JOURNAL OF MULTIDISCIPLINARY SCIENCES AND INNOVATIONS
VOLUME 5, ISSUE 02
MOPNTHLY JOURNALS
ISSN NUMBER: 2751-4390
IMPACT FACTOR: 9,08

DYNAMIC CYBERSECURITY RISK MANAGEMENT BASED ON EXPLAINABLE AI (XAI) AND LLMS FOR JUSTIFYING CYBERINSURANCE DECISIONS

N.B. Asrorova
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Samarkand Branch, Samarkand, Uzbekistan
asrorova0215@gmail.com

Abstract: Assessing cybersecurity risks is challenging due to dynamic threats, exploitation of vulnerabilities, and the constantly changing security context. Cyber insurance is an important tool for mitigating such risks. This paper proposes a dynamic cybersecurity risk management approach based on Explainable AI (XAI) and LLM, which evaluates risk levels in real time and ensures transparency in decision-making. Experimental results demonstrate 96.9% accuracy in identifying exploitable vulnerabilities and support informed cyber insurance decisions based on residual risk.

Keywords: XAI, LLM, Cyber Insurance, Dynamic Risk Management, Vulnerability

Introduction. The expansion of digital technologies has made cybersecurity a critical strategic concern for organizations. Cyber incidents not only lead to technical disruptions but also pose financial losses and legal liabilities, making systematic and proactive risk management increasingly urgent.

In the Republic of Uzbekistan, the Law "On Cybersecurity," adopted by the Legislative Chamber of the Oliy Majlis on February 25, 2022, along with the associated regulatory legal acts, currently imposes on organizations the responsibility to ensure information security, identify and assess cyber risks, and implement organizational and technical measures to mitigate them. These requirements underscore the importance of managing potential financial damages arising from cyber threats and highlight the need to consider cyber insurance as an additional instrument for financial risk management.

However, the effective implementation of cyber insurance requires an accurate and transparent assessment of an organization's actual security posture. Existing approaches primarily rely on static evaluations and insufficiently account for the dynamic nature of the security environment. Consequently, there is a growing need for modern risk management approaches based on explainable artificial intelligence (XAI).

This study proposes a dynamic cyber risk management approach based on XAI, aimed at supporting transparent and reliable justification of cyber insurance decisions.

Constrained risk management. Existing research has focused on managing cybersecurity risks and applying artificial intelligence (AI) technologies in the context of cyber insurance. Within the domain of dynamic risk management, approaches such as DRMRS, DCA, and DRA propose proactive risk assessment that accounts for both the probability and impact of threats. However, most of these methods rely on static or limited quantitative analyses and do not fully capture the dynamic security context or the residual risk after implementing security controls. This limitation complicates the scientifically grounded linkage of risk assessment results to insurance decision-making.

JOURNAL OF MULTIDISCIPLINARY SCIENCES AND INNOVATIONS
VOLUME 5, ISSUE 02
MOPNTHLY JOURNALS
ISSN NUMBER: 2751-4390
IMPACT FACTOR: 9,08

AI technologies, particularly large language models (LLMs) such as GPT and CodeBERT, are increasingly used for vulnerability detection and risk profiling. Nevertheless, much of the existing work focuses on individual attack scenarios or specific threats, such as ransomware, and does not adequately address the systematic and explainable connection between security measures and residual risk. While Explainable AI (XAI) enables transparent and interpretable decision-making, its integration into dynamic risk management and cyber insurance decision processes remains limited.

XAI-based solution. The proposed approach enables real-time identification and management of risks while allowing residual risks to be financially covered through cyber insurance. Key aspects include:

Identification of assets and services: All hardware, software, and operational systems within the organization are inventoried. The core business functions and their criticality are determined.

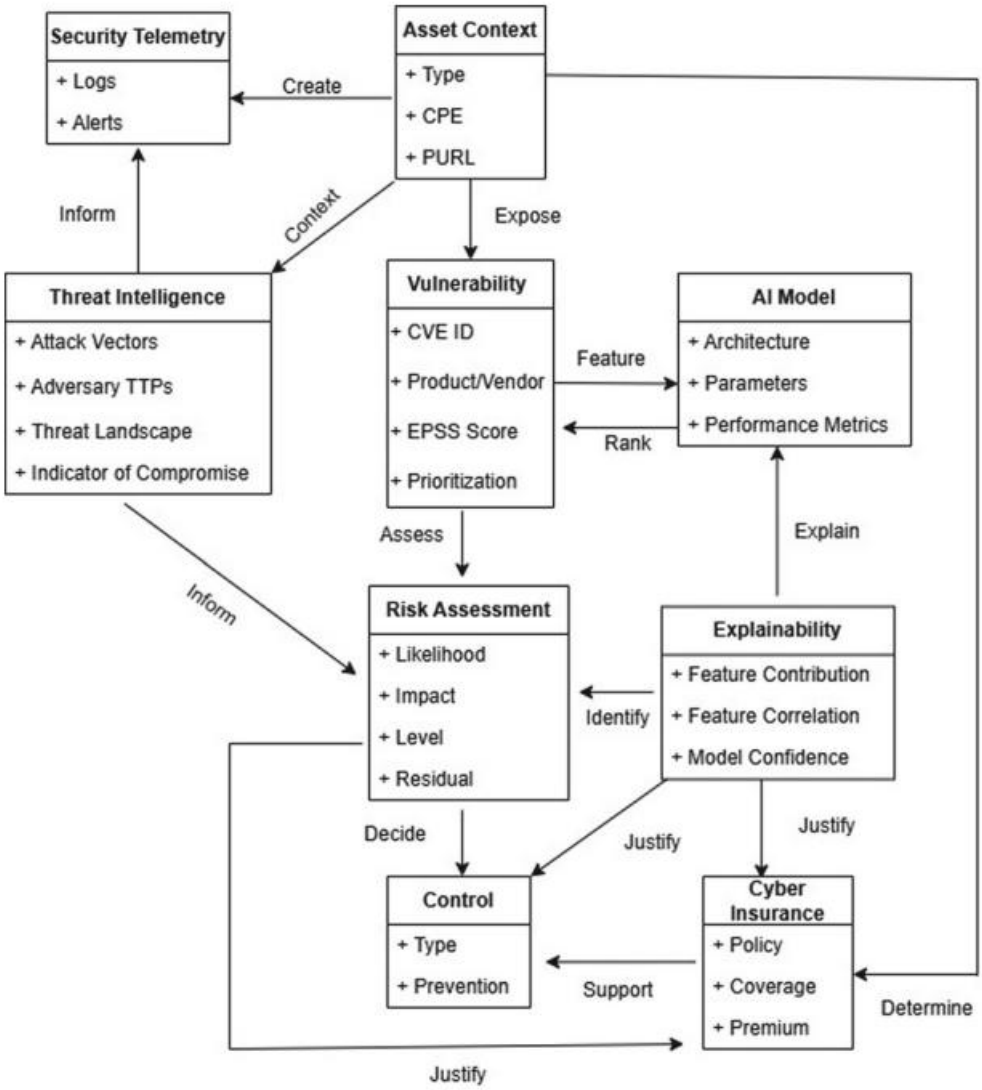

Figure 1. Conceptual Model

1. **Vulnerability identification and prioritization:** Based on the identified assets and services, vulnerabilities are analyzed using LLM/CodeBERT models. Vulnerabilities are categorized as LOW, MEDIUM, or HIGH according to CVSS and EPSS scores.

JOURNAL OF MULTIDISCIPLINARY SCIENCES AND INNOVATIONS
VOLUME 5, ISSUE 02
MOPNTHLY JOURNALS
ISSN NUMBER: 2751-4390
IMPACT FACTOR: 9,08

2. **Dynamic risk assessment:** Risk scenarios are generated based on high-priority vulnerabilities and assets. Risk is evaluated using the formula:

$$Risk = Likelihood \times Impact$$

3. **Selection of security controls (using XAI):** Feature correlations are analyzed to determine interdependencies among attributes. SHAP is applied to quantify the contribution of each feature to the model's prediction. The interpretability of XAI decisions enables justification for selecting specific security controls.

4. **Implementation of controls:** Technical, managerial, and operational controls are selected according to NIST SP 800-53 standards. These controls are linked to the most impactful features identified through SHAP and correlation analysis.

5. **Cyber insurance decisions:** Residual risk is determined after implementing additional controls. Insurance premiums and policy terms are aligned with the level of residual risk.

Process:

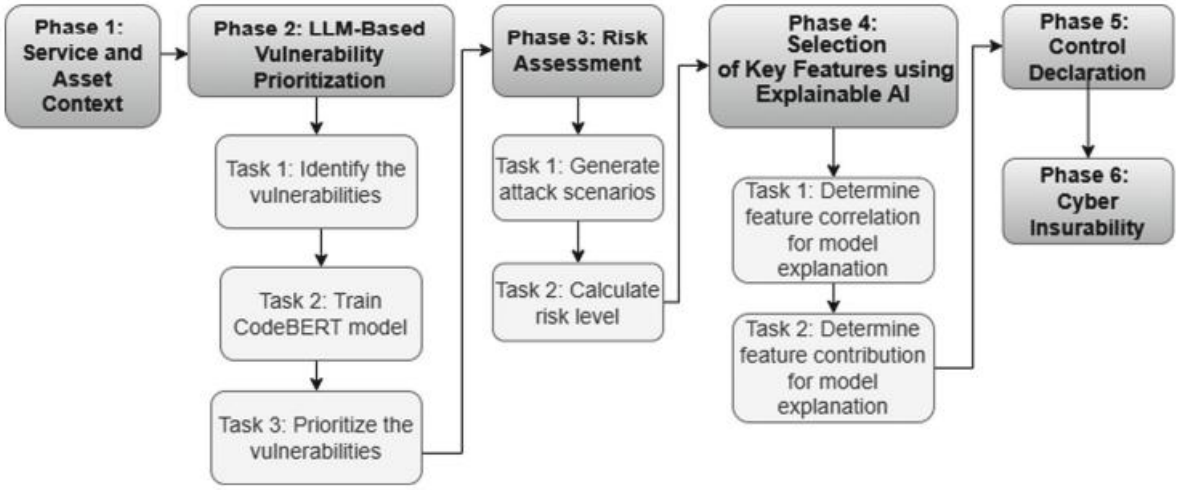

Figure 2. Process of the Proposed Approach

Analysis and conclusion. Assessing cybersecurity risks is inherently complex, as threats are dynamic and vulnerabilities are subject to exploitation. Consequently, risks are often inadequately identified, and cyber insurance requires transparent assessment.

This study proposes a dynamic cybersecurity risk management approach based on XAI and CodeBERT, which analyzes vulnerabilities, identifies exploitability and key factors, calculates risk levels in real time, and prioritizes high-risk vulnerabilities. Security controls are selected in accordance with NIST SP 800-53 standards, and residual risks can be financially mitigated through cyber insurance.

Practical evaluations demonstrated an accuracy of 96.9% and supported well-founded cyber insurance decisions based on residual risk. Therefore, the risk assessment and decision-making process is recommended to be AI-based, transparent, and dynamic, ensuring proactive security and enabling the financial coverage of residual risks through insurance. The proposed approach also promotes wider adoption of cyber insurance and reduces discrepancies in risk perception.

References:

1. Law of the Republic of Uzbekistan "On Cybersecurity." Adopted by the Legislative Chamber on February 25, 2022, ratified by the Senate on March 17, 2022, No. O'RQ–764.
2. Kumar, R., Singh, S., "Cyber insurance in India: An overview," *International Journal of Research in Finance and Management*, vol. 6, pp. 373–378, 2023. https://doi.org/10.33545/26175754.2023.v6.i1d.230

3. Biswas, B., Mukhopadhyay, A., Kumar, A., Delen, D., "A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks," *Decision Support Systems*, vol. 177, 114102, 2024. https://doi.org/10.1016/j.dss.2023.114102
4. Islam, S., Basheer, N., Papastergiou, S., Ciampi, M., Silvestri, S., "Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure," *Journal of Reliable Intelligent Environments*, vol. 11, Article 12, 2025. https://doi.org/10.1007/s40860-025-00253