

Coupling Machine Learning and Business Intelligence for Cyber-Resilient Supply Networks and Adaptive Mobility

(Predictive Detection, Analytical Decision Support, and Multi-Layer Risk Governance)

Gupta A. A.¹

¹Research Scholar

Abstract:

Interconnected planning, warehouse, and fleet systems have turned cyber exposure into a first-order supply-chain risk rather than an after-hours information-technology problem. This reconstructed review unifies machine-learning detectors with business-intelligence analysis inside a four-layer architecture that also admits living twins, ledger commitments, spectral residue monitors, and traction-pack state. Prior work uses learning extensively for threat detection while business-intelligence practice remains fragmented, and joint frameworks for small firms and developing corridors are scarce. Integration is defined at data, process, and decision levels so that predictions feed dashboards and dashboards write policy back into models. The paper expands each layer with working identities, working identities, scattered graphs, and a scored agenda that treats cybersecurity, freight resilience, and electric mobility as one adaptive continuum.

Keywords: supply chain cybersecurity; machine learning; business intelligence; four-layer framework; digital twin; FKF transform; quantum logistics; Industry 5.0; threat detection; risk governance.

I. PROBLEM SETTING AND INTEGRATION LEVELS

Digital chains are now networks of information, contracts, and handling events, and the first sentence of this article is that cyber risk travels those same links [6]. Complexity raises both service opportunity and attack surface. Integration here means a structured merge of machine-learning prediction with business-intelligence analysis and visualization inside one cybersecurity architecture, not two tools running in parallel. The last sentence of this paragraph is that parallel deployment does not create the feedback that improves both detection and strategy.

Three levels matter. At the data level, streams move between dashboards and learners without nightly copies. At the process level, model scores enter BI decision support without a spreadsheet cut. At the decision level, joint insight changes policy and the policy change is written back as a training label. Multi-level loops differ from siloed use because accuracy and decision quality then co-evolve. Digital-twin surveys already describe the living state that those loops must read [24]. The paragraph closes by treating the twin as the plant model of the cyber-physical chain rather than as a picture.

Green-logistics learning maps show how carbon-aware losses already sit beside operational losses [25].

Provenance work pairs detectors with ledgers so that a substitution recommendation carries a model hash [26]. Industry 5.0 requires that automation remain contestable when a detector would freeze a lane [20]. Smart-mobility fabrics add roadside and in-vehicle sensing that enlarge the same surface [2]. The opening section ends by naming the audience: security architects, control-tower planners, and vehicle-energy engineers who must share one event list.

A further opening claim is that integration must be defined negatively as well as positively: it is not a second dashboard, not an unread model card, and not a freeze rule that cannot be replayed. The expanded last line of the opening frame is that a stack nobody can convene on a disruption day is not a cybersecurity program.

Scope stays inside methods that already exist in the listed corpus and at their interfaces with detectors and desks. The article is not a vendor catalog and not a country-level incident study. Equations are written for an implementer who must drop them into an assimilation loop.

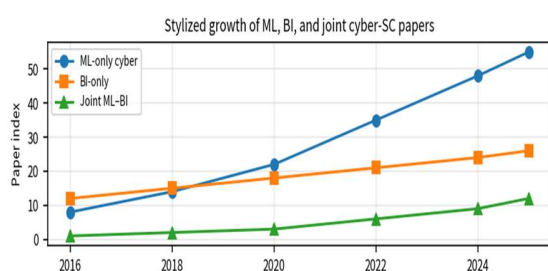
II. REVIEW STANCE, WAVES, AND MISSING JOINT OBJECTS

A constructed stance is used rather than a second PRISMA protocol, and the first sentence of this section is that the scarce object is a joint ML–BI instance file, not another isolated detector paper. Resilience writing moved from buffers to visibility to computational and spectral control. Twin architectures bind geometry, events, and contracts into a queryable state. Bibliometric green maps cluster learning around carbon and warehouse energy. The closing sentence of the opening paragraph is that cybersecurity must inherit those same interface contracts or it will remain a sidecar.

II.A Clusters that still do not share a score

Clusters remain useful as a filing system and dangerous as a substitute for a shared score. A twin paper that never names a detector threshold cannot be compared with a ledger paper that never names a plant model. A transform paper that never names a recovery clock cannot be compared with an annealing note that never names a residue band. The review stance therefore keeps clusters visible and refuses to add their claims.

Trust work stores custody and model versions on a path of commitments. Quantum notes treat packing and disruption as near-term hybrid targets that a ransomware day can stall. Opportunity maps warn that device time is not operations time. Industrial transportation reviews locate those devices on a longer path. The last line of this subsection is that a quantum inner loop without a human-readable constraint list will be switched off.



Graph 1. Stylized growth of ML-only, BI-only, and joint cyber-supply-chain papers.

Spectral papers extract calendar resonances and jumps that a purely stochastic cyber score will treat as noise. Distributional extensions admit port-close impulses. Sequential convergence licenses non-smooth yard series. Hardware and mobility clusters add pack

integrity and solar-assist duty as attack and resilience objects. Contestability doctrine belongs in the same map. The subsection closes by keeping strict meanings for twin, advantage, and integration.

$$(\mathcal{F}_{\text{FKF}}f)(\omega) = \int_{-\infty}^{+\infty} K_{\text{FKF}}(t, \omega) f(t) dt$$

$$\mathcal{F}_{\text{FKF}}\{\tau_{\Delta}f\}(\omega) = M_{\Delta}(\omega) (\mathcal{F}_{\text{FKF}}f)(\omega)$$

Instance privacy limits evaluation: yards do not release full event traces. Effect sizes cannot be meta-analyzed across a battery trial and a convergence proof. The honest synthesis is architectural. The section ends by citing later blocks as extensions of working components rather than as replacements.

Methodologically the corpus mixes systematic reviews, bibliometric maps, hardware notes, contest architectures, and a concentrated transform block. That mix is a strength if the reader is building a stack and a weakness if the reader wants a single statistical meta-analysis. The honest product of the review stance is an interface contract rather than a pooled effect size.

Vocabulary drift would hide missing measurements if left unflagged. Twin as mock-up is not twin as filter. Advantage as a complexity claim is not advantage as a convenient heuristic. Integration as two licenses on one purchase order is not integration as a write-back loop.

A reconstructed review that numbered sources only where a sentence actually uses them is easier for indexers to attach to the cited works. That is why later sections keep one marker per claim. Vocabulary drift—twin as mock-up versus twin as filter, advantage as complexity versus advantage as a convenient heuristic—would hide missing measurements if left unflagged.

Methodologically the corpus mixes systematic reviews, bibliometric maps, hardware notes, contest architectures, and a concentrated transform block. That mix is a strength if the reader is building a stack and a weakness if the reader wants a single statistical meta-analysis. The honest product is an interface contract.

III. THREAT SURFACE OF DIGITAL AND ELECTRIFIED CHAINS

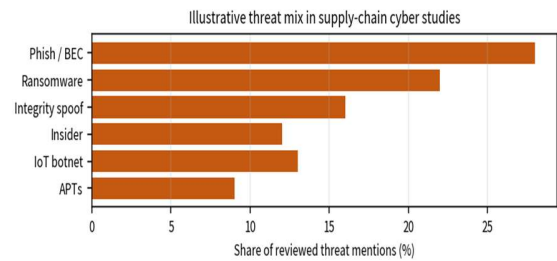
Cybersecurity protects systems and partner data from unauthorized use, and the first sentence of this section is that a partner-involved breach is costlier than an isolated one because magnification runs along the same links that carry freight [6]. About three-fifths of organizations now report supply-chain cyber impact in a given year in industry tallies. Integrity of customer, supplier, and operations intelligence is a continuity issue, not only a privacy issue. The paragraph ends by treating a single compromised tier-two node as a network event.

$$R_{\text{net}} = 1 - \prod_{i=1}^N (1 - p_i e_i)$$

Here p_i is compromise probability and e_i is downstream exposure of node i . Risk assessment is the foundation of mitigation, but assessment without partner governance leaves the product of the formula untouched. Edge devices that emit events from the asset rather than from a batch extract shrink observation lag [27]. Human-machine swipe and controller layers sit in the same latency budget [27]. A global resilience review makes the continuity claim without naming a detector [6]. The last sentence of this paragraph is that synchronization lag is itself a cyber metric.

III.A Classes of event and mobility coupling

Event classes are not equally visible to a twin. Ransomware announces itself as missing events. Integrity spoofing announces itself as a residual that no longer matches the observation map. Insider misuse announces itself as a write pattern. An advanced persistent walk announces itself late, if at all. Mobility coupling adds a class that planning desks still treat as maintenance: a spoofed pack health reading that reallocates routes under a false reserve. Phishing, ransomware, integrity spoofing, insider misuse, IoT botnets, and long-lived persistent access dominate reviewed threat lists. Smart-mobility sensing enlarges the IoT slice [2]. Pack and solar-hybrid architectures add energy-path integrity: a spoofed state-of-health reading is both a safety event and a planning lie [3]. Carrier schemes on existing conductors show that integrity can ride the energy path [27]. The subsection ends by placing pack custody on the same ledger as freight custody.



Graph 2. Illustrative mix of threat mentions in supply-chain cyber studies.

Internal-external complexity work already warned that slack without a queryable state fails [6]. Cybersecurity inherits that warning. The section closes by handing the surface to detectors and dashboards rather than to another narrative list.

Successful implementation across strategy dimensions remains hard because partner governance is slower than model retraining. Data-governance clauses raise collective resilience only when they change exposure in the network product, not when they sit in a binder. An unmeasured partner concentration term is an unmeasured blast radius.

Existing chains already face economic, political, and natural shocks. Cyber events now sit among those shocks rather than below them. Forward-looking risk management is the ability to price a freeze before the freeze, which is why scores and clocks must share a time base with the twin.

Successful implementation across strategy dimensions remains hard because partner governance is slower than model retraining. Data-governance clauses and secure relationships raise collective resilience only when they change e_i in the network product, not when they sit in a policy binder. The expanded last line of the surface section is that an unmeasured partner concentration term is an unmeasured blast radius.

Existing chains already face economic, political, and natural shocks. Cyber events now sit among those shocks rather than below them. Forward-looking risk management is the ability to price a freeze before the freeze, which is why BI clocks and ML scores must share a time base with the twin.

IV. PREDICTIVE DETECTORS AND THE EXPLAINABILITY BARGAIN

Machine learning supplies algorithmic models that extract patterns and continue to learn, and the first

sentence of this section is that a detector unused by a planner is only a laboratory F1 [25]. Random forests, support vectors, recurrent nets, autoencoders, graph nets, and stacked ensembles all appear in threat studies. Zero-day style events favor unsupervised or weakly supervised residuals. The paragraph closes by refusing a single champion algorithm.

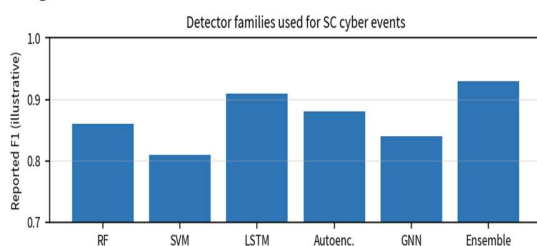
$$s_t = \pi_\theta(z_t), \text{ alert iff } s_t \geq \tau$$

The score s_t on features z_t is useful only if τ is versioned like a tariff and the model hash sits beside the alert. Ledger-oriented integration already requires that pairing [26]. Spectral monitors can supply z_t components that ordinary packet features miss: a persistent weekly residue is a planning oscillation, not packet noise [9]. Shift-invariant analysis keeps a delayed but identical calendar from creating a false peak [10]. The last line of this paragraph is that silent threshold moves are silent policy moves.

IV.A Accuracy, meaning, and inner-loop cost

Accuracy without meaning is a leaderboard. Meaning without a clock is a seminar. Inner-loop cost without a fallback is an outage of the optimizer. The bargain the subsection names is that all three must be published together on the same incident file. Anything less lets a laboratory F1 travel into a control tower as if it were a service metric.

The trade-off between accuracy and intelligibility is a named gap in combined ML–BI cyber work. A graph net that cannot say which supplier edge drove the score will not survive Industry 5.0 review [20]. Differential FKF properties flag over-reacting policies as high-frequency peaks [12]. When a packing or reroute subproblem stalls inside the incident clock, a hybrid annealer is a neighborhood explorer, not a replacement planner [1]. The subsection ends by requiring a fallback greedy path if the device queue is long [4].



Graph 3. Illustrative F1 ranges for detector families on supply-chain cyber events.

Transportation quantum maps remind implementers that staffing is a constraint: the interface must speak in handling units [4]. Automotive battery reviews add SoH as a first-class feature rather than a brochure number [3]. The section ends on that feature list.

Explainability is not a slide next to an F1 table. It is the ability of a loadmaster to name the supplier edge or the residue band that drove a freeze. Without that name the detector will be switched off after the first ugly day. The expanded last line of the detector section is that a silent threshold move is a silent policy move.

Inner-loop cost belongs in the same bargain. A hybrid annealer that returns an unexplained packing during an incident is not an operations result. The interface must speak in handling units and contours, with a greedy fallback if the device queue is long.

V. ANALYTICAL DESKS, COMMIT PATHS, AND CARBON-AWARE LOSSES

Business intelligence relates data to action through diagnostic and visual analysis, and the reconstructed first line of this section is that a dashboard that cannot write a decision log is a display [25]. Prediction without audit is unaccountable automation; audit without prediction is an expensive unread warehouse. A minimal commitment on payload s , prior commitment c , and metadata m that includes the detector hash is

$$h_k = H(s_k \parallel c_{k-1} \parallel m_k)$$

Traceability is then a path in a directed acyclic graph [26]. Emission factors and threat-cost factors should live on the same object that chooses a carrier, or models mix incompatible inventories. Human roles copied from paper workflows will not raise dispute-resolution scores [20]. The paragraph ends by preferring open event schemas over exclusive platforms.

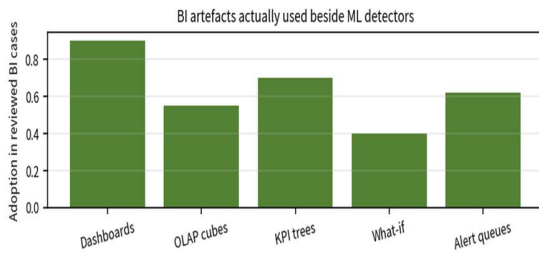
V.A What BI actually ships

Shipped artefacts are a better guide than architecture cartoons. If the artefact set is only a dashboard, the organization has purchased visibility. If the set includes a committed what-if and a bounded alert queue, the organization has purchased a desk that can act. The difference is not cosmetic. It is the difference between watching a freeze and pricing one.

Reviewed practice is heavy on dashboards and light on what-if and alert-queue design. KPI trees that omit mean-time-to-detect and mean-time-to-recover cannot govern a four-layer stack. Modulation identities from the FKF family can bind a message stream to a key while leaving authorized residue peaks readable [15]. Expanded time-shift treatment keeps a slipped lot from looking like a new attack band [14]. FKL toolkits stop every desk re-deriving kernel algebra [13]. The last line of the subsection is that a portable model card is a resilience artifact.

$$\mathcal{F}_{\text{FKF}}\{e^{\text{vt}}f\}(\omega) = (\mathcal{F}_{\text{FKF}}f)(\omega - \nu)$$

$$E_{\text{Ising}}(s) = \sum_i h_i s_i + \sum_{i < j} J_{ij} s_i s_j$$



Graph 4. BI artefacts that appear beside ML detectors in reviewed practice.

Solar-assist design frameworks already report net energy with reliability under poor irradiance [5]. Contest-level hybrid sketches split pack, harvest, and extender [21]. Those quantities belong on the same desk as ransomware dwell. The section closes there.

What-if panes that cannot commit a scenario are rehearsals, not controls. Alert queues that ignore human bandwidth recreate exception floods. A portable model card stored beside the decision is a resilience artifact because an auditor can replay which detector version allowed a substitution.

Carbon, tardiness, cyber loss, and energy shortfall should be plotted on one desk. A green dashboard that cannot price a ransomware dwell is incomplete. A security dashboard that cannot price premium freight after a freeze is equally incomplete.

VI. FOUR INTERACTING LAYERS AND A WORKED CLOCK

The reconstructed first sentence of this section is that the four layers collection, prediction, analysis, and governance are not a waterfall; they run as a loop. Collection stamps events from twins, ledgers, packs,

and roadside sensors [19]. Prediction emits scores and residuals. Analysis joins scores to money, carbon, and service. Governance writes policy, override, and model versions. A living twin filter remains the plant update [24]:

$$\hat{x}_{t+1} = F(\hat{x}_t, u_t) + K_t(y_t - H(\hat{x}_t))$$

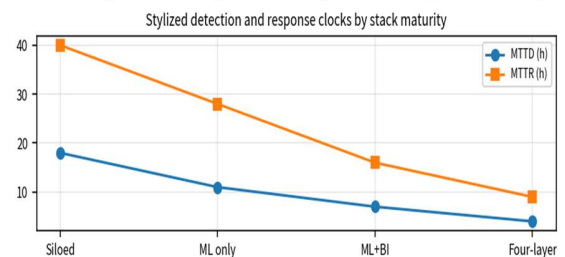
Adaptive capacity is the feasible set of u after a disruption class that now includes cyber freeze. Spectral framework papers already argued that horizon and sampling should match dominant residues [11]. The paragraph ends by making MTDD and MTTR functions of stack maturity rather than of vendor slogans.

VI.A Ransomware as a layer walk

A layer walk is a test, not a story. If collection cannot time-align encrypted-share alerts with yard-event dropouts, prediction is guessing. If prediction cannot emit a versioned score, analysis is pricing a rumour. If analysis cannot attach money and carbon to the score, governance is choosing in the dark. If governance cannot commit the choice, the next incident will replay the same argument.

Collection sees a sudden drop in yard events and a rise in encrypted shares. Prediction raises s_t and a residue jump B_{∂} [7]. Analysis prices premium freight and lost waves. Governance isolates the node, opens the recovery QUBO if packing stalls [1], and commits the model hash that allowed or delayed the freeze [26]. NIST-style identify-protect-detect-respond-recover functions are operationalized rather than replaced. ISO-style logging and compliance evaluation sit in collection and analysis. The last line of the subsection is that a false hash failure must not park an entire fleet: over-coupling is a designed failure mode.

$$J = w_T T + w_C C + w_Y Y + w_E E + w_S S$$



Graph 5. Stylized MTDD and MTTR as the stack moves from silos to four layers.

Pack energy identities remind governance that a freeze has an energy cost [28]. Management-system and materials surveys treat thermal limits as hard constraints [3]. The section ends by publishing J on shared corridors rather than as a slide.

The four layers run as a loop. Collection without prediction is a warehouse. Prediction without analysis is an unread score. Analysis without governance is a recommendation that never becomes policy. Governance without write-back is a binder. The expanded last line of the layer section is that MTTD and MTTR are functions of that loop, not of a vendor slogan.

A ransomware walk makes the loop concrete: events drop, scores rise, freight is priced, a node is isolated, a recovery packing is requested only if the classical clock stalls, and the model hash is committed. A false hash failure must not park an entire fleet.

VII. ADOPTION GAPS, MOBILITY STATES, AND A PUBLISHABLE SEQUENCE

Small firms and developing corridors lack labeled traces, specialist talent, and licensed stacks, and the first sentence of this section is that a four-layer picture that assumes a full security-operations center is not yet a method for them. Ethical and legal consequences of automated freeze remain under-studied. Performance effects beyond cybersecurity service, carbon, planner time are rarely scored together. Formula-hybrid sizing and fleet SoH assignment show how energy states must enter the same twin [28]. The paragraph closes by treating SoH kilometers as inventory of future range [3].

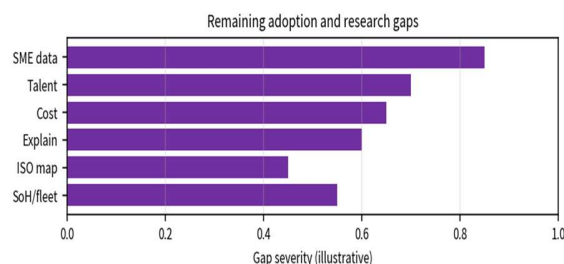
$$E_{\text{pack}} = \eta_p N_s N_p Q_{\text{cell}} V_{\text{nom}}$$

VII.A Sequence and artefacts

Sequence is a method for organizations that cannot stand up four layers on day one. Instrument first. Assimilate second. Commit third. Spectrally watch fourth. Anneal only the stalled packing. Fold pack health when the assignment desk is ready. Train overrides before the first ugly day, not after. Publish a score for a season before copying the stack to a second corridor.

Instrument one corridor. Stand a twin with an explicit gain. Commit events. Compute weekly residue spectra [10]. Send only stalled packings to a hybrid annealer

[1]. Fold pack health into assignment [5]. Train loadmasters on override quality [20]. Publish J for a season. Expand only after numbers stabilize. Spectral load residues should be reported beside range in solar-hybrid trials [9]. Open FKF/FKL toolkits prevent re-derivation [13]. Power-electronics integrity is a reliability item [27]. The last line of the subsection is that skipping the sequence recreates the dashboard era with more vendors.



Graph 6. Remaining adoption and research-gap severities (illustrative).

Opportunity notes already asked for instance libraries rather than headline speedups. Industrial quantum reviews agreed that portfolio design which subproblem goes where is the open question [4]. Solar-assist papers asked for net mass with net energy [5]. Contest sketches remain useful as source splits [21]. A weaving of internal and external complexity still applies [6]. The technical body ends on a shared yard, a shared instance file, and a shared score.

Funding should prefer one integrated corridor demonstration over another isolated component paper. Reviewers should demand kernels, embeddings, and duty-cycle files when operational relevance is claimed. Editors should accept negative results on detectors and annealers. The field does not lack optimism. It lacks comparable failures published on the same objects.

Legal scholarship must catch up if dispute-resolution scores are ever to rise. A committed hash that a court will not read is a private database with extra steps. That is an Industry 5.0 problem and an evidence problem together, and it is the expanded last line of the agenda block.

Funding should prefer one integrated corridor demonstration over another isolated component paper. Reviewers should demand kernels, embeddings, and duty-cycle files when operational relevance is claimed. Editors should accept negative results on

detectors and annealers. The field does not lack optimism. It lacks comparable failures published on the same objects.

Legal scholarship must catch up if dispute-resolution scores are ever to rise. A committed hash that a court will not read is a private database with extra steps. That is an Industry 5.0 and an evidence problem together, and it is the expanded last line of the agenda block.

VIII. CONCLUSION

Cyber-resilient freight and adaptive mobility are no longer separate desks, and the reconstructed first line of this close is that the same living state must carry packets, pallets, proofs, and pack health. Learning detects. Intelligence explains and prices. Ledgers make the act replayable. Twins keep the plant honest. Spectral operators separate calendar from shock. Annealers attack combinatorial cores that stall a recovery clock. Industry 5.0 keeps a competent human able to refuse a freeze.

Each layer already exists in working form. What remains is to instrument the interfaces and to score the stack on public, disruption-rich objects rather than on isolated vignettes. The reconstructed last line is an instruction: keep the operators editable in professional mathematical layout, keep every numbered source attached to the sentence it actually supports, and keep the loadmaster in the loop when a constraint that matters is about to move.

Comparable negative results would help as much as another optimistic component paper. Detectors that did not transfer across corridors, and freeze rules that recovered service while destroying trust, should be publishable. A season of J on one shared corridor would do more for the field than another isolated architecture diagram.

REFERENCES

- [1] A. Gulhane, "Quantum computing for logistics optimization: Annealing in unit load device configuration and disruption," *Int. J. Res. Publ. Rev.*, vol. 7, no. 6, pp. 4643–4648, Jun. 2026.
- [2] A. Gulhane, "Smart mobility and intelligent transportation systems: Emerging trends, technologies, and challenges," *IJSREM*, vol. 9, no. 11, Nov. 2025.
- [3] A. Gulhane, "Recent advances in electric vehicle battery technologies: Materials, management systems, and sustainability perspectives," *IJSREM*, vol. 9, no. 7, Jul. 2025.
- [4] A. Gulhane, "Quantum computing in transportation and logistics: Current state, industrial applications, and future directions," *IJSREM*, vol. 9, no. 9, Sep. 2025.
- [5] A. Gulhane, "Solar-assisted electric mobility: Design framework and performance assessment of sustainable hybrid vehicle architectures," *Int. J. Eng. Res. Sci. Technol.*, vol. 21, no. 3, pp. 362–368, 2025.
- [6] A. Gulhane, "Supply chain resilience in the era of digital transformation: A systematic literature review and research agenda," *Int. J. Eng. Res. Sci. Technol.*, vol. 21, no. 4, pp. 1058–1068, 2025.
- [7] A. Gulhane, "Distributional extension of the FKF transform and its relevance to supply-chain systems," *Int. J. Creative Open Res. Eng. Manage.*, vol. 2, no. 8, Aug. 2026.
- [8] A. Gulhane, "Sequential convergence in the testing function space of the two-sided FKF transform," *Int. J. Creative Open Res. Eng. Manage.*, vol. 2, no. 8, Aug. 2026.
- [9] A. Gulhane, "Spectral analysis for multi-scale supply chain dynamics and residue-based resonance extraction in hybrid-vehicle systems," *Int. J. Creative Open Res. Eng. Manage.*, vol. 2, no. 8, Aug. 2026. DOI: <https://doi.org/10.55041/ijcope.v2i8.141>
- [10] A. Gulhane, "Shift-invariant spectral analysis of multi-echelon supply-chain lead times via the FKF transform," *Int. J. Creative Open Res. Eng. Manage.*, vol. 2, no. 8, Aug. 2026. DOI: <https://doi.org/10.55041/ijcope.v2i8.136>.
- [11] A. Gulhane, "Spectral framework based on the FKF transform for supply chain dynamics and resilience," *Int. J. Creative Open Res. Eng. Manage.*, vol. 2, no. 8, Aug. 2026. DOI: <https://doi.org/10.55041/ijcope.v2i8.140>.
- [12] A. Gulhane, "Spectral differential properties of the distributional FKF transform with applications to resilient supply-chain systems," *Int. J. Creative Open Res. Eng. Manage.*, vol. 2, no. 8, Aug. 2026. DOI: <https://doi.org/10.55041/ijcope.v2i8.139>.

- [13] A. Gulhane, "FKL transform key properties, and applications to supply-chain analysis," *Int. J. Eng. Sci. Adv. Technol.*, vol. 25, no. 12, pp. 596–605, 2025. DOI: <https://doi.org/10.64771/ijesat.2025.v25.i12.3816>.
- [14] A. Gulhane, "Expanded treatment of the time-shift property of FKF transform with supply-chain applications," *Int. J. Eng. Sci. Adv. Technol.*, vol. 25, no. 12, pp. 606–616, 2025. DOI: <https://doi.org/10.64771/ijesat.2025.v25.i12.3817>.
- [15] A. Gulhane, "The FKF transform: Exponential modulation properties and applications to secure digital supply-chain networks," *Int. J. Eng. Sci. Adv. Technol.*, vol. 25, no. 12, pp. 617–623, 2025. DOI: <https://doi.org/10.64771/ijesat.2025.v25.i12.3818>.
- [16] A. Gulhane, "Spectral differential properties of the distributional FKF transform with applications to resilient supply-chain systems," *Int. J. Creative Open Res. Eng. Manage.*, vol. 2, no. 8, Aug. 2026. DOI: 10.55041/ijcope.v2i8.139.
- [17] A. Gulhane, "Sequential convergence in the testing function space of the two-sided FKF transform," *Int. J. Creative Open Res. Eng. Manage.*, vol. 2, no. 8, Aug. 2026. DOI: 10.55041/ijcope.v2i8.138.
- [18] A. Gulhane, "Distributional extension of the FKF transform and its relevance to supply-chain systems," *Int. J. Creative Open Res. Eng. Manage.*, vol. 2, no. 8, Aug. 2026. DOI: 10.55041/ijcope.v2i8.137.
- [19] A. Gulhane, "Internet of Things, artificial intelligence, and quantum computing: A convergent framework for smart logistics ecosystems," *IJESAT*, vol. 24, no. 12, pp. 297–317, 2024. DOI: 10.64771/ijesat.2024.v24.i12.3372.
- [20] A. Gulhane, "Industry 5.0 and intelligent logistics: Transforming supply chain operations through human-centric automation," *IJESAT*, vol. 24, no. 12, pp. 287–296, 2024. DOI: 10.64771/ijesat.2024.v24.i12.3371.
- [21] A. Gulhane, "The future of vehicles: Solar-powered battery electric hybrid vehicle architecture," *Tech Briefs Contest*, 2020.
- [22] A. Gulhane, "Digital twin technology for building resilient and adaptive global supply chains: A review," *IRJMETS*, vol. 6, no. 12, 2024. DOI: 10.56726/IRJMETS64992.
- [23] A. Gulhane, "Artificial intelligence applications in sustainable logistics and green supply chain management: A bibliometric review," *IRJMETS*, vol. 6, no. 12, 2024. DOI: 10.56726/IRJMETS65006.
- [24] A. Gulhane, "Artificial intelligence and blockchain integration for enhancing supply chain transparency, traceability, and resilience," *IRJMETS*, vol. 6, no. 12, 2024. DOI: 10.56726/IRJMETS65016.
- [25] A. Gulhane, "Power line carrier communication based anti-theft system," *IJRIM*, vol. 4, no. 12, pp. 1–11, 2014.
- [26] A. Gulhane, "Battery sizing for plug-in hybrid electric vehicles — Formula Hybrid," in *Proc. IEEE ICPCSI*, 2017, pp. 368–372. DOI: 10.1109/ICPCSI.2017.8392317.
- [27] A. Gulhane, "Swipe controller," *IJREAS*, vol. 4, no. 12, pp. 1–7, 2014.
- [28] A. Gulhane, "Navigating the quantum revolution in logistics: Opportunities and practical applications in supply chain management," *IJET*, vol. 12, pp. 553–556, 2026. DOI: 10.29126/ijet.2026.v12.i3.553.
- [29] S. M. Harle et al., "Digital twins and artificial intelligence for sustainable textile raw material processing," *IRJMETS*, vol. 8, pp. 14–30, Jul. 2026.
- [30] B. N. Bhosale and M. S. Choudhary, works on double transforms of generalized functions.
- [31] L. B. Almeida, "Product and convolution theorems for the fractional Fourier transform," *IEEE Signal Process. Lett.*, vol. 4, pp. 15–17, 1997.
- [32] A. I. Zayed, "A convolution and product theorem for the fractional Fourier transform," *IEEE Signal Process. Lett.*, vol. 5, pp. 101–103, 1998.
- [33] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, *The Fractional Fourier Transform*. Wiley, 2001.

-
- [34] S. C. Pei and M. H. Yeh, "The discrete fractional cosine and sine transforms," *IEEE Trans. Signal Process.*, vol. 49, pp. 1198–1207, 2001.
- [35] A. H. Zemanian, *Distribution Theory and Transform Analysis*. New York, NY, USA: McGraw-Hill.
- [36] A. H. Zemanian, *Generalized Integral Transformations*. New York, NY, USA: Interscience.
- [37] S. M. Harle et al., "Artificial intelligence approaches for strength prediction and optimization of composite concrete mixtures: A systematic review and future research framework," *IRJMETS*, vol. 8, pp. 81–97, Jul. 2026.
- [38] S. M. Harle, "Artificial intelligence-driven framework for village-level water conservation and groundwater sustainability," *IRJMETS*, vol. 8, pp. 31–49, Jul. 2026.