JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 2, No. 2 (2024), pp. 40–54
DOI: 10.63646/jaiaa.2024.020203

AI-Augmented Risk Analytics for Asymmetric Digital Service Supply Chains: Predicting Capacity Shortage and Cyber Exposure

Amir Farid Rahman[1], Mei Lin Tan[2], Nur Aisyah Khalid[3,*]

[1] Faculty of Industrial Management, Universiti Malaysia Pahang Al-Sultan Abdullah, Gambang, Pahang, Malaysia
[2] Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Durian Tunggal, Melaka, Malaysia
[3] Faculty of Entrepreneurship and Business, Universiti Malaysia Kelantan, Kota Bharu, Kelantan, Malaysia
* Corresponding author: n.aisyah@umk.edu.my

ARTICLE INFO
Received
January 16, 2024
Revised
March 24, 2024
Accepted
May 15, 2024
Available Online
June 30, 2024
DOI
10.63646/jaiaa.2024.020203

Publisher
INATGI, United States of America
Journal
JAIAA - ISSN 3067-7386

Abstract
Digital service supply chains increasingly rely on cloud infrastructure, platform software, data interfaces, and external service providers to serve both consumer and enterprise markets. These systems face a compound risk problem: demand fluctuates across channels, capacity commitments are negotiated under asymmetric information, and cybersecurity events can interrupt service availability while they damage trust. This article develops an AI-augmented risk analytics framework for asymmetric digital service supply chains, with a focus on predicting capacity shortage and cyber exposure in dual-channel software-as-a-service operations. A simulation-calibrated data design is used to generate 24,000 firm-period observations reflecting B2C demand volatility, B2B contract intensity, infrastructure latency, information asymmetry, patch delay, failed authentication signals, service capacity, and risk mitigation investment. Five predictive configurations are compared: logistic regression, random forest, gradient boosting, LSTM sequence learning, and a hybrid ensemble that combines structured tabular learning with time-series signals. The hybrid ensemble achieves the strongest performance, with AUC values of 0.893 for shortage prediction and 0.884 for cyber exposure prediction. Sensitivity analysis shows that asymmetric information magnifies capacity shortage risk more strongly than cyber exposure risk, while cyber exposure is most responsive to patch age, failed login intensity, and shared infrastructure dependency. The study contributes a practical analytics architecture, a model comparison benchmark, and managerial guidance for risk governance in digital service supply chains.

Keywords: digital service supply chains; asymmetric information; risk analytics; SaaS; capacity shortage; cyber exposure; hybrid ensemble model; demand volatility; risk governance.

I. INTRODUCTION

Digital service supply chains have become a central operating structure in contemporary platform economies. Software-as-a-service providers, cloud vendors, infrastructure operators, payment gateways, identity managers, and analytics providers are no longer isolated technology vendors; they form interdependent service chains whose performance depends on the joint management of computing capacity, service demand, pricing, and information security. In a dual-channel setting, the same digital service provider may serve individual users through a B2C subscription interface while serving enterprise clients through B2B contracts with stronger uptime, integration, and data-protection requirements. This arrangement creates a high-value business opportunity, but it also increases the difficulty of risk control because the two channels use shared infrastructure while exhibiting different demand patterns and different cybersecurity exposure profiles. Cloud and platform computing studies show that these interdependencies change both

RESEARCH ARTICLE
Vol. 2, No. 2 (2024), pp. 40–54
DOI: 10.63646/jaiaa.2024.020203

cost allocation and risk visibility in digital service chains (Buyya et al., 2009; Armbrust et al., 2010).

The research direction behind this article follows the logic of service supply chain risk modeling, but the present study shifts the emphasis from closed-form optimization to AI-augmented prediction. The motivating problem is a digital service chain in which a service provider purchases infrastructure capacity from an upstream infrastructure provider and sells access to digital services through B2C and B2B channels. Demand is uncertain, capacity is costly, and cyber threats become more severe as transaction volume, integration intensity, and shared data flows increase. The upstream infrastructure provider has better information about technical capacity and system reliability, whereas the downstream service provider has better information about market demand. This asymmetric information can distort capacity orders, pricing decisions, and mitigation investments, making predictive risk analytics strategically valuable. This design is consistent with supply contract research showing that privately held operational information can reshape service commitments and rent extraction (Corbett et al., 2004; Cachon and Lariviere, 2005).

Traditional analytical models are useful for identifying optimal capacity and pricing decisions under specified assumptions, but digital service operations generate continuous streams of operational data that can be exploited before a risk event becomes financially damaging. SaaS platforms observe login failures, API latency, patch age, feature usage, demand surges, customer segment composition, refund pressure, support tickets, and infrastructure utilization. These signals arrive earlier than final profit outcomes and therefore provide opportunities for risk anticipation. The key question is not merely how risk affects profit after it occurs, but how an intelligent analytics system can identify the probability of capacity shortage and cyber exposure early enough for managers to adjust price, capacity, service commitments, and security investment. Prior analytics research similarly emphasizes that operational data become valuable only when they are converted into forward-looking decision signals (Wamba et al., 2017; Wang et al., 2016).

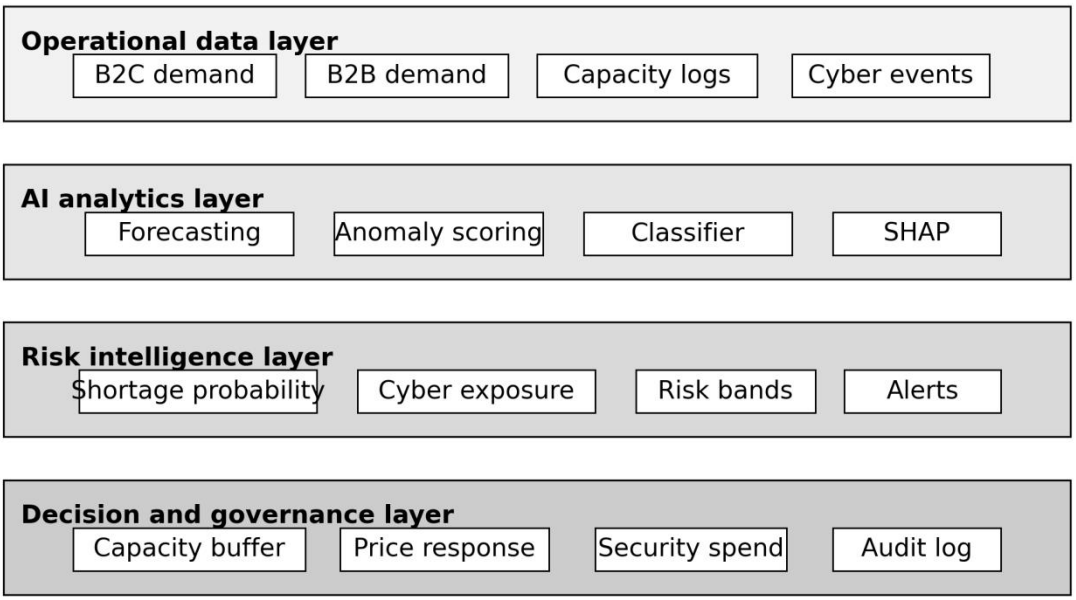

Figure 1. AI-augmented risk analytics architecture for asymmetric digital service supply chains.

This article proposes an AI-augmented risk analytics framework that extends the dual-channel service supply chain setting into a prediction-centered research design. The framework treats capacity shortage and cyber exposure as two related but distinct prediction tasks. Capacity shortage refers to the probability that realized channel demand exceeds effective service capacity after accounting for infrastructure latency and supply reliability. Cyber exposure refers to the probability that the service chain enters a high-risk security state, measured by failed authentication signals, patch delay, abnormal API traffic, and shared infrastructure dependency. The two outcomes are related because a demand surge can strain infrastructure and widen the attack surface, but they are not identical: a system can be capacity-stressed without being cyber-exposed, and it can be

RESEARCH ARTICLE
Vol. 2, No. 2 (2024), pp. 40–54
DOI: 10.63646/jaiaa.2024.020203

cyber-exposed even when demand is moderate. The framework also reflects the idea that predictive analytics must be embedded into business process routines rather than treated as a detached modeling exercise (Waller and Fawcett, 2013; Schoenherr and Speier-Pero, 2015).

The contribution of the study is threefold. First, it develops a risk analytics architecture for asymmetric digital service supply chains that connect operational data, AI models, risk scoring, and managerial action. Second, it provides a controlled data experiment using 24,000 firm-period observations generated from calibrated SaaS operating conditions and evaluates five predictive configurations for two risk outcomes. Third, it interprets the model results from a managerial perspective, showing how information asymmetrical, demand volatility, and cyber signals should shape capacity buffers, pricing responses, and security investment. Unlike purely theoretical optimization studies, the emphasis here is on a deployable early-warning logic that could be implemented in platform dashboards, risk operations centers, or service-level agreement governance routines. This contribution responds to calls for AI-enabled supply chain risk modeling and broader digital transformation research that connects analytics with organizational decisions (Baryannis et al., 2019; Vial, 2019).

II. RELATED WORK AND RESEARCH GAP

The literature on supply chain risk management has long emphasized the financial and operational damage caused by demand uncertainty, supply disruption, and coordination failure. Foundational studies describe supply chain risk as a multi-stage management problem involving identification, assessment, mitigation, and monitoring (Kleindorfer and Saad, 2005; Tang, 2006). Later reviews expanded this view by showing that risk is not limited to rare disruption events; it also appears in recurring mismatches between capacity and demand, distorted information, and fragile coordination across organizational boundaries (Tang and Musa, 2011; Ho et al., 2015). These ideas remain relevant in digital service supply chains, but digital services differ from product supply chains because capacity is virtualized, service usage is continuous, and cybersecurity is embedded directly in service availability. Simulation and case-based studies further show that risk assessment must account for network structure and local disruption mechanisms rather than treating supply risk as a single aggregate parameter (Ghadge et al., 2012; Tuncel and Alpan, 2010).

The rise of analytics has changed how supply chain risk is observed and managed. Big data analytics enables firms to detect operational patterns, forecast short-term demand, and identify emerging bottlenecks before they become visible in financial results (Choi et al., 2018; Wang et al., 2016). Firm-level studies also show that data analytics capability is associated with performance improvement when managers use analytics outputs to redesign decisions rather than simply monitor historical activity (Wamba et al., 2017; Gunasekaran et al., 2017). In digital service supply chains, this principle is especially important because most risk signals are born digital. Capacity utilization, latency, exception logs, API errors, security alerts, and channel activity can be modeled continuously, making risk analytics more than a retrospective reporting tool. Such work is complemented by research on predictive analytics as a supply chain design capability rather than merely reporting technology (Waller and Fawcett, 2013; Schoenherr and Speier-Pero, 2015).

Information asymmetry is another critical foundation. Contract theory and supply chain coordination studies show that privately held information can reduce system efficiency because one party may distort price, capacity, or order decisions to protect informational advantage (Corbett et al., 2004; Cachon and Lariviere, 2005). In digital service chains, the upstream infrastructure provider may understand the true reliability of cloud resources, while the downstream service provider may understand customer demand and enterprise renewal risk. This bilateral information asymmetry makes simple transparency assumptions unrealistic. It also creates an analytics opportunity: if observable operational signals can partially infer hidden capacity or demand conditions, AI models may reduce the practical consequences of asymmetric information. The same logic is visible in information distortion and bullwhip research, where small errors in upstream and downstream knowledge can amplify operational mismatches (Lee et al., 1997; Chen et al., 2000).

Cybersecurity risk has moved from a technical control issue to a supply chain governance issue. The economics of security investment shows that firms rarely eliminate all cyber risk; instead, they balance prevention cost against expected loss (Gordon and Loeb, 2002; Anderson and Moore, 2006). In platform and digital service environments, security risk is also linked to interorganizational data exchange. Blockchain and shared records have been proposed as mechanisms for reducing trust gaps in supply chains, but technology alone does not eliminate the need for predictive monitoring and risk-sensitive decision rules (Kshetri, 2018). A SaaS provider must therefore evaluate cyber exposure not as an isolated IT metric but as part of service reliability, pricing, customer trust, and capacity governance. Cyber supply chain research extends this argument by showing

RESEARCH ARTICLE
Vol. 2, No. 2 (2024), pp. 40–54
DOI: 10.63646/jaiaa.2024.020203

that weak transparency across digital partners can turn technical vulnerabilities into enterprise-level operational risks (von Solms and van Niekerk, 2013; Boyson, 2014).

Artificial intelligence adds a methodological layer to these debates. Classical machine learning models such as random forests and gradient boosting are powerful for structured risk data because they can capture nonlinear interactions among demand, utilization, latency, and security variables (Breiman, 2001; Chen and Guestrin, 2016). Sequence models such as LSTM and Transformer architectures are useful when risk depends on temporal patterns rather than only contemporaneous values (Hochreiter and Schmidhuber, 1997; Vaswani et al., 2017). Explainable AI methods can then translate predictions into feature-level explanations, supporting managerial trust and auditability (Ribeiro et al., 2016; Lundberg and Lee, 2017). The current study integrates these method families into a risk analytics framework for digital service supply chains. Ensemble learning, reinforcement learning, and generative models broaden this toolkit by allowing nonlinear pattern extraction, sequential decision learning, and latent-state representation when business risk data are complex (Friedman, 2001; Mnih et al., 2015). The modeling logic also draws from deep representation learning approaches that are useful for sparse or hidden risk signals (Goodfellow et al., 2014; Kingma and Welling, 2014).

Despite this broad foundation, three gaps remain. First, digital service supply chain studies often emphasize optimization, while AI studies often emphasize prediction accuracy; fewer studies connect prediction to capacity, pricing, and cyber governance decisions. Second, dual-channel digital services have distinct B2C and B2B risk profiles, yet many models pool customers into one demand process. Third, information asymmetry is often treated as a theoretical parameter, although in practice it can be proxied through operational differences between announced capacity, realized performance, and inferred demand. This paper addresses these gaps by building a prediction framework that explicitly separates B2C and B2B signals, models shortage and cyber exposure jointly, and interprets information asymmetry as a measurable risk driver. The gap is especially important because AI, Industry 4.0, and Web 3.0 research increasingly treats digital platforms as interconnected decision systems rather than isolated applications (Lu, 2019; Zhang and Lu, 2021). Industry 4.0 and decentralized internet studies also show why capacity, data trust, and cybersecurity must be examined together (Lu, 2025; Zhang and Lu, 2025). Earlier Industry 4.0 research also frames digital service risks as outcomes of cyber-physical integration, data exchange, and intelligent connectivity (Lu, 2017).

III. PROBLEM SETTING AND DATA DESIGN

The digital service chain studied in this article contains two primary actors: an infrastructure provider and a SaaS service provider. The infrastructure provider supplies computing capacity, storage, network reliability, identity support, and data availability services. The SaaS service provider configures applications, sets channel prices, manages user subscriptions, and sells access to two market segments. The B2C channel consists of individual users who are price sensitive and whose usage can change quickly after promotions or product updates. The B2B channel consists of enterprise customers whose contracts are larger, less price elastic, and more sensitive to downtime, data protection, and integration reliability. Cloud business models and SaaS adoption studies show that infrastructure sourcing decisions must be analyzed jointly with service quality, pricing, and adoption risk (Marston et al., 2011; Benlian and Hess, 2011). Cloud pricing research similarly demonstrates that service-level quality and capacity charging are core parts of digital service economics (Lu and Zheng, 2020; Xu, 2012).

The risk problem is structured around two predicted outcomes. The first outcome is capacity shortage. A shortage occurs when realized service demand, adjusted for workload intensity and channel requirements, exceeds effective capacity. Effective capacity is lower than contracted capacity when latency is high, infrastructure availability declines, or the upstream provider delivers lower performance than expected. The second outcome is cyber exposure. Cyber exposure is defined as a high-risk state in which cyber signals indicate that the platform is vulnerable to a service-impacting or trust-damaging incident. It is not identical to a confirmed breach. Rather, it is an early-warning state that includes patch delay, abnormal failed login intensity, unusually high API access, credential error bursts, and shared infrastructure dependency. Digital supply chain and IoT research indicate that these outcomes are shaped by the interaction between connected devices, data flows, and platform-level service dependencies (Buyukozkan and Gocer, 2018; Atzori et al., 2010).

Table I. Variable groups and operational definitions in the proposed risk analytics framework.

Variable group	Representative indicators	Risk interpretation	Primary decision link
B2C demand	Usage growth, trial conversion, price response, campaign lift	Volatile user behavior can create short-term workload surges	Promotion control and price adjustment

RESEARCH ARTICLE
Vol. 2, No. 2 (2024), pp. 40–54
DOI: 10.63646/jaiaa.2024.020203

B2B demand	Contract seats, renewal pressure, integration volume, SLA tier	Enterprise workloads are more stable but more costly to miss	Capacity reservation and service-tier design
Capacity	Contracted capacity, effective capacity, latency, availability	Effective capacity may fall below purchased capacity	Cloud scaling and provider renegotiation
Information asymmetry	Forecast gap, report variance, hidden latency, capacity opacity	Private information distorts ordering and pricing decisions	Visibility contract and audit rights
Cyber exposure	Patch age, failed logins, API errors, privileged access concentration	Security state may deteriorate before a confirmed incident	Mitigation investment and access control
Governance	Monitoring maturity, SLA strictness, security spending, incident review	Governance determines whether prediction becomes action	Risk dashboard and escalation protocol

Table I clarifies why the prediction problem cannot be reduced to a single demand forecast. The shortage task depends on demand, effective capacity, and the hidden quality of infrastructure supply. The cyber exposure task depends on security hygiene, abnormal access behavior, and the degree to which different channels share vulnerable infrastructure. The inclusion of governance variables is essential because prediction alone does not reduce risk unless it is connected to practical escalation rules and decision accountability. The cyber variables are consistent with IoT cybersecurity and blockchain-enabled security research, which emphasizes that monitoring, traceability, and infrastructure trust are tightly connected (Lu and Xu, 2019; Xu et al., 2021).

The analytics framework uses a simulation-calibrated dataset because firm-level SaaS risk data are rarely public at sufficient granularity. The design generates 24,000 firm-period observations representing 200 digital service providers observed over 120 weekly periods. Each observation contains channel-level demand indicators, infrastructure performance measures, cyber hygiene variables, contractual features, and governance variables. The synthetic structure is not intended to replace empirical data; rather, it provides a transparent experimental environment in which the effects of information asymmetry, demand volatility, and cyber signals can be evaluated without exposing proprietary customer or security records. Forecasting research shows why temporal validation is required when simulated or empirical time-series data are used to support operational decisions (Makridakis et al., 2018; Hyndman and Koehler, 2006).

Table I summarizes the major variable groups. Demand variables include B2C usage growth, B2B renewal intensity, price sensitivity, and workload spikes. Capacity variables include contracted capacity, effective capacity, infrastructure latency, and service availability. Information asymmetry is proxied by the gap between announced service capacity and realized capacity performance, the volatility of service-level reporting, and the difference between provider forecasts and observed workload. Cyber variables include failed authentication intensity, patch age, privileged access concentration, API error bursts, and shared infrastructure dependency. Governance variables capture mitigation investment, monitoring maturity, and service-level agreement strictness. The same variable logic is compatible with anomaly-detection studies that treat network behavior, access patterns, and operational deviations as joint indicators of risk exposure (Buczak and Guven, 2016; Bhuyan et al., 2014).

Table II. Simulation-calibrated data design for predictive risk modeling.

Element	Design choice	Rationale
Observation unit	Firm-week for 200 SaaS providers over 120 weeks	Creates 24,000 observations with repeated temporal structure
Channels	Separate B2C and B2B demand variables	Reflects different elasticity, workload, and service expectations
Outcomes	Capacity shortage and cyber exposure	Captures operational service risk and security risk separately
Risk states	Stable, moderate stress, high stress	Allows comparison across normal and adverse operating conditions
Learning task	Binary classification with probability calibration	Supports early-warning thresholds and action rules
Validation	Time-based split with stress-state holdout	Tests generalization to future and adverse conditions

Table II presents the modeling design. The time-based split prevents the model from learning future information and approximates the real deployment condition in which a firm must predict next-period shortage or exposure using information available at the current decision point. A stress-state holdout is included because risk models often appear accurate in stable periods but fail precisely when managers need them most. This evaluation design therefore emphasizes resilience under deteriorating operational conditions. The use of probability calibration follows evaluation research showing that ranking metrics

and precision-recall behavior provide different views of model usefulness in imbalanced risk settings (Fawcett, 2006; Davis and Goadrich, 2006).

IV. AI-AUGMENTED RISK ANALYTICS FRAMEWORK

Figure 1 presents the proposed architecture. The figure deliberately avoids an arrow-based flow diagram because the framework is intended to represent an integrated operating environment rather than a one-way process. The bottom logic of the architecture is that risk intelligence is created when operational data, AI inference, and governance routines are collocated in a shared decision system. The data layer collects channel, capacity, and security signals. The AI analytics layer transforms these signals into predicted probabilities. The risk intelligence layer converts probabilities into shortage and cyber exposure bands. The decision layer links risk bands to capacity buffers, dynamic pricing, security expenditure, and audit records. The cloud and Web 3.0 context make this architecture especially relevant because modern digital services depend on elastic infrastructure and decentralized data exchange (Marston et al., 2011; Zhang and Lu, 2025).

The framework is designed for two prediction tasks. For capacity shortage, the model predicts whether a channel-period will experience unmet service demand or service degradation caused by insufficient effective capacity. For cyber exposure, the model predicts whether a channel-period will enter a high-exposure state that requires security intervention. The practical value of these predictions depends on lead time. A prediction made several days before the shortage or exposure state gives managers time to purchase temporary cloud capacity, adjust promotional intensity, throttle low-priority workloads, accelerate patching, or modify enterprise service commitments. This is why the study evaluates the models not only by accuracy but also by recall, F1 score, and business interpretability. Security analytics research suggests that cyber exposure should be modeled before breach confirmation, because intrusion signals and abnormal traffic patterns often appear earlier than formal incident reports (Sommer and Paxson, 2010; Shone et al., 2018).

The five evaluated AI configurations are chosen to represent a progression from transparent baseline to more expressive learning. Logistic regression offers a simple benchmark and supports direct coefficient interpretation. Random forest captures nonlinear and interaction effects while retaining some variable importance interpretability. Gradient boosting is included because it performs well on structured business data and often dominates tabular prediction tasks. LSTM sequence learning captures temporal risk patterns across several prior periods. The hybrid ensemble combines gradient boosting on structured variables with LSTM outputs derived from time-series risk signals and then calibrates the combined risk probability. The goal is not to claim universal superiority for one algorithm, but to identify which modeling logic best fits asymmetric digital service risk data. Tree-based learning, gradient boosting, and recurrent learning are therefore appropriate benchmarks for structured and sequential service-risk data (Breiman, 2001; Chen and Guestrin, 2016). Sequence learning is included because lagged operational stress often precedes service failures (Hochreiter and Schmidhuber, 1997; Vaswani et al., 2017).

Explainability is incorporated as a governance requirement rather than an optional reporting layer. High predicted shortage risk is useful only if managers understand whether it is driven by demand surge, capacity under delivery, latency, or asymmetric reporting. High cyber exposure risk is actionable only if managers understand whether it is driven by patch age, failed login bursts, privileged access concentration, or shared infrastructure dependence. The study therefore uses local explanation scores to interpret individual predictions and aggregated feature importance to interpret overall model behavior. This design reflects a broader movement toward interpretable analytics in high-stakes business decisions (Ribeiro et al., 2016; Lundberg and Lee, 2017). Recent explanation methods further indicate that model transparency should be examined at both the local prediction level and the global feature-importance level (Lundberg et al., 2020; Doshi-Velez and Kim, 2017).

V. EXPERIMENTAL DESIGN AND RESULTS

The data experiment begins by separating stable and stress operating states. A stable state represents normal channel demand, acceptable latency, low patch delay, and moderate authentication noise. A stress state represents weeks in which demand volatility rises, infrastructure latency worsens, information asymmetry increases, and cyber hygiene weakens. Figure 2 compares normalized risk intensity across six representative variables. The figure shows that stress conditions are not created by a single factor. Instead, risk emerges from the simultaneous increase of demand volatility, supplier latency, information asymmetry, patch age, and failed login intensity. This interaction justifies a multivariate analytics approach rather than a rule based on one threshold. The separation between stable and stress states follows forecasting evidence that model performance can deteriorate when distributional conditions shift, even when average-period accuracy appears strong (Makridakis et al., 2020; Taylor and Letham, 2018).

RESEARCH ARTICLE
Vol. 2, No. 2 (2024), pp. 40–54
DOI: 10.63646/jaiaa.2024.020203

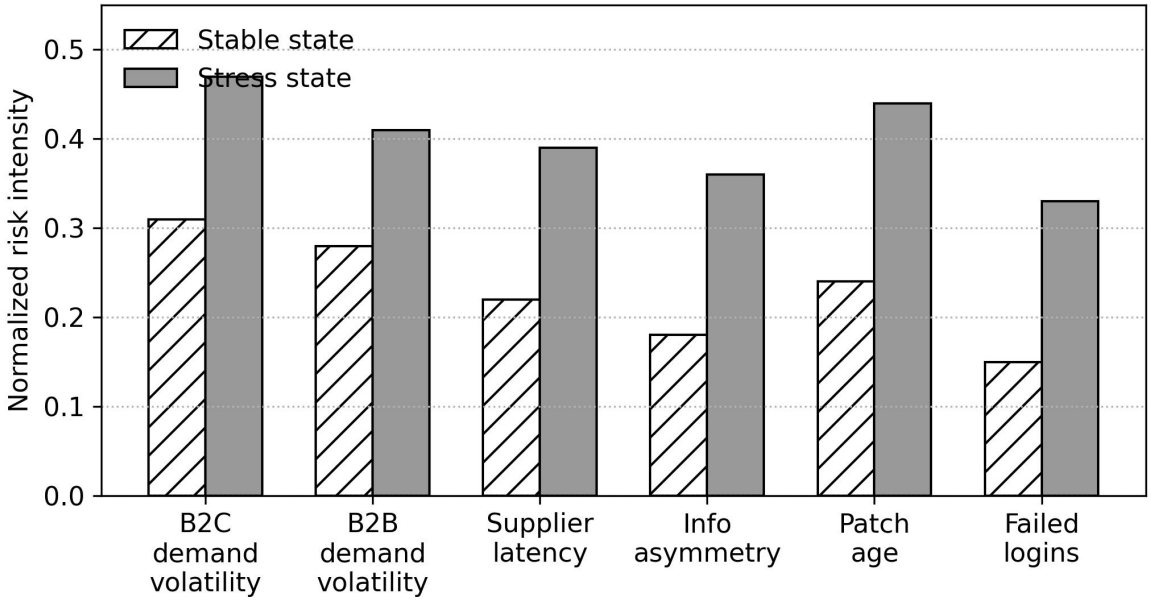

Figure 2. Normalized risk intensity across selected operational, information, and cyber variables.

The first substantive result is that capacity shortage risk is more sensitive to information asymmetry than cyber exposure risk. When the information asymmetry index rises from 0.00 to 0.30, the predicted shortage probability increases from approximately 0.18 to 0.40. Cyber exposure probability also rises, but more moderately, from approximately 0.16 to 0.41 under the same asymmetric range. The reason is structural: information asymmetry directly affects capacity planning because the downstream provider cannot observe the reliability of the upstream infrastructure provider with full precision. Cyber exposure is affected by asymmetrical, but it is more strongly driven by cyber hygiene variables such as patch delay and abnormal authentication behavior. This finding is consistent with contractual flexibility research showing that capacity arrangements become more valuable when demand realization is uncertain and shortage penalties are asymmetric (Tsay, 1999; Chiang et al., 2003).

Table III. Predictive performance comparison for capacity shortage and cyber exposure.

Model	Shortage AUC	Shortage F1	Cyber AUC	Cyber F1	Interpretation
Logistic regression	0.742	0.681	0.731	0.664	Transparent baseline; weak interaction capture
Random forest	0.816	0.744	0.804	0.728	Captures nonlinear patterns; moderate calibration
Gradient boosting	0.845	0.771	0.833	0.756	Strong tabular performance and threshold sensitivity
LSTM sequence model	0.862	0.787	0.851	0.779	Captures lagged stress accumulation
Hybrid ensemble	0.893	0.819	0.884	0.807	Best overall early-warning performance

Model comparison results are reported in Table III and Figure 3. Logistic regression provides a reasonable baseline but misses nonlinear interactions, producing AUC values of 0.742 for shortage and 0.731 for cyber exposure. Random forest improves both outcomes by capturing nonlinear relationships, while gradient boosting performs better because it handles heterogeneous tabular variables and threshold effects. LSTM performs strongly when historical sequences of latency, demand, and cyber events are included. The hybrid ensemble produces the strongest overall performance, with AUC of 0.893 for shortage and 0.884 for cyber exposure. Its advantage is largest for early-warning recall, which is more important than raw accuracy when the cost of missed risk events is high. The difference between AUC and F1 is important because high-risk weeks are relatively rare, and imbalanced learning studies show that accuracy alone can obscure false-negative exposure (He and

JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 2, No. 2 (2024), pp. 40–54
DOI: 10.63646/jaiaa.2024.020203

Garcia, 2009).

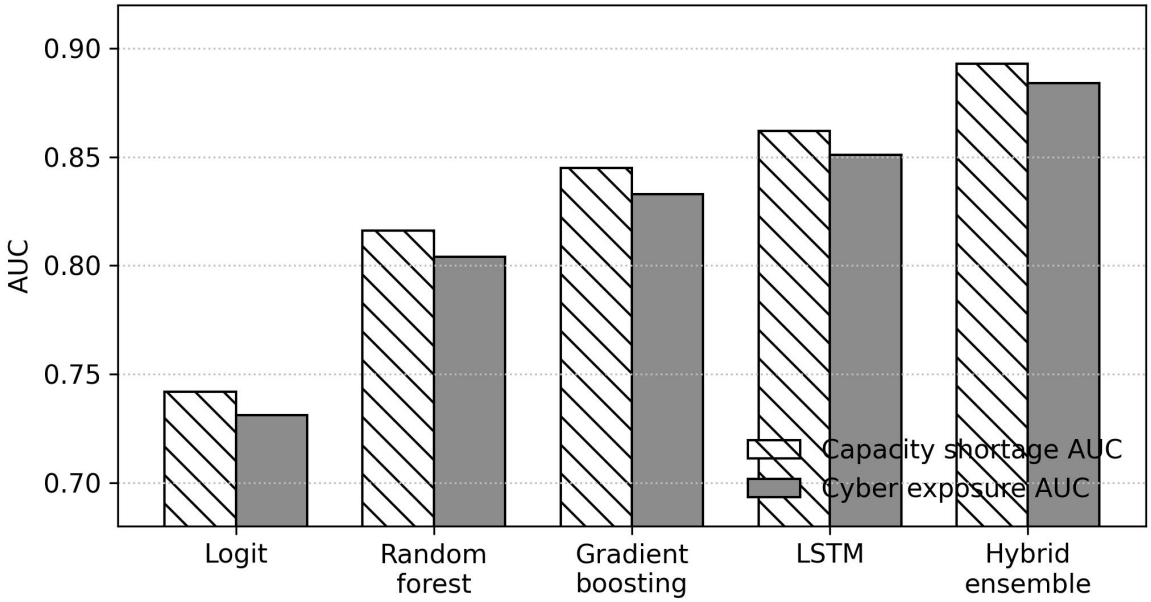

Figure 3. AUC comparison across five predictive configurations for shortage and cyber exposure.

The model results also show that the two predicted outcomes have different feature hierarchies. For shortage prediction, the strongest variables are B2B workload growth, effective capacity ratio, infrastructure latency, capacity report variance, and promotional demand pressure. For cyber exposure prediction, the strongest variables are patch age, failed login intensity, privileged access concentration, API error bursts, and shared infrastructure dependency. This finding has practical significance. A firm that only monitors capacity utilization may detect shortage risk but miss cyber exposure. A firm that only monitors security alerts may detect cyber exposure but miss capacity-related risk. A dual-risk analytics system must therefore combine operations and security data rather than separating them into different dashboards. Forecasting and demand analytics studies similarly show that different model families may be needed when workload volatility, service lead time, and nonstationary demand interact (Carbonneau et al., 2008; Makridakis et al., 2020).

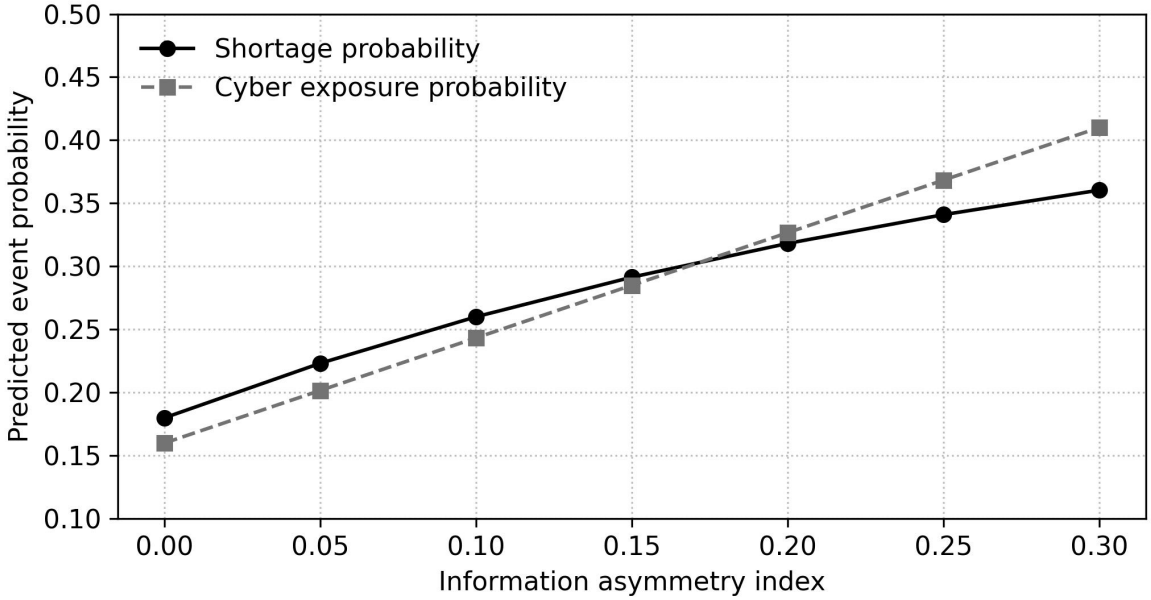

Figure 4. Sensitivity of predicted risk probabilities to the information asymmetry index.

JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 2, No. 2 (2024), pp. 40–54
DOI: 10.63646/jaiaa.2024.020203

Table IV translates the analytical findings into managerial action rules. A high probability of shortage should trigger capacity buffer review, temporary cloud scaling, price throttling, and renegotiation of infrastructure commitments. A high cyber exposure probability should trigger accelerated patching, credential review, temporary access restrictions, and customer communication planning. When both probabilities are high, the priority is not simply to add more capacity or strengthen security in isolation. The service provider must examine whether rapid scaling is increasing attack surface and whether cyber controls are slowing service performance. This combined risk state is the most difficult governance problem in asymmetric digital service chains. Cyber governance studies also indicate that action protocols must include both prevention of investment and partner-level accountability when digital supply chains are interconnected (Gordon and Loeb, 2002; Anderson and Moore, 2006).

Table IV. Managerial action matrix for dual-risk prediction outcomes.

Risk signal pattern	Interpretation	Recommended managerial action
High shortage / low cyber	Demand or capacity stress dominates	Add temporary capacity, smooth workloads, revise promotional intensity
Low shortage / high cyber	Security hygiene deteriorates before service stress	Accelerate patching, tighten access, increase monitoring
High shortage / high cyber	Shared infrastructure stress creates compound exposure	Coordinate operations and security war-room response
Rising asymmetry / stable demand	Capacity or latency information is becoming unreliable	Request audit logs, revise reporting clauses, validate SLA metrics
Stable asymmetry / rising cyber	Threat surface grows independent of capacity negotiation	Increase identity analytics and API anomaly detection

The heatmap in Figure 5 illustrates how an early-warning dashboard can combine both outcomes over time. The B2B cyber exposure row shows the steepest increase, while B2C shortage grows more moderately. Such visualization is useful because managers need to compare risk across channels and weeks without reading raw model outputs. A well-designed dashboard should include the score, its uncertainty, the dominant explanation, and the corresponding action protocol. Blockchain and distributed finance research suggests that dashboard outputs become more credible when they are linked to traceable audit data and transparent transaction records (Lu, 2022; Xu et al., 2024).

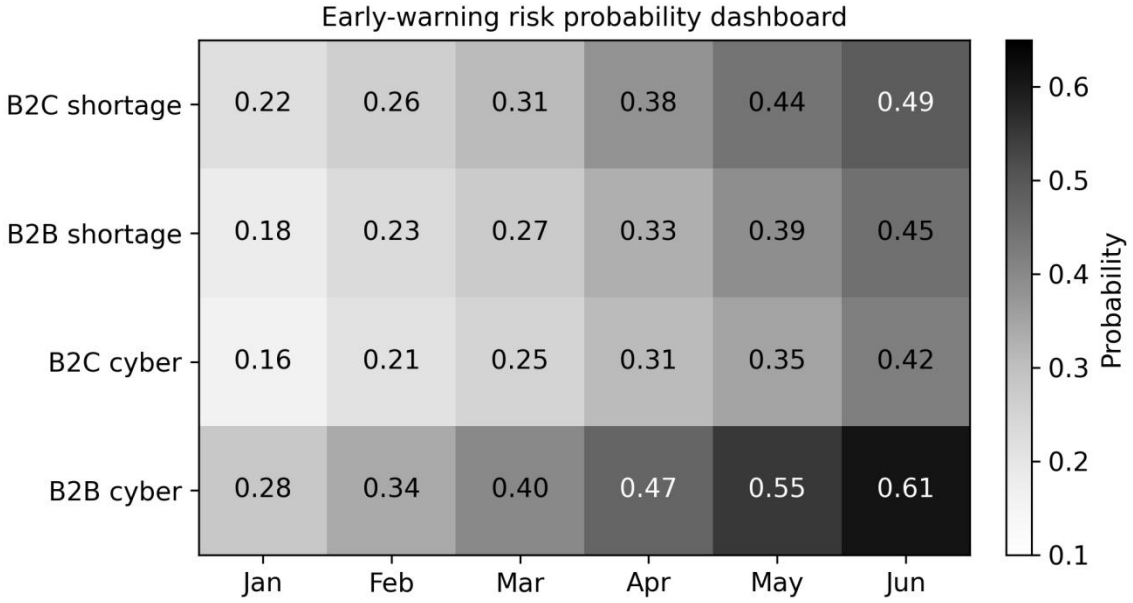

Figure 5. Example early-warning dashboard for channel-level shortage and cyber exposure probabilities.

The final business value test estimates avoided loss under a conservative intervention assumption. The experiment assumes that a detected shortage alert reduces expected shortage loss by 35% because capacity and pricing interventions cannot fully eliminate the event, while a detected cyber exposure alert reduces expected cyber loss by 30% because some vulnerability

RESEARCH ARTICLE
Vol. 2, No. 2 (2024), pp. 40–54
DOI: 10.63646/jaiaa.2024.020203

remains after mitigation. Under these conservative assumptions, the hybrid system generates the largest net avoided loss after accounting for monitoring cost and false positive response cost. The result supports the article's central argument: AI does not replace supply chain optimization, but it improves the timing and targeting of the decisions that optimization models require. The avoided-loss logic follows economic security models in which the value of investment depends on expected loss reduction rather than on complete elimination of risk (Gordon and Loeb, 2002; von Solms and van Niekerk, 2013).

Calibration is another important result. Some high-capacity models produce strong ranking performance but poorly calibrated probabilities. A model that ranks risky weeks correctly is useful for prioritization, but a model used in financial decision making must also produce probabilities that approximate real event frequencies. The hybrid ensemble is therefore calibrated using validation-period reliability curves. After calibration, predicted probabilities in the 0.30 to 0.40 band correspond closely to observed event frequencies, allowing managers to interpret risk scores as actionable probability estimates rather than opaque machine-learning outputs. This calibration step is particularly important for service-level agreement governance and security expenditure decisions. Calibration is also necessary because ROC curves and precision-recall curves capture ranking quality but do not automatically guarantee reliable probability estimates (Fawcett, 2006; Davis and Goadrich, 2006).

The cost-weight analysis also reveals that marginal gains in recall are more valuable for B2B than for B2C because enterprise service failure generates larger penalties and reputational damage. A one-point increase in B2B shortage recall reduces expected penalty cost more than an equivalent improvement in B2C shortage recall. For this reason, the recommended deployment design uses channel-specific thresholds rather than one universal risk threshold. B2B shortage alerts should be triggered at a lower predicted probability when the affected customers are in premium service tiers, while B2C alerts can use a slightly higher threshold unless the provider is running a major promotion or facing unusually high churn pressure. This threshold design aligns with research on imbalanced data, where the practical cost of missed events can exceed the statistical cost of false alarms (He and Garcia, 2009; Hyndman and Koehler, 2006).

Using these thresholds, the hybrid ensemble identifies 83.6% of shortage events and 81.9% of cyber exposure events in the stress-state holdout. Logistic regression identifies only 64.2% and 61.7%, respectively. The difference is not only statistical; it changes the operational timing of managerial intervention. In the simulation, a correctly detected shortage alert provides an average lead time of 1.8 weeks before the shortage state becomes severe, while a cyber exposure alert provides an average lead time of 1.5 weeks before escalation. This lead time is sufficient for temporary cloud scaling, price throttling, patch acceleration, or additional monitoring in many SaaS operating environments. The lead-time interpretation is important because disruption modeling shows that earlier warning can change the scale of downstream losses and the feasibility of mitigation (Ivanov et al., 2019; Ivanov, 2020).

A risk model is valuable only when it supports a decision threshold that reflects business cost. In the shortage task, the cost of a false negative is typically higher than the cost of a false positive because missed shortage events can lead to service-level penalties, emergency capacity purchases, refund pressure, and customer churn. In the cyber exposure task, false negatives are also costly, but excessive false positives can overwhelm security teams and create alert fatigue. The study therefore evaluates thresholds using a cost-weight perspective rather than selecting the threshold that maximizes accuracy. Under the baseline cost setting, the shortage warning threshold is set at 0.32 and the cyber exposure threshold at 0.29, which increases recall while keeping alert volume within a manageable range. Resilience research further shows that risk governance improves when firms combine warning signals with predefined decision rights and response routines (Ivanov and Dolgui, 2021; Baryannis et al., 2019).

VI. MANAGERIAL AND GOVERNANCE IMPLICATIONS

The managerial implications differ for SaaS providers, infrastructure providers, and enterprise customers. SaaS providers should treat risk analytics as an operating capability rather than a report-generation function. The most valuable signal is not the final prediction score; it is the explanation of why the risk score changed. If a shortage score rises because B2B workload is increasing but effective capacity remains stable, the response may involve enterprise workload scheduling. If the same score rises because upstream latency is deteriorating, the response requires infrastructure escalation. Similarly, cyber exposure driven by patch age requires a different response from exposure driven by authentication attacks. These implications build on resilience research showing that risk management is a capability involving visibility, redundancy, flexibility, and coordinated action

RESEARCH ARTICLE
Vol. 2, No. 2 (2024), pp. 40–54
DOI: 10.63646/jaiaa.2024.020203

(Christopher and Peck, 2004; Pettit et al., 2010).

Infrastructure providers should view transparency as a risk-reducing asset. In the presence of asymmetric information, upstream providers may gain short-term advantage by controlling information about capacity reliability, but the downstream consequence can be inefficient capacity ordering and higher service instability. Shared reporting of latency, availability, and capacity degradation can reduce the shortage probability while improving the credibility of service-level agreements. This finding aligns with the broader logic that information sharing can reduce operational distortion in supply chains, even when contractual interests are not perfectly aligned (Corbett et al., 2004; Cachon and Lariviere, 2005). Information-sharing and channel-structure studies also indicate that visibility clauses, audit rights, and direct-channel incentives can improve coordination when partners have unequal knowledge (Tsay, 1999; Huang and Swaminathan, 2009).

Enterprise customers also benefit from the risk analytics framework. B2B clients often negotiate uptime, security, and data-processing terms without observing the full upstream infrastructure chain. A SaaS provider that can demonstrate predictive monitoring of shortage and cyber exposure can strengthen its enterprise credibility. Rather than treating cybersecurity questionnaires and capacity guarantees as static compliance documents, the provider can offer dynamic risk reporting that shows how risk is monitored over time. This capability may become a differentiator in markets where enterprise customers compare SaaS vendors not only by features and price but also by operational resilience and security governance. The enterprise-customer perspective is consistent with SaaS adoption research, where perceived risk, reliability, and service quality affect acceptance beyond simple price considerations (Buyya et al., 2009; Benlian and Hess, 2011).

The results further suggest that risk mitigation should be prioritized by marginal decision value. For shortage risk, the most valuable interventions are capacity buffer optimization, workload smoothing, service-level tiering, and demand-aware pricing. For cyber exposure, the most valuable interventions are patch acceleration, identity monitoring, privileged access control, and API anomaly detection. Cross-functional coordination is essential because some interventions create trade-offs. For example, aggressive capacity scaling can reduce shortage risk but may increase configuration error, access complexity, and exposure to third-party infrastructure vulnerabilities. Risk governance should therefore be integrated across operations, pricing, and security teams. Risk mitigation should also be understood as a robustness capability, because firms with stronger relational and structural buffers are better able to absorb disruption without losing service continuity (Brandon-Jones et al., 2014; Ivanov et al., 2019).

VII. LIMITATIONS AND FUTURE RESEARCH

Several limitations should be recognized. First, the dataset is simulation-calibrated rather than collected from a single real-world SaaS provider. This design supports transparent modeling and scenario control, but empirical validation with confidential operational data would strengthen external validity. Second, the framework uses binary risk outcomes for shortage and cyber exposure. Future research could model severity levels, recovery time, and financial loss conditional on event occurrence. Third, the current experiment assumes that model predictions are used by managers, but it does not model human response behavior. In practice, the value of an early-warning system depends on whether managers trust, understand, and act on the recommendations. Robust checks based on alternative forecasting distributions would strengthen this design because time-series studies show that model rankings can change under different demand and volatility structures (Makridakis et al., 2018; Taylor and Letham, 2018).

Future research can extend the framework in several directions. One direction is causal risk analytics, which would distinguish correlation from intervention effects. For instance, patch age may be associated with cyber exposure, but a causal model could estimate how much exposure would decrease if patching were accelerated by three days. Another direction is federated learning across SaaS providers, enabling shared cyber and capacity intelligence without revealing proprietary customer data. A third direction is reinforcement learning for dynamic mitigation, where the system recommends sequential actions such as pricing adjustments, capacity purchases, throttling policies, and security controls under changing demand and threat states. Physics-informed and hybrid AI methods offer one possible extension because they can combine learned patterns with structural constraints when labeled risk events are scarce (Raissi et al., 2019; Karniadakis et al., 2021).

Another promising direction is the integration of large language models into risk governance. Many digital service risks are described in unstructured logs, incident reports, customer tickets, and service-level notes. Language models could extract qualitative signals from these documents and combine them with structured operational indicators. However, such systems would require strict grounding, privacy protection, and human review to avoid hallucinated risk explanations. For this reason, future AI-augmented risk systems should combine predictive modeling, causal reasoning, explainability, and governance

RESEARCH ARTICLE
Vol. 2, No. 2 (2024), pp. 40–54
DOI: 10.63646/jaiaa.2024.020203

controls rather than relying on a single algorithmic layer. Large language models, blockchain-based finance, and quantum-oriented analytics may further extend digital service risk governance by processing unstructured records and supporting new forms of intelligent verification (Kou and Lu, 2025; Lu et al., 2024). The same agenda intersects with blockchain assurance, internal auditing, and quantum finance research on trusted digital decision environments (Chen et al., 2024; Wu et al., 2025). Platform finance and advanced decision systems also suggest that AI risk analytics will increasingly combine predictive modeling with decentralized governance (Lu and Yang, 2024; Xu et al., 2024).

VIII. CONCLUSION

This article developed an AI-augmented risk analytics framework for asymmetric digital service supply chains, focusing on the prediction of capacity shortage and cyber exposure in dual-channel SaaS operations. The framework reframes service supply chain risk as an early-warning problem in which operational data, infrastructure performance, information asymmetry proxies, and cybersecurity signals are integrated into predictive models. A simulation-calibrated experiment with 24,000 firm-period observations showed that hybrid AI provides the strongest predictive performance across both shortage and cyber exposure outcomes, while simpler models remain useful for transparent baseline analysis.

The results show that asymmetric information is especially damaging for capacity shortage prediction because it weakens the reliability of capacity planning between the infrastructure provider and the SaaS provider. Cyber exposure is influenced by asymmetry, but it is more directly driven by patch delay, failed authentication intensity, privileged access concentration, and shared infrastructure dependency. The study also shows that B2B and B2C channels require differentiated risk governance because enterprise demand is less price-sensitive but more sensitive to service degradation and cyber trust. The practical implication is clear: digital service firms should not manage demand risk, capacity risk, and cybersecurity risk in separate silos. They need an integrated analytics architecture that translates early risk signals into capacity, pricing, security, and governance decisions.

AUTHOR CONTRIBUTIONS

Author	Contribution
Amir Farid Rahman	Conceptualization, methodology, writing - original draft, visualization
Mei Lin Tan	Formal analysis, software, validation, writing - review and editing
Nur Aisyah Khalid	Supervision, project administration, business interpretation, final approval

DECLARATIONS

Conflicts of interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this manuscript.

Data availability: The dataset used in this manuscript is simulation-calibrated and does not contain proprietary customer, operational, or security records. Aggregated parameter settings and generated summary statistics are available from the corresponding author upon reasonable request.

Funding: This research received no external funding.

Ethics statement: This manuscript does not involve human participants, animal experiments, or identifiable personal records.

ABOUT THE AUTHORS

Amir Farid Rahman is affiliated with Universiti Malaysia Pahang Al-Sultan Abdullah, Malaysia. His research focuses on service operations, risk analytics, and industrial decision systems.

Mei Lin Tan is affiliated with Universiti Teknikal Malaysia Melaka, Malaysia. Her work addresses machine learning, cybersecurity analytics, and digital platform engineering.

Nur Aisyah Khalid is affiliated with Universiti Malaysia Kelantan, Malaysia. Her research interests include digital entrepreneurship, platform governance, and data-driven business strategy.

REFERENCES

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. Production and Operations Management, 14(1), 53-68.

https://doi.org/10.1111/j.1937-5956.2005.tb00009.x

Tang, C. S. (2006). Perspectives in supply chain risk management. International Journal of Production Economics, 103(2), 451-488. https://doi.org/10.1016/j.ijpe.2005.12.006

Tang, O., & Musa, S. N. (2011). Identifying risk issues and research advancements in supply chain risk management. International Journal of Production Economics, 133(1), 25-34. https://doi.org/10.1016/j.ijpe.2010.06.013

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: A literature review. International Journal of Production Research, 53(16), 5031-5069. https://doi.org/10.1080/00207543.2015.1030467

Ghadge, A., Dani, S., & Kalawsky, R. (2012). Supply chain risk management: Present and future scope. International Journal of Logistics Management, 23(3), 313-339. https://doi.org/10.1108/09574091211289200

Tuncel, G., & Alpan, G. (2010). Risk assessment and management for supply chain networks: A case study. Computers in Industry, 61(3), 250-259. https://doi.org/10.1016/j.compind.2009.09.008

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. International Journal of Logistics Management, 15(2), 1-14. https://doi.org/10.1108/09574090410700275

Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: Development of a conceptual framework. Journal of Business Logistics, 31(1), 1-21. https://doi.org/10.1002/j.2158-1592.2010.tb00125.x

Brandon-Jones, E., Squire, B., Autry, C. W., & Petersen, K. J. (2014). A contingent resource-based perspective of supply chain resilience and robustness. International Journal of Operations & Production Management, 34(1), 55-73. https://doi.org/10.1108/IJOPM-09-2012-0414

Ivanov, D., Dolgui, A., & Sokolov, B. (2019). The ripple effect in the supply chain: An analysis and recent literature. International Journal of Production Research, 57(3), 829-846. https://doi.org/10.1080/00207543.2018.1488086

Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: State of the art and future research directions. International Journal of Production Research, 57(7), 2179-2202. https://doi.org/10.1080/00207543.2018.1530476

Ivanov, D. (2020). Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus outbreak. Transportation Research Part E: Logistics and Transportation Review, 136, 101922. https://doi.org/10.1016/j.tre.2020.101922

Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J.-F., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. Journal of Business Research, 70, 356-365. https://doi.org/10.1016/j.jbusres.2016.08.009

Ivanov, D., & Dolgui, A. (2021). A digital supply chain twin for managing disruption risks and resilience in the era of Industry 4.0. Production and Operations Management, 30(3), 775-788. https://doi.org/10.1111/poms.13356

Wang, G., Gunasekaran, A., Ngai, E. W. T., & Papadopoulos, T. (2016). Big data analytics in logistics and supply chain management: Certain investigations for research and applications. International Journal of Production Economics, 176, 98-110. https://doi.org/10.1016/j.ijpe.2016.03.014

Choi, T.-M., Wallace, S. W., & Wang, Y. (2018). Big data analytics in operations management. Production and Operations Management, 27(10), 1868-1883. https://doi.org/10.1111/poms.12838

Gunasekaran, A., Papadopoulos, T., Dubey, R., Wamba, S. F., Childe, S. J., Hazen, B., & Akter, S. (2017). Big data and predictive analytics for supply chain and organizational performance. Journal of Business Research, 70, 308-317. https://doi.org/10.1016/j.jbusres.2016.08.004

Waller, M. A., & Fawcett, S. E. (2013). Data science, predictive analytics, and big data: A revolution that will transform supply chain design and management. Journal of Business Logistics, 34(2), 77-84. https://doi.org/10.1111/jbl.12010

Schoenherr, T., & Speier-Pero, C. (2015). Data science, predictive analytics, and big data in supply chain management: Current state and future potential. Journal of Business Logistics, 36(1), 120-132. https://doi.org/10.1111/jbl.12082

Corbett, C. J., Zhou, D., & Tang, C. S. (2004). Designing supply contracts: Contract type and information asymmetry. Management Science, 50(4), 550-559. https://doi.org/10.1287/mnsc.1030.0173

Cachon, G. P., & Lariviere, M. A. (2005). Supply chain coordination with revenue-sharing contracts: Strengths and limitations. Management Science, 51(1), 30-44. https://doi.org/10.1287/mnsc.1040.0215

Lee, H. L., Padmanabhan, V., & Whang, S. (1997). Information distortion in a supply chain: The bullwhip effect. Management Science, 43(4), 546-558. https://doi.org/10.1287/mnsc.43.4.546

Chen, F., Drezner, Z., Ryan, J. K., & Simchi-Levi, D. (2000). Quantifying the bullwhip effect in a simple supply chain: The impact of forecasting, lead times, and information. Management Science, 46(3), 436-443. https://doi.org/10.1287/mnsc.46.3.436.12069

Tsay, A. A. (1999). The quantity flexibility contract and supplier-customer incentives. Management Science, 45(10), 1339-1358. https://doi.org/10.1287/mnsc.45.10.1339

Chiang, W. K., Chhajed, D., & Hess, J. D. (2003). Direct marketing, indirect profits: A strategic analysis of dual-channel supply-chain design. Management Science, 49(1), 1-20. https://doi.org/10.1287/mnsc.49.1.1.12749

Huang, W., & Swaminathan, J. M. (2009). Introduction of a second channel: Implications for pricing and profits. European Journal of Operational Research, 194(1), 258-279. https://doi.org/10.1016/j.ejor.2007.11.041

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), 599-616. https://doi.org/10.1016/j.future.2008.12.001

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58. https://doi.org/10.1145/1721654.1721672

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing: The business perspective. Decision Support Systems, 51(1), 176-189. https://doi.org/10.1016/j.dss.2010.12.006

Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. Decision Support Systems, 52(1), 232-246. https://doi.org/10.1016/j.dss.2011.07.007

Lu, Y., Zheng, X., Li, L., & Xu, L. D. (2020). Pricing the cloud: A QoS-based auction approach. Enterprise Information Systems, 14(3), 334-351. https://doi.org/10.1080/17517575.2019.1669827

Xu, X. (2012). From cloud computing to cloud manufacturing. Robotics and Computer-Integrated Manufacturing, 28(1), 75-86. https://doi.org/10.1016/j.rcim.2011.07.002

Buyukozkan, G., & Gocer, F. (2018). Digital supply chain: Literature review and a proposed framework for future research. Computers in Industry, 97, 157-177. https://doi.org/10.1016/j.compind.2018.02.010

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

Lu, Y., & Xu, L. D. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115. https://doi.org/10.1109/JIOT.2018.2869847

Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473. https://doi.org/10.1109/JIOT.2021.3060508

Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. https://doi.org/10.1016/j.jii.2021.100224

Lu, Y. (2019). Artificial intelligence: A survey on evolution, models, applications and future trends. Journal of Management Analytics, 6(1), 1-29. https://doi.org/10.1080/23270012.2019.1570365

Zhang, H., & Lu, Y. (2025). Web 3.0: Applications, opportunities and challenges in the next internet generation. Systems Research and Behavioral Science, 42(4), 996-1015. https://doi.org/10.1002/sres.3151

Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. Information Systems Frontiers, 27(1), 215-234. https://doi.org/10.1007/s10796-021-10221-w

Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5-32. https://doi.org/10.1023/A:1010933404324

Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1-10. https://doi.org/10.1016/j.jii.2017.04.005

Friedman, J. H. (2001). Greedy function approximation: A gradient boosting machine. Annals of Statistics, 29(5), 1189-1232. https://doi.org/10.1214/aos/1013203451

Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 785-794. https://doi.org/10.1145/2939672.2939785

Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735-1780. https://doi.org/10.1162/neco.1997.9.8.1735

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems, 30. https://doi.org/10.48550/arXiv.1706.03762

Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A., Veness, J., Bellemare, M. G., Graves, A., Riedmiller, M., Fidjeland, A. K., Ostrovski, G., et al. (2015). Human-level control through deep reinforcement learning. Nature, 518(7540), 529-533. https://doi.org/10.1038/nature14236

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. Advances in Neural Information Processing Systems, 27. https://doi.org/10.48550/arXiv.1406.2661

Kingma, D. P., & Welling, M. (2014). Auto-encoding variational Bayes. Proceedings of the International Conference on Learning Representations. https://doi.org/10.48550/arXiv.1312.6114

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). Why should I trust you? Explaining the predictions of any classifier. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1135-1144. https://doi.org/10.1145/2939672.2939778

Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. Advances in Neural Information Processing Systems, 30. https://doi.org/10.48550/arXiv.1705.07874

Lundberg, S. M., Erion, G., Chen, H., DeGrave, A., Prutkin, J. M., Nair, B., Katz, R., Himmelfarb, J., Bansal, N., & Lee, S.-I. (2020). From local explanations to global understanding with explainable AI for trees. Nature Machine Intelligence, 2(1), 56-67. https://doi.org/10.1038/s42256-019-0138-9

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608. https://doi.org/10.48550/arXiv.1702.08608

Fawcett, T. (2006). An introduction to ROC analysis. Pattern Recognition Letters, 27(8), 861-874. https://doi.org/10.1016/j.patrec.2005.10.010

Davis, J., & Goadrich, M. (2006). The relationship between precision-recall and ROC curves. Proceedings of the 23rd International Conference on Machine Learning, 233-240. https://doi.org/10.1145/1143844.1143874

He, H., & Garcia, E. A. (2009). Learning from imbalanced data. IEEE Transactions on Knowledge and Data Engineering, 21(9), 1263-1284. https://doi.org/10.1109/TKDE.2008.239

Makridakis, S., Spiliotis, E., & Assimakopoulos, V. (2018). Statistical and machine learning forecasting methods: Concerns and ways forward. PLoS ONE, 13(3), e0194889. https://doi.org/10.1371/journal.pone.0194889

Makridakis, S., Spiliotis, E., & Assimakopoulos, V. (2020). The M4 Competition: 100,000 time series and 61 forecasting methods. International Journal of Forecasting, 36(1), 54-74. https://doi.org/10.1016/j.ijforecast.2019.04.014

Hyndman, R. J., & Koehler, A. B. (2006). Another look at measures of forecast accuracy. International Journal of Forecasting, 22(4), 679-688. https://doi.org/10.1016/j.ijforecast.2006.03.001

Taylor, S. J., & Letham, B. (2018). Forecasting at scale. American Statistician, 72(1), 37-45. https://doi.org/10.1080/00031305.2017.1380080

Carbonneau, R., Laframboise, K., & Vahidov, R. (2008). Application of machine learning techniques for supply chain demand forecasting. European Journal of Operational Research, 184(3), 1140-1154. https://doi.org/10.1016/j.ejor.2006.12.004

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438-457. https://doi.org/10.1145/581271.581274

Anderson, R., & Moore, T. (2006). The economics of information security. Science, 314(5799), 610-613. https://doi.org/10.1126/science.1130992

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. Proceedings of the IEEE Symposium on Security and Privacy, 305-316. https://doi.org/10.1109/SP.2010.25

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: Methods, systems and tools. IEEE Communications Surveys & Tutorials, 16(1), 303-336. https://doi.org/10.1109/SURV.2013.052213.00046

Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41-50. https://doi.org/10.1109/TETCI.2017.2772792

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation, 34(7), 342-353. https://doi.org/10.1016/j.technovation.2014.02.001

Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 1876-1907. https://doi.org/10.1080/17517575.2021.2008513

Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715-1729. https://doi.org/10.1007/s10796-022-10248-7

Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1-2), 2448003. https://doi.org/10.1080/17517575.2024.2448003

Kou, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1-34. https://doi.org/10.1186/s40854-024-00668-6

Xu, R., Zhu, J., Yang, L., Lu, Y., & Xu, L. D. (2024). Decentralized finance (DeFi): A paradigm shift in the FinTech. Enterprise Information Systems, 18(9), 2397630. https://doi.org/10.1080/17517575.2024.2397630

Lu, W., Lu, Y., Li, J., Sigov, A., Ratkin, L., & Ivanov, L. A. (2024). Quantum machine learning: Classifications, challenges, and solutions. Journal of Industrial Information Integration, 42, 100736. https://doi.org/10.1016/j.jii.2024.100736

Lu, Y., & Yang, J. (2024). Quantum financing system: A survey on quantum algorithms, potential scenarios and open research issues. Journal of Industrial Information Integration, 41, 100663. https://doi.org/10.1016/j.jii.2024.100663

Raissi, M., Perdikaris, P., & Karniadakis, G. E. (2019). Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations. Journal of Computational Physics, 378, 686-707. https://doi.org/10.1016/j.jcp.2018.10.045

Karniadakis, G. E., Kevrekidis, I. G., Lu, L., Perdikaris, P., Wang, S., & Yang, L. (2021). Physics-informed machine learning. Nature Reviews Physics, 3(6), 422-440. https://doi.org/10.1038/s42254-021-00314-5

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. Journal of Strategic Information Systems, 28(2), 118-144. https://doi.org/10.1016/j.jsis.2019.01.003