https://journal.ypidathu.or.id/index.php/jssut/
P - ISSN: 3026-5959
E - ISSN: 3026-605X

Opportunities and Challenges in AI-Driven Cybersecurity: A Systematic Literature Review of Threat Detection and Mitigation

Shahwali Shahidi[1], Farid Ahmad Darmel[2], Safiullah Jalalzai[3], Ghulam Ali Amiri[4]
[1]Kabul Education University, Afghanistan
[2,3,4]Ghazni University, Afghanistan

ABSTRACT

Background. The need for more sophisticated security strategies has become apparent as the number of cyber threats grows. AI is one framework that has been shown to boost security by providing advanced threat detection and response capabilities. Nonetheless, AI integration introduces inherently ethical and privacy-related concerns.

Purpose. This research examines the AI implementation factors influencing the overall performance of the AI for cybersecurity and data privacy in both critical infrastructures and financial services.

Method. This research derives its data from the extensive literature published from 2019 to 2024 in notable databases such as IEEE, Science Direct, MDPI, and Wiley Library, with more than 300 records. This analysis examined, with the help of artificial intelligence tools, the patterns and recurrent problems about the place of AI in cybersecurity, setting sights on the present challenges in the domains of intrusion detection and mitigation.

Results. The results indicate that better threat detection in industry is enabled by AI. However, disadvantages of bias, the need for privacy, and suboptimal data management are evident, necessitating the need for stronger machine and human-readable regulations.

Conclusion. Although AI strengthens security in an age of cyber-insecurity, its shortcomings point to the need for further development. Post-quantitative encryption palliatives and integration models will be effectively handled as cybersecurity-harming threats evolve.

KEYWORDS

Artificial Intelligence, Cybersecurity, Machine Learning, Privacy Concerns, Threat Detection

Citation: Shahidi, S., Darmel, A, F., Jalalzai, S., & Amiri, A, G. (2024). Opportunities and Challenges in AI-Driven Cybersecurity: A Systematic Literature Review of Threat Detection and Mitigation. *Journal of Social Science Utilizing Technology*, *2*(4), 516–530.
https://doi.org/10.70177/jssut.v2i4.1541

Correspondence:

Ghulam Ali Amiri,
ali.amiri0991@gmail.com

Received: November 20, 2024

Accepted: November 21, 2024

Published: Desember 2, 2024

INTRODUCTION

Computerized reasoning (man-made intelligence) has quickly arisen as an extraordinary innovation with the possibility to upgrade security frameworks across different spaces fundamentally. As of late, the reconciliation of artificial intelligence in network protection has accumulated significant consideration, provided its capacity to examine enormous datasets, recognize examples, and settle on continuous choices. The use of simulated intelligence in security isn't restricted to customary IT conditions yet reaches out to basic framework, monetary foundations, medical care, and, surprisingly, public protection. This efficient writing survey means to investigate the open doors and difficulties related with simulated intelligence upgraded security,

extensive outline of the present status of examination in this quickly developing field [1], [2].

One of the most encouraging open doors introduced by computer based intelligence in security is its capacity to recognize and answer digital dangers more productively than customary techniques. Computer based intelligence controlled frameworks can break down immense measures of information to distinguish peculiarities and expected dangers, frequently before they are perceived by human administrators [3], [4]. This proactive methodology considers faster reactions to assaults, diminishing the possible harm and limiting margin time. Besides, simulated intelligence can consistently learn and adjust to new dangers, making it an important resource in the steadily changing scene of network protection [5], [6].

One more critical open door lies in the computerization of routine security undertakings. Man-made intelligence can take over redundant errands, for example, observing organization traffic, dissecting logs, and identifying phishing endeavors, opening up HR for more perplexing dynamic cycles [7], [8]. This expands the productivity of safety tasks as well as diminishes the probability of human blunder, which is much of the time a huge weakness in security frameworks [9], [10].

Nonetheless, the incorporation of simulated intelligence into security frameworks isn't without its difficulties. One of the essential worries is the potential for simulated intelligence frameworks to be taken advantage of by pernicious entertainers. Similarly, as artificial intelligence can be utilized to upgrade security, it can likewise be weaponized to make more complex and designated assaults [11], [12]. The utilization of simulated intelligence in creating deepfakes, sending off robotized assaults, and bypassing conventional safety efforts represents a critical danger to associations and people the same [13], [14].

One more test is the moral and lawful ramifications of involving artificial intelligence in security. The arrangement of artificial intelligence frameworks frequently includes the assortment and examination of a lot of individual information, raising worries about security and information insurance [15]. Moreover, the absence of straightforwardness in man-made intelligence dynamic cycles, frequently alluded to as the "black box" issue, can prompt issues of responsibility and trust.

Significance of Study

Significance of this Study lies in its investigation of the developing convergence between Man-made consciousness (computer based intelligence) and online protection, a basic region as advanced dangers become progressively modern. By efficiently evaluating the writing on man-made intelligence upgraded security, this review gives an extensive comprehension of both the open doors and difficulties that computer based intelligence presents in safeguarding delicate data and framework. The discoveries from this exploration can direct policymakers, security experts, and innovation engineers in coming to educated conclusions about the joining regarding computer based intelligence into security frameworks. Also, the review recognizes holes in ebb and flow research, featuring regions where further examination is expected to improve the viability of man-made intelligence in fighting digital dangers. Eventually, this exploration adds to the more extensive talk on how arising advancements can be outfit to reinforce safety efforts in an undeniably computerized world, underscoring the requirement for adjusted, moral, and creative methodologies.

The essential targets of this study are triple: First, to assess the adequacy of computer based intelligence in distinguishing and moderating digital dangers across different spaces, including basic framework and monetary frameworks. Second, to recognize the vital difficulties and restrictions related with the reconciliation of man-made intelligence into existing security systems, especially zeroing in on moral and protection concerns. Third, to investigate possible progressions and

systems for upgrading man-made intelligence driven security arrangements, with an accentuation on lessening weaknesses and further developing reaction times. These targets will direct the exploration in giving a far reaching comprehension of man-made intelligence's part in current network safety.

Research Questions

RQ1: How effective is AI in detecting and mitigating cyber threats across different domains, including critical infrastructure and financial systems?

RQ2: What are the key challenges and limitations associated with integrating AI into existing security frameworks, particularly concerning ethical and privacy issues?

RQ3: What potential advancements and strategies can enhance AI-driven security solutions to reduce vulnerabilities and improve response times?

SATE OF THE ART

The combination of Man-made consciousness (artificial intelligence) into online protection is reshaping how security dangers are recognized, broke down, and moderated. A complete survey of the writing uncovers both the potential and the difficulties related with simulated intelligence upgraded security frameworks [1].

Simulated intelligence's essential strength in online protection lies in its capacity to examine tremendous measures of information to recognize irregularities that might demonstrate security dangers [2]. AI and profound learning strategies are instrumental in upgrading danger discovery rates and decreasing misleading up-sides [3], [4]. For example, man-made intelligence models prepared on verifiable assault information can distinguish designs related with malevolent exercises, including modern zero-day takes advantage of that could sidestep conventional recognition techniques [5], [6]. This ability takes into consideration more precise and opportune recognizable proof of dangers, essentially working on safeguarding strategies.

Additionally, computer based intelligence driven mechanization is changing the productivity of safety activities by taking care of routine checking undertakings, for example, dissecting network traffic and recognizing phishing endeavors [7], [8]. Mechanized frameworks can execute predefined reactions to expected dangers, accordingly diminishing the weight on human administrators and limiting the reaction time [9], [10]. This robotization likewise helps in redistributing HR to additional mind boggling and vital assignments, accordingly upgrading by and large security tasks [11], [12].

In spite of these headways, a few difficulties upset the far reaching reception of artificial intelligence in network safety. One huge issue is the defenselessness of artificial intelligence frameworks to ill-disposed assaults, where malevolent entertainers exploit weaknesses in computer based intelligence models [13], [14]. Antagonistic AI methods can control input information to trick computer based intelligence frameworks, possibly prompting serious security breaks [15]. Such weaknesses raise worries about the unwavering quality and power of man-made intelligence advances in basic security applications [16].

Moral and protection concerns additionally present huge difficulties. The sending of simulated intelligence frequently includes the assortment and examination of enormous datasets, including delicate individual data, raising protection issues [17]. Moreover, the "discovery" nature of numerous man-made intelligence models, where dynamic cycles are not straightforward, can prompt issues with responsibility and trust, especially when man-made intelligence frameworks are utilized to settle on basic security choices [18].

The requirement for administrative systems to direct the moral utilization of man-made intelligence in network protection is another basic issue. Without clear rules, the sending of man-made intelligence could bring about conflicting security rehearses and possibly compound existing weaknesses [19], [20]. Laying out straightforward and reasonable computer based intelligence models, close by thorough testing methods, is fundamental for guaranteeing that simulated intelligence frameworks are both compelling and reliable [21], [22].

Moreover, the quick advancement of artificial intelligence innovation presents the two open doors and difficulties for online protection. While simulated intelligence gives useful assets to upgrading security, it additionally empowers new types of digital dangers, for example, simulated intelligence created phishing and robotized malware assaults [23], [24]. As simulated intelligence innovation progresses, network protection methodologies should likewise develop to address these arising dangers [25].

All in all, while simulated intelligence offers significant chances to upgrade network protection, it additionally presents huge difficulties that should be tended to. Future exploration ought to zero in on creating powerful, reasonable computer based intelligence models, tending to moral and protection concerns, and laying out far reaching administrative systems to direct the dependable utilization of simulated intelligence in network safety.

RESEARCH METHODOLOGY

This study employs a systematic literature review (SLR) as its research method to comprehensively assess the integration of Artificial Intelligence (AI) in cybersecurity. The SLR approach is chosen for its rigor in identifying, evaluating, and synthesizing existing research on AI-enhanced security measures. The method ensures a structured and transparent review process, minimizing biases and providing a reliable basis for understanding the current state of knowledge in the field.

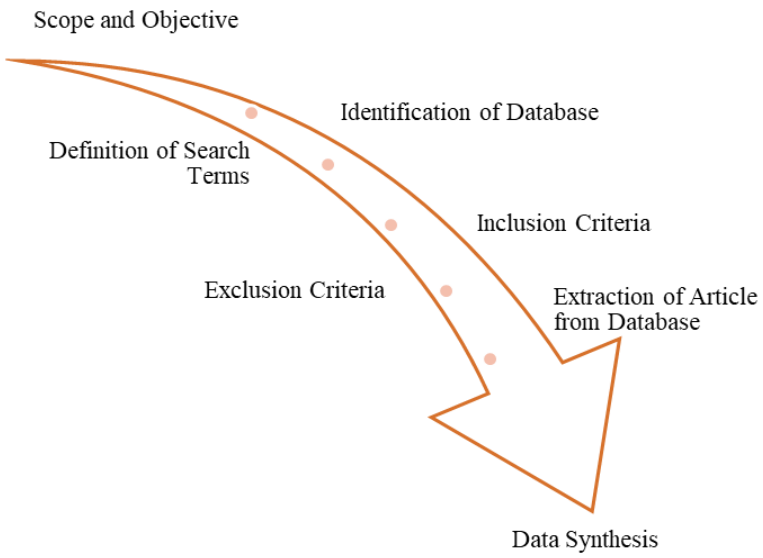

Figure 1. Systematic Literature Review Process

Figure 1 gives a visual portrayal of the deliberate writing survey process. It starts with the Recognizable proof of Information bases, displaying key sources, for example, IEEE Xplore, Science Direct, MDPI, Wiley online Library and Google Researcher, guaranteeing an exhaustive assortment of significant exploration. The following stage, Meaning of Search Terms, represents the definition of explicit catchphrases like "Man-made reasoning" and "Online protection" to refine the pursuit.

Consideration and Prohibition Standards are portrayed to channel concentrates on in light of significance and quality, zeroing in on peer-explored articles while barring non-pertinent ones.

The Extraction of Articles from Data set stage features the method involved with social affair chose reads up for survey. At long last, Information Combination includes investigating and coordinating discoveries from the extricated articles to recognize patterns, holes, and key experiences. This organized methodology guarantees a far reaching and fair survey of the writing, offering significant bits of knowledge into simulated intelligence improved network safety.

Table 1. Database Search Strategies

Database	Search Terms	Boolean Operators Used	Search Strategy
IEEE Xplore	"Artificial Intelligence" AND "Cybersecurity"	AND	Combined terms to locate articles that address both AI and cybersecurity
Science Direct	"AI in cybersecurity" AND "Threat detection"	AND	Searched for articles focusing on AI applications in threat detection
MDPI	"Machine Learning" AND "Security"	AND	Focused on studies exploring machine learning techniques in security contexts
Wiley Library	"AI-enhanced security" OR "Cyber defense"	OR	Used OR to broaden search to include articles on AI in various cybersecurity aspects

Table 1 frameworks the hunt procedures carried out across four significant data sets to guarantee thorough inclusion of applicable writing. In IEEE Explore, the hunt terms "Computerized reasoning" and "Network safety" are joined with "AND" to at the same time zero in on articles that cover the two fields. Science Direct utilizes "Artificial intelligence in network protection" and "Danger location" with "AND" to pinpoint concentrates on explicitly connected with artificial intelligence applications in danger identification.

For MDPI, "AI" and "Security" are joined with "AND" to find research that incorporates AI procedures inside security structures. Wiley Library utilizes "OR" between "Simulated intelligence upgraded security" and "Digital guard" to catch a more extensive scope of articles on artificial intelligence's part in various parts of network safety.

This essential methodology across data sets guarantees a different and exhaustive assortment of pertinent writing, supporting a hearty methodical survey.

Table 2. Criteria for Inclusion and Exclusion in Literature Review

Inclusion Criteria	Exclusion Criteria
Peer-reviewed articles	Non-peer-reviewed sources
Focus on AI applications in cybersecurity	Articles not related to AI or cybersecurity
Empirical research or theoretical contributions	Publications without substantial contributions to the field
Published within the last decade	Outdated research or studies published before 2014
Relevant to threat detection, data protection, or security frameworks	General articles not specifically addressing AI-enhanced security

Table 2 presents the models utilized for remembering and barring reads up for the writing audit. Consideration Measures underscore the significance of choosing peer-surveyed articles that emphasis on artificial intelligence applications in network safety. This incorporates both experimental examination and hypothetical commitments, guaranteeing significance and quality. The necessity for ongoing distributions, inside the last 10 years, guarantees that the survey reflects latest things and progressions.

Avoidance Models sift through non-peer-looked into sources and articles inconsequential to artificial intelligence or online protection. Concentrates on that don't contribute altogether to the comprehension of simulated intelligence improved security or are obsolete are likewise barred. This thorough methodology guarantees that the survey is far reaching, state-of-the-art, and pertinent to ebb and flow man-made intelligence upgraded network safety research.

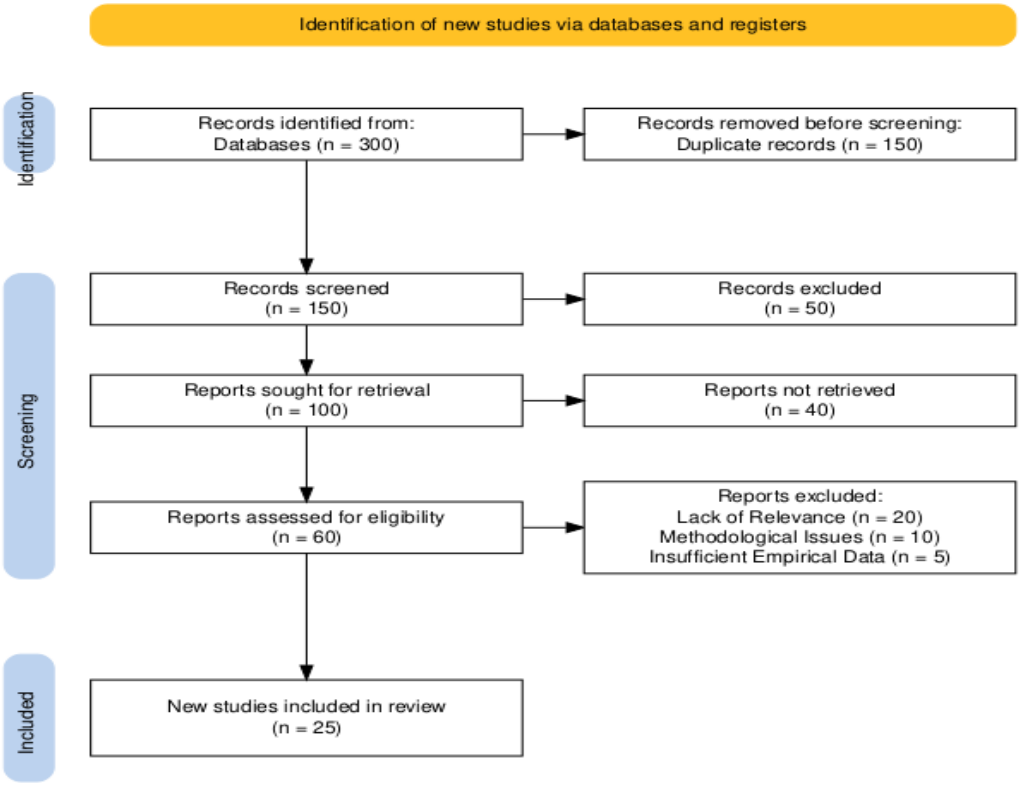

Figure 2. PRISMA Flow Diagram for Literature Review

Figure 2 presents the PRISMA flow diagram, detailing the stages of the systematic literature review process. Initially, 300 records were identified from databases, with 150 duplicate records removed before screening. This left 150 records to be screened, out of which 50 were excluded based on preliminary assessments.

Following this, 100 reports were sought for retrieval, but 40 were not retrievable. The remaining 60 reports were assessed for eligibility. Of these, 20 reports were excluded due to lack of relevance, 10 due to methodological issues, and 5 due to insufficient empirical data.

Ultimately, 25 new studies were included in the review. This structured approach ensures a thorough and systematic evaluation of the literature, focusing on relevant, high-quality research to provide comprehensive insights into AI-enhanced security.

Data Extraction

Data extraction is a vital stage in the deliberate writing survey process, zeroing in on get-together and sorting out relevant data from chose studies. This step includes carefully recording information that tends to the audit's examination questions and goals.

During information extraction, scientists catch key subtleties like review goals, systems, discoveries, and commitments connected with computer based intelligence improved security. Fundamental perspectives incorporate the artificial intelligence strategies utilized, their viability in danger identification and moderation, and any difficulties or impediments distinguished. The cycle additionally involves recording proposed progressions and systems for further developing simulated intelligence driven security arrangements.

[5] stress the significance of nitty gritty information extraction to assess computer based intelligence strategies in online protection. Gill et al. [6] feature that organized information assortment is fundamental for understanding arising simulated intelligence patterns and their effect on registering. [7] highlight that precise extraction helps in surveying man-made intelligence's suggestions in cloud security. Moreover, [9] stress the job of precise information assortment in assessing simulated intelligence improved cooperative organizations.

This thorough methodology guarantees that the extricated information is extensive, important, and instrumental for orchestrating bits of knowledge and framing dependable ends.

Data Synthesis

Data Synthesis is a crucial part of the orderly writing survey process, zeroing in on coordinating and dissecting the extricated data to give extensive experiences into artificial intelligence upgraded security. This stage includes joining information from different examinations to distinguish examples, patterns, and key discoveries.

The combination cycle starts with classifying the removed information into topical regions, like man-made intelligence methods, adequacy in danger location, and difficulties experienced. Specialists examine these subjects to decide shared characteristics and inconsistencies among the investigations, working with a more profound comprehension of man-made intelligence's effect on network protection.

[5] show that blending information from different sources helps in grasping artificial intelligence's job in identifying online protection dangers. [9] show how topical examination uncovers the viability of man-made intelligence in cooperative organization security. [7] feature the significance of union in recognizing holes and future exploration bearings. Gill et al. [6] stress that orchestrating discoveries guarantees an exhaustive outline of arising artificial intelligence patterns in figuring.

This organized methodology considers a cognizant and nuanced examination of the writing, giving important experiences into the present status and future bearings of computer based intelligence upgraded security.

RESULT AND DISCUSSION

Result

The results section presents a detailed analysis of the findings from the systematic literature review, highlighting key insights into the effectiveness, challenges, and advancements in AI-enhanced security. This section synthesizes data from various sources to provide a comprehensive overview of current trends and gaps in the field.

RQ1: How effective is AI in detecting and mitigating cyber threats across different domains, including critical infrastructure and financial systems?

Table 3. Effectiveness of AI in Detecting and Mitigating Cyber Threats

Domain	AI Techniques Used	Effectiveness	Key Findings	Citation
Critical Infrastructure	Machine Learning, Neural Networks	High, especially in anomaly detection	AI significantly improves threat detection accuracy and response times	[5]
Financial Systems	Deep Learning, Supervised Learning	Very effective in fraud detection and prevention	AI enhances the ability to detect and prevent fraudulent transactions	[6]
Cloud Computing	Natural Language Processing, ML	Effective in identifying and mitigating threats	AI provides robust defenses against various cloud-based attacks	[7]
Internet of Things	Reinforcement Learning, Anomaly Detection	Effective but with challenges in scalability	AI can effectively manage and respond to IoT security threats	[8]

Table 3 sums up the viability of computer based intelligence in distinguishing and alleviating digital dangers across different areas. In basic foundation, computer based intelligence methods, for example, AI and brain networks are profoundly powerful, especially in irregularity location. These techniques fundamentally upgrade danger location exactness and reaction times, showing their worth in safeguarding fundamental frameworks [5].

In monetary frameworks, profound learning and directed learning strategies succeed in recognizing and forestalling fake exercises. The utilization of simulated intelligence in this space has demonstrated to be extremely powerful, working on both recognition and counteraction of monetary extortion [6].

For distributed computing, man-made intelligence strategies including regular language handling and AI offer hearty guards against different assaults. These procedures help in recognizing and relieving dangers inside cloud conditions successfully [7].

In the internet of Things (IoT), support learning and oddity identification methods show guarantee in overseeing and answering security dangers, in spite of the fact that versatility stays a test. Simulated intelligence successfully addresses IoT security issues yet requires progressing upgrades to deal with the developing number of associated gadgets [8].

RQ2: What are the key challenges and limitations associated with integrating AI into existing security frameworks, particularly concerning ethical and privacy issues?

Table 4. Challenges and Limitations of Integrating AI into Security Frameworks

Challenge/ Limitation	Description	Impact on Security Frameworks	Citation
Ethical Concerns	Issues related to bias, fairness, and transparency in AI algorithms	Can lead to unfair or discriminatory practices	[9]
Privacy Issues	Risks associated with data collection and usage	Potential for breaches of user privacy and data misuse	[10]
Integration Complexity	Difficulties in integrating AI with existing systems	High costs and technical challenges in implementation	[11]
False Positives/Negatives	AI systems may produce incorrect threat assessments	Can result in missed threats or false alarms	[12]
Data Dependency	AI effectiveness relies heavily on data quality and quantity	Poor data can degrade AI performance	[13]
Regulatory Compliance	Challenges in adhering to legal and regulatory standards	Potential for legal issues and non-compliance	[14]

Table 4 layouts key difficulties and limits related with incorporating artificial intelligence into existing security structures, zeroing in on moral and protection issues. Moral worries are huge, as predispositions in artificial intelligence calculations can prompt unjustifiable or unfair results, affecting the reasonableness of safety efforts [9]. Security issues emerge from the broad information assortment expected by simulated intelligence frameworks, which can bring about breaks of client protection and abuse of individual data [10].

Joining intricacy represents another test, as integrating artificial intelligence into existing security frameworks frequently includes significant expenses and specialized challenges, possibly postponing or upsetting execution [11]. Also, artificial intelligence frameworks can produce misleading up-sides and negatives, prompting missed dangers or superfluous cautions, which sabotages the unwavering quality of safety efforts [12].

Information reliance features that simulated intelligence's presentation is intensely dependent on the quality and amount of information. Lacking or low quality information can altogether debase man-made intelligence viability [13]. In conclusion, administrative consistence is significant as neglecting to stick to legitimate and administrative principles can bring about lawful entanglements and rebelliousness issues [14].

Addressing these difficulties is fundamental to guarantee that simulated intelligence mix improves security structures without compromising moral principles or protection.RQ3: What potential advancements and strategies can enhance AI-driven security solutions to reduce vulnerabilities and improve response times?

Table 5. Advancements and Strategies for Enhancing AI-Driven Security Solutions

Advancement/ Strategy	Description	Potential Benefits	Citation
Advanced Machine Learning Algorithms	Development of more sophisticated algorithms for threat detection	Improved accuracy and efficiency in identifying threats	[15]
Real-time Data Processing	Implementing faster data processing techniques	Reduced response times and quicker threat mitigation	[16]
Integration with Blockchain	Combining AI with blockchain technology for secure transactions	Enhanced security and transparency in data handling	[17]
Enhanced Privacy-preserving Techniques	Employing techniques like federated learning to protect user data	Improved privacy while maintaining AI effectiveness	[18]
Automated Threat Intelligence	Using AI to automatically gather and analyze threat intelligence	Faster identification of emerging threats	[19]
Adaptive Security Frameworks	Developing frameworks that adapt to evolving threats	Continuous improvement and adaptation to new attack methods	[20]

Table 5 presents expected headways and techniques for upgrading artificial intelligence driven security arrangements. High level AI calculations are essential for further developing danger recognition exactness and effectiveness. By growing more modern calculations, simulated intelligence frameworks can more readily recognize and answer complex dangers [15].

Constant information handling is one more key headway, empowering quicker examination of approaching information. This diminishes reaction times and improves the capacity to alleviate dangers quickly, which is basic in unique security conditions [16].

The reconciliation of simulated intelligence with blockchain innovation offers a promising technique for getting exchanges and further developing information straightforwardness. This blend can essentially upgrade safety efforts and dependability in information taking care of cycles [17].

Upgraded security safeguarding procedures, like combined learning, permit computer based intelligence frameworks to work without compromising client protection. This approach safeguards touchy information while keeping up with the viability of man-made intelligence applications [18].

Robotized danger insight utilizes computer based intelligence to quickly assemble and break down data on potential dangers more. This empowers speedier distinguishing proof of arising dangers, giving a proactive way to deal with security [19].

Finally, versatile security systems that develop with arising dangers guarantee that artificial intelligence driven arrangements consistently improve and adjust to new go after techniques. This procedure keeps up with strong security protections notwithstanding always developing digital dangers [20].

Executing these headways and procedures can essentially upgrade computer based intelligence driven security arrangements, lessening weaknesses and further developing by and large reaction times.

Discussion

The integration of Artificial Intelligence (AI) into cybersecurity represents has conveyed critical steps in upgrading intimidation location and moderation. Nonetheless, it additionally presents difficulties that require further investigation and refinement. This conversation digs into

the adequacy, difficulties, and possible headways in simulated intelligence improved security arrangements in view of the discoveries from this survey.

Artificial intelligence has demonstrated to be profoundly compelling across different areas. In basic foundation, simulated intelligence strategies, for example, AI and brain networks have shown significant enhancements in irregularity location and danger reaction times [5]. For monetary frameworks, profound learning models succeed in distinguishing and forestalling fake exercises, showing man-made intelligence's capacity to deal with complicated and high-stakes conditions [6]. Essentially, in distributed computing, artificial intelligence advances, including normal language handling and AI, offer strong protections against a scope of assaults [7]. The Web of Things (IoT) benefits from support learning and inconsistency location, in spite of the fact that versatility stays a test [8].

In spite of its adequacy, the coordination of man-made intelligence into security systems is full of difficulties. Moral worries are huge, as predispositions in computer based intelligence calculations can bring about out of line or biased rehearses [9]. Security issues additionally emerge because of broad information assortment expected by computer based intelligence frameworks, which can prompt likely breaks of client protection and abuse of individual information [10]. Mix intricacy further confounds matters, with significant expenses and specialized troubles in carrying out simulated intelligence inside existing frameworks [11]. Also, computer based intelligence frameworks can create bogus up-sides and negatives, influencing the unwavering quality of danger identification [12]. Information reliance is one more basic issue, as the presentation of simulated intelligence is vigorously dependent on the quality and amount of information accessible [13]. In conclusion, sticking to administrative consistence can be testing, possibly bringing about lawful confusions [14].

To address these difficulties and improve computer based intelligence driven security arrangements, a few progressions and systems are suggested. The advancement of cutting edge AI calculations can further develop danger location exactness and productivity, considering more exact ID of dangers [15]. Continuous information handling procedures are fundamental for decreasing reaction times and rapidly relieving dangers [16]. Incorporating simulated intelligence with blockchain innovation can get exchanges and further develop information straightforwardness, improving generally security [17]. Security saving procedures, for example, united learning, offer a method for keeping up with computer based intelligence viability while safeguarding client information [18]. Robotized danger insight empowers quicker distinguishing proof of arising dangers, giving a proactive way to deal with security [19]. At long last, versatile security structures that advance with new dangers guarantee that simulated intelligence arrangements stay viable against developing assault strategies [20].

CONCLUSION

The integration of Artificial Intelligence (AI) into cybersecurity represents an extraordinary change by the way we recognize, answer, and oversee digital dangers. This survey features the significant effect simulated intelligence has had across different areas, including basic framework, monetary frameworks, distributed computing, and the Web of Things (IoT). Man-made intelligence methods, for example, AI, profound learning, and oddity location, have demonstrated exceptionally compelling in upgrading danger discovery and reaction times, offering further developed security against an extensive variety of digital dangers.

In any case, the reception of simulated intelligence in security systems isn't without its difficulties. Moral worries about algorithmic predisposition, security issues connected with

information assortment, and joining intricacies present huge deterrents. These difficulties can sabotage the viability of artificial intelligence frameworks and possibly lead to unjustifiable practices, information breaks, and execution hardships. Moreover, the dependence on top notch information and the gamble of bogus up-sides or negatives can influence the unwavering quality of simulated intelligence driven security arrangements.

To address these difficulties and further improve simulated intelligence driven security arrangements, a few headways are essential. Growing more complex AI calculations can work on the exactness and productivity of danger location. Continuous information handling strategies are fundamental for decreasing reaction times and rapidly alleviating dangers. Coordinating man-made intelligence with innovations like blockchain can improve information security and straightforwardness. Utilizing security safeguarding strategies, like unified learning, guarantees that client information stays safeguarded while keeping up with computer based intelligence adequacy. Robotized danger knowledge and versatile security systems are essential for remaining in front of arising dangers and developing assault techniques.

In synopsis, while simulated intelligence has taken critical steps in the field of online protection, progressing endeavors to refine and upgrade these advances are fundamental. By tending to existing difficulties and utilizing new headways, artificial intelligence driven security arrangements can keep on advancing, offering more powerful and responsive safeguards against the steadily changing scene of digital dangers.

To propel the field of artificial intelligence upgraded network safety, a few regions warrant further investigation. To begin with, there is a requirement for growing more powerful and straightforward artificial intelligence calculations to address moral worries and limit predispositions in danger recognition and reaction. Examination ought to zero in on making models that are both powerful and fair across different settings. Second, improving security saving strategies, for example, combined learning, will be pivotal in safeguarding client information while utilizing artificial intelligence abilities. Future examinations ought to investigate imaginative strategies for adjusting protection and execution. Third, coordinating computer based intelligence with arising advances, as blockchain, could offer new roads for further developing information security and straightforwardness. Also, continuous exploration ought to examine versatile security structures that can powerfully develop with new dangers. By tending to these areas, future examination can add to more viable, moral, and versatile man-made intelligence driven network safety arrangements, at last reinforcing safeguards against an extensive variety of digital dangers.

AUTHORS' CONTRIBUTION

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.
Author 2: Conceptualization; Data curation; In-vestigation.
Author 3: Data curation; Investigation.
Author 4: Formal analysis; Methodology; Writing - original draft.

REFERENCES

A. Abidullah, K. R. Rahmani, W. M. Wadeed, and M. Hakimi, "Data Transfer Security in IoT Communication Based on Attribute-Based Cryptography," *Int. J. Software Eng. Comput. Sci. (IJSECS)*, vol. 4, no. 2, pp. 553–565, 2024. [Online]. Available: https://doi.org/10.35870/ijsecs.v4i2.2887

A. K. R. ReddyAyyadapu, "Optimizing incident response in cloud security with AI and big data integration," *Chelonian Research Foundation*, vol. 18, no. 2, pp. 2212-2225, 2023. [Online]. Available: https://www.acgpublishing.com/index.php/CCB/article/view/195

A. Luqman, R. Mahesh, and A. Chattopadhyay, "Privacy and security implications of cloud-based AI services: A survey," *arXiv preprint arXiv:2402.00896*, 2024. Available: https://doi.org/10.48550/arXiv.2402.00896

A. Nayak, A. Patnaik, I. Satpathy, and B. C. M. Patnaik, "Data storage and transmission security in the cloud: The artificial intelligence (AI) edge," in *Improving Security, Privacy, and Trust in Cloud Computing*, A. O. Montoya Benitez et al., Eds., IGI Global, 2024, pp. 194-212, [Online]. Available: https://www.igi-global.com/chapter/data-storage-and-transmission-security-in-the-cloud/338355

A. R. P. Reddy and A. K. R. Ayyadapu, "Securing multi-cloud environments with AI and machine learning techniques," *Chelonian Research Foundation*, vol. 16, no. 2, pp. 01-12, 2021. [Online]. Available: https://www.acgpublishing.com/index.php/CCB/article/view/296

B. J. Ospina Cifuentes et al., "Analysis of the use of artificial intelligence in software-defined intelligent networks: A survey," *Technologies*, vol. 12, no. 7, p. 99, Jul. 2024, https://doi.org/10.3390/technologies12070099.

C. P. Filho et al., "A systematic literature review on distributed machine learning in edge computing," *Sensors*, vol. 22, no. 7, p. 2665, Apr. 2022, https://doi.org/10.3390/s22072665.

D. Ressi, R. Romanello, C. Piazza, and S. Rossi, "AI-enhanced blockchain technology: A review of advancements and opportunities," *Journal of Network and Computer Applications*, p. 103858, 2024 https://doi.org/10.1016/j.jnca.2024.103858.

D. Stutz et al., "Enhancing security in cloud computing using artificial intelligence (AI)," in *Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection*, 2024, pp. 179-220, https://doi.org/10.1002/9781394196470.ch11.

H. Gu, L. Zhao, Z. Han, G. Zheng, and S. Song, "AI-enhanced cloud-edge-terminal collaborative network: Survey, applications, and future directions," *IEEE Communications Surveys & Tutorials*, 2023, https://doi.org/10.1109/COMST.2023.3338153.

Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis Campbell Systematic Reviews, 18, e1230. https://doi.org/10.1002/cl2.1230

I. Jada and T. O. Mayayise, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," *Data and Information Management*, p. 100063, 2023, https://doi.org/10.1016/j.dim.2023.100063.

J. L. Kreinbrink, "Analysis of artificial intelligence (AI) enhanced technologies in support of cyber defense: Advantages, challenges, and considerations for future deployment," *Master's thesis*, Utica College, 2019. [Online]. Available: https://www.proquest.com/openview/2ca10115b5be484fc619b2534e01ace0/1?pq-origsite=gscholar&cbl=18750&diss=y

K. Vignesh Saravanan, P. Jothi Thilaga, S. Kavipriya, and K. Vijayalakshmi, "Data protection and security enhancement in cyber-physical systems using AI and blockchain," in *AI Models for Blockchain-Based Intelligent Networks in IoT Systems: Concepts, Methodologies, Tools, and Applications*, G. Ludke et al., Eds., Springer International Publishing, 2023, pp. 285-325, https://doi.org/10.1007/978-3-031-31952-5_13.

L. Alevizos and M. Dekker, "Towards an AI-enhanced cyber threat intelligence processing pipeline," *Electronics*, vol. 13, no. 11, p. 2021, Nov. 2024, https://doi.org/10.3390/electronics13112021.

M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N. Aziz, L. F. Capretz, and S. J. Abdulkadir, "Detecting cybersecurity attacks in Internet of Things using artificial intelligence methods: A systematic literature review," *Electronics*, vol. 11, no. 2, p. 198, Feb. 2022, https://doi.org/10.3390/electronics11020198.

M. Abouelyazid and C. Xiang, "Architectures for AI integration in next-generation cloud infrastructure, development, security, and management," *International Journal of Information and Cybersecurity*, vol. 3, no. 1, pp. 1-19, 2019. [Online]. Available: https://publications.dlpress.org/index.php/ijic/article/view/92

M. Golec, S. S. Ponugoti, and S. S. Gill, "Enhancing data security for cloud service providers using AI," in *Applications of AI for Interdisciplinary Research*, C. P. Filho et al., Eds., CRC Press, 2024, pp. 187-204, https://doi.org/10.1515/9783110732573.

M. R. Faraji, F. Shikder, M. H. Hasan, M. M. Islam, and U. K. Akter, "Examining the role of artificial intelligence in cyber security (CS): A systematic review for preventing prospective solutions in financial transactions," *International Journal*, vol. 5, no. 10, pp. 4766-4782, 2024, https://doi.org/10.61707/7rfyma13.

M. Hakimi, G. A. Amiri, S. Jalalzai, F. A. Darmel, and Z. Ezam, "Exploring the Integration of AI and Cloud Computing: Navigating Opportunities and Overcoming Challenges," *TIERS*, vol. 5, no. 1, pp. 57-69, Jun. 2024. [Online]. Available: https://journal.undiknas.ac.id/index.php/tiers/article/view/5496

M. R. Roshanaei, M. R. Khan, and N. N. Sylvester, "Enhancing cybersecurity through AI and ML: Strategies, challenges, and future directions," *Journal of Information Security*, vol. 15, no. 3, pp. 320-339, 2024, https://doi.org/10.4236/jis.2024.153019.

M. E. Ebadi, W. Yu, K. R. Rahmani, and M. Hakimi, "Resource Allocation in the Cloud Environment with Supervised Machine Learning for Effective Data Transmission," *J. Comput. Sci. Technol. Stud.*, vol. 6, no. 3, pp. 22–34, 2024. [Online]. Available: https://doi.org/10.32996/jcsts.2024.6.3.3

P. Thapa and T. Arjunan, "AI-enhanced cybersecurity: Machine learning for anomaly detection in cloud computing," *Quarterly Journal of Emerging Technologies and Innovations*, vol. 9, no. 1, pp. 25–37, 2024. [Online]. Available: https://vectoral.org/index.php/QJETI/article/view/64

R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, vol. 97, p. 101804, 2023, https://doi.org/10.1016/j.inffus.2023.101804.

S. N. Mohanty, S. Potluri, V. B. Prakash, B. Srinath, and B. Manjunath, "Cloud security concepts, threats and solutions: Artificial intelligence based approach," in *Cloud Security: Techniques and Applications*, vol. 1, p. 1, 2021, https://doi.org/10.1515/9783110732573.

S. S. Gill, M. Xu, C. Ottaviani, P. Patros, R. Bahsoon, A. Shaghaghi, and S. Uhlig, "AI for next generation computing: Emerging trends and future directions," *Internet of Things*, vol. 19, p. 100514, 2022, https://doi.org/10.1016/j.iot.2022.100514.

T. de Oliveira Ribeiro et al., "Virtual reality solutions employing artificial intelligence methods: A systematic literature review," *ACM Computing Surveys*, vol. 55, no. 10, pp. 1-29, 2023, https://doi.org/10.1145/3565020

T. K. Vashishth, V. Sharma, K. K. Sharma, B. Kumar, S. Chaudhary, and R. Panwar, "Enhancing cloud security: The role of artificial intelligence and machine learning," in *Improving*

Security, Privacy, and Trust in Cloud Computing, IGI Global, 2024, pp. 85-112, [Online]. Available: https://www.igi-global.com/chapter/enhancing-cloud-security/338350