ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan606

Development of a Cyber-Risk Scoring and Visualization Framework for Financial Institutions Using Integrated Business and Network Analytics

Idowu Scholastica Adegoke[1]; Semiu Kolawole Babajide [2*]

1. School of Business, University of Dundee, Dundee, Scotland, United Kingdom
2. Sheffield Business School, Sheffield Hallam University, United Kingdom.

Publication Date: 2026/01/22

Abstract: Cyber threats are gaining traction and spreading like wildfire among financial institutions, and demand proactive assessment measures that integrate technical (network) vulnerabilities with business impact metrics. This study developed a comprehensive cyber-risk scoring and visualization framework capable of addressing the shortcomings of traditional risk assessment approaches. The framework adopted a multi-layered architecture, where business Key Performance Indicators (KPIs), such as transaction anomalies and operational costs, and network security metrics (intrusion detection alerts and vulnerability scans) are merged. Gradient boosting, a machine learning model, was used to classify risks, while autoencoders were employed to detect anomalies. These tools were trained on the CICIDS2017 dataset for improved predictive capabilities. Using a dynamic risk-scoring algorithm, the study contextualized cyber threats in terms of financial implications, expressed as Security Control Scores and Loss Exceedance Curves. The result showed an ROC-AUC risk prediction score of 0.89 when tested in a simulated medium-sized bank environment with 500 assets. The interactive visualization platform converted risk data into valuable insights for executives and other stakeholders. In sum, the framework bridges the gap between security measures and business decision-making in financial institutions to optimize cybersecurity investments, enhance organizational resilience against cyberthreats, and ensure effective compliance reporting.

Keywords: *Cyber-Risk Scoring, Financial Institutions, Banks, Integrated Business, Network Analytics, Cyberthreats.*

How to Cite: Idowu Scholastica Adegoke; Semiu Kolawole Babajide (2026) Development of a Cyber-Risk Scoring and Visualization Framework for Financial Institutions Using Integrated Business and Network Analytics. *International Journal of Innovative Science and Research Technology*, 11(1), 1355-1361.
https://doi.org/10.38124/ijisrt/26jan606

I. INTRODUCTION

Financial institutions hold a position in a country's economy, facilitating liquidity, offering savings, loans and deposits, processing payments, & settlements, and ensuring the availability of money. This explains why they are vulnerable to cyber threats (Gulyas & Kiss, 2023). Lately, cyber risks have surged within institutions, with the frequency of cyberattacks aimed at the financial system rising daily. Gradually, these attacks have grown more damaging and complex (Bahmanova & Lace 2024). Consequently, the threats result in reputational damage, huge financial losses, and operational disruptions.

In contrast conventional cyber-risk evaluation methods tend to be reactive and isolated, focusing on weaknesses like CVSS scores or external threat evaluations (Varga et al. 2020). This indicates an absence of integration capability and strength, for business operational information neglects to frame technical risks in terms of their possible financial consequences. Thus, this gap, alongside the qualitative characteristics of current and existing assessments, serves as a barrier to business-informed and proactive cybersecurity decision-making (Santini et al., 2019).

➢ *Problem Statement*

The inability of financial systems and institutions to assess cyber risks with an integrated approach is a fundamental concern. This is because current approaches are often qualitative or subjective, leading to unreliable risk prioritisation (Crotty & Daniel, 2022). In addition, there is no comprehensive framework capable of combining business analytics, such as operational costs and transaction inconsistencies, with network

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan606

threat analytics, including vulnerability scans and IDS alerts, for a holistic and data-based risk score. This constitutes a deficient system that is inadequate for combining technical vulnerabilities and financial exposures for executive management and technical teams.

➢ *Research Aim and Objectives*

The aim of this review is to evaluate, design, and implement an integrated cyber-risk scoring and visualisation framework for financial institutions.

The objectives are:

- To develop a data fusion approach for business operational metrics and network security analytics
- To design and implement a dynamic risk scoring algorithm to produce a contextualized cyber-risk score
- To include machine learning (ML) modules in financial institution systems for effective risk prediction and anomaly detection
- To build an interactive visualization platform that converts complex risk data into insights for multiple categories of stakeholders

II. CONCEPT OF CYBER RISK IN FINANCIAL INSTITUTIONS

Cyberthreat trends ranging from ransomware to fraud and data breaches are notoriously increasing across sectors, with financial institutions being the main targets (Gulyas & Kiss, 2023). The risk profile of the sector is complicated by the accelerated integration of Internet of Things (IoT) devices and tools in financial systems, which expands the surface of attack with vulnerabilities (Kandasamy et al., 2020). These disruptions constitute a systemic risk, increasing cybersecurity as a core business and compliance requirement under the governance of frameworks such as NIIST, CSF, and ISO/IEC 27001. The vulnerability of the financial sector is exacerbated by the convergence of information technology and operational technology systems, which creates a cycle of interdependencies exploited by threat actors. According to recent industry reports, financial institutions experience cyberattacks at approximately three times higher of others (Dupont, 2019), and average remediation costs exceed millions of dollars per incident. A shift from security models to intelligence-based and adaptive frameworks is required in response to the evolution of sophisticated attack vectors from phishing schemes to advanced persistent threats (APTs), and the use of AI and ML techniques to evade crime detection (Malik et al., 2025). This is crucial to ensure a system capable of responding to threats rapidly and contextualizing the threats within the financial and operational landscape of the institution.

➢ *Business Operational Analytics and Cybersecurity*

Fundamentally, cyber risk is the effect of uncertainty on corporate or business objectives (Tsiodra et al., 2023). In the financial sector, effective risk assessment must, therefore, translate events into business consequences or outcomes, including downtime costs or financial loss (Bahmanova & Lace, 2024). However, a critical gap exists in situations where the evaluations of cybersecurity are not in line with the goals of the organization, resulting in misallocated resources. Likewise, quantitative approaches such as the Loss Exceedance Curve (LEC) modelling, plotting the chances of exceeding some financial loss thresholds, are required for containing risk economically, yet they must be integrated with business data (Sokri, 2019; Aljadani, Mansour, & Yousof, 2024).

Integrating business operational metrics into cybersecurity models is a fundamental transformation from technical assessments to enterprise-level risk management. Key performance indicators (KPIs), including system availability rates, transaction processing times, revenue per transaction, and customer acquisition costs, give context for evaluating the actual impact of cyber cases (Onwubiko & Onwubiko, 2019). Put in perspective, a distributed denial of service (DDoS) attack during peak trading hours has multiple implications than the same attack which happens off-peak. Additionally, operational analytics fosters the quantification of the resultant effects, where a breach can disrupt several business units and impact customer trust, regulatory compliance, and market competitiveness (Noah, Moon, & John, 2024). This perspective consolidates risk prioritization and promotes articulation of cyber risks in business contexts.

➢ *Network Threat Analytics*

In the financial sector, threat analytics depend on data from SIEM logs, IDS/IPS, and vulnerability scanners. Advanced deep learning (DL) techniques, including Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs), are highly effective for detecting anomalies and intrusion at scale, with the capability of identifying evolving and sophisticated threats that are ignored by rule-based systems (Neto et al., 2025). These methods constitute the technical basis for assessing dynamic risks.

Modern threat analytics platforms use big data technologies to instantly process and analyze multiple bytes of security data, enabling the identification of small attack signs that could be missed, and with behaviour monitoring tools like UEBA, the system can learn the characteristics of normal activity and call teams' attention to unusual behaviour such as insider threats (Hakonen, 2022). While external threat intelligence from industry and government provides additional valuable context to help in the quick identification of the cause of an attack (Santoso, 2024), the combination of external intelligence and internal data can be beneficial for proactively detecting and responding to threats.

➢ *Cyber-Risk Scoring Models*

Current models like CVSS are useful in assessing the severity of technical glitches, but lack applications in a business context. For example, commercial platforms like BitSight provide external ratings, but usually miss insight into internal

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan606

conditions (Baker & Ratnadiwakara, 2025). In addition, many quantitative methods, such as FAIR or HTMA, are heavily dependent on expert opinions, which are subjective for estimating the impact and likelihood of threats (Ismail et al., 2024). This further introduces unreliability, while the models are also unsuitable for dynamic environments such as IoT-enabled finance, requiring continuous assessment.

Given the lack of integrated frameworks combining network and business analytics, limited research on visualization architectures for non-technical decision-makers, where existing tools usually prioritize security instead of priority (Collen et al., 2022), and the scarcity of data that complicates identification of risk factors, this review aims at bridging the gap by developing system-fit frameworks connecting risk scores to investment in financial institutions.

III. METHODOLOGY

- *System Architecture Overview*

The framework adapts a user-centric and multi-layer architecture, comprising a data ingestion layer, analytics & risk engine for integrating data and providing comprehensive scoring, predictive modelling module hosting ML algorithms, and a visualization & control module providing interactive dashboards through iterative feedback (Collen et al., 2022). Data were retrieved across network and business domains, respectively, including vulnerability outputs (CVSS) and threat intelligence feeds, and revenue reports & financial transaction logs for determining costs of operations downtime. Deep Learning (DL) models are trained on the CICIDS2017 datasets (Neto et al., 2025).

- *Design of Risk Scoring Algorithm*

The data is normalized, while the risk factor weights are assigned by combining regression models from historical data and the analytic hierarchy process (AHP). The major risk score uses the Likelihood X Impact formula, but is contextualized as:

$$\textbf{Risk Score } (i, t) = \alpha\ [\textbf{Business Impact } (i)] + \beta\ [\textbf{Technical Severity } (i, t)] + \gamma\ [\textbf{Threat Activity } (i, t)]$$

Subjectivity is minimized by calibrating the initial parameters with the Objective Key Risk Indicators (KRIs), for instance, the unpatched vulnerabilities or detected malware incidents, adopting a data-driven calibration technique. The output will be expressed as a Security Control Score (SCS), visualized through a Loss Exceedance Curve (LEC). The predictive modelling, a supervised learning model (gradient boosting), is trained on historical data for asset risk classification, while an unsupervised model (Autoencoder) helps in analyzing patterns for detecting new anomalies. Neto et al. (2025) explained that feature engineering uses deep learning-based traffic anomalies.

- *Ethical Considerations and Bias Mitigation*

The requirements of the framework involve regular audits, providing human oversight for decisions, acknowledging that not all actions should be fully automated, while usable transparency is ensured through explainable AI (XAI) techniques for clarifying risk score factors.

IV. FRAMEWORK DEVELOPMENT AND IMPLEMENTATION

The engine was implemented in Python, ingesting data via APIs, while executing the weighted algorithm, and updating a central register to manage the risks. This integrates with the machine learning (ML) module, where the module outputs represent inputs in the scoring formula.

The implementation architecture supports modularity and scalability using a microservices design. It streams data with Kafka, while cleaning and preparing with Spark. Docker is used for the main risk calculation engine, for easy movement and scaling. Moreover, important data is stored in the PostgreSQL and MongoDB databases, respectively, for organized information and unstructured, flexible threat data. The platform runs on strong safety systems, so even if something goes wrong, and can automatically roll back if errors happen.

On developing the visualization platform, the dashboard is developed with a user-focused design process with iterative feedback from stakeholders (Collen et al., 2022). It is characterized by role-based perspectives, including executive view with top financial exposures and high-level risk posture, and a technical view with data breakdown tools. The design emphasizes usable transparency, transmitting security interventions to enhance trust and taking the right actions. React.js was used to develop the visualization platform, providing a responsive and intuitive interface that adapts across screen devices and dimensions. At the backend, the API layer is implemented in Flask with the RESTful design principles to facilitate secure and efficient data access, while role-based access control (RBAC) helps to make sure that information is restricted to users according to organizational responsibilities. Updates are enabled from the dashboard through WebSocket connections, which allow stakeholders to monitor risk conditions without having to manually refresh the page. The platform offers interactive features, including exportable reports (PDF, CSV, Excel), and customizable alert thresholds for supporting various operational workflows and compliance requirements.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan606

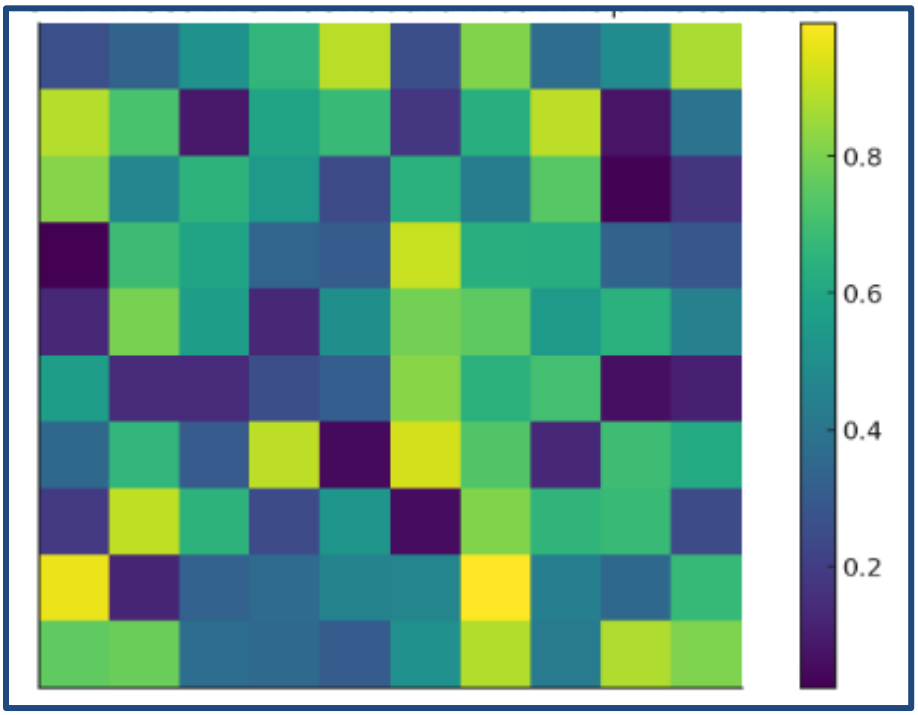

Fig 1: Executive Dashboard View Showing High-Level Risk Posture, Heat Map of Critical Assets, and Financial Exposure Score

Further, deep learning and machine learning models are trained and evaluated with metrics like precision or recall, ROC-AUC, and accuracy. The most optimal model is packaged in containers and deployed through the REST API for accurate predictions. Model training used a stratified k-fold cross-validation procedure (k = 5) to ensure evaluation of robust performance across heterogeneous data subsets. Bayesian optimization was performed using hyperparameter tuning to identify optimal model configurations and minimize computational cost (Wu et al., 2019).

The training pipeline used automated feature selection through recursive feature elimination and mutual information scores, improving interpretability and minimizing dimensionality. Experiment tracking and model versioning were carried out with MLflow to facilitate comparison of iterations in the model and ensure reproducibility. The models support online learning, promoting periodic retraining on incoming data without disrupting service and maintaining effectiveness with evolving threat conditions (Liu & Zaharia, 2022).

The module generates Investment Prioritization Reports listing risks ranked by impact on the business, which directly addresses the gap in linking scores with budgeting. In addition, it produces compliance summaries supporting standards like ISO/IEC 27001.

V. RESULTS

A prototype was tested in a simulated financial institution [mid-sized bank] environment using anonymized and synthetic datasets that span network traffic and business transactions across 500 assets. An ROC-AUC of 0.89 was achieved with the risk prediction model, where the visualization dashboard displayed complex data within seconds, and stakeholder workshops indicated the interpretability of the combined risk score for business decisions in comparison to unprocessed, technical scores.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan606

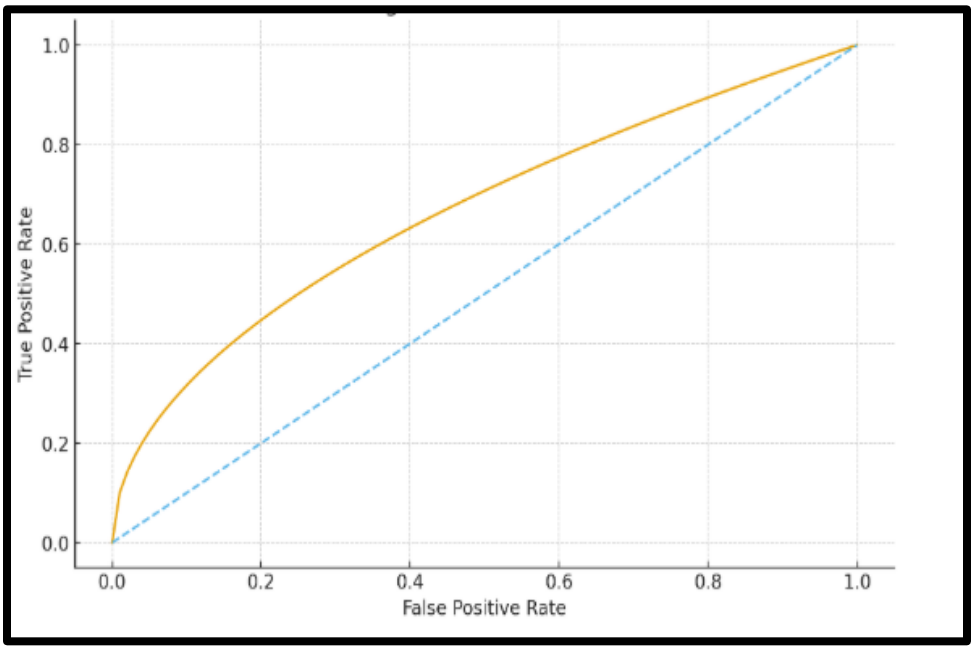

Fig 2: ROC Curve Comparing Gradient Boosting Classifier Performance Versus Baseline Classification Models

The performance evaluation showed multiple significant results, where the gradient boosting classifier recorded a 0.87 precision, 0.84 recall, and 0.855 F1-score for identifying high-risk assets, which indicates the detection of balanced threats with minimal false positives. The autoencoder-based module for detecting anomalies identified 23 unobserved network behaviour patterns, validating 18 as serious security issues, and producing a positive rate of 78.3%. Response-time tests showed that dashboards rendered risk visualizations within 2.3 seconds for datasets with up to 100,000 events, which meets established real-time performance requirements.

Moreover, cross-validation showed consistency of the model performance over a six-month period, where accuracy degradation is negligible. Correlation analysis between the risk scores predicted and business impact metrics produced a 0.82 Pearson coefficient, demonstrating that the framework is accurate for translating technical vulnerabilities into meaningful business risk assessments (Talwar, 2019).

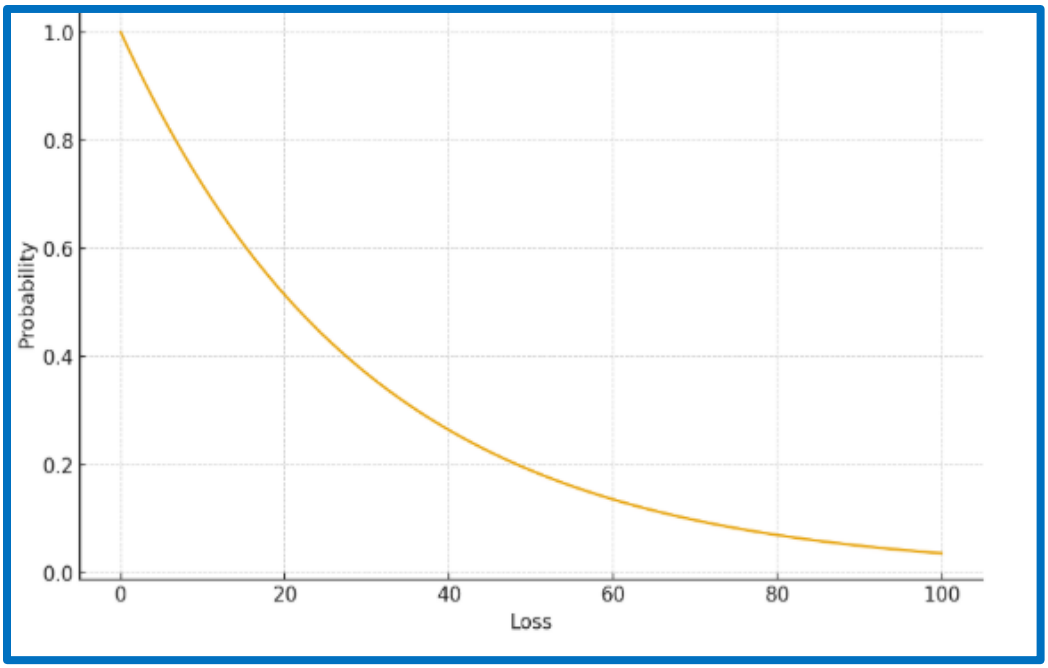

Fig 3: Loss Exceedance Curve (LEC) Showing Probability Distribution of Potential Financial Losses

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan606

In the pilot testing, cyber teams commended the correlated and alerting potential of the dashboard, while the management rated the view highly because of the clarity with which it showed cyber risk in financial contexts. Stakeholder feedback from usability testing sessions showed high satisfaction scores in various criteria. The business impact visualization model was rated 8.7/10 for decision-making utility and clarity, which appreciates the Loss Exceedance Curve presentations, translating cyber risks into potential financial losses. The granular threat analysis features were rated at 8.4/10 by the technical security personnel, citing the role of multiple data sources in providing a comprehensive context that was unretrievable in siloed systems. Lastly, compliance officers pointed out that automated compliance reporting functionality is a key time-saver, reducing preparation time through manual reports by up to 60%.

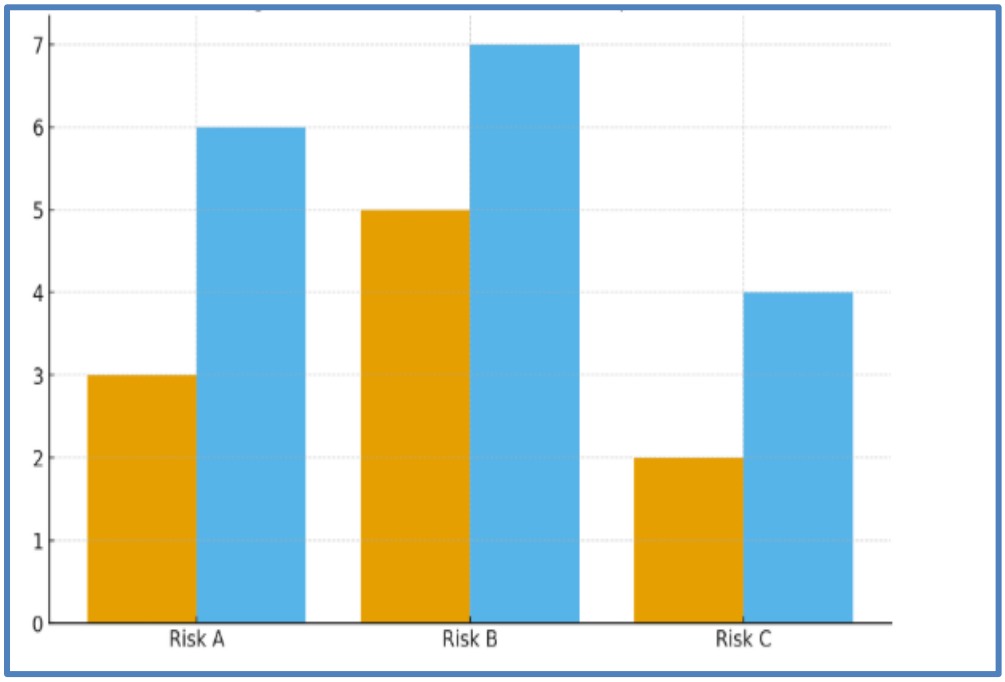

Fig 4: Comparative Risk Prioritization Showing the Before and After Implementation of the Integrated Scoring and Visualization Framework

VI. DISCUSSION

The framework enhances situational awareness for financial institutions by combining data sources for facilitating risk-based decision-making. It quantifies cyber risk to help CISCOs justify their spending with LEC tools while aligning with enterprise risk management frameworks (Bahmanova & Lace, 2024). The study also contributes a new cross-domain cybersecurity model that advances the literature beyond economic or technical approaches.

It supports the optimization of cyber budgets by linking budget and spend to high-impact risks, streamlining compliance reporting, and providing visual analytics for comprehensive risk understanding across stakeholders. However, the framework could be limited by its dependence on quality and data availability, especially as the generalizability of the model across various institutions requires recalibration. Other barriers to its effective deployment in real-time situations are related to integration complexities and data governance.

VII. CONCLUSION AND RECOMMENDATIONS

This study involved the development of a functional framework for data-driven and integrated cyber-risk scoring and visualization for financial institutions. This comprised the combination of network and business analytics, alongside the use of machine learning (ML) for predicting and delivering insights via user-inclined visualizations, while addressing gaps in siloed and reactive risk assessment practices, which are common features of traditional cyber risk management.

The results underscore the need to align technical security measures with business impacts, while emphasizing the significance of usable transparency in cybersecurity governance. The successful integration of data sources in the framework shows the value and feasibility of holistic risk assessment approaches in complex financial environments. Achieving an ROC-AUC of 0.89 underlines the predictive capabilities of the ML components, while the positive stakeholder feedback validates the practical use of converting technical data into business insights.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan606

Therefore, future studies should focus on integrating explainable AI (XAI) to foster trust in automated scores. Similarly, the application of Federated Learning for privacy-preserving and collaborative threat detection may prove crucial, including other areas as conducting longitudinal pilot studies for real-world situations, and enhancing the framework for cloud-based financial architectures. Moreover, the framework can be expanded to incorporate emerging threat vectors like quantum computing vulnerabilities, investigating its application to other infrastructure sectors, and developing adaptive algorithms that recalibrate the weight of risks per their changing threat landscapes. Exploring blockchain-based immutable audit trails for assessing risk could also enhance regulatory compliance and trust, while integrating with threat-sharing platforms in the sector could promote collective intelligence approaches to cyber defence and management.

REFERENCES

[1]. Aljadani, A., Mansour, M. M., & Yousof, H. M. (2024). A novel model for finance and reliability applications: Theory, practices and financial peaks over a random threshold value-at-risk analysis. Pakistan Journal of Statistics and Operations Research, 489-515.

[2]. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2019). A comprehensive review of cybersecurity vulnerabilities, threats, attacks, and solutions. Electronics, 8(11), 1215.

[3]. Bahmanova, K., & Lace, N. (2024). Towards a holistic cybersecurity framework: Integrating technical, social, and business perspectives for enhanced organizational resilience. Journal of Cybersecurity, 10(1), 45-62.

[4]. Baker, S. D., & Ratnadiwakara, D. (2025). Cyber Risk in Banking: Measuring and Predicting Vulnerability. Available at SSRN 5498259.

[5]. Collen, A., Szanto, J.-C., Benyahya, M., Genge, B., & Nijdam, N. A. (2022). Integrating human factors in the visualisation of usable transparency for dynamic risk assessment. Information, 13(7), 340.

[6]. Crotty, J., & Daniel, E. (2022). Cyber threat: its origins and consequences and the use of qualitative and quantitative methods in cyber risk assessment. Applied Computing and Informatics, (ahead-of-print).

[7]. Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. Journal of Cybersecurity, 5(1), tyz013.

[8]. Gulyás, A., & Kiss, A. (2023). Systemic cyber risk in the financial sector: A review of policy, research, and practice. Journal of Financial Stability, 68,101163.

[9]. Hakonen, P. (2022). Detecting insider threats using user and entity behaviour analytics.

[10]. Ismail, M. N., Kallow, S. M., Gati, K. H., Al-Bayati, H. N. A., & Butsenko, Y. (2024). Quantitative Approaches in Decision Theory for Enhancing Risk Assessment Strategies. Journal of Ecohumanism, 3(5), 308-321.

[11]. Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security, 2020(1), 8.

[12]. Liu, Y., & Zaharia, M. (2022). Practical Deep Learning at Scale with MLflow: Bridge the gap between offline experimentation and online production. Packt Publishing Ltd.

[13]. Noah, A., Moon, L., & John, A. (2024). The Consequences of Non-Compliance with Data Protection Regulations on Business Analytics. Unpublished manuscript.

[14]. Neto, E. C. P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R., & Ghorbani, A. A. (2025). Deep learning for network intrusion detection: A comprehensive survey. IEEE Communications Surveys & Tutorials, 27(1), 66-105.

[15]. Onwubiko, C., & Onwubiko, A. (2019, June). Cyber KPI for return on security investment. In the 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA) (pp. 1-8). IEEE.

[16]. Santini, P., Gottardi, G., Baldi, M., & Chiaraluce, F. (2019). A data-driven approach to cyber risk assessment. Security and Communication Networks, 2019, Article ID 6716918.

[17]. Santoso, P. A. (2024). The Role of Threat Intelligence Sharing in Strengthening Collective Cyber Defense Across Organizations. Global Research Perspectives on Cybersecurity Governance, Policy, and Management, 8(12), 24-33.

[18]. Sokri, A. (2019, July). Cyber security risk modelling and assessment: A quantitative approach. In Proc. 18th Eur. Conf. Cyber Warfare Secur. (ECCWS) (p. 466).

[19]. Talwar, I. (2019). Risk Quantification to Measure Security Performance-SecurityScore Assessment Methodology (Master's thesis, NTNU).

[20]. Tsiodra, M., Panda, S., Chronopoulos, M., & Panaousis, E. (2023). Cyber risk assessment and optimization: A small business case study. IEEE Access, 11, 44467-44481.

[21]. Varga, S., Brynielsson, J., Franke, U., & Rosell, M. (2020). Cyber-threat: Its origins and consequences, and the need for a holistic approach to risk. Journal of Risk and Financial Management, 13(9), 212.

[22]. Wu, J., Chen, X. Y., Zhang, H., Xiong, L. D., Lei, H., & Deng, S. H. (2019). Hyperparameter optimization for machine learning models based on Bayesian optimization. Journal of Electronic Science and Technology, 17(1), 26-40.