# RELEVANCE OF AI TECHNOLOGIES IN INFORMATION TECHNOLOGY SECURITY – A REVIEW

[1]Dhanya M, [2]Anju Omanakuttan, [3]Sithara Sasidharan, [4]Sumi Rehim
Computer Science and Engineering, Younus College of
Engineering & Technology , Kollam, Kerala
[1]dhanyaleji2012@gmail.com, [2]anjuomanakuttan1@gmail.com, [3]888.sithu@gmail.com,
[4]sumi@ycet.ac.in

## ABSTRACT

**As the number and cleverness of cyber-attacks increasing rapidly, it's more important to detect and prevent them. Cyber threats are becoming more advanced, creating serious risks for individuals, organizations, and nations. Strong cybersecurity is essential to prevent economic and societal damage caused by cybercrime. As cyber threats grow more sophisticated, traditional security methods are increasingly inadequate. Artificial Intelligence (AI) provides advanced tools to help counter these evolving risks and enhance cybersecurity. As cyber threats become more complex, traditional defenses fall short. This paper examines how Artificial Intelligence specifically Machine Learning, Deep Learning, Natural Language Processing, Explainable AI, and Generative AI can be applied to strengthen cybersecurity through a comprehensive analysis of their capabilities. Through a comprehensive analysis, the research aims to advance the state-of-the-art in AI- driven cybersecurity by identifying effective and reliable solutions for mitigating cyber risks and strengthening overall security**.

**INDEX TERMS: Cybersecurity, cyber-attack, machine learning, deep learning, explainable AI, generative AI**

## INTRODUCTION

Rapid technological advancement and growing interconnectivity have improved convenience but also intensifiedcybersecurity challenges. As business and individuals increasingly depend on digital platforms, cyber threats have become more frequent and severe. This paper explores how advanced AI techniques, such as machine learning, deep learning, Natural Language Processing, Explainable AI, and Generative AI, can address these evolving threats [1]. By providing a thorough analysis, the research aims to advance AI-driven cyber security solutions that effectively mitigate risks and enhance overall security. Technological advancements and increasing interconnectivity have brought significant convenience but also a surge in sophisticated cyber threats. These attacks pose serious risks to individuals, organizations, and nations, including financial losses, reputational harm, and threats to national security. Traditional security solutions are often inadequate against this evolving threat landscape. As a result, cybersecurity has become a top priority for governments, business, and individuals.Cybersecurity encompasses the technologies, processes, and practices designed to protect systems, networks, and data from cyber threats and vulnerabilities. As data volumes grow rapidly, maintaining robust security has become increasingly challenging. Modern cyber attackers' posses advanced technical skills and in-depth knowledge of system architectures, enabling them to breach even well-defended infrastructures. Numerous studies have shown that cybercrime has significantly impacted organizations, companies, and individuals in recent years [2].

As cyber threats continue to evolve in both complexity and frequency, traditional cybersecurity measures are increasingly inadequate for detecting and mitigating emerging attack techniques. Defending computer-based systems against these sophisticated threats has become more

challenging than ever. Consequently, there is a critical need to develop more effective and efficient cybersecurity solutions to proactively prevent cyberattacks. To mitigate security risks and reduce their impact, the cybersecurity field has concentrated research and development efforts on targeted areas. It is widely recognized within the cybersecurity community that the complete eradication of cyber threats is unfeasible [3]. As a result, many current strategies are reactive in nature rather the proactive.

In particular, significant academic focus in recent years has been directed toward incident response and intrusion detection, yielding encouraging advancements. However, these approaches are largely centered on post incident analysis, which limits their effectiveness in preventing attacks before they occur [4]. Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) are increasingly recognized as powerful tools for addressing cybersecurity challenges. These technologies can significantly enhance the capabilities of existing cybersecurity systems and help identify previously undetected threats. Although AI, ML, and DL are often used interchangeably, its important to understand their distinctions. AI is a broad field, encompassing systems that can sense, reason, act, and adapt. ML, a subset of AI, focuses on enabling machines to automatically learn from data and improve their performance over time. DL, a further specialization within ML, use complex algorithms and deep neural networks to train models, requiring vast amounts of data to achieve effective results.

## AI ENHANCING CYBERSECURITY: APPLICATIONS AND KEY BENEFITS

Artificial Intelligence is revolutionizing cybersecurity by offering new methods to detect, analyze, and respond to cyber threats. With its ability to process large volumes of data quickly and accurately, AI helps cybersecurity professionals stay ahead of evolving threats [5]. Below are some key benefits and applications of AI in cybersecurity:

- Threat Detection and Prevention
- Automated Incident Response
- Behavioral Analytics
- Advanced Malware Detection
- Phishing Prevention
- Vulnerability Management
- Threat Intelligence and Predictive Analysis
- Enhanced Endpoint Security

## ROLE OF MACHINE LEARNING (ML) IN THE CYBERSECURITY DOMAIN

Machine Learning (ML) plays a pivotal role in the evolving landscape of cybersecurity. With the rapid growth in cyber threats and the increasing complexity of attack methods, traditional security measures are no longer sufficient. ML provides a more adaptive and dynamic approach, enabling systems to identify and respond to threats in real time [6]. Below are some key roles ML plays in the cyber security domain:

- Threat Detection and Classification
  - Anomaly Detection
  - Malware Detection
- Real-Time Intrusion Detection and Prevention Systems (IDPS)
  - Network Traffic Analysis
  - User and Entity Behavior Analytics (UEBA)
- Phishing Attack Detection
  - E-Mail Filtering
  - Website Classification
- Automated Incident Response
  - Automated Threat Mitigation
- Predictive Analytics for Proactive defense
  - Risk Prediction
  - Vulnerability Management
- Behavioral Analytics for Insider Threat Detection
  - Insider Threat Detection
- Fraud Detection
  - Transaction Monitoring
  - Credit Card Fraud Prevention
- Data Privacy and Encryption
  - Access Control
  - Encryption Monitoring

## ROLE OF DEEP LEARNING (DL) IN THE CYBERSECURITY DOMAIN

Deep Learning (DL), a subset of Machine Learning (ML), has emerged as a transformative technology in the field of cybersecurity. By leveraging artificial neural networks that mimic the human brain, DL can process massive volumes of data, learn intricate patterns, and make accurate decisions with minimal human intervention [7]. Its ability to model highly complex, non-linear relationships makes it exceptionally well- suited for

identifying subtle, evolving, and previously unknown cyber threats. Below are the key roles and applications of Deep Learning in cybersecurity:

- Advanced Threat Detection
  - Zero-Day Exploit Detection
  - Polymorphic Malware Detection
- Intrusion Detection Systems (IDS)
  - Time Series Analysis
  - Feature Extraction
- Phishing and Social Engineering Detection
  - Text Classification
  - Fake Website Detection
- Malware Classification
- Network Traffic Analysis
- Spam and Botnet Detection

Challenges and Considerations

- Data Requirements
- Explainability
- Adversarial Attacks
- Computational Cost

## ROLE OF EXPLAINABLE ARTIFICIAL INTELLIGENCE (XAI) IN THE CYBERSECURITY DOMAIN

As Artificial Intelligence (AI), especially Machine Learning (ML) and Deep Learning (DL), becomes more deeply integrated into cybersecurity systems, a significant challenge has emerged: lack of transparency. Many AI models, particularly deep neural networks, operates "black boxes," offering little insight into how decisions are made. This lack of explainability can hinder trust, accountability, and adoption in high-stakes fields like cybersecurity. Explainability Artificial Intelligence (XAI) addresses this challenge by making AI decisions understandable to humans-crucial for ensuring reliability, trust, and compliance in cybersecurity operations [8]. Below are the key roles and benefits of XAI in the cybersecurity domain:

- Building Trust in AI-Driven Security Systems
- Improving Human AI Collaboration
- Reducing False Positives and Enhancing Decision Quality
- Compliance and Regulatory Requirements
- Debugging and Improving AI Models
- Detecting Adversarial Attacks on AI Models
- Training and Skill Development
- Model Transparency in High-Stakes Environments

Common XAI Techniques Used in Cybersecurity

- LIME (Local Interpretable Model-Agnostic Explanations): Explains individual predictions by approximating the model locally with an interpretable one.
- SHAP (Shapely Additive exPlanations): Quantifies the contribution of each feature to the model's output.
- Attention Mechanisms: Used in neural networks to highlight which parts of the input were most relevant to the decision.
- Decision Trees and Rule-Based Surrogates: Simplify complex models into interpretable rules.

## CONCLUSION

In the field of cybersecurity, Artificial Intelligence (AI) plays a pivotal role in analysing large datasets and monitoring a wide range of security threats and malicious activities. As the frequency and complexity of cyberattacks continue to rise, effectively addressing these challenges requires a synergistic integration of human expertise with AI-driven capabilities. This study presents a comprehensive overview of state-of-the-art benchmark cyberattack datasets, as well as the application of Machine Learning (ML) and Deep Learning (DL) techniques for the prediction and detection of various types of cyber threats.

## REFERENCES

[1] Shilpa Ankalaki, Aparna Rajesh Atmakuri, M. Pallavi GeetaBai S Hukkeri, Tony Jan and Ganesh R Naik, "Cyber Attack Prediction: From Traditional Machine Learning to Generative Artificial Intelligence,"

[2] R. von Solms and J. van Niekerk, ''From information security to cyber security,''

[3]J. W. Goodell and S. Corbet, ''Commodity market exposure to energy firm distress: Evidence from the colonial pipeline ransomware Atta,''

[4] R. Alkhadra, J. Abuzaid, M. AlShammari, and N. Mohammad, ''Solar winds hack: In-depth analysis and countermeasures,''

[5] D.-Y. Kao, S.-C. Hsiao, and R. Tso, ‘‘Analysing WannaCry ransomware considering the weapons and exploits,’’
[6] K. Bresniker, A. Gavrilovska, J. Holt, D. Milojicic, and T. Tran, ‘‘Grand challenge: Applying artificial intelligence and machine learning to cybersecurity,’’
[7] M. Husák, J. Komárková, E. Bou-Harb, and P. Celeda, ‘‘Survey of attack projection, prediction, and forecasting in cyber security,’’
[8] N. Mohamed, ‘‘Current trends in AI and ML for cybersecurity: A stateof-the-art survey,’’
[9] G. S. Emile and M. Kala, ‘‘Critical role of cyber security in global economy,’’