ISSN : 2455-135X © 2025 International Scientific and Academic Research (ISAR) Publisher

AI-Powered Risk Scoring and Optimization Techniques for Organizational Network Security

Deepak Tomar
System Analyst, Computer Center
Bundelkhand University
Jhansi, India
dr.deepak@bujhansi.ac.in

Kismat Chhillar
Dept of Mathematical Sciences & Computer Application
Bundelkhand University
Jhansi, India
drkismatchhillar @gmail.com

Saurabh Shrivastava
Dept of Mathematical Sciences & Computer Application
Bundelkhand University
Jhansi, India
dr.saurabh@bujhansi.ac.in

Alok Verma
Dept of Mathematical Sciences & Computer Application
Bundelkhand University
Jhansi, India
alokverma.bu@gmail.com

***Abstract*—Artificial intelligence (AI) has revolutionized the approach of organizations on network security by allowing for real-time responses to threats, proactive and data-driven risk assessment. Machine learning models, AI-driven risk scoring methods and sophisticated analytics are utilized to identify vulnerabilities, prioritize potential threats, and optimization of resources allocation. These systems aid to enable ongoing monitoring and flexible evaluation of risk which in turn offers valuable insights helpful for decision-making. It also boosts the effectiveness of security measures against cyber threats that are ever-changing. Optimization strategies that are AI-driven facilitates organizations in automation of compliance processes, shortens incident response times, and upholds regulatory standards with better precision. Organizations can address high-risk anomalies quickly while minimizing human error and day-to-day operational costs by incorporation of explainable AI, automated remediation tools and adaptive defenses into their network frameworks. Although there are challenges related to transparency of models, data quality, and scalability, AI-powered solutions play a significant role to leap forward in protecting businesses from contemporary cyber risks. AI-driven risk scoring plays a crucial role for organizations to assess, forecast, and prioritize network security threats using machine learning techniques and advanced analytics. These approaches enhance protections for complex enterprise systems by enabling swift threat detection and automation of response actions. Future research should focus on developing explainable AI and robust AI methods for improvement of understanding and resilience against the landscape of cyber risks that is evolving at a very fast pace.**

Keywords*— *AI-powered risk scoring, network security optimization, threat assessment, machine learning, explainable AI, automated remediation

I. INTRODUCTION

Artificial intelligence (AI) has become a game-changer in the field of organizational network security. AI has completely reshaped threat detection and risk management [1] [2] . In this fast-paced digital age, cyber threats are not only growing numerically but also becoming highly sophisticated, putting traditional security methods under pressure which are often based on rigid rules and signature detection. AI-driven techniques harness cutting-edge machine learning (ML) algorithms and real-time analytics for detecting unusual activities, anticipating potential attacks, and reacting in real-time [3] . This evolution has allowed organizations in bolstering their security measures while staying agile and proactive in the face of threats that are ever-changing. AI has enhanced network security at an exponential rate by automating essential tasks of ongoing monitoring, risk assessment and behavior analysis. AI systems with anomaly detection, get to know about the usual network behavior patterns and proactively highlight any irregularities that might suggest malicious intent or suspicious activity. Additionally, predictive analytics provides a heads-up to organizations by identifying future vulnerabilities that are based on past trends of data and new threat intelligence. These advanced capabilities and techniques pave the way for defenses that are proactive, which in turn significantly lowers the chances and consequences of sophisticated cyber incidents.

AI is really changing the network security game when it comes to optimization of resource allocation for network security. By assessing threats which are based on risk scores that are collected from a variety of data inputs, organizations can zero in on the critical vulnerabilities that pose the highest risk [4] [5] . This not only aids in streamlining the organizational efforts but also helps in automating response workflows, which in turn results in reduction of errors caused by humans and operational hiccups. Explainable AI models are crucial for compliance and governance that supports security teams to gain better transparency and allows them to understand the automated decision making. Companies in fields like healthcare, finance, and government are already witnessing success with network security solutions that are AI-driven and protect sensitive data and uphold regulatory standards. Some real-world examples show that AI can identify complex attacks, namely insider threats and zero-day exploits, much more accurately and quickly as compared to traditional methods. There are challenges to tackle inspite of numerous benefits of AI-driven techniques, like ensuring quality of data, addressing biasness of model, and dealing with issues of scalability and integration, which are significant barriers to broader adoption.

With the advancement of AI technology, the network security future is likely to embrace hybrid models. These models blend AI analytics with conventional security methods, stronger defenses against adversarial AI threats and ongoing learning techniques. The continuous research and development in this network security field promise to create more resilient, robust, adaptable, and intelligent environments for network security.

The rest of the paper is organized as follows: the next section will review the literature and AI-driven risk scoring and security optimization frameworks. Following that, the paper will dive into methodologies for risk scoring techniques and optimization strategies tailored specially for network security. In further sections, practical implementations, case studies, and real-world applications are discussed. Later sections of the research will tackle challenges and limitations. Then the paper is concluded with a summary of findings and recommendations. Lastly, future scope of the work is discussed.

II. BACKGROUND AND RELATED WORK

Artificial intelligence (AI) is really becoming a game-changer in the field of risk management, especially when it comes to organizational network security. Recent studies demonstrate the role of AI to effectively spot, detect, measure, and handle risks. AI Models learn from huge amounts of data and navigate complex environments. AI risk scoring refers to the process of assignment of numerical or categorical values to critical threats and vulnerabilities, which in turn helps organizations to focus their efforts and resources on really important matters [6] . On one hand, quantitative methods use mathematical and statistical models to figure out the probabilities of risks and impacts of risks. Qualitative methods, on the other hand lean on expert opinions and analysis of scenario to detect those subtle risks that might be overlooked by the raw data. Lately, hybrid approaches which is a blend of these methods are gaining popularity because they provide a view of risks from various aspects, combining insights which are data-driven with an understanding of the context in depth. AI's role in network security goes beyond the traditional signature-based detection techniques., AI allows to spot new threats like insider attacks and zero-day exploits. Machine learning (ML) algorithms dive deeper into patterns of network traffic, behaviors of users, and past incident data to detect anomalies that could signal a violation or breach [7]. Thanks to deep learning (DL) models, which excel at identifying subtle patterns and relationships that are complex. DL can help improve detection accuracy of threats while reducing false alarms [8] [9]. Network security teams are empowered by these advancements to act swiftly, proactively and effectively against tough emerging risks. This helps in reduction of potential damage and to keep operations running smoothly. Real-world examples show that AI outperforms manual or traditional methods especially in ever-changing network environments in maintaining high detection rates.

AI driven Optimization techniques play a crucial role in dynamically distributing resources of network security to reduce risks effectively. These techniques assess vulnerabilities on the basis of risk scores which allows for a focused defenses application where potential breaches could have the impact to a significant extent. AI also enhances bandwidth distribution, traffic routing, and system settings, boosting both performance and security at the same time. With predictive analytics, network failures and security threats can be anticipated which in turn enables proactive measures [10]. These optimizations cut operational costs by automation of routine decisions and also enhance experience of user by ensuring reliability and responsiveness of system, even under changing conditions. Threat detection and response automation through AI techniques marks a significant shift in our approach to network security. AI systems are not dependent on manual investigations and reactions, instead AI systems relies on continuous monitoring of real time network activity. This leads to automatic analysis of alerts, confirmation of threats, and initiation of remediation processes [11] . Incident response becomes faster by integrating AI techniques with existing frameworks of security like intrusion detection systems (IDS) and platforms of security information event management. It allows security teams to focus on strategic risk management. This automation leads to reduction of vulnerability windows and strengthening of overall security posture.

Explainable AI models are also becoming increasingly crucial in the realm of risk scoring and optimization of network security, as they are capable of tackling the important issues of transparency and trust [12]. It is essential for security teams to grasp the reason of AI identifying certain activities as critical or risky, especially while implementing automated controls that have direct effect on network operations. Research is diving into the methods that make decisions of AI more interpretable, such as attribution of features and visualization of model, which assist security analysts in validating insights of AI with their own expertise. Such transparency level is vital to meet regulatory requirements and also aids in making informed decisions which ultimately results in reducing dependence on opaque models. However, despite the potential benefits, the AI integration in network security has its own limitations and hurdles. The quality and data availability are paramount, since incomplete, biased, or outdated training datasets can distort risk assessments and can undermine defenses. Additionally, scalability issues can also arise in organizations having large and diverse networks as they find it challenging to smoothly implement AI tools across their systems. Above all, the growing use of AI by malicious agents or cybercriminals to create adversarial examples increases complexity of threat detection. This highlights the need for efficient and robust AI models that can withstand any manipulation by wrong entities. Ethical issues surrounding fairness, privacy, and accountability also demand for continuous focus to ensure the responsible deployment of AI.

Various frameworks have been introduced for helping organizations in effectively implementing risk scoring and optimization that is AI-driven. The AI Risk Management Framework of NIST lays out the policies for governance, processes and metrics that are important and crucial for using AI in a manner that is trustworthy within security applications. It also stresses the relevance of ongoing evaluation thorough documentation of risk and stakeholders collaboration to maintain a balance between innovation and management of risk. The aim of other approaches is to weave AI insights into organizational risk management and compliance strategies at a broader aspect which ensures that the role of AI is to enhance rather than complicate governance of cybersecurity. Recent research points towards exciting avenues that could aid in further elevation of AI-powered network security. These avenues include hybrid models that is a combination of AI and human expertise, multi-layered systems of defense where AI is integrated across various endpoints and different cloud resources, and real-time learning systems which are adaptive and can modify policies of security on the go. Innovations in privacy-preserving AI techniques and federated learning might allow for sharing of threat intelligence across different organizations without putting sensitive and crucial data at risk. All these advancements throw a light on picture of a future where AI is helpful in significantly boosting the accuracy, agility and resilience of defense of network for organizations. This detailed survey further highlights how risk scoring and optimization methods that is AI-powered have become essential tools in tackling the intricate challenges of cybersecurity faced by organizations. To fully harness the capabilities of such methods in the face of operational hurdles and ever-changing threats, strategic application and ongoing innovation will be crucial.

III. AI-POWERED RISK SCORING TECHNIQUES

A. Quantitative Risk Scoring

In quantitative risk scoring AI and machine learning(ML) are leveraged to assign numerical values to risks of cybersecurity. This approach helps the organizations in measuring and prioritizing threats by analysis of vast amounts of data, including vulnerability reports, network logs and threat intelligence. Various factors are taken into acount such as exploitability, asset sensitivity, threat severity and the lateral movement potential. By automation of the analysis process, human error is minimized and assessments are ensured to remain up-to-date. The key advantages include the gain of predictive insights from both real-time and historical behavior, which in turn allows for proactive mitigation of risk before escalation of problems. This automation also aids in the enhancement of resource allocation and sharpening the focus on incident response. With increasing complexity of digital environments, quantitative risk scoring that is AI-driven provides a flexible, scalable and cost-effective solution for management of risks in hybrid and multi-cloud systems.

B. Qualitative Risk Assessment Methods

Methods for qualitative risk assessment also play a vital role alongside quantitative risk assessment approaches by capturing the subtle and context-specific risks which are tough to pin down numerically alone. AI plays a crucial role in enhancing these methods by combining together scenario analyses, expert opinions, unstructured data, incident reports, policy documents threat assessments through natural language processing (NLP) and behavioral analytics. This powerful and impactful combination allows organizations to identify the faint signals of behavior that is questionable, evaluate the impact of potential threats on their business operations and reputation, and to craft response plans that are flexible. Different dimensions of qualitative risk assessment is shown in figure 1.

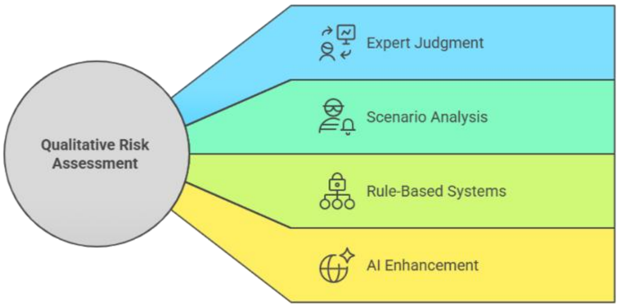

Figure 1: Qualitative Risk Assessment Dimensions

AI-driven qualitative assessments assist companies to spot compliance gaps, produce audit-ready reports, suggest solutions while bolstering their security governance and meeting regulatory standards. By weaving of qualitative data into frameworks of AI risk scoring, organizations gain a more nuanced and richer understanding of their landscape related to risk. Hybrid systems blend quantitative metrics with qualitative ratings and adjust scores in real-time which are based on the latest threat intelligence and stakeholders feedback. Explainable AI (XAI) methods take security a step further by providing clear insights to the security analysts on how AI makes its decisions. This in turn promotes transparency in governance. AI-driven qualitative assessments empower the organizations to tackle emerging threats of cybersecurity and reduce operational burdens. It also aids them to stay resilient against zero-day exploits, advanced persistent threats and insider attacks.

C. Hybrid Scoring Models

Hybrid models for risk scoring blend qualitative and quantitative techniques for providing thorough and context-sensitive assessments of risk. With these models, ensemble AI algorithms are leveraged to merge numerical analysis of data with insights from experts. This helps organizations in striking a balance between real-world experience and statistical reliability. For instance, a hybrid risk scoring system might begin with a baseline risk score that is derived from quantitative analytics and then the score is adjusted based on qualitative elements such as new regulatory changes or evolving threat actor profiles. This ongoing loop of feedback provides a guarantee of risk evaluations in staying relevant, precise and in tune with the goals of an organization. Hybrid approaches also supports in facilitating customized risk frameworks which are tailored to threats that are industry-specific, organizational risk tolerances and compliance requirements. AI systems also learn from past mitigation failures and successes. Thus, retraining scoring parameters in reflecting the evolving landscape of security. The use of hybrid models aids in improving operational decision-making, guiding the security teams to prioritize incidents that pose real danger and threat while avoiding alert fatigue. Hybrid AI risk scoring methods maximizes the transparency, trustworthiness and effectiveness of cybersecurity strategies, support proactive defenses and continuous improvement of complex digital environments. Figure 2 depicts hybrid risk scoring power.

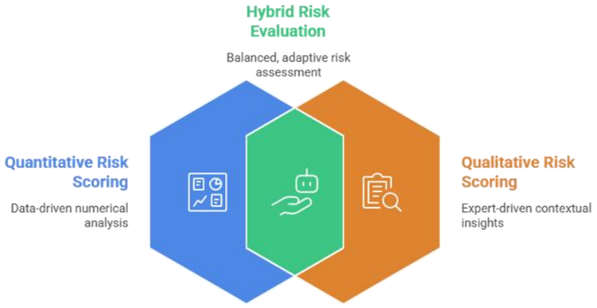
Hybrid Risk Evaluation
Balanced, adaptive risk assessment
Quantitative Risk Scoring
Data-driven numerical analysis
Qualitative Risk Scoring
Expert-driven contextual insights

Figure 2: Hybrid Risk Scoring Power

IV. OPTIMIZATION STRATEGIES FOR NETWORK SECURITY

A. AI-Driven Predictive Analytics

AI-driven predictive analytics has revolutionized the way of optimization of network security. It empowers organizations in spotting, predicting and tackling potential threats and performance hiccups before they emerge as serious issues. By constant gathering and analyzing a huge amount of network data like device performance, traffic patterns and user behaviors, AI and ML models can pick up on anomalies that are subtle, foresee future congestion of network and anticipate incidents of security with accuracy that is impressive. These systems continuously learn from both real-time data and past data which in turn enables them in predicting bandwidth needs, identifying new attack vectors and suggesting or even automating preventive measures such as deploying patches, reallocating bandwidth or isolating devices. This has resulted in significant shift of network management from reactive to proactive, where problems are resolved prior to affecting users. This has led to less downtime, better reliability and a stronger stance of security. In addition to this, predictive analytics also aids in strategic planning by providing actionable insights for infrastructure investments and capacity planning, ensuring networks to stay resilient and be prepared for whatever challenges that come their way.

B. Resource Allocation and Risk Prioritization

Resource allocation and prioritization of risk are essential strategies that utilize risk scoring techniques driven by AI to ensure that security resources are allocated in an optimized manner. AI systems extract and combine together data from different sources namely vulnerability scanners, external threat intelligence and endpoint protection platforms to create risk scores dynamically for user activities, network assets, and incidents. These risk scores assist security teams to zero in on the most critical vulnerabilities and threats, automate actions of patch deployment, enhance monitoring and isolating high-risk assets temporarily. AI prioritization lightens the work load for analysts and ensuring the optimized use of limited resources by constant updating of risk assessments based on new information. This method not only leads to boosting of operational efficiency but also helps in compliance by offering clear and auditable records of decision-making based on risk. This aids organizations in showcasing their due diligence to stakeholders and regulators.

C. Adaptive and Dynamic Defenses

Adaptive and dynamic defenses in network security mark a major leap forward. They leave behind the old static and rule-based controls. They evolve in real time by continuous monitoring and analysis of activity of network and threat intelligence. With the assistance of AI, security systems can automatically tweak configurations, policies and access controls whenever anomalies or new threats are spotted by them. When something suspicious is detected, AI-driven systems can swiftly block harmful traffic, enforce stricter access controls or isolate affected endpoints, which leads to significant cuts down of response times and minimization of damage. These adaptive defenses are thriving on continuous feedback loops, continuous learning from every incident to improve strategies for detection and response, ensuring synchronization of security measures with organizational goals and the ever-changing landscape of threat.

D. Integration of AI-Powered Tools in Security Infrastructure

Combination of AI-powered tools into current security setup is very crucial for unlocking of the full potential of optimization strategies for network. Today's organizations often deal with a variety of security solutions namely intrusion detection and prevention system, SIEM platforms, firewalls and endpoint protection tools. AI acts as a cohesive layer that extracts together data from various sources and coordinates responses in an effective manner. For achievement of successful integration, it is important to ensure orchestration platforms, standardized data formats and interoperability through APIs. This approach allows for transparency, centralized visibility and a very efficient incident response. AI tools can easily take over repetitive tasks of alert triage and data enrichment. It gives freedom to human analysts to dive into strategic planning and more complex investigations. With time, these systems adapt based on feedback of analyst and operational results. This leads to continuous enhancement of their ability to highlight critical incidents, filter out the noise and grow also alongside the organization. This ensures security measures to stay flexible and strong even if challenges and threats evolve.

V. IMPLEMENTATION IN ORGANIZATIONAL NETWORKS

A. Integration of AI-Powered Risk Scoring Tools

AI-powered tools for risk scoring in organizational networks requires a careful mapping of AI systems which are often guided by frameworks like the AI Risk Management Framework (AI RMF), NIST and ISO/IEC

42001. It is the need for organizations to pinpoint regulatory, operational and ethical risks across their systems powered by AI. It can be achieved by using structured methods for accurate categorization of these risks. Frameworks of AI risk scoring work by integration of existing security infrastructure, such as vulnerability scanners and SIEMs, which allows for dynamic and real-time risk evaluations which include both qualitative and quantitative assessments. For instance, risk scores that are AI-driven break down risks into different components, including compliance, cybersecurity, financial and operational risks, offering transparency in detail and helps in prioritization of resource allocation. The process of integration typically employs APIs (Application Programming Interface) and standardized data formats for maintaining centralized visibility and ensuring a smooth data flow. It's also crucial and important for security teams to receive ongoing training on ways to interpret AI insights, along with updates and regular audits of AI models to keep risk scoring process transparent, effective and in line with changing regulatory and business requirements. AI-Powered composite risk scores by assets are visualized in figure 3 and figure 4.

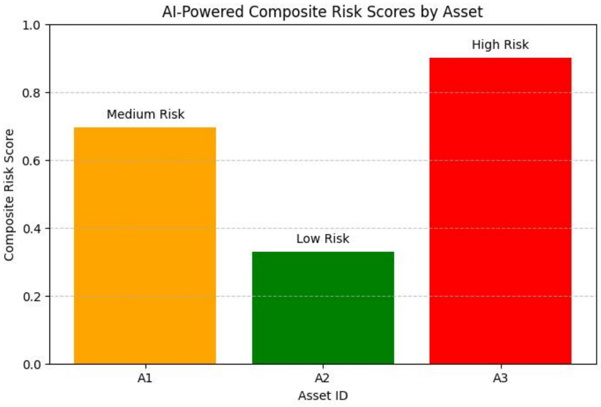

Figure 3: AI-Powered Composite Risk Scores by Asset

Automated risk scoring tools are effective in quantifying risk levels, classifying of assets into high, medium or low-risk tiers by considering factors namely criticality of asset, exploit frequency, and compliance status. By this, organizations are enabled to proactively manage and address critical vulnerabilities with metrics that drive workflows which are automated. By alignment of dynamic AI risk frameworks, organizations are able to ensure robustness and real-time risk management that adapts to evolving system contexts and new threats.

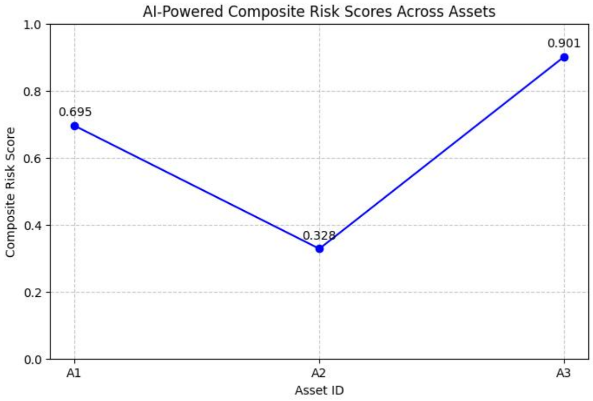

Figure 4: AI-Powered Risk Scores Across Assets

B. Integration with Security Infrastructure and Workflows

Integration of AI-powered risk scoring seamlessly with the current setup of security and workflows is crucial and essential to unlock its full potential and make a real impact. This involves extracting and gathering together data from various sources such as intrusion detection systems(IDS), firewalls, cloud services and endpoint protection through standardized interfaces to create a real-time and comprehensive snapshot of the network. The AI-generated risk scores are integrated into automated workflows of security which in turn allows for quick actions such as escalating incidents, isolating devices or deploying patches while popping up of high-risk activities. By connecting with platforms of governance, risk, and compliance (GRC), these risk scores aid in shaping of regulatory reports and audit trails and ensures compliance with standards like HIPAA, NIST and GDPR. Continuous monitoring and feedback loops helps security teams to assess tweak thresholds, automated actions and refine integration points. This keeps AI-driven risk scoring process agile and responsive to both internal shifts and the ever-changing landscape of threat.

C. Case Studies and Real-World Applications

Real-world applications of AI-driven risk scoring can be seen across various sectors like healthcare, finance and critical infrastructure, each showcasing its own set of hurdles and advantages. In the world of finance, AI platforms need to keep a close eye on network activity and transactions, assigning risk scores dynamically to spot cyber threats and any fraud. Quick action needs to be taken to minimize losses. Meanwhile, in healthcare sector, organizations leverage AI to sift through device usage and access logs, prioritizing incidents according to their potential impact for safeguarding sensitive information of patient and maintain regulatory compliance. In the sector of manufacturing, AI tools keep tabs on analyzing sensor data, industrial control systems, allocate risk scores and communications to foresee failures. This helps in prioritizing maintenance and avoiding downtime. Adaptable AI-powered risk scoring can be used for customizing solutions to fit industry needs that are specific.

D. Continuous Improvement, Compliance, and Future Directions

For effectiveness of AI-powered risk scoring, it is necessary to commit to the ongoing improvement, embrace innovative thinking and stay compliant with regulations. Regular review cycles should be set up by the organizations to evaluate the performance of their AI models, update criteria of risk and bring new threat intelligence. Risk scoring thus stays relevant and accurate. Maintaining compliance with industry regulations and data privacy laws involves routine audits, clear documentation and alignment with standards like ISO/IEC and NIST. Organizations should also consider using advanced analytics like explainable AI and federated learning for boosting transparency, collaboration, and trust in risk assessments which are automated. Ultimately, the key for successful implementation lies in a blend of flexible processes and strong technology for fully leveraging the advantages of security that is AI-driven in a constantly changing landscape of threat.

VI. CHALLENGES AND LIMITATIONS

AI-powered network security also has its own set of major challenges of data privacy and ethical concerns, especially under regulations of GDPR and CCPA. Organizations must ensure transparency and secure handling of data that is sensitive for avoiding any legal and trust issues. Ethical problems such as unexplainable security actions and bias might arise due to lack of transparency in AI decision-making. AI models are also vulnerable to adversarial attacks. Here the malicious inputs are able to bypass detection and reduce reliability. Adversarial hardening and continuous retraining are necessary but are also resource-intensive. Integrating AI into existing infrastructure of security often requires complex APIs and middleware, adding to costs for implementation and need for skilled professionals. False negatives and positives further complicate adoption which makes it crucial in balancing AI automation with regular model validation and human oversight and to maintain effectiveness and accountability.

VII. CONCLUSION

AI-driven risk scoring methods and optimization techniques have truly marked a transformation on the way organizations approach security of network. Teams are empowered to allocate resources dynamically, detect threats proactively and automate incident responses. There are significant advantages such as scalability, enhanced accuracy and operational efficiency that help organizations in staying a step ahead of cyber threats that are ever-evolving. Yet, embracement of AI in cybersecurity has its own set of hurdles. Issues of ethical questions, privacy concerns, adversarial vulnerabilities and the complexities of AI integration demands careful attention for unlocking the full potential of AI techniques and solutions. Achievement of success demands for a thoughtful balance of clear governance, strong technical safeguards, skilled human oversight and ongoing model enhancements. These challenges directly need to be tackled so that organizations can create adaptable and resilient security frameworks. Such frameworks can uphold stakeholder trust and safeguard vital assets in a rapidly changing world of digital era.

VIII. FUTURE SCOPE

Looking ahead at the future of AI-driven network security, it is set to be majorly influenced by breakthroughs in explainable AI (XAI), privacy-focused analytics and federated learning. These advancements will aid organizations in working together and sharing threat intelligence while taking safety of sensitive data into consideration. AI in combination with cutting-edge technologies like quantum computing and blockchain holds the promise of enhanced security and resilience. Since cybercriminals are becoming more adept in using AI techniques for complex attacks, it's crucial and need of the hour to continue researching ethical AI practices, adversarial robustness and ongoing training for professionals of cybersecurity. For future, AI is definitely poised to become a great solution for monitoring and response in real-time, paving a way for the development of zero trust models and thus helping organizations in creating more adaptable, secure, and future-ready environments for cybersecurity.

REFERENCES

[1] R. Gupta and P. Srivastava, "Artificial intelligence and machine learning in cyber security applications," in *Cyber Security Solutions for Protecting and Building the Future Smart Grid*, D. Asija, R. Viral, R. Das and G. Tuna, Eds., Elsevier, 2025, pp. 271-296.

[2] M. Danish and M. M. Siraj, "AI and Cybersecurity: Defending Data and Privacy in the Digital Age," *Journal of Engineering and Computational Intelligence Review,* vol. 3, no. 1, pp. 25-35, May 2025.

[3] K. Dhanushkodi and S. Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," *IEEE Access,* vol. 12, pp. 173127-173136, 2024.

[4] I. Zografopoulos, J. Ospina, X. Liu and C. Konstantinou, "Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies," *IEEE Access,* vol. 9, pp. 29775-29818, February 2021.

[5] J. Jacobs, S. romanosky, B. Edwards, I. Adjerid and M. Roytman, "Exploit Prediction Scoring System (EPSS)," *Digital Threats: Research and Practice,* vol. 2, no. 3, pp. 1-17, July 2021.

[6] F. H. Alshammari, "Design of capability maturity model integration with cybersecurity risk severity complex prediction using bayesian-based machine learning models," *Service Oriented Computing and Applications,* vol. 12, no. 1, pp. 59-72, March 2023.

[7] T. Zhukabayeva, A. Pervez, Y. Mardenov, M. Othman, N. Karabayev and Z. Ahmad, "A Traffic Analysis and Node Categorization- Aware Machine Learning-Integrated Framework for Cybersecurity Intrusion Detection and Prevention of WSNs in Smart Grids,"

IEEE Access, vol. 12, pp. 91715-91733, July 2024.

[8] F. R. Alzaabi and A. Mehmood, "A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods," *IEEE Access,* vol. 12, no. 1, pp. 30907-30927, February 2024.

[9] M. A. Hossain and M. S. Islam, "Enhanced detection of obfuscated malware in memory dumps: a machine learning approach for advanced cybersecurity.," *Cybersecurity,* vol. 7, no. 1, p. 16, 2024.

[10] A. Yeboah-Ofori, S. Islam, S. W. Lee, Z. U. Shamszaman, K. Muhammad and M. Altaf, "Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security," *IEEE Access,* vol. 9, pp. 94318-94337, June 2021.

[11] A. Tanikonda, B. K. Pandey, S. R. Peddinti and S. R. Katragadda, "Advanced AI-Driven Cybersecurity Solutions for Proactive Threat Detection and Response in Complex Ecosystems," *Journal of Science & Technology,* vol. 3, no. 1, pp. 196-217, January 2022.

[12] Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun and F. Taher, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," *IEEE Access,* vol. 10, no. 1, pp. 93104-93139, September 2022.