[1]Gaurang Deshpande,
[2]Sushant Suresh Jadhav

Using AI to Quantify and Continuously Update Cyber Risk Scores across Digital Assets

Journal of Electrical Systems

Abstract- ML models and data-oriented methods are used to ingest huge quantities of system logs, user activities, and threat intelligence in real-time to identify emerging threats and vulnerabilities in systems. AI models are capable of dynamically combining certain factors in a rule-based context, in a deep-learning approach, to produce risk scores that adapt to the environment. Automated systems help mitigate the burden faced by security teams by making them make decisions faster and provide better resource allocation, as well as minimise human mistakes and enhance the resilience of organisations in real-time. This study showcases the effectiveness of AI and machine learning in automating and updating cyber risk scores in real-time. The study results indicated high accuracy in prediction with dynamic changes in response to the vulnerabilities, as well as insights into the sector. These findings show the role of AI in establishing cyber risk management in a proactive, adaptive, data-driven process.

Index Terms- "Cyber risk scoring, Artificial Intelligence, Machine Learning, Real-time threat analysis, Vulnerability prediction, Digital asset protection"

I. INTRODUCTION

A. Background to the Study

The spread of digital assets in industries has resulted in the exposure to cyber threats at a greater rate. The conventional procedures of assessing cyber risks can be described as periodic, manual, and cannot adapt to the current changes in the threats. "Artificial Intelligence (AI)" proposes a smart solution to automate and develop cybersecurity through quantifying and real-time updating cyber risk ratings [1]. With the help of AI, organisations are able to explore their digital environment around the clock, discover risks on the spot, and keep reacting to them with a better-timed response. The transformation allows proactive risk management, minimises incident response time, and adjusts security controls to the instantaneous threat status.

B. Overview

This study focuses on how AI can be used to empower the process of quantifying and consistently refreshing the score of cyber risk across digital assets. Different methods conduct real-time tests, unlike the static ones, thus allowing organisations to manage risks efficiently [2]. The paper also looks at tools, techniques, and advantages of AI-based risk scoring systems in the AI era of cybersecurity so that the protection of assets and compliance with legal requirements are increased.

C. Problem Statement

The complexity of digital environments and continuous changes make the task of controlling cyber threats even more difficult in organisations. The conventional cyber risk evaluation practices are dynamic, applications are sporadic, and they seldom capture vulnerabilities in real-time. This leads to the main problem, slow action in detecting the threat, as well as poor prioritisation of risk [3]. A smarter, more continuous, and adaptive risk-monitoring mechanism that watches digital assets and is capable of continuously updating the risk score needs to be developed urgently. The issue is how to overcome this gap with the help of AI and make cyber risk management dynamic, efficient, and data-driven.

[1]Software Developer
IBM, USA
Email: gaurangdeshpande89@gmail.com
[2]Principal Product Software Engineer
WoltersKluwer, USA
Email: sushantjadhav21@gmail.com

D. Aim and Objectives

The study aims to create an AI-based platform that will record and constantly update cyber risk levels of various digital assets to support managing threats in real-time. The objectives are: 1. To execute models of AI for analysing real-time threats and vulnerabilities. 2. To evaluate the risk scoring by using threat intelligence, asset exposure and sensitivity. 3. To evaluate constant monitoring and immediate updating of the risk score when the digital situation changes.

E. Scope and Significance

The scope of the study focuses on the discussion of how AI will revolutionise the sector of cyber risk management through the automation of the risk scoring of digital assets. It discusses the functionality of AI in data analysis, threat determination and live risk revisions in various IT structures [4]. The significance lies in the smaller exposure to cyberattacks, better decisions, and a more secure posture with the help of constant monitoring. The study also has implications for regulatory compliance and resource optimisation, which is why it is quite useful in industries dealing with sensitive computer data, such as the financial, health, and e-commerce sectors.

II. LITERATURE REVIEW

A. Implementing Machine Learning and Artificial Intelligence Models for Real-Time Analysis of Vulnerabilities and Threats

Machine learning or ML and AI models are critical components in providing real-time vulnerability and threat analysis of digital assets, in terms of using AI to quantify and continuously update the cyber risk scores of the digital assets. The complexity of the digital ecosystems, which include services, IoT devices, and virtualised network environments, is more sophisticated, making the standard methods of static risk analysis insufficient to capture the nature of cyber risk. A rating score from 1 to 5 is created to measure which control addresses the specific control objective [5]. “Support vector machines” or SVM, Random Forest, and gradient boosting algorithms are semi-supervised learning methods that have demonstrated high accuracies in the classification of known attacks as well as the extrapolation of possible vulnerabilities through the usage of labelled samples. Additionally, AI has emerged as a transformative tool in cybersecurity, enabling organisations to recognise, predict, and mitigate potential threats effectively [6]. Unsupervised models, particularly clustering and anomaly detection models, become useful when working with attack vectors that have not been encountered before because of their capability to notice unusual behaviour. These “convolutional neural networks” or CNNs and “long short-term memory networks” or LSTMs enable deep learning models to further improve the detection by extracting the temporal and spatial aspects of data sets with a complex structure.

Furthermore, using AI models in partnership with a real-time data feed and security orchestration instruments is effective to update the scores of cyber-risks on an ongoing basis. A real-time feedback loop plays a crucial role in proactive risk management, and organisations plan remediation accordingly and according to the current threat landscapes and system vulnerabilities.

B. Automation in risk scoring

Automation of cyber risk scoring is a key contemporary interest in the management of cybersecurity, especially as institutions seek to streamline many more digital properties. Conventional risk assessment practices, frequently conducted manually and done in intervals, do not create timely knowledge on the ever-changing threats and weaknesses of the assets. Consequently, practitioners are giving more traction to AI-powered frameworks that combine machine learning, data analytics, and real-time threat intelligence and automate the quantification of risk, concentrating on asset exposure and sensitivity. Artificial Intelligence (AI) technologies create advanced capabilities to evaluate large amounts of data generated in real-time within cloud infrastructures [6]. Asset exposure is the ease with which an asset can be reached by possible adversaries, and the techniques that are being used to assess this exposure include attack surface mapping models and network graph analysis models. On the other hand, an energy efficiency artificial intelligence service can perform smart estimations on all energy data coming from the building and stored in the energy metrics database. All these elements are deployed in virtual machines (VMs) from private cloud providers [7]. The sensitivity is the significance of the asset, such as financial data or intellectual property, and is used in scoring algorithms to seek protection of high-value targets. Simultaneously, threat intelligence, which may be collected by means of vulnerability databases, intrusion detection systems, and monitoring of the dark web, generates contextual information that can be used to increase the relevance of scoring.

C. Continuous monitoring and dynamic risk score updates

Ongoing monitoring and risk scoring have been highlighted as a thriving element related to flexible cybersecurity models, particularly in such evolving digital landscapes. Static risk evaluations, which are generally run in scheduled periods, are not able to measure real-time transformation in threat environments, system parameters, and asset dynamics. Thus, to overcome such shortcomings, AI-based solutions are gaining ground to ensure real-time visibility and responsiveness in enterprise networks. Machine learning and data streaming enable the persistent gathering and analysis of telemetry information from the measurements at end-points, cloud structures, and also in the Internet of Things (IoT). On the other hand, AI has improved security or increased the cyber threats in extreme environments [3]. The tools can identify abnormalities in behaviour, critical weaknesses, and externally visible indicators of threat, and automatically push cyber risk scores upward or downward. Moreover, feedback controls in AI models, such as reinforcement learning, promote flexibility of risk scoring algorithms through the learning of historical incidents and changes in the environment. This is a dynamic model as it keeps risk scores topical and viable, such that it facilitates proactive security processes and knowledgeable decision making in fast-paced and highly complicated digital environments.

III. METHODOLOGY

A. Research Design

The research design uses an ***explanatory research design*** to establish how scoring of cyber risk can be determined and updated in real time through the application of AI technology. The design assists in revealing the connection between AI tools, cyber risk assessment activities, and the weaknesses of digital assets.

B. Data Collection and Analysis

The study focuses on the ***secondary qualitative and quantitative data*** methods. Qualitative data can be analysed through case studies, journals, articles, and industry reports to get a sense of the role of AI in creating a cyber risk score. Risk levels, threat frequency, and response efficiency across digital assets are conveyed as quantitative data through different charts and graphs. This method will encourage the analysis of the AI-driven cybersecurity performance comprehensively.

C. Case Studies/Examples

Case Study 1: Microsoft Azure Security Centre

The Azure Security Centre by Microsoft powers the system to securely monitor digital assets hosted on cloud computing with the combination of AI and machine learning. It also provides cyber risk scores to virtual machines, applications, and databases using real-time telemetry, configuration faults, and worldwide threat intelligence. All these scores are changed dynamically with the discovery of new vulnerabilities or threats. This strategy has allowed organisations to be more proactive on the most dangerous systems, improve the response to incident times, and align with the regulatory frameworks like ISO 27001, NIST [9]. The AI-driven system offered by Azure improves the visibility, precision, and safety of multi-cloud environments.

Case Study 2: Darktrace in Deloitte's Global Network

Deloitte deployed Darktrace AI-driven Cyber AI Analyst, which defends well-established IT infrastructure all around the world. In close time, the system can provide the degree of cyber risk to digital assets using unsupervised machine learning, which processes behavioural patterns, user behaviour, and external threat intelligence. This saved a lot in terms of false positives and efficiency in the operations [10]. The AI platform has been critical to Deloitte in terms of implementing its cybersecurity approach to the protection of its confidential customer data, such as in remote work areas.

Case Study 3: IBM QRadar at a Multinational Healthcare Provider

The global healthcare organisation has implemented the IBM QRadar with Watson AI to enhance cybersecurity in its hospital network. A given AI system gathers information on the medical devices utilising IoT, electronic health records, and network endpoints to give cyber risk ratings, which update in a manner that changes. It uses threat intelligence and machine learning to detect vulnerabilities, raises suspicions on activities, and monitors the implementation of standards such as the HIPAA and GDPR [11]. With the deployment, risk awareness was also enhanced, and the information on the patients was better protected, and the time it took to respond to the possible breach was also significantly reduced.

D. Metrics of Evaluation

The success of AI-driven cyber risk scoring will be measured in the main categories of ***threat detection accuracy***, ***the number of risk score updates***, the ***time of reaction*** to newly detected vulnerabilities, and, overall, the ***decreased risk exposure***. Other indicators to be evaluated are adherence to the cybersecurity guidelines, data integrity, and system scalability. These measures will facilitate the assessment of the efficiency of the implementation of AI in risk management from a real-time perspective of the activity in the digital environment.

IV. RESULTS

A. Data Presentation

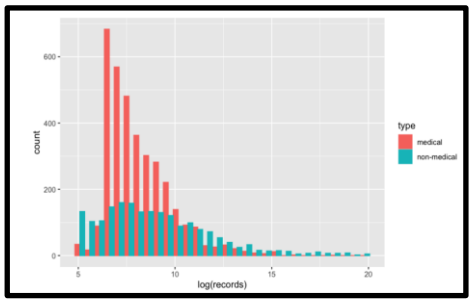

Figure 1: Distinguishes between cyber breach severities in medical vs non-medical organisations [12]

As shown in Figure 1, medical organisations have more cyber losses (~600 records), which signifies that they have significant breaches. By contrast, non-medical organisations are wider-tailed, with a flatter distribution, indicating a wider range with more diverse exposure. This variability underlines the necessity that AI-driven models change the differentiation on risk scoring by sectoral asset sensitivity and incident reporting maturity [12].

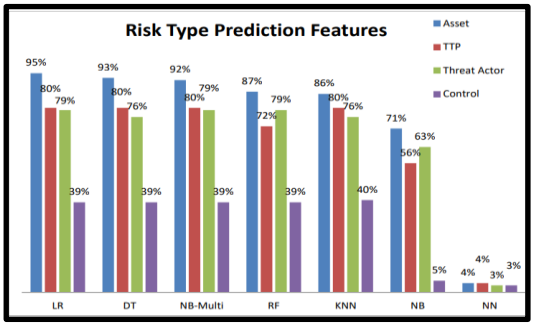

Figure 2: Performance of each classifier in predicting risk types [1]

The graph shows the accuracy of different machine learning classifiers (LR, DT, NB-Multi, RF, KNN, NB, NN) to predict several types of risks (Asset, TTP, Threat Actor, Control). As it is emphasised, the LR, DT, NB-Multi, RF, and KNN models demonstrate the high predictive accuracy (79%-95%) of the risk types like "Asset" and "TTP" [1]. The results would correlate directly with the existing research objective of applying ML solutions to analyse vulnerabilities on a real-time basis. This is essential to automate and continuously update the cyber risk scores as per the digital assets and threat intelligence.

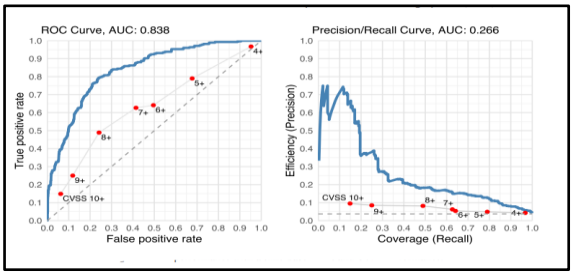

Figure 3: Prediction of Cyber Risk Score exploitation using input Model Performance [13]

The "Area Under the Curve" (AUC), 0.838 for the "Receiver Operating Characteristic" (ROC) Curve, shows that the model is ascribed a high capability of distinguishing between exploitable and non-exploitable vulnerabilities. This will efficiently facilitate the present research's objective of measuring cyber risk. Most of the relevant exploitations cannot be identified, thus some areas can be improved as indicated by the Precision-Recall Curve (AUC: 0.266). The "Common Vulnerability Scoring System" (CVSS) scores revealed that the model has a better ability to predict exploitation than the traditional CVSS scores that are important in automated and dynamic risk scoring updates [13].

B. Findings

The three figures show the importance of AI in the quantification of cyber risks altogether. Figure 1 stresses that breach patterns vary across sectors and require sector-specific scoring. The second figure proves that machine learning models can be trusted to perform a high-fidelity risk type prediction and assist in real-time threat analysis. The third figure shows that the AI models are more effective in predicting exploitability than traditional measures. For example, CVSS asserts the significance of using them in dynamic, automated risk ranking in digital assets [13].

C. Case Study Outcomes

Case Study Name	Company	Case Study Outcome	Relevance to Current Research
Microsoft Azure Security Centre	Microsoft	This has implemented dynamic risk scoring and an active responder to incidents of multi-cloud resources [9].	Presents AI continuous control and compliance with such standards as ISO 27001 and NIST.
Darktrace in Deloitte's Global Network	Deloitte	Minimised the false positives and secured confidential data with behavioural analytics [10].	Attracts attention to the success of unsupervised ML in the detection and analysis of risk in real-time.
IBM QRadar at a Multinational Healthcare Provider	Global healthcare organisation	Higher breach detection speed and patient data protection through the use of AI-enhanced threat detection [11].	Demonstrates how AI adjusts risk ranking with data available via the IoT and complies with regulations such as HIPAA and GDPR.

Table 1: Case Study Outcome

[Source: Self-Created]

Case study examples in the above table show the role of AI that leads to proactive risk scoring and threat detection in real-time in multiple sectors.

D. Comparative Analysis

Author	Aim	Findings	Gaps identified
[5]	"This paper aims for an effective Cyber Security Risk Management practice using assets criticality, prediction of risk types, and evaluating the effectiveness of existing controls."	There are CSRM concepts including "asset, threat actor, attack pattern, Tactic, Technique and Procedure (TTP), and controls", and maps these concepts with the "VERIS community dataset" (VCDB) features for the risk prediction.	This paper shows a limited incorporation of ML risk anticipation with the assessment of control effectiveness.

[6]	"This article examines how various ML algorithms enhance cybersecurity practices through real-time anomaly detection."	ML-based mitigations create proactive initiatives for confronting contemporary threats and empower companies to shift from reactive to anticipatory defence mechanisms.	Lack of primary research
[7]	This article aims to identify the role of AI in the context of proactive cyber threat detection.	AI systems can identify trends, identify malicious activity, and anticipate new threats with greater precision and effectiveness.	There is a lag in terms of empirical support for AI frameworks in real-world contexts.
[8]	"This article aims to conduct a quantitative analysis of different attack-defence scenarios towards informed decision-making of countermeasures."	ADTs could be enhanced in the future with conditional probabilities learned from continuous monitoring of the system and threat intelligence inputs.	This article lacks in terms of applying threat intelligence in a real-life segment in ADT frameworks.
[3]	"This article aims to create a dynamic and self-adapting system based on the incorporation of AI."	Machine Learning technologies are migrating to the periphery of the internet and into local IoT networks.	There is a lack in terms of practically validating AI frameworks in real-world contexts.

Table 2: Comparative Analysis of Literature Review Sources

[Source: Self-Created]

This comparative analysis helps to fulfil research aims and objectives by identifying gaps, trends, and outcomes, specifying refined knowledge of the future of AI incorporation to quantify and continuously update cyber risk scores.

V. DISCUSSION

A. Interpretation of Results

According to the findings of the research, AI-driven technology and especially machine learning (ML) could be actively used to conduct real-time threat intelligence, asset sensitivity, and exposure to quantify cyber risk scores. Random Forest and Logistic Regression are always accurate in predicting the risk type. Context-aware AI models require more attention because of the sector-specific patterns, like medical organisations not being like non-medical organisations. Moreover, such performance measures as AUC (0.838) show that the model has good capacity to predict exploitability [13]. Such findings confirm how constant surveillance and automated rating would enhance the responsiveness and efficacy of cybersecurity risk digital landscapes in real-time digital environments.

B. Practical Implications

The study provides organisations with the opportunity to apply AI-based models to automatically score and refresh cyber risks in real-time to respond timelier to the emerging threats. This automation improves compliance with regulations, decreases manual work and prioritises major vulnerabilities, raises general, cross-environmental cybersecurity resilience, particularly in complicated environments, like health administration, banking, and multi-cloud conditions.

C. Challenges and Limitations

The AI-based cyber risk scoring, though, has several challenges, including limited labelled data to train the model, the dynamic nature of threats, and the interpretability of the model. Real-time data aggregation might be inhibited by data silos, privacy rules and integrations with the legacy systems. Moreover, unbalanced training sets may cause false negatives or poor precision, as in lower precision-recall AUC scores of some exploit predictions.

D. Recommendations

Companies need to implement hybrid forms of AI that follow supervised and unsupervised learning to cover both familiar and unfamiliar types of threats. Quality and real-time telemetry data, cross-platform integration would require investment to enhance the accuracy of scoring. This is recommended to create industry-specific AI systems (e.g., healthcare or financial systems) to support tailored risk profiles better [14]. Moreover, the validation of models and feedback loops, along with a human-in-the-loop system, should be utilised when ensuring refinement of predictive capabilities and adaptation to changes in digital ecosystems [15]. Lastly, it is necessary to focus on explainability to facilitate stakeholder confidence and regulatory adherence.

VI. CONCLUSION AND FUTURE WORK

This study infers that AI, especially ML, is a revolutionary tool in the measurement and constant updating of the quantification of cyber risk values among digital assets. Risk simulation that makes use of traditional, manual, and periodic models cannot be sufficient in the current dynamic digital spaces. The research illustrates that using AI models, asset exposure, threat intelligence, and sensitivity might be successfully combined to generate correct risk scores in real-time. Visualisation of the Classifier performance and predictions in the vulnerability models demonstrates a greater accuracy and flexibility that AI offers compared to a fixed scoring mechanism such as CVSS. Also, sector-based patterns in the data of breaches emphasise the role of contextual scoring systems.

However, difficulties in factors like data accessibility, explainability of the model, and integration with the current systems persist. Addressing these points in the future, it is necessary to improve model explainability by using the tool of explainable AI (XAI) and create federated learning approaches. These will mitigate data privacy issues and create a standardised model of risk scoring across different industries. Also, adaptive response automation based on predictive scoring and score tuning through reinforcement learning is an option that can be looked at in future studies. Increasing the data to include a greater variety in industries will make models even more resilient.

VII. REFERENCE LIST

[1] Kure, H.I., Islam, S., Ghazanfar, M., Raza, A. and Pasha, M., 2022. Asset criticality and risk prediction for effective cybersecurity risk management of cyber-physical systems. *Neural Computing and Applications*, *34*(1), pp.493-514.

[2] Kaloudi, N. and Li, J., 2020. The AI-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), pp.1-34.

[3] Radanliev, P., De Roure, D., Page, K., Van Kleek, M., Santos, O., Maddox, L.T., Burnap, P., Anthi, E., and Maple, C., 2020. Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning, and real-time intelligence for predictive cyber risk analytics in extreme environments–cyber risk in the colonisation of Mars. *Safety in Extreme Environments*, *2*, pp.219-230.

[4] Möller, D.P., 2023. Cybersecurity in digital transformation. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 1-70). Cham: Springer Nature Switzerland.

[5] Kure, H.I., Islam, S., Ghazanfar, M., Raza, A. and Pasha, M., 2022. Asset criticality and risk prediction for effective cybersecurity risk management of cyber-physical systems. *Neural Computing and Applications*, *34*(1), pp.493-514.

[6] Adabala, S.K., 2021. Machine Learning in Cybersecurity: Proactive Threat Detection and Response. *International Journal For Multidisciplinary Research*, *3*(5).

[7] Reddy, A.R.P., 2021. The role of artificial intelligence in proactive cyber threat detection in cloud environments. *NeuroQuantology*, *19*(12), pp.764-773.

[8] Rios, E., Rego, A., Iturbe, E., Higuero, M. and Larrucea, X., 2020. Continuous quantitative risk management in smart grids using attack-defence trees. *Sensors*, *20*(16), p.4404.

[9] Azuremarketplace.microsoft.com, 2024, *marketplace* Available at: https://azuremarketplace.microsoft.com/en-us/marketplace/apps/microsoft.azuresecuritycenter?tab=overview [Accessed on: 9th May, 2024]

[10] Darktrace.com, 2017, *award-on-darktrace* Available at: https://www.darktrace.com/news/deloitte-bestows-prestigious-award-on-darktrace [Accessed on: 17th May, 2024]

[11] IBM.com, 2024, *qradar.* Available at: https://www.ibm.com/products/qradar [Accessed on: 15th May, 2024]

[12] Sun, M., 2023. A Breakthrough of Digital Assets Security in Crypto Insurance: Cyber Risk Prediction Models. *Research and Applications Towards Mathematics and Computer Science*, p.54.

[13] Jacobs, J., Romanosky, S., Edwards, B., Adjerid, I., and Roytman, M., 2021. Exploit prediction scoring system (EPSS). *Digital Threats: Research and Practice*, *2*(3), pp.1-17.

[14] Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E. and Alabbad, D.A., 2023. Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. *Sensors*, *23*(15), p.6666.

[15] Yaseen, A., 2022. Accelerating the SOC: Achieve greater efficiency with AI-driven automation. *International Journal of Responsible Artificial Intelligence*, *12*(1), pp.1-19.

[16] Chintale, P.: DevOps Design Pattern: Implementing DevOps Best Practices forSecure and Reliable CI/CD Pipeline (English Edition). BPB Publications, 2023.

[17] Goli, A. K. R. Journal of Innovation in Research and Education (JIRE).

[18] Konda, R. Journal of Innovation in Research and Education (JIRE).

[19] Goli, S. R. (2023). Scalable SRE Practices for AI Service Reliability: Monitoring and Alerting in Production ML Systems. Available at SSRN 5741663.