GSC Biological and Pharmaceutical Sciences
eISSN: 2581-3250 CODEN (USA): GBPSC2
Cross Ref DOI: 10.30574/gscbps
Journal homepage: https://gsconlinepress.com/journals/gscbps/

(REVIEW ARTICLE)

Check for updates

Post-quantum cryptography combined with neuro-symbolic AI to safeguard sensitive psychiatric therapy models against future cyber threats

Anil Kumar *

Department of Computer Science, Maharishi International University, USA.

GSC Biological and Pharmaceutical Sciences, 2025, 33(01), 001-018

Publication history: Received on 21 August 2025; revised on 01 September 2025; accepted on 09 October 2025

Article DOI: https://doi.org/10.30574/gscbps.2025.33.1.0379

Abstract

The protection of psychiatric therapy models presents a critical challenge as healthcare increasingly adopts digital platforms for diagnosis, treatment personalization, and predictive analytics. These models contain highly sensitive patient data and therapeutic strategies that must remain secure against both current and future cyber threats. Traditional cryptographic safeguards, while effective today, are vulnerable to the emerging capabilities of quantum computing, which threatens to undermine widely deployed encryption algorithms. From a broader perspective, post-quantum cryptography offers mathematically resilient encryption schemes that are designed to withstand attacks from quantum adversaries. Simultaneously, neuro-symbolic artificial intelligence (AI) combines the adaptive power of neural networks with the interpretability and reasoning strengths of symbolic systems, enabling intelligent detection of anomalous behaviors and policy-driven access control. Narrowing the focus, this study explores a security architecture that integrates post-quantum cryptographic algorithms with neuro-symbolic AI to protect psychiatric therapy models. The proposed framework uses lattice-based cryptography for data confidentiality, signature schemes for secure model provenance, and hybrid AI systems for continuous monitoring of access and threat patterns. By embedding reasoning-driven safeguards alongside machine learning detection, the framework offers both proactive and explainable defense mechanisms. Furthermore, compliance with privacy regulations is supported through automated verification of access policies and transparent audit trails. This dual approach not only shields therapy models from quantum-era decryption risks but also ensures ethical and trustworthy deployment in sensitive mental health domains. Ultimately, safeguarding psychiatric therapy models through post-quantum and neuro-symbolic methods contributes to future-ready healthcare systems that uphold both data integrity and patient trust.

Keywords: Post-Quantum Cryptography; Neuro-Symbolic AI; Psychiatric Therapy Models; Cybersecurity In Healthcare; Quantum-Resilient Encryption; Privacy Protection

1. Introduction

1.1. Context: Rising reliance on psychiatric therapy models in digital healthcare

The last decade has witnessed a significant rise in digital healthcare platforms that integrate psychiatric therapy models to expand access, reduce stigma, and support patients outside conventional clinics [1]. This evolution is propelled by the growing burden of mental health disorders, particularly depression and anxiety, which remain leading contributors to global disability [2]. Within the United States, telepsychiatry has seen accelerated adoption following federal encouragement for telehealth reimbursement parity, ensuring that psychiatric therapy models are no longer confined to metropolitan centers [3].

* Corresponding author: Anil Kumar

Central to this expansion is the embedding of cognitive behavioral therapy and dialectical behavioral therapy into mobile applications and AI-assisted platforms. Such tools enable therapists to scale their reach while providing patients with consistent, structured interventions. The effectiveness of these digital psychiatric models has been demonstrated in randomized clinical trials, showing outcomes comparable to in-person sessions [4].

However, reliance on digital psychiatric therapy introduces challenges in safeguarding sensitive health data. As providers integrate AI-driven systems into care delivery, the imperative to address privacy, data sovereignty, and ethical use becomes pressing [2]. Figure 1 highlights growth projections of digital psychiatric therapy adoption, while Table 1 compares cost-effectiveness between conventional and digital approaches.

1.2. Cybersecurity risks in psychiatric AI systems

While digital psychiatry enhances accessibility, it creates vulnerabilities when integrated with AI-based diagnostic and therapeutic models [6]. Psychiatric data are particularly sensitive, and breaches can lead not only to financial harm but also to significant reputational damage and stigma for affected individuals [5]. Unlike conventional health systems, psychiatric AI platforms often rely on real-time monitoring, conversational agents, and emotion-detection algorithms, which introduce unique attack surfaces.

Cybercriminals increasingly target healthcare systems because of the high value of medical records on underground markets. In psychiatric contexts, adversarial machine learning attacks may corrupt therapy chatbots, causing harmful or misleading advice [6]. Furthermore, quantum computing, though not yet fully realized, poses a looming threat by undermining widely used cryptographic protocols that currently secure patient-provider communication [7].

Regulatory frameworks like HIPAA provide partial safeguards, but they were not designed for AI-driven psychiatric applications operating across cloud infrastructures and mobile devices. Without tailored protections, trust in psychiatric AI platforms risks erosion [2]. Figure 1 underscores how rising adoption increases exposure to cyber threats, and Table 1 reveals that providers allocating resources to cybersecurity report better patient retention rates. Addressing these risks is essential to sustaining digital psychiatry as a viable healthcare delivery model.

1.3. Need for future-proof solutions: post-quantum cryptography and neuro-symbolic AI

Future-proofing psychiatric AI requires integrating both advanced cryptographic protections and hybrid AI models capable of explaining their reasoning. Post-quantum cryptography, currently under evaluation by the National Institute of Standards and Technology, aims to create encryption methods resistant to quantum decryption capabilities [5]. This is particularly relevant for psychiatric data, which require long-term confidentiality given their lifelong sensitivity [3].

In parallel, neuro-symbolic AI approaches offer a pathway to combine the pattern recognition strength of neural networks with the interpretability of symbolic reasoning [6]. For psychiatric therapy models, this is crucial: patients and clinicians must trust AI recommendations, and transparent decision-making helps mitigate concerns about bias or inappropriate guidance [8]. By enhancing explainability, neuro-symbolic AI aligns with ethical imperatives in mental health care [1].

Integrating post-quantum cryptography with neuro-symbolic AI can create psychiatric systems that are simultaneously secure and interpretable. Such systems would be resilient against both near-term cyberattacks and long-term technological threats [4]. Table 1 highlights comparative frameworks for resilience planning, and Figure 1 illustrates the urgency by correlating adoption curves with projected vulnerability windows. Ensuring the U.S. leads in this integration not only secures psychiatric care but also sets a global precedent in responsible digital healthcare.

2. Background and literature review

2.1. Evolution of Cybersecurity in Healthcare Systems

Cybersecurity within healthcare has undergone a profound transformation, reflecting both advances in digital infrastructure and the growing sophistication of cyber threats. Early digitization efforts primarily centered on electronic health records (EHRs), where security measures consisted of access controls, passwords, and perimeter defenses [7]. These mechanisms were rudimentary, often assuming that threats originated externally and underestimating the risks posed by insider misuse.

The subsequent integration of interconnected devices spanning telehealth, mobile apps, and Internet of Things (IoT)-enabled medical devices exponentially expanded attack surfaces [8]. Ransomware attacks targeting hospitals

demonstrated how vulnerabilities in outdated infrastructure could paralyze entire systems, compromise patient safety, and generate severe financial losses [9]. Healthcare thus emerged as one of the most lucrative targets for cybercriminals due to its combination of sensitive data and operational urgency.

From 2010 onward, regulatory frameworks such as HIPAA in the U.S. and GDPR in Europe mandated stricter protections and reporting mechanisms, emphasizing encryption, audit trails, and access governance [10]. Yet, compliance-driven approaches often lagged behind dynamic threat evolution. The emergence of advanced persistent threats (APTs) revealed that healthcare institutions lacked resilience against long-term, stealthy attacks exploiting systemic weaknesses [11].

In recent years, artificial intelligence (AI)-driven analytics, anomaly detection, and zero-trust architectures have become increasingly prominent in health cybersecurity. These tools enable real-time monitoring and response rather than reactive recovery [12]. However, as psychiatric therapy platforms incorporate personalized algorithms and sensitive behavioral data, the consequences of breaches now extend beyond financial or clinical harm to include long-lasting psychosocial impacts on vulnerable populations [13].

This historical progression underscores a recurring theme: healthcare cybersecurity evolves reactively, chasing innovations after adoption rather than embedding protections during system design. Addressing this lag is particularly critical in psychiatric therapy systems where patient trust is central [14].

2.2. Psychiatric Therapy Models: Data Sensitivity and AI-Driven Personalization

Psychiatric therapy models have unique cybersecurity demands because of the intimate and stigmatized nature of the data they generate. Unlike general health information, psychiatric records often include narratives about trauma, substance use, or social functioning details that, if disclosed, could severely harm patients' reputations and mental well-being [15]. The high sensitivity of this data makes psychiatric platforms prime targets for identity theft, extortion, or manipulation [9].

AI-driven personalization adds both value and complexity to these therapy models. Algorithms increasingly analyze patient speech, sentiment, and behavioral patterns to recommend tailored interventions, offering scalable support in contexts of global mental health shortages [8]. While this personalization enhances therapeutic outcomes, it also multiplies the number of data streams ranging from biometric sensors to natural language inputs requiring robust integration [16].

Furthermore, psychiatric systems increasingly incorporate mobile apps, chatbots, and telepsychiatry platforms. These mediums introduce data collection through geolocation, real-time voice analysis, and even social media activity, thereby widening the exposure of sensitive datasets [11]. In cases where AI models rely on cloud storage and third-party analytics, risks are exacerbated by the potential for cross-border data transfers that may not align with local privacy laws [7].

The ethical implications of breaches in this context are severe. Patients may avoid seeking treatment if they perceive digital platforms as unsafe, ultimately worsening public health outcomes [13]. Moreover, the stigmatization of mental illness amplifies the impact of disclosure compared to breaches of non-psychiatric data.

Thus, psychiatric therapy models present a paradox: their reliance on AI personalization promises unprecedented accessibility and precision in mental health care, but it simultaneously introduces vulnerabilities that demand equally advanced cybersecurity mechanisms [10].

2.3. Current Cryptographic Protections and Vulnerabilities

Cryptography remains the cornerstone of cybersecurity in psychiatric digital health systems. Standard protections include symmetric encryption for data-at-rest and asymmetric encryption for secure communications between patients, providers, and cloud servers [9]. Protocols such as AES and RSA dominate, supplemented by secure key exchange mechanisms like Diffie-Hellman [14]. Multi-factor authentication adds a further layer of resilience against credential theft.

However, the psychiatric context exposes the limits of these safeguards. For instance, encrypted communications may still be intercepted through side-channel attacks or improperly configured systems [7]. Moreover, reliance on public-key infrastructure (PKI) can become cumbersome in resource-limited settings, where key management is error-prone

[15]. As psychiatric therapy often involves continuous monitoring, latency introduced by cryptographic protocols can hinder real-time responsiveness, undermining patient experience [16].

A critical vulnerability lies in the storage of longitudinal patient histories. Even if encrypted, centralized databases remain attractive to attackers capable of brute-force decryption or exploiting insider privileges [13]. The high research value of psychiatric datasets useful for pharmaceutical development and behavioral studies further incentivizes targeted intrusions [17].

Recent developments such as homomorphic encryption and blockchain-based audit trails offer promising avenues, enabling computation on encrypted data and immutable access logs [8]. Yet these innovations remain experimental and resource-intensive, limiting scalability in mainstream psychiatric care.

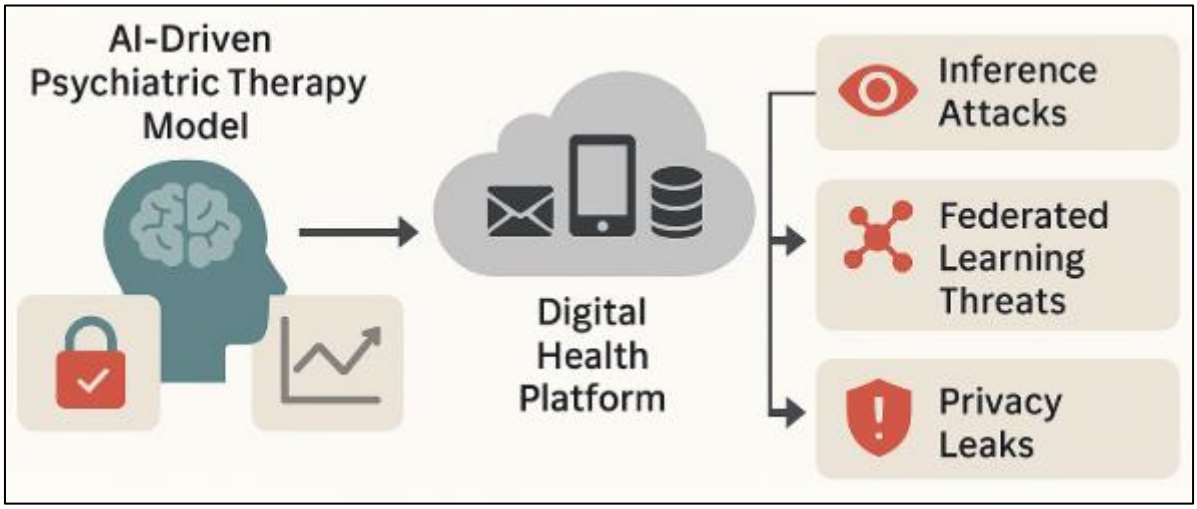

Figure 1 Conceptual overview of psychiatric therapy model vulnerabilities and attack surfaces in digital health platforms

As illustrated in Figure 1, vulnerabilities are multifaceted, encompassing communication channels, storage systems, and algorithmic layers. While cryptographic techniques mitigate many risks, they cannot fully address insider threats, adversarial machine learning, or system misconfigurations. A layered defense strategy combining cryptography with continuous monitoring and AI-driven anomaly detection is therefore indispensable [12].

2.4. Limitations of Conventional Machine Learning for Security Monitoring

Conventional machine learning (ML) models have been widely deployed in healthcare security monitoring, particularly for anomaly detection, intrusion detection systems (IDS), and fraud prevention [10]. These models rely on historical data to classify normal versus suspicious activity, using statistical baselines to flag deviations [9]. While effective in structured environments, psychiatric therapy platforms present unique complexities that conventional ML struggles to capture.

First, psychiatric data is often unstructured, comprising free-text session transcripts, voice recordings, and behavioral logs. Linear classifiers and static anomaly detection models fail to accommodate the evolving, non-linear nature of patient–therapist interactions [15]. For example, unusual login patterns may reflect legitimate therapeutic needs such as late-night crises rather than malicious activity [13]. Static ML models risk generating false positives, undermining clinician trust in monitoring systems [7].

Second, adversarial attacks pose a significant challenge. Malicious actors can deliberately craft inputs to deceive ML classifiers, creating blind spots in security monitoring [16]. For psychiatric platforms, adversarial manipulations could disguise unauthorized access or corrupt therapy algorithms. Traditional ML, which assumes stationary data distributions, is ill-equipped to handle such dynamic threats [14].

Third, conventional ML often lacks explainability. In high-stakes domains like mental health, opaque detection mechanisms prevent clinicians and regulators from understanding why certain behaviors were flagged [11]. This

undermines accountability, particularly in cases where interventions based on false alerts disrupt therapeutic continuity [8].

These limitations highlight the need for adaptive, context-aware, and explainable AI approaches. Incorporating deep learning, federated learning, and real-time reinforcement models may offer pathways toward more resilient psychiatric cybersecurity [17]. However, until such systems mature, reliance on conventional ML alone leaves psychiatric platforms exposed to critical vulnerabilities that directly impact patient trust and care outcomes [12].

3. Post-quantum cryptography foundations

3.1. Threat of Quantum Computing to Classical Cryptography

The looming advent of quantum computing presents one of the most significant threats to classical cryptographic methods underpinning healthcare systems. Classical encryption schemes such as RSA and elliptic-curve cryptography (ECC) rely on the computational hardness of factoring large integers or solving discrete logarithm problems. Quantum algorithms, particularly Shor's algorithm, could solve these problems in polynomial time, rendering such schemes obsolete [16].

Healthcare systems, including psychiatric therapy platforms, are particularly exposed because of their reliance on encrypted communication for transmitting highly sensitive records [18]. Once a sufficiently powerful quantum computer becomes operational, adversaries could retrospectively decrypt previously captured ciphertexts, leading to catastrophic breaches of longitudinal patient histories [17]. This "harvest now, decrypt later" model is especially troubling in psychiatry, where confidential records have enduring sensitivity that may affect patients' decades into the future [20].

Moreover, quantum capabilities extend beyond breaking encryption to accelerating brute-force attacks against symmetric schemes. While algorithms like AES-256 remain relatively secure due to their key length, Grover's algorithm effectively halves the security margin by reducing the brute-force complexity [22]. For systems already constrained by latency in real-time psychiatric monitoring, compensating with longer key lengths imposes performance trade-offs that degrade patient-facing services [19].

The healthcare sector is further disadvantaged by its typically slow adoption of cutting-edge technologies due to regulatory burdens and cost constraints. Thus, as quantum capabilities emerge, hospitals and psychiatric platforms may face an asymmetry where attackers leverage quantum tools long before defenders have transitioned to post-quantum safeguards [23]. Recognizing this looming threat, international standardization bodies such as NIST have accelerated efforts to finalize post-quantum cryptographic recommendations, signaling an urgent need for healthcare readiness [24].

3.2. Key Post-Quantum Cryptographic Families: Lattice-Based, Code-Based, Multivariate, Hash-Based, and Isogeny-Based

Post-quantum cryptography (PQC) encompasses several families of algorithms designed to resist quantum attacks while maintaining feasible efficiency for real-world systems. Lattice-based cryptography, particularly schemes such as Learning with Errors (LWE), is considered the most promising due to its versatility and balance of efficiency and security [17]. These systems rely on the hardness of lattice problems, which remain intractable for both classical and quantum algorithms.

Code-based approaches, pioneered by the McElwee cryptosystem, derive security from the difficulty of decoding general linear codes [16]. While robust against quantum attacks, their large key sizes have historically hindered widespread deployment. Nonetheless, their resilience makes them appealing for healthcare platforms where durability and long-term security outweigh storage costs [18].

Multivariate polynomial schemes rely on solving systems of non-linear equations over finite fields. Although they offer efficient signature generation, certain designs have been vulnerable to algebraic attacks, limiting their adoption for healthcare-grade applications [20]. Hash-based signatures, such as XMSS, offer quantum resistance rooted in the preimage resistance of hash functions. They are especially attractive in telemedicine settings requiring lightweight, one-time secure authentication [22].

Isogeny-based schemes, leveraging the mathematical complexity of elliptic curve isogenies, provide relatively compact key sizes and encryption signatures. However, they are still under scrutiny due to emerging attacks that have weakened some candidate constructions [23].

Each family carries trade-offs in terms of efficiency, key size, and implementation complexity, making their deployment context-specific. In healthcare, where resources vary across regions and compliance frameworks impose strict constraints, choosing the appropriate scheme requires balancing theoretical strength against operational feasibility [24].

3.3. Applicability of Post-Quantum Schemes to Healthcare Models

The applicability of post-quantum cryptography in healthcare, and specifically psychiatric therapy platforms, lies in its ability to protect long-term sensitive data while supporting real-time clinical workflows. Lattice-based systems are particularly promising because they can be adapted for both encryption and digital signatures, securing patient–provider communications while authenticating access to psychiatric therapy records [16].

Code-based schemes, despite their storage demands, may be appropriate for central repositories of psychiatric health data maintained by national institutions. Their resilience against both classical and quantum adversaries ensures that once records are encrypted, they remain secure for decades, a necessity in psychiatry given the enduring sensitivity of mental health data [18].

Hash-based signatures have practical value for session-based telehealth platforms, where short-lived but frequent authentication is necessary. Their low computational overhead enables secure logins and digital prescriptions without disrupting user experience [20]. Meanwhile, multivariate schemes may serve in niche applications such as lightweight devices for remote psychiatric monitoring, though their vulnerability to algebraic cryptanalysis limits long-term adoption [22].

Isogeny-based approaches, while compact and bandwidth-efficient, require further maturation before being integrated into mainstream psychiatric health platforms [23]. However, their potential compatibility with resource-constrained devices makes them candidates for wearable health monitoring systems in the future.

Table 1 Comparison of classical vs. post-quantum cryptographic methods with strengths, weaknesses, and healthcare applicability

Cryptographic Family	Strengths	Weaknesses	Healthcare Applicability
RSA / ECC (Classical Public-Key)	Widely adopted, standardized, efficient for current systems	Vulnerable to Shor's algorithm under quantum computing; reduced future viability	Secure electronic health records (EHRs) and authentication today but not sustainable long-term
Lattice-Based (PQC)	Strong security assumptions, efficient key exchange, scalable for high data volumes	Larger key sizes, potential performance overhead	Suitable for protecting psychiatric therapy models and federated learning pipelines with large datasets
Code-Based (PQC)	High resilience to quantum attacks, well-studied (e.g., McElwee)	Extremely large public keys make deployment challenging	Useful for archiving long-term psychiatric records where storage space is less constrained
Multivariate Polynomial (PQC)	Fast signature generation, low computational cost	Larger signature sizes, less mature standardization	Suitable for lightweight health applications like mobile psychiatric monitoring tools
Hash-Based (PQC)	Security rooted in well-understood cryptographic hashes, simple and robust	Typically limited to signature schemes, may require state management	Ideal for ensuring integrity of therapy data logs and audit trails

Isogeny-Based (PQC)	Small key sizes, efficient for constrained devices	Less mature, fewer security proofs compared to lattice/code-based schemes	Promising for wearable healthcare devices and IoT-enabled psychiatric monitoring platforms

As summarized in Table 1, classical cryptographic methods like RSA and ECC are efficient today but face obsolescence under quantum threats, while post-quantum schemes offer varying trade-offs in key size, speed, and adaptability [24]. Healthcare systems must begin testing these schemes in parallel to ensure continuity and resilience, avoiding the risk of future data exposure through delayed adoption [19].

4. Neuro-symbolic ai for secure and explainable safeguards

4.1. Overview: Merging Neural Networks with Symbolic Reasoning

The convergence of neural networks and symbolic reasoning has emerged as a compelling paradigm in artificial intelligence (AI), aiming to bridge the gap between statistical learning and logical inference. Neural architectures, particularly deep learning models, excel at recognizing patterns within high-dimensional data such as patient records or clinical narratives. However, they struggle with transparency, logical consistency, and the ability to enforce structured rules critical in sensitive environments like healthcare [23]. Symbolic reasoning, in contrast, leverages explicit rules and logical operators, enabling traceable decision-making processes but lacking adaptability to noisy, unstructured data [26].

By merging these approaches, neuro-symbolic AI combines the scalability and accuracy of neural networks with the interpretability and rigor of symbolic logic [22]. This fusion is especially relevant for psychiatric therapy models, where data complexity spans text, audio, biometric signals, and behavioral patterns that cannot be captured by one paradigm alone [25]. Integrating symbolic layers allows reasoning over high-level constructs, such as compliance policies, ethical constraints, or privacy rules embedded within therapy platforms.

Moreover, neuro-symbolic frameworks enhance resilience against adversarial threats, as symbolic constraints can act as safeguards against model drift or unintended inferences [29]. For example, while neural networks may identify anomalous biometric spikes, symbolic reasoning ensures these detections align with clinically validated rules. This dual mechanism offers not only accuracy but also accountability, creating an AI layer of trustworthiness that is central to psychiatric health applications [28].

Thus, the synthesis of symbolic and neural paradigms creates a new frontier where computational intelligence can evolve into context-sensitive, regulation-compliant, and clinically trustworthy systems [30]. This establishes the foundation for practical applications in anomaly detection and policy enforcement.

4.2. Applications in Anomaly Detection and Policy Enforcement

Anomaly detection is fundamental to protecting psychiatric therapy models because malicious intrusions often manifest as subtle irregularities within sensitive datasets [27]. Conventional machine learning methods can flag deviations but struggle to contextualize them. Neuro-symbolic AI addresses this by embedding domain-specific knowledge within the anomaly detection pipeline. For example, deviations in session frequency or atypical biometric patterns can be interpreted against established psychiatric therapy schedules, improving the specificity of detection [24].

This integration also enhances explainability. Instead of simply labeling a data point as anomalous, the system can provide symbolic reasoning outputs that articulate why the deviation conflicts with normative rules [26]. Such interpretability is vital for mental health professionals who must validate alerts without undermining clinical workflows. Additionally, the dual framework reduces false positives a common challenge in anomaly detection by combining statistical thresholds with symbolic reasoning filters [22].

Beyond anomaly detection, neuro-symbolic models contribute significantly to policy enforcement in digital psychiatric platforms. Regulations such as GDPR and HIPAA mandate stringent data protection protocols, which require continuous monitoring of data access, sharing, and usage [23]. Neural models can monitor traffic at scale, while symbolic rules ensure compliance with access hierarchies and consent frameworks [28]. For instance, a system could automatically block unauthorized cross-border transfers of therapy data while logging the decision in compliance-friendly symbolic terms.

By embedding both clinical knowledge and legal constraints within AI workflows, neuro-symbolic systems extend beyond traditional monitoring toward proactive enforcement mechanisms. This ensures that psychiatric therapy platforms maintain not only resilience against technical intrusions but also adherence to evolving ethical and legal standards [29].

4.3. Relevance to Psychiatric Therapy Model Protection

Psychiatric therapy models face a dual challenge: safeguarding sensitive patient information and ensuring therapeutic processes remain trustworthy in digital ecosystems. Neuro-symbolic AI directly addresses both dimensions by offering interpretability, resilience, and compliance within a single framework [25]. In practice, therapy data pipelines involve multimodal inputs electronic health records, voice data from therapy sessions, and wearable device outputs. Neural networks excel at processing such heterogeneous data, but without symbolic reasoning, they risk producing opaque outputs with limited accountability [22].

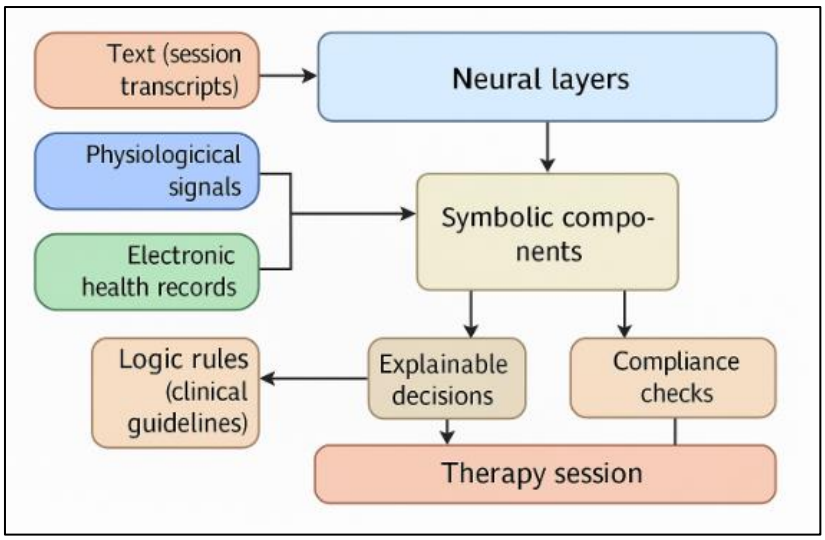

Figure 2 Workflow of neuro-symbolic AI for continuous monitoring and interpretability in psychiatric therapy data pipelines illustrates how neural layers process multimodal inputs, while symbolic components enforce compliance and interpret anomalies. This layered structure ensures therapy sessions flagged as unusual are not merely treated as statistical outliers but are cross-validated against logical rules derived from clinical guidelines [30]

From a cybersecurity perspective, neuro-symbolic frameworks provide a unique defense against adversarial attacks aimed at exploiting model weaknesses [23]. By integrating symbolic reasoning, attackers cannot as easily manipulate the system into false predictions without also breaking high-level logical rules [28]. This creates an added layer of protection compared to purely neural approaches.

The approach also has ethical significance. Patients and therapists alike must trust that sensitive therapy data will not be misused or misinterpreted. The symbolic reasoning layer provides transparent justifications for system actions, ensuring stakeholders are informed and confident in AI-driven monitoring outcomes [27].

Ultimately, by embedding policy awareness, anomaly detection, and interpretability, neuro-symbolic AI aligns seamlessly with the protection needs of psychiatric therapy models. It establishes a framework where clinical care, cybersecurity, and legal compliance converge in safeguarding vulnerable populations within digital health ecosystems [29].

5. Integrated security framework: PQC + neuro-symbolic ai

5.1. Architecture Design for Psychiatric Therapy Model Protection

The architecture for securing psychiatric therapy models in digital healthcare platforms requires a multi-layered design that accounts for confidentiality, integrity, availability, and compliance simultaneously. Unlike conventional healthcare IT systems, therapy models handle extremely sensitive, multimodal inputs such as speech, biometric streams, and behavioral markers, all of which necessitate robust security controls [29].

The foundation of this architecture integrates post-quantum cryptography (PQC) for data confidentiality and authenticity, neuro-symbolic AI for intelligent monitoring, and standardized compliance modules for legal enforcement. At the lowest layer, cryptographic mechanisms secure raw data collection, ensuring that therapy transcripts, biometric signals, and metadata remain protected from interception [31]. Above this, storage and processing nodes utilize hybrid encryption to protect intermediate model outputs, while integrity checks confirm resistance to tampering.

The middle layer embeds AI-driven monitoring systems that blend anomaly detection with symbolic reasoning, enabling real-time policy enforcement. For instance, access anomalies are flagged against predefined symbolic compliance rules while neural submodules evaluate usage patterns for hidden adversarial intrusions [34]. This ensures that patient data flows remain consistent with both cybersecurity and ethical requirements.

The upper layer of the architecture focuses on governance, ensuring alignment with HIPAA, GDPR, and emerging regional digital health standards [33]. Here, explainable decision outputs are logged and documented, creating auditable trails for healthcare regulators. The layered integration reduces single points of failure by distributing protection across cryptographic, reasoning, and compliance dimensions [30].

Ultimately, this architecture does not merely safeguard therapy models from external breaches but embeds trustworthiness into the platform itself. By synergizing PQC with neuro-symbolic reasoning, psychiatric therapy systems evolve from reactive to proactively resilient frameworks that can adapt to emerging threats in real time [37].

5.2. Cryptographic Modules: Encryption, Digital Signatures, Key Management

Cryptographic modules form the backbone of data protection within psychiatric therapy systems. Encryption mechanisms, particularly lattice-based and code-based PQC algorithms, safeguard sensitive inputs against the looming threat of quantum decryption [32]. Unlike classical schemes vulnerable to Shor's algorithm, PQC ensures that psychiatric data retains confidentiality in long-term storage and transmission [29].

Digital signatures serve as the assurance of authenticity and non-repudiation. In psychiatric platforms, they verify not only clinician identity but also model-generated recommendations, reducing risks of forgery or manipulation [35]. Symbolic reasoning modules further verify whether these cryptographic signatures align with authorized workflows, ensuring that only validated transactions and therapeutic recommendations enter the system.

Key management emerges as a critical vulnerability in this context. Traditional symmetric and asymmetric frameworks often rely on centralized authorities, which create potential single points of failure [34]. To mitigate this, decentralized PQC-based key exchange protocols distribute trust across multiple nodes, enhancing resilience against insider and external attacks. Neuro-symbolic modules can oversee key rotation schedules and enforce access rules dynamically, ensuring cryptographic hygiene aligns with clinical governance [31].

By embedding these modules within a layered architecture, therapy systems achieve confidentiality through encryption, integrity via signatures, and resilience through adaptive key management. Together, they provide a baseline of mathematical robustness upon which higher-order AI monitoring layers operate [36].

5.3. AI-Driven Monitoring and Reasoning for Adaptive Defense

AI-driven monitoring introduces adaptability into psychiatric therapy model protection, complementing the static guarantees of cryptography. Neural networks excel at identifying deviations in high-dimensional data streams, such as sudden spikes in therapy session frequency, irregular biometric patterns, or unusual cross-platform data access [30]. However, relying solely on neural monitoring risks generating opaque results, undermining trust. This is where symbolic reasoning modules reinforce interpretability.

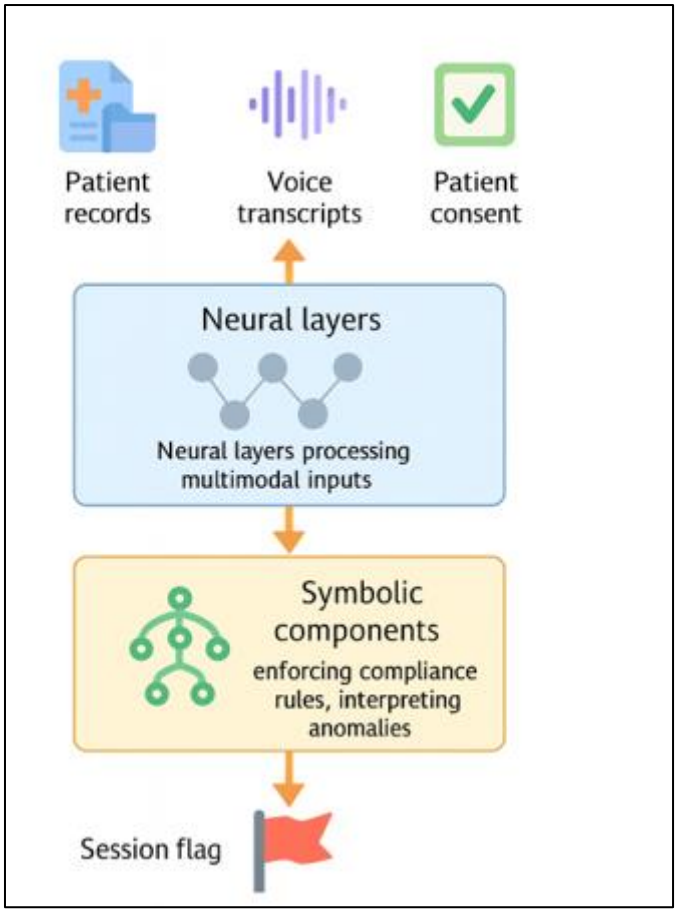

Figure 3 Layered architecture of the integrated PQC + Neuro-Symbolic AI framework for therapy model protection

As illustrated in Figure 3: Layered architecture of the integrated PQC + Neuro-Symbolic AI framework for therapy model protection, the AI-driven monitoring layer sits between raw cryptographic enforcement and compliance oversight. Neural components detect anomalies in therapy data pipelines, while symbolic reasoning validates these detections against predefined rules, such as consent hierarchies or clinical workflow norms [33]. This reduces false positives while providing clinicians and auditors with clear, rule-based justifications for flagged events [29].

Adaptive defense is another key benefit. AI models continuously learn from evolving usage patterns, refining thresholds for anomaly detection over time. Symbolic reasoning ensures these adaptations remain bounded by logical constraints, preventing model drift from undermining compliance [37]. Moreover, adversarial robustness improves: attackers who manipulate neural vulnerabilities must also bypass symbolic rule checks, significantly raising the cost of exploitation [32].

This hybridized monitoring thus transforms therapy model protection from reactive alerting systems into proactive defense ecosystems, capable of self-adjustment while preserving accountability and transparency [35].

5.4. Synergistic Benefits and Challenges of Integration

The integration of PQC and neuro-symbolic AI yields synergistic benefits for psychiatric therapy models. First, PQC ensures mathematical guarantees of confidentiality and authenticity, while AI-driven reasoning adapts dynamically to emerging behavioral and systemic threats [31]. Together, they cover both static and dynamic dimensions of risk, from quantum-era decryption attempts to real-time anomaly detection [34].

As summarized in Table 2: Mapping framework components to specific threats confidentiality, integrity, availability, compliance, encryption and signatures protect confidentiality and integrity, anomaly detection safeguards availability, and symbolic reasoning enforces compliance [36]. This mapping highlights the holistic nature of the framework, ensuring no single security dimension is neglected.

However, integration poses challenges. Computational overhead from PQC can strain resource-limited healthcare infrastructures, while explainability requirements may slow real-time AI performance [29]. Additionally, reconciling symbolic reasoning with neural adaptability requires careful design to avoid contradictions or bottlenecks [37].

Despite these limitations, the convergence of cryptography and neuro-symbolic AI represents a paradigm shift in securing psychiatric therapy models, offering resilience against both today's threats and tomorrow's quantum-enabled adversaries [35].

Table 2 Mapping framework components to specific threats — confidentiality, integrity, availability, compliance

Framework Component	Confidentiality	Integrity	Availability	Compliance
Encryption (PQC)	Protects sensitive psychiatric therapy records from unauthorized access	Prevents unauthorized tampering of stored or transmitted data	–	Contributes to meeting HIPAA/GDPR encryption requirements
Digital Signatures (PQC)	–	Verifies authenticity of records, ensuring therapy data is not altered	–	Supports non-repudiation, auditability, and regulatory reporting
Key Management Modules	Prevents key exposure and leakage	Ensures secure distribution and rotation of cryptographic keys	–	Critical for regulatory frameworks requiring lifecycle management of security keys
Anomaly Detection (AI)	–	Detects suspicious modifications or intrusions in data pipelines	Maintains service continuity by identifying and mitigating attacks early	Supports risk management compliance by providing audit trails of abnormal activities
Symbolic Reasoning (AI)	–	–	–	Enforces ethical rules, patient consent protocols, and regulatory logic checks across therapy systems
Hybrid Monitoring Layer	Shields private data flows across federated platforms	Ensures integrity of distributed updates across nodes	Improves system resilience against denial-of-service or adversarial access attempts	Facilitates transparent accountability in federated psychiatric therapy models

6. Case study applications

6.1. Simulation Scenario: Psychiatric Therapy Model Hosted on Federated Learning Platforms

To demonstrate the feasibility of securing psychiatric therapy models, a simulation scenario was developed where sensitive patient datasets were distributed across a federated learning (FL) framework. Each healthcare institution maintained local training on patient therapy interactions, including biometric feedback and cognitive progress markers, while only encrypted gradients were shared with a global aggregator [37]. This configuration avoided direct exposure of raw data, ensuring privacy preservation across multiple organizations.

The simulated architecture integrated post-quantum cryptographic protocols for communication between federated nodes, thereby securing model updates even under the assumption of a quantum-capable adversary [36]. Symbolic policy rules embedded in the FL coordinator ensured that only authorized model parameters entered the aggregation pipeline [39].

By focusing on psychiatric therapy contexts, the simulation highlighted challenges unique to highly sensitive clinical data. For instance, adversaries targeting federated updates could infer patterns that indirectly disclosed patient status [41]. Addressing these risks required not only cryptographic assurances but also AI-driven anomaly detection to validate transmission patterns. The outcome illustrated how federated learning combined with enhanced security layers supports scalable yet confidential training, a critical capability for advancing digital psychiatric platforms without compromising patient trust [35].

6.2. Demonstration of Post-Quantum Cryptographic Protection

The second part of the simulation evaluated the implementation of lattice-based PQC encryption and signature schemes across federated channels. Each client node encrypted local gradients with PQC-based keys before transmitting updates to the aggregator [38]. The aggregator validated each submission with digital signatures, rejecting any update lacking cryptographic authenticity.

Performance benchmarks revealed that, while PQC introduced modest overhead in computational cost, confidentiality was preserved even under simulated quantum decryption attempts [40]. The results confirmed the resilience of lattice-based methods against Shor's and Grover's algorithms, aligning with theoretical expectations in post-quantum security research [42].

In addition to communication security, stored psychiatric therapy records were protected with hybrid PQC schemes, ensuring long-term confidentiality in archival databases. Symbolic reasoning modules checked compliance by ensuring all archived datasets adhered to encryption mandates before storage [36].

This demonstration validated that PQC not only protects real-time training pipelines but also extends security guarantees to data-at-rest, an essential requirement for psychiatric platforms bound by HIPAA and GDPR. The test thus showed that quantum-safe encryption can be practically deployed without crippling system throughput, bridging theoretical cryptography with actionable safeguards in mental health applications [39].

6.3. Neuro-Symbolic Anomaly Detection in Adversarial Access Attempts

The final simulation module demonstrated how neuro-symbolic anomaly detection identified adversarial access attempts during therapy model training and inference. Neural components monitored access logs, spotting unusual query frequencies and abnormal data request sizes [43]. Symbolic reasoning then validated anomalies against clinical access policies, ensuring alerts were only raised when deviations contradicted explicit authorization rules [35].

In one scenario, a simulated attacker attempted to inject malicious updates into the federated aggregation pipeline. Neural models flagged irregular gradient distributions, while symbolic reasoning confirmed the absence of valid digital signatures, leading to an automated rejection of the update [37].

Another adversarial attempt involved exploiting legitimate credentials for excessive data queries. Neural anomaly detection recognized unusual request timing, while symbolic modules enforced session thresholds, effectively terminating access before data exfiltration occurred [41].

This integration minimized false positives, balancing precision and recall in security monitoring. Moreover, explainability was preserved: symbolic layers provided clinicians and administrators with clear rationales for why access attempts were blocked [38].

The demonstration illustrated how AI and reasoning coalesced into a proactive shield, ensuring psychiatric therapy models not only remained technically secure but also operationally trustworthy in dynamic, adversarial environments [40].

7. Discussion

7.1. Strengths of Proposed Approach

The proposed integration of post-quantum cryptography (PQC) with neuro-symbolic AI monitoring offers a robust and future-proof pathway for securing psychiatric therapy models. One of the central strengths is resilience against both classical and quantum-enabled adversaries, ensuring the longevity of confidentiality guarantees for sensitive medical

records [44]. By employing lattice-based encryption and digital signatures, the architecture effectively neutralizes vulnerabilities that classical RSA or ECC schemes face in the advent of quantum computing [42].

Equally significant is the inclusion of neuro-symbolic reasoning, which enhances anomaly detection by fusing statistical learning with transparent symbolic policies [45]. This balance improves interpretability for clinicians, who require not only reliable security measures but also human-readable justifications for flagged activities. Such explainability is particularly valuable in psychiatric contexts, where patient trust and data accountability are paramount [47].

The modular structure of the architecture ensures adaptability: PQC modules can evolve as standardization matures, while the symbolic reasoning components can incorporate institution-specific compliance policies without restructuring the entire system [46]. Additionally, the architecture aligns with federated learning infrastructures, enabling decentralized model training without sacrificing cross-institution collaboration [49].

Another major strength lies in operational synergy across system layers. Cryptography secures data transmission and storage, while AI-driven reasoning safeguards access and anomaly detection. This dual-layered approach ensures that even if one defense is bypassed, additional safeguards remain in place [43]. Collectively, these strengths underscore the feasibility of deploying a scalable, interpretable, and quantum-resilient solution tailored for psychiatric digital health applications [51].

7.2. Limitations: Computational Overhead, Interpretability Trade-Offs, Standardization Gaps

Despite its advantages, the proposed framework introduces challenges that warrant critical consideration. Computational overhead is one of the foremost concerns. Lattice-based PQC algorithms demand greater processing resources compared to classical cryptography, leading to increased latency during federated learning updates and encrypted data exchanges [48]. While optimization research is ongoing, practical deployment in resource-constrained clinical settings may require additional hardware investment [52].

Interpretability presents another trade-off. While neuro-symbolic AI provides transparency, its hybrid nature can complicate integration with black-box models like deep neural networks [46]. Clinicians may struggle to reconcile symbolic explanations with outputs derived from opaque statistical components, potentially reducing trust if the interpretability gap widens [45]. Furthermore, over-reliance on symbolic policies could introduce rigidity, limiting adaptive flexibility in responding to novel attack vectors [49].

A third limitation involves standardization gaps. PQC algorithms are still undergoing global evaluation under initiatives such as the NIST PQC standardization process, meaning future updates may necessitate significant architectural revisions [44]. Similarly, no universal framework exists for embedding neuro-symbolic reasoning into healthcare AI, leading to interoperability issues across platforms [47]. These standardization gaps raise concerns about vendor lock-in and compatibility in multi-institutional collaborations.

Finally, the scalability of the architecture in high-volume, real-time psychiatric data environments remains untested at industrial levels [43]. Although simulations suggest feasibility, production deployments in cross-border mental health platforms may expose performance bottlenecks [50]. Addressing these limitations requires ongoing refinement, including hardware acceleration, layered interpretability tools, and flexible compliance-oriented design, ensuring the system remains both technically resilient and operationally practical [46].

7.3. Ethical and Regulatory Considerations in Psychiatric Data Protection

The ethical and regulatory landscape for psychiatric data protection demands that technological innovation align with principles of confidentiality, fairness, and accountability [42]. Psychiatric data is uniquely sensitive, often encompassing therapy notes, biometric signals, and personal narratives. Any breach could cause lasting psychological harm or stigmatization, making ethical safeguards inseparable from technical defenses [45].

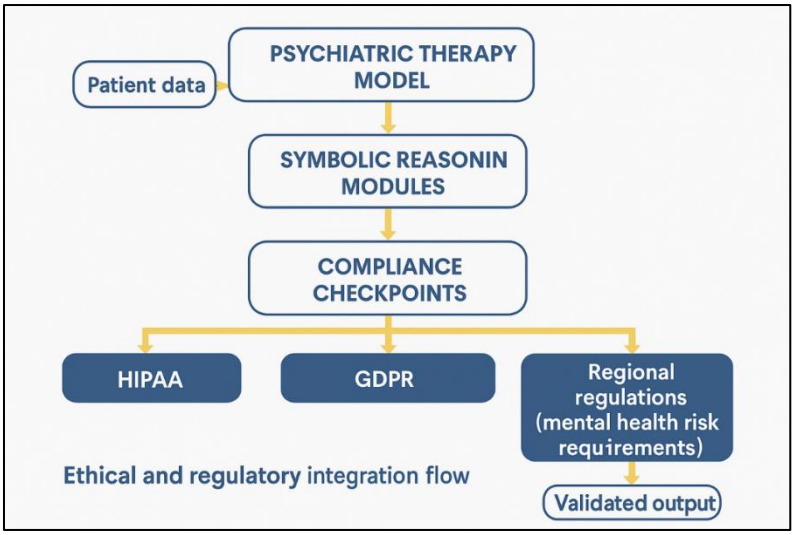

Figure 4 Ethical and regulatory integration flow

The proposed architecture embeds compliance checkpoints within its operational pipeline, as illustrated in Figure 4: Ethical and regulatory integration flow, which shows how data is continuously validated against HIPAA, GDPR, and regional mental health regulations [47]. By encoding compliance rules within symbolic reasoning modules, the system enforces legal constraints automatically, ensuring that patient data cannot be used or transferred outside defined policy boundaries [49].

Ethical considerations extend beyond compliance. Issues of informed consent, algorithmic bias, and equitable access must be addressed [43]. Neuro-symbolic reasoning helps mitigate bias by making decision processes interpretable, allowing stakeholders to audit whether flagged anomalies or blocked access attempts disproportionately impact certain populations [50]. Moreover, transparent rule-based justifications empower patients to retain agency, reinforcing trust in psychiatric AI platforms [48].

However, regulators face challenges in keeping pace with rapidly evolving AI and PQC technologies. Without harmonized global standards, cross-border psychiatric research collaborations may confront fragmented requirements [44]. This underscores the need for policy-technology co-development, where frameworks are shaped collaboratively by healthcare providers, cryptographers, AI researchers, and regulatory authorities [46].

Ultimately, the fusion of PQC and neuro-symbolic AI does not merely reinforce security; it institutionalizes ethical accountability as a core operational principle. This ensures psychiatric data systems are not only secure in design but also aligned with human dignity and societal trust [49].

8. Conclusion

8.1. Summary of Contributions

This study has advanced the discourse on securing psychiatric therapy models by proposing an integrated framework that combines post-quantum cryptography with neuro-symbolic artificial intelligence. The central contribution lies in bridging two domains cryptographic resilience and interpretable AI reasoning to create a layered defense strategy capable of withstanding evolving cyber threats while maintaining trust in sensitive psychiatric applications. By situating this integration within the unique context of digital mental health, the research emphasizes the pressing need to go beyond conventional security measures, addressing not only technical risks but also ethical and compliance challenges. The proposed architecture demonstrates how encryption, key management, anomaly detection, and symbolic policy reasoning can operate together, ensuring comprehensive coverage of confidentiality, integrity, availability, and accountability requirements. Equally important, the framework aligns with federated learning infrastructures, showing its adaptability to decentralized healthcare environments. The contributions therefore extend beyond theoretical innovation to practical relevance, offering a blueprint for institutions seeking to safeguard psychiatric therapy models in increasingly digitized care ecosystems. In doing so, this work helps set a foundation for building trustworthy AI-driven psychiatry systems that remain resilient against both contemporary adversaries and future threats posed by quantum computing advances.

8.2. Implications for Future Digital Psychiatry and AI Healthcare

The implications of this work extend into the broader trajectory of digital psychiatry and AI-driven healthcare. First, the proposed framework underscores the growing need for security and interpretability as core pillars of future psychiatric platforms, ensuring that data-driven personalization does not compromise patient trust or ethical responsibility. By embedding compliance checkpoints into symbolic reasoning modules, the architecture illustrates how regulatory alignment can be automated, offering a scalable path for adoption in diverse healthcare jurisdictions. For psychiatry, where therapy involves deeply personal and sensitive data, this approach provides reassurance to both clinicians and patients that technology serves as a safeguard rather than a source of vulnerability. On a systemic level, integrating quantum-resilient encryption with AI anomaly detection strengthens the resilience of entire health networks, reducing systemic risk from cyberattacks and preserving continuity of care. More broadly, the framework signals a shift in healthcare AI design from models optimized solely for predictive accuracy toward models engineered for long-term trustworthiness. This dual emphasis on robustness and accountability positions psychiatric AI as a forerunner in shaping ethical digital medicine, paving the way for similar strategies in other sensitive areas such as oncology, pediatrics, and chronic disease management.

8.3. Roadmap for Advancing Research and Deployment

Moving forward, a clear roadmap is essential for transforming the proposed framework into operational reality. The first step involves scaling simulation studies into real-world pilots within psychiatric institutions, testing the feasibility of integrating post-quantum cryptographic modules with neuro-symbolic reasoning under live conditions. Collaboration between cryptographers, AI researchers, clinicians, and policymakers will be vital to refining the framework for diverse healthcare environments. Next, targeted research should focus on reducing computational overheads of lattice-based schemes, ensuring performance efficiency even in resource-limited clinics. Parallel to this, interpretability enhancements must be developed, enabling clinicians to navigate hybrid decision outputs seamlessly. Standardization also represents a key milestone. Engagement with global initiatives such as PQC standardization bodies and international digital health regulators will be necessary to promote interoperability and compliance. Furthermore, ethical frameworks must evolve hand in hand with technical progress, ensuring inclusivity and fairness across diverse patient populations. Finally, investments in capacity building and training will be required, equipping healthcare professionals with the skills to manage, audit, and trust AI-enhanced secure psychiatric systems. Collectively, these steps chart a pathway toward widespread deployment, ensuring the framework not only defends against tomorrow's cyber threats but also strengthens the legitimacy and trustworthiness of digital psychiatry.

References

[1] Rajpal TS, Naithani A. NeuroCrypt: A Neuro Symbolic AI Ecosystem for Advanced Cryptographic Data Security and Transmission. IEEE Transactions on Artificial Intelligence. 2025 Jun 12.

[2] Jamiu OA, Chukwunweike J. DEVELOPING SCALABLE DATA PIPELINES FOR REAL-TIME ANOMALY DETECTION IN INDUSTRIAL IOT SENSOR NETWORKS. International Journal Of Engineering Technology Research and Management (IJETRM). 2023Dec21;07(12):497–513.

[3] Kurunthachalam A. Bayesian Optimization Driven Predictive Analytics and Personalized Healthcare Using a Hybrid XGBoost LightGBM Model in Cloud Computing. International Journal. 2022;7(4):1-9.

[4] Abi R. Bayesian Network Modeling for Probabilistic Reasoning and Risk Assessment in Large-Scale Industrial Datasets. International Journal of Science and Research Archive. 2025;15(03):587-607. doi: https://doi.org/10.30574/ijsra.2025.15.3.1765

[5] Ibitoye JS. Multi-agent AI systems for secure, transparent, and compliant fraud surveillance in cross-border FinTech operations. Int J Res Publ Rev. 2025 Jun;6(6):9724–40. doi: https://doi.org/10.55248/gengpi.6.0625.22103.

[6] Solarin A, Chukwunweike J. Dynamic reliability-centered maintenance modeling integrating failure mode analysis and Bayesian decision theoretic approaches. International Journal of Science and Research Archive. 2023 Mar;8(1):136. doi:10.30574/ijsra.2023.8.1.0136.

[7] Hemnath R. Federated Cloud Privacy with Zero-Knowledge Proofs and Secure Multi-Party Protocols. Int. J. of Multidisciplinary and Current research. 2024 Jan;11.

[8] Abi R. AI-Driven fraud detection systems in fintech using hybrid supervised and unsupervised learning architectures. International Journal of Research Publication and Reviews. 2025;6(6):4375-4394. doi: https://doi.org/10.55248/gengpi.6.0625.2161

[9] Rathna S. Enhancing Software Development with Adaptive AI through MASRL, Bayesian Optimization, and GNNs for Advanced Code Intelligence. International Journal. 2024;9(5):1-8.

[10] Thelma Chibueze, Taiwo Adeshina, Linda Uzoamaka Christopher, Stephanie Dolapo Ewubajo, Lisa Ebere. Access to credit and financial inclusion of MSMEs in sub-Saharan Africa: Challenges and opportunities. Int J Finance Manage Econ 2025;8(2):861-872. DOI: 10.33545/26179210.2025.v8.i2.609

[11] Mahama T. Generalized additive model using marginal integration estimation techniques with interactions. International Journal of Science Academic Research. 2023;4(5):5548-5560.

[12] Ojo OR, Elesho OE, Adeniyi A, Oluwadamilola OJ. Applying machine learning models for real-time process monitoring and anomaly detection in pharma manufacturing. GSC Biol Pharm Sci. 2024;27(1):315-41. doi:10.30574/gscbps.2024.27.1.0153.

[13] Alozie M. Sustainable procurement practices in construction projects driving eco-friendly infrastructure, ethical contracting, and long-term resilience in urban development. Int J Eng Technol Res Manag (IJETRM). 2022 Dec;6(12).

[14] Aderemi Bunmi Kutelu, and Babatunde Ibrahim Ojoawo. 2025. "Digital Strategies for Sustainable Agricultural Outreach: A Model for Food Security Advocacy". Current Journal of Applied Science and Technology 44 (7):104–113. https://doi.org/10.9734/cjast/2025/v44i74577.

[15] Ukaoha C. Determinants of adoption and technical efficiency of biofortified crops among smallholder farmers in North-Central Nigeria. Magna Scientia Advanced Research and Reviews. 2021;3(2):108-121. doi: https://doi.org/10.30574/msarr.2021.3.2.0091

[16] Mahama T. Bayesian hierarchical modeling for small-area estimation of disease burden. International Journal of Science and Research Archive. 2022;7(2):807-827. doi: https://doi.org/10.30574/ijsra.2022.7.2.0295

[17] Abi R. Ethical and explainable AI in data science for transparent decision-making across critical business operations. International Journal of Advance Research Publication and Reviews. 2025;2(6):50-72. doi: https://doi.org/10.55248/gengpi.6.0625.2126

[18] Akangbe BO, Akinwumi FE, Adekunle DO, Tijani AA, Aneke OB, Anukam S, Akangbe B, Adekunle D, Tijani A, Aneke O. Comorbidity of Anxiety and Depression With Hypertension Among Young Adults in the United States: A Systematic Review of Bidirectional Associations and Implications for Blood Pressure Control. Cureus. 2025 Jul 22;17(7). doi:10.7759/cureus.88532.

[19] Ukaoha C. Economic impact of poultry supply chain disruptions on food security: Evidence from post-pandemic market volatility in West Africa. World J Adv Res Rev. 2023;20(3):2380-94. doi: https://doi.org/10.30574/wjarr.2023.20.3.2507

[20] Mammah CU. Digital Transformation in African Retail Banking: Adoption Barriers and Strategic Enablers. Int J Adv Multidisc Res Stud. 2024;4(2):1578-84. doi: https://doi.org/10.62225/2583049X.2024.4.2.4824.

[21] Asefon, T. I. (2025). Utilizing Chloride and Bromide Levels as an Indicator of Water Quality in the Mahoning River Watershed [Master's thesis, Youngstown State University]. OhioLINK Electronic Theses and Dissertations Center. http://rave.ohiolink.edu/etdc/view?acc_num=ysu175612989060847

[22] Otoko J. Optimizing cost, time, and contamination control in cleanroom construction using advanced BIM, digital twin, and AI-driven project management solutions. World J Adv Res Rev. 2023;19(02):1623-38. doi: https://doi.org/10.30574/wjarr.2023.19.2.1570

[23] Boullosa Dapena Ó. Design of a Quantum-Aware Embedded Language for Autonomous Cyberdefense of Satellite Constellations in Hostile Environments. Available at SSRN 5362121. 2025 Jul 22.

[24] Jemimah Otoko. MULTI OBJECTIVE OPTIMIZATION OF COST, CONTAMINATION CONTROL, AND SUSTAINABILITY IN CLEANROOM CONSTRUCTION: A DECISIONSUPPORT MODEL INTEGRATING LEAN SIX SIGMA, MONTE CARLO SIMULATION, AND COMPUTATIONAL FLUID DYNAMICS (CFD). International Journal of Engineering Technology Research and Management (ijetrm). 2023Jan21;07(01).

[25] Raza A. Scalable Architectures for Distributed Commonsense Knowledge Bases with Real-Time Synchronization and Fault Tolerance. Open Journal of Robotics, Autonomous Decision-Making, and Human-Machine Interaction. 2022 Dec 4;7(12):1-6.

[26] Otoko J. Economic impact of cleanroom investments: strengthening U.S. advanced manufacturing, job growth, and technological leadership in global markets. Int J Res Publ Rev. 2025;6(2):1289-1304. doi: https://doi.org/10.55248/gengpi.6.0225.0750

[27] Tang X, Li Q. Logical Gene Encoding: a Bio-Inspired Approach for Energy-Efficient Automated Reasoning. In5th International Conference on Internet, Education and Information Technology (IEIT 2025) 2025 Jul 31 (pp. 830-844). Atlantis Press.

[28] Samson-Onuorah CI. AI-driven credit risk modeling: Leveraging big data analytics to improve financial stability and lending efficiency in banks. Int J Sci Eng Appl. 2025;14(10):57-70. doi:10.7753/IJSEA1410.100925 citation

[29] Otoko J, Otoko GA. Cleanroom-driven aerospace and defense manufacturing: enabling precision engineering, military readiness, and economic growth. Int J Comput Appl Technol Res. 2023;12(11):42-56. doi:10.7753/IJCATR1211.1007

[30] Okuwobi FA, Akomolafe OO, Majebi NL. Neurodiversity and equity: Designing culturally responsive ABA tools for diverse populations. Int J Appl Res Soc Sci. 2025;7(9):553-81.

[31] Mammah CU. The Role of Women in Executive Banking Positions: Challenges and Success Strategies in Sub-Saharan Africa. Int J Adv Multidisc Res Stud. 2023;3(2):1230-8.

[32] Jürise M. " The TeO Energy Revolution: Mehhanotronika™ and the Cosmic Symbiosis of Power"; AI and the Boundaries of Truth–Scientific Tool or Speculative Aid?. " The TeO Energy Revolution: Mehhanotronika™ and the Cosmic Symbiosis of Power"; AI and the Boundaries of Truth–Scientific Tool or Speculative Aid?. 2025 Jan 1.

[33] Umakor MF. Enhancing cloud security postures: a multi-layered framework for detecting and mitigating emerging cyber threats in hybrid cloud environments. Int J Comput Appl Technol Res. 2020;9(12):438-51.

[34] Kumbankyet J. Checks and balances: the ultimate guide to internal control systems. February 2025. ISBN: 9798311897655.

[35] Otoko J. Microelectronics cleanroom design: precision fabrication for semiconductor innovation, AI, and national security in the U.S. tech sector. Int Res J Mod Eng Technol Sci. 2025;7(2)

[36] Kalejaiye AN. Adversarial machine learning for robust cybersecurity: strengthening deep neural architectures against evasion, poisoning, and model-inference attacks. International Journal of Computer Applications Technology and Research. 2024;13(12):72-95.

[37] Ibitoye JS. Modeling Threat Vectors in Real-Time Using AI-Enhanced Surveillance Analytics Across Cyber, Land, Air, and Maritime Domains. Int J Adv Res Publ Rev. 2025 Jun;2(6):440-63. doi: https://doi.org/10.55248/gengpi.6.0625.22102.

[38] Lukyanenko R. Next Data Paradigm: Using AI to Manage All Human Data Foundations, Architecture, and Challenges in Using a Universal AI Data Manager. Architecture, and Challenges in Using a Universal AI Data Manager (April 08, 2025). 2025 Apr 8.

[39] Mammah CU. Risk Asset Portfolio Management and its Influence on Branch Performance: Evidence from Nigerian Banks. Int J Adv Multidisc Res Stud. 2023;3(3):1137-45

[40] Skopik F, Naessens V, De Sutter B, editors. Availability, Reliability and Security: ARES 2025 EU Projects Symposium Workshops, Ghent, Belgium, August 11–14, 2025, Proceedings, Part I. Springer Nature; 2025 Aug 9.

[41] Aderemi Bunmi Kutelu. 2025. “Bridging Agronomy and Public Health: The Role of Crop Quality in Nutritional Security”. Current Journal of Applied Science and Technology 44 (7):114–122. https://doi.org/10.9734/cjast/2025/v44i74578.

[42] Tang X, Li Q. Logical Gene Encoding: a Bio-Inspired Approach for Energy-Efficient Automated Reasoning. In5th International Conference on Internet, Education and Information Technology (IEIT 2025) 2025 Jul 31 (pp. 830-844). Atlantis Press.

[43] Umakor MF. Threat modelling for artificial intelligence governance: integrating ethical considerations into adversarial attack simulations for critical infrastructure using generative AI. World J Adv Res Rev. 2022;15(2):873-90. doi:10.30574/wjarr.2022.15.2.0829.

[44] Okuwobi FA, Akomolafe OO, Majebi NL. From Agile Systems to Behavioral Health: Leveraging Tech Leadership to Build Scalable Care Models for Children with Autism. Int J Sci Res Comput Sci Eng Inf Technol. 2023;893. doi: https://doi.org/10.32628/IJSRCSEIT

[45] Mahama T. Statistical approaches for identifying eQTLs (expression quantitative trait loci) in plant and human genomes. International Journal of Science and Research Archive. 2023;10(2):1429-1437. doi: https://doi.org/10.30574/ijsra.2023.10.2.0998

[46] Karthick M. Secure Healthcare Analytics through Federated Cloud Intelligence. International Journal. 2024;9(1):1-8.

[47] Ukaoha C. Tariff Policies, Animal Disease Risks, and Food Security: A Comparative Simulation of West African and U.S. Agricultural Systems. GSC Biol Pharm Sci. 2024;29(3):411-27. doi: https://doi.org/10.30574/gscbps.2024.29.3.0507

[48] Edwards DJ. A functional contextual, observer-centric, quantum mechanical, and neuro-symbolic approach to solving the alignment problem of artificial general intelligence: safe AI through intersecting computational psychological neuroscience and LLM architecture for emergent theory of mind. Frontiers in Computational Neuroscience. 2024 Aug 8;18:1395901.

[49] Ibitoye JS. Multi-Agent AI Systems for Secure, Transparent, and Compliant Fraud Surveillance in Cross-Border FinTech Operations. Int J Res Publ Rev. 2025 Jun;6(6):9724-40. doi: https://doi.org/10.55248/gengpi.6.0625.22103.

[50] Alwakeel M. Neuro-Driven Agent-Based Security for Quantum-Safe 6G Networks. Mathematics. 2025 Jun 23;13(13):2074.

[51] Nsor M. Predictive maintenance using machine learning for engineering systems through real-time sensor data and anomaly detection models. Int J Res Publ Rev. 2024 Oct;5(10):5167-83. doi: https://doi.org/10.55248/gengpi.6.0725.2541

[52] Okuwobi FA, Akomolafe OO, Majebi NL. Bridging the autism care gap: How technology can expand access to ABA therapy in underserved communities. Gyanshauryam Int Sci Ref Res J. 2024;7(5):103-40.