IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 1, January 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 1, January 2024 ||

| DOI:10.15680/IJIRSET.2024.1301007 |

Enhancing Cybersecurity and Privacy using Artificial Intelligence: Trends and Future Directions of Research

Dhruvitkumar V. Talati

AAMC, Washington, D.C. , USA

ORCID ID :0009-0005-2916-4054

ABSTRACT: The speed with which cyber threats are evolving is calling for fresh approaches to enhance cybersecurity and protection of privacy. Artificial Intelligence (AI) is proving to be a revolutionary factor in enhancing cybersecurity, providing powerful capabilities for intrusion detection, malware detection, and privacy protection. This article outlines an in-depth review of the use of AI in cybersecurity with particular reference to future directions and trends in research. Applying the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) format, we discuss more than 9,350 papers from the years 2004 to 2023. The research discerns 14 wide-ranging categories, such as AI-driven intrusion detection, privacy-preserving federated learning, malware classification via deep learning, and blockchain-assisted integration of cybersecurity. AI makes cybersecurity more effective despite the computationally extensive resource requirements, adversarial attack vulnerabilities, and ethical issues. This article prioritizes the use of further research in secure AI, normative AI-based practices, and regulation to further support privacy protection. Furthermore, new frontiers of quantum machine learning, AI explainability, and deepfake countermeasures are explored, potentially as routes for future security growth.

KEYWORDS: Artificial Intelligence, Cloud Computing, cybersecurity, PRISMA, Quantum Machine Learning

I. INTRODUCTION

As threats in the cyberspace evolve, classical security measures fall behind. AI has brought innovations that are paradigm-shifting in making security systems more effective at sensing, predicting, and defending against cyber attacks autonomously. But although promising, AI-powered cybersecurity is bedeviled with a number of challenges, among them adversarial vulnerabilities and ethics. This research seeks to aggregate the extensive literature on AI-powered cybersecurity, demarcating emergent trends and research areas to be explored.

This study systematically reviewed more than 9,350 articles from 2004 to 2023 using the PRISMA protocol. BERTopic modeling was applied for topic classification and verification of top topics in AI-based cybersecurity. Topics were classified and examined using algorithmic and expert-based assessments for semantic consistency and real-world usability. Four key patterns and contributions were identified from the literature through a multi-faceted analysis.

First, AI applications have expanded significantly in cybersecurity, manifesting in areas like intrusion detection, malware analysis, and privacy-preserving technologies. The research attributes this surge to the growing sophistication of cyber threats and the rising need for more robust security solutions (Achuthan et al., 2024) (Ökdem & Okdem, 2024).

Second, the paper highlights recent AI advancements that have unlocked new frontiers in cybersecurity, including federated learning for privacy protection, blockchain-based security, and XAI for improving AI accountability. (Salem et al., 2024)

Third, the paper examines the limitations of AI-powered cybersecurity, such as the need for secure and ethical AI practices, concerns over adversarial attacks, and the challenge of preserving human oversight.
And finally, the paper explores future directions for AI-cybersecurity research, including the potential of quantum machine learning, deepfake detection, and other innovations to tackle emerging cyber threats.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 1, January 2024 ||

| DOI:10.15680/IJIRSET.2024.1301007 |

II. METHODS

2.1 PRISMA Framework

The PRISMA framework guided the analysis in this study according to guidelines by Page et al. (2021). The PRISMA framework adopts a formalized five-step approach to formulating research questions, developing detailed search strategies including databases, search terms, and inclusion and exclusion criteria, and conducting searches before assessing the findings. This systematic process simplifies the process of choosing and filtering studies to include in systematic reviews or meta-analyses. Identification phase started with the search of the Dimensions database on February 12, 2024, between the years 2004-2023.

The Dimensions database was used because it is extensively indexed for journals compared to Scopus (48.1%) and Web of Science (82.2%). The database uses the Australian and New Zealand Standard Research Classification (ANZSRC) structure, classifying research into 22 broad Fields of Research (FoR) divisions. From the ANZSRC structure, 11,733 publications were extracted in artificial intelligence (ANZSRC 4602), machine learning (ANZSRC 4611), and cybersecurity and privacy (ANZSRC 4604). Following screening on the basis of non-English publication exclusion and absence of author details or abstracts, 9,352 publications were left to be processed.

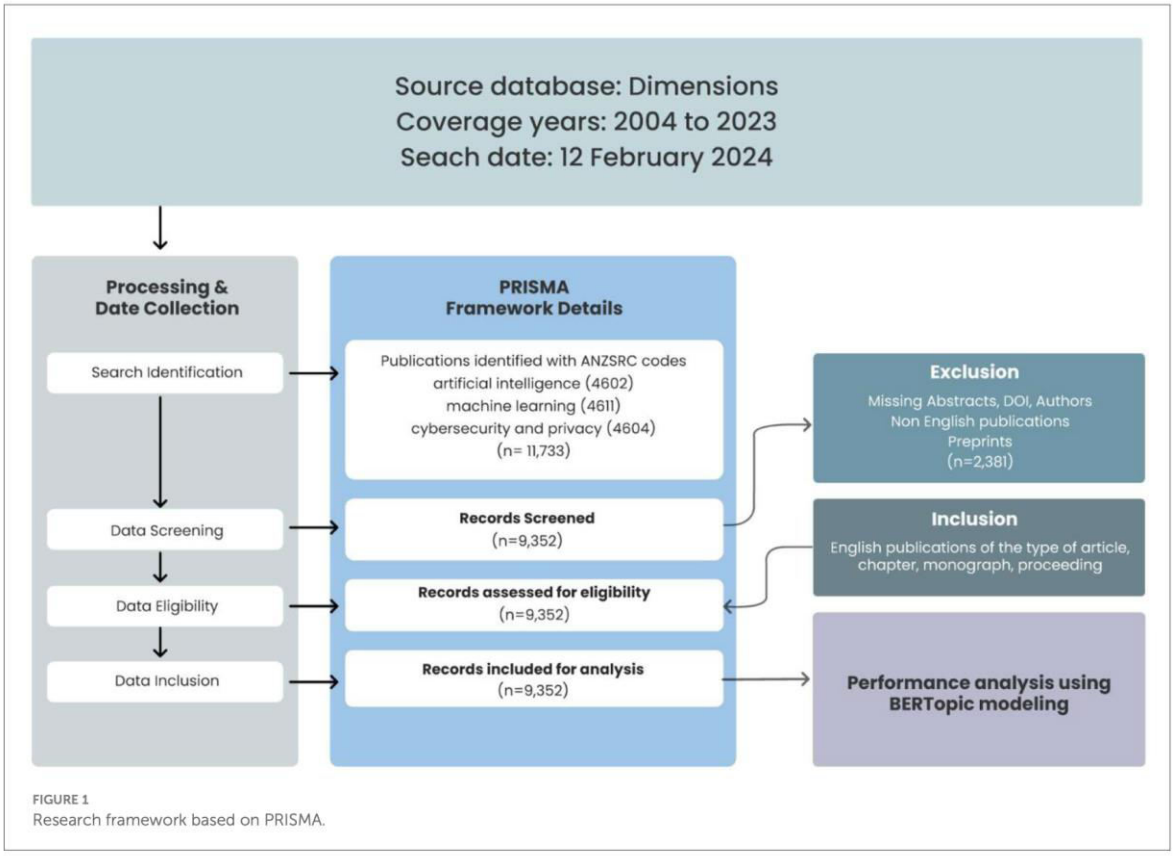

FIGURE 1
Research framework based on PRISMA.

2.2 BERTopic Modeling

Topic modeling utilizes different methodologies, including Non-Negative Matrix Factorization (NMF), Latent Dirichlet Allocation (LDA), Probabilistic Latent Semantic Analysis (PLSA), and To2Vec. Though effective as they are, these do not necessarily pick up semantic word relationships and perform poorly with short-text data. Previous topic models, like the Bag-of-Words (BoW) model, focus on word frequency but are devoid of contextual depth. BERTopic, on the other hand, is based on embeddings that map documents to a lower-dimensional space, providing contextual depth.

BERTopic, based on Google's bidirectional language model BERT, analyzes text contextually to improve topic clustering precision. Modeling starts with embedding vectorization, where input text is transformed into numerical

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 1, January 2024 ||

| DOI:10.15680/IJIRSET.2024.1301007 |

representations. Embeddings are then reduced in dimensionality by Unified Manifold Approximation and Projection (UMAP), which clusters similar points into separate topic clusters. Hierarchical Density-Based Spatial Clustering of Applications with Noise (HDBSCAN) subsequently identifies clusters by clustering densely packed data points without outliers.

To map the clusters, the model employs class-based Term Frequency-Inverse Document Frequency (c-TF-IDF), which identifies influential words or phrases for each cluster. For the current analysis, the model utilized the "all-MiniLM-L6-v2" text representation that is fine-tuned for clustering and English semantic search. This improved TF-IDF annotates documents with topics using weighted term frequency, providing accurate topic relevance.

UMAP algorithm was seeded with default settings, e.g., document-topic association probability estimation. The topics were fixed by qualitative and quantitative testing on intertopic distance and coherence measures. Testing over topic numbers 4 to 20 ensured proper separation of topics. Angular similarity of vectors was tested using the "cosine" measure with a random state maintained at 100 for reproducibility. In addition, the number of nearest neighbors parameter (n_neighbors) was set at 15 to achieve a trade-off between local clustering subtleties and global topic structure. This value yielded 14 top-level topics, of which 20 representative publications were identified for each.

For better accuracy and interpretability, both the topics and their representative publications underwent manual review. Three domain experts assessed the cohesiveness and salience of each topic based on probability values, citation frequencies, and full-text evaluations. This review helped to verify that the result of unsupervised topic modeling was accurate and of practical applicability, allowing for identification of dominant themes. Subsequent to this process, the initial 14 topics were maintained, and an in-depth analysis was performed on each topic's top three representative publications.

III. RESULTS AND DISCUSSION

3.1 Topic Distribution (RQ1)

Figure 2 depicts the prevalence of significant research topics in the examined publications, reflecting the contributions of AI towards cybersecurity and privacy. The primary concern is intrusion detection, with about 13% of all publications focused on this topic. This is evidence of extensive interest in the application of AI in detecting and responding to unauthorized access to systems. The second most studied topic is malware classification, particularly using machine learning (ML) methods, due to the growing sophistication of malware and the necessity for sophisticated classification models.

3.2 Research Topic Evolution (RQ1)

Figure 3 shows the trend of cybersecurity research topics from 2004 to 2023. AI-based intrusion detection research has increased remarkably, particularly since mid-2010s, indicating the focus of the field on defense against unauthorized access attacks. Similarly, machine learning use in malware classification has risen step by step, which emphasizes novel malware patterns and the need for adaptive detection approaches.

Federated learning for privacy protection has also received considerable interest over the past decade, consistent with the growth of distributed data systems. Additionally, support vector machines (SVM) in intrusion detection and AI usage in IoT system protection are also seeing growing interest, and this is a balanced issue for both traditional network security and new IoT threats.

Other specialized fields like UAV security and prevention of DDoS attacks with the aid of AI have emerged since 2015, probably because they are gaining popularity in their applications to critical infrastructure.

Even though deep reinforcement learning and cryptography using ML are on the rise, they are less prominent than fundamentals like intrusion detection. New research niches, such as adversarial ML, cybersecurity ontologies, and blockchain for decentralized security, are relatively low-volume publication areas with increasing interest. Overall, although intrusion detection and malware classification are widespread, the cybersecurity research field is becoming increasingly diversified, with new fields being investigated increasingly. ####

3.3 Global Research Contributions (RQ2) Figure 4 shows the worldwide scope of cybersecurity research, classifying contribution by country. The United States and United Kingdom are at the forefront of research, emphasizing intrusion

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 1, January 2024 ||

| DOI:10.15680/IJIRSET.2024.1301007 |

detection, malware categorization, and system vulnerabilities. China, although included under Global South, has become a player in AI-based cybersecurity, specifically intrusion detection using deep neural networks (DNNs) and federated learning to ensure privacy.
India also makes considerable research contributions in a couple of areas of cybersecurity, indicating an approximately equal level of interest.
Australia and Canada have minimal contributions, although not as much as China, the US, or the UK.

Focused research in one area of cybersecurity exists among South Korea, Italy, Saudi Arabia, and Japan, indicating niche concentration or new interest. Blockchain-focused security and privacy research seems to be quite less prominent in contrast to mainstream AI-focused cybersecurity application. Scope of research efforts dissemination indicates global cybersecurity prioritization as well as differences in specialization levels across countries.

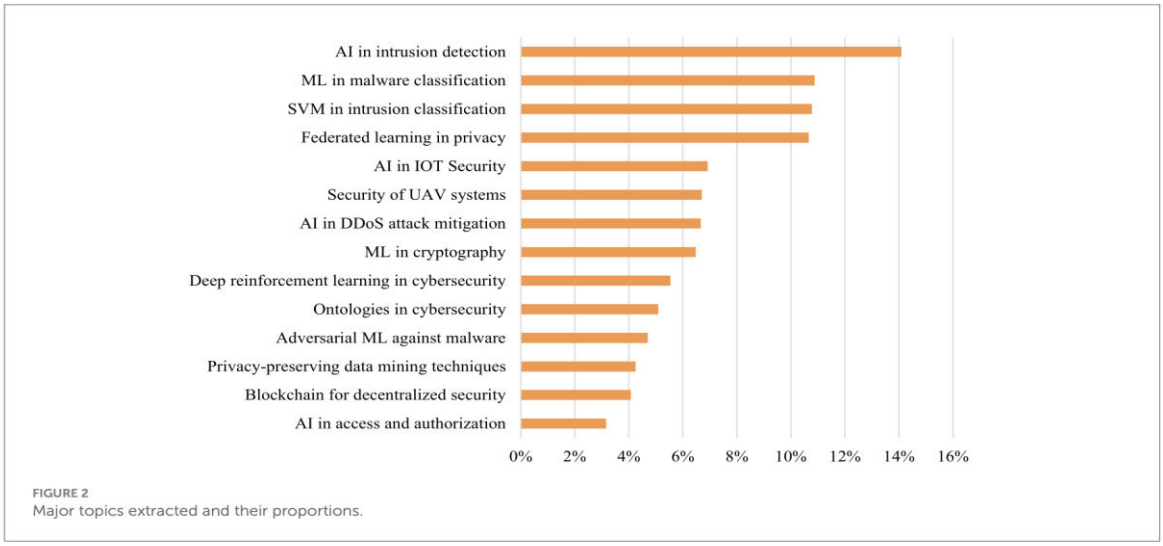

FIGURE 2
Major topics extracted and their proportions.

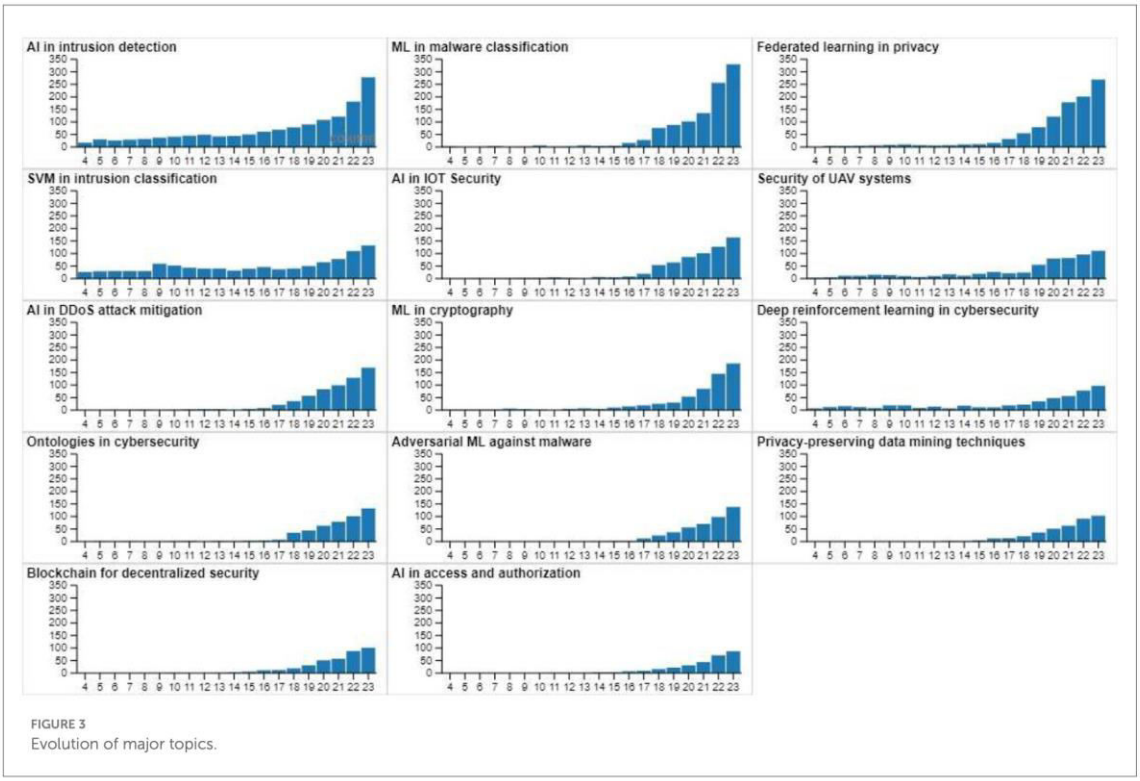

FIGURE 3
Evolution of major topics.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 1, January 2024 ||

| DOI:10.15680/IJIRSET.2024.1301007 |

3.4 Interrelation of Cybersecurity Topics (RQ2)

Similarity comparison indicates that there are very strong interrelations between some areas of cybersecurity. As an example, intrusion detection with deep neural networks (DNNs) is very highly related to machine learning classifiers such as support vector machines (SVMs), showing the focal dominance of ML in contemporary cybersecurity. Blockchain use towards security, on the other hand, is relatively much more specialized and hence potentially distinctive data protection needs beyond regular cybersecurity.
Privacy-preserving algorithms and access controls exhibit moderate correlation, i.e., mutual interest in the protection of user information and secure authentication procedures. Recognition of these relations is necessary to plan future research investment and cybersecurity strategy formulation.

3.5 Main Research Issues (RQ3)
The following outline major research developments in several areas of cybersecurity through BERTopic modeling.

3.5.1 AI for Intrusion Detection
The argument for the best AI-driven intrusion detection approach persists. Yin et al. (2017) believe in the use of recurrent neural networks (RNNs) as they perform better in binary and multi-class classification tasks. Ding and Zhai (2018) propose that CNNs perform better in general compared to conventional ML approaches such as random forests and SVMs for dealing with intricate cyber traffic data. Kumar et al. (2022) propose a hybrid method of using deep learning along with nature-inspired algorithms such as ant colony optimization (ACO) to enhance intrusion detection in cloud systems. While deep learning models yield high accuracy, problems such as the need for computational resources and adaptability to evolving threats still exist.

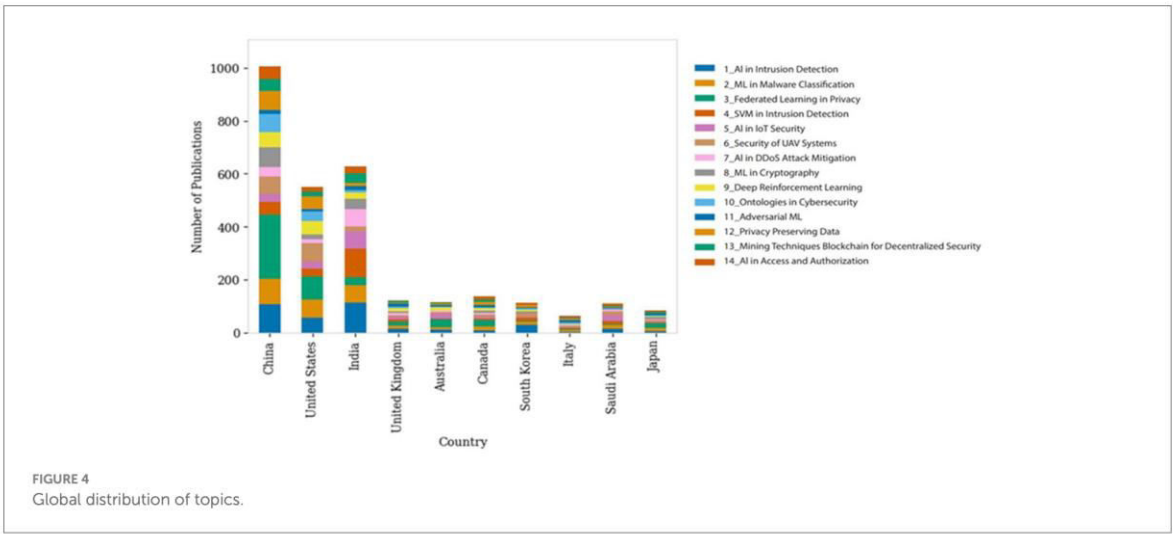

FIGURE 4
Global distribution of topics.

3.5.2 Machine Learning in Malware Classification
Jung et al. (2018) suggest a byte-level deep learning model for malware classification with extremely high accuracy.
Snow et al. (2020) follow a different approach, suggesting an end-to-end deep learning model based on the use of multiple neural networks to enhance efficiency. Gayathri and Vijaya (2021) concentrate on CNN-based models for malware family classification, asserting that they are capable of effectively detecting polymorphic malware variants. However, although CNN and byte-level models enhance classification performance, their novelty in learning to fit new malware types is a challenge since it involves continuous model tuning and refreshing.

3.5.3 Federated Learning for Privacy Protection Loopholes for privacy in deep learning models have evoked new safeguards. Wei et al. (2020) suggest an adversarially-robust self-healing model, while Fisichella et al. (2022) suggest partially federated learning for greater privacy control. Fontenla-Romero et al. (2023) contend federated learning to be vulnerable to privacy leakages and recommend the application of homomorphic encryption as a countermeasure. Federated learning remains hampered by computational efficiency and privacy assurance with large-scale deployment.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 1, January 2024 ||

| DOI:10.15680/IJIRSET.2024.1301007 |

3.5.4 AI for IoT Security

With IoT devices more common, AI-based security products are the need of the hour. Ullah and Mahmoud (2021) construct an anomaly-based IDS with CNNs having better classification accuracy. Their follow-up study (2022) incorporates RNNs, with better performance in IoT security detection. Debnath et al. (2023) suggest a seven-layer IoT security architecture based on ML techniques. But with such high complexity, it is questionable whether they can be implemented on resource-limited IoT devices.

3.5.5 Blockchain for Decentralized Security

Blockchain integration in cybersecurity is ongoing. Gul et al. (2020) examine its use in healthcare security, while Haddad et al. (2021) integrate blockchain with ML for secure information exchange. Aggarwal et al. (2022) present DeMed, a decentralized blockchain-based platform for secure medical image analysis. Blockchain adds security, but scalability, latency, and computational overhead are still major impediments to mass adoption.

3.5.6 Adversarial Machine Learning for Malware Detection

The new threats have prompted research into adversarial machine learning (AML) methods. Phan et al. (2022) present reinforcement learning models to generate adversarial malware samples. Arif et al. (2023) present IF-MalEvade, a GAN-DRL-based hybrid framework for malware detector evasion. These adversarial models, though powerful, need to be constantly updated and use a lot of computational power, which creates practical issues to their real-time use.

IV. IMPLICATIONS AND FUTURE RESEARCH DIRECTIONS (RQ4)

More deployment of AI in cybersecurity has brought numerous various methodologies in responding to novel kinds of cyber attacks. Knowledge of such developments is important for decision-makers as well as professionals tasked with setting the rate of cybersecurity development.

It is important that AI models process large and complex data streams effectively (Khamis, 2024). Models need to be periodically retrained to counter adversarial attacks and ensure detection effectiveness. Malware detection must employ new approaches such as byte-level deep learning and CNN-based malware image analysis for improved detection. Models need to be enhanced to counter polymorphic malware attacks (Catalano et al., 2022).Federated learning practitioners need to handle security weaknesses in distributed learning models. Methods like homomorphic encryption and differential privacy need to be employed in order to secure federated learning deployments, especially for high-stakes applications such as finance and healthcare (Wei and Liu, 2024). Interorganizational coordination can strengthen models against privacy violation and adversarial attacks. In the same way, SVM-based intrusion classification can also be improved using PCA and feature selection to improve accuracy and mitigate computational burden. Maintaining intrusion detection models current with the latest datasets and adversarial training practices can greatly help make them successful at detecting new attacks.

4.1 Implications for Policymakers

Policymakers must recognize the contribution of AI in cybersecurity and encourage AI adoption into national and global security policies. The efficacy of deep learning techniques like RNNs, CNNs, and hybrids necessitates funding models for AI-based cybersecurity technology research and development (Gardner et al., 2022). Policies should also include regular review and renewal of AI-based security solutions to provide resilience against surge threats.

In typology of malware, consistent AI-based methods must be implemented across industries to ensure maximum detection power (Jeon, 2024). Encouraging transnational cooperation to facilitate threat intelligence sharing will allow AI algorithms to learn from evolving cyber threats. Ethical guidelines for AI deployment must be established to safeguard personal and organizational data while performing cybersecurity operations.
Federated learning presents a unique opportunity for balancing privacy and innovation.

It will be essential for policymakers to establish environments that provide protection for federated learning areas, especially sensitive sectors such as finance and healthcare (Kaissis et al., 2020). Legislation must include encryption solutions, such as homomorphic encryption, to secure data on decentralized networks while enabling advancement in technology (Dizon and Upson, 2021). Policymakers will also be required to fund open-access data sets and support studies to optimize learning algorithms and ensure AI-based security models remain responsive and efficient.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 1, January 2024 ||

| DOI:10.15680/IJIRSET.2024.1301007 |

4.2 Practitioner Implications

For AI practitioners, the implication of AI in intrusion detection is to integrate deep learning models into current security systems. AI algorithms have to be fine-tuned to satisfy particular cybersecurity needs for effectiveness. The models have to be retrained continuously to obtain high detection rates as a result of evolving cyber threats.

In computer security, malware detection requires computer security experts to investigate new AI-based techniques like byte-level deep learning and CNN-based image processing of malware. Model robustness against adversarial attacks is of particular interest in polymorphic malware attack prevention (Catalano et al., 2022).

Researchers using federated learning should be concerned with protecting gaps in distributed machine learning models in terms of security. Homomorphic encryption and differential privacy methods become a requirement while keeping federated learning applications intact, especially when dealing with private data (Wei and Liu, 2024). Cross-organizational sharing of information can render federated machine learning models secure against privacy attacks and adversarial attacks.

For SVM-based intrusion classification, PCA with feature selection techniques enhances model accuracy with minimal computation overhead. Periodic intrusion detection model update with new data sets as well as adversarial training techniques can greatly enhance their capacity to detect new attack methods.

V. FUTURE DIRECTIONS

• AI-powered security solutions need to be frequently updated to address the latest cyber threats. Techniques like continuous learning and reinforcement learning can help make these solutions more adaptive and responsive.
• Federated learning holds promise for enhancing privacy in AI-based cybersecurity applications, but challenges around security and trustworthiness need to be addressed.
• Multimodal AI approaches that combine different ML techniques like CNNs, RNNs, and transformers can provide more robust and comprehensive threat detection and response capabilities.
• Explainable AI will become crucial for building trust and accountability in high-stakes AI-powered cybersecurity systems.
• The use of generative adversarial networks for creating synthetic cyberattack data can help expand training datasets and improve model generalization.
• Leveraging emerging technologies like quantum computing and neuromorphic hardware can boost the efficiency and speed of AI-based cybersecurity tools.

Overall, the future of AI in cybersecurity is promising, but it will require continuous innovation, interdisciplinary collaboration, and responsible development to realize its full potential.

Future research in cybersecurity must address growing challenges with advanced AI-based methods. The shortcomings of traditional computing methods need solutions that can scale to combat advanced cyber attacks. Quantum computing's capability to exploit parallel processing and resistance, in turn, to encryption presents promising leads towards improving cybersecurity.

Quantum Machine Learning (QML) in Cybersecurity: Implementation of QML for cybersecurity will facilitate improved real-time threat identification and dynamic defense capabilities (Rajawat et al., 2023). Quantum-resistant security protocols research will be needed for cybersecurity solutions during the period of quantum computing.

Resilience against Quantum Threats: Quantum-secure networks and the enhancement of quantum key distribution (QKD) protocols shall be critical in resisting adversary attacks in quantum environments (West et al., 2023).

Quantum AI in Cybersecurity Education: Incorporation of quantum artificial intelligence (QAI) into cybersecurity education can help prepare the workforce to anticipate quantum-age threats (Baldassarre et al., 2023).

Explainable AI (XAI) in Cyber Threat Analysis: It is critical to design XAI algorithms with a balance between privacy and explainability for the purpose of improving the threat detection capability (Rjoub et al., 2023).

Neuro-Symbolic AI for Stronger Cybersecurity: Integrating neural networks and symbolic reasoning can potentially enhance threat detection and response against adversarial cyberattacks (Piplai et al., 2023).

AI-Based Malware Detection Breakthroughs: Study should be concentrated on the adversarial training methods to further advance malware detection models and enhance responsiveness towards emerging threats (Lucas et al., 2023).

Cyber-Physical System Security Based on Deep Learning: Deep reinforcement learning and federated learning studies for cyber-physical system (CPS) security will probably enhance threat detection within critical infrastructures.

Deepfake Threat Mitigation: Transfer learning and data augmentation are AI-driven strategies that can improve deepfake detection and reduce misinformation risks.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 1, January 2024 ||

| DOI:10.15680/IJIRSET.2024.1301007 |

Blockchain-AI Integration for IoT Security: Predictive analytics driven by AI and blockchain security features can improve IoT network defenses (Alharbi et al., 2022).
Privacy-Preserving Federated Learning: Exploring federated deep relationship prediction (FDRP) frameworks can reduce privacy risks without lowering model accuracy (Zhang L. et al., 2023).
AI-Cybersecurity in the Metaverse: With more virtual and augmented reality environments, cybersecurity strategies also need to counter new metaverse-related threats (Chow et al., 2022).
Sector-Specific AI for Cybersecurity: Sector-specific AI solutions for sector-specific threats (health, finance, energy, government) will enhance the security of key infrastructures.
Human-Centered AI for Cybersecurity: Blending psychological, sociological, and legal views into AI-foundation security frameworks will improve online safety.
Global AI Cybersecurity Standards: Establishing internationally recognized standards for AI-driven cybersecurity solutions will ensure consistent data security and threat mitigation practices.
AI and Sustainable Development Goals (SDGs): Exploring AI's role in achieving SDGs, particularly in digital security and infrastructure protection, can contribute to safer, more resilient societies.

VI. CONCLUSION

The rapid advancements in artificial intelligence have significantly impacted the cybersecurity landscape, offering new opportunities and challenges. AI-powered tools have demonstrated immense potential in enhancing threat detection, incident response, and data protection.

However, the successful integration of AI in cybersecurity requires careful consideration of ethical, privacy, and security implications. Ensuring the transparency, reliability, and accountability of AI-based security solutions is crucial for building user trust and acceptance.

As the cybersecurity threat landscape continues to evolve, future research should focus on developing AI techniques that are adaptive, resilient, and interoperable. Emerging technologies like quantum computing, neuro-symbolic AI, and federated learning hold promise for fortifying cybersecurity defenses. By fostering interdisciplinary collaboration and responsible innovation, the cybersecurity community can harness the transformative power of artificial intelligence to create a more secure and resilient digital future.

REFERENCES

1.Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions [Review of Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions]. Frontiers in Big Data, 7. Frontiers Media. https://doi.org/10.3389/fdata.2024.1497535
2.Ökdem, S., & Okdem, S. (2024). Artificial Intelligence in Cybersecurity: A Review and a Case Study [Review of Artificial Intelligence in Cybersecurity: A Review and a Case Study]. Applied Sciences, 14(22), 10487. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/app142210487
3.Salem, A., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques [Review of Advancing cybersecurity: a comprehensive review of AI-driven detection techniques]. Journal Of Big Data, 11(1). Springer Science+Business Media. https://doi.org/10.1186/s40537-024-00957-y
4.Aggarwal, G., Huang, C. Y., Fan, D., Li, X., & Wang, Z. (2022). DeMed: A novel and efficient decentralized learning framework for medical image classification on blockchain. *International Workshop on Distributed, Collaborative, and Federated Learning*, 100–109. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-18523-6_10
5.Ahanger, A. S., Khan, S. M., & Masoodi, F. (2021). An effective intrusion detection system using supervised machine learning techniques. *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, 1639–1644. IEEE. https://doi.org/10.1109/ICCMC51019.2021.9418291
6.Alamsyah, A., & Girawan, N. D. (2023). Improving clothing product quality and reducing waste based on consumer review using RoBERTa and BERTopic language model. *Big Data and Cognitive Computing, 7*(4), 168. https://doi.org/10.3390/bdcc7040168
7.Alharbi, S., Attiah, A., & Alghazzawi, D. (2022). Integrating blockchain with artificial intelligence to secure IoT networks: Future trends. *Sustainability, 14*(23), 16002. https://doi.org/10.3390/su142316002

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 1, January 2024 ||

| DOI:10.15680/IJIRSET.2024.1301007 |

8.Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 56306. https://doi.org/10.3389/fcomp.2021.563060
9.Alshahrani, E., Alghazzawi, D., Alotaibi, R., & Rabie, O. (2022). Adversarial attacks against supervised machine learning-based network intrusion detection systems. *PLoS ONE, 17*(e0275971). https://doi.org/10.1371/journal.pone.0275971
10.Arif, R. M., Aslam, M., Al-Otaibi, S., Martinez-Enriquez, A. M., Saba, T., & Bahaj, S. A. (2023). A deep reinforcement learning framework to evade black-box machine learning-based IoT malware detectors using GAN-generated influential features. *IEEE Access, 11*, 133717–133729. https://doi.org/10.1109/ACCESS.2023.3334645
11.Baldassarre, M. T., De Vincentiis, M., Pal, A., & Scalera, M. (2023). Quantum artificial intelligence for cyber security education in software engineering. *IS-EUD Workshops.*
12.Behl, A., Jayawardena, N., Pereira, V., Islam, N., Giudice, M. D., & Choudrie, J. (2022). Gamification and e-learning for young learners: A systematic literature review, bibliometric analysis, and future research agenda. *Technological Forecasting and Social Change, 176*, 121445. https://doi.org/10.1016/j.techfore.2021.121445
13.Benaddi, H., Ibrahimi, K., Benslimane, A., Jouhari, M., & Qadir, J. (2022). Robust enhancement of intrusion detection systems using deep reinforcement learning and stochastic game. *IEEE Transactions on Vehicular Technology, 71*(11), 11089–11102. https://doi.org/10.1109/TVT.2022.3186834
14.Bertino, E., Fovino, I. N., & Provenza, L. P. (2005). A framework for evaluating privacy-preserving data mining algorithms. *Data Mining and Knowledge Discovery, 11*(2), 121–154. https://doi.org/10.1007/s10618-005-0006-6
15.Bolbot, V., Kulkarni, K., Brunou, P., Banda, O. V., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection, 39*, 100571. https://doi.org/10.1016/j.ijcip.2022.100571
16.Campedelli, G. M. (2021). Where are we? Using Scopus to map the literature at the intersection between artificial intelligence and research on crime. *Journal of Computational Social Science, 4*, 503–530. https://doi.org/10.1007/s42001-020-00082-9
17.Catalano, C., Chezzi, A., Angelelli, M., & Tommasi, F. (2022). Deceiving AI-based malware detection through polymorphic attacks. *Computers in Industry, 143*, 103751. https://doi.org/10.1016/j.compind.2022.103751
18.Chen, W., Zhang, H., Zhou, X., & Weng, Y. (2021). Intrusion detection for modern DDoS attack classification based on convolutional neural networks. *International Conference on Intelligence Science* (pp. 45–60). Springer International Publishing. https://doi.org/10.1007/978-3-030-79474-3_4
19.Chow, Y. W., Susilo, W., Li, Y., Li, N., & Nguyen, C. (2022). Visualization and cybersecurity in the metaverse: A survey. *Journal of Imaging, 9*(1), 11. https://doi.org/10.3390/jimaging9010011
20.Cil, A. E., Yildiz, K., & Buldu, A. (2021). Detection of DDoS attacks with a feed-forward deep neural network model. *Expert Systems with Applications, 169*, 114520. https://doi.org/10.1016/j.eswa.2020.114520
21.Dahiya, S., & Garg, M. (2020). Unmanned aerial vehicles: Vulnerability to cyber attacks. *Proceedings of UASG 2019: Unmanned Aerial System in Geomatics, 1*, 201–211. Springer International Publishing. https://doi.org/10.1007/978-3-030-37393-1_18
22.Debnath, O., Debnath, S., Karmakar, S., Mallick, M. D., & Saha, H. N. (2023). A novel IoT architecture, assessment of threats, and their classification with machine learning solutions. *Journal of Internet of Things, 5*, 39391. https://doi.org/10.32604/jiot.2023.039391
23.Ding, Y., & Zhai, Y. (2018). Intrusion detection system for NSL-KDD dataset using convolutional neural networks. *Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence* (pp. 81–85). ACM. https://doi.org/10.1145/3297156.3297230
24.Dizon, M. A. C., & Upson, P. J. (2021). Laws of encryption: An emerging legal framework. *Computer Law & Security Review, 43*, 105635. https://doi.org/10.1016/j.clsr.2021.105635

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details