (2019) broke down the morals of simulated intelligence and online protection according to power and key independence, calling attention to moral quandaries in cautious and hostile activities [71]. Finally, Navdeep et al. (2023) investigated the role of morals in creating secure network safety approaches, underscoring moral goals and difficulties inherent in strategy-making processes [72].

3.10 Future Directions and Emerging Trends

The unique scene of computer-based intelligence and online protection requires consistent exploration to address existing holes and investigate new regions. Hummelholm (2023) dove into AIQUSEC, zeroing in on quantum-safe network protection arrangements, highlighting the dire requirement for adaptable, successful activities against digital dangers, and featuring regions for future investigation, for example, quantum security and AI-based mechanization arrangements [73]. Sarker et al. (2021) introduced a thorough view of AI-driven network safety, proposing bearings for clevering online protection benefits and bringing up holes, for example, security knowledge demonstration and the mix of different simulated intelligence techniques [74]. Ramakrishnan (2023) analysed the expected dangers in store for online protection, encouraging a proactive way to address improving network safety measures against developing dangers in regions such as the IoT, artificial intelligence, and quantum registering [75]. Zeadally et al. (2020) investigated computer-based intelligence's true capacity in further developing network protection arrangements, featuring the improvement of computer-based intelligence methods as future exploration chances to counter all the more heartily [6].

Arising patterns in computer-based intelligence and network safety are forming the fate of advanced security. Farahmand et al. (2021) underlined the reconciliation of simulated intelligence and network safety research in instructive systems, featuring the need for a gifted labor force mindful of the most recent simulated intelligence patterns and online protection challenges [76]. Molloy et al. (2021) investigated simulated intelligence versus simulated intelligence stories in network protection, highlighting the significance of understanding ill-disposed assaults and confirming successful safeguard frameworks in simulated intelligence applications [77]. Sarker (2023) gave bits of knowledge into computer-based intelligence-based demonstrating and antagonistic learning for online protection insight, focusing on the requirement for hearty simulated intelligence models to increase network safety viability and trustworthiness [78]. Corbett and Sajal (2023) examined the role of artificial intelligence in upgrading network safety measures, calling attention to new dangers and the need for new security elements to safeguard computer-based intelligence frameworks [79].

3.11 Regulatory and Policy Implications

Current guidelines and strategies around AI-fueled digital dangers plan to provide structures to alleviate these arising gambles. Srinivas et al. (2019) highlighted the importance of network safety guidelines to force associations to shield their frameworks from cyberattacks, examining different norms in digital safeguarding and engineering of the network protection system [80]. Kaloudi and Li (2020) zeroed in on the simulated intelligence-based digital danger scene, demonstrating the need to understand computer-based intelligence's job in cyberattacks for better administrative systems [5]. Clarke (2019) checked key administrative ideas for simulated intelligence, upholding co guidelines as the most suitable methodology because of specialized and political intricacies [81]. King et al. (2020) dissected the predictable dangers of AI-enabled wrongdoings, providing an establishment for grasping administrative necessities in this space [82].

Future regulatory and strategy measures should improve online protection, considering simulated intelligence advancements. Blessing et al. (2022) inspected artificial intelligence-fuelled cyberattacks and proposed that current digital protection foundations need variation to address the speed and intricacy of computer-based intelligence-driven assaults [40]. Rakha (2023) discussed artificial intelligence's fast development and related administrative difficulties, stressing the requirement for clear guidelines to adjust advancements and chance administrations [83]. Khder et al. (2023) focused on the effect of AI on network protection and proposed that computer-based intelligence can further develop network safety methodologies while additionally requiring updates to security structures to address new difficulties [61]. Nand Kumar et al. (2023) investigated artificial intelligence's extraordinary impact on network protection danger identification and reactions, highlighting the requirement for administrative systems that include artificial intelligence's capacities and limits [62].

TABLE III. SUMMARY OF INCLUDED STUDIES

Study Reference	Year	Objective	Methodology	AI Technologies Evaluated	Types of Cyber Threats	Key Findings	Proposed Solutions	Limitations	Future Research Directions
Mishra (2023)	2023	Explore the role of AI in enhancing cybercriminals' effectiveness, especially in the banking sector.	Empirical study	AI analytics	AI-driven fraud schemes	AI empowers cybercriminals to refine the effectiveness of their attacks, especially in banking.	Not specified	Not specified	Innovation in cyber defense mechanisms.
Tweneboah-Koduah et al. (2018)	2018	Examine the impact of cyberattacks on the stock performance of the financial sector.	Empirical study	Not specified	General cyberattacks	Cyberattacks significantly impact stock performance in the financial sector.	Not specified	Limited to the financial sector.	Sector-specific vulnerability assessments.
Varga et al. (2021)	2021	Explore cyber situational awareness within the Swedish financial sector.	Sector-specific study	Not specified	Sector-specific threats	Identifies unique threats and highlights the need for tailored cybersecurity solutions.	Tailored defenses	Focused on the Swedish financial sector.	Expansion to other sectors and geographical areas.
Kaloudi & Li (2020)	2020	Map out malicious uses of AI across the cyber-attack lifecycle.	Theoretical and empirical framework development	AI-based cyber threat lifecycle	Various AI-based threats	Varying challenges and countermeasures required across different industries.	Dynamic and adaptive security solutions	Generalization issues across different contexts.	Empirical validation and interdisciplinary research.
Darem et al. (2023)	2023	Investigate cybersecurity classifications and countermeasures in the banking and financial sectors.	Sector-specific study	Not specified	AI-powered financial threats	Stresses the importance of tailored defenses against AI-powered threats.	Sector-specific strategies	Focuses on banking and financial sectors only.	Development of more adaptive frameworks.
Shehu et al. (2023)	2023	Develop a framework integrating AI tools to analyse the Cyber Kill Chain.	Conceptual framework development	AI tools, Cyber Kill Chain	Various AI-based threats	Aids in understanding and mitigating AI-based threats.	Integrative AI tools	Conceptual nature without empirical testing.	Empirical testing of the framework's effectiveness.

Ahmad & Krishna Prasad (2023)	2023	Propose an AI-enabled cybersecurity framework for IoT applications.	Conceptual framework development	Machine learning techniques	IoT security threats	Enhances cybersecurity across different IoT scenarios.	AI-enabled cybersecurity solutions	Lack of extensive real-world testing.	Testing across various IoT environments.
Humayun et al. (2020)	2020	Highlight the need for innovation in cyber defense mechanisms against evolving AI-powered threats.	Review	Not specified	Evolving AI-powered threats	Continuous innovation is required in cyber defense mechanisms.	Not specified	Broad focus without specific solutions.	Innovations in defense mechanisms against AI-powered threats.
Bago (2023)	2023	Examine how cybercriminals leverage AI for more targeted and evasive attacks.	Analysis	Not specified	Targeted and evasive attacks	Cybercriminals' capabilities increased with AI utilization.	Not specified	Broad focus without detailing specific AI technologies.	Development of targeted countermeasures and AI-driven defense strategies.

4. DISCUSSION

4.1 Summary of Evidence

The orderly survey of computer-based intelligence-fueled digital dangers reveals the development of refinement and predominance of these dangers across different areas. The development from fundamental AI applications to cutting-edge deep learning models and prescient investigations has essentially affected the distinguishing proof, examination, and relief of digital dangers. The types and systems of simulated intelligence-fueled dangers differ, including computer-based intelligence-driven phishing, malware, ransomware, and high-level constant dangers, revealing a shift towards additional robotized and versatile assaults that challenge existing network protection measures. Figure 8 shows a heatmap in view of speculative information for illustrative purposes, addressing the effect of AI-controlled digital dangers across various areas, including finance, medical services, the government, schooling, and assembly.

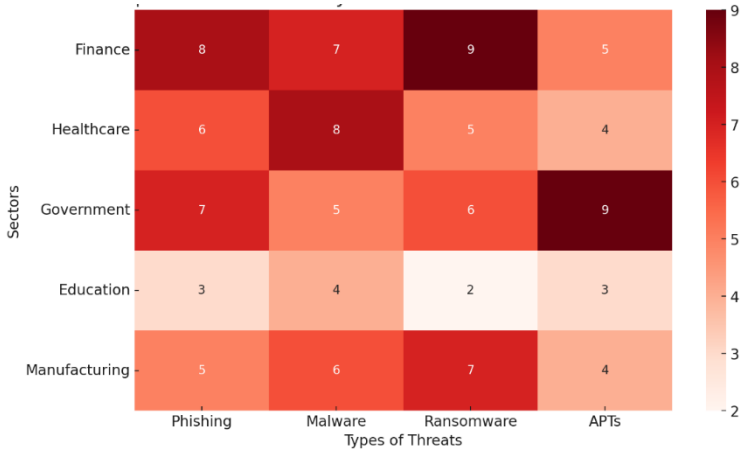

Fig. 8. Heatmap for the impact of AI-powered cyber threats across different sectors

4.2 Limitations

The audit interaction and the included examinations display specific impediments. There, right off the bat, is a potential distribution inclination, as studies with adverse outcomes might be less inclined to be distributed. The rapid advancement of computer-based intelligence innovations and digital dangers implies that even ongoing investigations may not completely capture the ongoing danger scene. In addition, there is geographic and sectoral lopsidedness in the investigation, with an emphasis on unambiguous endeavors and regions, limiting the generalizability of the findings. Moreover, the heterogeneity of study plans and procedures makes it challenging to consider results straightforwardly, which could impact the steadfastness of the blend. These constraints are likewise included in a few investigations, for example:

The inquiry systems might have language limits and information base choices inclinations. For example, limiting the search to English-language articles might reject pertinent examinations in different dialects, possibly prompting a language predisposition. Additionally, the selection of datasets could have discarded enormous examinations distributed in less available or different disciplinary datasets. These angles could restrict the exhaustiveness of the review [84].

The consideration and rejection measures could likewise present determination predispositions, as they could coincidentally sift through investigations with unpredictable strategies or results not expected by the review parameters. This can prompt a slanted portrayal of the subject being reviewed [85].

The course of information extraction is inclined to human mistakes and interpretative predispositions, particularly in the event that the cycle is not checked two times or in the event that the extraction apparatuses utilized are not normalized. This can lead to errors in the information utilized for union and examination [86].

4.3 Implications for Practice

These discoveries highlight the need for network protection practices to develop because of the changing idea of simulated intelligence-fueled dangers. Associations ought to put resources into cutting-edge computer-based intelligence-driven network protection arrangements that can anticipate, recognize, and answer dangers progressively. There should be an emphasis on constant preparation and refreshing of AI models to keep up with the rapidly developing danger scene. Moreover, cross-area joint efforts and data sharing are important for understanding and relieving simulated intelligence-controlled digital dangers. For example, the following studies did that:

Kaloudi and Li (2020) introduced a structure for planning AI-based digital assaults throughout the digital assault life cycle. This system has been applied to dissect AI-based digital assaults in basic foundations such as brilliant networks, providing noteworthy bits of knowledge to online protection experts to foresee and counter future dangers [5]. Lee et al. (2019) developed an artificial intelligence method for digital danger identification in light of counterfeit brain organizations, which was carried out in an AI SIEM framework. This approach has been applied in real situations, essentially further developing the discovery rates and reaction times to digital dangers by utilizing profound learning-based identification techniques [42]. Li et al. (2022) proposed a reasonable knowledge-driven protection component against cutting edge diligent dangers (APTs), which is explicitly intended for asset-restricted edge gadgets in cutting-edge organizations. This component has been shown to further develop the security levels and protection capacities of edge gadgets against complex APTs, providing a model for improving network safety in IoT and edge conditions [87]. Zeadally et al. (2020) examined the coordination of artificial intelligence in network protection arrangements, illustrating the qualities and shortcomings of current AI advances. The experiences from this study have been utilized by associations to reinforce their online protection guards, especially in distinguishing and answering new and modern digital dangers [6].

4.4 Implications for Research

Future examinations should focus on creating normalized systems for assessing simulated intelligence-fuelled digital dangers and their countermeasures. There is a need for additional exact investigations that provide true proof of the viability of various simulated intelligence-driven network safety arrangements. An examination should likewise investigate the moral, legitimate, and administrative parts of involving AI in network safety, resolving issues such as protection, responsibility, and the potential for abuse. Moreover, studies that look at the effects of AI-controlled digital dangers in various areas and geographic locations are needed to foster designated and successful relief techniques.

Figure 9 is a near-bar graph showing the viability of different AI-controlled digital danger moderation techniques in view of speculative information for illustrative purposes. The diagram contrasts customary network protection measures with computer-based intelligence-improved online protection estimates across various danger types, such as phishing, malware, ransomware, and high-level constant dangers (APTs). Every danger type is addressed by two bars, demonstrating the adequacy of conventional and artificial intelligence-upgraded procedures individually. This representation features the regions where computer-based intelligence-driven arrangements have enormous effects compared with conventional techniques.

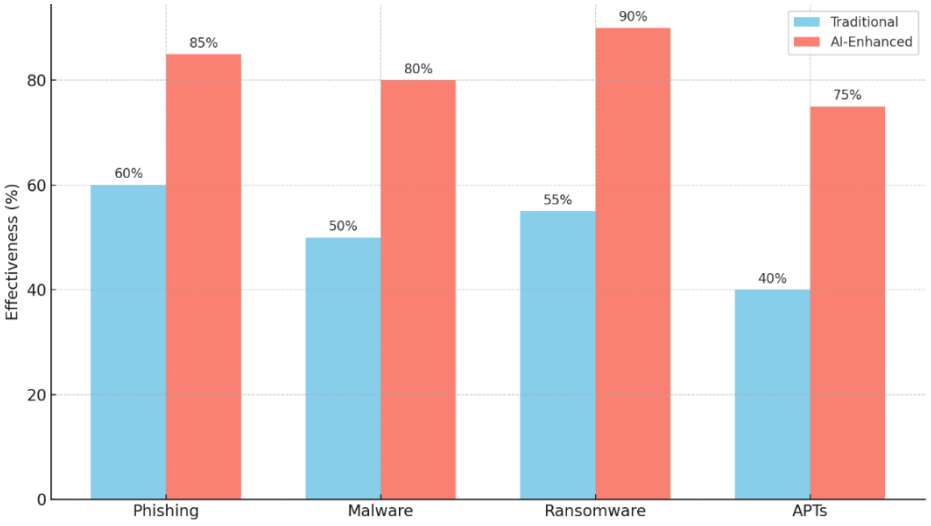

Fig. 9. The effectiveness of various mitigation strategies

Figure 10 shows a pattern line graph outlining the turn of events and reception of simulated intelligence-driven network protection arrangements over the long run, which contrasts with the development of simulated intelligence dangers from 2010--2023. The blue line addresses the development of computer-based intelligence-driven online protection arrangements, whereas the red line portrays the advancement and expansion of simulated intelligence dangers. This perception assists in conveying how headways in online protection resemble the rising intricacy and complexity of computer-based intelligence dangers, highlighting the continuous weapon contest between digital guards and assistants.

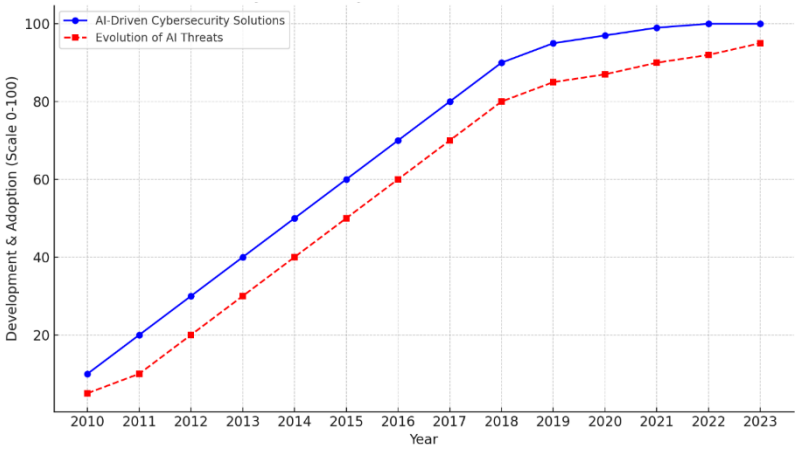

Fig. 10. Trends in AI-driven cybersecurity solutions vs. AI threat evolution (2010--2023)

4.5 Challenges and Ethical Considerations

Tending to address the challenges and ethical considerations in AI-powered cybersecurity is fundamental to exploring the complexities and obligations of this advancing field.

- Challenges in AI-Powered Cybersecurity: The complexity of AI-based threats and the refinement of cyberattacks present challenges in detection and mitigation. For example, AI-powered malware can adjust to sidestep customary safeguards, making static security techniques less compelling. The fast development of AI algorithms likewise requires consistent updates to cybersecurity protocols.
- Resource Constraints: Carrying out advanced AI-driven guards is resource-serious, and more modest associations might battle to embrace these actions, making a uniqueness in cybersecurity status.
- Ethical Considerations: The dual-use nature of AI presents ethical quandaries. The very advances that upgrade cybersecurity can be weaponized by malicious actors. Furthermore, issues of algorithmic bias and the potential

for AI to encroach on user protection should be addressed. There is likewise the requirement for straightforwardness and responsibility in AI-driven frameworks to guarantee that they line up with ethical rules.

4.6 Future Directions

Future exploration should investigate incorporating quantum computing and AI to strengthen cybersecurity guards, underscoring the advancement of algorithms equipped for expecting and appropriating threats as opposed to just responding. Accomplishing robust, adaptive, and ethically sound AI-driven security estimates will require continuous cooperation among technologists, policymakers, and ethicists. Furthermore, laying out worldwide principles and tailored guidelines for AI in cybersecurity is essential to maintain steady and viable practices across areas, closely examining how administrative structures impact the reception and adequacy of these advanced innovations.

Additionally, future studies should emphasize the versatility and integration of these AI systems into different sectors past finance and healthcare, such as government and energy, where data security is principal. By tending to these examination holes, future work can make more far-reaching, adaptable AI models that further develop real-time detection abilities as well as increase data security across various basic infrastructures.

5. CONCLUSIONS

The methodical survey features the rising complexity and pervasiveness of simulated intelligence-fuelled digital dangers, highlighting the critical requirement for cutting-edge network safety estimates that can keep up with the advancing danger scene. The integration of computerized reasoning into online protection has made considerable progress in danger identification, investigation, and reaction capacities. Be that as it may, a similar innovation has been utilized by cybercriminals to foster more modern, computerized, and versatile dangers, testing existing protection instruments.

The key conclusions drawn from the survey highlight the need for consistent variation and improvement in network safety practices to address the unique idea of simulated intelligence-fueled dangers. There is a basic requirement for interest in computer-based intelligence-driven online protection arrangements that are fit for prescient examination, constant recognition, and independent reactions to rising dangers.

Moreover, the survey recognizes a hole in flow research with respect to the complete comprehension of artificial intelligence-controlled digital dangers across various areas and geological districts. This requires more purposeful exertion in observational examination, cross-area cooperation, and data sharing to foster designated and successful online protection systems.

Finally, moral, lawful, and administrative contemplations remain paramount as the utilization of computer-based intelligence in network protection progresses. Tending to these contemplations is fundamental for guaranteeing the mindful and viable utilization of artificial intelligence advances in defending against digital dangers.

All in all, the discoveries of this audit highlight the basic job of simulated intelligence in both the execution and anticipation of digital dangers, featuring the requirement for progressing exploration, advancement, and joint effort to saddle the maximum capacity of computer-based intelligence in improving online protection measures while tending toward related difficulties.

Conflicts of interest

The paper asserts that there are no personal, financial, or professional conflicts of interest.

Acknowledgement

The authors are grateful to the ICT Research Unit at the Computer Center/University of Mosul, Iraq, for supporting the scientific research.

References

[1] A. Clim, “Cyber Security Beyond the Industry 4.0 Era. A Short Review on a Few Technological Promises,” *Inform. Econ.*, vol. 23, no. 2/2019, pp. 34–44, Jun. 2019, doi: 10.12948/issn14531305/23.2.2019.04.

[2] P. Bagó, “Cyber security and artificial intelligence,” *Econ. Finance*, vol. 10, no. 2, pp. 189–212, 2023, doi: 10.33908/EF.2023.2.5.

[3] M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, “Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview,” *Mesopotamian J. Cyber Secur.*, pp. 57–63, Mar. 2023, doi: 10.58496/MJCS/2023/010.

[4] "Cyber Threat Intelligence Market Report 2024 - Cyber Threat Intelligence Market Trends And Overview." Accessed: Nov. 06, 2024. [Online]. Available: https://www.thebusinessresearchcompany.com/report/cyber-threat-intelligence-global-market-report
[5] N. Kaloudi and J. Li, "The AI-Based Cyber Threat Landscape: A Survey," *ACM Comput. Surv.*, vol. 53, no. 1, p. 20:1-20:34, Feb. 2020, doi: 10.1145/3372823.
[6] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," *IEEE Access*, vol. 8, pp. 23817–23837, 2020, doi: 10.1109/ACCESS.2020.2968045.
[7] R. Sarkis-Onofre, F. Catalá-López, E. Aromataris, and C. Lockwood, "How to properly use the PRISMA Statement," *Syst. Rev.*, vol. 10, no. 1, pp. 117, s13643-021-01671-z, Dec. 2021, doi: 10.1186/s13643-021-01671-z.
[8] V. Welch *et al.*, "Extending the PRISMA statement to equity-focused systematic reviews (PRISMA-E 2012): explanation and elaboration," *J. Clin. Epidemiol.*, vol. 70, pp. 68–89, Feb. 2016, doi: 10.1016/j.jclinepi.2015.09.001.
[9] R. Briner and D. Denyer, "Systematic Review and Evidence Synthesis as a Practice and Scholarship Tool," in *Handbook of evidence-based management: Companies, classrooms and research*, 2012, pp. 112–129. doi: 10.1093/oxfordhb/9780199763986.013.0007.
[10] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *Int. J. Surg.*, vol. 8, no. 5, pp. 336–341, Jan. 2010, doi: 10.1016/j.ijsu.2010.02.007.
[11] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits, "Taxonomy for description of cross-domain attacks on CPS," in *Proceedings of the 2nd ACM international conference on High confidence networked systems*, Philadelphia Pennsylvania USA: ACM, Apr. 2013, pp. 135–142. doi: 10.1145/2461446.2461465.
[12] Y. Lecun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015, doi: 10.1038/nature14539.
[13] J. Heaton, "Ian Goodfellow, Yoshua Bengio, and Aaron Courville: Deep learning," *Genet. Program. Evolvable Mach.*, vol. 19, no. 1, pp. 305–307, Jun. 2018, doi: 10.1007/s10710-017-9314-z.
[14] J. Seymour and P. Tully, "Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter," 2016.
[15] Apruzzese et al., "Cyber Law and Espionage Law as Communicating Vessels," 2018.
[16] L. A. E. Al-saeedi *et al.*, "Artificial Intelligence and Cybersecurity in Face Sale Contracts: Legal Issues and Frameworks," *Mesopotamian J. CyberSecurity*, vol. 4, no. 2, Art. no. 2, Aug. 2024, doi: 10.58496/MJCS/2024/0012.
[17] J. Hong, T. Kim, J. Liu, N. Park, and S.-W. Kim, "Phishing URL Detection with Lexical Features and Blacklisted Domains," in *Adaptive Autonomous Secure Cyber Systems*, S. Jajodia, G. Cybenko, V. S. Subrahmanian, V. Swarup, C. Wang, and M. Wellman, Eds., Cham: Springer International Publishing, 2020, pp. 253–267. doi: 10.1007/978-3-030-33432-1_12.
[18] J. Gao, J. Lanchantin, M. L. Soffa, and Y. Qi, "Black-Box Generation of Adversarial Text Sequences to Evade Deep Learning Classifiers," in *2018 IEEE Security and Privacy Workshops (SPW)*, May 2018, pp. 50–56. doi: 10.1109/SPW.2018.00016.
[19] G. Wangen and A. Shalaginov, "Quantitative Risk, Statistical Methods and the Four Quadrants for Information Security," in *Risks and Security of Internet and Systems*, C. Lambrinoudakis and A. Gabillon, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2016, pp. 127–143. doi: 10.1007/978-3-319-31811-0_8.
[20] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017, doi: 10.1109/ACCESS.2017.2762418.
[21] B. Dolhansky *et al.*, "The DeepFake Detection Challenge (DFDC) Dataset," Oct. 27, 2020, *arXiv*: arXiv:2006.07397. Accessed: Mar. 10, 2024. [Online]. Available: http://arxiv.org/abs/2006.07397
[22] M. Jagielski, A. Oprea, B. Biggio, C. Liu, C. Nita-Rotaru, and B. Li, "Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning," Sep. 28, 2021, *arXiv*: arXiv:1804.00308. Accessed: Mar. 10, 2024. [Online]. Available: http://arxiv.org/abs/1804.00308
[23] B. Biggio and F. Roli, "Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning," *Pattern Recognit.*, vol. 84, pp. 317–331, Dec. 2018, doi: 10.1016/j.patcog.2018.07.023.
[24] I. Goodfellow, P. McDaniel, and N. Papernot, "Making machine learning robust against adversarial inputs," *Commun. ACM*, vol. 61, no. 7, pp. 56–66, Jun. 2018, doi: 10.1145/3134599.
[25] U. Kumar, S. Navaneet, N. Kumar, and S. C. Pandey, "Isolation of DDoS Attack in IoT: A New Perspective," *Wirel. Pers. Commun.*, vol. 114, no. 3, pp. 2493–2510, Oct. 2020, doi: 10.1007/s11277-020-07486-w.
[26] A. A. Cain, M. E. Edwards, and J. D. Still, "An exploratory study of cyber hygiene behaviors and knowledge," *J. Inf. Secur. Appl.*, vol. 42, pp. 36–45, Oct. 2018, doi: 10.1016/j.jisa.2018.08.002.

[27] Y. Wang, M. Singgih, J. Wang, and M. Rit, "Making sense of blockchain technology: How will it transform supply chains?," *Int. J. Prod. Econ.*, vol. 211, pp. 221–236, May 2019, doi: 10.1016/j.ijpe.2019.02.002.
[28] S. Mishra, "Exploring the Impact of AI-Based Cyber Security Financial Sector Management," *Appl. Sci.*, vol. 13, no. 10, p. 5875, May 2023, doi: 10.3390/app13105875.
[29] S. Tweneboah-Kodua, F. Atsu, and W. Buchanan, "Impact of cyberattacks on stock performance: a comparative study," *Inf. Comput. Secur.*, vol. 26, no. 5, pp. 637–652, Jan. 2018, doi: 10.1108/ICS-05-2018-0060.
[30] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," *Arab. J. Sci. Eng.*, vol. 45, no. 4, pp. 3171–3189, Apr. 2020, doi: 10.1007/s13369-019-04319-2.
[31] P. Bagó, "Cyber security and artificial intelligence," *Econ. Finance*, vol. 10, no. 2, pp. 189–212, 2023, doi: 10.33908/EF.2023.2.5.
[32] S. Varga, J. Brynielsson, and U. Franke, "Cyber-threat perception and risk management in the Swedish financial sector," *Comput. Secur.*, vol. 105, p. 102239, Jun. 2021, doi: 10.1016/j.cose.2021.102239.
[33] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms," *J. Inf. Secur.*, vol. 09, no. 02, pp. 133–153, 2018, doi: 10.4236/jis.2018.92010.
[34] A. A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, S. M. Alanazi, and S. A. Ebad, "Cyber Threats Classifications and Countermeasures in Banking and Financial Sector," *IEEE Access*, vol. 11, pp. 125138–125158, 2023, doi: 10.1109/ACCESS.2023.3327016.
[35] J.-H. Syu, J. C.-W. Lin, and G. Srivastava, "AI-Based Electricity Grid Management for Sustainability, Reliability, and Security," *IEEE Consum. Electron. Mag.*, vol. 13, no. 1, pp. 91–96, Jan. 2024, doi: 10.1109/MCE.2023.3264884.
[36] L. Papadopoulos *et al.*, "Protection of critical infrastructures from advanced combined cyber and physical threats: The PRAETORIAN approach," *Int. J. Crit. Infrastruct. Prot.*, vol. 44, p. 100657, Mar. 2024, doi: 10.1016/j.ijcip.2023.100657.
[37] A. Shehu, M. Umar, and A. Aliyu, "Cyber Kill Chain Analysis Using Artificial Intelligence," *Asian J. Res. Comput. Sci.*, vol. 16, no. 3, pp. 210–219, Aug. 2023, doi: 10.9734/ajrcos/2023/v16i3357.
[38] N. Abbas, T. Ahmed, S. H. U. Shah, M. Omar, and H. Park, "Investigating the applications of artificial intelligence in cyber security," *Scientometrics*, vol. 121, pp. 1189–1211, 2019, doi: 10.1007/s11192-019-03222-9.
[39] S. S. Ahmad and Krishna Prasad K, "An Artificial Intelligence (AI) Enabled Framework for Cyber Security Using Machine Learning Techniques," 2023.
[40] G. Blessing, A. Azeta, S. Misra, V. Osamor, L. F. Sanz, and V. Pospelova, "The Emerging Threat of Ai-driven Cyber Attacks: A Review," *Appl. Artif. Intell.*, vol. 36, 2022, doi: 10.1080/08839514.2022.2037254.
[41] B. Fakiha, "Enhancing Cyber Forensics with AI and Machine Learning: A Study on Automated Threat Analysis and Classification," *Int. J. Saf. Secur. Eng.*, 2023, doi: 10.18280/ijsse.130412.
[42] J. Lee, J. Kim, I. Kim, and K. Han, "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles," *IEEE Access*, vol. 7, pp. 165607–165626, 2019, doi: 10.1109/ACCESS.2019.2953095.
[43] P. R. Sai and K. S. Niraja, "Cyber Threat Detection Based on Artificial Neural Networks," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 10, pp. 1469–1472, Oct. 2023, doi: 10.22214/ijraset.2023.56193.
[44] K. V. S. Ram, "Detecting Cybersecurity Threats Using AI Network," vol. 5, no. 5, 2023.
[45] V. S. Sree, C. S. Koganti, S. K. Kalyana, and P. Anudeep, "Artificial Intelligence Based Predictive Threat Hunting In The Field of Cyber Security," *2021 2nd Glob. Conf. Adv. Technol. GCAT*, pp. 1–6, 2021, doi: 10.1109/GCAT52182.2021.9587507.
[46] S. Xun, X. Li, and Y. Gao, "AITI: An Automatic Identification Model of Threat Intelligence Based on Convolutional Neural Network," in *Proceedings of the 2020 the 4th International Conference on Innovation in Artificial Intelligence*, in ICIAI '20. New York, NY, USA: Association for Computing Machinery, Jun. 2020, pp. 20–24. doi: 10.1145/3390557.3394305.
[47] R. Maurya, "Analyzing the Role of AI in Cyber Security Threat Detection & Prevention," *Int. J. Res. Appl. Sci. Eng. Technol.*, 2023, doi: 10.22214/ijraset.2023.56510.
[48] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, 2019, doi: 10.1186/s42400-019-0038-7.
[49] H. Wang *et al.*, "Design and research of network security threat detection and traceability system based on AI," vol. 12079, pp. 120790–120790, 2021, doi: 10.1117/12.2622727.
[50] M. Alanezi and Aldabagh, *An Immune Inspired Multilayer IDS*. 2011. doi: 10.13140/RG.2.2.30769.02405.
[51] E. Aghaei and E. Al-Shaer, "ThreatZoom: neural network for automated vulnerability mitigation," *Proc. 6th Annu. Symp. Hot Top. Sci. Secur.*, 2019, doi: 10.1145/3314058.3318167.
[52] H. Alavizadeh, J. Jang, T. Alpcan, and S. Çamtepe, "A Markov Game Model for AI-based Cyber Security Attack Mitigation," *ArXiv*, vol. abs/2107.09258, 2021, Accessed: Mar. 11, 2024. [Online]. Available:

https://consensus.app/papers/markov-game-model-aibased-cyber-security-attack-alavizadeh/eed995d94a6255b7b9e6dc4f5a4fb8f2/
[53] N. Duan *et al.*, "Mitigation Strategies Against Cyberattacks on Distributed Energy Resources," *2021 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. ISGT*, pp. 1–5, 2021, doi: 10.1109/ISGT49243.2021.9372173.
[54] A. Jha, R. Bahuguna, S. Kathuria, G. Sunil, M. Gupta, and V. Pachouri, "Role of AI in Combating Cyber Terrorism," *2023 4th Int. Conf. Smart Electron. Commun. ICOSEC*, pp. 1156–1160, 2023, doi: 10.1109/ICOSEC58147.2023.10275910.
[55] R. Meier, A. Lavrenovs, K. Heinäaro, L. Gambazzi, and V. Lenders, "Towards an AI-powered Player in Cyber Defence Exercises," *2021 13th Int. Conf. Cyber Confl. CyCon*, pp. 309–326, 2021, doi: 10.23919/CyCon51939.2021.9467801.
[56] M. Fazelnia, I. Khokhlov, and M. Mirakhorli, "Attacks, Defenses, And Tools: A Framework To Facilitate Robust AI/ML Systems," *ArXiv*, vol. abs/2202.09465, 2022, Accessed: Mar. 13, 2024. [Online]. Available: https://consensus.app/papers/attacks-defenses-tools-framework-facilitate-robust-aiml-fazelnia/f158fd5a4ea058958c911cb772e58bbf/
[57] R. Stevens, D. Votipka, E. M. Redmiles, C. Ahern, and M. L. Mazurek, "Applied Digital Threat Modeling: It Works," *IEEE Secur. Priv.*, vol. 17, pp. 35–42, 2019, doi: 10.1109/MSEC.2019.2909714.
[58] R. Raj, J. Kumar, and A. Kumari, "HOW AI USED TO PREVENT CYBER THREATS," *Int. Res. J. Comput. Sci.*, 2022, doi: 10.26562/irjcs.2022.v0907.002.
[59] M. Alanezi and Aldabagh, *Using Two levels danger model of the Immune System for Malware Detection*. 2012. doi: 10.13140/RG.2.2.36221.61924.
[60] R. R. Shanthi, N. K. Sasi, and P. Gouthaman, "A New Era of Cybersecurity: The Influence of Artificial Intelligence," *2023 Int. Conf. Netw. Commun. ICNWC*, pp. 1–4, 2023, doi: 10.1109/ICNWC57852.2023.10127453.
[61] M. A. Khder, S. Shorman, D. A. Showaiter, A. Zowayed, and S. I. Zowayed, "Review Study of the Impact of Artificial Intelligence on Cyber Security," *2023 Int. Conf. IT Innov. Knowl. Discov. ITIKD*, pp. 1–6, 2023, doi: 10.1109/ITIKD56332.2023.10099788.
[62] N. K. et Kumar et al., "AI in Cybersecurity: Threat Detection and Response with Machine Learning," *Tuijin JishuJournal Propuls. Technol.*, vol. 44, no. 3, Art. no. 3, Sep. 2023, doi: 10.52783/tjjpt.v44.i3.237.
[63] P. Chandana and C. M. Gulzar, "Securing Cyberspace: A Comprehensive Journey through AI's Impact on Cyber Security," *Tuijin JishuJournal Propuls. Technol.*, 2023, doi: 10.52783/tjjpt.v44.i2.136.
[64] A. Ali *et al.*, "The Effect of Artificial Intelligence on Cybersecurity," *2023 Int. Conf. Bus. Anal. Technol. Secur. ICBATS*, pp. 1–7, 2023, doi: 10.1109/ICBATS57792.2023.10111151.
[65] M. Coeckelbergh, "Artificial Intelligence: Some ethical issues and regulatory challenges," vol. 2019, pp. 31–34, 2019, doi: 10.26116/TECHREG.2019.003.
[66] D. Jackson, S. Matei, and E. Bertino, "Artificial Intelligence Ethics Education in Cybersecurity: Challenges and Opportunities: a focus group report," *ArXiv*, vol. abs/2311.00903, 2023, doi: 10.48550/arXiv.2311.00903.
[67] P. Bago, "Cyber security and artificial intelligence," *Econ. Amp Finance*, 2023, doi: 10.33908/ef.2023.2.5.
[68] S. Chahal, "AI-Enhanced Cyber Incident Response and Recovery," *Int. J. Sci. Res. IJSR*, 2023, doi: 10.21275/sr231003163025.
[69] S. Gerke, T. Minssen, and G. Cohen, "Ethical and legal challenges of artificial intelligence-driven healthcare," *Artif. Intell. Healthc.*, 2020, doi: 10.1016/B978-0-12-818438-7.00012-5.
[70] N. Naik *et al.*, "Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?," *Front. Surg.*, vol. 9, 2022, doi: 10.3389/fsurg.2022.862322.
[71] P. Timmers, "Ethics of AI and Cybersecurity When Sovereignty is at Stake," *Minds Mach.*, vol. 29, pp. 635–645, 2019, doi: 10.1007/s11023-019-09508-4.
[72] A. G. Navdeep, "The Role of Ethics in Developing Secure Cyber-Security Policies," *Tuijin JishuJournal Propuls. Technol.*, 2023, doi: 10.52783/tjjpt.v43.i4.2346.
[73] A. Hummelholm, "AI-based quantum-safe cybersecurity automation and orchestration for edge intelligence in future networks," *Eur. Conf. Cyber Warf. Secur.*, 2023, doi: 10.34190/eccws.22.1.1211.
[74] S. Y. . Mohammed and M. . Aljanabi, "From Text to Threat Detection: The Power of NLP in Cybersecurity", SHIFRA, vol. 2024, pp. 1–7, Jan. 2024, doi: 10.70470/SHIFRA/2024/001
[75] R. Ramakrishnan, "The Future of Cybersecurity and Its Potential Threats," *Int. J. Res. Appl. Sci. Eng. Technol.*, 2023, doi: 10.22214/ijraset.2023.54603.
[76] F. Farahmand, J. Grossklags, J. Mirkovic, and B. Newhouse, "Integrating Cybersecurity and Artificial Intelligence Research in Engineering and Computer Science Education," *IEEE Secur. Priv.*, vol. 19, pp. 104–110, 2021, doi: 10.1109/MSEC.2021.3103460.

[77] I. Molloy, J. Rao, and M. Stoecklin, “AI vs. AI: Exploring the Intersections of AI and Cybersecurity,” *Proc. 2021 ACM Workshop Secur. Priv. Anal.*, 2021, doi: 10.1145/3445970.3456286.
[78] I. H. Sarker, “Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview,” *Secur. Priv.*, vol. 6, 2023, doi: 10.1002/spy2.295.
[79] M. Corbett and S. Sajal, “AI in Cybersecurity,” *2023 Intermt. Eng. Technol. Comput. IETC*, pp. 334–338, 2023, doi: 10.1109/IETC57902.2023.10152034.
[80] J. Srinivas, A. Das, and N. Kumar, “Government regulations in cyber security: Framework, standards and recommendations,” *Future Gener Comput Syst*, vol. 92, pp. 178–188, 2019, doi: 10.1016/j.future.2018.09.063.
[81] R. Clarke, “Regulatory alternatives for AI,” *Comput Law Secur Rev*, vol. 35, pp. 398–409, 2019, doi: 10.1016/J.CLSR.2019.04.008.
[82] M. Burhanuddin, “Secure and Scalable Quantum Cryptographic Algorithms for Next-Generation Computer Networks”, KHWARIZMIA, vol. 2023, pp. 95–102, Jul. 2023, doi: 10.70470/KHWARIZMIA/2023/009
[83] L. Hussain, “Fortifying AI Against Cyber Threats Advancing Resilient Systems to Combat Adversarial Attacks”, EDRAAK, vol. 2024, pp. 28–33, Mar. 2024, doi: 10.70470/EDRAAK/2024/004
[84] E. Grames, A. N. Stillman, M. Tingley, and C. Elphick, “An automated approach to identifying search terms for systematic reviews using keyword co-occurrence networks,” *Methods Ecol. Evol.*, vol. 10, pp. 1645–1654, 2019, doi: 10.1111/2041-210X.13268.
[85] A. Booth *et al.*, “Structured methodology review identified seven (RETREAT) criteria for selecting qualitative evidence synthesis approaches.,” *J. Clin. Epidemiol.*, vol. 99, pp. 41–52, 2018, doi: 10.1016/j.jclinepi.2018.03.003.
[86] V. Garousi and M. Felderer, “Experience-based guidelines for effective and efficient data extraction in systematic reviews in software engineering,” *Proc. 21st Int. Conf. Eval. Assess. Softw. Eng.*, 2017, doi: 10.1145/3084226.3084238.
[87] H. Li, J. Wu, H. Xu, G. Li, and M. Guizani, “Explainable Intelligence-Driven Defense Mechanism Against Advanced Persistent Threats: A Joint Edge Game and AI Approach,” *IEEE Trans. Dependable Secure Comput.*, vol. 19, pp. 757–775, 2022, doi: 10.1109/tdsc.2021.3130944.