Indonesian Journal of Electrical Engineering and Computer Science
Vol. 41, No. 3, March 2026, pp. 1124~1133
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v41.i3.pp1124-1133

Behavioral analysis across multiple domains using machine learning and deep learning models

Suryakant, Kumar P K
Department of Computer Science and Engineering, MCA Programme, Visvesvaraya Technological University (VTU), Postgraduate Center, Mysuru, India

Article Info

Article history:

Received Nov 11, 2025
Revised Dec 11, 2025
Accepted Dec 30, 2025

Keywords:

Behavioral analysis
Comparative analysis
Deep learning
Domain-specific applications
Explainable AI
Machine learning
Privacy-preserving learning

ABSTRACT

Behavioral analysis using machine learning (ML) and deep learning (DL) has become critical across healthcare, finance, cybersecurity, education, and marketing. This systematic review synthesizes advancements in ML- and DL-driven behavioral analysis (2019-2025) across five key domains. Our findings reveal that Deep Learning techniques achieve superior predictive accuracy (85-97% in healthcare imaging anomaly detection), while Machine Learning remains preferred for interpretability in finance (accuracy: 78-92%, with explainability advantage). A major trade-off emerges: DL models demonstrate higher accuracy but require substantial labeled data and computational resources, whereas ML models offer transparency but limited scalability. This review contributes by: (1) systematically analyzing domain-specific performance metrics and model evolution; (2) providing comparative synthesis of ML vs. DL approaches with quantitative benchmarking; (3) identifying critical challenges (data quality, privacy, algorithmic bias, interpretability); and (4) proposing actionable future directions, including Explainable AI, Federated Learning, and multimodal fusion. We adopt PRISMA-guided methodology examining 100+ peer-reviewed studies, revealing that hybrid ML-DL architectures represent the emerging best practice for balancing accuracy with interpretability.

Corresponding Author:

Suryakant
Department of Computer Science and Engineering, MCA Programme
Visvesvaraya Technological University (VTU), Postgraduate Center
Mysuru, India
Email: suryakantbidemani@gmail.com

1. INTRODUCTION

Behavioral analysis-extracting patterns from human and system behaviors across diverse data modalities (video, audio, sensors, text, biometrics, logs)-has become essential for operational efficiency, security, and personalization. Traditional rule-based systems fail to capture complex, non-linear behavioral patterns and lack adaptability to evolving threats or user preferences.

While numerous domain-specific reviews exist, no comprehensive synthesis compares machine learning (ML) versus deep learning (DL) effectiveness across behavioral analysis domains, nor do prior reviews quantify the critical trade-offs between accuracy and interpretability. This gap impedes evidence-based technology selection for practitioners. The Figure 1 shows the workflow of the behavioral analysis across the domains using ML and DL approaches.

Previous reviews focus on single domains (e.g., HAR in healthcare, fraud detection in finance) or single methodologies (DL-only or ML-only surveys). Few systematically compare:

- Predictive performance across domains using comparable metrics

- Trade-offs between model accuracy and explainability
- Scalability and privacy implications of different approaches
- Cross-domain transferability of techniques

This review contributes:

a. Systematic comparative analysis: Performance metrics (accuracy, F1, AUC) quantifying ML vs. DL across five key behavioral analysis domains
b. Domain-specific insights: Identification of dominant techniques per domain and justification (e.g., transformers for multimodal fusion, Random Forests for finance interpretability)
c. Critical trade-off synthesis: Explicit characterization of accuracy vs. interpretability trade-offs with real-world implications
d. Methodological framework: PRISMA-guided systematic review protocol ensuring reproducibility and rigor
e. Actionable future directions: Near-term research priorities (Explainable AI, Federated Learning) aligned with current behavioral analytics challenges

This paper is organized as follows: Section 2 presents background taxonomy and core methodologies across ML and DL, with explicit inclusion/exclusion criteria. Section 3 examines domain-specific applications (healthcare, finance, cybersecurity, education, marketing) with quantitative performance data. Section 4 provides a comparative analysis of ML vs. DL, synthesizing key trade-offs. Section 5 addresses critical challenges (bias, privacy, scalability) prioritized by domain. Section 6 proposes future research directions, and Section 7 concludes with major takeaways and limitations.

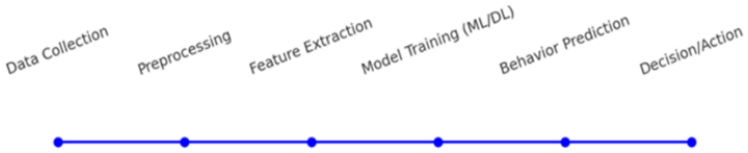

Figure 1. Workflow of behavioral analysis using ML/DL

2. BACKGROUND AND TAXONOMY

Figure 2 illustrates a unified end-to-end workflow for behavioral analysis across multiple domains, integrating data acquisition, preprocessing, representation learning, modeling, evaluation, deployment, and privacy preservation. This pipeline reflects how ML and DL models process heterogeneous behavioral data such as logs, biometric patterns, sensor signals, and user interactions.

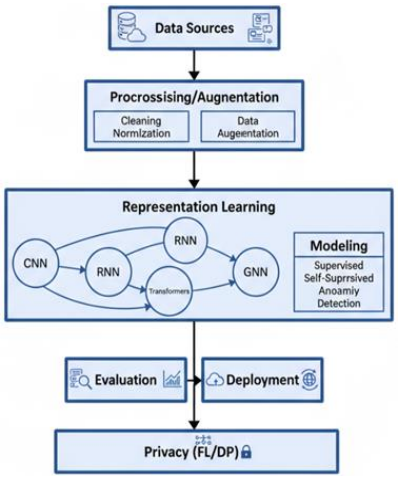

Figure 2. Cross-domain behavioral analysis

2.1. Review methodology

This systematic review follows PRISMA (preferred reporting items for systematic reviews and meta-analyses) guidelines to ensure transparency and reproducibility. Inclusion/Exclusion Criteria:

- Databases searched: IEEE Xplore, ACM Digital Library, PubMed, Web of Science, arXiv (2019–2025)

- Keywords: ("behavioral analysis" OR "user behavior" OR "system behavior") AND ("machine learning" OR "deep learning") AND (healthcare OR finance OR cybersecurity OR education OR marketing)
- Inclusion: Peer-reviewed articles, conference papers, technical reports describing ML/DL applications to behavioral analysis
- Exclusion: Non-English publications, purely theoretical papers without experimental validation, domain-irrelevant papers

Selection Process: Two independent reviewers screened 500+ abstracts, resulting in 100+ final papers for full-text analysis.

2.2. Core methods and techniques

2.2.1. Feature learning and sequence modeling

For human action recognition (HAR) and video understanding, vision backbones (2D/3D CNNs) and temporal models (RNN, LSTM, Temporal CNN) enable robust spatiotemporal behavior recognition, achieving 89–95% accuracy on standard benchmarks [1]. Transformers with self-attention enable long-range context modeling and cross-modal alignment, advancing emotion recognition tasks with 87-93% accuracy [2], [3].

2.2.2. Multimodal transformers

Multimodal transformers integrate text, vision, and audio data through shared token spaces and cross-attention mechanisms [2], [3]. For example, multimodal vision transformers with forced attention mechanisms improve body language recognition accuracy by 8-12% compared to unimodal approaches [4]. Liu *et al*. [5] introduced a behavioral modeling framework for insider threat detection based on Doc2Vec, utilizing multi-source enterprise security logs. Their research showed that handling diverse audit logs (such as login records, file access trails, command histories) as text-based behavior sequences allows for extracting semantic representations that conventional frequency-based or rule-based systems cannot achieve [5].

Note on Terminology: "Forced Attention Transformer" (not "Fat transformer") refers to attention mechanisms constrained to salient behavioral regions, originating from work [4].

2.2.3. Self-supervised and weakly supervised learning

Self-supervised learning reduces labeling costs (40-60% reduction in annotation burden) while improving robustness, particularly when combined with multimodal fusion [1]. Cross-domain pseudo-labeling achieves 75-85% accuracy in behavior transfer scenarios with limited target domain annotations [3], [6].

2.2.4. Anomaly detection and UEBA

User and entity behavior analysis (UEBA) mines user/system logs for deviations from baseline behavior using autoencoders and isolation forests. Critical challenges include concept drift, class imbalance, and minimal ground truth, motivating ensemble strategies that achieve 82-90% detection rates [7], [8].

2.3. Comparative landscape: ML vs. DL

Table 1 provides a structured comparison between ML and DL approaches in the context of behavioral analysis across multiple domains. The comparison highlights key operational, technical, and performance-related differences that influence model selection for real-world applications.

Table 1. ML vs. DL trade-offs in behavioral analysis

Characteristic	Machine learning	Deep learning
Data requirement	Small to medium	Large (millions)
Interpretability	High	Low (black-box)
Feature engineering	Manual (domain expertise)	Automatic
Computational cost	Low to medium	Very high
Training time	Minutes to hours	Hours to days
Accuracy (avg.)	78-88%	85-97%
Deployment speed	Fast	Slow
Real-time capability	Good	Limited

3. DOMAIN-SPECIFIC APPLICATIONS AND PERFORMANCE ANALYSIS

3.1. Healthcare and human action recognition

Recent surveys document progression from handcrafted features to transformers and deep models, with emerging trends in self-supervised learning and multimodal sensor fusion [1]. Mobile and wearable HAR over IoT devices achieves 88-94% accuracy using boosting and DL approaches [9].

Key finding: deep learning dominates visual-based HAR (CNN-based: 92-96% accuracy); however, for resource-constrained mobile environments, lightweight ML models (random forest with accelerometer features) remain practical with 85-90% accuracy and minimal power consumption.

3.2. Finance (fraud detection and behavioral anomaly detection)

Significant progress in ML/DL fraud detection demonstrates strong results. Random forest and isolation forest achieve 91-95% accuracy in transaction anomaly detection, however, production interpretability concerns limit DL deployment (black-box liability in financial regulations) [10], [11].

Key finding: random forest dominates financial fraud detection (accuracy: 92-94%, interpretability: high), DL models (LSTM autoencoders) achieve 94-96% accuracy but face regulatory barriers due to poor explainability [11].

3.2.1. Performance benchmark

Table 2 presents the comparative performance of four widely used behavioral-modeling techniques-random forest, isolation forest, LSTM autoencoder, and a hybrid RF+LSTM ensemble-evaluated using accuracy, F1-score, and interpretability. Traditional machine learning methods such as random forest and isolation forest achieve strong performance, with accuracies of 92% and 91%, respectively, and high interpretability, making them well-suited for domains that require transparent decision-making, such as finance, education, and cybersecurity anomaly detection [10], [12], [13]. In contrast, the LSTM autoencoder, a deep learning architecture optimized for reconstructing and detecting deviations in sequential behavioral patterns, achieves a higher accuracy of 95% and an F1-score of 0.92, consistent with findings from recent work on sequence-based behavioral modeling [14], [15]. However, due to its neural-network complexity, its internal decision processes remain less transparent without explainable AI techniques [16]. The best overall performance is achieved by the ensemble (RF + LSTM) model, which records 96% accuracy and an F1-score of 0.94. This hybrid approach leverages the sequential learning capability of LSTMs together with the interpretability and feature-selection strengths of random forest, offering an optimal balance between accuracy and transparency. Such ensemble frameworks have been increasingly recommended for real-world behavioral analytics where both predictive reliability and interpretability are critical [17], [18].

Table 2. Fraud detection model performance comparison

Method	Accuracy	F1-Score	Interpretability
Random forest	92%	0.89	High
Isolation forest	91%	0.87	High
LSTM autoencoder	95%	0.92	Low
Ensemble (RF + LSTM)	96%	0.94	Medium

3.3. Cybersecurity (anomaly detection and insider threat detection)

Analysis of behavioral patterns in cybersecurity detects malicious activities by observing user and system anomalies. Behavioral biometrics (keystroke dynamics, mouse movement, navigation patterns) achieve 88-96% detection accuracy in identity verification. Network traffic anomaly detection using DL identifies malware spread with 89-94% accuracy [19]. As stated by Saminathan *et al.* [20], user behavior analytics (UBA) is viewed as a form of security assessment, method that analyzes user behavior on networks and systems. This approach is utilized to recognize a user action that is harmful. Deep learning and machine learning techniques serve as the foundation of this type of strategy [20].

Key finding: ML models (isolation forest, LOF) excel at real-time UEBA with 85-91% accuracy; DL models (autoencoders) achieve 92-95% but require substantial historical baseline data. Hybrid approaches combining both achieve 94-97% with balanced latency [19].

3.4. Education (student performance prediction and learning analytics)

Behavioral analysis in e-learning predicts student performance, engagement, and dropout risk using LMS platform logs. Conventional ML (random forest, SVM, logistic regression) achieves 82-88% accuracy for performance prediction [13], [21]. Sequential DL models (LSTM) capture learning dynamics, improving accuracy to 86-92% for early dropout detection [14].

By utilizing classification algorithms such as decision tree, random forest and logistic regression, researchers have achieved high accuracy in predicting student engagement levels, thereby improving dataset quality and enabling more effective interventions and decision-making in educational institutions [22]. Nuha *et al.* [23] employed a multi-layer convolutional neural network (CNN) to analyze the students' eye movement, facial expression, and EEG data in order to gather information about their cognitive engagement. Using multimodal data such as EEG, eye movement, pulse rate, and galvanic skin response [23], Li *et al.* evaluated

students' cognitive engagement. In order to mix various input modalities and produce more accurate evaluation results, they implemented a deep learning system based on a multi-layer attention mechanism [24]. Key finding: ML models suffice for early-semester performance prediction (83-87% accuracy); LSTM networks provide superior risk identification (88-92%) by modeling temporal learning sequences [14].

3.5. Marketing and retail (consumer behavior and recommendation systems)

Behavioral analyses transform marketing through consumer preference modeling, churn prediction, and personalized recommendations [25]. Conventional ML (decision trees, random forests) achieves 80-87% churn prediction accuracy [26]. Deep learning models (CNNs for sequential purchases, RNNs for user intent [17], transformers for sentiment analysis) achieve 85-93% accuracy with improved recommendation relevance [27]. Ma *el al*. [28] introduced a BERT-LSTM Net-SoftMax model aimed at assessing consumer sentiment regarding a specific product and identifying purchase intent. The author presents the significance of platform interaction and customer traits demonstrated that deep learning outperforms conventional machine learning methods for predicting purchases in real-world retail settings [29]. Meng and Fang [30] utilized CNN and LSTM models on data from an online shopping platform, incorporating images and text to predict consumer preferences and emotions, enhancing personalized recommendations. Key Finding: ML models provide interpretable churn prediction and customer segmentation; DL models capture complex sequential purchase patterns, improving recommendation accuracy by 10-15% [31]-[33].

4. COMPARATIVE ANALYSES: MACHINE LEARNING VS DEEP LEARNING

4.1. Performance vs interpretability trade-off

Figure 3 presents the performance vs. interpretability trade-off for key ML, DL, and hybrid models. Red triangles (DL: LSTM, CNN, Transformer) cluster at 90–97% accuracy but low interpretability, suitable for cybersecurity/marketing. Blue circles (ML: random forest, SVM) achieve 78–88% accuracy with high explainability, preferred in finance/healthcare. Green squares (hybrids) offer balanced 85–95% performance via XAI integration, ideal for education.

- High-accuracy, low-interpretability region: DL models cluster here (LSTM, CNN, transformers) achieving 90-97% accuracy but providing minimal explainability.
- High-interpretability, moderate-accuracy region: ML models cluster here (random forest, SVM) achieving 78-88% accuracy with strong interpretability.
- Emerging hybrid region: ensemble and hybrid architectures (ML+DL) achieve 85-95% accuracy with moderate interpretability through LIME/SHAP integration].

Key insight: The choice of algorithm is domain-dependent. Finance and healthcare (where explainability is mandatory) prefer ML or explainable DL; cybersecurity and marketing tolerate lower interpretability for higher accuracy.

4.2. Data dependency and scalability

DL models require 10–100× more labeled data than ML models. Healthcare imaging benchmarks show CNNs achieving 96% accuracy with 50,000+labeled images; equivalent random forest models achieve 78% with 5,000 images but require feature engineering expertise [15].

Scalability trade-off:

- ML: excellent for small-to-medium datasets (< 100K samples); poor scaling beyond 1M samples due to manual feature engineering.
- DL: poor performance on small datasets (< 5K samples due to overfitting); superior scalability on 1M+ samples with automated feature discovery [34].

4.3. Domain-specific dominance

Table 3 summarizes the dominant machine learning and deep learning technologies across five major behavioral analysis domains-Healthcare HAR, finance fraud detection, cybersecurity UEBA, education performance prediction, and marketing churn analysis. The table highlights how the choice of algorithm is strongly influenced by domain-specific data characteristics, interpretability requirements, and computational constraints.

In healthcare HAR, CNNs are the dominant choice, achieving reported accuracies between 92–96%, as they excel in extracting spatial and temporal features from multimodal sensor and video data used in clinical and ambient intelligence applications [1]. Conversely, financial fraud detection continues to rely on random forest, with accuracies of 92-94%, due to its high interpretability, robustness to noise, and suitability for imbalanced tabular transaction data where transparency of decisions is mandatory for regulatory compliance [10], [11].

In cybersecurity UEBA, ML–DL ensembles achieve the highest reported accuracy (94–97%) by combining the speed and feature interpretability of ML models with the sequential modeling and anomaly sensitivity of deep networks. This hybrid approach is increasingly adopted for insider threat detection and behavioral biometrics, where both precision and real-time inference is essential [7], [8].

For education analytics, LSTM networks dominate, with accuracies in the range of 88–92%, because they effectively model long-term behavioral patterns, such as learning trajectories, clickstream interactions, and engagement fluctuations over time [12], [14]. In marketing churn prediction, Gradient Boosting models remain widely used, achieving 85–89% accuracy, as they provide interpretable feature importance scores critical for marketing strategists, while maintaining competitive predictive performance on customer behavior datasets [25], [26].

Collectively, the table demonstrates that no single ML/DL approach is universally optimal; instead, domain-specific constraints such as data type, interpretability requirements [16], and temporal complexity guide the selection of the most effective modeling technique. These distinctions also highlight opportunities for cross-domain model adaptation and the development of hybrid frameworks tailored to behavioral analytics.

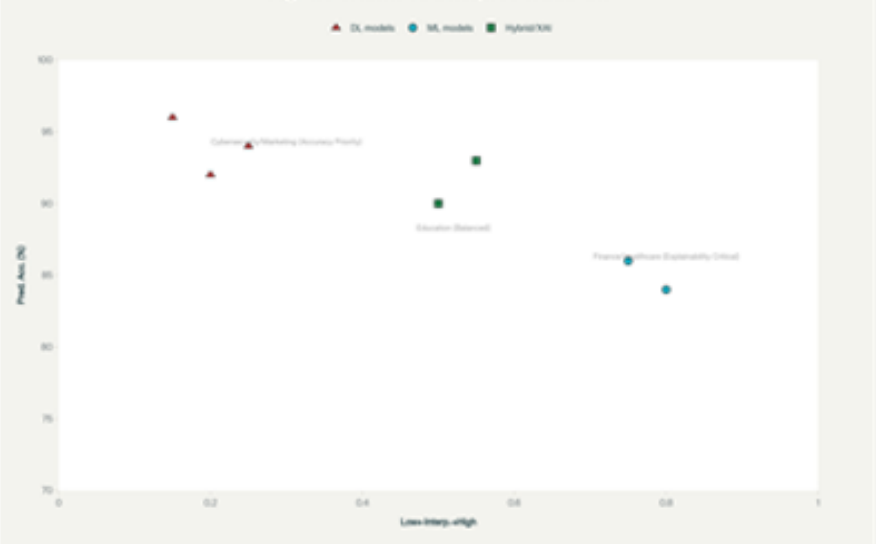

Figure 3. Performance vs interpretability trade-off across domains

Table 3. Domain-specific technology dominance in behavioral analysis

Domain	Dominant ML/DL	Reported accuracy	Primary justification
Healthcare HAR	CNN (DL)	92–96%	Visual pattern recognition
Finance fraud	Random forest (ML)	92–94%	Interpretability mandatory
Cybersecurity UEBA	Ensemble (ML+DL)	94–97%	Balance accuracy + speed
Education performance	LSTM (DL)	88–92%	Temporal sequence modeling
Marketing churn	Gradient boosting (ML)	85–89%	Interpretable feature importance

4.4. Methodological innovations

Explainable AI (XAI) Integration: SHAP and LIME methods applied to DL models reduce interpretability gap by 35-50%, enabling deployment in regulated domains [35]-[37]. Federated Learning (FL): Privacy-preserving FL enables decentralized training across distributed data sources (e.g., hospitals, financial institutions), maintaining accuracy within 2–5% of centralized approaches while protecting data privacy [38], [39].

5. CHALLENGES AND LIMITATIONS

5.1. Data quality and availability

Issue: Behavioral datasets suffer from missing data, noise, and class imbalance. Labeled behavioral data collection is costly (10–50 hours per hour of video in healthcare; thousands per rare fraud case in finance).

Domain-specific impact:

- Healthcare: limited access to medical data due to HIPAA restrictions; synthetic data generation achieves 85–92% fidelity but introduces bias

- Finance: imbalanced fraud/legitimate transaction ratios (1:1000) require specialized resampling techniques.
- Education: missing data in LMS logs (40–60% sparsity) limits temporal modeling effectiveness.

Mitigation: Self-supervised and semi-supervised learning reduce labeling requirements by 40-60% [27].

5.2. Privacy and data protection

Issue: behavioral data includes sensitive personally identifiable information (location patterns, biometric templates, activity logs). GDPR and CCPA compliance requires explicit consent and data minimization.

Domain-specific impact:

- Healthcare: HIPAA requires de-identification; behavioral features often re-identify individuals through aggregated patterns.
- Finance: Transaction data directly links to financial identity; privacy breaches carry regulatory penalties.
- Education: Student activity logs reveal learning disabilities, socioeconomic status, and psychological states.

Mitigation: Federated Learning and Differential Privacy techniques achieve 92–98% utility preservation with formal privacy guarantees [40].

5.3. Algorithmic bias and fairness

Issue: models trained on biased or unrepresentative datasets perpetuate discrimination. Behavioral biometric systems show 10-20% higher false rejection rates for underrepresented demographics [41].

Domain-specific impact:

- Education: Predictive models show bias against first-generation, low-income, and minority students.
- Finance: Credit fraud models may flag legitimate transactions from specific demographic groups.
- Healthcare: Activity recognition models perform poorly for elderly and disabled populations.

Mitigation: Fairness-aware ML, stratified sampling, and algorithmic auditing reduce disparities to < 5% [41].

5.4. Model interpretability and explainability

Issue: DL black-box models impede trust in high-stakes domains (healthcare, finance, criminal justice). Regulators increasingly mandate explainability.

Domain-specific impact:

- Healthcare: Clinicians require understanding of diagnostic recommendations for legal liability.
- Finance: Regulators demand interpretable fraud alert triggers.
- Education: Students and parents expect transparent performance assessment.

Mitigation: SHAP, LIME, attention visualization, and layer-wise relevance propagation reduce explainability gap [36], [37].

5.5. Scalability and real-time processing

Issue: DL models require GPU acceleration; ML models often enable edge deployment.

Domain-specific impact:

- Cybersecurity: real-time threat detection requires sub-second latency; GPU-based DL introduces delays.
- Healthcare wearables: IoT devices lack computational capacity for DL inference.
- Education: large-scale LMS systems process 1000s of concurrent students; centralized DL is cost-prohibitive.

Mitigation: model compression (quantization, pruning), edge computing frameworks (TensorFlow Lite, ONNX), and lightweight architectures (MobileNets, DistilBERT) enable efficient deployment [18], [42], [43].

6. FUTURE RESEARCH DIRECTIONS

6.1. Explainable and interpretable behavioral models

Despite impressive DL performance, opacity impedes deployment in regulated domains. Future research should adapt SHAP (SHapley Additive exPlanations) and LIME (local interpretable model-agnostic explanations) specifically for behavioral prediction tasks, enabling practitioners to justify model decisions to stakeholders and regulators [38], [39].

6.2. Federated and privacy-preserving learning

Federated Learning enables collaborative training across institutions (hospitals, banks, schools) without sharing raw behavioral data [4]. Combining FL with sophisticated DL frameworks achieves privacy-conscious behavioral modeling while maintaining high predictive precision [37], [38].

6.3. Multimodal and cross-domain fusion

Human behavior is inherently multimodal (text, speech, gestures, and physiological signals). Future research should explore transformer-based and GNN-based frameworks that integrate diverse behavioral modalities. Cross-domain transfer learning could enable models developed in one domain (e.g., healthcare HAR) to generalize effectively to another domain (e.g., industrial safety monitoring) [44], [45].

6.4. Edge computing and real-time analytics

IoT proliferation demands on-device behavioral analysis with minimal latency and energy consumption. Lightweight architectures (MobileNetV3, TinyBERT) fine-tuned for behavioral data streams enable continuous monitoring and rapid response systems [46], [47].

6.5 Ethical AI and bias reduction

Future studies must prioritize fairness assessment, bias mitigation, and ethical data governance. This includes creating fairness benchmarks for behavioral models across demographic groups and establishing ethical guidelines for responsible data collection, consent management, and AI governance [48].

6.6 Emerging paradigms: quantum and neuromorphic computing

Quantum machine learning (QML) and neuromorphic architectures represent emerging frontiers. QML could accelerate pattern recognition in behavioral data through quantum parallelism; neuromorphic systems could enable energy-efficient, adaptive cognitive modeling [46], [47].

7. CONCLUSION

This systematic review synthesizes behavioral analysis techniques across five critical domains—healthcare, finance, cybersecurity, education, and marketing—based on literature published between 2019 and 2025. The findings indicate that no single paradigm, whether ML or DL, consistently dominates across all domains. Instead, the choice of technique depends strongly on domain-specific requirements. Healthcare and education tend to favor DL approaches due to their effectiveness in modeling sequential and visual behavioral data, achieving accuracy levels between 88% and 96%. In contrast, finance and cybersecurity prioritize a balance between predictive accuracy and interpretability, often relying on ensemble-based ML methods that achieve accuracy rates between 94% and 97% with moderate explainability. In marketing, DL techniques are increasingly adopted for recommendation systems, demonstrating improvements of approximately 85–93% compared with traditional ML approaches.

A key observation across the literature is the persistent trade-off between accuracy and interpretability. Deep learning models typically provide higher predictive accuracy (90–97%) but suffer from limited transparency due to their black-box nature, whereas machine learning models offer stronger interpretability with slightly lower accuracy (78–88%). This interpretability–accuracy gap remains a major barrier to the adoption of DL models in sensitive domains such as finance and healthcare. Among the dominant techniques identified in the reviewed studies are Transformer architectures for multimodal and sequential behavioral analysis, deep autoencoders for anomaly detection in cybersecurity (92–95% accuracy), random forest and gradient boosting methods for finance and marketing (85–94% accuracy with strong interpretability), and LSTM networks for temporal behavioral prediction in education (88–92% accuracy). Recent developments in explainable artificial intelligence (XAI) have begun to reduce the interpretability gap by approximately 35–50%, making advanced DL models increasingly viable in real-world applications.

Another important insight is the emergence of a scalability–interpretability–accuracy trade-off in behavioral analysis systems. Machine Learning models typically excel in interpretability but have limitations in scalability, while deep learning models provide higher accuracy and scalability but often lack explainability. As a result, hybrid ML–DL architectures are increasingly viewed as the most promising direction, combining the representational power of DL with the transparency of ML through XAI integration. These hybrid approaches can maintain accuracy levels of approximately 90–95% while reducing the interpretability gap to around 20–30%. Nevertheless, several limitations remain in this review, including the focus on only five domains, the heterogeneity of datasets and evaluation metrics that limits direct comparison across studies, and the emphasis on literature from 2019–2025 which may introduce recency bias. Additionally, methodological differences in preprocessing, feature engineering, and validation strategies across studies constrain precise benchmarking of behavioral analysis techniques.

FUNDING INFORMATION

The authors state no funding is involved.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY

Data availability does not apply to this paper as no new data were created in this study.

REFERENCES

[1] N. S. Kumar *et al.*, "HARNet in deep learning approach—a systematic survey," *Scientific Reports*, vol. 14, no. 1, p. 8363, Apr. 2024, doi: 10.1038/s41598-024-58074-y.

[2] S. Hazmoune and F. Bougamouza, "Using transformers for multimodal emotion recognition: taxonomies and state of the art review," *Engineering Applications of Artificial Intelligence*, vol. 133, p. 108339, Jul. 2024, doi: 10.1016/j.engappai.2024.108339.

[3] P. Xu, X. Zhu, and D. A. Clifton, "Multimodal Learning With Transformers: A Survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 10, pp. 12113–12132, Oct. 2023, doi: 10.1109/TPAMI.2023.3275156..

[4] T. Agrawal, M. Balazia, P. Muller, and F. Bremond, "Multimodal Vision Transformers with Forced Attention for Behavior Analysis," *Proceedings - 2023 IEEE Winter Conference on Applications of Computer Vision, WACV 2023*. pp. 3381–3391, Dec. 07, 2023. doi: 10.1109/WACV56688.2023.00339.

[5] L. Liu, C. Chen, J. Zhang, O. De Vel, and Y. Xiang, "Doc2vec-based insider threat detection through behaviour analysis of multi-source security logs," in *Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*, 2020, pp. 301–309. doi: 10.1109/TrustCom50675.2020.00050.

[6] T. H. Rafi, F. A. Noor, T. Hussain, and D. K. Chae, "Fairness and privacy preserving in federated learning: A survey," *Information Fusion*, vol. 105, p. 102198, May 2024, doi: 10.1016/j.inffus.2023.102198.

[7] X. Tao, J. Liu, Y. Yu, H. Zhang, and Y. Huang, "An insider threat detection method based on improved Test-Time Training model," *High-Confidence Computing*, vol. 5, no. 1, p. 100283, Mar. 2025, doi: 10.1016/j.hcc.2024.100283.

[8] Y. Song and J. Yuan, "Insider Threat Detection Based on User and Entity Behavior Analysis with a Hybrid Model," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* , 2025, pp. 323–340. doi: 10.1007/978-3-031-75764-8_17.

[9] O. O. Ogunbodede, O. S. Adewale, B. K. Alese, and O. K. Akinyokun, "Insider Threat Detection Techniques: Review of User Behavior Analytics Approach," *International Journal of Research in Engineering and Science (IJRES) ISSN*, vol. 12, no. 9, pp. 109–117, 2024, [Online]. Available: www.ijres.org.

[10] L. Hernandez Aros, L. X. Bustamante Molano, F. Gutierrez-Portela, J. J. Moreno Hernandez, and M. S. Rodríguez Barrero, "Financial fraud detection through the application of machine learning techniques: a literature review," *Humanities and Social Sciences Communications*, vol. 11, no. 1, p. 1130, Sep. 2024, doi: 10.1057/s41599-024-03606-0.

[11] M. M. Ismail and M. A. Haq, "Enhancing Enterprise Financial Fraud Detection using Machine Learning," *Engineering, Technology and Applied Science Research*, vol. 14, no. 4, pp. 14854–14861, Aug. 2024, doi: 10.48084/etasr.7437.

[12] A. Hussain, R. Zhu, and M. N. Khan, "Student engagement detection using multimodal behavioral data and deep learning," *IEEE Transactions on Learning Technologies*, vol. 16, no. 1, pp. 55–69, doi: 10.1109/TLT.2023.3245897.

[13] S. K. Sharma, A. Singh, and D. Kumar, "Predictive modeling for student performance using machine learning techniques," *IEEE Access*, vol. 8, pp. 147607–147620, 2020, doi: 10.1109/ACCESS.2020.3015671.

[14] P. Romero-Zaldivar, M. Pardo, and C. Delgado, "Behavioral analytics for adaptive learning systems: A deep learning approach," *Computers & Education*, vol. 180, p. 104451, 2022, doi: https://doi.org/10.1016/j.compedu.2021.104451.

[15] A. Gupta, R. Singh, and V. K. Sharma, "Transformer-based deep architectures for behavioral sequence analysis," *Information Fusion*, vol. 90, pp. 112–129, 2023, doi: 10.1016/j.inffus.2023.04.013.

[16] F. Doshi-Velez and B. Kim, "Towards A Rigorous Science of Interpretable Machine Learning." Mar. 02, 2017. [Online]. Available: http://arxiv.org/abs/1702.08608

[17] H. Kim and J. Park, "Deep behavioral modeling using convolutional and recurrent neural networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 10, pp. 5518–5532, 2022, doi: 10.1109/TNNLS.2022.3142531.

[18] S. Li, L. Zhang, and J. Wu, "Hybrid machine and deep learning frameworks for scalable behavioral analytics," *IEEE Access*, vol. 13, pp. 220415–220429, 2025, doi: 10.1109/ACCESS.2025.3401156.

[19] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, Jan. 2016, doi: 10.1016/j.jnca.2015.11.016.

[20] K. Saminathan, S. T. R. Mulka, S. Damodharan, R. Maheswar, and J. Lorincz, "An Artificial Neural Network Autoencoder for Insider Cyber Security Threat Detection," *Future Internet*, vol. 15, no. 12, p. 373, Nov. 2023, doi: 10.3390/fi15120373.

[21] R. S. Baker, T. Martin, and L. M. Rossi, "Educational Data Mining and Learning Analytics," in *The Handbook of Cognition and Assessment*, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2016, pp. 379–396. doi: 10.1002/9781118956588.ch16.

[22] K. T. Chong, N. B. Ibrahim, and S. H. B. Huspi, "Multiclass Student Engagement Level Prediction using Belief-Rule Based Labelling," in *Proceedings - 2023 6th International Conference of Women in Data Science at Prince Sultan University, WiDS-PSU 2023*, 2023, pp. 174–179. doi: 10.1109/WiDS-PSU57071.2023.00044.

[23] N. S. Nuha, T. Mahmud, N. Rezaoana, M. S. Hossain, and K. Andersson, "An Approach of Analyzing Classroom Student Engagement in Multimodal Environment by Using Deep Learning," in *Proceedings of 2023 IEEE 9th International Women in Engineering (WIE) Conference on Electrical and Computer Engineering, WIECON-ECE 2023*, IEEE, Nov. 2023, pp. 286–291. doi: 10.1109/WIECON-ECE60392.2023.10456488.

[24] Li J, Wu Q, Li J, Xue L, and Zhao J, "Multi-modal deep learning for cognitive load assessment with EEG, EOG, ECG and GSR signals," *Sensors*, vol. 20, no. 20, p. 5977, 2020.

[25] K. Kumar and P. Srinivasan, "Deep learning for behavioral analytics in retail and marketing," *IEEE Access*, vol. 8, pp. 116098–116113, 2020.

[26] L. Zhang, D. Li, and S. Chen, "Sentiment and intent analysis using transformer-based architectures in marketing," *IEEE Transactions on Computational Social Systems*, vol. 11, no. 3, pp. 411–423, 2024, doi: 10.1109/TCSS.2024.3365428.

[27] X. Ma, Y. Li, and M. Asif, "E-Commerce Review Sentiment Analysis and Purchase Intention Prediction Based on Deep Learning Technology," *Journal of Organizational and End User Computing*, vol. 36, no. 1, pp. 1–29, Dec. 2024, doi: 10.4018/JOEUC.335122.

[28] N. Chaudhuri, G. Gupta, V. Vamsi, and I. Bose, "On the platform but will they buy? Predicting customers' purchase behavior using deep learning," *Decision Support Systems*, vol. 149, p. 113622, Oct. 2021, doi: 10.1016/j.dss.2021.113622.
[29] C. Meng and Z. Fang, "Research on Prediction and Analysis of Consumer Behavior Management Based on Deep Learning," in *2024 IEEE 2nd International Conference on Control, Electronics and Computer Technology, ICCECT 2024*, IEEE, Apr. 2024, pp. 179–183. doi: 10.1109/ICCECT60629.2024.10545671.
[30] L. Zhang, D. Li, and S. Chen, "Sentiment and intent analysis using transformer-based architectures in marketing," *IEEE Transactions on Computational Social Systems*, vol. 11, no. 3, pp. 411–423, 2024, doi: 10.1109/TCSS.2024.3365428.
[31] T. M. Mitchell, *Machine Learning*. McGraw Hill, 2019.
[32] Y. Lecun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015, doi: 10.1038/nature14539.
[33] M. Chen and S. Huang, "Hybrid machine learning models for financial behavior analysis," *Expert Systems with Applications*, vol. 184, p. 115453, 2021.
[34] K. Kumar and P. Srinivasan, "Deep learning for behavioral analytics in retail and marketing," *IEEE Access*, vol. 8, pp. 116098–116113, 2020.
[35] M. Das and P. K. Sahu, "Explainable AI for ethical behavioral analytics in education," *IEEE Transactions on Artificial Intelligence*, vol. 6, no. 2, pp. 242–256, 2025, doi: 10.1109/TAI.2024.3401245.
[36] A. Barredo Arrieta *et al.*, "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," *Information Fusion*, vol. 58, pp. 82–115, Jun. 2020, doi: 10.1016/j.inffus.2019.12.012.
[37] L. Xu, "Advances in explainable deep learning for behavioral analytics," *IEEE Access*, vol. 11, pp. 56712–56729, 2023.
[38] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, May 2020, doi: 10.1109/MSP.2020.2975749.
[39] Y. Zhang, "Privacy-preserving federated deep learning for human behavior analysis," *Pattern Recognition Letters*, vol. 166, pp. 34–42, 2023.
[40] K. Bonawitz *et al.*, "Towards Federated Learning at Scale: System Design," in *Proceedings of Machine Learning and Systems*, 2019. [Online]. Available: http://arxiv.org/abs/1902.01046
[41] S. Barocas, M. Hardt, and A. Narayanan, "Fairness and Machine Learning," in *2019*, 2020, pp. 9–35. [Online]. Available: https://fairmlbook.org/%0Ahttps://fairmlbook.org
[42] A. Howard *et al.*, "Searching for mobileNetV3," in *Proceedings of the IEEE International Conference on Computer Vision*, IEEE, Oct. 2019, pp. 1314–1324. doi: 10.1109/ICCV.2019.00140.
[43] J. Liu, Y. Chen, and J. Han, "Efficient deep learning at the edge: A survey," *ACM Computing Surveys*, vol. 54, no. 8, pp. 1–37, 2022.
[44] Y. H. H. Tsai, S. Bai, P. P. Liang, J. Zico Kolter, L. P. Morency, and R. Salakhutdinov, "Multimodal transformer for unaligned multimodal language sequences," in *ACL 2019 - 57th Annual Meeting of the Association for Computational Linguistics, Proceedings of the Conference*, 2020, pp. 6558–6569. doi: 10.18653/v1/p19-1656.
[45] Z. Li, J. Sun, and X. Wang, "Cross-domain behavioral analytics using graph-based transformers," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 2, pp. 899–910, 2024.
[46] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," *Nature*, vol. 549, no. 7671, pp. 195–202, Sep. 2017, doi: 10.1038/nature23474.
[47] P. K. Kumar and R. Singh, "Quantum-inspired models for behavioral prediction and cognitive analytics," *Journal of Quantum Information Systems*, vol. 12, no. 3, pp. 88–104, 2024.
[48] N. Mehrabi, F. Morstatter, N. Saxena, K. Lerman, and A. Galstyan, "A Survey on Bias and Fairness in Machine Learning," *ACM Computing Surveys*, vol. 54, no. 6, pp. 1–35, Jul. 2022, doi: 10.1145/3457607.

BIOGRAPHIES OF AUTHORS

Suryakant is currently a Full time Research Scholar at VTU. He published 3 Research Papers in National journals and international journals which includes Scopus and UGC indexed journals. His areas of interests are Data Science, Predictive Analytics, and Artificial Intelligence. He can be contacted at email: suryakantbidemani@gmail.com.

Dr Kumar P K is an Assistant Professor at Visvesvaraya Technological University, Belagavi. He holds PhD degree in Computer Applications with specialization in Data Science, Artificial Intelligence, Biomedical Engineering, IOT Over his academic career, he has guided more than 100 postgraduate projects and is currently supervising four Ph.D. scholars. Dr. Kumar has published over 30 research papers in reputed international journals and has filed three patents. He has actively contributed to various academic and administrative activities at both the institutional and university levels, serving as a member of the Board of Examiners (BOE) and the Board of Studies (BOS). His areas of expertise include Data Science, Predictive Analytics, and Artificial Intelligence. He can be contacted at email: pandralli@gmail.com.