Akademika 95(3), October 2025
https://doi.org/10.17576/akad-2025-9503-14

Can AI Outsmart Cybercriminals? A Systematic Review of AI-Driven Cyber Defense

Bolehkah AI Mengatasi Penjenayah Siber? Satu Sorotan Bersistematik Terhadap Pertahanan Siber Berasaskan AI

MUHAMMAD ADNAN PITCHAN*, AKMAR HAYATI AHMAD GHAZALI & EDY PRIHANTORO

Received: 20-3-2025 /Accepted: 13-8-2025

ABSTRACT

Cybercrime has become a critical challenge in the digital age, posing significant threats to individuals, businesses, and global infrastructures. As cybercriminals leverage sophisticated techniques, traditional cybersecurity measures often struggle to keep pace. Artificial Intelligence (AI) has emerged as a transformative tool in cybersecurity, offering automated, adaptive, and intelligent solutions for threat detection, incident response, and fraud prevention. This systematic literature review (SLR) synthesizes findings from 47 peer-reviewed studies, selected from an initial pool of 67 eligible studies, to examine AI's role in cyber defense. Articles were retrieved from Scopus, Web of Science, and IEEE Xplore through systematic screening based on inclusion and exclusion criteria. The review explores machine learning (ML), deep learning (DL), blockchain security, adversarial AI, and explainable AI (XAI) in mitigating cyber threats, including malware, phishing, ransomware, and financial fraud. Findings indicate that AI-driven threat detection systems significantly improve accuracy, with models achieving over 99% precision in malware and fraud detection. AI-powered forensic tools enhance cybercrime investigations, while deep reinforcement learning (DRL) and user behavior analytics bolster proactive cybersecurity measures. However, challenges remain, including algorithmic bias, adversarial attacks, ethical concerns, and regulatory gaps. The study underscores the need for transparent AI policies, interdisciplinary cybersecurity strategies, and global cooperation to ensure responsible AI deployment. This review provides key insights for researchers, policymakers, and cybersecurity professionals by identifying emerging trends, limitations, and future research directions. It emphasizes the necessity of adaptive, ethical, and explainable AI frameworks to address evolving cyber threats and fortify digital security in an increasingly interconnected world.

Keywords: Artificial Intelligence; Cybersecurity; Machine Learning; Fraud Detection; Cyber Threats; Policy Development

ABSTRAK

Jenayah siber telah menjadi cabaran kritikal dalam era digital, menimbulkan ancaman besar kepada individu, perniagaan, dan infrastruktur global. Memandangkan penjenayah siber menggunakan teknik yang semakin canggih, langkah-langkah keselamatan siber tradisional sering kali bergelut untuk mengikutinya. Kecerdasan Buatan (AI) telah muncul sebagai alat transformatif dalam keselamatan siber, menawarkan penyelesaian yang automatik, adaptif, dan pintar bagi pengesanan ancaman, tindak balas insiden, serta pencegahan penipuan. Kajian literatur sistematik (SLR) ini mensintesis penemuan daripada 47 kajian yang telah dikaji semula oleh rakan penyelidik (peer-reviewed), yang dipilih daripada jumlah awal 67 kajian yang layak, untuk meneliti peranan AI dalam pertahanan siber. Artikel diperoleh daripada Scopus, Web of Science, dan IEEE Xplore melalui saringan sistematik berdasarkan kriteria inklusi dan eksklusi. Kajian ini meneroka penggunaan pembelajaran mesin (ML), pembelajaran mendalam (DL), keselamatan rantaian blok (blockchain security), AI musuh (adversarial AI), dan AI yang boleh dijelaskan (XAI) dalam mengurangkan ancaman siber seperti perisian hasad (malware), serangan pancingan data (phishing), perisian tebusan (ransomware), serta penipuan kewangan. Dapatan kajian menunjukkan bahawa sistem pengesanan ancaman yang dipacu oleh AI secara ketara meningkatkan ketepatan, dengan model mencapai lebih daripada 99% ketepatan dalam pengesanan perisian hasad dan penipuan kewangan. Alat forensik yang dikuasakan oleh AI mempertingkatkan penyiasatan jenayah siber, manakala pembelajaran pengukuhan mendalam (DRL) serta analitik tingkah laku pengguna mengukuhkan langkah keselamatan siber secara proaktif. Walau bagaimanapun, masih terdapat cabaran yang perlu diatasi, termasuk bias algoritma, serangan musuh terhadap AI, kebimbangan etika, serta jurang dalam peraturan dan dasar kawal selia. Kajian ini menekankan keperluan untuk dasar AI yang telus, strategi keselamatan siber yang merentas disiplin, serta kerjasama global bagi memastikan penggunaan AI yang bertanggungjawab. Sorotan ini menyediakan pandangan utama kepada penyelidik, pembuat dasar, dan profesional keselamatan siber dengan mengenal pasti trend yang sedang muncul, batasan, serta arah penyelidikan masa depan. Ia turut menekankan keperluan untuk kerangka AI yang adaptif, beretika, dan boleh dijelaskan dalam menangani ancaman siber yang semakin berkembang serta memperkukuhkan keselamatan digital dalam dunia yang semakin saling berhubung.

Keywords: Kecerdasan Buatan; Keselamatan Siber; Pembelajaran Mesin; Pengesanan Penipuan; Ancaman Siber; Pembangunan Dasar

INTRODUCTION

The Internet has become a fundamental component of everyday life across societies, industries, and regions worldwide. Every segment of the population is influenced by new media, reflecting the increasing advancement of information and communication technology in the country. With the Internet, daily tasks can be carried out more quickly and conveniently (Muhammad Adnan, 2019). However, cybercrime has emerged as one of the most pressing challenges in the digital age, posing significant threats to individuals, businesses, and critical infrastructures (Ahmad Arifin et al., 2019). The evolution of cyber threats from rudimentary viruses like the ILOVEYOU worm (2000) to sophisticated, AI-powered attacks such as ransomware epidemics like WannaCry (2017) and deepfake fraud has disrupted critical infrastructure, compromised sensitive data, and is projected to cost the global economy an estimated $10.5 trillion annually by 2025 (Rishad, 2025). Sectors such as healthcare, finance, and energy face disproportionate risks, with healthcare breaches now averaging $10.9 million per incident (IBM, 2023) and ransomware attacks on energy grids, like the 2021 Colonial Pipeline incident, exposing vulnerabilities in legacy cybersecurity systems. As digital systems become increasingly interconnected, cybercriminals exploit vulnerabilities in technologies such as blockchain, the Internet of Things (IoT), and cross-border payment systems, revealing the limitations of traditional cybersecurity measures such as signature-based detection and rule-driven protocols (Gushelmi et al., 2024).

In response, Artificial Intelligence (AI) has gained prominence as a transformative force, offering intelligent, automated (Junaidi, 2024) and adaptive solutions for detecting, mitigating, and preventing cyber threats. AI-driven cybersecurity solutions enhance proactive defense through deep reinforcement learning (DRL), which simulates cyberattacks to train systems (Oh et al., 2024), and explainable AI (XAI) frameworks that improve transparency in malware detection (Galli et al., 2024). AI models also significantly improve fraud detection, with XGBoost achieving 99.1% accuracy (Almurshid et al., 2024), while IBM's Watson has reduced threat investigation time by 60% (IBM, 2023), and Darktrace's AI has successfully stopped ransomware attacks in as little as four seconds (2022).

For instance, blockchain-based systems, widely adopted in financial and healthcare industries, remain vulnerable to fraudulent transactions. Mohammed et al. (2023) propose a machine learning (ML)-driven system for fraud detection in blockchain-based healthcare networks, where Random Forest outperforms other models. Similarly, Lokanan & Maddhesia (2025) explore AI's role in supply chain fraud detection, demonstrating the effectiveness of CatBoost classifiers in identifying deceptive consumer behaviors. Beyond fraud detection, AI plays a crucial role in countering malware, ransomware, and insider threats. Ahmed (2024) applies the Modified Single Value Neutrosophic Fuzzy Soft Expert Set (M-SVNFSES) technique for ransomware detection in financial datasets, while Yilmaz & Can (2024) investigate AI-driven insider threat detection, leveraging user behavior analytics and Natural Language Processing (NLP) to identify malicious activities before they escalate.

The financial sector, a frequent target of cybercriminals, has seen significant AI-driven innovations. Bryssinck et al. (2024) explore the use of synthetic data to develop fraud prevention models for cross-border payments, addressing key challenges related to data privacy and sharing restrictions. Wen & Han (2024) propose an IoT-based transaction security framework, integrating blockchain and AI to detect unauthorized access and prevent fraudulent transactions. Additionally, Karacayılmaz & Artuner (2024) develop an expert system for securing Industrial Internet of Things (IIoT) infrastructures, leveraging rule-based reasoning, anomaly detection, and

reinforcement learning to defend against threats such as denial-of-service (DoS) attacks, data manipulation, and device hijacking.

Despite AI's successes, its deployment in cybersecurity presents significant challenges. Adversarial attacks exploit AI vulnerabilities, as seen in Barik & Misra (2024) study, where evasion techniques bypassed deep learning models. Ethical dilemmas also arise: Italy's 2023 ban on AI facial recognition (Maras & Logie, 2024) underscores tensions between security and privacy under GDPR. Furthermore, while Africa's cybersecurity market grows at a 15% CAGR (World Bank, 2023), AI adoption lags due to resource constraints. These gaps technical, ethical, and regional highlight the need for interdisciplinary research and policy innovation to ensure responsible AI deployment in cybersecurity.

However, studies investigating the mechanisms through which AI enhances cybersecurity and combats cybercrime have been relatively scarce, particularly regarding long-term effectiveness, adaptability, and ethical considerations. This study aims to review existing literature on AI-driven cybersecurity solutions, focusing on their role in threat detection, incident response, fraud prevention, and policy development. Additionally, it examines how AI interacts with other cybersecurity technologies such as blockchain and big data analytics to strengthen digital security. This review is expected to provide meaningful insights into the current applications of AI in cybersecurity, highlight emerging challenges and limitations, and offer recommendations for future studies on improving AI-driven cyber defense strategies.

The aim of this systematic literature review is to fill gaps in previous reviews by assessing trends in AI-driven cybersecurity research. First, we investigate contextual trends, such as the domains and sectors where AI cybersecurity solutions have been implemented, including applications across different cyber threats such as malware detection, phishing prevention, fraud detection, and intrusion response. Second, we explore the mechanisms through which AI enhances cybersecurity, particularly whether AI is predominantly used for proactive threat prevention or reactive incident response. Finally, we examine the ethical considerations and policy trends related to AI-driven cybersecurity, including concerns about privacy, bias, and regulatory frameworks.

To provide deeper insights and contribute to ongoing research on AI applications in cybersecurity, this systematic literature review (SLR) is based on the following research questions:

RQ1: How is AI being applied to detect and prevent different types of cyber threats, such as hacking, malware, phishing, and fraud?
RQ2: What are the primary AI-driven mechanisms used for cybersecurity, and are they more focused on proactive prevention or reactive incident response?
RQ3: What ethical and regulatory challenges arise from AI-driven cybersecurity solutions, and how can they be addressed to ensure responsible AI deployment?

By analyzing AI's role in blockchain security (Mohammed et al., 2023), cross-border fraud prevention (Bryssinck et al., 2024), and adversarial defense (Louati et al., 2024), this review provides actionable insights for researchers, policymakers, and cybersecurity professionals. It emphasizes the urgency of transparent AI governance, global collaboration, and adaptive frameworks to combat evolving cyber threats in an interconnected world.

LITERATURE REVIEW

In an era where digital transformation is reshaping industries and societies, the proliferation of cyber threats has emerged as a critical challenge (Tin et al., 2024). Cybercriminals are leveraging advanced technologies to orchestrate sophisticated attacks, ranging from ransomware and phishing to deepfakes and Advanced Persistent Threats (APTs). These threats not only jeopardize individual privacy and organizational integrity but also undermine global economic stability. Against this backdrop, artificial intelligence (AI) has emerged as a transformative force in cybersecurity, offering innovative solutions for detecting, preventing, and mitigating cybercrime.

The integration of AI into defensive strategies and detection mechanisms has revolutionized the ability to counteract cyber threats. AI-driven cybersecurity solutions leverage machine learning models, deep learning architectures, and graph-based analytics to enhance threat identification and mitigation. Alshattnawi et al. (2024) highlight the use of contextualized embeddings like BERT and ELMo to enhance spam detection on platforms like Twitter and YouTube, achieving accuracy scores of up to 94%. Similarly, Chibi et al. (2024) propose a novel approach that integrates machine learning, blockchain, and Markov Decision Processes to secure smart grids, ensuring accurate storage of events reported by network devices.

AI-based intrusion detection systems (IDS) have also demonstrated significant improvements in accuracy and adaptability. Almurshid et al. (2024) address the rising threat of cryptojacking malware by developing a holistic detection system with 99% accuracy, using deep static and dynamic analysis techniques. Termos et al. (2024) introduce a Graph Deep Learning framework based on centrality measures (GDLC) for intrusion detection in IoT networks, improving detection rates by up to 7.7%. Additionally, Allafi & Alzahrani (2024) present an Artificial Orca Algorithm combined with Ensemble Learning to enhance cyberattack detection in IoT environments, achieving a maximum accuracy of 99.31%. Bouke et al. (2023) developed an AI-based DDoS detection system using Decision Trees and Gini index feature selection, achieving an accuracy of 98%, effectively reducing computational costs and false alarms. These studies collectively demonstrate AI's potential to enhance detection accuracy, adapt to evolving threats, and streamline cybersecurity operations through automation and continuous learning mechanisms.

AI technologies have proven instrumental in detecting and preventing various forms of fraud across multiple sectors. Machine learning models, anomaly detection systems, and predictive analytics have enhanced the identification of fraudulent transactions, reduced false positives and improved response times. Ismaeil (2024) explores the application of AI, particularly machine learning algorithms, in improving the accuracy and efficiency of financial fraud detection, significantly reducing false positives. AI-driven fraud prevention frameworks have also been applied to the financial sector, where deep learning models have been utilized to detect anomalies in real-time transactional data. Abu-Zanona (2023) introduced an AI-based security system that detects and mitigates Mirai and BASHLITE attacks in IoT devices using an ensemble-based weighted voting model, achieving an outstanding accuracy of 99.9955%, highlighting AI's effectiveness in strengthening network security.

Beyond financial fraud, AI is increasingly used in phishing prevention. Soon et al. (2024) examine user perceptions of AI-powered phishing attacks on Facebook, emphasizing the need for awareness campaigns and improved training. Fan et al. (2024) leverage explainable AI techniques to investigate phishing susceptibility, revealing that psychological factors such as impulsivity and conscientiousness significantly affect an individual's likelihood of falling victim to phishing

schemes. The integration of AI-powered phishing detection systems with behavioral analytics has further strengthened cybersecurity defenses by enabling real-time threat identification.

Other domains have also benefited from AI-driven fraud detection frameworks. Sattarov (2024) discusses a multimedia support system for aerospace monitoring of emergency situations using AI technologies, underscoring the importance of forecasting and preventing emergencies. Esraa (2024) investigates the role of expert systems and neural networks in detecting maritime fraud, demonstrating AI's effectiveness in improving efficiency and accuracy. Alsubaei et al. (2024) propose a hybrid deep learning framework (ResNeXt-GRU) for real-time phishing detection, achieving 98% accuracy and significantly reducing false positives. Singh et al. (2024) introduce an ML-based cyber-attack detection system using Support Vector Machines (SVM) and logistic regression to predict cybercriminal behavior. These studies collectively highlight AI's capacity to enhance predictive capabilities, enable proactive fraud prevention strategies, and address the complex interplay between cyber threats and real-world crime dynamics.

While AI offers transformative potential in cybersecurity, ethical considerations and future research directions remain paramount. The widespread deployment of AI-driven security mechanisms raises concerns about algorithmic bias, privacy infringement, and the misuse of AI in adversarial cyberattacks. Zandi et al. (2024) provide a comprehensive overview of the evolving AI threat to cybersecurity, emphasizing the urgent need for enhanced cybersecurity strategies and international cooperation. As AI becomes more integrated into cybersecurity infrastructures, researchers and policymakers must ensure that AI-driven security systems adhere to ethical standards and minimize unintended harm.

The role of generative AI in cybersecurity is another emerging area of concern. Al-Dahoud et al. (2024) explore the potential of generative AI in various industries, including cybersecurity, highlighting the need for further research and development to mitigate risks associated with AI-generated misinformation, deepfake technology, and automated hacking tools. Furthermore, Yang et al. (2024) examine the potential of Automated ML (AutoML) technologies in developing robust security solutions for Zero-Touch Networks (ZTNs), emphasizing the need for minimal human intervention and protection against adversarial attacks. AI-driven security frameworks must incorporate safeguards against adversarial machine learning attacks, which exploit vulnerabilities in AI models to evade detection and manipulate security protocols.

In addition to security concerns, AI’s role in regulatory compliance and governance has become increasingly important. Regulatory bodies and industry leaders must establish guidelines to ensure transparency, accountability, and fairness in AI-driven cybersecurity implementations. Esraa (2024) highlights the need for enhanced collaboration between regulatory agencies, financial institutions, and technology companies to create AI governance frameworks that address cybersecurity risks while upholding ethical principles. Li (2023) proposes an AI-based domain name security access system using bidirectional recurrent neural networks to combat cyber threats, underscoring the importance of continuous AI innovation in cybersecurity. These studies underscore the importance of ethical AI deployment, transparency, and continuous innovation to address emerging cybersecurity challenges effectively.

METHODOLOGY

SEARCH STRATEGY

A systematic search was conducted in January 2025 to identify relevant peer-reviewed studies on the role of Artificial Intelligence (AI) in combatting cybercrime. The search process involved three major academic databases: Scopus, Web of Science, and IEEE Xplore. The keywords used included terms such as "artificial intelligence," "cybersecurity," "machine learning," "threat detection," "fraud prevention," "phishing detection," and "AI ethics." TABLE 1 presents the database-specific search strings used during this process. The initial search retrieved a total of 1,972 documents (685 from Scopus, 728 from Web of Science, and 559 from IEEE Xplore). Following a rigorous screening process, duplicates were removed, and articles that did not meet the inclusion criteria were excluded. Specifically, studies published in non-peer-reviewed sources, non-indexed journals, or those not written in English were eliminated. Additionally, non-empirical studies, theoretical papers, and articles unrelated to AI-driven cybersecurity solutions were excluded. After applying these criteria, the final selection yielded a total of 67 studies deemed relevant for inclusion in this systematic literature review. These studies provide a comprehensive overview of AI applications in cyber threat detection, fraud prevention, adversarial AI, and ethical challenges in cybersecurity (see FIGURE 1).

TABLE 1. Database Search Strings

Database	**Search String**
Scopus	TITLE-ABS-KEY ("artificial intelligence" AND "cybersecurity") OR ("machine learning" AND "threat detection") OR ("phishing detection") OR ("fraud prevention") OR ("adversarial AI")
Web of Science	TS=("AI-powered security" AND "cybercrime") OR ("deep learning" AND "malware detection") OR ("blockchain cybersecurity") OR ("explainable AI" AND "security policies")
IEEE Xplore	("cybersecurity" AND "machine learning") OR ("ransomware detection" AND "AI") OR ("privacy-preserving AI") OR ("AI-driven intrusion prevention systems")

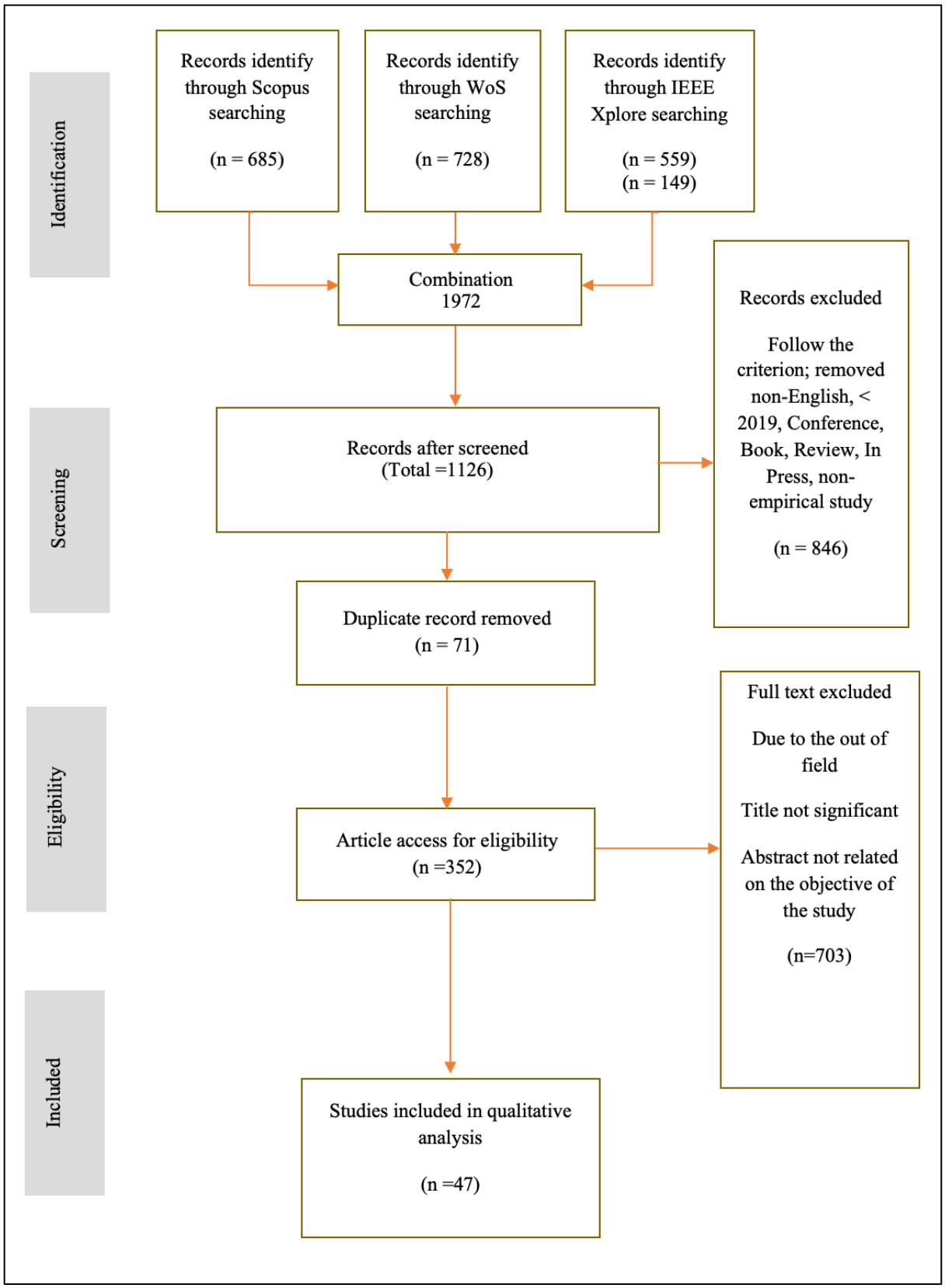

FIGURE 1. Flow diagram of the proposed searching study (Moher et al., 2009)

INCLUSION AND EXCLUSION CRITERIA

The inclusion criteria applied in this systematic literature review were as follows: (1) Peer-reviewed journal articles: Only studies published in reputable, peer-reviewed academic journals were included to ensure reliability and validity; (2) Focus on AI-driven cybersecurity solutions: Studies had to specifically examine the role of AI in cybersecurity, including applications in fraud detection, malware defense, phishing prevention, and ethical AI governance; (3) Written in English: To maintain consistency and accessibility, only articles written in English were included; (4) Empirical studies from indexed journals: The review prioritized empirical studies published in indexed journals (e.g., Scopus, Web of Science, IEEE Xplore) to ensure methodological rigor; (5) Full-text availability: Studies for which the full text was unavailable or inaccessible were excluded; (6) Relevant study samples: Studies were required to examine AI applications in cybersecurity within real-world settings, including enterprises, government agencies, and financial institutions. The application of these criteria ensured a focused and rigorous selection process. Initially, 67 studies were selected after applying the inclusion criteria. However, following full-text screening and final eligibility assessment, a total of 47 studies were included in this review (see TABLE 2).

TABLE 2. Summary of Inclusion and Exclusion Criteria

Criteria	**Inclusion**	**Exclusion**
Publication Type	Peer-reviewed journal articles	Non-peer-reviewed sources, books, book chapters, dissertations, conference proceedings
Focus of Study	AI applications in cybersecurity (e.g., fraud prevention, intrusion detection, AI-driven security frameworks)	Studies unrelated to AI or cybersecurity
Language	Written in English	Non-English publications
Study Design	Empirical studies using qualitative, quantitative, or mixed methods	Non-empirical studies (e.g., editorials, commentaries, conceptual papers)
Journal Indexing	Indexed in repuTABLE databases (e.g., Scopus, Web of Science, IEEE Xplore)	Non-indexed journals or non-academic sources
Availability of Full Text	Full text available and accessible	Unavailable or inaccessible full texts
Sample Type	Studies applying AI in cybersecurity settings	Studies lacking real-world AI cybersecurity applications

SCREENING, ELIGIBILITY, AND EXTRACTION

Titles and abstracts from the retrieved studies were reviewed in the initial screening process, with articles selected based on the predefined inclusion and exclusion criteria. From the 1,972 articles retrieved (685 from Scopus, 728 from Web of Science, and 559 from IEEE Xplore), duplicate records were removed, resulting in 1,901 unique articles. A total of 352 studies were shortlisted for eligibility assessment after initial screening.

During the eligibility stage, all shortlisted articles were thoroughly reviewed to ensure alignment with the research objectives and inclusion criteria. Articles that did not meet the criteria such as non-empirical studies, non-peer-reviewed publications, or studies unrelated to AI-driven cybersecurity were excluded. This process resulted in 47 articles being retained for the data extraction stage.

In the data extraction stage, the full texts of the 47 articles were evaluated to identify key themes and insights relevant to this research. The author extracted detailed information on the following aspects: (1) Study samples; Characteristics of the data sources, such as cybersecurity datasets, real-world security incidents, or AI-driven security models; (2) Mechanisms and AI models used: Factors related to machine learning, deep learning, blockchain security, explainable AI, adversarial AI, and fraud detection frameworks; (3) Types of cybersecurity interventions: AI-driven threat intelligence systems, AI-enhanced fraud prevention tools, and autonomous cybersecurity frameworks; (4) Theoretical frameworks applied: Security models such as the Cyber Kill Chain, Zero Trust Architecture, or AI-driven risk assessment frameworks; (5) Research design; Qualitative, quantitative, or mixed-methods approaches employed in the studies; (6) Analysis methods: Techniques such as deep learning model validation, statistical analysis, adversarial attack simulation, and NLP-driven threat detection; (7) Key findings: Major insights related to AI's effectiveness in cyber threat detection, security automation, ethical AI challenges, and regulatory implications.

After a thorough review of the full texts, one article was excluded due to insufficient relevance to the research objectives, leaving a final selection of 47 studies included in this systematic literature review. This systematic review was conducted following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure a rigorous and transparent selection and reporting process. These studies collectively provide a comprehensive understanding of AI's role in cybersecurity, offering valuable insights for researchers, policymakers, and industry practitioners.

RESULTS AND FINDINGS

AI-DRIVEN THREAT DETECTION AND PREVENTION MECHANISMS

Artificial intelligence (AI) has transformed cybersecurity by enhancing threat detection and prevention. Machine learning (ML) and deep learning (DL) algorithms have been widely adopted to detect cyber threats such as malware, phishing, and Distributed Denial of Service (DDoS) attacks. Research by Ibrahim et al. (2024) highlights AI's role in network segmentation, endpoint protection, and anomaly detection to counter Advanced Persistent Threats (APTs). Alashhab et al. (2024) proposed an ensemble online ML model for DDoS detection in Software-Defined Networks (SDN), achieving a remarkable 99.2% detection rate. Min et al. (2024) introduced a DL-driven SDN-inspired adversary detection framework (Cu-BLSTMGRU) for IoT-based industrial networks, boasting an attack detection accuracy of 99.65%. Similarly, Zhuravchak et al. (2024) designed an integrated defense-in-depth system with an AI assistant, which detected 98% of malicious files and 99% of tactics used in APT attacks. These advancements demonstrate AI's ability to significantly enhance the accuracy and efficiency of cybersecurity defenses.

In addition to malware detection, AI has been instrumental in threat prediction and proactive defense mechanisms. Oh et al. (2024) utilized deep reinforcement learning (DRL) to simulate cyber threats, enabling organizations to anticipate and respond to potential attacks before they occur. AI-powered biometric authentication systems have also been widely explored, with Khairnar et al. (2024) combining deep learning models with local interpreTABLE model-agnostic interpretation (LIME) to improve transparency and prevent spoofing attacks. Moreover, Hu & Zhang (2024) employed a metaheuristic approach to optimize ML-based phishing detection, significantly improving classification accuracy. By integrating AI-driven approaches across

different domains, cybersecurity experts can mitigate emerging threats in a proactive and adaptive manner.

AI-AUGMENTED INCIDENT RESPONSE AND CYBERCRIME INVESTIGATION

AI plays a crucial role in incident response and forensic investigations by automating cybersecurity workflows, improving intrusion detection accuracy, and reducing response times. Min et al. (2024) introduced a deep learning-powered adversary detection framework for Industrial IoT networks, demonstrating superior accuracy in identifying and classifying cyberattacks. Zhuravchak et al. (2024) developed an AI-assisted defense-in-depth system that enhances malware detection, automates threat analysis, and optimizes response time in mitigating APTs. These AI-powered systems enable cybersecurity teams to efficiently detect and respond to threats in real time, reducing manual intervention and increasing overall effectiveness.

AI-driven forensic investigations have also significantly improved cybercrime detection and law enforcement efforts. Rao et al. (2024) propose an AI-powered framework integrating crime rate predictions with cybersecurity intelligence, utilizing ML algorithms such as Random Forest and SARIMAX to analyze crime trends. Similarly, Bansal et al. (2025) highlight the benefits of AI-assisted behavioral analysis in detecting online fraud within the banking sector, emphasizing the role of psychological profiling in identifying fraudulent activities. The ability to process vast amounts of digital evidence and uncover hidden attack patterns makes AI an indispensable tool for cybercrime investigations.

Moreover, AI is increasingly being used in ransomware detection and mitigation strategies. B N & S H (2024) developed a hybrid ML model capable of classifying ransomware attacks with high precision, improving cyber resilience against encryption-based threats. AI-powered attack simulations have also been explored to enhance cybersecurity preparedness, as demonstrated by Oh et al. (2024), who applied DRL techniques to simulate cyber threats and train AI-based security systems. Additionally, Nurmansyah et al. (2024) emphasize the role of AI in strengthening legal frameworks against AI-based phishing crimes, highlighting the need for stronger regulatory measures and international cooperation in combating cyber threats. These studies collectively showcase AI's transformative role in automating cybersecurity responses, strengthening cyber resilience, and supporting forensic investigations.

AI IN POLICY DEVELOPMENT AND ETHICAL CONSIDERATIONS IN CYBERSECURITY

Beyond technical applications, AI's role in cybersecurity extends to policy development and ethical concerns. AI-driven financial monitoring has emerged as a crucial tool in anti-money laundering (AML) efforts. Chitimira et al. (2024) explore AI's role in detecting suspicious financial transactions in the South African banking sector, emphasizing the potential of AI to enhance financial fraud prevention. Similarly, Ali et al. (2024) examine how AI and blockchain improve forensic accounting by increasing transparency and fraud detection capabilities. Sood et al. (2023) further investigate AI's application in financial fraud detection, using natural language processing (NLP) and big data analytics. These AI-driven innovations not only improve financial security but also enhance the efficiency of fraud detection and prevention mechanisms.

Ethical considerations remain a significant topic of discussion in AI-driven cybersecurity. Rodriguez & Oppenheimer (2024) analyze AI ethics from an African Ubuntu perspective, advocating for inclusive and responsible AI governance frameworks. The ethical dilemmas of

deepfake technology are also explored by Maras & Logie (2024), who emphasize the need for stricter regulations to combat nonconsensual manipulated media. AI-powered surveillance and predictive policing raise privacy concerns, as addressed by Chen & Wu (2024), who examine the trade-off between security and user privacy in telecom fraud detection. Balancing security with individual rights remains a critical challenge, necessitating the implementation of ethical AI guidelines to prevent misuse and ensure transparency.

Furthermore, AI has the potential to enhance global cybersecurity collaboration and policy development. Naguji et al. (2024) propose a blockchain-enabled AI land registry system to combat fraudulent land transactions, demonstrating how AI can enhance digital trust and security. Johnson (2024) discusses AI's role in future crime prevention through situational awareness models, highlighting the need for advanced predictive analytics in cybersecurity strategies. These studies highlight the necessity of transparent AI policies, regulatory frameworks, and ethical considerations in cybersecurity applications. Moving forward, policymakers must establish legal and ethical standards to ensure the responsible deployment of AI technologies in cybersecurity.

DISCUSSION

THE IMPACT OF AI-DRIVEN THREAT DETECTION AND PREVENTION MECHANISMS

The findings of this study highlight the significant role of AI in enhancing cyber threat detection and prevention. The ability of AI-powered machine learning (ML) and deep learning (DL) models to detect and mitigate cyber threats such as malware, phishing, and Distributed Denial of Service (DDoS) attacks demonstrates not only the effectiveness of AI but also its growing necessity in modern cybersecurity frameworks. As cyber threats become more sophisticated, AI-driven security solutions offer adaptive and scalable defense mechanisms capable of real-time threat analysis and mitigation. The studies by Ibrahim et al. (2024) and Alashhab et al. (2024) underscore the effectiveness of AI in enhancing network segmentation, anomaly detection, and automated threat intelligence gathering, significantly improving security outcomes. Min et al. (2024) and Zhuravchak et al. (2024) further confirm the high accuracy of AI-assisted defense-in-depth systems, reinforcing the idea that AI-driven cybersecurity solutions can drastically improve the speed and efficiency of cyber defense mechanisms while reducing false positives and improving response coordination across security operations centers (SOCs).

AI's role in predictive threat modeling and proactive defense strategies also offers promising advancements in cybersecurity. As Oh et al. (2024) illustrate, the use of deep reinforcement learning (DRL) enables organizations to anticipate and mitigate cyber threats before they materialize. By continuously learning from evolving attack patterns, DRL-based systems enhance the resilience of digital infrastructures against both known and emerging threats. AI-powered biometric authentication systems, such as those examined by Khairnar et al. (2024), provide further security enhancements by reducing the risk of identity fraud. Beyond traditional biometric methods, AI-integrated behavioral biometrics and multi-modal authentication approaches are being increasingly adopted to strengthen access control and prevent unauthorized breaches. Additionally, Hu & Zhang (2024) demonstrate the effectiveness of metaheuristic optimization techniques in phishing detection, further supporting AI's role in proactive cybersecurity measures.

Despite these advancements, challenges remain. The reliance on AI-driven security tools introduces concerns regarding algorithmic bias, adversarial machine learning attacks, and the ethical implications of autonomous decision-making in cybersecurity. Moreover, as cybercriminal tactics evolve to bypass AI-based defenses, continuous improvements in AI model robustness and adversarial training will be crucial. Future research should address the evolving sophistication of cybercriminal tactics, ensuring that AI-based systems remain not only adaptive and resilient against adversarial attacks but also transparent and explainable to foster trust in automated security solutions.

AI-AUGMENTED INCIDENT RESPONSE AND CYBERCRIME INVESTIGATION

The ability of AI to augment incident response and forensic investigations is another critical finding of this study. As cyber threats grow in complexity and frequency, AI-driven automation is increasingly essential for efficient and scalable cybersecurity operations. The automation of cybersecurity workflows, as demonstrated by Min et al. (2024) and Zhuravchak et al. (2024), has significantly improved intrusion detection accuracy and reduced response times. The rapid identification and classification of cyberattacks in real time highlight AI's potential to minimize human error and expedite cybersecurity operations. By integrating AI with Security Orchestration, Automation, and Response (SOAR) platforms, organizations can streamline threat containment, reducing mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR) to security incidents. Furthermore, AI-driven forensic tools, such as those explored by Rao et al. (2024) and Bansal et al. (2025), have enhanced cybercrime investigations by enabling the processing of vast amounts of digital evidence at unprecedented speeds. These AI-assisted forensic systems utilize deep learning for pattern recognition in malware analysis, network anomalies, and digital footprint tracking, aiding law enforcement agencies in efficiently identifying cybercriminal networks. The integration of ML algorithms, including Random Forest and SARIMAX models, provides law enforcement agencies with predictive capabilities for identifying crime trends and potential cybercriminal behaviors. Such predictive analytics can proactively guide cybersecurity strategies, allowing organizations to anticipate and counteract threats before they escalate.

Another noTABLE application of AI in cybersecurity is ransomware detection and mitigation. The hybrid ML model proposed by B N & S H (2024) showcases AI's potential in classifying and responding to ransomware attacks with high precision. By leveraging behavior-based analysis, AI can detect novel ransomware variants and autonomously trigger containment measures to prevent data encryption. Similarly, AI-powered attack simulations, as described by Oh et al. (2024), contribute to proactive security measures by preparing organizations for emerging cyber threats. Through automated red teaming and adversarial simulations, AI enables cybersecurity professionals to test and reinforce their defensive postures against evolving attack methodologies. However, while AI has proven effective in automating cybersecurity responses and strengthening forensic investigations, concerns remain regarding the interpretability and accountability of AI-driven decisions. The "black box" nature of AI models raises challenges in legal and ethical contexts, particularly in digital forensics where decision transparency is paramount for court-admissible evidence. Future research should focus on explainable AI (XAI) approaches to enhance transparency in cybersecurity applications, ensuring ethical and legally sound investigative practices. Additionally, collaboration between AI researchers, cybersecurity professionals, and legal experts is necessary to establish standardized frameworks for AI-driven forensic methodologies, ensuring both reliability and compliance with regulatory standards.

Beyond its technical applications, AI's role in shaping cybersecurity policies and ethical considerations is an essential aspect of modern digital security. As AI continues to revolutionize cybersecurity, policymakers and regulatory bodies must adapt to ensure that AI-driven security measures align with global ethical and legal frameworks. AI-driven financial monitoring tools, as explored by Chitimira et al. (2024) and Ali et al. (2024), provide substantial improvements in anti-money laundering (AML) efforts and forensic accounting. These AI-enhanced AML systems leverage anomaly detection and real-time transaction monitoring to identify suspicious financial activities with greater accuracy, minimizing human oversight while improving compliance with financial regulations. The integration of AI and blockchain technologies, as discussed by Sood et al. (2023), further strengthens financial fraud detection by enhancing data security and transparency. Blockchain's decentralized architecture, combined with AI-driven pattern recognition, not only improves traceability in financial transactions but also mitigates risks associated with fraudulent manipulations and illicit money flows.

However, ethical considerations surrounding AI deployment remain a key concern. As AI becomes more deeply embedded in cybersecurity operations, its potential for misuse raises significant ethical and legal questions. The study by Rodriguez & Oppenheimer (2024) highlights the importance of inclusive and responsible AI governance, particularly from an African Ubuntu perspective. This perspective emphasizes ethical AI development that prioritizes community welfare, transparency, and fairness, ensuring that AI-driven cybersecurity policies benefit diverse global populations. Similarly, Maras & Logie (2024) emphasize the challenges associated with deepfake technology, underscoring the need for regulatory measures to prevent AI-enabled disinformation. Deepfake-based cyber threats, including identity fraud, misinformation campaigns, and social engineering attacks, necessitate advanced AI countermeasures and stringent legal frameworks to curb their harmful impacts. Privacy concerns in AI-powered surveillance, as raised by Chen & Wu (2024), further stress the importance of balancing cybersecurity advancements with individual rights and ethical considerations. The rapid expansion of AI-driven surveillance tools calls for clear legal boundaries to prevent mass surveillance abuses while ensuring national security interests are met. These studies collectively illustrate the need for robust regulatory frameworks to govern AI implementation in cybersecurity, ensuring that AI-driven security measures align with ethical and legal standards.

Global cybersecurity collaboration is another crucial area for future research. As Naguji et al. (2024) and Johnson (2024) discuss, AI has the potential to facilitate international cybersecurity initiatives by improving digital trust and crime prevention strategies. AI-enhanced threat intelligence sharing among nations and organizations can lead to faster detection of cyber threats, reducing global cyber risks. However, policymakers must establish clear regulations to mitigate the risks associated with AI-driven cybersecurity tools. This includes addressing AI bias, ensuring data privacy protections, and defining accountability in cases of AI-driven security breaches. Future research should focus on developing standardized policies that address AI biases, privacy concerns, and the ethical implications of automated decision-making in cybersecurity. Additionally, fostering interdisciplinary collaboration between AI researchers, legal experts, ethicists, and policymakers will be essential in creating AI-driven cybersecurity policies that are both effective and ethically responsible.

IMPLICATIONS OF AI IN CYBERSECURITY

The findings of this study carry significant implications for both academic research and practical cybersecurity applications. From an academic perspective, this study contributes to the growing body of literature on AI in cybersecurity by synthesizing current trends, advancements, and challenges. It provides a foundation for future research on AI-driven security solutions, particularly in areas such as explainable AI, adversarial machine learning, and ethical AI governance. For practitioners, the study highlights the need for organizations to adopt AI-driven security measures proactively. The demonstrated effectiveness of AI in cyber threat detection, fraud prevention, and forensic investigations underscores its value in strengthening digital security. Cybersecurity professionals must invest in AI-powered security solutions to enhance resilience against emerging threats. Additionally, policymakers must collaborate with industry leaders and researchers to develop robust regulations that ensure the ethical and secure implementation of AI-driven cybersecurity systems.

LIMITATIONS OF THE STUDY

While this study provides valuable insights into AI-driven cybersecurity solutions, several limitations must be acknowledged. First, the study relies on a systematic literature review, which, while comprehensive, may not fully capture the latest advancements in AI-based cybersecurity solutions due to the rapid evolution of the field. The findings are based on existing literature, and emerging AI technologies may introduce new security capabilities or challenges that are not yet well-documented.

Second, the study does not include empirical validation or experimental testing of AI-driven cybersecurity models. The effectiveness of AI in cybersecurity varies based on implementation context, dataset quality, and adversarial threat landscape. Future research should incorporate real-world testing and performance evaluations of AI-driven security systems to validate theoretical findings. Lastly, ethical and regulatory considerations remain dynamic and subject to regional differences. The study acknowledges ethical concerns related to AI-driven surveillance, bias, and data privacy, but further research is needed to assess how different legal frameworks influence AI deployment in cybersecurity across various jurisdictions.

THE FUTURE OF AI IN CYBERSECURITY

The results of this study indicate that AI is a game-changer in cybersecurity, offering enhanced capabilities in threat detection, incident response, forensic investigations, and policy development. However, challenges remain in ensuring that AI-driven cybersecurity solutions remain transparent, unbiased, and resilient against adversarial threats. Future research should explore the integration of AI with other emerging technologies, such as quantum computing and federated learning, to further strengthen cybersecurity defenses. Moreover, the importance of AI ethics cannot be overlooked. While AI offers promising advancements in cybersecurity, its deployment must be carefully managed to prevent misuse and potential security risks. Ethical AI frameworks, regulatory compliance, and explainable AI models should be prioritized in future cybersecurity research to ensure the responsible and transparent implementation of AI technologies.

CONCLUSION

AI has the potential to revolutionize cybersecurity by enhancing threat detection, automating response mechanisms, and shaping policy frameworks. As cyber threats continue to evolve, interdisciplinary research efforts and international collaboration will be essential in maximizing AI's effectiveness in combating cybercrime while ensuring ethical and legal compliance. Future studies should address the limitations of AI-driven security measures and focus on developing adaptive, transparent, and ethical AI solutions to safeguard digital infrastructures globally. by enhancing threat detection, automating response mechanisms, and shaping policy frameworks. As cyber threats continue to evolve, interdisciplinary research efforts and international collaboration will be essential in maximizing AI's effectiveness in combating cybercrime while ensuring ethical and legal compliance. Future studies should address the limitations of AI-driven security measures and focus on developing adaptive, transparent, and ethical AI solutions to safeguard digital infrastructures globally.

ACKNOWLEDGEMENT

Grateful appreciation to the Centre for Media and Communication Studies for their support in this research.

REFERENCES

Abu-Zanona, M. (2023). Efficient IoT Security: Weighted Voting for Bashlite and Mirai Attack Detection. *International Journal of Advanced Computer Science and Applications*, *14*(12), 925–933. https://doi.org/10.14569/IJACSA.2023.0141293

Ahmed, A. (2024). Enhancing Cybersecurity in Financial Services using Single Value Neutrosophic Fuzzy Soft Expert Set. *International Journal of Neutrosophic Science*, *24*(2), 246–257. https://doi.org/10.54216/IJNS.240222

Ahmad Arifin, N., Mokhtar, U. A., Hood, Z., Tiun, S., & Jambari, D. I. (2019). Parental awareness on cyber threats using social media. *Jurnal Komunikasi*, 35(2), 485–498.

Alashhab, A. A., Zahid, M. S., Isyaku, B., Elnour, A. A., Nagmeldin, W., Abdelmaboud, A., Abdullah, T. A. A., & Maiwada, U. D. (2024). Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model. *IEEE Access*, *12*, 51630–51649. https://doi.org/10.1109/ACCESS.2024.3384398

Al-Dahoud, A., Fezari, M., Aqel, D., Mimi, H., & Daoud, M. S. (2024). Revolutionizing Space: The Potential of Artificial Intelligence. *WSEAS Transactions on Computer Research*, *12*, 404–414. https://doi.org/10.37394/232018.2024.12.40

Ali, A. M., Futaih, R. F., Shukur, M., & Al-Orfali, A. K. (2024). Forensic Accounting and Fraud Detection Emerging Trends and Techniques. *Journal of Ecohumanism*, *3*(5), 525–542. https://doi.org/10.62754/joe.v3i5.3921

Allafi, R., & Alzahrani, I. R. (2024). Enhancing Cybersecurity in the Internet of Things Environment Using Artificial Orca Algorithm and Ensemble Learning Model. *IEEE Access*, *12*, 63282–63291. https://doi.org/10.1109/ACCESS.2024.3390093

Almurshid, H. A., Almomani, I., Khalifa, M. A., & El-Shafai, W. (2024). A Holistic Intelligent Cryptojacking Malware Detection System. *IEEE Access*, *12*, 161417–161439. https://doi.org/10.1109/ACCESS.2024.3488192

Alshattnawi, S., Shatnawi, A., AlSobeh, A. M. R., & Magableh, A. A. (2024). Beyond Word-Based Model Embeddings: Contextualized Representations for Enhanced Social Media Spam Detection. *Applied Sciences (Switzerland)*, *14*(6). https://doi.org/10.3390/app14062254

Alsubaei, F. S., Almazroi, A. A., & Ayub, N. (2024). Enhancing Phishing Detection: A Novel Hybrid Deep Learning Framework for Cybercrime Forensics. *IEEE Access*, *12*, 8373–8389. https://doi.org/10.1109/ACCESS.2024.3351946

B N, C., & S H, B. (2024). Revolutionizing ransomware detection and criticality assessment: Multiclass hybrid machine learning and semantic similarity-based end2end solution. *Multimedia Tools and Applications*, *83*(13), 39135–39168. https://doi.org/10.1007/s11042-023-16946-x

Bansal, K., Paliwal, A. C., & Singh, A. K. (2025). Analysis of the benefits of artificial intelligence and human personality study on online fraud detection. *International Journal of Law and Management*, *67*(2), 191–209. https://doi.org/10.1108/IJLMA-08-2023-0198

Barik, K., & Misra, S. (2024). Adversarial attack defense analysis: An empirical approach in cybersecurity perspective. *Software Impacts*, *21*. https://doi.org/10.1016/j.simpa.2024.100681

Bouke, M. A., Abdullah, A., ALshatebi, S. H., Abdullah, M. T., & Atigh, H. E. (2023). An intelligent DDoS attack detection tree-based model using Gini index feature selection method. *Microprocessors and Microsystems*, *98*. https://doi.org/10.1016/j.micpro.2023.104823

Bryssinck, J., Jacobs, T., Simini, F., Doddasomayajula, R., Koder, M., Curbera, F., Vishwanath, V., & Neti, C. (2024). Harnessing synthetic data to address fraud in cross-border payments. *Journal of Payments Strategy and Systems*, *18*(3), 261–275. https://doi.org/10.69554/igxu1561

Chen, D., & Wu, Y. (2024). Research on the use of communication big data and AI artificial intelligence technology to construct telecom fraud prevention behavior portrait. *Intelligent Decision Technologies*, *18*(3), 2589–2605. https://doi.org/10.3233/IDT-240386

Chibi, N. T., Oualhaj, O. A., Fihri, W. F., & Ghazi, H. E. (2024). A Novel Approach Based on Machine Learning, Blockchain, and Decision Process for Securing Smart Grid. *IEEE Access*, *12*, 33190–33199. https://doi.org/10.1109/ACCESS.2024.3370239

Chitimira, H., Torerai, E., & Jana, V. L. M. (2024). Leveraging Artificial Intelligence to Combat Money Laundering and Related Crimes in the South African Banking Sector. *Potchefstroom Electronic Law Journal*, *27*, 1–30. https://doi.org/10.17159/1727-3781/2024/v27i0a18024

Esraa, A. S. M. H. (2024). The Role of Artificial Intelligence in Maritime Fraud. *International Journal of Criminal Justice Sciences*, *19*(1), 411–427. https://doi.org/10.5281/zenodo.19123

Fan, Z., Li, W., Laskey, K. B., & Chang, K.-C. (2024). Investigation of Phishing Susceptibility with Explainable Artificial Intelligence. *Future Internet*, *16*(1). https://doi.org/10.3390/fi16010031

Galli, A., La Gatta, V., Moscato, V., Postiglione, M., & Sperlì, G. (2024). Explainability in AI-based behavioral malware detection systems. *Computers and Security*, *141*. https://doi.org/10.1016/j.cose.2024.103842

Gushelmi, G., Latih, R., & Mohd. Zin, A. (2024). Cybersecurity behavior in the West Sumatra universities. JOIV: *International Journal on Informatics Visualization*, 3-2(8), 1976–1986.

Hu, B., & Zhang, S. (2024). Addressing Phishing Threats Using A Metaheuristic Perspective On Machine Learning Classification Models Code. *Journal of Applied Science and Engineering*, *28*(7), 1503–1514. https://doi.org/10.6180/jase.202507_28(7).0011

IBM. (2023). *IBM 2023 Annual Report*.

Ibrahim, N., Rajalakshmi, N. R., & Hammadeh, K. (2024). Exploration of Defensive Strategies, Detection Mechanisms, and Response Tactics against Advanced Persistent Threats APTs. *Nanotechnology Perceptions*, *20*(S4), 439–455. https://doi.org/10.62441/nano-ntp.v20is4.33

Ismaeil, M. K. A. (2024). Harnessing AI for Next-Generation Financial Fraud Detection: A Data-Driven Revolution. *Journal of Ecohumanism*, *3*(7), 811–821. https://doi.org/10.62754/joe.v3i7.4248

Johnson, S. D. (2024). Identifying and preventing future forms of crimes using situational crime prevention. *Security Journal*, *37*(3), 515–534. https://doi.org/10.1057/s41284-024-00441-5

Junaidi, Pujiono, & Mohamed Fadzil, R. (2024). Legal reform of artificial intelligence's liability to personal data: Perspectives of progressive legal theory. *Journal of Law and Legal Reform*, 5(2), 587–612.

Karacayılmaz, G., & Artuner, H. (2024). A novel approach detection for IIoT attacks via artificial intelligence. *Cluster Computing*, *27*(8), 10467–10485. https://doi.org/10.1007/s10586-024-04529-w

Khairnar, S., Gite, S., Mahajan, K., Pradhan, B., Alamri, A., & Thepade, S. D. (2024). Advanced Techniques for Biometric Authentication: Leveraging Deep Learning and Explainable AI. *IEEE Access*, *12*, 153580–153595. https://doi.org/10.1109/ACCESS.2024.3474690

Li, L. (2023). The Construction of Network Domain Name Security Access Identification System Based on Artificial Intelligence. *International Journal of Information Technology and Web Engineering*, *18*(1). https://doi.org/10.4018/IJITWE.333636

Lokanan, M. E., & Maddhesia, V. (2025). Supply chain fraud prediction with machine learning and artificial intelligence. *International Journal of Production Research*, *63*(1), 286–313. https://doi.org/10.1080/00207543.2024.2361434

Louati, H., Louati, A., Almekhlafi, A., ElSaka, M., Alharbi, M., Kariri, E., & Altherwy, Y. N. (2024). Adopting Artificial Intelligence to Strengthen Legal Safeguards in Blockchain Smart Contracts: A Strategy to Mitigate Fraud and Enhance Digital Transaction Security. *Journal of Theoretical and Applied Electronic Commerce Research*, *19*(3), 2139–2156. https://doi.org/10.3390/jtaer19030104

Maras, M.-H., & Logie, K. (2024). Countering the complex, multifaceted nature of nude and sexually explicit deepfakes: an Augean task? *Crime Science*, *13*(1). https://doi.org/10.1186/s40163-024-00226-6

Min, W., Almughalles, W., Muthanna, M. S. A., Ouamri, M. A., Muthanna, A., Hong, S., & El-Latif, A. A. A. (2024). An SDN-Orchestrated Artificial Intelligence-Empowered Framework to Combat Intrusions in the Next Generation Cyber-Physical Systems. *Human-Centric Computing and Information Sciences*, *14*. https://doi.org/10.22967/HCIS.2024.14.011

Mohammed, M. A., Boujelben, M., & Abid, M. (2023). A Novel Approach for Fraud Detection in Blockchain-Based Healthcare Networks Using Machine Learning. *Future Internet*, *15*(8). https://doi.org/10.3390/fi15080250

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. (2009). Moher D, Liberati A, Tetzlaff J, Altman DG, Group PPreferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. PLoS Med 6: e1000097. *Open Medicine : A Peer-Reviewed, Independent, Open-Access Journal*, *3*, e123-30. https://doi.org/10.1016/j.jclinepi.2009.06.005

Muhammad Adnan, Omar, S. Z., & Ahmad Ghazali, A. H. (2019). Amalan keselamatan siber pengguna internet terhadap buli siber, pornografi, e-mel phishing dan pembelian dalam talian. *Jurnal Komunikasi*, 35(3), 212–227.

Naguji, F., Kumar Jadav, N., Tanwar, S., Pau, G., Sharma, G., Alqahtani, F., & Tolba, A. (2024). GreenLand: A Secure Land Registration Scheme for Blockchain and AI-Enabled Agriculture Industry 5.0. *IEEE Access*, *12*, 120994–121009. https://doi.org/10.1109/ACCESS.2024.3451627

Nurmansyah, G., Wiranata, I. G. A. B., Fardiansyah, A. I., & Mladenov, S. V. (2024). Preventing AI-based phishing crimes across national borders through the reconstruction of personal data protection laws. *Jurnal Hukum Novelty*, *15*(2), 286–311. https://doi.org/10.26555/jhn.v15i2.27558

Oh, S. H., Kim, J., Nah, J. H., & Park, J. (2024). Employing Deep Reinforcement Learning to Cyber-Attack Simulation for Enhancing Cybersecurity. *Electronics (Switzerland)*, *13*(3). https://doi.org/10.3390/electronics13030555

Rao, T. K. R. K., Balagoni, Y., Vekariya, V., Irfan, B. M., Vasmatkar, A. D., Patil, H., Selvan, P., Natarajan, K., & Rajaram, A. (2024). CYBERSECURITY AND ARTIFICIAL INTELLIGENCE FOR PREDICTING CRIME RATES. *Journal of Environmental Protection and Ecology*, *25*(5), 1395–1404. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85204039539&partnerID=40&md5=828def2054e9aeace386fda00fac92d3

Rishad, S. M. S. I. (2025). Leveraging AI and Machine Learning for Predicting, Detecting, And Mitigating Cybersecurity Threats: A Comparative Study of Advanced Models. *International Journal of Computer Science & Information System*, *10*(01), 06–25. https://doi.org/10.55640/ijcsis/Volume10Issue01-02

Rodriguez, C., & Oppenheimer, D. M. (2024). Creating a Bot-tleneck for malicious AI: Psychological methods for bot detection. *Behavior Research Methods*, *56*(6), 6258–6275. https://doi.org/10.3758/s13428-024-02357-9

Sattarov, N. (2024). Multimedia Support System for Aerospace Monitoring of Emergency Situation Based on Ai Technologies. *Reliability: Theory and Applications*, *19*(Special issue 6), 203–209. https://doi.org/10.24412/1932-2321-2024-681-203-209

Singh, C., Singh, R., Tiwari, M., & Hazela, B. (2024). Analyse and Predict the Detection of the Cyber-Attack Process by Using a Machine-Learning Approach. *EAI Endorsed Transactions on Internet of Things*, *10*. https://doi.org/10.4108/eetiot.5345

Sood, P., Sharma, C., Nijjer, S., & Sakhuja, S. (2023). Review the role of artificial intelligence in detecting and preventing financial fraud using natural language processing. *International Journal of System Assurance Engineering and Management*, *14*(6), 2120–2135. https://doi.org/10.1007/s13198-023-02043-7

Soon, J. P., Chan, R. Q., Lee, Q. H., En Loke, D., Chun, S. L. H., & Yuen, P. K. (2024). User perceptions of artificial intelligence powered phishing attacks on Facebook's resilient infrastructure. *International Journal of Advances in Applied Sciences*, *13*(4), 878–886. https://doi.org/10.11591/ijaas.v13.i4.pp878-886

Termos, M., Ghalmane, Z., Brahmia, M.-E.-A., Fadlallah, A., Jaber, A., & Zghal, M. (2024). GDLC: A new Graph Deep Learning framework based on centrality measures for intrusion detection in IoT networks. *Internet of Things (Netherlands)*, *26*. https://doi.org/10.1016/j.iot.2024.101214

Tin, T. T., Cheah, K. M., Khiew, J. X., Lee, Y. C., Chaw, J. K., & Teoh, C. K. (2024). Validation of cyber security behaviour among adolescents at Malaysia University: Revisiting gender as a role. *International Journal of Innovative Research and Scientific Studies*, 7(1), 127–137.

Wen, W., & Han, X. (2024). An introduction of transaction session-induced security scheme using blockchain technology: Understanding the features of Internet of Things–based financial security systems. *Managerial and Decision Economics*, *45*(4), 1817–1834. https://doi.org/10.1002/mde.4043

Yang, L., El Rajab, M., Shami, A., & Muhaidat, S. (2024). Enabling AutoML for Zero-Touch Network Security: Use-Case Driven Analysis. *IEEE Transactions on Network and Service Management*, *21*(3), 3555–3582. https://doi.org/10.1109/TNSM.2024.3376631

Yilmaz, E., & Can, O. (2024). Unveiling Shadows: Harnessing Artificial Intelligence for Insider Threat Detection. *Engineering, Technology and Applied Science Research*, *14*(2), 13341–13346. https://doi.org/10.48084/etasr.6911

Zandi, G., Yaacob, N. A., Tajuddin, M., & Rahman, N. K. N. A. (2024). Artificial Intelligence and the Evolving Cybercrime Paradigm: Current Threats to Businesses. *Journal of Information Technology Management*, *16*(4), 162–170. https://doi.org/10.22059/jitm.2024.99505

Zhuravchak, D., Opanovych, M., Tolkachova, A., Dudykevych, V., & Piskozub, A. (2024). Design Of an Integrated Defense-In-Depth System with An Artificial Intelligence Assistant to Counter Malware. *Eastern-European Journal of Enterprise Technologies*, *6*(2(132)), 64–73. https://doi.org/10.15587/1729-4061.2024.318336

Muhammad Adnan Pitchan (Corresponding author)
Centre for Research in Media and Communication
Faculty of Social Sciences and Humanities
The National University of Malaysia, Malaysia
Email: adnan86@ukm.edu.my

Akmar Hayati Ahmad Ghazali
Department of Communications
Faculty of Modern Languages and Communication
University of Putra Malaysia, Malaysia
Email: akmar@upm.edu.my

Edy Prihantoro
Gunadarma University, Indonesia
Email: edipri@staff.gunadarma.ac.id