International Journal of Core Engineering & Management

Volume-6, Issue-08, 2020 ISSN No: 2348-9510

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN CYBER-SECURITY

Anvesh Gunuganti
maverickanvesh@gmail.com

Abstract

Security in cyberspace has been deemed essential as firms are experiencing new and complex forms of security threats. The more conventional approaches to security, like firewalls and virus checkers, are not doing enough to protect against modern threats. This paper explores the application of AI and ML in strengthening cybersecurity measures. AI algorithms can work in real-time and process huge volumes of data to identify suspicious events and endangered conditions. At the same time, ML models can enhance result precision owing to the analysis of data obtained using specific patterns. Using a PESTEL approach, the paper systematically determines the key political, economic, social, technological, environmental, and legal factors driving and facilitating the use of AI and ML for cybersecurity, as well as the factors that may affect the efficiency of this application. They also underline how AI and ML can be used to increase automation of threat detection, improve response mechanisms, and reduce cyber threats. Finally, the paper points out the importance of ethical circumstances, legislation, and environmentally friendly principles on policymakers, organizations, and technical creators based on the prospects of artificial intelligence in defending cybersecurity. Thus, based on the present research findings and applying the existing literature and empirical evidence, this paper advances knowledge about the role and application of AI and ML in strengthening cybersecurity measures in the modern networked environment.

Keywords— Artificial Intelligence, Machine Learning, Cybersecurity, Threat Detection, PESTEL Analysis

I. INTRODUCTION

Cyber threats become more diverse and numerous in the digital era, affecting ordinary citizens, taxpayers, and the state. These threats are still sophisticated, and traditional means of protection cease to be effective against them, which creates the need for a better approach [1]. AI and ML hold a huge potential for boosting cybersecurity by enhancing the observed threats, automating the responses, and offering forecasted outlooks. However, the factors affecting the choice and use of AI and ML in conjunction with tackling cyber security threats are political, economic, social, technical, environmental, and legal factors. Based on the research objectives of this paper, this paper will systematically assess the potential of AI and ML in improving cybersecurity, as well as the results of the PESTEL analysis that will indicate the factors that affect the ability to maximize their potential. Fig 1 explains the cybersecurity and other security domains.

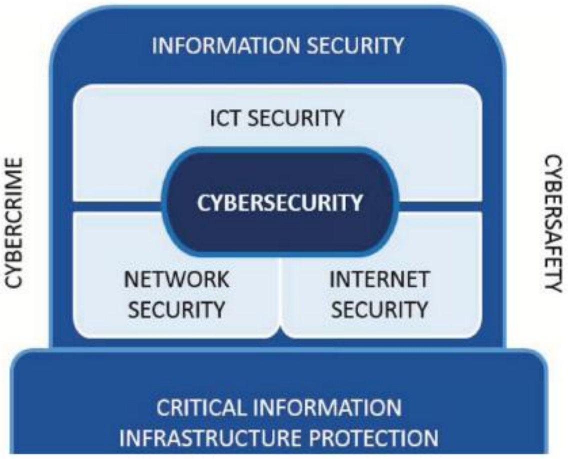

Fig. 1. Cyber security and other security domains [5]

A. *Overview*

The threat of cyber-attacks has increased, and the attacks are more frequent and complex than before, negatively impacting every segment of society. These stateful security measures depend largely on rigid rules and signature-based detection, which are increasingly incapable of identifying new emergent threats. These challenges are further exacerbated by the dynamism and novelty of cyber threats such as ransomware, phishing, and advanced persistent threats (APTs) that exploit vulnerabilities in digital frameworks [2].

In an attempt by organizations to protect their data and operations, the drawbacks of traditional security methods in the modern world are evident. Traditional security methods are slowly becoming ineffective for modern attackers since they are always in a constant state of evolution [12]. The scale and consequences of cyber incidents are growing, which indicates that new applications that can be adjusted to threats at their occurrence are needed.

B. *Problem Statement*

This is true because emerging risk levels of cyber threats are unmanageable, and organizational cybersecurity models do not change at the same pace as new threats and strategies are developed. Accurate malware detection is relatively difficult because of the use of signature-based detection systems and static rules, mainly because of the current complex and real-time attacks that will always attempt to remain unnoticed.

These drawbacks of the traditional cybersecurity approaches explain why advanced and intelligent ones are needed. AI and Machine learning, in particular, hold the promise of real-time and self-learning systems, which means that security will not be a reactive measure. To begin with, AI can crunch big amounts of data in real-time; first and foremost; it can identify existing threats and possible patterns of threats emerging in the network. For this reason, ML models make a progressive adjustment to the growing data to boost the effectiveness of cybersecurity activities.

C. *Research Purpose*

Consequently, the main purpose of this paper is to analyze how AI and ML improve cybersecurity practices owing to the somewhat altered threat landscape. Thus, this research aims to analyze the various aspects that affect the application of AI and ML in cybersecurity using the PESTEL approach, which consists of Political, Economic, Social, Technological, Environmental, and Legal factors analyses.

Knowledge of these factors is imperative to comprehend the prospects and inconveniences of implementing artificial intelligence and machine learning technologies into cybersecurity. To this end, this study wants to systematically review the external factors likely to affect AI and ML adoption in cybersecurity to offer a holistic approach to discussing their deployment's possibilities of contributing to improving organizational preparedness for cyber threats.

D. Research Aims and Objectives

- Assess AI and ML's capability to enhance protective measures against cyber-security threats.
- Determine global political elements, regional economic factors, social trends, technological advances, and legal regulations influencing the incorporation of AI and ML in cyber-security.
- Review the potentials and risks of using AI and ML in cyber-security.
- Make recommendations to the various stakeholders on better adopting AI and ML for increased security.

E. Research Questions

- How do artificial intelligence and machine learning enhance cyber-security?

II. LITERATURE REVIEW

Cyber-security has become one of the significant fields where the nature of threats is constantly growing more complex. Perimeter protection based on firewalls and antivirus is still the basis of protection, but it has become insufficient for modern threats. Modern threats such as social engineering attacks, ransomware, and zero-day are attacks that traditional security tools cannot overcome [3].

To these challenges, there has been a shift to using artificial intelligence (AI) and machine learning (ML) for cyber-security. AI capabilities in the current world are particularly useful in large amounts of data analysis in real-time, which helps organizations identify instances of discrepancies and threats that may exist. The feedback from the patterns results in data representation, which allows the enhancement of the efficiency of the ML models in detecting and managing cyber risks in the future. These technologies equip cyber-security personnel with threat identification tools, big data and analytics tools, and flexible countermeasures [4].

However, the incorporation of AI and ML in cyber-security is not without flaws. Issues on the protection of data used to train the AI models have not reached the aspect of irrelevance. Also, tackling how ethical AI will be employed, how algorithm biases can be eliminated, and how the cyber-security skills deficit can be addressed represent important points for reflection while moving forward. Fig. 2 explains the cyber attack cycle.

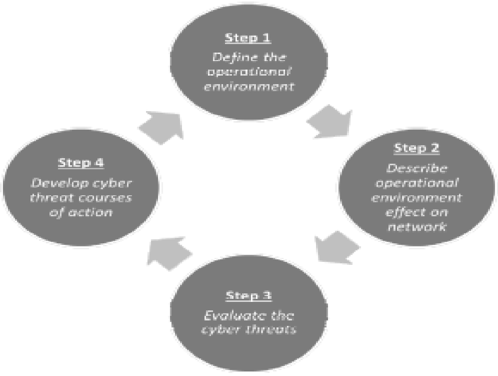
Step 1
Define the operational environment
Step 2
Describe operational environment effect on network
Step 3
Evaluate the cyber threats
Step 4
Develop cyber threat courses of action

Fig. 2. Cyber attack cycle [8]

A. *Current State of Cyber-security*

Today's cyber-security environment is evolving and growing in diverse forms due to cyber criminals' persistence and creativity. Countless complex threats are aimed directly at institutions and persons worldwide and seek to exploit network weaknesses. Thus, conventional protection and defense strategies are slow to adapt to the ever-changing threat landscape despite being at the core [5].

The first implemented tools were firewalls, antivirus programs, and intrusion detection systems (IDS). However, cyber adversaries are always evolving, and they use various methods to break the mentioned barriers, which are considered traditional. Consequently, social engineering uses human beings' vulnerabilities, ransomware keeps crucial data hostage to extort money from the organization, and zero-day vulnerabilities attack systems that have not been patched, constituting major threats to organizations [6].

The nature of these threats is gradually transforming, which means the need for more flexible and preventive approaches to cyber-security. AI and ML have potential solutions for detecting novel threats affecting organizations, predicting future attacks, and automating response automation. This is why cyber-security professionals should adopt these technologies: to enhance their security postures and prevent risks [7]. Fig. 3 shows the Neural Network Model in Cyber-security.

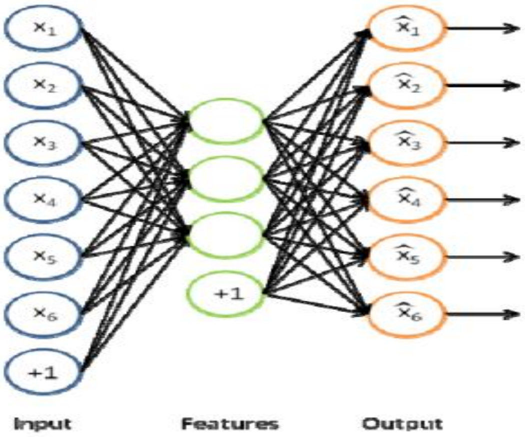

Fig. 3. Neural Network Model [6]

B. AI and ML in Cyber-security

AI and ML have become key enablers in improving a company's cyber-security strength and structure. Machine learning abilities of AI can evaluate large amounts of data in real-time, which can be potentially efficient for revealing different sorts of abnormal activity that rule-based systems may not recognize. Supervised and unsupervised learning, reinforcement learning, and deep learning are some of the ML techniques that make cyber-security systems intelligent by allowing cyber-security systems to learn from previous mishaps and enhance their abilities to prevent or at least reduce the rate of cyber tips [8]. Fig. 4 shows an example of the decision tree in cyber-security.

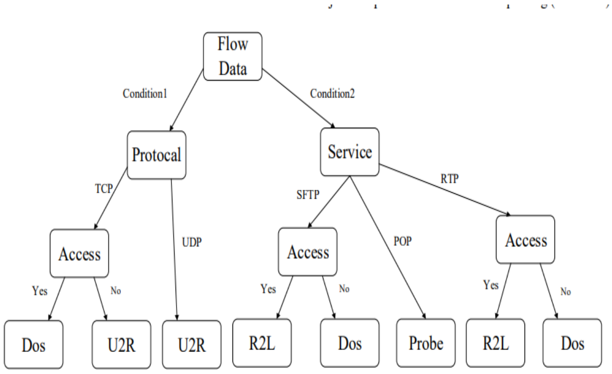

Fig. 4. Decision tree in cyber-security [11]

The literature on AI and ML in cyber-security demonstrates their effectiveness in various applications:

- **Threat Detection:** Artificial intelligence can recognize patterns that can potentially be a threat, especially in a vast and dynamic attack panorama.
- **Incident Response:** Mirroring on different frontlines allows the implementation of response strategies via automated means, thus reducing system response times and the effects of cyber incidents.
- **Predictive Analytics:** AI can forecast future threats using past data and contemporary trends, which enterprising organizations use to improve their security postures.

However, it is also worth noting that AI and ML technologies are not without certain problems. Data privacy, potential bias in the algorithms used, and the dynamics of threats in cyberspace can be considered the major challenges to their wider implementation [9].

Nevertheless, there are obstacles associated with the application of AI and ML in cybersecurity, which would define the further research and development of concepts in this area [10].

III. METHODOLOGY

This research takes a qualitative approach, and the most extensive plan for data collection is the PESTEL analysis to ensure the identification of all the factors influencing AI and ML integration in cyber-security. PESTEL analysis examines six key external macro-environmental factors: PESTEL strategic analysis: Political, Economic, Social, Technological, Environmental, and Legal factors. Altogether, these factors offer a synthesis to analyze the substantially greater environment within which AI and ML are used in cyber-security practices.

- **Political Factors:** This aspect focuses on governmental strategies, laws, and global engagements regarding AI and ML implementation in cyberspace protection. These are the roles of political systems, local legal requirements within data privacy parameters, cybersecurity norms, and intergovernmental treaties on the cyber-defense of consequential technologies.
- **Economic Factors:** Social has aspects like the broad impacts that financial investments needed for AI/ML deployments, costs and benefits of adopting these technologies about traditional cybersecurity practices, and stimuli/restraints put forward by stakeholders for integrating AI and ML into cybersecurity frameworks [14].
- **Social Factors:** Social aspects include society's attitude and acceptance of AI and ML in cyberspace, risks associated with the use of AI in cybersecurity, including bias and transparency in decision-making, and the overall effect on the cyber workforce concerning skills demand and job losses.
- **Technological Factors:** AI and all the related advancements stem from technological breakthroughs in cybersecurity. This involves increased computational processing capabilities, augmentation of existing algorithms for applications like deep learning for anomaly detection, and incorporating AI-based automation into cybersecurity work to improve threat detection, response time, and system robustness.
- **Environmental Factors:** Although often not included in the classical PESTEL frameworks, environmental factors are significant in AI and ML. This involves the effects of data centers, AI electronics and components, and issues concerning sustainable AI and ML practices in cyber security products.
- **Legal Factors:** Legal factors include compliance with data protection laws (such as GDPR and CCPA), the legal effects of AI decision-making in cyber security, IP law of AI algorithms, legal aspects regarding the International transfer of data, and reporting of cyber security incidences.

A. Data Collection

Article [1]

Trends indicate that cyber threats are rising and becoming a major concern for businesses. AI and ML are significant tools in threat detection and analysis; therefore, advancing AI and ML in cyber-security requires collaborative efforts from all stakeholders, including industrialists, academia, and governments worldwide.

Article [2]

Focused on developing AI, ML, and deep learning in the cyber-security field in terms of the velocity at which it progresses and its impact. The article under discussion concentrated on how AI is useful for delivering advanced cyber-security activities that can't be performed manually, such as threat identification and counteractions for new threats. Futures will be characteristic of AI as an agent that will prevent significant infrastructures and societal institutions from complex cyber threats.

B. Data Analysis: How the Data Will Be Analyzed Within the PESTEL Framework

The data collected from the articles will undergo rigorous analysis within the PESTEL framework to identify and evaluate the key factors influencing the adoption and effectiveness of AI and ML in cyber-security:

- **Political Analysis:** A study on how government policies, regulations, and international organizations affect AI and ML in cyber defense measures. This involves the analysis of cyber-security legislation, government funding programs, and geopolitical aspects that influence global cyber-security plans.
- **Economic Analysis:** Budget allocation for acquiring funds needed for AI and ML to be adopted in cyber-security, economic comparative analyses between AI solutions and conventional methods, and policies that encourage organizations to embrace AI and ML in cyber-security.
- **Social Analysis:** The perception of society on AI and ML in relation to cyber-security. This area would encompass public perception of AI and ML towards cyber-security, ethical issues on AI and cyber-security, impacts of artificial intelligence on the workforce regarding job loss, and requirements of talent for cyber-security jobs, among other aspects of AI-influenced cyber-security solutions.
- **Technological Analysis:** Assessment of emerging technologies in AI, ML, and cyber-security, such as the elucidation of new enhancements in AI algorithms, increased computation power, and the use of Artificial intelligence-based automation in numerous threat identification and response systems.
- **Environmental Analysis:** There is general concern about environmental sustainability practices in the AI and ML technologies currently employed in cyber-security, such as the power draw of AI boards/ chips and the footprint of data centers that support AI-intense cyber-security solutions.
- **Legal Analysis:** Explaining the existing legal standards in the field of AI/ML concerning cyber-security, data protection relevant to the present legal frameworks, legal responsibility in conjunction with AI-enabled decision-making in the context of cyber-attacks, and finally, the principles of intellectual property regarding technological developments including AI in the area of cyber-security.

Therefore, adopting the PESTEL analysis for these dimensions, this study seeks to give a comprehensive perspective of the external forces that impact the application, integration, and performance of AI and ML technologies in cyberspace. The research will provide rich information for researchers, policymakers, and ICT and security professionals who wish to implement better risk analysis and management techniques using AI and ML for advanced cybersecurity.

IV. ANALYSIS AND SYNTHESIS

Political Factors

- **Government Policies and Regulations Impacting AI and ML in Cybersecurity:** National policies and legal requirements are extremely relevant to properly utilizing AI and ML techniques in cybersecurity protection. These regulations are data protection laws, cybersecurity measurements, and policies on AI applications in critical infrastructure and protection.

- **National and International Cybersecurity Strategies:** National cybersecurity strategies describe governments' approaches to protecting against cyber threats and may involve AI and ML as the main components. International relations and policies also affect cybersecurity practices and policies worldwide since these require cooperation in threat intelligence and cyber defense.

Economic Factors

- **Cost-Benefit Analysis of AI and ML in Cybersecurity:** The various organizations undergoing research and implementation of AI and ML in cybersecurity experience cost-benefit analysis. This can entail considering the initial costs of various automation processes, the way automation increases efficiency, and the costs that can be saved through the minimization of cyber threats and breaches [13].
- **Market Trends and Investment in AI-Driven Cybersecurity Solutions:** The cybersecurity market is interested in investing in solutions based on artificial intelligence, as the technology can improve the ability to detect threats and countermeasures. Market trends suggest increasing demand for security analysis by AI, threat intelligence platforms, and automatic incident response systems.

Social Factors

- **Public Perception and Trust in AI and ML Technologies:** Understanding the general public's perception of AI and ML technologies has a bearing on the deployment of the technology in cybersecurity. Any worries about the dependability of data protection, the discriminatory nature of algorithms, and the proper use of AI in cyber security are critical factors that need to be considered to gain public trust in AI.
- **Ethical Considerations and Societal Impact of AI and ML in Cybersecurity:** The ethical issue covers equity, responsibility, and compelled disclosure as it relates to AI decision-making, particularly in cybersecurity. Social effects range from employment fluctuation and the use of people sans their jobs because of the emergence of technology to the general effects on digital security and privacy.

Technological Factors

- **Advancements and Innovations in AI and ML Relevant to Cybersecurity:** The application of AI and ML in cybersecurity becomes more effective due to frequent changes in the technologies used, which help to develop appropriate algorithms in areas like anomaly recognition, behavior analysis, and predictive modeling. New developments in aspects such as deep learning and natural language processing also enhance the potential of AI solutions in cybersecurity.
- **Integration Challenges and Technological Limitations:** Adopting AI/ML to enhance cybersecurity paradigms is challenging. These are issues such as compatibility with existing systems, scalability, and the constant need to update designs to the latest threats.

Environmental Factors

- **Environmental Impact of AI and ML Technologies:** AI/ML involves using data centers that run AI/ML-based cybersecurity solutions and influence energy consumption and carbon emissions. Various strategies for developing and deploying AI should be more sustainable, and the issue is more relevant now.

- **Sustainable Practices in the Development and Deployment of AI and ML:** As for energy efficiency, organizations seek green strategies for AI and ML by improving the energy consumption in AI chips, using green energy for data centers, and adopting the principles of green computing.

Legal Factors

- **Regulatory Frameworks Governing AI and ML in Cybersecurity**: AI and ML regulation in cybersecurity includes legal frameworks or laws that pertain to the use of AI and ML in cybersecurity, such as data protection legislation(GDPR, CCPA), cybersecurity laws and guidelines concerning AI ethics and responsibility. Adherence to these regulations is important in reducing legal exposure and deploying AI in the best possible manner.
- **Intellectual Property and Data Privacy Laws:** These laws, especially concerning AI algorithms and cybersecurity innovations, require protecting the associated intellectual property rights. Rules on data protection regulate Personal information requirements for collection, storage, and processing; these shape AI and ML in matters related to cybersecurity.
- **Legal Challenges and Compliance Issues:** Key legal issues arise when organizations adopt AI and ML, as this is accompanied by legal issues, including considerations of legal frameworks governing the technologies, legal responsibilities of organizations in AI decisions, and legal uncertainties of applying AI and ML. Legal standards are important for building trust and increasing the responsibility for using AI technologies in cybersecurity.

V. DISCUSSION

A. Interpretation of Findings

The major aspects of the business environment outside the organization can be evaluated using a PESTEL scheme to analyze the factors influencing the implementation of Artificial Intelligence (AI) and Machine Learning (ML) in cyber-security.

- **Political Factors:** Government measures and analytical legislation play a crucial role in the penetration of AI and ML in cyber-security. While data privacy acts and cyber security laws can be a double-edged sword in the development of AI security applications, that doesn't mean they aren't equally useful. International cyber-security strategies also have an important function in forming cooperation and using standards at the international level.
- **Economic Factors:** Business case assessments play a critical role in informing the implementation of AI and ML in cyber-security. AI solutions in cyber-security are promoted to create more efficient methods of threat identification, increasing efficiency and minimizing financial losses in case of a cyberattack.
- **Social Factors:** People's opinions and confidence in AI and ML technologies being applied affect their adequacy in cyber-security. Ethical issues like the fairness of algorithms and the method through which they reach decisions are the major factors that need to be met to gain societal acceptance. Therefore, using AI and ML in decision-making requires considering the workforce effect regarding displacement and skills development.
- **Technological Factors:** Integrating deep learning for anomaly detection and natural language processing for threat intelligence as some waves in AI and ML improve cyber-security strengths. However, it becomes complex when these technologies are integrated with the existing structures regarding interoperability, capacity growth, and constant technological advancement.

- **Environmental Factors:** The necessity of high sustainability levels in AI and ML technologies due to their environmental effecting can be observed; data centers hosting cybersecurity solutions, for instance. It is necessary to implement green computing practices and energy-efficient information technology assets to reduce the adverse environmental impacts that AI-based cybersecurity entails.
- **Legal Factors:** AI and ML cybersecurity enablement is strong on legal frameworks of AI ethics, data privacy, and IPR. Adherence to such legislation as GDPR and CCPA guarantees compliance with data management and the prevention of legal ramifications concerning the usage of AI in handling cybersecurity events.

B. *Comparative Analysis*

Comparing the results to other sources indicates the general trends and novel tendencies concerning integrating AI and ML in cybersecurity. Prior literature has discussed how AI can revolutionize cybersecurity by automating some of its tasks and improving protection mechanisms. However, the results also reveal some persistent issues, like ethical and regulatory issues, and the fact that cybersecurity never ceases to be an area of constant development due to threats.

C. *Implementation of Stakeholders*

- **Policymakers:** At this stage, policy should focus on establishing favorable legal frameworks to promote the use of AI and ML in cybersecurity while protecting data and cybersecurity rights.
- **Businesses:** AI and, more specifically, ML can help businesses enhance cybersecurity measures, achieve optimization, and reduce losses due to cyber-attacks. An organization that needs to compete effectively in today's economy should be keen on investing in AI-based security solutions.
- **Technology Developers:** The current problem with AI in cybersecurity is that technology developers must solve technical issues and consider ethical problems. Any new advancements in AI algorithms and cybersecurity should ensure that they are open, just, and fungible.

D. *Challenges & Opportunities*

- Challenges: Some deal with intricate legal frameworks and policies, handle ethical issues related to AI biases, implement AI within the existing systems, ensure cybersecurity risks related to AI systems, and contain the environmental effects of AI-associated data centers.
- Opportunities: More prospects exist in using AI to boost threat identification and counteraction, aggregate various routine processes in cybersecurity, speed up the response to unexpected attacks, increase collaboration between countries in cybersecurity, and develop AI that respects the principles of sustainable utilization.

VI. CONCLUSION

- The advancement in AI and ML has significantly enhanced cybersecurity, marking a new chapter in protecting against ever-evolving threats, with AI and ML being examined within the PESTEL framework to understand external factors.
- AI and ML developments offer unique opportunities for advancing cybersecurity by increasing incident prevention capabilities, response rates, and defense controllability through real-time

data analysis, improved decision-making, and complementing human perception of cyber threats.

- AI enhances automatic procedures by proactively performing repetitive security tasks, allowing cybersecurity professionals to focus on critical threats and opportunities.
- The progression of AI and ML highlights the importance of addressing ethical issues, laws, and social changes, which are crucial for AI's trustworthiness in cybersecurity and appropriate adoption in various organizational settings.
- Future advancements in cybersecurity will involve studying AI algorithms, cooperating with other fields, and adopting environmentally friendly practices, supported by strategic recommendations from SWOT analysis and aligned with industry best practices and expert advice.

A. *Summary of the key findings*

- **Political Factors:** Global cybersecurity policies and international frameworks, which define the state and trends of intelligent technologies' development, influence the regulatory framework for implementing AI and ML in cybersecurity.
- **Economic Factors:** Evaluations on cost-benefit analysis show how organizational leaders stand to gain regarding financial gains concerning adopting AI-related cybersecurity measures, such as enhanced detection of cyber threats and enhanced efficiency in operations.
- **Social Factors:** Awareness level and ethical factors are two key factors involving social acceptance in implementing AI and ML in cybersecurity.
- **Technological Factors:** This is due to the present integration troubles and tech limitations of AI and ML in protecting critical networks.
- **Environmental Factors:** The effects of AI and ML technologies indicate that adopting green practices in cyberspace is important, especially while performing cybersecurity duties.
- **Legal Factors:** The legal liabilities arising from AI-driven cybersecurity require compliance with data privacy laws, intellectual property rights, and best practices within relevant legal frameworks, ethical frameworks, and regulations guiding the use of AI.

B. *Overall Impact of AI and ML on Cyber-security*

AI and ML are transforming cyber-security by improving the methods of threat identification and response and increasing the level of protection for businesses against new cyber threats. They help contain threats that are anticipated in advance and real-time defense to reduce the effects of cyber threats on institutions and society in general. The synergy of incorporating AI and ML assures a proactive continuum of cyber-security operations to counter and prevent threats than conventional practices.

C. *Future Research Directions*

Moving forward, future research in AI and ML for cyber-security should focus on several key areas to address identified gaps and capitalize on emerging trends:

- **Enhancing AI Algorithms:** Sort more efficient algorithms for AI to improve the capabilities of threat identification and the further changes in cyber-security protection methods.
- **Ethical AI Practices:** Understand the moral values at the foundation of AI prejudices and investigate its prejudices, transparency, and accountability in information technology security.

- **Interdisciplinary Approaches:** Encourage combined efforts of IT professionals specializing in cyber-security and data science and the policymakers who set up these security frameworks.
- **Regulatory Frameworks:** See the case of legal initiatives to encourage the use of AI while protecting privacy and security policies.
- **Sustainable AI Solutions:** Adopt appropriate policies to ensure that AI technology advances have little effect or will not significantly harm the environment and reduce the amount of energy consumed.

REFERENCES

1. K. Bresniker, A. Gavrilovska, J. Holt, D. Milojicic, and T. Tran, “Grand Challenge: Applying Artificial Intelligence and Machine Learning to Cybersecurity,” Computer, vol. 52, no. 12, pp. 45–52, Dec. 2019, doi: https://doi.org/10.1109/MC.2019.2942584.
2. B. Geluvaraj, P. M. Satwik, and T. A. Ashok Kumar, “The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace,” International Conference on Computer Networks and Communication Technologies, vol. 15, pp. 739–747, Sep. 2018, doi: https://doi.org/10.1007/978-981-10-8681-6_67.
3. P. Sornsuwit and S. Jaiyen, “A New Hybrid Machine Learning for Cybersecurity Threat Detection Based on Adaptive Boosting,” Applied Artificial Intelligence, vol. 33, no. 5, pp. 462–482, Mar. 2019, doi: https://doi.org/10.1080/08839514.2019.1582861.
4. A. Handa, A. Sharma, and S. K. Shukla, “Machine learning in cybersecurity: A review,” WIREs Data Mining and Knowledge Discovery, vol. 9, no. 4, Feb. 2019, doi: https://doi.org/10.1002/widm.1306.
5. J. Martínez Torres, C. Iglesias Comesaña, and P. J. García-Nieto, “Review: machine learning techniques applied to cybersecurity,” International Journal of Machine Learning and Cybernetics, vol. 10, no. 10, pp. 2823–2836, Jan. 2019, doi: https://doi.org/10.1007/s13042-018-00906-1.
6. J. B. Fraley and J. Cannady, “The promise of machine learning in cybersecurity,” SoutheastCon 2017, Mar. 2017, doi: https://doi.org/10.1109/secon.2017.7925283.
7. M. Taddeo, T. McCutcheon, and L. Floridi, “Trusting artificial intelligence in cybersecurity is a double-edged sword,” Nature Machine Intelligence, vol. 1, no. 12, pp. 557–560, Dec. 2019, doi: https://doi.org/10.1038/s42256-019-0109-1.
8. R. Trifonov, O. Nakov, and V. Mladenov, “Artificial Intelligence in Cyber Threats Intelligence,” IEEE Xplore, Dec. 01, 2018. https://ieeexplore.ieee.org/abstract/document/8601235
9. L. Chan et al., “Survey of AI in Cybersecurity for Information Technology Management,” IEEE Xplore, Jun. 01, 2019. https://ieeexplore.ieee.org/abstract/document/8813605
10. S. BS, N. S., N. Kashyap, and S. DN, "Providing Cyber Security using Artificial Intelligence – A survey," 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Mar. 2019, doi: https://doi.org/10.1109/iccmc.2019.8819719.
11. Y. Xin et al., “Machine Learning and Deep Learning Methods for Cybersecurity,” IEEE Access, vol. 6, no. 6, pp. 35365–35381, 2018, doi: https://doi.org/10.1109/access.2018.2836950.
12. M. Hofstetter, R. Riedl, T. Gees, A. Koumpis, and T. Schaberreiter, “Applications of AI in cybersecurity,” 2020 Second International Conference on Transdisciplinary AI (TransAI), Sep. 2020, doi: https://doi.org/10.1109/transai49837.2020.00031.

13. "What is a Data Breach? | Understanding Powerful Cyber Threats," Relay Platform. https://www.relayplatform.com/what-is-a-data-breach/
14. "Multi-stakeholder partnerships for implementing the 2030 Agenda | Global Policy Forum," www.globalpolicy.org. https://www.globalpolicy.org/en/article/multi-stakeholder-partnerships-implementing-2030-agenda

ACRONYMS

1. AI - Artificial Intelligence
2. ML - Machine Learning
3. PESTEL - Political, Economic, Social, Technological, Environmental, and Legal
4. APTs - Advanced Persistent Threats
5. IDS - Intrusion Detection Systems
6. GDPR - General Data Protection Regulation
7. CCPA - California Consumer Privacy Act