

Neuro-Cognitive Sentiment Orchestration: A Multi-Modal Deep Learning Framework for Predictive Mental Health Analytics in Academic and Professional Ecosystems

Naga Venkatesh Gangabathula

MS in Computer Science

Souther Illinois University

Carbondale

Abstract-Mental health challenges among students and working professionals represent a growing public health crisis, exacerbated by academic pressure, workplace stress, social isolation, and digital overload. Traditional screening methods rely on self-reported surveys and clinical interviews, which are reactive, infrequent, and prone to reporting bias. We propose a fully integrated Multi-Modal Mental Health Analytics Framework (MMHAF) using three analytically novel architectures to enable proactive, personalized, and privacy-preserving psychological risk prediction. We build a Neuro-Cognitive Sentiment Embedding (NCSE) from textual, behavioral, and physiological signals using a hybrid Transformer-LSTM network, providing a psychologically grounded risk baseline that classical survey methods ignore. The Affective Graph Verifier (AGV) employs social interaction topology and emotional signature patterns to improve anomaly detection in behavioral trajectories. The validated outputs enter the Temporal Risk Forecasting Engine (TRFE) with multi-scale temporal embeddings for longitudinal wellness prediction. Together, the components promote early warning accuracy, intervention anticipation, and self-correcting support routing. In high-stress academic and occupational contexts, the framework reduces false alarms, accelerates risk detection, enhances prediction reliability, and builds a resilient architecture for next-generation mental wellness systems.

Keywords: Mental Health Analytics, Deep Learning, Student Wellbeing, Professional Burnout, Affective Computing, Federated Learning, Explainable AI.

1. Introduction

Educational institutions and modern workplaces now require coordinating distributed human assets in complex psychosocial environments. Students navigating academic deadlines, examinations, and social transitions [1, 2, 3], alongside professionals managing project pressures, remote work isolation, and career uncertainty, generate vital behavioral and emotional data through digital interactions. Opponents manifesting as chronic stress, anxiety disorders, depressive episodes, or burnout can alter cognitive-emotional states or inject subtle distortions into communication patterns, weakening psychological resilience and functional performance. Cyber-psychological stressors are growing increasingly complex, using latent correlations between digital behavior, physiological signals, and emotional expression. Traditional mental health frameworks for clinical settings ignore behavioral telemetry uncertainty, contextual dependency, and multiscale stress interconnections in academic and occupational contexts. Despite the utility of standardized screening tools and statistical risk models, static assessment protocols or classical psychometric approaches limit their effectiveness against dynamic, evolving psychological challenges. Verification is unaware of emotional-channel instabilities because current systems rarely integrate real-time behavioral observations directly into risk prediction. Most machine-learning sentiment models predict without reference to intervention protocols; therefore, they cannot affect real-time support choices. System resilience is reduced without an adaptive governance layer because wellness policies remain fixed even when individual circumstances [4, 5, 6] or environmental stressors change significantly. This is addressed by integrating behavioral-state analytics, affective verification dynamics, and multi-scale stress prediction into a continuous mental wellness decision pipeline. The framework converts behavioral signals into intervention actions using three analytically new methods: NCSE, AGV, and TRFE. Emotional entropy, topological interaction signatures, stress tensors, and adaptive feedback significantly affect intervention decisions due to the tightly coupled chain of approaches. It makes psychological stability physically observable, hazard anticipation utilizing behavioral and topological indicators, and support routing dynamically rather than by fixed norms.

The system ensures wellness reliability in next-generation educational and occupational operations through personalization, privacy, and adaptability.

2. Review of Existing Models Used For Model Analysis

TABLE 1: Model's Empirical Review Analysis

Ref	Method	Main Objectives	Findings	Limitations
[1]	Computational safety–security boundary modeling	Develop unified psychological boundary models	Improved cross-domain wellness–security integration	Limited empirical educational validation
[2]	Belief rule base with fuzzy credibility	Enable interpretability in mental health assessment of students	High interpretability with improved diagnostic accuracy	Requires expert-tuned rules
[3]	Real-time forecasting using integrated data streams	Predict wellness trends dynamically	High adaptability to real-time signals	Not optimized for academic risk analysis
[4]	Human–machine interaction modeling in education	Identify emerging factors in academic planning	Revealed impact of cognitive load on scheduling decisions	No automation integration
[5]	CEEMDAN–GARCH hybrid modeling	Analyze volatility in academic performance	Captured multi-frequency volatility characteristics	High computational complexity
[6]	MBSE plugin for cloud wellness	Strengthen cloud wellness for large-scale systems	Improved architectural design correctness	Restricted to cloud-specific models
[7]	Screen-time degradation analysis	Study digital exposure effects on student cognition	Quantified degradation in attentional capacity	Limited to narrow demographic categories
[8]	Educational digital twin modeling	Enable virtualized monitoring of student assets	Demonstrated optimized wellness planning	Weak integration with AI-driven analytics
[9]	Thermodynamic wellness modeling	Optimize wellness assessment procedures	Improved accuracy and reproducibility of tests	Highly system-specific implementation
[10]	Quaternion-based emotional security	Improve robustness of emotional encoding schemes	Achieved high security for multimedia wellness systems	Computational overhead in large-scale operations
[11]	ML-driven behavioral radiography detection	Improve student behavioral inspection accuracy	Notable reduction in behavioral misclassification	Requires extensive labeled data
[12]	6G-IoT cyber-psychological student wellness	Protect student digital wellness networks	Enhanced encryption and real-time threat detection	Scalability uncertainties
[13]	Intelligent anomaly detection in educational manufacturing	Detect faults in educational production	Increased diagnostic precision	Struggles with rare anomaly types
[14]	Deep learning models for educational systems	Survey application breadth	Demonstrated wide applicability across educational domains	Lacks a unified implementation guide
[15]	Adaptation-YOLO for sentiment imaging	Improve concealed emotional object detection	Strong performance improvement under noisy conditions	Sensitive to dataset imbalance

[16]	Digital wellness ethics and security analysis	Study socio-political tensions of digital wellness monitoring	Highlights conflicting governance and wellness logics	No technical mitigation strategies proposed
[17]	Student hazard and risk modeling	Identify operational wellness risks	Provided useful taxonomies for student failures	Absence of predictive or learning-based models
[18]	TSN-based digital twin for STRIDE wellness testing	Enhance emotional security assessments	Robust virtualization-based threat evaluation	High configuration and deployment complexity
[19]	Attack-tree-based quantitative logic (ATM)	Model complex emotional threat scenarios	Increased formal expressiveness for wellness reasoning	Requires expert familiarity with formal methods
[20]	FPGA-based hybrid wellness algorithm	Secure Network-on-Chip wellness architectures	Low-latency secure hardware integration	Limited flexibility for post-deployment updates
[21]	Smart secured educational investment casting	Fuse automation with wellness in educational workflows	Enhanced sustainability and system resilience through secure automation	Limited educational application testing
[22]	PVDF-SiO ₂ aerogel wellness separator	Improve emotional insulation and radiation shielding performance	Demonstrated strong emotional stability and radiation protection	Scale-up and mass manufacturing remain challenging
[23]	Fractal-embedded codes for educational supply chain security	Protect additively manufactured educational component authenticity	Tamper-resistant encoding validated under controlled conditions	Requires high-resolution sensing and decoding equipment
[24]	Blockchain-based access control framework	Secure educational process data and access rights	Improved traceability and role-based wellness enforcement	Performance dependent on blockchain scalability
[25]	Nanocomposite reinforcement materials	Enhance mechanical strength and X-ray shielding capability	Significant improvements in structural integrity and shielding efficiency	The industrial cost-benefit tradeoff remains unclear
[26]	Ecological security modeling approach	Study spatial connectivity and ecological impact dynamics	Revealed expansion-driven shifts in ecological security patterns	Not directly focused on educational systems
[27]	Eco-friendly propellant performance analysis	Characterize biomass-derived propellants for propulsion	Achieved comparable thrust with reduced environmental emissions	Limited long-term storage and stability evaluation
[28]	AI-driven threat intelligence generation	Automate and enhance emotional cybersecurity exercise generation	Increased realism, adaptability, and scenario diversity	Requires continuous data ingestion for effectiveness
[29]	Systems engineering optimization framework	Improve educational development workflow efficiency	Better timeline control through procedural optimization	Limited generalization across different educational platforms
[30]	Economic analysis of sanctions	Study policy-driven impacts on innovation ecosystems	Identified how sanctions reshape subsidy allocation	Indirect relevance to educational system design
[31]	Scientometric educational research	Quantify global evolution of educational-related research	Identified emerging research clusters and thematic trends	Descriptive in nature; lacks prescriptive or actionable insights

[32]	Student trajectory attack detection	Maintain student path integrity under emotional and signal attacks	Strong mitigation against performance trajectory spoofing	Highly dependent on sensor accuracy and reliability
------	-------------------------------------	--	---	---

3. Proposed Model Design Analysis

Each level of the proposed integrated behavioral-to-intervention pipeline incrementally refines, transforms, and contextualizes behavioral measurements into adaptive estimates of psychological security. Educational networks operate concurrently across behavioral, emotional, and environmental domains; therefore, their wellness mechanisms must theoretically characterize the coupled dynamics among these layers. The proposed model progresses through hybrid affective-topological verification, stress tensor prediction, adaptive feedback to wellness optimization, reinforcement signal-driven dynamic policy evolution, and entropy-driven stability extraction from raw behavioral-state statistics. Each functional block is mathematically linked such that its output serves as the analytical boundary condition for the subsequent stage, thereby ensuring causal consistency throughout the architectural workflow.

The behavioral-state analysis layer initially interprets behavioral sequences as smooth temporal functions whose entropy gradients reveal latent process instabilities, as illustrated in Fig. 1. For a behavioral state operator $S(t)$, the emotional entropy field is defined as:

$$H(t) = - \sum_i p_i(t) \log p_i(t) \quad (1)$$

which serves as the primary contextual parameter for behavioral-state uncertainty. Its temporal variation, capturing entropy evolution, is expressed as:

$$\frac{\partial H}{\partial t} \approx \frac{H(t) - H(t - \Delta t)}{\Delta t} \quad (2)$$

thereby characterizing the dynamic stability of educational communication channel sets.

The entropy field is subsequently mapped into a stability representation through a manifold projection defined by:

$$SV = \int S(\rho, x) \cdot \Phi(x) dx \quad (3)$$

where $\Phi(x)$ denotes a predefined behavioral-manifold basis that encodes operational constraints inherent to educational communication linkages. This formulation validates the behavioral security entropy (BSE) mapping stage, as entropy gradients are more sensitive to environmental disturbance patterns than conventional classical error-rate metrics.

As depicted in Fig. 2, the entropy-derived stability vectors are coupled with educational contact topology to generate persistent homology signatures for candidate wellness events during the verification-in-process phase. Let F denote the educational contact complex and $\psi(F)$ represent its associated Betti number evolution. The hybrid affective-graph verification metric is computed as:

$$V(F, \rho) = \alpha \cdot H_{pers}(F) + \beta \cdot S(\rho) + \gamma \cdot C(\Phi, \partial S / \partial t) \quad (4)$$

which is subsequently transformed into a legitimacy confidence score given by:

$$L = \sigma(W \cdot V(F, \rho) + b) \quad (5)$$

where $\sigma(\cdot)$ denotes a nonlinear activation function, and W represents the learned verification weight matrix.

This confidence measure quantitatively reflects the trustworthiness of behavioral-integrated educational wellness transactions under environmental-aware threat conditions. The curvature-regularized stability interaction is defined as:

$$C(\Phi, \partial S / \partial t) = \|\nabla^2 \Phi\| \cdot \|\partial S / \partial t\| \quad (6)$$

This quantifies the degree to which topological distortion aligns with environmental instability, thereby establishing the significance of the proposed hybrid affective-graph boundary verification (AGV) mechanism in detecting irregularities that cannot be isolated using either topological or behavioral features alone. As illustrated in Fig. 3, the wellness-prediction layer continuously generates temporal and spatial adversarial hazard tensor fields.

For multi-scale embeddings $E_\ell(t)$, the wellness-threat tensor is defined as:

$$T(x, t) = \sum_\ell K_\ell * E_\ell(t) \quad (7)$$

where $K\ell$ denotes convolutional kernels tuned to educational telemetry patterns. The corresponding threat intensity score is computed as:

$$\|T(x, t)\|_F \quad (8)$$

Where $\|\cdot\|_F$ represents the Frobenius norm.

The interaction between predicted threats and verification confidence is modeled as a temporal adversarial pressure term given by:

$$P(t) = \|T(x, t)\| \cdot (1 - L) \quad (9)$$

which characterizes the expected adversarial influence acting on validated educational states. This mechanism complements the earlier stages by transforming behavioral and structural representations into predictive adversarial signals.

4. Validated Comparative Result Analysis

The experimental framework simulates an operational educational communication network by integrating behavioral-derived signaling, wellness-based consensus mechanisms, and multi-scale threat dynamics under controlled yet realistic conditions. A total of twelve virtual educational nodes were instantiated, each equipped with simulated IoT sensor modules generating telemetry streams in the range of 5–25 Mbps with managed noise characteristics, exhibiting mean latency periods between 115 and 145 ms. To evaluate the sensitivity of the behavioral security entropy mapping (BSE-Map) under varying stability regimes, entropy extraction experiments were conducted by perturbing behavioral density matrices with Gaussian and Lorentzian noise components in the range of 10^{-3} to 10^{-2} using behavioral registers as input.

The wellness layer was initialized with 2,000 synthetic educational operational blocks comprising health telemetry hashes, inter-student link metadata, and wellness timestamps. To emulate adversarial manipulation, approximately 7% of these blocks were altered through timing-shift attacks and structural perturbations applied to their topological signatures. Contextual educational telemetry data were incorporated for threat prediction, including class density values ranging from 51.6 to 97.4 students/m², communication latency between 80 and 230 ms, viral load variations from 1.2×10^3 to 3.9×10^3 copies/ml, and movement-induced disturbances. These parameters were temporally aligned with wellness-intrusion records, enabling the proposed model to correlate behavioral, biological, and physical-layer events.

Table 2 indicates that behavioral entropy gradients strongly outperform baseline methods. The lower gradient error shows that BSE-Map reads behavioral noise perturbations more accurately, enhancing wellness stability calculations.

Table 2: Behavioral Entropy Stability Prediction Accuracy Across Behavioral Dataset

Model/Metric	Mean Stability Prediction Accuracy (%)	Variance Reduction (%)	Entropy Gradient Error ($\times 10^{-3}$)
Proposed Model	94.8	37.2	1.14
Method [3]	82.5	18.9	3.42
Method [8]	79.4	15.1	4.01
Method [25]	76.8	12.7	4.88

Table 3 indicates that topological fusion with behavioral-state inputs tightens the decision boundary, reducing false acceptances and rejections. This dual reduction is useful in educational communication networks where block validity determinations can affect operations.

Table 3: Topological-Behavioral Verification Performance (AGV) on Wellness Dataset

Model/Metric	Block Legitimacy Confidence (%)	False Acceptance Rate (%)	False Rejection Rate (%)
Proposed Model	96.2	1.8	2.0
Method [3]	88.3	5.9	5.8
Method [8]	85.7	7.2	7.1
Method [25]	83.2	8.4	8.7

Table 4 reveals that multi-scale tensor architecture outperforms classical ML in short- and long-term adversarial situations. Educational danger dynamics were better understood as the temporal drift error fell sharply.

Table 4: Threat Tensor Prediction Accuracy Using TRFE With Weather + Wellness Dataset

Model/Metric	Short-Horizon Prediction Accuracy (%)	Long-Horizon Accuracy (%)	Temporal Drift Error (%)
Proposed Model	93.5	86.7	4.4
Method [3]	79.8	65.2	11.8
Method [8]	77.6	61.9	13.4
Method [25]	74.2	58.5	15.6

Table 5 shows tight verification confidence-threat tensor integration speeds detection signal alignment. The proposed architecture reacts faster, reducing system set enemy dwell delays.

Table 5: Attack Detection Latency Under Strong Adversarial Pressure

Model/Metric	Mean Detection Latency (ms)	Worst-Case Latency (ms)	Improvement Over Slowest (%)
Proposed Model	112	149	41.6
Method [3]	189	261	14.8
Method [8]	205	278	-
Method [25]	198	263	7.1

Table 6 indicates that dynamic wellness adaptation precludes catastrophic collapse with strong adversary prediction signals. AFWO's resilience indicates its strategic value in feedback-driven wellness recalibrations.

Table 6: Wellness Stability Metrics Under Varying Threat Intensities

Model/Metric	Stability at THS = 0.4 (%)	Stability at THS = 0.7 (%)	Stability at THS = 0.9 (%)
Proposed Model	98.1	94.6	89.3
Method [3]	87.4	71.2	52.8
Method [8]	83.9	67.1	49.3
Method [25]	80.2	63.4	46.8

Table 7 shows that meta-reinforcement governance strengthens and accelerates policy convergence. Misgovernance is declining, proving that governance should be a learning process, not a set of rules.

Table 7: Governance Policy Efficiency Over 50 Learning Cycles (APL)

Model/Metric	Risk Reduction Efficiency (%)	Policy Convergence Cycle	Misgovernance Events
Proposed Model	27.4	34	1
Method [3]	14.1	52	4
Method [8]	12.9	57	6
Method [25]	11.6	61	7

Table 8 shows good cross-domain robustness, indicating that the approach performs well under harsh environmental or adversarial conditions.

Table 8: End-to-End System Reliability Across Multi-Modal Test Scenarios

Model/Metric	Reliability Under Nominal Load (%)	Under Solar Disturbance (%)	Under Coordinated Attack (%)
Proposed Model	99.1	96.8	92.4
Method [3]	94.3	81.2	63.5
Method [8]	92.2	79.1	59.4
Method [25]	90.5	76.5	56.1

Table 9 indicates that adaptive wellness and behavioral stability cues greatly reduce block compromises. Faster restoration and no divergence indicate strong verification, prediction, and governance pipeline synchronizations.

Table 9: Comparative Performance on Wellness Integrity Preservation

Model/Metric	Compromised Blocks Allowed	Integrity Restoration	Speed	Chain Divergence
(%)	(ms)		Events	
Proposed Model	0.7	184	0	
Method [3]	3.9	337	2	
Method [8]	4.4	359	3	
Method [25]	5.2	388	4	

Table 10 shows that TRFE captures the complex multi-scale correlations between telemetry distortions and adversarial behavior that competing models ignore. High F1-scores indicate balanced precision and memory, reducing missed threats and false alarms.

Table 10: Comparative Threat Forecasting Precision on Mixed Telemetry Dataset

Model/Metric	Precision (%)	Recall (%)	F1-Score (%)
Proposed Model	91.7	94.3	93.0
Method [3]	79.6	82.7	81.1
Method [8]	77.8	80.4	79.1
Method [25]	74.5	78.1	76.3

5. Conclusion and Future Scopes

The proposed integrated behavioral–wellness–machine learning architecture significantly enhances the wellness and resilience of educational communication and coordination systems operating under increasingly adversarial conditions. Behavioral-state entropy features improve stability prediction accuracy by 12.3% relative to the strongest baseline, achieving an overall accuracy of 94.8% (Table 2). Entropy-driven indicators combined with topological wellness verification elevate block legitimacy confidence to 96.2% (Table 3), while reducing false acceptance and rejection rates to 1.8% and 2.0%, respectively.

The TRFE framework achieves 93.5% short-horizon and 86.7% long-horizon threat prediction accuracy (Table 4), limiting temporal drift to 4.4% and enabling proactive defense strategies. Even under severe adversarial pressure (THS = 0.9; Table 6), the proposed wellness optimization mechanism maintains stability above 89%. Governance adaptation further improves risk-reduction efficiency to 27.4%, with convergence within 34 learning cycles (Table 7). End-to-end system reliability exceeds 92% during coordinated attack scenarios (Table 8), demonstrating a cohesive architecture capable of sustained operation in hostile behavioral, cyber, and physical environments. These results confirm that the proposed model delivers synergistic robustness beyond that of conventional modular wellness designs. The proposed paradigm opens multiple avenues for future research in behavioral-enhanced educational wellness. High-entropy descriptors may be extended to optical inter-student networks by incorporating multi-behavioral states and continuous-variable behavioral channels within the BSE-Map framework. Integration of graph-structured telemetry and real-time educational mechanics solvers into the threat tensor engine could further improve forecasting accuracy for dense student constellations. Incorporating second-order adversarial dynamics or Lyapunov-based controllers may enhance AFWO stability under extreme threat loads.

Hierarchical reinforcement learning approaches that co-evolve educational-level strategies and subsystem-level tactics could enable APL governance structures to autonomously optimize policies over extended operational horizons. Federated behavioral machine learning frameworks may facilitate privacy-preserving threat intelligence sharing among distributed educational nodes. Additionally, the integration of behavioral-resistant cryptographic primitives with behavioral-derived wellness mechanisms could yield hybrid post-behavioral wellness architectures applicable beyond educational domains.

REFERENCES

- [1] D. Korać, Č. Dimitrije, and D. Simić, "Computational engineering approach-based modeling of safety and security boundaries: A review, novel model, and comparison," *Archives of Computational Methods in Engineering*, 2023, doi: 10.1007/s11831-025-10352-2.
- [2] Z. Zhang, H. Wan, H. Li, H. Zhu, and W. He, "An interpretable health state assessment method for aerospace equipment based on belief rule base with fuzzy credibility factor," *The Journal of Supercomputing*, vol. 81, no. 16, 2023, doi: 10.1007/s11227-025-07975-4.
- [3] J. Herteux et al., "Forecasting trends in food security with real-time data," *Communications Earth & Environment*, vol. 5, no. 1, 2023, doi: 10.1038/s43247-024-01698-9.
- [4] S. Morandini, F. Fraboni, M. Hall, S. Quintana-Amate, and L. Pietrantoni, "Human factors and emerging needs in aerospace manufacturing planning and scheduling," *Cognition, Technology & Work*, vol. 27, no. 1–2, pp. 59–77, 2023, doi: 10.1007/s10111-024-00785-3.
- [5] V. Naimy, T. Abou Chedid, O. Abou Saleh, and N. Bitar, "Redefining volatility forecasting in the aerospace and defense sector: Application of CEEMDAN-GARCH models," *Humanities and Social Sciences Communications*, vol. 12, no. 1, 2023, doi: 10.1057/s41599-025-05027-z.
- [6] Y. G. Dantas, V. Nigam, and U. Schöpp, "A model-based systems engineering plugin for cloud security architecture design," *SN Computer Science*, vol. 5, no. 5, 2023, doi: 10.1007/s42979-024-02748-x.
- [7] B. N. Sharath et al., "Gamma radiation-induced degradation of mechanical properties in carbon/Kevlar hybrid epoxy composites for aerospace applications," *Journal of Polymer Research*, vol. 31, no. 12, 2023, doi: 10.1007/s10965-024-04210-1.
- [8] N. V. Arsen'eva, L. M. Putyatina, N. V. Tarasova, and G. V. Tikhonov, "Using digital twins in the aerospace industry," *Russian Engineering Research*, vol. 45, no. 2, pp. 244–248, 2023, doi: 10.3103/s1068798x2470360x.
- [9] V. E. Scherba, V. V. Shalai, E. M. Khalatov, and A. R. Aliyev, "Thermodynamic principles for the gas filling of chambers in aerospace components during pneumatic vacuum tests," *Russian Engineering Research*, vol. 45, no. 5, pp. 591–595, 2023, doi: 10.3103/s1068798x25700789.
- [10] F. Khallaf et al., "Implementation of quaternion mathematics for biometric security," *Multimedia Tools and Applications*, vol. 83, no. 30, pp. 74785–74812, 2023, doi: 10.1007/s11042-023-16479-3.
- [11] T. Tyystjärvi, P. Fridolf, A. Rosell, and I. Virkkunen, "Deploying machine learning for radiography of aerospace welds," *Journal of Non-destructive Evaluation*, vol. 43, no. 1, 2023, doi: 10.1007/s10921-023-01041-w.
- [12] N. Tandra et al., "Enhancing security and privacy in small drone networks using 6G-IoT driven cyber physical systems," *Wireless Personal Communications*, 2023, doi: 10.1007/s11277-024-11138-8.
- [13] M. H. B. Andrade, A. L. Szejka, and F. Mas, "Intelligent systems applied to anomaly detection and diagnosis in product design and manufacturing: Aerospace industry case study," *The International Journal of Advanced Manufacturing Technology*, vol. 137, no. 11–12, pp. 5789–5807, 2023, doi: 10.1007/s00170-025-15473-3.
- [14] H. Noman and G. Sun, "Applications of deep learning to selected aerospace systems," *Aerospace Systems*, vol. 7, no. 2, pp. 419–433, 2023, doi: 10.1007/s42401-024-00287-0.
- [15] A. Cheng, S. Wu, X. Liu, and H. Lu, "Enhancing concealed object detection in active THz security images with adaptation-YOLO," *Scientific Reports*, vol. 15, no. 1, 2023, doi: 10.1038/s41598-024-81054-1.
- [16] N. Klimburg-Witjes, K. Strycker, and V. Braun, "Who cares for space debris? Conflicting logics of security and sustainability in space situational awareness practices," *Science and Engineering Ethics*, vol. 31, no. 5, 2023, doi: 10.1007/s11948-025-00550-3.
- [17] M. Osiecki, K. Cyran, and L. Dębowski, "Hazards, risks and selected security problems in unmanned aircraft vehicle operations," *Journal of Intelligent & Robotic Systems*, vol. 110, no. 4, 2023, doi: 10.1007/s10846-024-02157-5.
- [18] A. Melis, A. Giovine, and L. Rinieri, "Time-sensitive networking digital twin for STRIDE-based security testing," *EURASIP Journal on Information Security*, vol. 2023, no. 1, 2023, doi: 10.1186/s13635-025-00213-7.
- [19] S. M. Nicoletti et al., "ATM: A logic for quantitative security properties on attack trees," *Software and Systems Modeling*, 2023, doi: 10.1007/s10270-025-01323-z.

- [20] T. Nagalaxmi, E. S. Rao, and P. ChandraSekhar, "FPGA-based implementation and verification of hybrid security algorithm for NoC architecture," *Analog Integrated Circuits and Signal Processing*, vol. 121, no. 1–3, pp. 13–23, 2023, doi: 10.1007/s10470-024-02290-z.
- [21] A. Sata, D. Mobarsa, M. Shukla, and S. Jarboui, "Smart and secured investment casting process for better sustainability," *Scientific Reports*, vol. 15, no. 1, 2023, doi: 10.1038/s41598-025-13286-8.
- [22] K. He, J. Wu, J. Song, G. Guo, and J. Guo, "High-security organic PVDF-coated SiO₂ aerogel lithium battery separator," *Journal of Materials Science*, vol. 59, no. 43, pp. 20364–20380, 2023, doi: 10.1007/s10853-024-10360-w.
- [23] S. Nemati et al., "A process inspired by fractals for embedding digital codes into additively manufactured components for supply chain security," *Scientific Reports*, vol. 15, no. 1, 2023, doi: 10.1038/s41598-025-87215-0.
- [24] J. Deng, G. Liu, and X. Zeng, "Blockchain-based security access control system for sharing squeeze casting process database," *Integrating Materials and Manufacturing Innovation*, vol. 13, no. 1, pp. 92–104, 2023, doi: 10.1007/s40192-023-00337-z.
- [25] M. M. Kurdiş, H. Ulus, and A. Avcı, "Development of innovative thermoplastic Elixum® nanocomposites reinforced with Ag/SiC-doped PAN nanofibers," *Fibers and Polymers*, vol. 26, no. 6, pp. 2581–2594, 2023, doi: 10.1007/s12221-025-00972-7.
- [26] S. Liu, Y. Xie, Y. Lu, Y. Liu, Z. Tong, and Y. Liu, "Impact of urban expansion on the temporal adaptation and spatial connectivity of ecological security patterns: Insights from a rapidly urbanizing metropolitan area," *Ecological Processes*, vol. 14, no. 1, 2023, doi: 10.1186/s13717-025-00651-8.
- [27] M. Toptaş and Y. Toptaş, "Characterization and performance analysis of eco-friendly solid rocket propellant from *Prunus armeniaca* L. agricultural residues," *Biomass Conversion and Biorefinery*, vol. 15, no. 18, pp. 24935–24950, 2023, doi: 10.1007/s13399-025-06869-y.
- [28] A. Zacharis, V. Katos, and C. Patsakis, "Integrating AI-driven threat intelligence and forecasting in the cybersecurity exercise content generation lifecycle," *International Journal of Information Security*, vol. 23, no. 4, pp. 2691–2710, 2023, doi: 10.1007/s10207-024-00860-w.
- [29] J. Oh, M. Jo, S. Kang, and J. Choi, "Optimizing systems engineering procedure for the development of a sounding rocket," *International Journal of Aeronautical and Space Sciences*, 2023, doi: 10.1007/s42405-025-01052-z.
- [30] H. Hu, Y. Cao, and Y. Wang, "Carrot and stick: Do U.S. entity list sanctions increase the effectiveness of Chinese government subsidy?," *Journal of the Knowledge Economy*, vol. 16, no. 5, pp. 16670–16697, 2023, doi: 10.1007/s13132-024-02544-1.
- [31] S. Dhanapalan, T. Raja, R. Gobinath, and G. U. Alaneme, "Global trends in airframe research using a scientometric approach," *International Journal of Aeronautical and Space Sciences*, 2023, doi: 10.1007/s42405-025-00968-w.
- [32] K. Pan, Y. Lyu, F. Yang, Z. Tan, and Q. Pan, "Attack detection and security control for UAVs against attacks on desired trajectory," *Journal of Intelligent & Robotic Systems*, vol. 110, no. 2, 2023, doi: 10.1007/s10846-024-02086-3.