JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 08 Issue 02
2025

Research Article
https://doi.org/10.56979/802/2025

AI-Driven Predictive Threat Detection and Cyber Risk Mitigation: A Survey

Muhammad Sarfraz[1], Irshad Ahmed Sumra[2*], Benish Khalid[3], and Ezzah Fatima[1]

[1]Department of Information Technology, Lahore Garrison University, Lahore, 54000, Pakistan.
[2]Department of Computer Science, Lahore Garrison University, Lahore, 54000, Pakistan.
[3]Lahore University of Biological and Applied Sciences (UBAS),Lahore, 54000, Pakistan.
*Corresponding Author: Irshad Ahmed Sumra. Email: irshadahmed@lgu.edu.pk

Accepted: January 09, 2025 **Published:** March 01, 2025

Abstract: Predictive analytics is revolutionizing cybersecurity and various industries by leveraging artificial intelligence (AI) and machine learning (ML) to enhance threat detection, risk mitigation, and decision-making processes. By enabling a shift from reactive to proactive security strategies, AI-driven predictive models improve the accuracy of cyber threat detection, reduce response times, and strengthen overall resilience against evolving attack vectors. Advanced techniques such as deep learning, anomaly detection, and natural language processing (NLP) enhance the adaptability and precision of these systems. A comprehensive review of existing research highlights key advancements, challenges including data integrity, algorithmic bias, and scalability and ethical concerns related to privacy, fairness, and transparency. Beyond cybersecurity, predictive analytics optimizes efficiency across sectors such as healthcare, finance, manufacturing, and energy, supporting smarter resource allocation and operational improvements. The integration of emerging technologies, including quantum computing, federated learning, and blockchain, further enhances predictive capabilities while ensuring security and compliance. By addressing these aspects, this research provides valuable insights to advance AI-driven predictive analytics, guiding the development of intelligent, ethical, and scalable solutions for a rapidly evolving digital landscape.

Keywords: Predictive Analytics; Cybersecurity; Artificial Intelligence; Machine Learning.

1. Introduction

The rapid expansion of digital infrastructure and the increasing interconnectivity of systems have revolutionized industries, enhancing efficiency and innovation. However, these advancements have also introduced complex cybersecurity challenges, with cyber threats becoming more sophisticated and pervasive. Organizations across various sectors face growing risks, including financial fraud, data breaches, ransomware attacks, and disruptions to critical services. As these threats evolve, traditional security mechanisms, which primarily rely on rule-based detection and manual intervention, are proving insufficient. Conventional approaches struggle to detect and mitigate advanced threats such as zero-day vulnerabilities, polymorphic malware, and advanced persistent threats (APTs), which can bypass static security measures. This necessitates the adoption of more proactive and intelligent security strategies. Predictive analytics, powered by artificial intelligence (AI) and machine learning (ML), has emerged as a transformative solution in cybersecurity. By leveraging vast datasets, ML-driven systems can identify hidden attack patterns, detect anomalies in real-time, and anticipate cyber threats before they materialize. Unlike static security measures, predictive models continuously evolve, adapting to emerging attack techniques and improving threat detection accuracy. These AI-driven systems analyze diverse data sources, including network traffic, user behavior, and threat intelligence feeds, to generate actionable insights and enhance decision-making. This shift from reactive to proactive cybersecurity significantly strengthens an organization's ability to mitigate threats before they escalate.

This study contributes to the field by developing a comprehensive framework that integrates predictive analytics into cybersecurity, improving threat detection accuracy, response efficiency, and risk

prioritization. It explores how AI and ML techniques can be optimized to analyze large-scale cybersecurity datasets, enhancing the detection of sophisticated cyberattacks. Furthermore, this study examines the challenges associated with AI-driven cybersecurity, including data quality issues, algorithmic bias, ethical concerns, and the need for greater transparency in predictive models. It also investigates privacy-preserving techniques, such as federated learning, to ensure secure and responsible data utilization.

Additionally, this study highlights the integration of predictive analytics with emerging technologies such as the Internet of Things (IoT), blockchain, and quantum computing to build resilient cybersecurity infrastructures. It provides insights into best practices for organizations seeking to implement AI-driven threat intelligence while maintaining compliance with regulatory frameworks. By addressing these key aspects, this study aims to guide researchers, industry professionals, and policymakers in designing adaptive and scalable cybersecurity solutions.

As cyber threats continue to evolve at an unprecedented pace, the findings of this study underscore the necessity of AI-powered predictive analytics in fortifying cybersecurity. By shifting from traditional reactive models to intelligent, anticipatory security frameworks, organizations can significantly enhance their resilience against modern cyber threats, ensuring long-term digital security and stability.

2. Literature Review

The following literature review explores the contributions and findings of several research papers that focus on the application of Artificial Intelligence (AI), Machine Learning (ML), and Predictive Analytics to improve cyber threat intelligence and enhance threat detection in cybersecurity.

Siva Subrahmanyam Balantrapu [1] explores the growing complexity of cyber threats and the limitations of conventional cybersecurity measures. The study focuses on the potential of advanced technologies to predict and prevent cyberattacks by analyzing both historical and current data. It highlights the role of techniques such as Natural Language Processing (NLP) and deep learning in enhancing the accuracy of threat detection and prediction. The study also emphasizes the ability of these technologies to reduce false positives and improve threat detection capabilities, leading to more proactive defense strategies. However, the paper also addresses challenges, including concerns related to data privacy, algorithm transparency, and the requirement for specialized expertise. This study offers valuable insights into the evolving role of technology in transforming cybersecurity practices.

Vegesna et. al. [2] introduces a predictive framework for cyber threat intelligence (CTI) that leverages advanced technologies. Their research underscores the significance of employing machine learning and natural language processing (NLP) to analyze large datasets, including open-source intelligence (OSINT) and dark web data. The study presents a framework designed to predict potential threats and generate actionable insights, transforming traditional reactive security approaches into proactive ones. Vegesna and Adepu also emphasize the precision of AI in forecasting threats, highlighting its potential to enhance the efficiency and effectiveness of CTI practices. The paper advocates for the development of AI-driven systems capable of providing deeper insights into emerging threats, thereby improving overall security strategies and defense capabilities.

R Shad et. al. [3] examines the increasing adoption of AI-driven threat intelligence in automating and enhancing the analysis and prediction of cyber threats. Their research highlights how AI techniques, such as machine learning and deep learning, enable real-time threat detection by processing large amounts of data. The authors emphasize the ability of AI to improve the accuracy of threat identification, which leads to more proactive and efficient threat mitigation strategies. Furthermore, Shad et al. explore the changing roles of cybersecurity professionals, underscoring the need for ongoing education and adaptation to keep up with the evolving threat landscape. The paper also discusses the ethical and privacy issues surrounding the use of AI in cybersecurity, offering recommendations to address these challenges and ensure responsible implementation of AI technologies.

A Emeka et. al. [4] examines the pivotal role of AI in enhancing predictive cyber threat intelligence (CTI). The authors highlight various AI methodologies, including machine learning, deep learning, and natural language processing (NLP), which aid in detecting potential threats, analyzing data, and forecasting emerging attack trends. The study underscores how AI improves the detection of early threats, reduces false positives, and strengthens incident response efforts. However, the authors also point out challenges such as issues with data quality, biases in models, and the integration of AI with existing

security systems, which must be addressed for AI to achieve its full potential in cybersecurity. The paper further discusses the future of AI-powered predictive CTI, proposing that it will lead to more intelligent, efficient, and adaptive security measures.

A Manoharan et. al. [5] examines how AI and machine learning (ML) are reshaping cybersecurity. The study highlights their ability to detect anomalies, assess behavioral patterns, and anticipate threats, significantly advancing threat detection capabilities. It explores the application of natural language processing (NLP) and neural networks to uncover complex threat patterns and streamline automated responses. While acknowledging challenges like ethical concerns and data privacy issues, the research emphasizes the substantial progress these technologies have made in enhancing cybersecurity. The paper demonstrates how AI and ML facilitate proactive, real-time threat detection, reinforcing organizational security measures.

JK Manda [6] explores how AI-powered systems enable real-time threat detection and intelligence gathering, allowing telecom operators to respond quickly to potential security threats. Manda highlights the ability of AI to automate repetitive tasks, enabling human analysts to concentrate on more complex security challenges. The study emphasizes AI's capability to identify patterns and anomalies within telecom network data, helping to prevent and address cyberattacks before they escalate. This research underscores the transformative role of AI in improving threat intelligence and incident response, contributing to a more secure telecom network environment.

F Ekundayo et. al. [7] examines the role of predictive analytics to enhance cybersecurity in the FinTech industry. It emphasizes the potential of Big Data and Machine Learning to forecast, detect, and address cyber threats targeting financial organizations. The study explores how predictive analytics can be integrated into Cyber Threat Intelligence (CTI) frameworks by processing unstructured data from sources such as dark web forums, malware logs, and phishing attempts. The authors highlight the value of techniques like anomaly detection and Natural Language Processing (NLP) in generating actionable insights and improving threat prediction. Their findings demonstrate that predictive analytics plays a critical role in dynamic risk assessment and strengthens incident response capabilities within the FinTech domain.

S Duary [8] investigates the use of predictive analytics in tackling cybersecurity challenges within intelligent networks. It emphasizes how integrating predictive analytics with advanced technologies enables task automation, the analysis of large datasets, and the detection of intricate patterns that traditional methods might fail to identify. The study highlights the critical role of innovative solutions in enhancing cybersecurity defenses. The study addresses concerns such as ethical issues, the importance of transparency in models, and the need for collaboration among experts to fully realize the potential of these technologies. Their findings contribute to the ongoing discussion on how predictive analytics is transforming cybersecurity in intelligent networks.

3. Comparative Analysis of AI-Driven Approaches in Cybersecurity Approaches

This table below showcases the unique contributions and viewpoints of each study, providing a thorough understanding of their comparative insights into the role of AI and predictive analytics in cybersecurity.

Table 1. Comparative Analysis

Aspect	Focus	Key Technologies	Strengths	Challenges Identified	Application Domain	Contribution to Cybersecurity
Siva Subrahmanyam Balantrapu [1]	Predictive technologies for threat detection and prevention	NLP, deep learning	Enhances accuracy of threat prediction, reduces false positives	Data privacy, algorithm transparency, need for specialized expertise	General cybersecurity	Demonstrates how predictive technologies enhance cybersecurity practices

Vegesna et al. [2]	Predictive CTI framework leveraging AI	Machine learning, NLP	Proactive threat prediction and actionable insights	Data integration challenges, reliance on OSINT and dark web data	Cyber Threat Intelligence (CTI)	Introduces a predictive framework for CTI, enabling proactive defenses
R Shad et al. [3]	AI in automating cyber threat detection and prediction	Machine learning, deep learning	Real-time threat detection, improved accuracy	Ethical and privacy concerns	General cybersecurity	Highlights automation in threat detection
A Emeka et al. [4]	Role of AI in enhancing predictive CTI	Machine learning, deep learning, NLP	Early threat detection, reduced false positives	Data quality issues, model biases, integration challenges	Predictive CTI	Suggests AI-driven predictive CTI can lead to more adaptive security
A Manoharan et al. [5]	Impact of AI and ML on anomaly and threat detection	NLP, neural networks	Proactive, real-time anomaly detection	Ethical concerns, data privacy issues	General cybersecurity	Demonstrates AI/ML capabilities in behavioral analysis and anomaly detection
JK Manda [6]	Real-time threat detection in telecom networks	AI-powered systems	Automates repetitive tasks, identifies telecom network patterns	Requires collaboration among analysts for complex issues	Telecom industry	Showcases AI's transformative role in telecom threat detection
F Ekundayo et al. [7]	Predictive analytics for FinTech cybersecurity	Big Data, machine learning, NLP	Enhances dynamic risk assessment and incident response	Unstructured data processing, reliance on diverse data sources	FinTech industry	Emphasizes predictive analytics in improving risk management and incident response
S Duary [8]	Predictive analytics in intelligent networks	Predictive analytics, advanced technologies	Automates tasks, detects complex patterns,	Ethical concerns, model transparency, and need	Intelligent networks	Offers insights into the integration of predictive analytics and

	and analyzes large datasets	for expert collaboration	AI for intelligent networks

4. Ethical and Privacy Considerations in Advanced Cybersecurity Solutions

The adoption of advanced technologies in cybersecurity has revolutionized the ability to detect, analyze, and mitigate cyber threats. However, these advancements bring forth critical ethical and privacy challenges that must be addressed to ensure the responsible use of such technologies. Below are key areas of concern and approaches to tackle them effectively.

4.1. Protecting Data Privacy in Advanced Cybersecurity

The implementation of advanced cybersecurity solutions often involves processing vast amounts of sensitive data, which raises concerns about data breaches, unauthorized access, and compliance with privacy regulations. Robust encryption techniques, decentralized processing models, and frequent privacy audits are essential measures to safeguard user data and maintain compliance with regulatory frameworks like GDPR and CCPA.

4.2. Eliminating Bias and Ensuring Fairness in Security Algorithms

Bias within security algorithms can lead to inaccurate threat detection or discriminatory outcomes. Addressing these issues requires the use of diverse training data, periodic evaluation of algorithmic fairness, and the incorporation of transparent methodologies to ensure equitable and unbiased decision-making processes.

4.3. Promoting Transparency and Accountability in Cybersecurity Systems

Advanced technologies often face criticism for their opaque decision-making processes, commonly referred to as the "black box" problem. To overcome this, organizations should prioritize the use of transparent technologies, implement explainable models, and maintain comprehensive documentation to build trust and demonstrate accountability.

4.4. Ethical Implications of Automation in Cybersecurity

Automation in cybersecurity introduces ethical dilemmas such as excessive monitoring and potential misuse of technology. Establishing clear ethical policies, limiting intrusive surveillance, and embedding safeguards against the misuse of automation are necessary steps to address these concerns and promote responsible use.

4.5. Balancing Security Priorities with Privacy Rights

A critical challenge in cybersecurity is achieving a balance between implementing strong security measures and protecting individual privacy rights. This balance can be achieved by adopting privacy-by-design principles, ensuring informed user consent, and fostering collaboration among industry stakeholders to align security practices with ethical values.

4.6. Establishing Clear Regulatory and Ethical Guidelines

The rapid growth of advanced cybersecurity technologies necessitates the creation of comprehensive regulatory frameworks to address ethical and privacy issues. Policymakers and industry leaders must collaborate to establish global standards, enforce compliance, and advocate for ethical practices in the deployment of cutting-edge technologies.

5. Advancements in AI-Powered Predictive Analytics

Predictive analytics has become an essential tool for modern industries, revolutionizing processes by enabling organizations to anticipate risks, enhance operations, and make informed decisions. In the field of cybersecurity, advancements in predictive analytics are paving the way for proactive threat prevention and mitigation. Below are the significant developments and their implications for cybersecurity practices.

5.1. Improved Accuracy with Advanced Machine Learning Techniques

Cutting-edge machine learning (ML) techniques have enhanced the accuracy of predictive models by analyzing large and complex datasets. These methods uncover hidden patterns and evolving trends that traditional approaches often overlook. As these models continuously learn and adapt, they provide

organizations with precise predictions, enabling effective identification and prevention of emerging threats.

5.2. Real-Time Monitoring and Rapid Response

AI-driven predictive systems excel in real-time data analysis, enabling organizations to detect anomalies and respond swiftly to potential threats. By analyzing network activity, user behavior, and historical data, these systems identify irregularities that may indicate cyberattacks. This capability significantly reduces response times, preventing threats from escalating and minimizing potential damage.

5.3. Integration with Big Data and IoT Platforms

The convergence of AI with Big Data and Internet of Things (IoT) technologies has expanded the reach and potential of predictive analytics. By leveraging data generated by IoT devices and Big Data platforms, AI systems can detect vulnerabilities across interconnected networks. This comprehensive approach ensures more robust and holistic cybersecurity measures.

5.4. Advanced Threat Intelligence and Risk Prioritization

Predictive analytics has redefined threat intelligence by delivering deeper insights into evolving risks. AI systems detect subtle threat indicators, allowing organizations to understand the broader threat landscape. By prioritizing critical risks, these systems help allocate resources more effectively, ensuring that the most pressing vulnerabilities are addressed first.

5.5. Automation for Faster Incident Management

The automation capabilities of AI have transformed the way organizations handle incident response. Predictive analytics enables systems to take immediate action, such as isolating compromised systems or blocking malicious actors, without requiring manual intervention. This automation reduces response times, lightens the workload for security teams, and enhances overall efficiency.

5.6. Transition to Proactive Cybersecurity Approaches

Predictive analytics is driving the shift from reactive to proactive security strategies. By anticipating potential attack scenarios and implementing preventive measures, organizations can strengthen their defenses before vulnerabilities are exploited. This forward-thinking approach enhances resilience against increasingly sophisticated cyber threats.

5.7. Adaptive Learning for Evolving Threats

AI-powered predictive analytics systems are designed to learn from past incidents and adapt to new challenges. This continuous learning process ensures that predictive models remain effective against emerging and sophisticated attack techniques. The ability to evolve enhances long-term security and helps organizations stay ahead in the fight against cybercrime.

The rapid advancements in predictive analytics are transforming cybersecurity, offering organizations the tools to predict, prevent, and respond to threats with unparalleled efficiency. These innovations provide a foundation for stronger, more adaptive security frameworks that can keep pace with the ever-changing digital landscape.

6. The Influence of Predictive Analytics Across Various Industries

Predictive analytics is revolutionizing industries by enabling data-driven decision-making and improving operational efficiency. In healthcare, it supports early disease detection, personalized treatments, and efficient resource management, transforming patient care and medical practices. The financial sector leverages predictive tools for risk assessment, fraud prevention, and market trend analysis, enhancing security and optimizing financial operations. Retail businesses use predictive analytics to improve customer engagement, manage inventory more effectively, and streamline supply chains. In manufacturing, it enhances productivity through predictive maintenance, quality control, and better resource allocation. The energy sector benefits by forecasting demand, optimizing grid management, and supporting the integration of renewable energy sources. Transportation and logistics use predictive models to enhance route planning, fleet efficiency, and delivery accuracy. Education systems apply predictive analytics to customize learning, track student progress, and allocate resources strategically. In cybersecurity, predictive tools enable proactive threat detection and prevention. The public sector utilizes these technologies for improved governance, disaster readiness, and citizen services. Across these sectors, predictive analytics drives innovation, supports sustainable practices, and builds resilience, marking a significant shift toward smarter and more efficient systems.

7. Challenges and Research Gaps in Predictive Analytics

Predictive analytics has transformed numerous industries, yet it encounters several challenges and unresolved research gaps that limit its broader adoption. Factors such as inadequate data quality, restricted access, and biases inherent in datasets can undermine the accuracy and dependability of predictive models. Ethical dilemmas, including concerns over privacy violations, data exploitation, and algorithmic unfairness, are particularly pressing in sectors that manage confidential information. Furthermore, the opacity and complexity of advanced models, such as those utilizing deep learning, reduce trust and hinder widespread implementation. Technical hurdles, such as ensuring scalability and seamless integration with existing systems, demand substantial expertise and financial resources, often making these solutions less accessible to smaller enterprises. Key areas for further research include developing models tailored to specific industries, addressing unique sectoral needs, and ensuring adherence to ethical principles. Progress is also needed in refining real-time analytics, enhancing anomaly detection, and integrating predictive analytics with cutting-edge technologies like IoT, blockchain, and quantum computing. Addressing these challenges and filling these gaps will require a concerted effort from researchers, industry practitioners, and policymakers to design ethical, innovative, and scalable solutions that enhance the utility of predictive analytics across various domains. The study will be expanded to address critical challenges and explore potential advancements aimed at enhancing the effectiveness of predictive analytics across multiple industries. Future research will prioritize improving data quality, mitigating algorithmic biases, and enhancing model transparency to build systems that are both dependable and unbiased. Further exploration will include the integration of conventional statistical models with advanced machine learning approaches, aiming to improve prediction accuracy and adaptability. Additionally, the study will investigate the use of privacy-preserving technologies, such as federated learning, to protect data security while fostering collaboration across different entities. The integration of predictive analytics with emerging technologies like quantum computing will also be explored, as it has the potential to significantly enhance computational capabilities. Moreover, the study will work towards developing industry-wide standards and regulatory frameworks, in collaboration with experts, to ensure the ethical and effective deployment of predictive analytics in diverse sectors.

8. Conclusion

The study underscores the transformative influence of predictive analytics across various industries, particularly in enhancing decision-making, operational efficiency, and security measures. By leveraging advanced machine learning, real-time monitoring, and automated systems, predictive analytics has greatly improved the accuracy of threat detection and facilitated proactive, adaptive cybersecurity strategies. Its applications span numerous sectors, including healthcare, finance, retail, manufacturing, energy, transportation, education, and the public sector, where it drives innovation, resilience, and smarter, more efficient systems. However, challenges such as data integrity, algorithmic bias, lack of transparency, and ethical concerns around privacy remain significant barriers to widespread adoption. The complexity and scalability of predictive models also present technical difficulties, especially for smaller organizations. Addressing these issues requires targeted research to improve data quality, incorporate emerging technologies like quantum computing, and create sector-specific solutions. Additionally, the development of privacy-preserving techniques and the establishment of clear regulatory guidelines are essential for the responsible deployment of predictive analytics. Looking ahead, continued advancements in this field hold great promise for furthering transformative changes, strengthening security, and promoting sustainable practices across industries. By overcoming these obstacles and embracing innovation, predictive analytics will play a key role in building more secure, efficient, and adaptive systems in the future.

References

1. Balantrapu, S. S. (2024). AI for predictive cyber threat intelligence. International Journal of Management Education for Sustainable Development, 7(7), 1-28.
2. Vegesna, V. V., & Adepu, A. (2024). Leveraging Artificial Intelligence for Predictive Cyber Threat Intelligence. International Journal of Creative Research in Computer Technology and Design, 6(6), 1-19.
3. Shad, R., Broklyn, P., & Potter, K. (2024). AI-Powered Threat Intelligence: Automating Cyber Threat Analysis and Prediction.
4. Emeka, A., Sanctuary, S., & Christopher, G. Leveraging AI for Predictive Cyber Threat Intelligence.
5. Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. DOI: https://www. doi. org/10.56726/IRJMETS32644, 1.
6. Manda, J. K. (2024). AI-powered Threat Intelligence Platforms in Telecom: Leveraging AI for Real-time Threat Detection and Intelligence Gathering in Telecom Network Security Operations. Available at SSRN 5003638.
7. Ekundayo, F., Atoyebi, I., Soyele, A., & Ogunwobi, E. (2024). Predictive Analytics for Cyber Threat Intelligence in Fintech Using Big Data and Machine Learning. Int J Res Publ Rev, 5(11), 1-15.
8. Duary, S., Choudhury, P., Mishra, S., Sharma, V., Rao, D. D., & Aderemi, A. P. (2024, February). Cybersecurity threats detection in intelligent networks using predictive analytics approaches. In 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM) (pp. 1-5). IEEE.
9. Laato, S., Farooq, A., Tenhunen, H., Pitkamaki, T., Hakkala, A., & Airola, A. (2020). AI in Cybersecurity Education-A Systematic Literature Review of Studies on Cybersecurity MOOCs. 2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT), 6-10.
10. Zeadally, S., Adi, E., Baig, Z.A., & Khan, I.A. (2020). Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. IEEE Access, 8, 23817-23837.
11. Hofstetter, M., Riedl, R., Gees, T., Koumpis, A., & Schaberreiter, T. (2020). Applications of AI in cybersecurity. 2020 Second International Conference on Transdisciplinary AI (TransAI), 138- 141
12. Sree, V.S., Koganti, C.S., Kalyana, S.K., & Anudeep, P. (2021). Artificial Intelligence Based Predictive Threat Hunting In The Field of Cyber Security. 2021 2nd Global Conference for Advancement in Technology (GCAT), 1-6.
13. Morovat, K., & Panda, B. (2020). A Survey of Artificial Intelligence in Cybersecurity. 2020 International Conference on Computational Science and Computational Intelligence (CSCI), 109-115.
14. D. Saxena, I. Gupta, R. Gupta, A. K. Singh and X. Wen, "An AIDriven VM Threat Prediction Model for Multi-Risks Analysis-Based Cloud Cybersecurity," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 53, no. 11, pp. 6815-6827, Nov. 2023, doi: 10.1109/TSMC.2023.3288081.
15. Sarker, I.H., Furhad, M.H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Computer Science, 2.
16. Chan, L., Morgan, I., Simon, H., Alshabanat, F., Ober, D., Gentry, J., Min, D., & Cao, R. (2019). Survey of AI in Cybersecurity for Information Technology Management. 2019 IEEE Technology & Engineering Management Conference (TEMSCON), 1-8.
17. Kamoun, F., Iqbal, F., Esseghir, M.A., & Baker, T. (2020). AI and machine learning: A mixed blessing for cybersecurity. 2020 International Symposium on Networks, Computers and Communications (ISNCC), 1-7.