Quantum Computing Techniques to Protect Mental Health Data

INFOSEC PRIVACY AND SECURITY – PROJECT 5

Cree Brownlee
NEW MEXICO STATE UNIVERSITY
ET 539 | ADVANCED ENTERPRISE SECURITY
PROFESSOR LAWRENCE

NO ORCHID ID
NO CONFLICTS OF INTEREST
ALL SOURCES CITED

ABSTRACT

Machine Learning model adoption, privacy infringements, induced stress by surveillance, real-time monitoring, biometrics and questionable data collection ethics impact millions daily. The importance of securing transmittable mental health data, and healthcare or human-centric IoT (H-IoT), hinges on the continued eruption of mental health crises. Crippled usability and lack of security hinder interaction, implementation and system transformations. The increasing reliance on digital technology heightens the need for robust cybersecurity technologies to protect against digital threats. Additionally, the stress of maintaining secure connections during digital asset collections multiplies with every network connection.

Although these concerns affect every corner of business security needs, making ML systems secure and usable for mental health applications is a blind spot in the infosec arena. Mental health application blockchain for secure data sharing, and AI-driven anomaly detection with manipulation deterrents will enhance the healthcare ecosystem. Securing personalized patient monitoring applications/devices, as well as preventing data leaks and HIPAA violations, are at the forefront of H-IoT innovations. Advancements in post-quantum computing/cryptography (PQC) and AI strengthen anomalous behavior detection, securing applications with encryption algorithms. With proactive tooling in quantum-era decryption safeguards, future-ready, secure mental health applications will emerge trustworthy, increasing zero-trust infrastructure.

An increase in reports of cybersecurity-related incidents impacts the emotional and psychological well-being of individuals, leaving them hesitant to seek help from professionals. By using a mental health app, individuals can maintain a healthy mental and physical lifestyle and better cope with life's challenges. However, hackers illegally penetrating companies that host data stored by applications break public trust. Fears of data breaches can lead to unrealistic concerns about unauthorized access or misuse of personal data. Just knowing we're being watched all the time leaves people feeling exposed, while upholding self-imposed censorship. An elevated state of self-consciousness fosters a perpetual sense of scrutiny, and even expressing an opinion or participating in activities can evoke fear or insecurity. (Malik A S, 2024)

A vulnerable mindset, infused with circumspection, weakens a person's ability to relax. Good mental health is the solution to increasing positive responses in protecting personal privacy, helping individuals navigate life's daily experiences without succumbing to cognitive dissonance. The use of IoT devices to monitor patient health and collect data on disease management enables individuals with challenges to exchange data with healthcare professionals, improving their health conditions. Yet, these devices and systems introduce critical security vulnerabilities in large-scale distributed networks. These positive and negative impacts on mental well-being offer valuable insights into future research and public discourse surrounding encryption techniques for mitigating cyberattacks. (Rajaprakash, 2024) (Malik A S, 2024)

Understanding the current landscape and the future of technology is more critical now than it was in the 80s or 90s. For example, quantum computers are estimated to emerge within 10-20 years, thereby accelerating the need to develop quantum-resistant cybersecurity solutions. With a strong start in 1994, Shor's algorithm breaks RSA, elliptic curve cryptography and discrete logarithm problems. Quantum Key Distribution (QKD) protocols, equipped with eavesdropping

detection, securely establish integrated communication channels with practical transmission distances over 500 kilometers—bit rate errors rated below 2%, blocking intercept-resend and photon-number-splitting attacks. The Quantum-Enhanced Security Protocol (QESP) provides guaranteed non-repudiation, utilizing quantum fingerprinting in conjunction with error-correcting codes for unconditional message authentication security. (Williams, 2025)

Adding this schema to the increasing reliance on healthcare- and human-centric Internet of Things (H-IoT) and smart environments raises concerns regarding real-time anomaly detection, adaptive access control, and data integrity. The geographic ranges, quickness of healthcare and advent of telemedicine expose how vulnerable, wearable and other H-IoT devices are and how they rely on traditional frameworks to secure high-latency decision-making. Additionally, sensitive patient information processing along the edge introduces cyberattacks, data breaches, and threatens system integrity. (Naik, 2025) (Abdul Lateef, 2024)

Unfortunately, the large-scale adoption and active usage of ML Systems in implementing frameworks and making them usable by end-users of mental health applications have not been realized. Considering how exposed people feel, usable security is an area of focus for evaluating interactions with users at a system level. One framework proposes a four-pillar framework consisting of context, functionality, trustworthiness, and recovery. In computer system lifecycle terms, the pillars are summarized as design/implementation, deployment, mass adoption and usage, and maintenance/disposal. For example, with a therapy chatbot, usable security mechanisms prioritize availability and robustness to accommodate varying users, a broader range of behaviors, and legitimate user actions. Still, trust in a secure app would be diminished. (Jiang, 2020)

Personal medical histories, genetic information, and real-time physiological data underscore the critical importance of patient data security. The heterogeneity of IoT devices, scalability, and real-time communication are not fully adapted or tested in large-scale environments, highlighting a gap in decentralized authentication within blockchain models. Against robust IoT architecture, H-IoT flexibility is compromised as dynamic IoT networks frequently join and leave decentralized settings. (Panahi, 2025) (Rajaprakash, 2024)

Deep learning (DL) advancements, which capture complex medical data and accelerate high-level analytics in H-IoT systems, have led to the development of Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and Variational Autoencoders (VAEs). CNNs excel at extracting raw medical images and physiological signals, while LSTM networks excel at identifying sequential time-series data. The VAE model compresses data, detects anomalies, and is tamper-resilient through generative reconstruction. Optimization and model compression methods, including quantization, knowledge distillation, and TinyML frameworks, minimize the costs of CNNs and LSTMs while maintaining accuracy. Yet, DLs' singular objectives lack integration of the security triad, data integrity, and real-time, end-to-end operational performance. (Naik, 2025)

According to Naik et al., blockchain and cryptography-based approaches incur computational and energy expenses that don't compensate for the limited resources in edge devices. Naik believes that DL models from autoencoders and VAEs are best utilized as a lightweight solution for data validation and reconstruction of input signals, thereby maximizing transmission efficiency. With few realistic edge computing test models with real-world constraints, real-time operational management isn't studied under a single architecture, which reduces accuracy in multi-signal environments. (Naik, 2025)

IoT security is a critical research area striving to enhance secure communication protocols, IDSs, decentralized security models and various encryption methods. Authentication is crucial in protecting IoT networks against unauthorized access, command spoofing, and data breaches. Unlike Naik, Rajaprakash et al. advocate for lightweight cryptographic algorithms that minimize computational loads on IoT devices, thereby requiring minimal processing power and energy. To that end, decentralized or peer-to-peer authentication schemes are more likely to reduce bottlenecks, thereby eliminating single points of failure in IoT systems. (Rajaprakash, 2024)

Rajaprakash et al. propose an RNN-based framework for H-IoT. The logic behind the suggestion is RNNs' ability to catch temporal dependencies, finding anomalies and patterns in streams of continuous data within healthcare networks. The model learns from historical patterns, filtering out subtle nuances from the data flow that may indicate a security threat. RNNs' dynamic adaptability in changing network traffic increases data quality when it can't be modeled predictively or linearly, and they can handle variable-length input sequences. The ability to train the model to detect individual device time-based abnormalities or coordinated attacks across several devices is a key capability in protecting interconnected networks across an established baseline. (Rajaprakash, 2024)

In another study on the importance of transmitting Electroencephalography (EEG) and Electrocardiography (ECG) recordings to detect and monitor mental health conditions and improve healthcare efficiency. High-dimensional, susceptible artifacts benefit from the emergence of Quantum Machine Learning (QML), which utilizes quantum variational autoencoders (QVAEs) to enhance feature extraction from EEG and ECG signals, thereby mapping data into low-dimensional quantum latent representations. This process improves classification and noise robustness. The combination of Quantum Wasserstein Distance (QWD)

and Quantum Fisher Information (QFI) can introduce quantum-inspired loss functionality, improving regulatory feature sensitivity, reconstruction quality and classification accuracy. Although the model lacks rich inter-modal dependencies, it offers insights into the growing need for telehealth devices to support quantum-based architectures for transmitting and securing diagnostic transmissions. (Jabbar, 2025)

A paradigm in AI is the emergence of neural networks and symbolic reasoning, creating neuro-symbolic AI. The fusion encompasses text, audio biometric signals, and behavioral patterns, enabling reasoning over high-level constructs within therapy platforms. This new frontier in computational intelligence may evolve into clinically resilient, compliant and trustworthy systems. For example, atypical biometric patterns can become more explainable, improving the specificity of detection. This means attackers exploiting the system with false predictions can't break high-level logical rulesets. (Kumar, 2025)

Psychiatric therapy models are applicable in healthcare but can also transform any business with a need to offer more relaxation methods as the adoption of ML models and AI frameworks increases. The evolution of supporting patients outside the conventional clinic model enables mental health professionals to deliver structured interventions to patients consistently and effectively. To ease fear and increase adoption, systems that integrate post-quantum cryptography with neuro-symbolic AI, enabling the transmission of data to and from H-IoT devices, will enhance consumer trust. (Kumar, 2025)

SUMMARY

Finding the right balance between healthcare, security, and post-quantum computing proved to be a challenging task. Writing the paper with the articles I found proved to be the most challenging part of the assignment. It has compelled me to refine my writing style to accommodate the growing presence of AI detection mechanisms.

Understanding how to utilize ten articles and produce something readable was my top priority. I wanted the result to be consistent and seamless, as if it were one thought. I removed ambiguity but added complexity, providing little explanation for each suggested framework, as I couldn't test the conclusions.

REFERENCES

Abdul Lateef, H. P. (2024). FEASIBLE IMPLEMENTATION OF EXPLAINABLE AI EMPOWERED SECURED EDGE BASED HEALTH CARE SYSTEMS. *Journal of Smart Internet of Things (JSIoT), 2024*(02), 1-12. https://doi.org/10.2478/jsiot-2024-0008

Jabbar, A. J. (2025). Fusion-aware quantum variational autoencoder for brain-heart signal modeling in mental health applications. *Journal of King Saud University Computer and Information Sciences , 37*(268). https://doi.org/10.1007/s44443-025-00264-3

Jiang, H. S. (2020). Usable Security for ML Systems in Mental Health: A Framework. *arxiv.org, 1*(2008.07738), 1-9.

Kumar, A. (2025). Post-quantum cryptography combined with neuro-symbolic AI to safeguard sensitive psychiatric therapy models against future cyber threats . *GSC Biological and Pharmaceutical Sciences, 33*(1), 1-18. https://doi.org/10.30574/gscbps.2025.33.1.0379

Malik A S, A. S. (2024). Exploring the Impact of Security Technologies on Mental Health: A Comprehensive Review. *DMIHER Datta Meghe Medical College*, 1 - 13. https://doi.org/10.7759/cureus.53664

Manchanda, R. P. (2025). Energy-efficient clustering and routing for IoT-enabled healthcare using adaptive fuzzy logic and hybrid optimization. *Scientific Reports, 15*(34619). https://doi.org/10.1038/s41598-025-18243-z

Naik, N. S. (2025). Hybrid deep learning-enabled framework for enhancing security, data integrity, and operational performance in Healthcare Internet of Things (H-IoT) environments. *Scientific Reports, 15*(31039). https://doi.org/10.1038/s41598-025-15292-2

Panahi, O. (2025). Secure IoT for Healthcare. *European Journal of Innovative Studies and Sustainability , 1*, 17-23. https://doi.org/10.59324/ejiss.2025.1(1).03

Rajaprakash, S. B. (2024). RNN-Based Framework for IoT Healthcare Security for Improving Anomaly Detection and System Integrity. *Mesopotamian Academic Press, 2024*, 106-114. https://doi.org/10.58496/BJIoT/2024/013

Williams, R. (2025). Quantum Computing Applications in Cryptographic Protocol Enhancement. *International Journal of Engineering and Computational Applications, 01*(05), 12-15.