Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

Predictive Risk Analytics for Financial Technology Infrastructure: Integrating Machine Learning, Data Quality Intelligence, and Cybersecurity Threat Modeling

David Excel Ozowara (0009-0003-2386-2949)[1*], Chukwudera Obumneke Anunagba (0009-0003-3949-5290) [2]

[1] *Goldman Sachs, Dallas, Texas, USA.*

[2] *Barclays, Whippany, New Jersey, USA.*

***Corresponding author:** David Excel Ozowara, daveozzy6@gmail.com*

***Author emails:** David Excel Ozowara: daveozzy6@gmail.com; Chukwudera Obumneke Anunagba: chiokemuo@gmail.com*

ARTICLE INFO

Received: 02 Sept 2025

Revised: 20 Oct 2025

Accepted: 29 Oct 2025

ABSTRACT

The growing interdependence of financial technology infrastructure, cybersecurity systems, and third-party digital services has created complex risk environments that conventional, isolated assessment methods cannot adequately capture. Although machine learning has demonstrated considerable potential in financial risk forecasting and cybersecurity threat detection, existing approaches often overlook the influence of data quality, infrastructure dependencies, changing threat conditions, and operational decision-making. This paper critically reviews developments in machine learning-based financial risk prediction, dynamic cybersecurity risk assessment, cyber threat intelligence, and data governance, and proposes an integrated conceptual framework for predictive risk intelligence in FinTech environments. The proposed framework combines asset and dependency intelligence, vulnerability and threat modeling, data quality assessment, financial consequence estimation, explainable machine learning, and risk-based mitigation decisions. Mathematical formulations are introduced to conceptualize multidimensional data quality, quality-adjusted risk estimation, dependency propagation, and resource-constrained mitigation. The review identifies significant research gaps in end-to-end validation, temporal generalizability, cross-institutional evaluation, and the measurement of data quality as a component of predictive uncertainty. It also outlines an evaluation strategy incorporating predictive performance, calibration, operational response, and resilience outcomes. The study contributes a theoretically grounded architecture for connecting cyber exposure with financial consequences while preserving explainability, uncertainty awareness, and human accountability. Future empirical research is required to establish the framework's effectiveness across heterogeneous financial technology environments.

Keywords: Financial Technology; Predictive Risk Analytics; Machine Learning; Data Quality Intelligence; Cybersecurity Threat Modeling; Cyber-Financial Risk; Explainable Artificial Intelligence; Operational Resilience.

1 INTRODUCTION: FROM ISOLATED RISK MODELS TO RESILIENT FINTECH INFRASTRUCTURE

FinTech infrastructure combines payment platforms, banking applications, cloud services, mobile devices, data exchanges, and third-party software into continuously connected operating systems. This connectivity changes risk from a set of separable exposures into a networked problem in which a cyber incident can interrupt services, compromise data, alter transactions, and transmit losses across organizational boundaries. Reviews of FinTech security identify privacy violations, data breaches, malware, hacking, insider threats, identity theft, social engineering, and distributed denial-of-service attacks as recurring classes of exposure (G. Ali et al., 2024; Javaheri et al., 2023). Financial institutions therefore require analytical systems that connect technical vulnerabilities with operational disruption and financial consequences rather than ranking isolated weaknesses alone.

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

Traditional financial risk models and static cybersecurity assessments remain useful reference points, but they assume more stable variables and clearer boundaries than digital financial systems permit. Machine learning extends prediction across credit, market, operational, liquidity, and systemic risk, while dynamic cybersecurity assessment incorporates changing vulnerabilities, exploitation conditions, asset dependencies, and security posture (Cheimonidis & Rantos, 2023; Islam et al., 2025; Mashrur et al., 2020). The resulting challenge is methodological: predictive accuracy cannot substitute for valid data, interpretable reasoning, or an operational link to mitigation.

This review treats **predictive risk intelligence** as an integrated capability with four connected functions: estimating financial and cyber risk, identifying the conditions that produce it, explaining model outputs to accountable decision-makers, and directing scarce protective resources. Evidence from financial-risk studies shows that relevant predictors vary between normal and extreme market conditions (Chen et al., 2024). Cybersecurity studies similarly show that threat patterns, exploitation likelihood, asset dependencies, and breach impacts must be updated as systems change (Islam et al., 2025; Kia et al., 2023). The following sections examine these domains separately before specifying an architecture that joins them through assets, threats, controls, and financial consequences.

1.1 Research Objectives and Contributions

Despite substantial progress in machine learning-based financial risk prediction and cybersecurity risk assessment, several methodological and operational challenges limit their integration into a unified FinTech risk intelligence capability. Existing approaches frequently evaluate financial risk, cybersecurity exposure, and infrastructure resilience through separate analytical pipelines, restricting the ability to investigate how technical vulnerabilities propagate through interconnected services and generate operational or financial consequences. Furthermore, inadequate treatment of data quality, temporal dependencies, model uncertainty, and mitigation effectiveness can undermine the reliability and usefulness of integrated predictions.

This study addresses these limitations through four research objectives:

1. To critically examine existing machine learning approaches for financial risk prediction, cybersecurity threat assessment, and dynamic vulnerability prioritization.
2. To investigate how data quality dimensions, including completeness, timeliness, consistency, provenance, and reliability, influence the trustworthiness of predictive risk estimates.
3. To develop an integrated conceptual architecture linking infrastructure assets, cybersecurity threats, operational dependencies, financial consequences, and risk mitigation decisions.
4. To formulate a structured approach for evaluating predictive performance, explainability, operational effectiveness, and infrastructure resilience within FinTech environments.

The principal contribution is a cross-domain conceptual framework that explicitly incorporates data quality intelligence into cyber-financial risk estimation and mitigation planning. Unlike approaches that focus primarily on predictive accuracy or vulnerability severity, the proposed architecture emphasizes contextual exposure, uncertainty, infrastructure dependencies, and decision-oriented risk management.

The framework is presented as a theoretical contribution requiring subsequent empirical validation rather than as a deployed or experimentally verified predictive system.

1.2 Review Methodology and Analytical Framework

This study adopts a narrative, integrative literature review approach to synthesize research across machine learning, financial risk management, cybersecurity threat intelligence, data quality governance, and digital infrastructure resilience. The review emphasizes the relationships among these disciplines and their implications for the development of integrated predictive risk analytics architectures.

The reviewed literature is organized into five analytical domains: (1) machine learning-based financial and systemic risk prediction; (2) dynamic cybersecurity risk assessment and vulnerability prioritization; (3) threat intelligence,

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

attribution, and supply-chain security; (4) data quality, explainability, and governance; and (5) integrated cyber-financial risk management and operational resilience.

The synthesis applies four comparative dimensions. First, the predictive objective identifies the risk outcome, including financial loss, credit deterioration, exploitability, threat detection, or service disruption. Second, the data dimension examines the sources, preprocessing requirements, temporal characteristics, and quality limitations influencing model reliability. Third, the analytical dimension considers machine learning approaches, interpretability mechanisms, and validation strategies. Fourth, the operational dimension assesses how model outputs support intervention, resource allocation, risk mitigation, and resilience decisions.

Particular attention is given to the distinction between experimentally demonstrated findings and conceptual recommendations. Reported predictive performance is interpreted within the dataset and validation conditions described by each study, while architectural integration and mathematical formulations developed in this paper are treated as proposals for future evaluation.

As a narrative review, the study does not claim exhaustive coverage of the literature or undertake a formal meta-analysis. Its conclusions should therefore be interpreted as a structured synthesis of selected relevant research rather than as pooled estimates of model effectiveness.

2 MACHINE LEARNING FOR FINANCIAL, BANKING, AND SYSTEMIC RISK PREDICTION

Machine learning has expanded financial risk analysis from relatively constrained statistical relationships toward models that can process heterogeneous firm, market, macroeconomic, and network information. A survey of financial-risk research organizes applications across prediction, assessment, and management tasks, while a review of banking studies reports sustained attention to credit risk and growing application to market and operational risk (Heß & Damásio, 2025; Mashrur et al., 2020). This expansion does not imply that one algorithm or data source is appropriate for every risk class. Credit decisions involve borrower-level classification, market risk reflects changing prices and volatility, liquidity risk depends on funding and flows, and enterprise risk combines operational, regulatory, technological, and financial exposures.

2.1 Predictive Modeling Across Credit, Market, Liquidity, and Enterprise Risk

Credit-risk prediction remains the most developed banking application because institutions possess structured records of borrowers, repayment histories, debt measures, loan terms, and outcomes. A recent financial-risk study reports a hybrid CatBoost and support-vector-machine model with an accuracy of 95.93% and an F1 score of 0.95 on its dataset, while identifying total debt-to-income ratio, loan duration, and interest rate as important predictors (Hossan et al., 2025). These results indicate how nonlinear classifiers and feature analysis can support classification under high-dimensional and imbalanced conditions. They do not establish universal superiority, because performance depends on the dataset, target definition, preprocessing choices, and validation design.

The broader literature maps neural networks, tree-based methods, support-vector methods, and other algorithms to multiple financial-risk tasks (Mashrur et al., 2020). Tree ensembles can represent nonlinear interactions among firm characteristics, market indicators, and macroeconomic variables, whereas neural models can process sequential or high-dimensional inputs. Yet the banking review identifies a persistent imbalance in the evidence: credit applications receive more attention than liquidity and some other risk types (Heß & Damásio, 2025). This uneven coverage matters for FinTech firms whose exposure may arise from rapid payment outflows, platform outages, dependence on external funding, or concentrated service providers rather than conventional loan portfolios.

Market and enterprise risk require models that recognize changing regimes and dependencies. Machine learning can classify risk states, estimate expected impacts, or identify features associated with adverse conditions, but the output must be interpreted in relation to the decision horizon. A short-horizon fraud or transaction model may optimize detection latency, whereas enterprise risk management must consider service continuity, regulatory exposure, customer trust, and correlated losses. AI-based FinTech risk frameworks therefore place data infrastructure, model development, operational integration, and continuous adaptation alongside algorithm

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

selection (Battula, 2025). The analytical question is not simply whether a model predicts an event, but whether its prediction arrives in a form that can change an authorized decision.

2.2 Systemic Risk Drivers Under Normal and Extreme Financial Conditions

Systemic risk analysis demonstrates why context-sensitive prediction is necessary. Using random forests and gradient-boosted regression trees, research on FinTech and traditional institutions evaluates macroeconomic variables, firm characteristics, and network topologies under normal and extreme market conditions, with Shapley individual and interaction values used for interpretation (Chen et al., 2024). Under extreme upside and downside conditions, market volatility, individual stock volatility, and market capitalization are positive systemic-risk drivers. Under normal conditions, high price-earnings ratios, large market capitalization, and low individual volatility are associated with market stabilization (Chen et al., 2024). The same feature can therefore change meaning when the market regime changes.

The study also distinguishes the information value of different feature groups. Macroeconomic variables are the most important extreme-condition drivers, whereas firm characteristics matter more under normal conditions (Chen et al., 2024). Interactions between individual volatility and market capitalization or market volatility are prominent sources of extreme systemic risk, while market capitalization is the most important interaction attribute under normal conditions (Chen et al., 2024). These findings caution against treating feature importance as a fixed property of an institution. A model trained on ordinary observations may understate variables that become influential during stress.

Network information is especially relevant to FinTech because institutions depend on shared payment rails, cloud providers, identity services, application programming interfaces, and outsourced technology. The systemic-risk evidence supports the broader proposition that interactions among variables can carry more information than isolated predictors (Chen et al., 2024). A cyber event affecting a highly connected provider may consequently create a financial effect that cannot be inferred from the provider's standalone risk score. Integrated platforms must therefore retain interaction terms and dependency representations rather than reducing every exposure to an independent probability.

2.3 The Trade-Off Between Predictive Performance, Interpretability, and Decision Usefulness

High predictive performance is valuable only when the model's target, data, and decision context are credible. The financial-risk literature presents machine learning as promising while identifying challenges involving data, changing environments, and the translation of predictions into risk management (Mashrur et al., 2020). A reported accuracy or F1 score describes performance on a defined dataset and endpoint; it does not by itself demonstrate stability across institutions, market regimes, or future attack conditions. Class imbalance, synthetic oversampling, dimensionality reduction, and feature selection can improve measured performance, but each choice changes the relationship between observed data and operational use (Hossan et al., 2025).

Explainability addresses a separate requirement. Shapley values can show how features contribute to a systemic-risk prediction and can reveal interactions that would be hidden by a single aggregate score (Chen et al., 2024). Feature importance in a credit model can similarly identify variables that decision-makers may examine, but explanation does not prove causality. A plausible variable may proxy for an omitted factor, reflect institutional policy, or become unstable after a regime change.

Decision usefulness also depends on calibration, timing, actionability, and accountability. A model that identifies a high-risk borrower, market state, or institution must connect the score to an intervention, escalation rule, or resource allocation choice. Banking research therefore recommends greater integration of machine learning into established risk-management frameworks rather than treating models as detached prediction engines (Heß & Damásio, 2025). The same principle applies to cybersecurity, where dynamic risk estimates must be connected to vulnerability remediation, monitoring, incident response, and resilience planning.

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

Table 1. Comparative Analysis of Machine Learning Approaches for Financial and Cybersecurity Risk Prediction

Study	Research Focus	Methods / Approach	Key Contribution	Identified Limitation
Mashrur et al. (2020)	Financial risk management	Survey of ML methods	Maps ML applications across financial risk tasks	Limited demonstration of integrated operational deployment
Chen et al. (2024)	Systemic risk prediction	Random forests, gradient boosting, SHAP	Identifies regime-dependent systemic risk drivers	Findings depend on observed market conditions and data
Hossan et al. (2025)	Financial risk prediction	Hybrid CatBoost and SVM	Reports 95.93% accuracy and 0.95 F1 on the evaluated dataset	Cross-institutional generalizability not established
Kia et al. (2023)	Cyber risk forecasting	CVE topic modeling and supervised regression	Predicts cyber-risk patterns from vulnerability descriptions	Limited visibility into organization-specific exposure
Islam et al. (2025)	Dynamic cyber risk assessment	Linear regression and deep learning	Incorporates exploitation, dependencies, and explainability	Broader operational and financial effects require evaluation
Noor et al. (2019)	Cyber threat attribution	NLP and ML classification	Uses high-level attack patterns for attribution	Historical reports and attribution uncertainty
Yeboah-Ofori et al. (2021)	Cyber supply-chain security	LR, SVM, RF, decision trees	Predicts selected threat classes from cyber intelligence	Financial loss propagation not established
Zangana & Mohammed (2025)	Mobile payment security	Random forests, isolation forests, autoencoders	Integrates behavioral, device, and network evidence	Long-term concept drift robustness remains uncertain

Table 1 compares representative predictive approaches reviewed in this study. The comparison highlights the differences in prediction targets, analytical methods, and research limitations, demonstrating that existing models predominantly address individual financial or cybersecurity risk domains rather than end-to-end cyber-financial risk intelligence.

3 DYNAMIC CYBERSECURITY RISK ASSESSMENT AND QUANTIFICATION IN FINTECH ENVIRONMENTS

FinTech systems change faster than conventional periodic risk assessments can represent. Applications are added, configurations are altered, dependencies shift, vulnerabilities are disclosed, and attackers adapt their methods. A systematic review of dynamic cybersecurity risk assessment examines 50 models and reports that these approaches seek near-real-time assessment by incorporating changing information into organizational risk estimates (Cheimonidis & Rantos, 2023). The central problem is therefore temporal and relational: risk depends on what

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

assets exist, how they are connected, which weaknesses are exploitable, and what consequences follow from compromise.

3.1 From Static Vulnerability Assessment to Dynamic Cyber Risk Prediction

Static vulnerability assessment generally assigns severity to a weakness and leaves the surrounding operational context implicit. Dynamic assessment updates the estimate as asset exposure, exploitation evidence, dependencies, and organizational conditions change (Cheimonidis & Rantos, 2023). The distinction is material for FinTech platforms because a vulnerability in an isolated test service differs from one in an internet-facing payment component connected to identity, settlement, and customer-data systems. A useful model must therefore represent both vulnerability properties and the state of the environment in which they appear.

The d-CSRM framework addresses this problem by combining vulnerability exploitation and asset dependencies with a hybrid model based on linear regression and deep learning (Islam et al., 2025). Its experiment uses CVE data to prioritize vulnerabilities and identifies exploit type, exploit platform, and impact among the selected features associated with dynamic risk (Islam et al., 2025). The framework also incorporates explainability and interpretability so that users can examine influential features and the model's decision process (Islam et al., 2025). This approach moves beyond a static severity label, although CVE-based evaluation cannot by itself capture every organizational condition, attacker intention, or business consequence.

A related prediction model, CyRiPred, uses CVE descriptions, maps textual content to relevant topics, aggregates topic occurrence and severity into time series, and applies supervised regressors to predict cyber-risk groups (Kia et al., 2023). Its design reduces reliance on expert judgment by deriving risk estimates from structured vulnerability information (Kia et al., 2023). That reduction can improve reproducibility, but it also creates a dependence on the completeness, consistency, and semantic stability of CVE descriptions. The model predicts from recorded vulnerability patterns; it cannot observe undisclosed weaknesses, unreported exploitation, or asset-specific exposure unless those variables enter the data.

Dynamic assessment can be represented as a recurrent process rather than a one-time score (Figure 1):

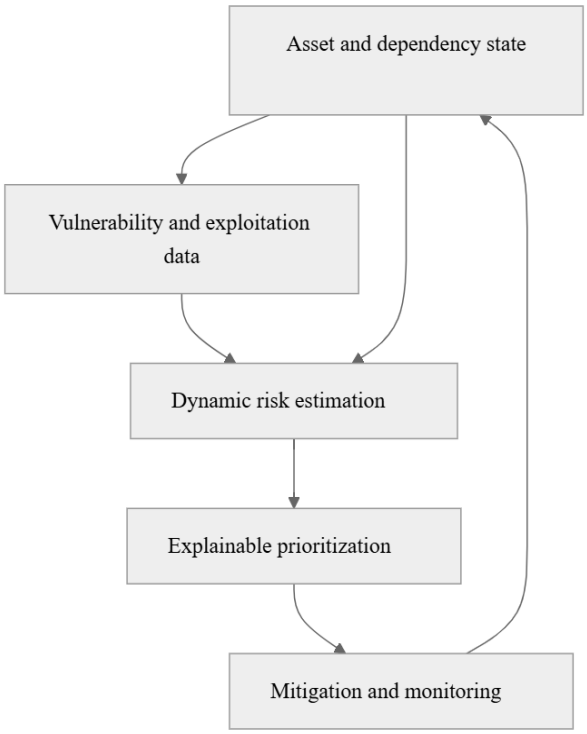


Figure 1. Dynamic cyber-risk assessment cycle.

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

This cycle links changing infrastructure to updated prioritization and then feeds mitigation effects back into the next assessment. The literature supports the need for such updating, but the maturity and application domains of dynamic models remain uneven (Cheimonidis & Rantos, 2023). A model should consequently disclose its update frequency, data provenance, prediction horizon, and conditions under which its outputs cease to be reliable.

3.2 Quantifying Breach Severity, Exposure, and Mitigation Priority

Prediction becomes operationally useful when it distinguishes likelihood, impact, and exposure instead of collapsing them prematurely. A cybersecurity risk quantification framework combines content analysis of real data breaches with a likelihood-impact matrix to classify breach severity and inform mitigation (Zadeh et al., 2023). Applied to breaches involving S&P 500 organizations, the framework identifies hacking and loss or theft of portable media as breach types with the highest reported impact and probability (Zadeh et al., 2023). The result illustrates how event categories can support prioritization, while also showing that severity assessment requires more than counting incidents.

Breach severity should encompass the affected information, compromised systems, service disruption, recoverability, and consequences for affected parties. The cited framework provides a structured classification approach, but the reported evaluation does not establish that its categories predict future losses across all FinTech settings (Zadeh et al., 2023). Financial platforms may experience immediate transaction disruption even when data exfiltration is limited, whereas a data breach may generate delayed regulatory, legal, and reputational effects. Risk quantification must preserve these distinct endpoints rather than treating every breach as one financial loss variable.

Exposure also depends on asset centrality and dependency. Islam and colleagues incorporate asset dependencies into dynamic prioritization, indicating that a vulnerability's importance rises or falls with the systems connected to it (Islam et al., 2025). A vulnerability score can therefore be combined with exploit evidence, exposure status, affected asset value, and dependency criticality. This combination should remain auditable: decision-makers need to know whether a high score reflects exploitability, impact, connectivity, or missing data.

Mitigation priority is a decision output, not a synonym for predicted risk. The appropriate intervention may be patching, compensating controls, access restriction, enhanced monitoring, service segmentation, backup testing, or supplier engagement. A model that ranks vulnerabilities without estimating remediation cost, implementation time, residual risk, and service consequences offers only partial decision support. The risk-management framework and investment analysis literature treats cybersecurity as a continuous process in which security performance and cyberinvestment costs must be considered together (Lee, 2021). Quantification should therefore support portfolio choices, not merely produce a ranked list.

3.3 AI-Enabled Risk Management for Digital and Critical Infrastructure Resilience

AI-enabled cybersecurity systems can process transaction data, logs, vulnerability records, threat reports, and infrastructure telemetry at a scale that manual assessment cannot sustain. A FinTech predictive-analytics review describes anomaly detection, reinforcement learning, and natural language processing as methods for identifying threat patterns, extracting intelligence, and supporting dynamic risk assessment (Ekundayo et al., 2024). The same review connects cloud analytics with defenses against distributed denial-of-service attacks and ransomware, and describes automated incident response as a means of reducing response time and operational disruption (Ekundayo et al., 2024). These claims establish a broad operating agenda, but they do not replace evaluation of false positives, missed attacks, or response harms.

Critical-infrastructure research illustrates a complementary architecture. A threat-hunting system uses distributed, scalable, online-configurable components, machine learning analysis, and visualization to help specialists examine large volumes of mostly benign data and identify unusual behavior (Lozano et al., 2023). The value lies in reducing analyst overload while preserving human situational awareness, rather than delegating every security decision to an opaque classifier. A national critical-infrastructure study reports high classification performance for several machine-learning and deep-learning models after imputation, transformation, class balancing, and feature selection, with the LSTM obtaining 99% accuracy and the CNN obtaining 98% accuracy, precision of 98%, recall of

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

97%, and an F1 score of 97% (S. M. Ali et al., 2025). These results are model- and dataset-specific, and the preprocessing pipeline itself becomes part of the evidence that must be governed.

Resilience requires recovery and adaptation as well as detection. FinTech security reviews recommend continuous monitoring, zero-trust policies, testing, backup, access control, and collaboration among firms, regulators, and specialists (G. Ali et al., 2024). AI can prioritize signals and controls, but it cannot eliminate dependence on reliable inventories, trained analysts, tested recovery procedures, or accountable governance. Dynamic cybersecurity assessment therefore provides the bridge from changing technical evidence to resilience decisions, while threat intelligence supplies information about adversaries and attack campaigns.

4 THREAT INTELLIGENCE, ATTRIBUTION, AND THREAT MODELING ACROSS THE FINTECH ATTACK SURFACE

Threat intelligence adds adversary behavior and campaign context to vulnerability and asset data. FinTech systems expose several attack surfaces at once: mobile applications, payment transactions, cloud services, APIs, employee endpoints, identity systems, and suppliers. A systematic review identifies 11 central FinTech cyber-threat categories and nine corresponding defense strategies across the reviewed literature (Javaheri et al., 2023). Predictive analytics is most useful when it relates these threat observations to specific assets, attack stages, and possible financial consequences.

4.1 Machine Learning for Threat Detection in Mobile Payments and FinTech Networks

Mobile payments generate behavioral and technical signals that signature-based systems may not capture. A mobile-payment framework combines behavioral analytics, device fingerprinting, network anomaly detection, static application metadata, and dynamic transaction behavior, using supervised and unsupervised models including random forests, isolation forests, and autoencoders (Zangana & Mohammed, 2025). This combination supports detection of known and zero-day threats by linking what an application is, how a device behaves, and how transactions move through the network (Zangana & Mohammed, 2025). The conceptual advantage is the integration of heterogeneous evidence rather than reliance on a single indicator.

Anomaly detection is particularly relevant where labeled attack examples are scarce. Isolation Forest and autoencoder approaches can identify observations that depart from learned patterns, while supervised models can classify known threat types when labels are available (Zangana & Mohammed, 2025). Yet unusual behavior is not equivalent to malicious behavior. Legitimate travel, device replacement, service changes, high-value payments, or sudden market activity can produce anomalies, so alerts require contextual review and calibrated thresholds.

Predictive CTI broadens the input beyond transaction systems. Research on FinTech threat intelligence describes processing dark-web forums, phishing campaigns, malware logs, social media, and other unstructured sources with big-data methods and natural language processing (Ekundayo et al., 2024). These sources may indicate emerging campaigns before they appear in internal telemetry, but their reliability, duplication, access conditions, and adversarial manipulation must be assessed. A threat model should record the provenance and confidence of each signal instead of treating every extracted phrase or anomaly as equivalent evidence.

Detection performance also has operational dimensions. A classifier with high recall may generate an unmanageable alert volume, while a precise model may miss low-frequency attacks. The mobile-payment study reports superior precision, recall, and F1 performance relative to signature- and rule-based systems on its datasets (Zangana & Mohammed, 2025), but the reported evaluation does not establish performance under sustained concept drift or coordinated adversarial manipulation. Deployment decisions should therefore consider false-alert cost, investigation capacity, latency, and the consequences of automated blocking.

4.2 Indicators of Compromise, Threat Attribution, and Collaborative Intelligence Sharing

Low-level indicators of compromise, such as hashes, addresses, and isolated technical artifacts, can be changed or reused across unrelated campaigns. Noor and colleagues argue that attribution should incorporate higher-level tactics, techniques, procedures, software, and malware patterns that evolve less rapidly than individual indicators (Noor et al., 2019). Their framework extracts attack patterns from textual CTI reports through distributional

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

semantics, profiles threat actors, and trains five classifiers using 327 publicly available incident reports covering events from May 2012 to February 2018 (Noor et al., 2019). The deep-learning classifier reached 94% accuracy, while the framework's reported attribution precision was 83%, compared with 33% for other public profiles (Noor et al., 2019).

These results support structured representation of adversary behavior, but attribution remains an inferential task. Shared tools, copied procedures, false flags, incomplete reports, and changing campaign behavior can make an actor profile appear more certain than the underlying evidence permits. High-level patterns are more reusable than single indicators, yet they can still be adopted by multiple actors. Attribution outputs should therefore guide defensive preparation and intelligence prioritization without being treated as definitive identity claims.

Collaborative intelligence can improve detection when institutions share more than raw indicators. Preuveneers and Joosen propose sharing machine-learning models through MISP, TheHive, and Cortex, using counter-evidence to reduce false positives and false negatives (Preuveneers & Joosen, 2021). Their design also addresses confidentiality through fine-grained access to encrypted models and related artifacts, while recognizing that the models themselves can be attacked (Preuveneers & Joosen, 2021). This finding changes the governance object: organizations must protect shared models, training data, access rights, and update processes in addition to conventional CTI records.

A collaborative system requires common semantics and safeguards against poisoning, leakage, and strategic non-disclosure. The attribution study demonstrates the value of converting unstructured reports into machine-readable profiles (Noor et al., 2019), while the model-sharing study demonstrates why shared intelligence must preserve confidentiality and adversarial robustness (Preuveneers & Joosen, 2021). Together, they suggest that effective CTI depends on both representation and trust. Threat intelligence can inform financial-risk models only when its provenance, confidence, and intended use are visible.

4.3 Threat Hunting and Predictive Analytics for Cyber Supply Chain Security

Supply-chain risk extends beyond an institution's direct control. FinTech firms depend on software libraries, cloud infrastructure, payment processors, identity providers, telecommunications, data vendors, and managed security services. A cyber supply-chain study frames the supply chain as a set of interconnected subsystems in which a weakness or threat at any point can disrupt broader business continuity (Yeboah-Ofori et al., 2021). Threat modeling must consequently represent supplier relationships and inherited exposure rather than limiting assessment to internally managed assets.

The study combines CTI and machine learning using attack and tactics, techniques, and procedures as inputs and vulnerabilities and indicators of compromise as outputs. It evaluates logistic regression, support-vector machines, random forests, and decision trees on the Microsoft Malware Prediction dataset (Yeboah-Ofori et al., 2021). Spyware or ransomware and spear phishing were the most predictable threats in that experiment, and the authors recommend corresponding controls (Yeboah-Ofori et al., 2021). Because the data and labels define what can be learned, these results should inform prioritization for comparable threat classes rather than be generalized to every supplier ecosystem.

Threat hunting complements predictive classification by searching for weak signals and unknown behavior. The critical-infrastructure architecture described earlier uses modular, distributed components and visualizations to support analysts facing high-volume data and delayed discovery of previously unknown attacks (Lozano et al., 2023). In a supply-chain setting, hunting can examine unusual software updates, unexpected authentication paths, anomalous supplier traffic, or changes in dependency behavior. Such hypotheses require asset inventories and relationship data that many organizations do not maintain consistently.

Predictive supply-chain security should therefore combine three views: vulnerability exposure, observed adversary behavior, and dependency consequences. A vulnerable component with no reachable path may receive less immediate attention than a moderately severe weakness in a highly connected provider. Conversely, an apparently quiet supplier may warrant monitoring when intelligence indicates a campaign targeting its technology sector. This

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

logic connects CTI to dynamic risk assessment and creates the need for data-quality controls before integrated financial and cyber scores can be trusted.

5 DATA QUALITY, EXPLAINABILITY, AND GOVERNANCE AS CONDITIONS FOR TRUSTWORTHY RISK INTELLIGENCE

Predictive risk intelligence inherits the weaknesses of its data. Financial records may contain missing or inconsistent fields, cyber reports may use incompatible vocabularies, and asset inventories may omit dependencies. The resulting problem is not limited to model accuracy: poor data can distort priorities, conceal vulnerable services, and produce unjustified confidence. Data quality, explanation, and governance must therefore be treated as operating conditions for risk analysis rather than post hoc technical refinements.

5.1 Data Dependence in Vulnerability, Threat, and Financial-Risk Prediction

CVE-based models offer scale and reproducibility, but they describe reported vulnerabilities rather than the complete state of an organization. CyRiPred derives time series from textual CVE topics and severity, then predicts occurrence and impact (Kia et al., 2023). The d-CSRM framework adds exploitation and asset dependency information, showing why environmental context changes prioritization (Islam et al., 2025). The contrast identifies a basic data-quality requirement: vulnerability records must be linked to asset identity, exposure, configuration, exploit evidence, and business function.

Threat intelligence creates a different data problem. CTI reports are often textual and unstructured, making machine interpretation difficult (Noor et al., 2019). NLP can extract higher-level attack patterns, but errors in entity recognition, terminology, translation, duplication, or attribution labels can propagate into classifier training. Model-sharing research further shows that shared intelligence requires protection against adversarial machine-learning attacks and confidentiality loss (Preuveneers & Joosen, 2021). Data provenance must therefore accompany both human-authored reports and derived indicators.

Financial models face analogous issues. The systemic-risk study shows that the importance of macroeconomic, firm, and network variables changes with market conditions (Chen et al., 2024). A dataset dominated by normal periods may not represent extreme conditions, while a credit dataset shaped by historical lending policies may reproduce those policies rather than measure borrower risk alone. Preprocessing methods such as multiple imputation, standard scaling, feature elimination, and SMOTE can address particular technical problems, but they do not make missingness, selection, or label bias disappear (S. M. Ali et al., 2025; Hossan et al., 2025).

5.2 Quantitative Data Quality Intelligence for Predictive Risk Models

Data quality should be incorporated into predictive risk assessment as a measurable and continuously monitored analytical variable rather than treated exclusively as a preprocessing requirement. In complex FinTech environments, incomplete transaction records, delayed security events, inconsistent asset identifiers, unreliable threat intelligence, and missing dependency relationships may collectively distort risk estimates. Consequently, an integrated framework should evaluate the quality of its supporting evidence before translating model predictions into operational decisions.

This study proposes a multidimensional Data Quality Intelligence Index (DQII) comprising five dimensions: completeness, timeliness, consistency, provenance reliability, and label reliability. These dimensions address both the structural integrity of recorded information and the credibility of its interpretation.

Table 2. Proposed Data Quality Intelligence Metrics for FinTech Predictive Risk Models

Data Quality Dimension	Definition	Proposed Measurement	Risk Implication
Completeness	Availability of required data fields and records	Valid required observations / expected observations	Missing records may conceal exposure or distort predictions

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

Timeliness	Freshness of information relative to its operational use	Proportion meeting defined freshness thresholds	Delayed signals may increase detection and response latency
Consistency	Agreement of values across integrated systems	Consistent records / evaluated records	Conflicting records may distort asset and transaction relationships
Provenance reliability	Traceability and credibility of information sources	Validated provenance records / evaluated records	Unverifiable sources may reduce evidential reliability
Label reliability	Accuracy and consistency of assigned outcome labels	Verified labels / assessed labels	Incorrect labels may bias supervised learning and evaluation

Table 2 defines the proposed dimensions of data quality intelligence and their operational implications for predictive risk analytics. The metrics provide candidate measurements for the Data Quality Intelligence Index (DQII). Measurement rules, normalization procedures, and acceptable quality thresholds should be adapted to the application and empirically validated.

The proposed index is expressed in Equation (1).

$$DQII_t = w_c C_t + w_t T_t + w_s S_t + w_p P_t + w_l L_t$$

Subject to:

$$\sum_{j \in \{c,t,s,p,l\}} w_j = 1, \qquad w_j \geq 0$$

Where C_t = completeness, T_t = timeliness, S_t = consistency, P_t= provenance reliability, and L_t = label reliability at time t. All five component scores and the resulting index are in [0,1].

The weights represent relative importance and require justification through expert assessment or calibration.

The weights may be determined through expert judgment, risk-based governance priorities, or empirical optimization using historical prediction errors. All dimensions should be normalized to a common scale before aggregation. For applications where one critical quality dimension cannot be compensated for by stronger performance elsewhere, the weighted index should be supplemented by minimum quality thresholds.

The index is not intended to imply that the influence of poor data quality on model reliability is necessarily linear. Instead, it provides an interpretable starting point for monitoring evidence quality and testing the relationship between data degradation, predictive calibration, and operational decision outcomes.

The proposed framework also distinguishes data quality from predictive confidence. High-quality observations may support an incorrect or poorly calibrated model, while incomplete evidence may occasionally coincide with an accurate estimate. Accordingly, data quality should enter model confidence assessment through empirically evaluated relationships rather than through unsupported assumptions of equivalence.

5.3 Quality-Adjusted Predictive Risk Estimation

The relationship between data quality and risk prediction requires explicit treatment of uncertainty. Conventional predictive models typically estimate risk conditional on the available observations, assuming that their inputs adequately represent the underlying environment. In practice, missing asset relationships, delayed vulnerability disclosures, inconsistent transaction records, and unreliable incident labels can increase uncertainty and lead to unstable risk assessments.

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

To represent this relationship, the proposed framework distinguishes the baseline predicted risk from the quality-related uncertainty surrounding that prediction. The baseline estimate is obtained from a machine learning model incorporating financial, cybersecurity, and infrastructure-related features, as expressed in Equation (2).

$$\hat{R}_{i,t} = f_\theta\left(X_{i,t}^F, X_{i,t}^C, X_{i,t}^D\right)$$

A conservative quality-adjusted risk prioritization score can subsequently be formulated using Equation (3).

$$R_{i,t}^{QA} = \hat{R}_{i,t} + \lambda\left(1 - DQII_{i,t}\right)U_{i,t}$$

Where:

- $\hat{R}_{i,t}$ = baseline risk score for asset or service i at time t.
- $X^F, X^C and\ X^D$ = financial, cybersecurity, and dependency features.
- f_θ = predictive model parameterized by θ
- $U_{i,t}$ = normalized uncertainty indicator.
- λ = nonnegative uncertainty-penalty coefficient.
- R^{QA} = quality-adjusted prioritization score.

For these equations, define $\hat{R}$, U and $DQII$ as normalized quantities when comparisons across assets are required. The quality-adjusted score is not automatically bounded to 1; a model implementation must explicitly define any normalization or clipping policy.

These are proposed mathematical models, not experimentally established relationships.

The uncertainty adjustment is designed to increase the priority of cases in which potentially consequential exposure is supported by incomplete or unreliable evidence. Importantly, the resulting score represents a decision-oriented prioritization measure rather than a calibrated probability of loss. The adjustment parameter should be determined through historical analysis, scenario testing, or institutional risk tolerance rather than assigned arbitrarily.

This formulation permits a system to distinguish between an observed low-risk condition supported by reliable evidence and an apparently low-risk condition arising from incomplete monitoring. Such differentiation is particularly important in financial infrastructure, where missing evidence can conceal highly connected vulnerabilities or emerging threats.

Empirical validation should determine whether the adjustment improves decisions, reduces missed high-impact events, or merely increases false-positive investigations.

5.4 Explainable and Interpretable Models for Human-Centered Risk Decisions

Interpretability concerns how a model's internal operation can be understood, whereas **explainability** concerns how a particular output can be related to influential evidence. The d-CSRM framework explicitly incorporates both, identifying features linked to vulnerability priority and exposing aspects of model decision-making (Islam et al., 2025). The systemic-risk study uses Shapley individual and interaction values to show how predictors contribute under different market conditions (Chen et al., 2024). These methods can make scores more reviewable, but they do not establish that the model's associations are causal.

Human-centered use requires explanations matched to the decision. A security engineer may need the affected asset, exploit condition, dependency path, and compensating control, while a risk committee may need expected disruption, financial exposure, uncertainty, and remediation cost. A global feature ranking cannot answer all of these questions. Explanation should therefore be generated at the level of the action being considered and should display data freshness and confidence where possible.

Interpretability also has limits when models are combined or updated. A hybrid model may improve predictive flexibility while making it harder to identify one stable decision rule. A feature that is influential during extreme systemic conditions may be less relevant during normal periods (Chen et al., 2024). Explanations must

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

consequently be conditional, time-stamped, and tested for stability rather than presented as permanent descriptions of risk.

5.5 Investment, Cost, and Governance Constraints on AI-Based Cybersecurity

AI adoption requires expenditure on data infrastructure, model development, monitoring, skilled personnel, secure integration, and incident response. Cybersecurity investment analysis frames risk management as a continuous improvement process that must consider both security performance and investment cost (Lee, 2021). A high-risk prediction does not automatically justify the most expensive control if a lower-cost measure provides comparable risk reduction or if implementation would disrupt a critical service. Governance should compare residual risk, control effectiveness, cost, and operational feasibility.

Regulation and privacy add constraints to data collection and sharing. FinTech reviews recommend regulatory compliance, access control, encryption, testing, security training, and collaboration among stakeholders (G. Ali et al., 2024). Shared machine-learning models can improve collective detection, but encrypted access and protection against attacks on the models are required (Preuveneers & Joosen, 2021). Governance must define who may inspect data, alter models, approve automated actions, and challenge a risk score.

The practical objective is accountable augmentation. Models should prioritize evidence and surface changing conditions, while human authorities retain responsibility for consequential decisions, exceptions, and recovery trade-offs. This governance position prepares the final integration: financial and cyber models should exchange structured evidence without erasing their different endpoints, uncertainties, or accountability requirements.

6 INTEGRATING FINANCIAL RISK ANALYTICS WITH CYBERSECURITY THREAT MODELS

Integration should not mean merging every variable into one opaque score. Financial risk models estimate effects such as credit deterioration, market stress, liquidity pressure, or enterprise loss, whereas cybersecurity models estimate vulnerability, exploitation, threat activity, breach severity, and control weakness. Their relationship is causal and operational: a cyber condition can alter a financial exposure, and a financial condition can change the resources available for protection or recovery. An integrated platform should preserve these distinctions while making their dependencies explicit.

6.1 A Layered Architecture Linking Assets, Vulnerabilities, Threats, and Financial Consequences

A useful architecture begins with an **asset layer** that identifies applications, data stores, payment components, identities, devices, cloud services, and suppliers. The asset layer should record ownership, business function, connectivity, dependency relationships, and service criticality. Dynamic cybersecurity research establishes why assets and dependencies must be updated as infrastructure changes (Islam et al., 2025). Without this inventory, a vulnerability score cannot reveal whether an exposed component supports settlement, authentication, customer communication, or a low-consequence internal function.

The second layer represents vulnerabilities and controls. CVE records, configuration findings, patch status, exploit evidence, access conditions, and compensating controls describe the technical state. CyRiPred shows how vulnerability text and temporal occurrence can feed supervised prediction, while d-CSRM demonstrates the added value of exploitation and dependency features (Islam et al., 2025; Kia et al., 2023). Control data should include remediation status and residual exposure so that a predicted risk can be compared with the protection already in place.

The third layer represents threats and adversary behavior. High-level TTPs, malware, software, phishing patterns, and campaign information provide more durable features for attribution than isolated low-level indicators (Noor et al., 2019). CTI models can extract these patterns from unstructured reports, but confidence and provenance must remain attached to each observation. Collaborative intelligence can extend detection by sharing machine-learning models and counter-evidence, subject to confidentiality and adversarial-robustness controls (Preuveneers & Joosen, 2021).

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

The fourth layer translates technical exposure into operational and financial consequences. A breach framework distinguishes likelihood and impact in severity assessment (Zadeh et al., 2023). Financial analytics then estimate consequences such as transaction interruption, liquidity pressure, market reaction, credit deterioration, recovery cost, or regulatory exposure, provided that the relevant data and endpoint are defined. The architecture should not assume that every cyber event produces the same financial pathway; a denial-of-service event, credential compromise, ransomware incident, and data exfiltration can affect different services and time horizons.

The layers can be represented as a directed evidence chain (Figure 2):



Figure 2. Directed evidence chain linking assets, vulnerabilities, threats, controls, and financial consequences.

This structure permits separate models at each layer and explicit links between their outputs. A vulnerability model can estimate exploitability, a threat model can estimate campaign relevance, and a financial model can estimate consequence conditional on affected service. Their combination can be reviewed more easily than a single model trained on an undifferentiated target.

Table 3. Proposed Integrated Cyber-Financial Risk Intelligence Architecture

Architecture Layer	Data Inputs	Analytical Function	Expected Output
Asset and Dependency Intelligence	Asset inventories, service maps, cloud configurations, supplier relationships	Dependency mapping and criticality analysis	Asset exposure and dependency profiles
Data Quality Intelligence	Source metadata, timestamps, validation records, missingness indicators	Completeness, timeliness, consistency, provenance, and reliability assessment	DQII and quality alerts
Vulnerability and	CVEs, exploit evidence, CTI	Threat classification,	Threat likelihood and

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

Threat Intelligence	reports, attack patterns, security logs	exploitability estimation, anomaly detection	vulnerability priorities
Financial Risk Analytics	Transactions, liquidity indicators, business impact records, financial exposures	Financial consequence estimation and scenario analysis	Conditional financial loss estimates
Integrated Risk Evaluation	Cyber predictions, financial estimates, dependencies, uncertainty	Quality-aware risk scoring and cross-domain risk assessment	Integrated risk estimates and prioritization
Mitigation and Resilience	Control inventories, remediation costs, recovery requirements	Resource-constrained control selection and response planning	Mitigation recommendations and residual-risk estimates
Governance and Feedback	Model logs, explanations, monitoring results, incident outcomes	Explainability, performance monitoring, accountability	Audit records, escalation decisions, model updates

Table 3 operationalizes the proposed layered architecture by identifying the information, analytical functions, and outputs associated with each component. Data Quality Intelligence and governance operate across multiple layers, while feedback from mitigation and observed incidents supports continuous reassessment. The architecture represents a proposed conceptual design rather than an implemented system.

Network structure should be treated as evidence rather than decoration. The systemic-risk study finds that network topologies and interactions among predictors help explain risk under normal and extreme conditions (Chen et al., 2024). In FinTech infrastructure, dependency centrality may amplify the effect of a cyber incident by exposing several institutions or services to a common provider. The integrated model should therefore represent shared infrastructure, substitution options, concentration, and recovery dependencies where reliable data exist.

To operationalize the proposed integration of machine learning, data quality intelligence, and cybersecurity threat modeling, Figure 3 presents a unified conceptual framework illustrating the relationships among heterogeneous data sources, quality assessment, predictive risk estimation, financial consequence modeling, mitigation decisions, and continuous governance.

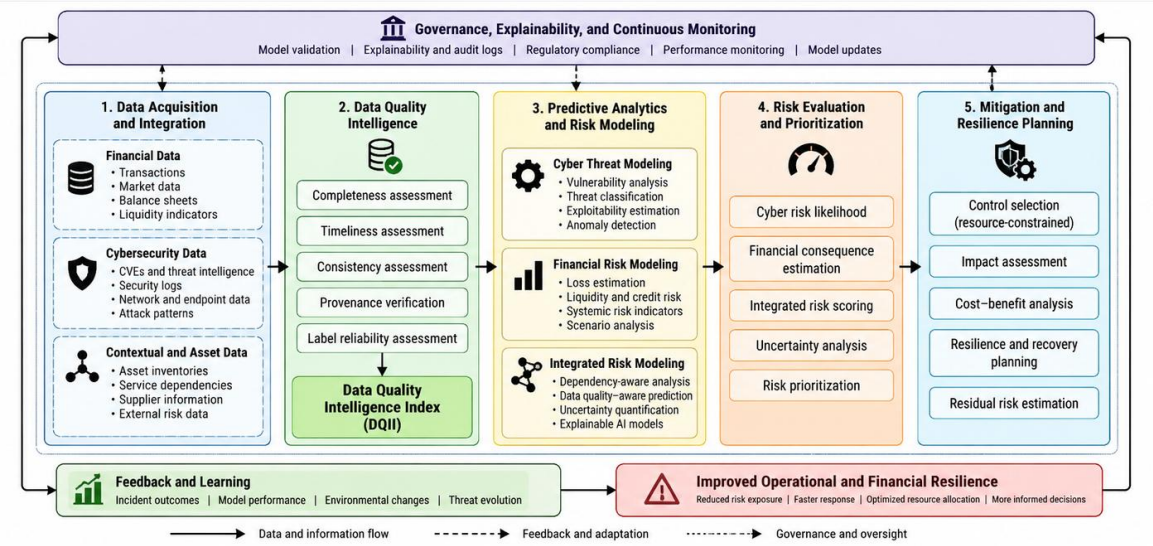


Figure 3. Integrated Cyber-Financial Risk Intelligence Framework with Data Quality Feedback.

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

Figure 3 illustrates the proposed end-to-end cyber-financial risk intelligence framework, integrating data acquisition, data quality intelligence, predictive analytics, risk evaluation, and mitigation planning within a unified governance structure. Financial transaction records, cybersecurity telemetry, vulnerability intelligence, and infrastructure dependency information are subjected to multidimensional quality assessment encompassing completeness, timeliness, consistency, provenance, and label reliability. The resulting Data Quality Intelligence Index (DQII) informs predictive modeling and uncertainty-aware risk prioritization. Cybersecurity threat models and financial risk analytics are subsequently integrated to estimate potential operational disruptions and financial consequences. The framework supports risk-based control selection, resource allocation, residual-risk assessment, and recovery planning. Continuous feedback from incident outcomes, model performance, infrastructure changes, and evolving threats supports periodic reassessment and adaptation. This architecture provides a conceptual foundation for explainable, data-quality-aware, and resilience-oriented risk management in FinTech environments.

6.2 Mathematical Formulation of Integrated Cyber-Financial Risk

The proposed integrated architecture requires an analytical formulation connecting the probability of cybersecurity-related disruptions with their potential financial and operational consequences. Rather than combining heterogeneous risk indicators into a single uncalibrated score, the framework separates the likelihood of adverse events, conditional financial impact, infrastructure dependency, and uncertainty.

For an asset or service, financial exposure may be represented through the expected loss associated with a set of defined cyber incident scenarios over a specified prediction horizon.

The integrated expected cyber-financial loss is expressed in Equation (4).

$$ECL_{i,t}(H) = \sum_{k=1}^{K} p_{i,k,t}\,(H)\,\mathbb{E}\left[L_{i,k,t} \mid A_{i,k,t}(H)\right]$$

Where:

- $ECL_{i,t}(H)$ = expected cyber-financial loss associated with asset i over horizon H.
- K = number of mutually exclusive incident scenarios, including combinations of simultaneous events where relevant.
- $p_{i,k,t}(H)$ = probability of scenario k occurring during the prediction horizon.
- $L_{i,k,t}$ = financial loss conditional on that incident scenario.
- $A_{i,k,t}(H)$ = event representing scenario k.

This scenario partition is important: adding probabilities or expected losses from overlapping scenarios without accounting for dependence can overstate the aggregate exposure.

The formulation permits different incidents to produce distinct consequences, including payment interruption, transaction loss, recovery expenditure, regulatory costs, and service restoration requirements. By conditioning loss estimates on the specific incident scenario and affected asset, the framework avoids assuming that all technical vulnerabilities produce equivalent financial effects.

Threat intelligence, vulnerability information, control effectiveness, and infrastructure dependencies are used to estimate scenario likelihood, while operational and financial records support estimation of conditional consequences. This structure enables separate validation of event likelihood and loss severity, making the overall prediction more interpretable.

The framework also accommodates changing conditions through time-indexed estimates. As threats emerge, controls are deployed, financial conditions change, or service dependencies are modified, the expected-loss calculation can be updated using the latest verified evidence.

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

A critical implementation requirement is that likelihood estimates must be calibrated against a clearly defined event outcome and time horizon. Moreover, the framework should avoid double-counting financial consequences when incidents share underlying causes or affect overlapping services.

6.3 Connecting Predictive Risk Scores to Mitigation, Allocation, and Resilience Decisions

A predictive score becomes useful when it changes an action. Vulnerability prioritization can direct patching, segmentation, access restriction, threat hunting, or additional monitoring. Breach-severity estimates can inform containment, notification, recovery, and customer protection. Financial-risk predictions can guide liquidity buffers, credit review, market hedging, or escalation to enterprise risk committees. These actions should be linked through decision rules that state what evidence triggers intervention and what uncertainty requires human review.

Risk scores should be decomposed into at least likelihood, impact, exposure, confidence, and time horizon. A high likelihood with low service impact may receive a different treatment from a low likelihood event that could interrupt payment settlement. The likelihood-impact matrix in breach quantification research provides a structured basis for this distinction (Zadeh et al., 2023). Dynamic vulnerability frameworks add the requirement to consider exploitation and asset dependencies, which can alter both likelihood and impact as the environment changes (Islam et al., 2025).

Resource allocation should compare expected risk reduction with cost and implementation constraints. Cyberinvestment analysis frames security improvement as continuous and cost-sensitive rather than as a one-time technology purchase (Lee, 2021). A financial institution might prioritize a supplier-facing authentication weakness over a more severe but isolated defect if the former threatens a highly connected payment service. Such prioritization is defensible only when the dependency evidence and consequence assumptions are visible to reviewers.

Decision support should also include counterfactual and residual-risk information. If a patch reduces exploitability but requires downtime, the platform should show the temporary service consequence and the remaining exposure after deployment. If a compensating control reduces detection time rather than breach probability, the model should preserve that distinction. Explanatory methods from systemic-risk and dynamic-cybersecurity studies can identify influential features, but the organization must still validate whether the proposed control changes those features or merely changes their measurement (Chen et al., 2024; Islam et al., 2025).

Resilience extends beyond prevention. Threat-hunting architectures emphasize analyst visualization and situational awareness when attacks are unknown or delayed (Lozano et al., 2023). Predictive CTI proposes automated response and dynamic analysis, but response automation must be bounded by service criticality and the cost of erroneous blocking (Ekundayo et al., 2024). An integrated platform should therefore support graduated actions: observe, investigate, contain, remediate, recover, and reassess. Each action should produce new evidence for the next model update.

The operational loop can be organized around four questions: what is exposed, what is changing, what could happen, and what should be done now. The first question uses assets, vulnerabilities, and dependencies. The second uses telemetry, CTI, market conditions, and model-drift indicators. The third combines threat likelihood with operational and financial consequence. The fourth compares mitigation options, cost, uncertainty, and resilience objectives. This sequence prevents predictive analytics from becoming a dashboard that reports danger without allocating responsibility.

6.4 Risk-Based Mitigation Optimization

Predictive risk assessment generates operational value when its outputs support the allocation of limited cybersecurity and resilience resources. Financial technology institutions typically face competing remediation requirements, finite budgets, service availability constraints, and varying implementation costs. Consequently, vulnerability ranking alone is insufficient to establish an optimal mitigation strategy.

The proposed framework introduces a resource-constrained optimization model that evaluates candidate cybersecurity controls according to their expected contribution to risk reduction and implementation cost.

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

The optimization objective is formulated in Equation (5).

$$\min_{\mathbf{x}} J(\mathbf{x}) = ECL^{res}(\mathbf{x}) + \sum_{j=1}^{M} c_j x_j$$

The associated budget constraint is given in Equation (6).

$$\sum_{j=1}^{M} c_j x_j \leq B, \qquad x_j \in \{0,1\}$$

Where:

- $ECL^{res}(\mathbf{x})$ = residual expected cyber-financial loss after the selected controls are applied.
- x_j = binary decision to implement control \(j\).
- c_j = total implementation cost of control \(j\).
- B = available mitigation budget.
- M = number of candidate controls.

All financial amounts should refer to the same planning horizon and currency. The objective minimizes residual expected loss plus mitigation expenditure, subject to the budget. Additional constraints may be required to represent mandatory controls or operational incompatibilities.

The formulation enables decision-makers to evaluate alternative mitigation portfolios rather than independently ranking vulnerabilities. Controls affecting highly connected infrastructure components may receive increased consideration when their implementation reduces expected losses across several dependent services.

Mitigation effectiveness should be estimated under clearly defined counterfactual conditions. A control that reduces the probability of compromise may have different financial and operational implications from one that reduces detection latency, limits breach severity, or improves recovery time.

Implementation should also account for control interactions, service interruption requirements, mandatory security obligations, and risk tolerance. Where controls influence one another, their combined risk reduction should be estimated directly rather than calculated as the sum of independent benefits.

The proposed formulation provides a foundation for cost-sensitive mitigation planning, but its effectiveness must be evaluated against existing remediation procedures and observed operational outcomes.

6.5 Managing Cross-Domain and Supply Chain Dependencies in FinTech Infrastructure

Cross-domain dependencies create the greatest challenge for integration because financial and cyber systems use different vocabularies, time scales, and validation standards. A vulnerability may be recorded in days, a threat campaign may develop over hours, and a liquidity effect may unfold over minutes or weeks. A common data model should preserve event time, observation time, prediction horizon, asset identity, source provenance, and confidence. Without these fields, analysts may compare predictions that refer to different states of the system.

Supply-chain dependencies require information that firms may not own. The cyber supply-chain study shows that threats can arise from any subsystem and disrupt overall continuity, while CTI and machine learning can predict selected threat classes and support control recommendations (Yeboah-Ofori et al., 2021). Vendor risk assessments should therefore include software provenance, service connectivity, incident notification, control evidence, recovery arrangements, and concentration. The model should distinguish known supplier weaknesses from unobserved risk rather than assigning low risk to a supplier simply because evidence is absent.

Collaborative intelligence can reduce blind spots, but sharing creates legal, commercial, privacy, and security constraints. Model-based sharing through established CTI and incident-response platforms offers a way to exchange detection capability while limiting raw-data disclosure (Preuveneers & Joosen, 2021). Encryption and

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

fine-grained access help protect shared artifacts, yet adversaries may target the models themselves or poison the evidence used for updates (Preuveneers & Joosen, 2021). Governance should specify validation, revocation, model versioning, and accountability for actions taken from shared intelligence.

Financial contagion and cyber contagion should be analyzed together without assuming that either is automatic. Systemic-risk research shows that macroeconomic conditions, firm characteristics, market volatility, and interactions can change the drivers of risk across regimes (Chen et al., 2024). Cyber supply-chain research shows that interconnected technical subsystems can transmit operational disruption (Yeboah-Ofori et al., 2021). An integrated scenario should ask whether a technical incident affects market confidence, liquidity, settlement, credit, or service continuity, and should identify the evidence required to support each link.

6.6 Dependency-Aware Risk Propagation Modeling

Interconnected financial infrastructure may transmit operational disruptions across applications, payment services, cloud environments, and third-party providers. The extent of propagation depends on service connectivity, dependency criticality, available redundancy, and the ability of dependent components to maintain operation during an upstream failure.

To represent these interactions, the proposed framework models FinTech infrastructure as a directed weighted dependency graph. Nodes represent services, assets, or providers, while directed edges represent operational dependencies through which disruptions may propagate.

The dependency network is represented in Equation (7).

$$G_t = (V_t, E_t, W_t)$$

Where V_t represents infrastructure assets, E_t represents directed dependency relationships, and $W_t = [w_{ij,t}]$ is the corresponding weighted adjacency matrix.

A first-order approximation of propagated service impact is subsequently expressed in Equation (8).

$$I_{i,t}^{prop} = I_{i,t}^{direct} + \sum_{j=1}^{N} w_{ji,t}\, I_{j,t}^{direct}$$

Here, $w_{ji,t}$ represents the influence of a disruption at asset j on asset i. I^{direct} and I^{prop} must use compatible impact units.

Equation (8) models one-step propagation only. It is a suitable conceptual starting point but does not capture recursive cascades, nonlinear saturation, or recovery dynamics. Future research should examine calibrated multi-step propagation models and avoid counting the same downstream loss more than once.

This formulation distinguishes direct impact from additional impact transmitted through connected assets. The dependency weights indicate how strongly a disruption originating from one asset may affect another asset. For example, an identity service supporting multiple payment applications may transmit operational disruption more widely than an isolated internal component.

Although network-based modeling can support identification of potentially influential dependencies, propagation estimates require empirical calibration and should not automatically be interpreted as incident probabilities. Dependency strength may vary with system redundancy, transaction volume, failover capacity, and recovery arrangements.

The graph model also provides a basis for scenario analysis in which the effects of supplier outages, cascading service failures, and concentrated infrastructure dependencies are evaluated before and after proposed mitigation actions.

The final architecture is therefore a governed network of models rather than a universal predictor. Asset and dependency records establish what can be affected; vulnerability and threat models estimate how exposure may be

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

exploited; financial models estimate the consequences under specified conditions; and decision layers compare mitigation and recovery options. Data-quality checks, explanations, human review, and continuous reassessment must accompany every transition. This design retains the predictive advantages documented across financial and cybersecurity studies while making their assumptions visible, their outputs actionable, and their limits relevant to resilient FinTech infrastructure.

7 EVIDENCE TENSIONS AND METHODOLOGICAL LIMITS IN PREDICTIVE FINTECH RISK RESEARCH

7.1 Prediction Versus Explanation in High-Stakes Financial and Cybersecurity Decisions

Predictive accuracy does not by itself establish decision usefulness in financial or cybersecurity risk management. Machine-learning studies report strong classification or prioritization results, yet decision-makers also need to know which features generated a score, whether those features remain valid, and what intervention the score supports (Islam et al., 2025; Mashrur et al., 2020). Systemic-risk research addresses this problem through Shapley individual and interaction values, showing that drivers change across normal and extreme market conditions (Chen et al., 2024). Explanations therefore require both feature attribution and contextual interpretation, rather than a static ranking of influential variables.

The tension is sharper when outputs allocate capital, defer transactions, or prioritize vulnerability remediation. A breach framework converts content analysis into likelihood-impact classifications, whereas a dynamic cybersecurity framework combines regression and deep learning with explanations of vulnerability priorities (Islam et al., 2025; Zadeh et al., 2023). These approaches clarify different decision objects, but neither demonstrates that explanations improve human decisions or reduce realized losses. Explanations may also create misplaced confidence when the underlying data omit dependencies, adversarial behavior, or changing exposure.

7.2 Model Generalizability Under Changing Attack Vectors and Market Conditions

Generalizability is limited when models learn from fixed datasets while the environments they describe change. CyRiPred forecasts cyber risk from CVE topics and historical occurrence and impact, but its reliance on CVE descriptions leaves exposure, organizational controls, and attacker adaptation outside the model (Kia et al., 2023). CTI attribution similarly achieves high reported performance from textual profiles of attack patterns, yet its training material consists of public incident reports covering a defined historical period (Noor et al., 2019). These designs support pattern recognition, not assurance that performance will persist after novel campaigns or altered reporting practices.

Financial models face an analogous regime problem. The relative importance of macroeconomic variables, firm characteristics, volatility, and network attributes changes between normal and extreme market conditions (Chen et al., 2024). Cybersecurity reviews likewise describe dynamic assessment as a response to newly discovered vulnerabilities and shifting threats, while noting uneven maturity across proposed models (Cheimonidis & Rantos, 2023). Validation should therefore separate temporal generalization from random holdout accuracy and test model degradation after changes in attacks, markets, infrastructure, and reporting.

7.3 The Uneven Evidence Base for Data Quality Intelligence and Integrated Risk Analytics

Data quality intelligence remains less developed than predictive modeling itself. Studies describe preprocessing, imputation, feature selection, and class-imbalance correction, but these procedures are usually presented as preparation for model performance rather than as measurable dimensions of operational risk (S. M. Ali et al., 2025; Hossan et al., 2025). CTI research must also transform unstructured reports into machine-readable patterns, creating dependence on extraction quality and source consistency (Noor et al., 2019). Few studies establish how missingness, stale records, duplicated indicators, label uncertainty, or provenance affect downstream financial-risk estimates.

The evidence is thinner still for integrated cyber-financial analytics. Reviews identify extensive work on separate banking risk categories and recommend greater integration into risk-management frameworks (Heß & Damásio, 2025). Cyber supply-chain studies predict selected threats and recommend controls, but do not demonstrate a

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

complete path from supplier evidence through cyber exposure to financial loss or resilience outcomes (Yeboah-Ofori et al., 2021). This uneven evidence cautions against treating a connected architecture as empirically validated merely because its component models perform well.

8 RESEARCH GAPS: TOWARD VALIDATED, DATA-AWARE, AND ADAPTIVE FINTECH RISK PLATFORMS

8.1 Limited Empirical Validation of End-to-End Integrated Frameworks

The principal gap concerns **end-to-end validation**. Existing studies commonly evaluate a classifier, a vulnerability ranking, a breach matrix, or a threat-hunting architecture in isolation (Lozano et al., 2023; Zadeh et al., 2023). Integrated frameworks describe useful links among assets, vulnerabilities, dependencies, threats, and controls, but published evaluations rarely measure whether those links improve mitigation choices or operational continuity (S. M. Ali et al., 2025; Islam et al., 2025). Future research should compare integrated workflows with existing practice using decision quality, remediation timeliness, false-alarm burden, and realized incident consequences.

8.2 Underdeveloped Data Quality Metrics for Predictive Cyber-Financial Models

Research also needs explicit **data quality metrics** tied to model validity. Useful measures should distinguish completeness, timeliness, consistency, provenance, label reliability, and representation of changing attack or market states. Current predictive studies report accuracy, precision, recall, F1 scores, or ranking performance, but these metrics do not reveal whether missing dependencies or biased incident reporting distort risk estimates (S. M. Ali et al., 2025; Zangana & Mohammed, 2025). Data-quality assessment should become a monitored input to model confidence, retraining thresholds, and human escalation.

8.3 Need for Longitudinal, Cross-Institutional, and Operational Evaluations

Short, dataset-bound evaluations cannot establish resilience across institutions or changing conditions. The literature includes synthetic business data, public CVE records, malware-prediction data, and selected mobile-payment datasets, but these settings provide limited evidence about deployment across organizational contexts (Franco et al., 2022; Yeboah-Ofori et al., 2021; Zangana & Mohammed, 2025). Longitudinal studies should test temporal drift, transfer across institutions, adversarial manipulation, and performance during extreme financial conditions. Operational evaluation must connect predictions to actions, costs, recovery, and unintended effects rather than stopping at benchmark scores.

Table 4. Research Gaps and Future Research Directions in Integrated FinTech Risk Analytics

Research Gap	Limitation Identified in Reviewed Literature	Proposed Research Direction	Expected Contribution
Fragmented risk models	Financial and cybersecurity risks are often assessed separately	Develop linked cyber-financial risk models	Improved cross-domain risk assessment
Insufficient data quality measurement	Data preparation is emphasized more than quality-driven uncertainty	Evaluate multidimensional DQII and its predictive value	More transparent data reliability assessment
Limited end-to-end validation	Component models are often evaluated independently	Compare integrated workflows with standalone baselines	Evidence of added decision value
Incomplete dependency modeling	Asset relationships and supplier effects are not consistently quantified	Test dependency-aware impact propagation	Better understanding of cascading disruptions
Limited temporal generalization	Models depend on historical conditions	Conduct longitudinal and regime-sensitive	Improved understanding of model stability

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

		validation	
Uncertain operational effectiveness	Prediction scores are not consistently linked to realized mitigation outcomes	Evaluate cost-sensitive control selection	More defensible mitigation allocation
Explainability limitations	Feature attribution does not demonstrate improved decisions	Conduct analyst-centered decision experiments	Evidence of explanation usefulness
Cross-institutional transfer limitations	Datasets and operational environments vary across institutions	Evaluate transfer learning and external validation	Stronger evidence of generalizability

Table 4 synthesizes the principal research gaps identified by the review and connects them with proposed future research directions. These gaps establish the rationale for extending conventional predictive modeling toward quality-aware, dependency-sensitive, explainable, and operationally validated cyber-financial risk intelligence.

8.4 Proposed Empirical Evaluation Strategy

The proposed framework requires systematic empirical evaluation before claims of predictive superiority, operational effectiveness, or improved resilience can be established. Future studies should adopt a multidimensional evaluation strategy comparing integrated cyber-financial analytics against conventional cybersecurity prioritization and standalone financial-risk prediction approaches.

Table 5. Evaluation Metrics for Predictive Risk Analytics and Operational Resilience

Evaluation Dimension	Proposed Metrics	Evaluation Objective
Predictive discrimination	Precision, recall, F1 score, PR-AUC	Determine the ability to distinguish adverse events from normal observations
Probability calibration	Brier score, calibration curves	Assess agreement between predicted and observed event frequencies
Financial loss estimation	MAE, RMSE, prediction interval coverage	Assess accuracy and uncertainty of loss forecasts
Data quality robustness	Performance degradation under controlled data corruption	Measure sensitivity to incomplete, delayed, or inconsistent data
Threat detection efficiency	False alerts per day, detection latency	Quantify operational monitoring burden
Infrastructure resilience	Recovery time, service interruption duration, affected transaction volume	Evaluate disruption and recovery consequences
Mitigation effectiveness	Estimated loss reduction, control cost, residual exposure	Assess effectiveness of recommended interventions
Explainability and decision quality	Expert agreement, decision accuracy, explanation stability	Evaluate whether model explanations improve decisions
Temporal generalization	Out-of-time performance, drift indicators	Assess reliability under changing operational and threat conditions

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

Table 5 presents a proposed multidimensional evaluation framework. The metrics distinguish predictive accuracy from probability calibration, financial consequences, operational efficiency, and resilience outcomes. Evaluation should be conducted using temporally separated and, where feasible, cross-institutional datasets.

The evaluation should include four complementary experiments.

Experiment 1: Comparative Predictive Performance

Independent financial-risk and cybersecurity models should be compared against an integrated model incorporating asset dependencies, threat intelligence, and operational context. Depending on the prediction target, appropriate measures include precision, recall, F1 score, area under the precision-recall curve, probability calibration, and expected-loss prediction error. Time-based training and testing partitions should be used to minimize temporal information leakage.

Experiment 2: Data Quality Sensitivity Analysis

Controlled data degradation scenarios should be created through missing records, delayed event timestamps, inconsistent asset identifiers, unreliable labels, and incomplete dependency information. The resulting changes in predictive accuracy, calibration, uncertainty, and mitigation decisions should be evaluated. Ablation experiments should determine whether the proposed Data Quality Intelligence Index contributes information beyond conventional preprocessing and missingness indicators.

Experiment 3: Infrastructure Dependency and Scenario Analysis

The dependency-aware model should be evaluated using simulated or historical disruptions affecting payment gateways, authentication systems, database services, cloud providers, and third-party service dependencies. Outcomes should include estimated downstream service impact, affected transaction volume, recovery duration, and the consistency of predicted consequences with observed or independently simulated results.

Experiment 4: Operational Mitigation Effectiveness

Risk-based mitigation recommendations should be compared with severity-based vulnerability ranking and existing organizational remediation procedures under equivalent resource constraints. Relevant outcomes should include expected loss reduction, remediation cost, prioritization agreement with expert assessments, false-alert burden, service availability, and recovery performance.

Model robustness should additionally be examined under changing market conditions, evolving threats, institutional differences, and adversarial manipulation. Explainability should be evaluated not only through feature attribution but also through the ability of qualified analysts to recognize unreliable predictions and select defensible interventions.

Taken together, these experiments would establish whether cross-domain integration and explicit data quality intelligence offer measurable advantages over isolated predictive models. Until such evaluation is completed, the proposed framework should be regarded as a conceptual research contribution rather than an empirically validated operational system.

9 CONCLUSION: BUILDING EXPLAINABLE AND RESILIENT PREDICTIVE RISK INTELLIGENCE FOR FINTECH

The increasing interdependence of financial services, cloud infrastructure, payment systems, cybersecurity controls, and third-party technology providers requires predictive risk management approaches that move beyond isolated analytical models. This study reviewed machine learning applications in financial risk management, dynamic cybersecurity assessment, threat intelligence, data quality governance, and digital infrastructure resilience. The reviewed literature demonstrates the potential of predictive analytics to identify emerging exposures, support vulnerability prioritization, and improve situational awareness. However, predictive performance remains dependent on data quality, institutional context, changing market regimes, infrastructure dependencies, and evolving adversarial behavior.

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The principal contribution of this paper is an integrated conceptual architecture that connects cybersecurity exposure, infrastructure dependencies, operational disruptions, and potential financial consequences. The proposed extensions formalize this architecture through multidimensional data quality assessment, uncertainty-aware risk prioritization, scenario-based cyber-financial loss estimation, dependency-aware impact modeling, and resource-constrained mitigation optimization. These components provide a structured foundation for examining how predictive risk intelligence could support more transparent and financially informed resilience decisions.

An important implication is that data quality should be treated as a monitored component of predictive risk intelligence rather than solely as a preprocessing concern. Similarly, explainability should extend beyond feature rankings to communicate uncertainty, operational dependencies, estimated consequences, and the reasoning supporting mitigation recommendations. Effective implementation also requires human oversight, governance controls, continuous reassessment, and clear accountability for consequential actions.

The study has important limitations. It presents a narrative synthesis and conceptual framework without empirical implementation, independent benchmark evaluation, or longitudinal institutional validation. The mathematical formulations are proposed analytical constructs whose assumptions, parameterization, predictive value, and operational feasibility remain to be tested.

Future research should prioritize longitudinal and cross-institutional validation, data quality sensitivity analysis, dependency propagation modeling, calibrated cyber-financial loss estimation, and comparisons of mitigation effectiveness under realistic operational constraints. By combining technical risk intelligence with financial consequence modeling and accountable decision processes, the proposed framework establishes a foundation for developing adaptive, explainable, and resilience-oriented risk analytics in FinTech infrastructure.

DECLARATIONS

Author contributions: David Excel Ozowara: Conceptualization, Writing – original draft, Writing – review & editing. Chukwudera Obumneke Anunagba: Conceptualization, Writing – original draft, Writing – review & editing.

Funding: This research received no external funding.

Competing interests: The authors declare no competing interests.

Data availability: No new data were generated or analysed in this study.

Use of generative AI: Generative AI tools were used to assist with drafting and language editing. The authors reviewed and edited all content and take full responsibility for the manuscript.

REFERENCES

[1] Ali, G., Mijwil, M. M., Buruga, B. A., & Abotaleb, M. S. A. (2024). A comprehensive review on cybersecurity issues and their mitigation measures in FinTech. *Iraqi Journal for Computer Science and Mathematics*, *5*(3). https://doi.org/10.52866/ijcsm.2024.05.03.004

[2] Ali, S. M., Razzaque, A., Yousaf, M., & Ali, S. S. (2025). A novel AI-Based integrated cybersecurity risk assessment framework and resilience of national critical infrastructure. *IEEE Access*, *13*, 12427–12446. https://doi.org/10.1109/access.2024.3524884

[3] Battula, S. T. (2025). Artificial intelligence-driven risk management for fintech enterprises: Enhancing decision-making through predictive analytics. *International Journal on Science and Technology*, *16*(1). https://doi.org/10.71097/ijsat.v16.i1.2804

[4] Cheimonidis, P., & Rantos, K. (2023). Dynamic risk assessment in cybersecurity: A systematic literature review. *Future Internet*, *15*(10), 324. https://doi.org/10.3390/fi15100324

[5] Chen, Y., Wang, G., Zhu, Y., Xie, C., & Uddin, G. S. (2024). Identifying systemic risk drivers of FinTech and traditional financial institutions: machine learning-based prediction and interpretation. *European Journal of Finance*, *30*(18), 2157–2190. https://doi.org/10.1080/1351847x.2024.2358940

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[6] Ekundayo, F., Atoyebi, I., Soyele, A., & Ogunwobi, E. O. (2024). Predictive analytics for cyber threat intelligence in fintech using big data and machine learning. *International Journal of Research Publication and Reviews*, *5*(11), 5934–5948. https://doi.org/10.55248/gengpi.5.1124.3352

[7] Franco, M. F., Sula, E., Celdrán, A. H., Scheid, E. J., Granville, L. Z., & Stiller, B. (2022). SecRiskAI: a machine learning-based approach for cybersecurity risk prediction in businesses. In 2022 IEEE 24th Conference on Business Informatics (CBI) (pp. 1–10). https://doi.org/10.1109/cbi54897.2022.00008

[8] Heß, V. L., & Damásio, B. (2025). Machine learning in banking risk management: Mapping a decade of evolution. *International Journal of Information Management Data Insights*, *5*(1), 100324. https://doi.org/10.1016/j.jjimei.2025.100324

[9] Hossan, M. Z., Riipa, M. B., Hossain, Md. S., Dhar, S. R., Zaman, A. M., Hossain, Md. A., Hossen, A., & Sozib, H. M. (2025). AI-Powered predictive analytics for financial risk management in U.S. markets. *EAI Endorsed Transactions on AI and Robotics*, *4*. https://doi.org/10.4108/airo.9532

[10] Islam, S., Basheer, N., Papastergiou, S., Ciampi, M., & Silvestri, S. (2025). 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*, *11*(3), 12. https://doi.org/10.1007/s40860-025-00253-3

[11] Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2023). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, *241*, 122697. https://doi.org/10.1016/j.eswa.2023.122697

[12] Kia, A. N., Murphy, F., Sheehan, B., & Shannon, D. (2023). A cyber risk prediction model using common vulnerabilities and exposures. *Expert Systems with Applications*, *237*, 121599. https://doi.org/10.1016/j.eswa.2023.121599

[13] Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

[14] Lozano, M. A., Pérez-Llopis, I., & Domingo, M. E. (2023). Threat hunting architecture using a machine learning approach for critical infrastructures protection. *Big Data and Cognitive Computing*, *7*(2), 65. https://doi.org/10.3390/bdcc7020065

[15] Mashrur, A., Luo, W., Zaidi, N. A., & Robles-Kelly, A. (2020). Machine learning for financial risk management: A survey. *IEEE Access*, *8*, 203203–203223. https://doi.org/10.1109/access.2020.3036322

[16] Noor, U., Anwar, Z., Amjad, T., & Choo, K. R. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems*, *96*, 227–242. https://doi.org/10.1016/j.future.2019.02.013

[17] Preuveneers, D., & Joosen, W. (2021). Sharing machine learning models as indicators of compromise for cyber threat intelligence. *Journal of Cybersecurity and Privacy*, *1*(1), 140–163. https://doi.org/10.3390/jcp1010008

[18] Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M. M., & Al-Rakhami, M. S. (2021). Cyber threat predictive analytics for improving cyber supply chain security. *IEEE Access*, *9*, 94318–94337. https://doi.org/10.1109/access.2021.3087109

[19] Zadeh, A. H., Lavine, B., Zolbanin, H. M., & Hopkins, D. (2023). A cybersecurity risk quantification and classification framework for informed risk mitigation decisions. *Decision Analytics Journal*, *9*, 100328. https://doi.org/10.1016/j.dajour.2023.100328

[20] Zangana, H. M., & Mohammed, H. S. (2025). Cybersecurity in FinTech: A machine learning-based framework for threat detection in mobile payments. *Intelligent Methods in Engineering Sciences*. https://doi.org/10.58190/imiens.2025.151

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.