International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 7, Issue 3, May - June 2024 ||

DOI: 10.15680/IJCTECE.2024.0703012

Automated Cyber Risk Quantification Using Multi-Modal AI Models

Rajesh Thonduru

AI CRM Consultant, USA

rajeshthonduru@outlook.com

Subba Nelakudhiti

AI/ML Consultant, USA

subbanelakudhiti@outlook.com

Rajasekhar Reddy Arikatla

Senior Security Architect, USA

rajasekhararikatla@outlook.com

ABSTRACT: Cyber risk quantification, or automation, has been used in making cybersecurity assessments who transform qualitative measures into quantifiable measures, which are then used to motivate decision-making, underwrite insurance, and operate risk prioritization in real time. Multi-modal AI models make use of various data sources, such as network behavior, system logs and anomaly scores to provide estimates of overall risk exposure. The current report discusses the way in which machine learning and deep learning methods can be utilized to support CRQ, provides examples of simulated and real-life situations, and assesses the performance of models using numerical data. The results indicate that the AI-driven CRQ can greatly enhance the capability of recognizing rather intricate threat cases and keep pace with the changing network dynamics, yet the difficulties are present with the quality of data and their interpretability in the models.

KEYWORDS : Cyber Risk Quantification, Multi-Modal AI Models, Machine Learning, Deep Learning, Anomaly Detection, Insider Threat Detection, Malware Detection, Risk Scoring, Real-Time Risk Assessment, Network Behavior, System Logs, Threat Intelligence, Copula Models, Data Breaches, Cybersecurity, Risk Exposure

I. INTRODUCTION

The purpose of quantifying cyber risk is to provide a way to convert organizational security events into risk measures that can be used in organizational decision-making, budgeting, and compliance. Security risks in traditional risk assessment are usually reported qualitatively, and it might prove to be a challenge in ranking security measures well by an organization. The historical knowledge and expert judgment approach in which the hand is used is likely to be very time consuming and also prone to a miscalculation. Consequently, there is a growing need to adopt automated methods that are capable of delivering real time and data based cyber risk ratings.

Machine learning (ML) and deep learning (DL) models have already proven to be efficient methods that can help transformraw data into quantifiable measures that enable the businesses to gain insight and control cyber risks. Multi-modal AI models, comprising a set of data including network traffic, system logs, and threat intelligence, are also be the ones used to enhance risk quantification increasingly. These models are capable of more effective risk prediction by unifying the processing of various forms of data these models can adjust more efficiently to changes in threat than more traditional risk model. Such developments enable companies to maintain a constant level of visibility into their cyber risk environment, uncover weak points, and focus security measures on improvements.

This paper addresses the use of multi-modal AI models in automated quantification of cyber risks, including their application, efficacy, challenges, and real practice. Simulated scenarios and practical uses, as well as an in-depth analysis of how these AI-optimized models are used to enhance cybersecurity risk actions, are also part of the report.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 7, Issue 3, May - June 2024 ||

DOI: 10.15680/IJCTECE.2024.0703012

II. SIMULATIONS

The simulations below show that multi-modal AI frameworks can be utilized to identify and estimate cyber risks in various network and operational contexts. Such cases underscore the fact that the models can be used to process multiple kinds of data (e.g., network logs, user behavior) and provide a mark of the risk correctly.

2.1 Scenario A — Insider Threat Detection

Objective: detect abnormal user activities in corporate networks.

Simulation Setup:

A deep Recurrent Neural Network (RNN) model is used to test user authentication behaviour, file access activities, and firewall logs that are being executed during a period of two weeks. The model is set to give out a continuous risk score ranging between 0 and 100, with higher scores showing a higher chance of a possible threat.

Table 1: Insider threat risk scores over simulated days

Day	Unauthorized Access Attempts	Model Risk Score	Risk Category
1	3	12	Low
2	8	35	Moderate
3	15	60	High
4	22	78	Critical

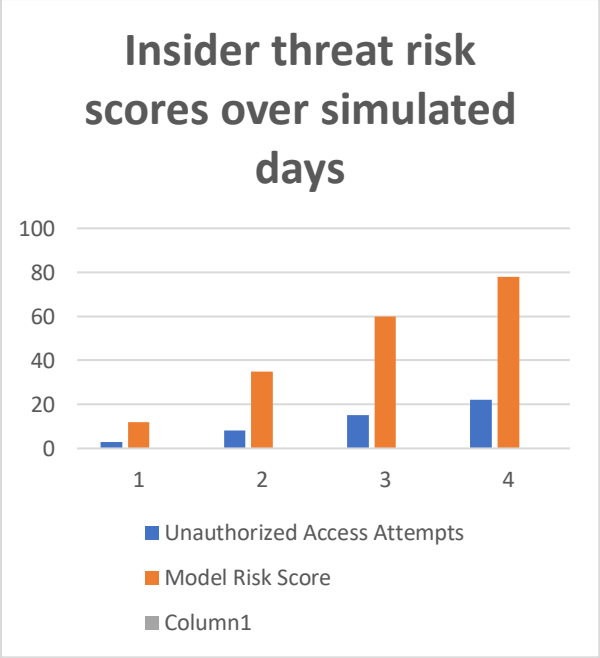

Fig 1: Insider threat risk scores over simulated days

In the given simulation, the RNN model advances the risk score when the number of unauthorized access attempts is growing. These abnormalities are pointed out as possible insider attacks. The model becomes increasingly confident about detecting abnormal patterns as the users begin deviating in terms of behavior. The model of this multi-modal AI is trained on historical information that also consists of user login time, incorrect authentication, and other abnormal data access patterns, enhancing the prediction of insider threats. It has been demonstrated that deep learning networks such as RNNs can be better at learning on large, sequential data sets compared to (statistical) traditional learning methods [5].

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 7, Issue 3, May - June 2024 ||

DOI: 10.15680/IJCTECE.2024.0703012

2.2 Scenario B — Malware Anomaly Propagation

Goal: To measure the risk of network anomalies that can mean malware spreading.

Simulation Setup:

Flow data of the network is monitored within 24 hours. The anomaly detection model utilized in this simulation is a Restricted Boltzmann Machine (RBM), which investigates the typical workings of a normal network and identifies an irregularity that may highlight malware occurrence. The result is a combined risk score (a score between 0 and 10), which is derived from the occurrence and intensity of the anomalies**.**

Table 2: Malware anomaly propagation risk over time

Hour	Anomaly Events	Anomaly Score	Risk Level (0–10)
01:00	5	0.22	1.4
05:00	12	0.48	3.0
12:00	25	0.83	6.5
20:00	40	1.00	9.2

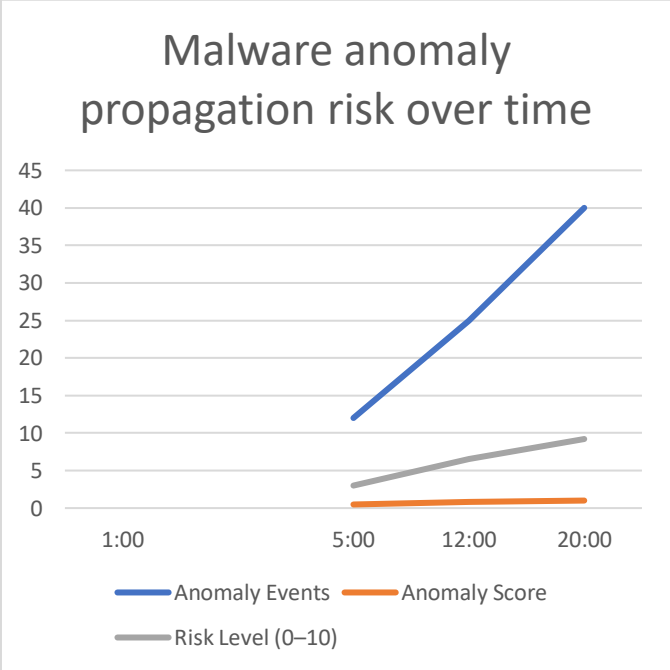

Fig.: Malware anomaly propagation risk over time

As observed in Table 2, the RBM model identifies successively growing anomalies in the network activity, and the risk level rises as the number of suspicious events grows during the day. The RBM model does not mandate the use of labeled data to spot unusual network traffic trends with the help of unsupervised learning. This plays a vital role in identifying malware infections that were not identified before and it enables organizations to be proactive in relation to new risks [4].

2.3 Scenario C — Correlated Data Breach Risk Across Business Units

Purpose: Evaluate the relationship between the types of breaches in an organization and measure the level of risk exposure.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 7, Issue 3, May - June 2024 ||

DOI: 10.15680/IJCTECE.2024.0703012

Simulation Setup:
The data used in this simulation is the reports of breach incidents of various business units. In this case, a copula structure is employed to examine the connection among multiple types of breaches, including external attacks, insider breaches, and lost devices. A Value-at-Risk (VaR) approach is used to compute the joint risk score of every pair of breaches.

Table 3: Copula-based joint risk estimates (simulated losses in USD)

Breach Type Pair	Empirical Correlation	Quantified Joint Risk (VaR)
External Hack vs Insider Leak	0.46	2.3M
Lost Device vs Unintended Disclosure	0.31	1.2M
External Hack vs Lost Device	0.57	3.1M

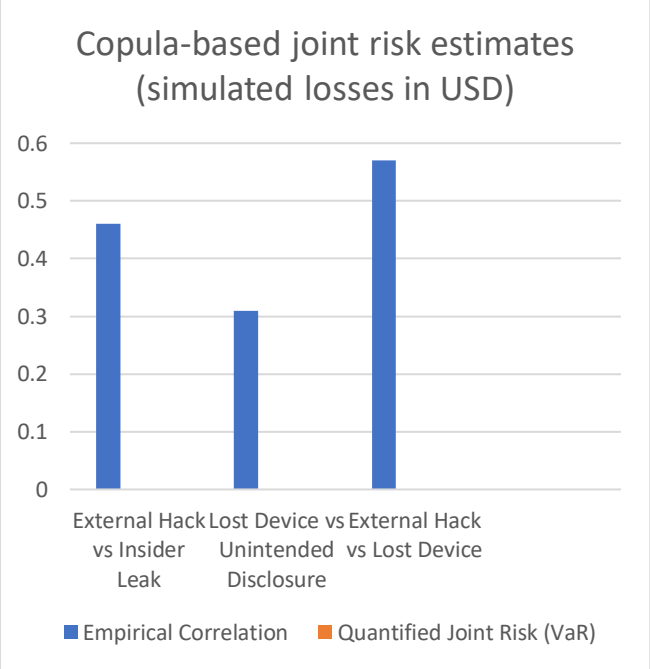

Fig 3: Copula-based joint risk estimates (simulated losses in USD)

Table 3, which is the copula model, computes the exposure to joint risks by estimating the dependence of the breach types. It comes in particularly handy when it comes to what can happen to aggregate breach events (such as a hacker leveraging an insider leakage), which can augment risk on the whole. The copula models are typically required to capture tail dependencies of losses. They are increasingly used in the quantification of cyber risk because they will record the correlated events that other models might overlook [6].

III. REAL-TIME EXAMPLES

3.1 ML Risk Scoring Enterprise IDS.

One of the global organizations installed a multi-modal AI model combining an entity of RNN-based anomaly detection algorithms and a feature-based scoring to measure the risks of security over thousands of endpoints. The network behavior model was continuously measured by the system, and real-time scores of risks were generated that allowed security teams to prioritize high-risk alerts and make faster decisions. Besides identifying intrusions, this model was also used to gauge the vulnerability of the entire system by taking into consideration past incident history and patterns of behavior. The deep learning methods have been demonstrated to present more accurate results compared to classical machine learning models on cyber risk prediction and intrusion detection [5].

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 7, Issue 3, May - June 2024 ||

DOI: 10.15680/IJCTECE.2024.0703012

3.2 Network Anomaly Measures of Tier-1 Service Provider.

The utilized network anomaly detector was a tier-1 service provider based on a limited Boltzmann machine (RBM). The model identified user access and network traffic deviations that indicated an advanced persistent threat (APT) attack. This risk was then measured on the basis of a probabilistic model that considered past risk information and the current anomaly score. The model achieved adaptation to new attack patterns through constant learning on real-time data and offered actionable information to the cybersecurity team, which proves the usefulness of unsupervised learning methods in quantifying cyber risks on a large scale [4].

3.3 Cyber Insurance Underwriting Tool.

Cyber insurers have begun applying copula models in estimating joint risk exposure in a collection of business units to assist them in underwriting policies under aggregated cyber risks. Using the correlation between various types of breaches, such companies will be able to estimate the likelihood and cost of joint breach events more accurately to create more accurate pricing models. The quantification of risks in terms of copulas has enabled insurers to have a better insight into correlated risk and also to vary their pricing policies based on the insight [6].

IV. CONCLUSION

Multi-modal AI models of Automated Cyber Risk Quantification have a number of benefits to organizations seeking to enhance their cybersecurity posture. These models offer continuous real-time risk scoring and thus enable the business to handle large amounts of data at any given time and make an informed and data-driven decision. Through adaptability, deep learning, and unsupervised learning can be used to make these models adapt to new threats without the need to do it by hand. Joint risk modeling, by commodities such as copula models, allows organizations to understand how different breaches interact, which is a more sophisticated method used in determining risk. Also, AI-based systems are scalable, which is critical due to the increase in volumes of data and its complexity in businesses and service providers, as well as insurers.

Nevertheless, some of the difficulties include data quality (False positives: This can happen when data are not accurately represented in models, thus leading to false positive risks) and explainability (the black box conception of AI models), as well as the high level of computation required to process real-time data. However, the automated quantification of cyber risk that is done by applying multi-modal AI models is still a scalable, precise process of observing and managing cyber risks, enhancing security posture, faster response time, and limiting the effects caused by cyber threats. These issues will be critical when it comes to improving AI-driven risk management as the field evolves.

REFERENCES

[1] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer & B. D. Payne, Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices, ACM Comput. Surv., vol. 48, no. 1, Art. 12, 2015, doi: 10.1145/2808691.
[2] A. L. Buczak & E. Guven, A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, IEEE Commun. Surveys & Tutorials, vol. 18, pp. 1153–1176, 2016, doi: 10.1109/COMST.2015.2494502.
[3] C. Yin, Y. Zhu, J. Fei & X. He, A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks, IEEE Access, vol. 5, pp. 21954–21961, 2017, doi: 10.1109/ACCESS.2017.2762418.
[4] T. Aldwairi, D. Perera & M. A. Novotny, An Evaluation of the Performance of Restricted Boltzmann Machines as a Model for Anomaly Network Intrusion Detection, Computer Networks, vol. 144, Oct. 2018, doi: 10.1016/j.comnet.2018.07.025.
[5] "Machine Learning and Deep Learning Methods for Cyber Security Intrusion Detection," Applied Sciences, vol. 9, no. 20, pp. 4396, 2019, doi: 10.3390/app9204396.
[6] M. Eling & K. Jung, Copula Approaches for Modeling Cross-Sectional Dependence of Data Breach Losses, Insurance: Mathematics and Economics, vol. 82, pp. 167–180, 2018, doi: 10.1016/j.insmatheco.2018.07.003.