International Journal of Emerging Engineering and Technology (IJEET)
ISSN (e): 2958-3764
Volume: 4, Number: 2, Pages: 111 - 117, Year: 2025

AI-Driven Dynamic Risk Management in Cybersecurity

Abaidullah Butt[1,*], Irshad Ahmed Sumra[2], Muhammad Sohail Athar[2], Malik Adnan[1]

[1]Department of Artificial Intelligence, School of Systems and Technology, University of Management & Technology, Lahore, 54000, Pakistan
[2]Department of Informatics and Systems, School of Systems and Technology, University of Management & Technology, Lahore, 54000, Pakistan
* Corresponding author: Abaidullah Butt (Email: aabaidullahbutt@gmail.com)

Received: 07/08/2025, Revised: 17/11/2025, Accepted: 13/12/2025

***Abstract*—Because of the growing technological sophistication of companies, the threat of attacks grows, and static risk assessments can no longer meet the requirements. AI-powered systems can provide real-time detection capabilities, but the "black box" nature of the technology makes it difficult to ensure their adoption and to justify their financial cost. This brings the need for transparency and explanations of how AI works in cybersecurity, so that organizations can better comprehend, validate, and rely on AI's intelligent decision-making. The survey assesses recent progress in explaining AI (XAI) in dynamic cybersecurity risk management in critical infrastructure systems such as 5G and banking. We examine techniques from LLM-based vulnerability prioritization to hybrid cascading risk models. This paper outlines how recent frameworks have leveraged multiple datasets, such as EPSS and CISA KEV, to enhance remediation efficiency by up to 95%. Unlike existing surveys, this paper provides a unified review of explainable AI, dynamic cybersecurity risk management, governance, and cyber insurance. It also highlights existing research on these fields, explores practical implementation issues like computational needs, data protection, and model generalization, and proposes future research avenues to create not only transparent but also trusted frameworks for mitigating cyberattacks using AI techniques. The analysis further demonstrates that XAI tools such as SHAP and LIME are essential for the financial health of cybersecurity. Lastly, attention must be given to changing the auditable logic to make technical evidence measurable and insurable.**

***Index Terms*—Explainable AI, Cyber Insurance, Dynamic Risk Assessment, Vulnerability Prioritization.**

I. INTRODUCTION

Today, organizations heavily depend on digital systems to perform normal activities. The paper suggests that cybersecurity doesn't exist as simply a technical issue – one that was used to safeguard computers – but as an essential survival issue for today's businesses [1]. As companies become more technologically advanced, the risk of attacks increases. This means the subject becomes more concerning, particularly as companies begin to look to cyber insurance to address what they can't fix or avoid [2]. Conventional risk evaluation works very slowly, like a yearly audit, and attackers are continuously evolving. This much delay makes old defense strategies virtually useless [3]. Not only can financial losses be incurred due to weak security, but operations can be disrupted, and the company's integrity can be damaged as well [4]. Attacks are dynamic, constantly changing, and continuously increasing in number and sophistication in assaults on weaknesses that are known and new vulnerabilities that are not known. This old-fashioned approach is inadequate for traditional security threats.

It is a game of management technique that's not haunted anymore. There were weak points in the old days, and the effect of them was known, and preventive actions were undertaken. However, the cybersecurity market is constantly evolving. Systems change all the time, with new vulnerabilities being discovered and new attack techniques being created. Because of this, risks are assessed by traditional methods only at a specific period of time, and major security updates are often missed by them; using those techniques is no longer efficient. And now the industry is facing difficulties with the “black box” logic [5]. An AI system can flag a system as at risk but not explain why, making it difficult for security analysts to justify blocking an account or making a major investment. This widespread disappointment has made Explainable AI (XAI) a central theme [5].

The implicit framework is intended to be clarified so that security teams can confirm that the model is actually identifying security threats, rather than just meeting them by chance. For organizations, a strategy to maintain the momentum and work is essential to keep them in real time. Cybersecurity insurance has been gaining popularity [4] as techniques to shield finances against cyberattacks have been examined by organizations. Basically, the theory is streamlined, and companies pay a healthy premium to transfer some of the financial risk to the insurance provider rather than bearing it entirely themselves. However, multiple constraints are faced in this process. Cyber risks are often imprecisely assessed by insurance companies, largely due to the frequent lack of valid historical data, and many organizations can be affected by cyber risks concurrently [4]. At the same time, cyber risks can badly affect many organizations [1]. Moreover, the evolving cybersecurity threats are hard to identify and evaluate. In contrast, the expertise of security systems is often badly demonstrated by organizations. Mis-predict policies can lead to these discrepancies, which is risk modeling, resulting in over-insurance or coverage gaps that are compromising the stability

of the cyber insurance market. It has been reported that these issues can be mitigated by machine learning and large language models (LLMs). Vast, diverse datasets can be analyzed by them to generate more accurate, real-time risk assessments. The study uses the Pearson correlation coefficient to filter out unnecessary duplicate input features [6]. This allows us to identify and eliminate linear relationships and clearly understand the information in the feature set, while excluding non-correlated information that could otherwise bias the model. Now it is no longer a limitation that snapshots are out of date; the risk assessment can be kept up to date, and consistent results can be delivered instead of merely receiving occasional status updates. Despite its progress, AI still has significant issues, many of which are often ignored. The biggest challenge is that these systems are independent, and the methods by which their answers are reached are not understood by anyone. It is a process in which the input and output are observable, but the steps between them cannot be seen. Vital information on how the answer is formed is missing, and steps are masked. These are perceived as problematic in a field such as this. The decision-makers want to know why, when something is identified as high risk by the system, or when a particular security action is recommended by the system.

The output of a model can only be inspected after the input data are thoroughly analyzed. Security data sets usually consist of features that are very similar, such as packet lengths or byte counts. Multicollinearity arises when two variables, which measure the same behavior, are near each other. This may cause the AI to double-count evidence when calculating, resulting in skewed outcomes and ratings. Thus, the objectivity of the input must be considered crucial, not merely repeated evidence. They can help with this, such as tools like SHAP [7], or feature importance and correlation analysis, which reveal the reasoning of the AI, and what makes a difference to its decisions. When the reasons for decisions are made visible, it is much easier to build trust in the system and understand the reasons behind the decisions.

This paper aims to fill the gap by offering a comprehensive assessment of the latest developments in explainable AI applications for dynamic cybersecurity risk management, particularly in cyber insurance. It highlights key developments in dynamic risk assessment, the use of AI and large language models in vulnerability analysis, and the current use of XAI techniques in cybersecurity. It also provides insight into how these factors can be combined to improve the process of making insurance decisions. Through a review of current research, this paper characterizes the problems of today, presents a helpful blend of methods, and proposes some future paths to solve these problems by making the solutions more reliable, transparent, and useful.

This paper narrows this focus to a single approach that combines the concepts of Explainable AI (XAI), dynamic cybersecurity risk management, and cyber insurance decision-making in a single package. It further summarizes the latest approaches by AI technologies and discusses explainable techniques, including SHAP and LIME, and their potential to gain transparency, governance, and trust in cybersecurity risk assessment. Moreover, it highlights the rapidly growing importance of “real-time” threat intelligence and regulatory mapping to support an auditable and insurable cyber practice.

The distinguishing value of this survey is that it comparatively analyzes the latest studies on combining vulnerability prioritization, explainability, governance, and cyber insurance. Many previously published reviews cover these subjects individually, but this book brings them together into a single focus and illustrates how AI-powered risk assessment can aid technical security operations and strategic finance decisions. The survey also identifies aspects of the ongoing research requirements, practical implementation challenges and provision of potential future direction of the evolution of transparent and trustworthy cybersecurity frameworks.

II. BASIC CONCEPT OF DYNAMIC RISK ASSESSMENT

The major challenge is that AI systems usually operate as black boxes, so it is difficult to understand the logic behind it. A snapshot of a network’s defenses is offered by them that effectively becomes a liability the moment a zero-day exploit is weaponized by an antagonist. The “unknown, the unknowns” that emerge between audit cycles cannot be predicted by them, so assessments often abandon organizations defending against yesterday’s threats. A transition to a six-phase operational loop is facilitated for organizations by the reviewed methodology [1].

The shift toward a dynamic approach requires a fundamental change in the operational workflow of an organization. As shown in Fig. 1, the modern risk management lifecycle is no longer a linear path but a continuous loop. This cycle ensures that once assets are identified and prioritized, the resulting "Residual Risk" is used to inform financial decisions, specifically regarding cyber insurance procurement [1], [8]. By maintaining this circular feedback, organizations avoid the trap of "stale audits" and ensure that their security posture evolves at the same speed as the threats themselves [3], [9].

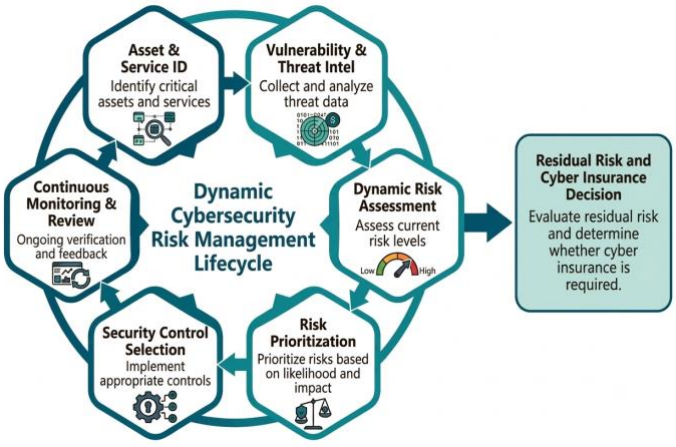

Fig. 1. Dynamic cybersecurity risk management lifecycle.

Figure 1 illustrates the dynamic cybersecurity risk management lifecycle. It starts with identifying assets and services, then collects vulnerabilities and threats, performs dynamic risk assessments, prioritizes risks, and chooses security controls. The residual risk, once covered, is used to inform cyber insurance decision-making, and the risk posture is continually monitored and reviewed to ensure it remains current with changes.

The operational lifecycle depicted in Fig. 1 is a paradigm shift in the management of uncertainty in modern organizations. This circular model takes a different view from the traditional linear process of identifying and compiling into a static report, keeping risk management an "always-on" process. In recent literature, the link between the 'Security Control Selection' and 'Residual Risk' is important [1], [8]. The researchers say the goal of the dynamic lifecycle is to "measure just how much that is not protected after they put controls in place." That "Residual Risk" is then quantified, and becomes the main data point for the last step in the process: the 'Cyber Insurance Decision.' This integration makes it possible to coordinate the financial aspects of a business with the technical reality of the entire 5G or industrial infrastructure, thereby minimizing the "adverse selection" problem, that is, the difference between the perception of a risk by a mandated insurance company and by the client [1], [4], [9].

A. Asset Contextualization and 5G Logic

The first step is to define "ICT Stack." The audit of the p-NET 5G infrastructure that was reviewed focused on a complete inventory of the ecosystem that included Cisco switching fabrics up to Oracle Linux host environments [1]. In order to give consistency to the terminology, each component was not just a list but was included in the NIST Common Platform Enumeration (CPE) standard [10]. The Common Criteria Security Functional Requirements (SFRs) are directly linked to physical assets [11] as reviewed in the risk model. This consistency for arguments means that each noted vulnerability in the reviewed study is analyzed according to the actual security needs set for that hardware or software level. The required "Business Logic" is given to the model by this relationship: a database kernel vulnerability is ranked higher by the model if the "O.DATA_INTEGRITY" objective of a mission-critical analytics service is impacted.

B. LLM-Driven Prioritization Engine

The following methodology, including the assets listed, is reviewed and uses CodeBERT, a specialized transformer trained on natural language and source code. The only model that can map the CVE description to the actual code patterns in the 5G stack is CodeBERT [10]. The architecture under review was tested by using the CVEjoin corpus [1], [11], which is a large data aggregator covering more than 200,000 different security exposures. The combined data set was used to feed the model with a statistically significant sample of the present threat landscape – instead of relying on limited or insufficient individual data sets. This training process would enable the system to learn from a rich history of documented flaws, and thus, reported risk predictions would be based on a deep knowledge of historical exploits.

The inner workings of this dynamic engine are shown in Fig. 2. The first step is the collection of dynamic security inputs, which are automatically gathered, including EPSS scores and threat intelligence [12]. These inputs are then fed into the "Dynamic Risk Assessment Engine," which calculates the risk level in real time. One of the important decision gates in the concept is "Is the risk level acceptable?" Automated actions to be taken in the event of a risk, for an acceptable level of risk. Otherwise, additional risk assessment and mitigation work is triggered. This process allows companies to concentrate their efforts on issues that are most important and minimizes the amount of manual work required [13].

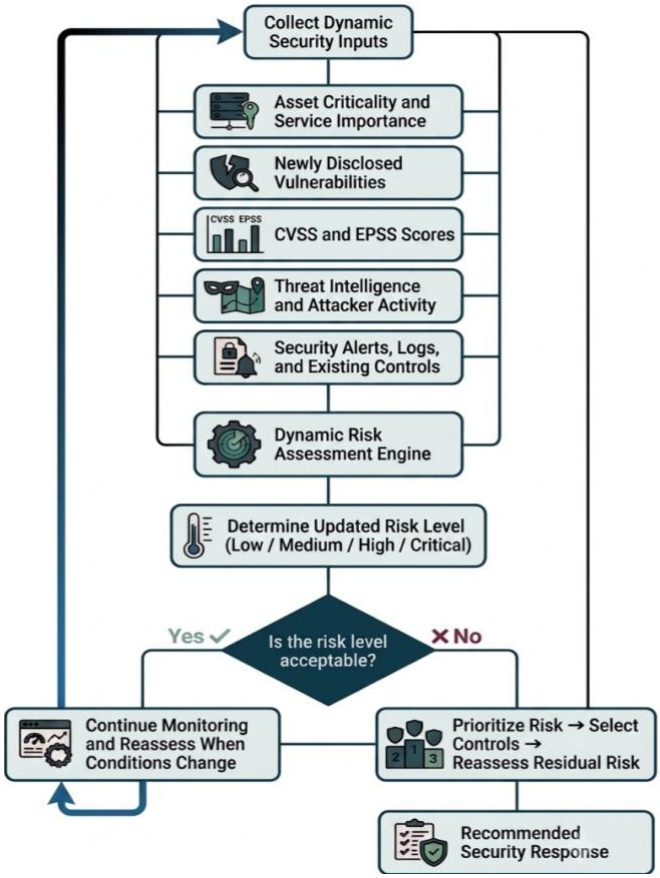

Fig. 2. Procedural flow of dynamic cybersecurity risk assessment.

Figure 2 shows a flow diagram of Dynamic Cybersecurity Risk Assessment. It starts with capturing dynamic security data like asset criticality, newly discovered vulnerabilities, CVSS and EPSS [12] scores, CISA Known Exploited Vulnerabilities (KEV) intelligence [14], security alerts, logs, and legacy controls. The dynamic risk assessment engine processes these inputs to calculate the new risk level (low, medium, high, or critical). The next security decision is to accept the risk (the risk acceptability decision gate) or to move on to prioritization of risks, selection of security controls, reassessment of residual risks, and a recommended security response. This workflow illustrates how real-time intelligence and automated decision logic can assist with more rapid, structured, and evidence-based cybersecurity risk management.

According to Shimizu et al. [13], the proposed Vulnerability Management Chaining framework substantiates the reported reduction in remediation workload. Experimental results on a dataset of 28,377 real-world vulnerabilities, using a combination of CVSS, EPSS, and KEV intelligence sources, showed an average reduction of about 95% in workload and a maximum reduction of 96.9%, while maintaining high vulnerability coverage at 85.6%. The results show that

prioritizing vulnerabilities in an effort-driven manner can be effective in significantly decreasing the number of analysts' efforts required, as well as increasing the operational efficiency without a noticeable impact on the number of vulnerabilities covered. This helps security analysts not to suffer from 'alert fatigue' and focus on vulnerabilities for which there are known paths of attack, bringing the distance between vulnerability and weaponized attacks down.

III. INTERPRETABLE ARCHITECTURES IN CYBERSECURITY

In order to be used in consequential environments, such as defense, the Artificial Intelligence systems need to be more understandable than the "black box" systems as they are right now[5]. When implemented, the framework reviewed in [1] would seek to align with those two principles: feature interaction validation, individual attribution—this does not necessarily mean a simple "low risk index" would satisfy the requirement of a Security Operations Center (SOC) lead (or insurance evaluator) for whom they would expect a "body of evidence."[1].

A. Statistical Input Integrity: Pearson Correlation

A survey is no way to validate a model's output if it's not sensible to have the objectivity of the data sources validated. One problem commonly encountered in security datasets is known as the mirroring effect of features, e.g., the byte counts and packet lengths are typically correlated. Because the variables are so tightly connected, sometimes the algorithm will overestimate the significance of one of the behavioral signals. To avoid this type of bias, vision must be reflected by the input features rather than the same information being repeated. The Pearson correlation coefficient is used for the reviewed study to determine linear dependencies [1], [6].

B. Causal Attribution: The SHAP Framework

To support a specific elevated risk, SHAP (Shapley Additive Explanations) is employed [7]. Sentence-BERT models are widely used for semantic similarity and attack mapping [15], [16]. Developed from the cooperative game theory, in which team members collaborate to earn a prize, each technical feature is considered a "player" in a game, whose "payout" is the final risk prediction. SHAP considers the "marginal contribution" of a feature for all possible subsets of the other features, rather than just the importance from a simple weight standpoint.

IV. THE ROLE OF EXPLAINABILITY (XAI) IN DYNAMIC RISK MANAGEMENT

The "black-box" problem in the context of cybersecurity refers to the fact that while AI systems can generate risk scores, the underlying logic or rationale behind the score is often opaque and may not be understandable to the user. Recent publications highlight the need to be able to explain dynamic risk management [1], [9]. This transparency is essential for security analysts who need to defend emergency patching or for insurance underwriters who need to determine insurance premiums based on facts and figures [1], [4].

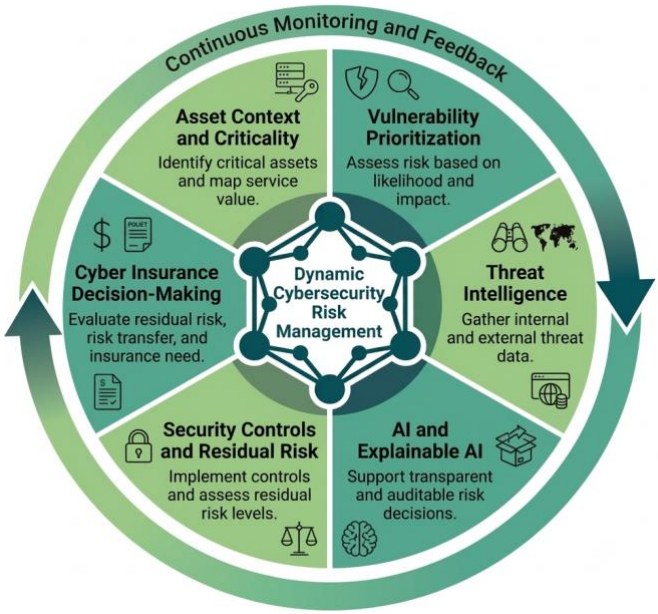

Fig. 3. Key dimensions of dynamic cybersecurity risk management.

Figure 3 shows the key dimensions of dynamic cybersecurity risk management. It demonstrates that the effectiveness of risk assessment relies on asset context and criticality, prioritizing vulnerability, threat intelligence, explainable AI, security controls, the evaluation of residual risk, and the decision-making process for cyber insurance. The continuous monitoring and feedback loop suggest that cybersecurity risk management should not be a one-size-fits-all assessment anbutn ongoing process. It also emphasizes the importance of explainable AI in enhancing transparency, auditability, and usefulness in risk decisions by both technical security teams and cyber insurance stakeholders.

As shown in Fig. 3, "AI and Explainable AI" is one of the six elements of a contemporary cybersecurity framework. Explainability is the linkage between "Threat Intelligence" and "Security Controls" [4], [9]. When a model detects high risk, the reasons are auditable and transparent. If only the other elements are considered without this dimension, they cannot have an impact because there is no evidence.

Technical accuracy is not the only indicator of success, as recent studies point out [5], [9], and the focus has shifted to auditability. Organizations can identify specific aspects of a high-risk rating, like "Exploitability" or "Network Attack Vector", using these XAI techniques [1], [9]. The insurance industry's move from a prediction engine to a stability and claims-reducing mechanism is made possible by the creation of a "body of evidence" by researchers in the insurance industry [1], [17].

A. Causal Attribution and Decision Justification

Researchers utilize specific methodologies to provide both global and local insights into AI behavior:

Global Explanations: These tools, such as SHAP, are used to determine which factors are generally associated with risk for an infrastructure at the global level [7]. For 5G and industrial applications, it is suggested in the literature that exploitability scores (EPSS) and confidentiality impact are the most persistent attributes linked to high-risk categories.

Local Interpretability: Techniques such as LIME offer a local interpretation of a model, enabling responders to understand why a vulnerability was marked at a given moment and location [9]. This enables a "surgical" reaction to threats and gives analysts more time in resource-constrained environments [16].

B. Mapping AI Insights to Regulatory Standards

One of the main points in the research literature is the process of translating AI findings into human-readable security measures. Modern frameworks can automatically recommend mitigation strategies based on industry best-practice frameworks like NIST SP 800-53 [17], the MITRE ATTACK framework [16], [18], and the CIS Critical Security Controls [16]. This sets the foundation for bridging the gap between complex data science and operational security management.

C. Practical Deployment Challenges

While AI-based cybersecurity systems have many benefits, the reviewed studies also highlight some practical challenges. The more advanced models, such as CodeBERT and transformer-based models, come with a heavy price tag for training and deployment. Additionally, cybersecurity data may contain confidential details about an organization that could cause privacy and compliance concerns. Model generalization is another difficulty; models that are successful in one environment may not be as effective in another environment, industry, or threat setting [20]. Lightweight designs, privacy-preserving learning algorithms, and cross-domain validation can be used in future research to increase the system's acceptance in practice.

V. CRITICAL ANALYSIS OF RECENT STUDIES

This section evaluates the current state of research in AI-driven cybersecurity risk management. The analysis considers different methods for addressing the problems of scaling and explainability.

The comparative analysis of the recent AI-based cybersecurity risk management studies is shown in Table I. The basis of the comparison is the methods and working mechanisms proposed in each study, as well as the limitations and future directions stated by the authors. This table highlights some key research trends such as Explainable AI, Dynamic Risk Assessment, Vulnerability Prioritization, Cyber Insurance Support[21], and Governance-based Security Frameworks. It also identifies the typical limitations, including limited datasets, sector-specific validation, absence of a financial impact model, and generalization issues across various operational environments.

Synthesis of Comparative Findings: The combination of these studies, as presented in Table I, shows that the field of cybersecurity risk management research is characterized by certain trends. First, the traditional static risk assessment method is replaced with an AI-based, dynamic risk assessment method. In this method, the risk is monitored and dynamically updated based on the real-time intelligence sources [1], [8], [9], [18]. Most of the frameworks combine several sources of security intelligence, such as vulnerability databases, threat intelligence feeds, vulnerability/exploitability prediction metrics (EPSS), and catalogs of known exploited vulnerabilities to further refine risk prioritization and decision-making accuracy [16]. Moreover, explainability has become a key feature and not a nice-to-have; methods like SHAP and LIME have gained widespread popularity to boost the explainability, trust, and accountability of AI-driven cybersecurity systems [1], [7], [9], [19], [20-21]. A key emerging trend is the integration of AI-driven results with existing cybersecurity frameworks and standards, such as NIST SP 800-53 and MITRE ATT&CK, allowing organizations to convert analytical results into security controls that can be implemented [17], [18]. However, some weaknesses have been identified, such as quantification of financial impacts, reaction to new attacks, and verification in varied operational environments. The outcomes show that cybersecurity risk management approaches should be adaptable, easily interpretable, compliant with regulations, and able to offer actionable, understandable, and trustworthy decision guidance [1], [8], [9], [18].

VI. CONCLUSION

This survey reviewed the change from “snapshot” to AI-driven risk management. A recent study has demonstrated that incorporating real-time intelligence and explainability tools can be an effective solution to the so-called “black-box” problem. The evolution makes risk management a strategic governance process, rather than a technical triage process. Perhaps most importantly, these developments have created a direct connection between technical and financial risk transfer via cyber insurance. The focus has been on organizational trust based on logic that is clear and can be understood by human beings, with accuracy growing in this regard. However, there are still some problems to be addressed. Implementing AI-powered cybersecurity solutions can be challenging, particularly in resource-constrained environments. Also, cybersecurity datasets may contain sensitive data, posing privacy and compliance risks. Another difficulty is model generalization, as a model trained in a particular setting could not be as effective in other organizations and threat contexts. These are important areas of future research. Finally, explainable AI is the backbone of auditable and insurable AI cybersecurity. These flexible designs enable security roles to remain flexible and robust in the face of security threats.

FUNDING STATEMENT

The authors received no specific funding for this study.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest to report regarding the present study.

AUTHOR CONTRIBUTIONS

All authors contributed to the conception, literature review, drafting, and critical revision of this manuscript and approved the final version for submission.

DATA AVAILABILITY STATEMENT

Data is available on reasonable request.

INSTITUTIONAL REVIEW BOARD STATEMENT

Not applicable.

INFORMED CONSENT STATEMENT

Not applicable.

REFERENCES

[1] S. Papastergiou, N. Basheer, K. Lampropoulos, P. Verrios, and S. Islam, "Explainable AI based dynamic cybersecurity risk management for cyber insurability," *Int. J. Inf. Secur.*, vol. 25, no. 36, 2026, doi: 10.1007/s10207-025-01189-8.

[2] A. Refsdal, B. Solhaug, and K. Stølen, *Cyber-Risk Management*. 2015. doi: 10.1007/978-3-319-23570-7.

[3] S. Romanosky, "Examining the costs and causes of cyber incidents," *J. Cybersecurity*, vol. 2, no. 2, pp. 121–135, 2016, doi: 10.1093/cybsec/tyw001.

[4] M. Eling and W. Schnell, "What do we know about cyber risk and cyber risk insurance?," *J. Risk Finance*, vol. 17, no. 5, pp. 474–491, 2016, doi: 10.1108/JRF-09-2016-0122.

[5] C. Molnar, *Interpretable Machine Learning*. 2022. [Online]. Available: https://christophm.github.io/interpretable-ml-book/

[6] J. Benesty, J. Chen, Y. Huang, and I. Cohen, "Pearson correlation coefficient," *Noise Reduct. Speech Process.*, pp. 1–4, 2009, doi: 10.1007/978-3-642-00296-0_5.

[7] S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," presented at the Advances in Neural Information Processing Systems, 2017, pp. 4765–4774. [Online]. Available: https://proceedings.neurips.cc/paper/7062-a-unified-approach-to-interpreting-model-predictions

[8] Y. T. Y. Azura, M. A. Azad, and H. Ahmed, "An integrated cyber security risk management framework for online banking systems," *Complex Intell. Syst.*, 2025, doi: 10.1007/s42786-025-00056-3.

[9] S. Islam, "Intelligent dynamic cybersecurity risk management framework for organizational risk assessment," *J. Reliab. Intell. Environ.*, 2025, doi: 10.1007/s40860-025-00253-3.

[10] Z. Feng *et al.*, "CodeBERT: A pre-trained model for programming and natural languages," presented at the Findings of the Association for Computational Linguistics: EMNLP 2020, Association for Computational Linguistics, 2020, pp. 1536–1547. doi: 10.18653/v1/2020.findings-emnlp.139.

[11] R. Parente, "CVEjoin: A dataset of information security vulnerability and threat intelligence," *GitHub repository*. GitHub. [Online]. Available: https://github.com/rodrigoparente/cvejoin-security-dataset

[12] FIRST, "Exploit Prediction Scoring System (EPSS)." [Online]. Available: https://www.first.org/epss/

[13] N. Shimizu, "Vulnerability Management Chaining: An Integrated Framework for Efficient Cybersecurity Risk Prioritization," *ArXiv Prepr. ArXiv250601220*, 2025, [Online]. Available: https://arxiv.org/abs/2506.01220

[14] Cybersecurity and Infrastructure Security Agency, "Known Exploited Vulnerabilities Catalog." [Online]. Available: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[15] N. Reimers and I. Gurevych, "Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks," presented at the Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing, Association for Computational Linguistics, 2019, pp. 3982–3992. doi: 10.18653/v1/D19-1410.

[16] E. Sherif, "Connecting Cyber Incidents to MITRE ATT&CK Techniques Through an Integrated Cyber Catalog," *ArXiv Prepr. ArXiv260312455*, 2026, [Online]. Available: https://arxiv.org/abs/2603.12455

[17] Joint Task Force, "Security and Privacy Controls for Information Systems and Organizations," NIST, 2020. doi: 10.6028/NIST.SP.800-53r5.

[18] MITRE, "MITRE ATT&CK." [Online]. Available: https://attack.mitre.org/

[19] S. Slapničar, M. Axelsen, and M. Eulerich, "Cyber risk management: an illusion of a risk-based approach," *Schmalenbach J. Bus. Res.*, 2025, doi: 10.1007/s00187-025-00401-z.

[20] Sumra, I.A., Hasbullah, H., Ab Manan, J.-L.: Effects of attackers and attacks on availability requirement in vehicular network: a survey. In: International Conference on Computer and Information Sciences (ICCOINS2014), Malaysia, 3–5 June 2014.

[21] Sumra, I.A., Hasbullah, H.B., AbManan, Jl.B. (2015). Attacks on Security Goals (Confidentiality, Integrity, Availability) in VANET: A Survey. In: Laouiti, A., Qayyum, A., Mohamad Saad, M. (eds) Vehicular Ad-hoc Networks for Smart Cities. Advances in Intelligent Systems and Computing, vol 306. Springer.

TABLE I: Comparative analysis of the various mathods.

Author Name / Year	Proposed Method	Working of the Model	Limitation	Authors' Stated Solution
Papastergiou et al. [1] (2026)	Explainable-AI-based dynamic cybersecurity risk management for informed cyber-insurability decisions.	• Incorporates EPSS scores into CodeBERT. • Uses SHAP and correlation analysis. • NIST SP 800-53 control mapping.	• Impact not based on financial losses or reputation. • Not able to identify non-linear relationships. • Restricted to one pilot.	• Include financial loss and reputational damage. • Add LIME and counterfactual explanations. • Support zero-day exploit parameters.
Sherif et al. [16] (2025)	Operational Cyber-Risk Management with AI – Cyber Catalog.	• Links CIS Controls, MITRE ATT&CK, and SMART metrics. • Sentence-transformer maps incident narratives to techniques.	• Only covers historical events in English. • Requires regular training due to changing threats. • The map was determined to require manual review for low-confidence maps.	• Plugin designed for open-source host intrusion detection (HIDS). • Addition of NIST SP 800-53 control mappings.
Azura et al. [8] (2025)	A comprehensive cybersecurity risk-management system for online banking systems.	• 4 interrelated parts: Threat, Risk, Methodology, and Treatment Tasks. • Recognizes threat scenarios and bank assets.	Limited access to confidential banking information. • Exposures may be underestimated in public databases. • Limited amount of time for tool validation.	• Financial-sector emerging-threat data integration. • Automated risk-matrix calculations. • Sector-specific banking case studies.
Islam et al. [9] (2025)	A cybersecurity risk management framework that is intelligent, explainable, and interpretable.	• Hybrid linear-regression and deep-learning model. • SHAP and LIME give descriptions of model behavior.	• Very limited generalization to other datasets and models. • Restricted sector-specific cases. • Storing multiple types of data in a single source.	• Tune other models like gradient boosting and SVM. • Include source code and penetration-testing information. • Use broader sector-specific case studies.
Slapničar et al. [19] (2025)	Qualculation approach for cyber-risk measurement and management.	• Integration of qualitative judgement and quantitative measurement. • 27 in-depth organizational interviews.	• Limited generalizability because of qualitative design. • Cites a lack of leadership understanding and a lack of consistent metrics.	• Learn organizational influences on integration practices. • Replicate qualculation in other operational-risk scenarios.