Communication in Physical Sciences 2023, 9(4): 878-898

Autonomous Response Systems in Cybersecurity: A Systematic Review of AI-Driven Automation Tools

Name: Dahunsi Samuel Adeyemi

Received: 17 June 2023/Accepted: 09 September 2023/Published: 19 September 2023

Abstract: *Generally, it has been observed that there is a growing need for strong security solutions that can safeguard and improve the dependability of autonomous systems. Thus, this study examined the autonomous response systems in cybersecurity using a systematic review to understand AI-driven automation tools. The study adopts a qualitative systematic review design. Using the Preferred Reporting Items for Systematic Reviews and Meta-analysis (PRISMA), the study adopted a structured approach to search for relevant literature. The final selected literature for the study is sixteen (16). The findings showed that machine learning, deep learning, and natural language processing models are used by organizations to implement AI-driven autonomous response systems. It also emphasized the use of anomaly detection, behavioural analytics, autonomous incident responses, SISMECA, and ontology-based models for securing autonomous transport systems. Results showed that both supervised and unsupervised learning approaches are used for algorithms and methodologies in AI-driven autonomous cybersecurity response systems. Findings showed that AI-driven systems are effective in the mitigation of cyber threats. Results indicate that challenges faced in the deployment of AI-driven autonomous response systems in cybersecurity include adversarial machine learning techniques and the dual-use dilemma. Findings showed that the ethical considerations associated with the deployment of AI-driven autonomous response systems in cybersecurity include collaboration, transparency, and accountability. The study concludes that autonomous response systems are highly effective in cybersecurity. However, there are ethical issues that should be considered in the deployment of the systems.*

Keywords: *Autonomous response systems, cybersecurity, cyberthreat, artificial intelligence, autonomous transport systems*

Dahunsi Samuel Adeyemi
Address: University of Central Missouri, Missouri, US
Email: dxa26930@ucmo.edu
Orcid id: 0009-0007-5485-8052

1.0 Introduction

The continuous evolution of cyber threats has established the limitations of traditional or human-centered mechanisms, which creates challenges that require the need for intelligent and automated solutions. Consequently, this brought about the emergence of autonomous response systems, which are powered by artificial intelligence (AI). These autonomous response systems can enhance cybersecurity resilience, which involves the detection, analysis, and response to threats instantaneously. Ultimately, this can help reduce response latency and minimize human errors. With the use of machine learning, natural language processing, and automated decision-making, AI-driven tools offer scalable and adaptive security measures against sophisticated attacks. Thus, it becomes imperative to understand the advancements, challenges, and opportunities associated with the use of autonomous cybersecurity response systems.

Elayan *et al*. (2021) noted that advances in technology of autonomous systems established the need for understanding the factors that confer resilience on the human-machine system. The term “autonomous response systems" refers to a defence approach for cloud systems that uses a scalable and elastic architecture without a central coordinator to provide risk assessment and mitigation capabilities by monitoring and analyzing system events and computing security and risk metrics (Kholidy *et al*. 2016). An autonomous response system is made up of agents, objects, and components of predetermined types that share an environment and are coordinated to fulfil predetermined global goals through their collective behaviour. It was stressed further that the primary feature of autonomous systems is their capacity to manage information and react to changes in their surroundings in an adaptable manner (Sifakis, 2019).

According to Kholidy (2021), autonomous response systems are defined as those that, depending on the criticality of the cyber-physical space systems (CPPS) asset that can be safeguarded, react to attacks across CPPSS in a scalable and autonomous manner with or without human intervention. Machine learning is now one of the best ways to make decisions for intelligent autonomous systems. Hawkins *et al*. (2021) corroborated this by emphasizing that machine learning (ML) is now used, with results showing it exceeds what is obtainable with human performance. The authors noted that these are in domains such as healthcare, automotive, and manufacturing, where a high degree of autonomy and safety are essential. This accentuates that autonomous systems are more accurate and robust than manual software engineering because they may automatically adapt to a new environment based on the real state of operation by searching through a large number of precise data points for dependable patterns (Chen *et al*., 2021).

Namburi *et al*. (2023) observed that the rapid development of autonomous and connected vehicles has resulted in their incorporation of many software and technologies, which makes them susceptible to cyberattacks. The authors suggested that there is a need for the development of frameworks that integrate cutting-edge cybersecurity techniques like intrusion detection, encryption, and authentication to reduce vulnerabilities and protect vital antivirus systems. This highlights the importance of the current study, which is understanding autonomous response systems in cybersecurity through a systematic review of available evidence in the literature. Dehghantanha *et al*. (2023) noted that autonomous response systems in cybersecurity is an important development in information security, which allows computers to detect, respond, and neutralise cyberthreats on their own without the assistance of humans. Thus, the authors advocated for cybersecurity experts to leverage advanced machine learning (ML) and artificial intelligence (AI) in mitigating cyberthreats.

Noman *et al*. (2022) noted that cybersecurity experts have observed that there is a growing need for strong security solutions that can safeguard and improve the dependability of autonomous systems. The authors argued that there is a need for the integration of cybersecurity to increase autonomous system resilience, which enables proactive threat detection, instantaneous monitoring, and adaptive responses to cyberthreats. Axelrod (2017) argued that cybersecurity requirements should be introduced early in the autonomous response systems lifecycle and maintained stringent standard throughout. The author noted that while it may be insufficient to focus only on in-vehicle systems, the in-vehicle systems cannot be strengthened in isolation. Thus, their security and safety are crucial. Based on the types of communication networks and attack objects, Sun *et al*. (2021) classified cybersecurity risks and vulnerabilities in the environment of connected and autonomous vehicles into in-vehicle network attacks, vehicle to everything network attacks, and other kinds of attacks. This underscores the importance of AI-driven automation tools in cybersecurity.

Mylrea and Gourisetti (2017) noted that AI-based cybersecurity systems are needed for smart decision-making and autonomous defence in the face of evolving threats such as polymorphic malware and hybrid cyber-physical attacks. The authors noted further that AI cybersecurity systems can contribute to the improvement of state-of-the-art by rapidly responding to the evolving cyberattack scenario and improving overall cyber situational awareness, even as the threat changes. Madan *et al*. (2019) argued that a lot of attacks can defile security systems, and the cost of managing these attacks may be too huge that it would be more cost-effective to use cyber-threat modelling and cyber risk analysis techniques. Jamil *et al*. (2022) have called for the continuous development of practical threat modelling methods for autonomous response systems in cybersecurity. Although prior studies have explored AI-driven defence mechanisms, there is limited systematic evidence on their effectiveness, algorithms employed, and ethical implications, leaving a critical gap in understanding their holistic deployment in cybersecurity. The significance of this study lies in its potential to consolidate fragmented evidence on AI-driven autonomous response systems, providing a comprehensive understanding of their effectiveness, algorithms, and ethical considerations. By doing so, the review offers valuable insights to cybersecurity researchers, practitioners, and policymakers, guiding the development of resilient, adaptive, and ethically aligned defence frameworks for autonomous systems. It is against the foregoing that this study seeks to carry out a systematic review on autonomous response systems in cybersecurity. The following are the research questions:

(i) What are the types and characteristics of AI-driven autonomous response systems that have been implemented in cybersecurity?

(ii) What are the algorithms and methodologies frequently used in AI-driven autonomous cybersecurity response systems?

(iii) How effective are autonomous response systems in mitigating cybersecurity threats?

(iv) What are the challenges faced in the deployment of AI-driven autonomous response systems in cybersecurity?

(v) What are the ethical considerations associated with deploying AI-driven autonomous response systems in cybersecurity?

2.0 Methodology

A qualitative systematic review design was adopted to understand autonomous response systems in cybersecurity, carrying out a systematic review of AI-driven automation tools. This kind of research design involves the formulation of research questions, searching of literature across databases, screening of relevant literature using predetermined criteria, the quality of the selected literature was evaluated, relevant information or data was extracted from the final selected studies/literature, and themes are generated by analyzing the information/data extracted (Page *et al*., 2022). In contrast to meta-analysis, which does not allow for qualitative evidence on the data extracted from the literature, this method is a systematic review of the literature to establish the prevailing themes in a specific study (Ahn *et al*., 2018). Thus, this study seeks to qualitatively understand autonomous response systems in cybersecurity, with a focus on AI driven automation tools.

In order to achieve credibility and reliability, there should be repeatability of the study and findability of the relevant literature that was used for the study. A comprehensive search was conducted using techniques and search terms that would aid in answering of formulated research questions. The study used a structured approach to search for relevant literature. The search technique used the Preferred Reporting Items for Systematic Reviews and Meta-analysis (PRISMA). The PRISMA framework

(Fig. 1) provides a structured and transparent approach to data collection and reporting (Helach *et al*., 2023) emphasized that PRISMA is the most popular and widely adopted framework for systematic reviews of literature. The 27-item PRISMA is divided into identification, screening, eligibility, and inclusion. The identification stage concerns literature search, including the sources and databases consulted. The screening stage concerns the evaluation of the titles and abstracts of the literature retrieved. The eligibility phase highlights the inclusion and exclusion criteria. Using this PRISMA framework, the final selected literature for this study is sixteen (16).

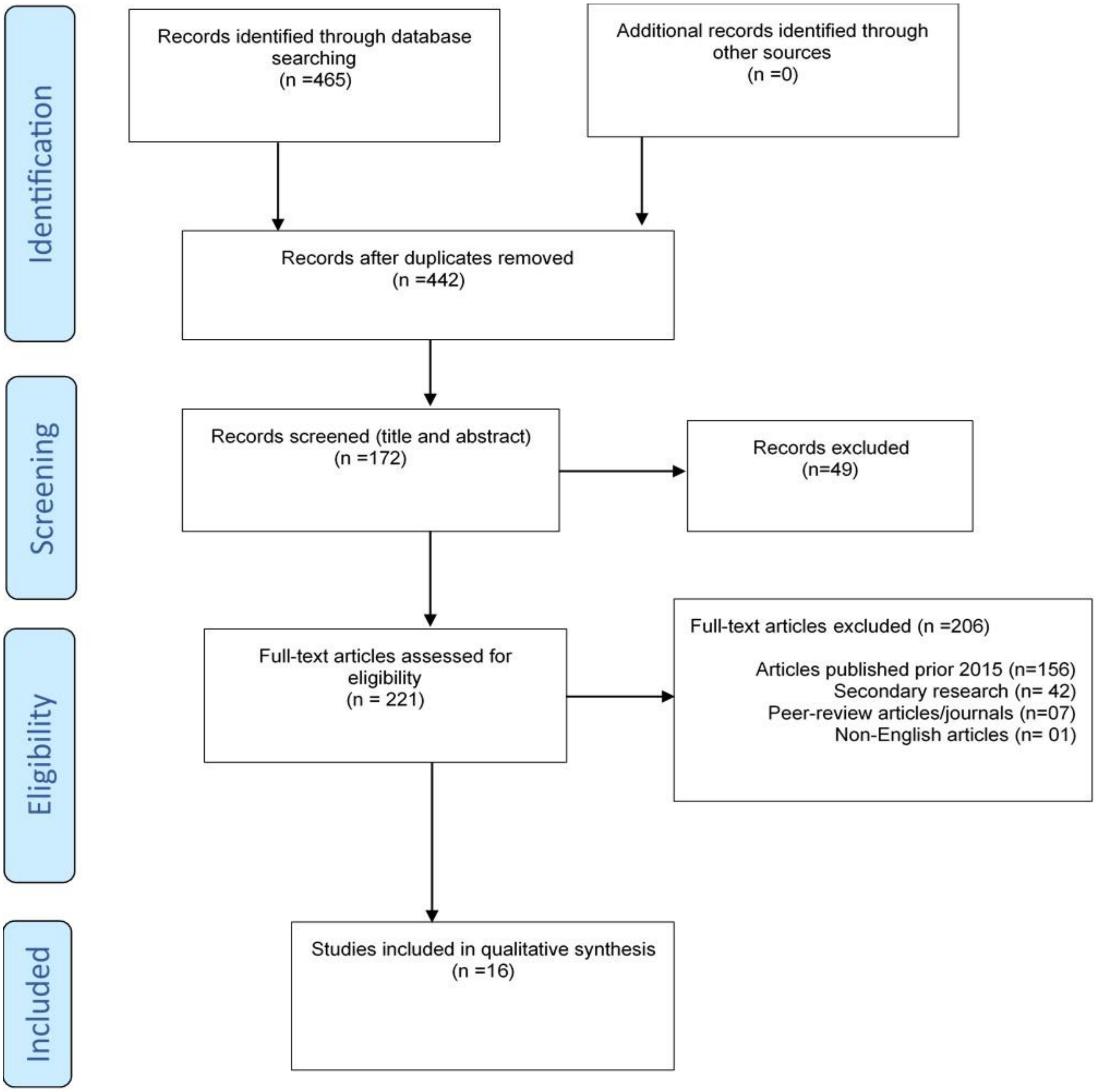
Identification
Records identified through database searching (n =465)
Additional records identified through other sources (n =0)
Records after duplicates removed (n =442)
Screening
Records screened (title and abstract) (n =172)
Records excluded (n=49)
Eligibility
Full-text articles assessed for eligibility (n = 221)
Full-text articles excluded (n =206)
Articles published prior 2015 (n=156)
Secondary research (n= 42)
Peer-review articles/journals (n=07)
Non-English articles (n= 01)
Included
Studies included in qualitative synthesis (n =16)

Fig. 1: PRISMA diagram flow (Author's self-designed, 2023)

To start with, five (5) databases were consulted for relevant literature for the study. These databases include IEEE Xplore, Web of Science, Scopus, Google Scholar, and ACM Digital Library. All these were considered as they have literature on autonomous response systems in cybersecurity. Different search terms were used for this study, which are premised on the main aim and the research questions formulated for the study. Boolean operators of "AND" and "OR" were used for this study owing to the nature of their relevance in connecting the autonomous response systems with cybersecurity. These search terms include "autonomous response systems and cybersecurity", "autonomous response systems OR cybersecurity", "AI-driven automation tools AND cybersecurity", "AI-driven automation tools OR cybersecurity". Having retrieved the relevant literature for the study, scanning was conducted on the methodology sections of the literature to ascertain those studies that were carried out in the focus areas. While this may be considered strenuous, it gives room for an exhaustive assessment of literature in the studied area. Meanwhile, the search period was left between 2013 and 2023. This was considered to allow for the retrieval of recent evidence in the area of study.

To enhance the transparency and reproducibility of the review process, the electronic search strategy adopted for this study is presented in Table 1. The table outlines the search terms employed across the five selected databases (IEEE Xplore, Web of Science, Scopus, Google Scholar, and ACM Digital Library), the number of hits retrieved, and the subsequent screening steps applied. This provides a concise summary of the search outcomes and demonstrates the systematic approach used to identify and refine the final body of literature included in the review.

Table 1: Electronic Search Strategy (Extracts for five databases)

S/N	Search terms	IEEE Xplore	Web of Science	Scopus	Google Scholar	ACM Digital Library
				Number of hits		
S1	Autonomous response systems AND cybersecurity	2890	1200	595	752	1502
S2	Autonomous response systems OR cybersecurity	2173	750	123	981	1742
S3	AI-driven automation tools AND cybersecurity	23000	21000	17300	27000	5211
S4	AI-driven automation tools OR cybersecurity	21000	28000	14000	17000	3590
Databases search limits adopted						
Duplicates removed		89	91	75	82	75
Titles and abstracts checked		56	70	46	28	51
Articles < or = 10 years (2013-2023)		33	19	29	55	24
Secondary research		21	09	12	28	14
Peer-reviewed articles/journals		13	04	05	15	06
English language only		NA	N/A	02	N/A	N/A
Final selected		5	1	2	6	2

Source: Author's Literature Search (2023)

3.0 Results and Discussion

On the research question one, the findings of the study showed that there are different types and characteristics of AI-driven autonomous response systems that have been implemented in cybersecurity. Two of the studies (Tanikonda *et al*., 2022; Yaseen, 2023) demonstrate how machine learning (ML), deep learning (DL), and natural language processing (NLP) models are used by organizations to ensure a paradigm shift. This is done by moving from reactive to proactive security strategies through the prediction and countering of threats in complex ecosystems. Mainoo *et al*. (2022) emphasized on the use of anomaly detection, behavioural analytics, and autonomous incident responses, while Illiashenko *et al*. (2023) demonstrated that SISMECA and ontology-based models can be used in the protection of autonomous transport systems. These findings indicate that AI-based systems combine tools such as digital twins, multi-agent frameworks, and zero-trust architecture to enhance resilience and trust. It was revealed that the AI-based systems are modelled to be adaptive, predictive, and scalable.

On the research question two, the findings showed that there is heavy reliance on supervised and unsupervised learning approaches with respect to algorithms and methodologies frequently used in AI-driven autonomous cybersecurity response systems. Tiwari *et al*. (2020) identified more than fifty (50) algorithms and methodologies, which include artificial neural networks (ANN), decision trees (DT), convolutional neural networks (CNN), support vector machines (SVM), random forests (RF), and reinforcement learning (RL). Some of the final selected studies (Maka *et al*., 2021; Rahman *et al*., 2023) highlighted that reinforcement learning is a powerful tool for detecting new attack patterns and recommending optimal countermeasures. Meanwhile, Santoso and Finn (2023) underscore the relevance of hybrid approaches, which include the integration of fuzzy logic, ML, and neural networks. This hybrid approach generates novel hybrid knowledge for intelligent cybersecurity. Studies (Maka *et al*., 2021) established that these methodologies are complemented by preprocessing and simulation techniques, which strengthen instantaneous decision-making and operational testing.

On the third research question , it was revealed that AI-driven systems are effective in mitigating cyberthreats. The results demonstrated that there is a 98% detection accuracy for network intrusions using deep learning (Dalal, 2018), while Rahman *et al*. (2023) showed the ability of RL systems to adapt to changing attack strategies and improve detection performance over time. Similarly, Tiwari *et al*. (2020) revealed that the AI-enabled intrusion detection and prevention systems reduced false positives to just 0.012%, which is an improvement over the traditional methods. Studies (Madan *et al*., 2019) showed that AI enhances situational awareness, early warning, and incident response, which contribute to national resilience and the safe operation of autonomous and unmanned systems. Generally , the synthesis of the final selected literature indicates that autonomous response systems improve speed, accuracy, and adaptability in alleviating cybersecurity threats.

On research question four, the findings revealed that there are several challenges faced in the deployment of AI-driven autonomous response systems in cybersecurity. Wickramasinghe (2023) highlights that adversarial machine learning techniques can manipulate AI models, which causes misclassification of threats. Aramide (2022) underscores the dual-use dilemma, which shows that AI strengthen defences and introduces new vulnerabilities that adversaries exploit. Dalal (2018) highlights data quality challenges and model bias as recurrent problems, while other studies (Sarsam, 2023; Yağdereli *et al*., 2015) demonstrated that the challenges in developing comprehensive regulatory frameworks and standards for securing autonomous systems. All of these challenges show that the frailty of static AI models and the necessity of continuous retraining, explainability, and integration with human experts.

On research question five, the findings showed that there are several ethical considerations associated with the deployment of AI-driven autonomous response systems in cybersecurity. Karunamurthy *et al*. (2023) argued that artificial intelligence is essential, which requires collaboration among AI experts, cybersecurity professionals, ethicists, and policymakers to ensure responsible deployment. Tiwari *et al*. (2020) advocated for explainable AI to enhance transparency, while Aramide (2022) shows the risk of opaque decision-making that may compromise accountability. It was shown that the issue of trust, privacy, and fairness are important as autonomous systems assume greater control in cyberspace defence. The results advocated for the design of ethical frameworks that balance technological autonomy with human oversight, which ensures that the use of AI in cyber security aligns with broader societal values.

4.0 Conclusion

The study established that there are various types and characteristics of AI-driven autonomous response systems, which highlight the use of machine learning (ML), deep learning (DL), and natural language processing (NLP) models to move from the reactive to proactive security strategies through the prediction and countering of threats in complex ecosystems. The study recognized that AI-based systems that integrate tools such as digital twins, multi-agent frameworks, and zero-trust architecture to enhance resilience and trust. The study recognized that there is heavy reliance on supervised and unsupervised learning approaches with respect to algorithms and methodologies frequently used in AI-driven autonomous cybersecurity response systems. The study established that AI-driven systems are effective in the mitigation of cybersecurity threats. It was recognized that autonomous response systems improve speed, accuracy, and adaptability in the alleviation of cybersecurity threats. The study concludes that there are several challenges faced in the deployment of AI-driven autonomous response systems in cybersecurity. All of the challenges point to the frailty of static AI models and the necessity of continuous retraining, explainability, and integration with human experts. In conclusion, the study highlights that there are several ethical considerations associated with the deployment of AI-driven autonomous response systems in cybersecurity.

5.0 Implications

The findings of the study demonstrate that AI-driven systems enhance resilience, accuracy, and adaptability in cybersecurity, which emphasize the need for policymakers to create policies that guide AI-driven cybersecurity measures. Also, challenges such as adversarial attacks, data bias, and dual-use dilemma accentuate the limitations of the current practice. Policymakers should, therefore, develop frameworks for transparency, accountability, and ethical use of AI in cybersecurity. The study recognized hybrid approaches and reinforces learning, which means that policies must be flexible to accommodate the evolving technological advancements. Moreover, the involvement of different stakeholders like AI developers, cybersecurity experts, and ethicists necessitates policies that foster cross-sector collaborations. The emphasis on the capacity of AI to improve situational awareness and response implies that the government should prioritize investment in secure and ethical AI infrastructures.

The findings of the study emphasized the paradigm shift in operational approaches to cybersecurity. The deployment of machine learning, deep learning, natural language processing, and anomaly detection techniques indicates that security professionals must adopt proactive, predictive, and adaptive methods rather than reactive ones. The study reinforces learning and hybrid models, which indicates that practitioners need to be trained continuously on the emerging AI methodologies and simulation tools. Moreover, given the challenges associated with adversarial attacks and model bias, cybersecurity experts should consider the integration of human oversight into AI-driven decision-making processes. This highlights the importance of human-AI collaboration, where professionals remain important in the verification of outputs and ensure that models are retrained with unbiased data. Cybersecurity experts must develop ethical awareness when designing and deploying AI-driven systems.

The findings of the study highlight the integration of diverse methodologies, which advance push theory beyond traditional frameworks of intrusion detection and incident response toward models of autonomous and adaptive resilience. The study highlights the effectiveness of hybrid approaches, which suggest that there is a need for a new technique that integrates computational intelligence, behavioural analytics, and ethical governance into a holistic cybersecurity theory. Moreover, the challenges of explainability and adversarial manipulation demand the incorporation of sociotechnical perspectives where interaction among human values, organizational systems, and AI technologies is critical in theoretical modelling.

The study underscores the opportunities and risks associated with the use of AI-driven technologies in cybersecurity. The improved detection accuracy and reduction in false positives promise safer digital ecosystems, which improve public trust in digital transactions, communication, and governance. However, the ethical issues regarding fairness, accountability, and transparency indicate the potential for societal harm if these systems are not developed with safeguarding measures. Trust and privacy emerge as important societal values that give citizens assurance that autonomous cybersecurity systems protect rather than infringe on their rights. Moreover, there is a need for renewed awareness and education programs that elucidate the intricacies of AI and encourage responsible digital citizenship. Collaborations among technologists, ethicists, and policymakers can enhance societal expectations in respect to technological capabilities, which prevents misuse and strengthens resilience against cyberthreats.

5.0 References

Ahn, E., & Kang, H. (2018). Introduction to systematic review and meta-analysis. *Korean Journal of Anesthesiology*, 71, 2, pp. 103-112.

Aramide, O. O. (2022). AI-Driven cybersecurity: The double-edged sword of automation and adversarial threats. *International Journal of Humanities and Information Technology*, 4, 4, pp. 19-38.

Axelrod, C. W. (2017). Cybersecurity challenges of systems-of-systems for fully-autonomous road vehicles. In *2017 13th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT)* (pp. 1-6). IEEE.

Chen, H., Wen, Y., Zhu, M., Huang, Y., Xiao, C., Wei, T., & Hahn, A. (2021). From automation system to autonomous system: An architecture perspective. *Journal of Marine Science and Engineering*, 9, 6, pp. 645-655.

Dalal, A. (2018). Cybersecurity and Artificial Intelligence: How AI is being used in cybersecurity to improve detection and response to cyber threats. *Turkish Journal of Computer and Mathemafics Educafion*, 9*,* 3, pp. 1704-1709.

Dehghantanha, A., Yazdinejad, A., & Parizi, R. M. (2023). Autonomous cybersecurity: Evolving challenges, emerging opportunities, and future research trajectories. In *Proceedings of the Workshop on Autonomous Cybersecurity* (pp. 1-10).

Elayan, H., Aloqaily, M., Salameh, H. B., & Guizani, M. (2021). Intelligent cooperative health emergency response system in autonomous vehicles. In *2021 IEEE 46th Conference on Local Computer Networks (LCN)* (pp. 293-298). IEEE.

Hawkins, R., Paterson, C., Picardi, C., Jia, Y., Calinescu, R., & Habli, I. (2021). Guidance on the assurance of machine learning in autonomous systems (AMLAS). *arXiv preprint arXiv2102 .01 564*.

Helach, J., Hoffmann, F., Pieper, D., & Allers, K. (2023). Reporting according to the preferred reporting items for systematic reviews and meta-analyses for abstracts (PRISMA-A) depends on abstract length. *Journal of Clinical Epidemiology*, 154, pp. 167-177.

Illiashenko, O., Kharchenko, V., Babeshko, I., Fesenko, H., & Di Giandomenico, F. (2023). Security-informed safety analysis of autonomous transport systems considering AI-powered cyberattacks and protection. *Entropy*, *25,* 8, 1123, https://doi.org/10.3390/e25081123.

Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, *1*, pp. 564-74.

Maka, S. R., Boppana, S. B., Sadaram, G., Katnapally, N., Murthy, L., & Sakuru, M. (2021). Automating cyber threat response using agentic AI and reinforcement learning techniques. *Journal of Electrical Systems*, 17, 4, pp. 138-148.

Karunamurthy, A., Kiruthivasan, R., & Gauthamkrishna, S. (2023). Human-in-the-loop intelligence: Advancing ai-centric cybersecurity for the future. *Quing: International Journal of Multidisciplinary Scientific Research and Development*, 2, 3, pp. 20-43.

Kholidy, H. A. (2021). Autonomous mitigation of cyber risks in the Cyber–Physical Systems. *Future Generation Computer Systems*, 115, pp. 171-187.

Kholidy, H. A., Erradi, A., Abdelwahed, S., & Baiardi, F. (2016). A risk mitigation approach for autonomous cloud intrusion response system. *Computing*, *98*(11), 1111-1135.

Madan, B. B., Banik, M., & Bein, D. (2019). Securing unmanned autonomous systems from cyber threats. *The Journal of Defense Modeling and Simulation*, 16, 2, pp. 119-136.

Mylrea, M., & Gourisetti, S. N. G. (2017). Cybersecurity and optimization in smart "autonomous" buildings. In *Autonomy and Artificial Intelligence: A Threat or Savior?* (pp. 263-294). Cham: Springer International Publishing.

Namburi, V. L., Adapa, S. R., Chamala, S. S. K., Yerram, M., Gupta, P., & Upreti, K. (2023). Integrating AI and cybersecurity: Advancing autonomous vehicle security and response mechanisms. In *2023 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)* (pp. 253-258). IEEE.

Noman, I. R., Bortty, J. C., Bishnu, K. K., Aziz, M. M., & Islam, M. R. (2022). Data-driven security: Improving autonomous systems through data analytics and cybersecurity. *Journal of Computer Science and Technology Studies*, 4, 2, pp. 182-190.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., & Chou, R. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Systematic Reviews*, 10, 1, pp. 1-11.

Rahman, M. M., Hossain, M. S., Mashfiquer, M., Rahman, M. S. U., Nahar, S., & Rahman, M. M. (2023). Reinforcement learning for adaptive cybersecurity: AI-driven threat detection and response mechanisms. *ICONIC Research and Engineering Journals*, 7, 1, pp. 721-732.

Santoso, F., & Finn, A. (2023). An in-depth examination of artificial intelligence-enhanced cybersecurity in robotics, autonomous systems, and critical infrastructures. *IEEE Transactions on Services Computing*, 17, 3, pp. 1293-1310.

Sarsam, S. M. (2023). Cybersecurity challenges in autonomous vehicles: Threats, vulnerabilities, and mitigation strategies. *SHIFRA*, 2023, pp. 34-42.

Sifakis, J. (2019). Autonomous systems–an architectural characterization. In *Models, Languages, and Tools for Concurrent and Distributed Programming: Essays Dedicated to Rocco De Nicola on the Occasion of His 65th Birthday* (pp. 388-410). Cham: Springer International Publishing.

Sun, X., Yu, F. R., & Zhang, P. (2021). A survey on cyber-security of connected and autonomous vehicles (CAVs). *IEEE Transactions on Intelligent Transportation Systems*, 23, 7, pp. 6240-6259.

Tanikonda, A., Pandey, B. K., Peddinti, S. R., & Katragadda, S. R. (2022). Advanced AI-driven cybersecurity solutions for proactive threat detection and response in complex ecosystems. *Journal of Science & Technology*, 3, 1, pp. 196-217.

Tiwari, S., Sresth, V., & Srivastava, A. (2020). The role of explainable AI in cybersecurity: Addressing transparency challenges in autonomous defense systems. *International Journal of Innovative Research in Science Engineering and Technology*, 9, pp. 718-733.

Wickramasinghe, A. (2023). An evaluation of big data-driven artificial intelligence algorithms for automated cybersecurity risk assessment and mitigation. *International Journal of Cybersecurity Risk Management, Forensics, and Compliance*, 7, 12, pp. 1-15.

Yağdereli, E., Gemci, C., & Aktaş, A. Z. (2015). A study on cyber-security of autonomous and unmanned vehicles. *The Journal of Defense Modeling and Simulation*, 12, 4, pp. 369-381.

Yaseen, A. (2023). AI-driven threat detection and response: A paradigm shift in cybersecurity. *International Journal of Information and Cybersecurity*, 7, 12, pp. 25-43.

Declaration

Consent for publication

Not applicable

Availability of data

Data shall be made available on demand.

Competing interests

The authors declared no conflict of interest

Ethical Consideration

Not applicable

Funding

There is no source of external funding.

Authors' Contribution

The work was carried out and written by the author

APPENDIX I
DATA EXTRACTION TOOL
Autonomous Response Systems in Cybersecurity: A Systematic Review of AI-Driven Automation Tools

S/N	Research titles and authors	Methodology	Models	Findings
1	Advanced AI-driven cybersecurity solutions for proactive threat detection and response in complex ecosystems Tanikonda *et al*. (2022)	Case study research design.	The study integrated machine learning (ML), deep learning (DL), and natural language processing (NLP).	- This comprehensive analysis demonstrates that AI-driven cybersecurity solutions are indispensable for proactively managing threats in increasingly interconnected and complex ecosystems. By leveraging the predictive capabilities of AI, organizations can transition from a reactive to a proactive security posture, enhancing their ability to anticipate, detect, and respond to cyber risks.
2	AI-driven threat detection and response: A paradigm shift in cybersecurity Yaseen (2023)	Experimental research design.	The study adopts machine learning and deep learning.	- The study showed that the vital job of man-made intelligence-driven arrangements in expanding danger location and reaction components, enabling frameworks to battle developing cyber dangers proactively. - The study highlighted the flexibility and prescient capacities of AI, essential in exploring the unique danger scene. The study shed light on the advancement of man-made intelligence inside cybersecurity, portraying the direction from customary guard systems to computer-based intelligence-driven proactive techniques. It featured the adequacy of simulated intelligence in knowing

				perplexing examples and abnormalities inside enormous datasets, sustaining the strength of cybersecurity conventions against refined dangers.
3	National resilience through ai-driven data analytics and cybersecurity for real-time crisis response and infrastructure protection	Qualitative case study approach.	Machine learning, deep learning, and AI models.	- The study reveals that AI-driven data analytics significantly improve early warning capabilities, situational awareness, and decision-making speed in high-risk scenarios. It also demonstrates that the adoption of AI-enhanced cybersecurity tools—such as anomaly detection, behavioral analytics, and autonomous incident response—plays a crucial role in securing digital infrastructure against evolving cyber threats. - Furthermore, the application of simulation models and digital twins was found to support real-time modeling, predictive planning, and operational testing, thereby strengthening the adaptability of critical systems. Multi-agent decision support systems and explainable AI interfaces facilitated better interagency coordination and user trust, while zero-trust architectures enabled granular control over access and threat containment.
4	Security-informed safety analysis of autonomous transport systems considering AI-powered cyberattacks and protection	The study adopted SIS-based methodology and the SISMECA technique, in combination with the	The study implemented SISMECA using ontology model	- SISMECA is an example of an attribute-scalable analysis technique, since it allows one to assess ATS characteristics under various options of artificial intelligence applications, such

	Illiashenko *et al*. (2023)	well-known FMECA technique		as AI-powered protection against AI-powered attacks - As AI-based cybersecurity tools evolve, so do the functional safety and cybersecurity concerns surround their use in attacks on ATS. Various factors, including the increasing complexity of ATS, the growing sophistication of cyber attackers, and the need for improved safety and security in these systems, drive the evolving nature of these concerns. - The adopted approach of combining SIS- and AIQM-based assessment techniques brings together security, safety, and AI considerations to address emerging challenges, provide holistic assessments, enhance transparency and traceability, minimise uncertainty, and benefit a wide range of stakeholders involved in autonomous transport systems.
5	Reinforcement learning for adaptive cybersecurity: AI-driven threat detection and response mechanisms Rahman *et al*. (2023)	Experimental research design. The analysis of reinforcement learning (RL) models for cybersecurity will rely on five performance metrics, which measure accuracy, detection rate, and false positive/negative occurrences, as well as	Machine learning and reinforcement learning.	- Implementing machine learning (ML) systems has started to improve traditional cybersecurity methods because of their current deficiencies. The combination of anomaly detection with intrusion detection systems (IDS) and malware classification technologies uses machine learning algorithms to recognize irregular behavior and potential threats through pattern recognition methods in data.

		real-time capabilities and scalability.		- Reinforcement learning technology produced substantial cybersecurity upgrades because it enabled threat detection of unknown attacks while adjusting to shifting attack patterns. The RL-based models discovered novel intruder pathways, which they modified their security methods to counter. Because of its adaptive nature, RL systems optimized their threat detection twice, becoming more effective in detecting changing cyber threats.
6	An evaluation of big data-driven artificial intelligence algorithms for automated cybersecurity risk assessment and mitigation Wickramasinghe (2023)	Case-study research design.	Deep learning and machine learning.	- The dynamic and evolving nature of the threat landscape further complicates the deployment of AI in cybersecurity. Cyber attackers are continuously developing new tactics, techniques, and procedures (TTPs) to bypass existing security measures, rendering static AI models obsolete over time. For instance, adversaries may employ techniques such as adversarial machine learning to exploit vulnerabilities in AI systems, causing them to misclassify malicious activities as benign. To remain effective against novel threats, AI systems must be designed for adaptability, with mechanisms for ongoing updates and retraining.

7	Automating cyber threat response using agentic AI and reinforcement learning techniques Maka *et al*. (2021)	Preprocessing techniques are implemented to cleanse and organize the data prior to modeling, thereby facilitating the cleaning of data and making it ready for use.	Reinforcement learning and machine learning models.	- Agentic AI systems and reinforcement learning-based technologies are introduced. These technologies contribute to swiftly accommodating the evolving nature of cyber threats and enhancing cybersecurity responses, reducing the discrepancy between the speed of threat response construction and incidents. - Agentic AI frameworks take control in cyber threat responses by analyzing diverse possibilities to harness the emerging trends among malware and bots, before instructing their counterparts. Reinforcement learning outcomes are incorporated in the threat response of the cyber defense arrangement through the recommendation of the optimal countermeasure, surpassing manual policy drafting.
8	Cybersecurity and Artificial Intelligence: How AI is being used in cybersecurity to improve detection and response to cyber threats Dalal (2018)	Quantitative and qualitative select human intelligence attributes are discussed by analysing case studies and real-world examples of AI powered cybersecurity systems	Deep learning and machine learning model.	- The paper suggests that the AI-based, cybersecurity systems can highly facilitate threat detection accuracy, diminish response time and help in identifying the emerging phenomenon to some extent. - The deep learning model, from particular research, was able to detect network intrusions more than 98% precisely, while a novel unsupervised machine learning algorithm has been

				successfully used for detecting up to 90% of undetected malware samples. - Quantitative data gives us perspective on both the benefits like increased efficiency, a scalable platform, proactive threat detection, and continuous learning, and the obstacles, including the question of quality of the data, bias of models, and the necessity of the human factor.
9	Human-in-the-loop intelligence: Advancing ai-centric cybersecurity for the future Karunamurthy *et al*. (2023)	Experimental research design.	Natural Language Process (NLP), deep learning-based model, and Loop Intelligence Cybersecurity Model.	- The symbiotic interplay between AI experts, cybersecurity specialists, ethicists, policymakers, and communication professionals are not just a strategic choice but a necessity. The convergence of diverse expertise is crucial not only for technical problem-solving but also for developing ethical frameworks, effective policies, and transparent communication strategies.
10	The role of explainable AI in cybersecurity: Addressing transparency challenges in autonomous defense systems Tiwari *et al*. (2020)	Mixed-methods research approach.		- It was shown that the number of articles devoted to AI methods to provide cybersecurity has grown considerably during the last few years. AI techniques in cybersecurity started appearing about 2015. - Techniques and Field of Uses in Cybersecurity: In each of the studies that formed the basis of the review, it was possible to identify over 50 different algorithms. The most dominant algorithms were: Supervised: ANN,

				CNN, DT, KMeans, KNN, AdaBoost, q-Learning, RF, RNN, SVM. - Effectiveness of AI Methods on Cyberspace Security: In detection and prevention systems the most notable impact of AI has been the optimization of false positives in IDPS. In the improvement of its detection algorithm, all studies on IDPS cited a lower incidence of false alerts. For instance, one research has revealed that their IDPS approach have a very low false alarm rate of approximately 0.012% which is the lowest on record for impersonation attack detection.
11	AI-Driven cybersecurity: The double-edged sword of automation and adversarial threats Aramide (2022)	Case study research design. This study adopts a mixed-methods approach, combining qualitative case analysis with comparative evaluation of AI-driven cybersecurity tools and adversarial techniques.	Natural language process and deep learning model	- The incorporation of artificial intelligence into cybersecurity is the turning point in the war against the more complicated and proficient online threats. Allowing an AI to liberate capabilities that nobody in this world can effectively reproduce in threat detection, incident response accelerations, and improving predictive intelligence, AI itself also creates new vulnerabilities in the system as it is being exploited by enemies, and the decision-making process is obscure. Such dual-use nature characterizes AI as a significant tool and a possible source of danger in the field of cybersecurity.

12	Securing unmanned autonomous systems from cyber threats Madan *et al*. (2019)	Quantitative and qualitative research methods.	Deep learning model	- Findings showed that the operation of unmanned systems, and of applications that use these systems, are heavily dependent on cyber systems that are used to collect, store, process and communicate data, making data a critical resource. At the same time, undesirable elements of our society and adversarial states have also realized the high value of this resource. - The study identified the security requirements of unmanned autonomous systems, and follow this up with modeling how attacks achieve their objectives. The study established that a large number of threats that can materialize as attacks and the costs of managing these attacks in cost effective ways require ranking threats using cyber threat modeling and cyber risk analysis techniques.
13	Cybersecurity challenges in autonomous vehicles: Threats, vulnerabilities, and mitigation strategies Sarsam (2023)	Qualitative research design.	The study integrated machine learning (ML) and deep learning (DL).	- The study provides comprehensive mitigation strategies, with policy recommendations to develop effective global cybersecurity standards and regulatory frameworks including encryption, intrusion detection systems, secure software updates, and integrating post-quantum cryptography to address future threats from quantum computer programming. - The results highlight the need for a multilevel cybersecurity strategy that

				incorporates both technical and legal solutions. The findings suggest that a holistic approach is needed to secure AV systems, addressing not only implementation can significantly reduce the risk of cyberattacks, and ensure that autonomous vehicles operate safely and reliably in a highly connected world.
14	Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses Jimmy (2021)	Qualitative research design.	Ransomware-as-a-service (RaaS) models.	- The findings showed that from the insidious spread of ransomware to the sophisticated tactics employed by malicious actors in phishing schemes and insider threats, the digital realm remains fraught with peril. However, amidst these challenges, we have illuminated a beacon of hope – the transformative potential of artificial intelligence (AI) in fortifying our defenses against cyber threats. - Findings revealed a promising frontier where machine learning algorithms, neural networks, and other AI technologies stand as bulwarks against the rising tide of cyber-attacks. Through real-time threat detection, behavioral analysis, and adaptive response mechanisms, AI empowers security professionals with unprecedented capabilities to anticipate, identify, and neutralize threats before they wreak havoc. From anomaly detection to predictive analytics, AI augments human expertise, enabling

				proactive defense strategies in an increasingly complex digital ecosystem.
15	A study on cyber-security of autonomous and unmanned vehicles Yağdereli *et al*. (2015)	Mixed-methods research design.	Deep learning model.	- The security of autonomous vehicles (AVs) is paramount as they become an integral part of modern transportation systems. The sophisticated technology and vast amounts of data that AVs rely on make them vulnerable to a wide range of cyber threats. As these vehicles evolve, so too do the tactics employed by cybercriminals, making traditional cybersecurity measures inadequate for addressing the complexity and scope of potential risks. Artificial Intelligence (AI) has emerged as a powerful tool in securing AVs, providing advanced threat detection, analysis, and response capabilities that are essential for safeguarding these vehicles from cyberattacks. - AI-powered threat analysis enhances the ability to predict and assess risks, allowing AVs to take proactive measures before an attack occurs. By analyzing historical data and recognizing patterns in cyberattack strategies, AI can anticipate potential threats and mitigate them before they affect vehicle performance or safety. Furthermore, AI systems can autonomously respond to detected threats, isolating compromised components and initiating countermeasures to prevent further

				damage, ensuring the continued safe operation of AVs. AI plays a pivotal role in securing autonomous vehicles from cyber threats.
16	An in-depth examination of artificial intelligence-enhanced cybersecurity in robotics, autonomous systems, and critical infrastructures Santoso and Finn (2023)	Quantitative research approach.	Machine learning, fuzzy logic, and neural networks	- The study established that the implementation of multiple AI algorithms to tackle current security issues in robotics will transform and create novel hybrid knowledge for intelligent cybersecurity at the application level.