Mathematical Foundations and Computational Techniques for Emerging Technologies
Volume 14: Special Issue: SVGASCA Palem: Mar-2026

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752
J.Bindhu Bhargavi , 2026, 14:Special

Network Intrusion Detection with the Assistance of Artificial Intelligence

J.Bindhu Bhargavi
Research scholar in SR University, Warangal Lecturer in Computer Science and Applications
SR&BGNR Government Arts and science college(A), Khammam

Abstract- The relevance of resolving network intrusion issues in AI applications has increased due to the integration of artificial intelligence (AI) into vital infrastructure and daily life. While AI systems have many advantages, like improved productivity, automation, and decision-making, they also present new risks and weaknesses. It is essential to guarantee these systems' dependability and security. The main cybersecurity issues related to AI are examined in this study, including data privacy, integrity, adversarial attacks, and the moral ramifications of AI in security. Artificial Intelligence (AI) has revolutionized several industries in the digital age, providing previously unheard-of chances for efficiency and creativity. Nevertheless, these developments provide intricate cybersecurity issues that affect people, businesses, and society as a whole. It is crucial to protect these systems from malicious assaults, unauthorized access, and unforeseen repercussions as AI becomes more and more integrated into everyday life and vital infrastructure. We examine important cybersecurity concerns in AI applications, including adversarial assaults, data privacy violations, ethical challenges, and AI-driven cyberthreats. It also looks at how Shapley Additive explainable AI contributes to transparency by making AI models easier to understand and providing insights into how decisions are made.

Keywords- AI security, cybersecurity, Intrusion detection systems,cyber threats, generative AI, explainable AI, data privacy.

I. INTRODUCTION

AI becomes more and more integrated into everyday life and vital infrastructure. We examine important cybersecurity concerns in AI applications, including adversarial assaults, data privacy violations, ethical challenges, and AI-driven cyberthreats. Developing strong security measures, guaranteeing ethical AI use, and preserving confidence in digital systems all depend on an understanding of these issues. To combine AI's potential with efficient risk mitigation, technologists, legislators, and stakeholders must work together. This study offers a thorough examination of cybersecurity issues pertaining to AI, highlighting its limitations, pinpointing particular cyberthreats, and analyzing risk-reduction tactics. It also looks at the future of explainable AI and discusses the moral and legal ramifications of AI security. This paper serves as a resource for developers, business managers, and government agencies by making these subjects accessible and providing insights into the technical and strategic factors required for managing and safeguarding AI systems. As AI continues to change the digital landscape, maintaining vigilance and protecting privacy are essential.

http://doi.org/10.5281/zenodo.19439582

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752
J.Bindhu Bhargavi , 2026, 14:Special

Objectives of the study

- **An Intrusion Detection System (IDS) analyzes**
- Network traffic (Network-based IDS – NIDS)
- Host activities such as logs, processes, and file changes (Host-based IDS – HIDS)
- Traditional IDS relies on
- Signature-based detection (known attack patterns)
- Rule-based systems

Limitation: They struggle to detect zero-day attacks and evolving threats.

II. AI-BASED INTRUSION DETECTION FRAMEWORK

Data Acquisition and Preprocessing

- **IDS systems gather network traffic or log data. Preprocessing includes:**
- Data Cleaning: Removing noise and incomplete records.
- Feature Extraction: Statistical features such as packet rate, flow duration, byte counts.
- Normalization: Rescaling features for consistent model performance.

Model Training

AI models can be trained through:

1. Supervised Learning

Requires labeled datasets (normal vs attack). Common algorithms include:

- Decision Trees
- Random Forests
- Support Vector Machines (SVM)
- Convolutional Neural Networks (CNN)

Pros: High accuracy when labeled data is sufficient.
Cons: Requires large, well-labeled datasets.

2 Unsupervised Learning

Learns normal behavior to detect deviations:

- K-Means Clustering
- Autoencoders
- Principal Component Analysis (PCA)

Useful when labels are unavailable, but prone to false alarms.

3 Deep Learning

Deep learning models capture complex, non-linear relationships:

- Recurrent Neural Networks (RNN)
- Long Short-Term Memory (LSTM)
- Deep Belief Networks (DBN)

Especially effective for sequence-based network traffic.
Impact of generative AI in IDS

Cybersecurity and privacy are significantly impacted by generative AI, which comprises technology that may create data, content, and simulations that resemble human-generated output. Its effects are complex, presenting both novel ways to improve security and fresh difficulties that require cautious handling. The following are some of the main ways that generative AI affects privacy and cybersecurity:

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752
J.Bindhu Bhargavi , 2026, 14:Special

BeneficialEffects

By mimicking cyberattacks, finding flaws, and bolstering security measures, generative AI improves threat detection. By creating configurations and policies, adjusting to changing threats, and minimizing human labor for dynamic security management, it also automates security activities. Additionally, generative AI can produce lifelike phishing simulations to teach users how to identify and react to threats. Additionally, it promotes data privacy by the use of differential privacy to create anonymised datasets, preserving data usefulness for AI training while safeguarding individual privacy.

AdverseEffects

People and security systems may face difficulties as a result of generative AI's ability to create complex phishing content that is hard to discern from authentic communications.Strong defenses against AI-generated dangers and ongoing research on safe and moral AI practices are necessary for effective risk mitigation.

Ethical considerations and privacy with AI applications

Technology, human values, and social conventions all play a role in privacy and ethical issues in AI-driven cybersecurity.

1.Privacy, Bias, Security, and Fairness in AI

Because AI systems rely on enormous volumes of data, there are serious privacy and consent issues. To guarantee the ethical treatment of personal data, clear consent procedures and transparent data gathering procedures are crucial. Additionally, biases in training data may be amplified by AIsystems.

2.Transparency and Human Control in AI

The development of explainable AI (XAI) systems that non-experts can comprehend and evaluate is crucial since AI's opaque decision-making processes undermine transparency. Ensuring fairness requires algorithmic transparency, which enables people to track data sources and decision-making processes.

3.Development of secured and ethical AI

Strong security measures are essential to prevent vulnerabilities and misuse since the quick adoption of AI creates new security threats. To address any breaches, access controls, frequent security assessments, and incident response preparation are essential.

Research gap

Realistic multi-stage, lateral-movement behaviors are absent from cyberattack simulations. New simulators and benchmark datasets for actual, dynamic cyberthreats. There are no universal security frameworks for diverse IoT ecosystems. There are still unfixed architectural flaws in cloud native security (such as serverless and containers). (implied in works of literature) Further study is needed on edge computing security for real-time IoT operations. There is still little connection between organizational behavior studies and security awareness, decision-making, and reaction techniques. (implied by gaps in the literature)Practical defensive gaps are caused by a lack of talent and skills. Curriculum knowledge gaps, particularly in web and mobile security and emergency response—have an impact on workforce preparedness.

contribution of study

Many Capability Maturity Models (CCMMs) lack empirical validation and workable adoption procedures, making structured approaches like maturity models ineffective. Proactive, adaptive risk prediction is subordinated to reactive frameworks. Critical infrastructure industries, such as energy and healthcare, lack specialized security frameworks, and cybersecurity requires contextual study for many sectors. Real-time attack data for modeling and predictive research is lacking in maritime cybersecurity. Due to the limitations of developing nations' resources and legislative frameworks, cybersecurity research is rapidly

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752
J.Bindhu Bhargavi , 2026, 14:Special

evolving due to the sophistication ofadversaries, technical advancements, and the need to defend digital infrastructures globally. Research ranges from in-depth technical studies to more general organizational and behavioral evaluations. Despite significant progress, maintaining reliable, flexible, and human-centered security systems continues to present significant obstacles.

III. LITERATURE REVIEW

The protection of information systems against theft, damage, interruption, and illegal access is known as cybersecurity. Technical, organizational, and human-centered viewpoints are all included in this field's research. The literature shows that as cyberattacks and digital expansion across industries increase, there is a growing worry about digital dangers and the necessity for effective countermeasuresProtecting data availability, confidentiality, and integrity as well as developing defensive strategies against changing threats are two of the literature's main motivations Being aware of the organizational and human aspects of cybersecurity.

IV. METHODOLOGY OF DATA

Securing AI systems will be crucial as these technologies develop further. This will entail preventing manipulation or exploitation of models, algorithms, and training data. The integrity and dependability of AI systems will depend heavily on best practices, such as secure development, model verification, and runtime defenses.F. Frameworks for Regulation and EthicsBy creating frameworks, standards, and recommendations, governments and regulators will have a significant impact on AI cybersecurity. To reduce dangers and encourage responsible AI use, these frameworks will contain ethical concepts like accountability, fairness, and openness.

Findings in the study

1. Interdisciplinary collaboration between policy, economics, and cybersecurity.
2. Domain-specific methods as opposed to universal ones.
3. Empirical research on security behavior and human-centered cybersecurity models.
4. Defense systems that work in dispersed, resource-constrained settings.

Limitations and Future Directions

A.Cyber Defense with Power

The development of AI technologies, creative solutions, and stakeholder cooperation to counter new risks will all influence the future of AI cybersecurity.

B. Machine Learning Adversarial

Adversaries will use AI to create increasingly complex cyberattacks as AI-based defenses advance. As attackers take use of AI flaws to avoid detection and alter data, adversarial machine learning will pose serious difficulties. The development of sophisticated countermeasures and continuous study on adversarial robustness are necessary to counter these attacks.

C. Cybersecurity Explainable AI

Explainable AI (XAI) will be used in cybersecurity due to the growing desire for transparency in AI systems.

D. AI Security That Preserves Privacy

Privacy-preserving AI solutions will become essential as worries about data privacy and regulatory compliance grow.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752
J.Bindhu Bhargavi , 2026, 14:Special

V. CONCLUSION

Concerns about cybersecurity in AI applications are intricate and varied, involving technological, moral, and legal issues. Strong data protection, resilience against adversarial assaults, and careful consideration of the ethical aspects of AI security are all necessary components of a holistic approach to defend AI systems from these dangers. Strong security mechanisms, ongoing monitoring, and adversarial training are crucial for fixing vulnerabilities in order to stop AI exploitation. Shapley By providing clear and understandable insights into model decisions, explainable AI plays a crucial role in promoting responsibility and confidence. To develop standards, guidelines, and best practices for protecting AI applications and guaranteeing their safe, useful usage in society, cooperation between researchers, industry professionals, and politiciansisessential.

REFERENCES

1. Yerlikaya, F. A., & Bahtiyar, S. (2022). Data poisoning attacks against machine learning algorithms. Expert Systems with Applications, 208, 118101. https://doi.org/10.1016/j.eswa.2022.118101
2. Cui, L., et al. (2022). A covert electricity-theft cyberattack against machine learning-based detection models. IEEE Transactions on Industrial Informatics, 18(11), 7824–7833. https://doi.org/10.1109/TII.2021.3089976
3. Miao, Y., Chen, C., Pan, L., Han, Q., Zhang, J., & Xiang, Y. (n.d.). Machine learning based cyber attacks targeting controlled information: A survey.
4. Tuna, Ö. F., & Kadan, F. E. (2023). A novel method to mitigate adversarial attacks on AI-driven power allocation in D-MIMO. In Proceedings of the IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) (pp. 336–341). https://doi.org/10.1109/BlackSeaCom58138.2023.10299750
5. Yoshida, K., Kubota, T., Okura, S., Shiozaki, M., & Fujino, T. (2020). Model reverse-engineering attack using correlation power analysis against systolic array based neural network accelerator. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 1–5). https://doi.org/10.1109/ISCAS45731.2020.9180580
6. Rani, J. V., Saeed Ali, H. A., & Jakka, A. (2023). IoT network intrusion detection: An explainable AI approach in cybersecurity. In Proceedings of the 4th International Conference on Communication, Computing and Industry 6.0 (C2I) (pp. 1–6). https://doi.org/10.1109/C2I659362.2023.10430601