Artificial Intelligence and Quantum Computing in Criminal Justice Systems: A Communication Engineering Perspective

Sejoon Yang[1] and Hongchul Shin[2,*]

[1]*Law School, Kyung Hee University, Seoul 02447, Republic of Korea*

[2]*Department of Biotechnology, College of Life Sciences and Biotechnology, Korea University, Seoul 02841, Republic of Korea*

Abstract: Modern communication systems face unprecedented challenges in ensuring secure data transmission and real-time processing across distributed networks. The convergence of artificial intelligence (AI) and quantum computing (QC) fundamentally transforms communication engineering by introducing both enhanced capabilities for intelligent network management and critical threats to cryptographic security protocols that underpin global communications. These challenges are particularly acute in high-security domains such as criminal justice systems, where communication infrastructure must balance stringent security requirements with evidentiary reliability. The administration of criminal justice has historically relied on the epistemological reliability of evidence and the ontological security of information. However, the legal profession currently faces a radical discontinuity driven by the simultaneous maturation of Generative Artificial Intelligence (AI) and the accelerating development of Quantum Computing (QC). Generative AI has introduced a regime of "probabilistic truth," leading to the proliferation of hallucinated legal texts and synthetic media that threaten evidentiary standards. Parallel to this, the looming reality of QC poses a fundamental threat to the cryptographic locks securing sensitive criminal justice data, notably through strategies that target current encrypted data for future decryption. As the integration of these advanced technologies becomes an irreversible trend, there is a critical need to synthesize these divergent yet interconnected threats to understand their collective impact on judicial integrity. This review analyzes the epistemological crisis precipitated by the integration of algorithmic text generation into legal workflows and the challenges posed to digital forensics by the potential compromise of encryption standards. Furthermore, it explores the transformative potential of Quantum Machine Learning (QML) in unraveling sophisticated modern criminal schemes, particularly for identifying complex patterns in financial crimes and criminal networks, while also addressing the technical hurdles limiting the practical deployment of these models. This study underscores the critical necessity for the legal system to fortify procedural defenses against AI-generated misinformation and to accelerate the migration to quantum-resistant security infrastructures. Ultimately, this review highlights that preserving the validity of the justice system requires commitment to technological literacy and the establishment of rigorous verification frameworks to navigate the dual disruption of algorithmic probabilities and quantum insecurity.

Keywords: Artificial intelligence, Quantum computing, Criminal justice systems, Digital forensics.

1. INTRODUCTION

Modern communication systems face unprecedented challenges in ensuring secure, efficient, and reliable data transmission across increasingly complex networks [1]. The convergence of Artificial Intelligence (AI) and Quantum Computing (QC) represents a transformative paradigm shift in communication engineering, fundamentally altering how we approach network security, real-time data analysis, and distributed system architecture [2]. AI-driven technologies enable intelligent network optimization, automated threat detection, and adaptive resource allocation in large-scale communication infrastructures, while quantum computing promises both revolutionary computational capabilities and existential threats to current cryptographic foundations that secure global communication networks [2, 3].

The integration of these technologies addresses three critical challenges in contemporary communication engineering. First, protecting sensitive data transmission against both classical cyberattacks and emerging quantum threats [4]. Second, enabling intelligent real-time analysis of massive data flows across distributed networks [5]. Third, maintaining system integrity and availability in increasingly complex interconnected environments [1, 2]. These challenges transcend individual application domains, affecting healthcare information systems, financial transaction networks, telecommunications infrastructure, and government communication systems. Each domain demands specialized security protocols, fault-tolerant architectures, and privacy-preserving mechanisms that can adapt to rapidly evolving technological landscapes while maintaining backward compatibility with existing systems.

Among these application domains, criminal justice systems represent a particularly demanding test case that exemplifies the most stringent requirements for secure communication infrastructure [6]. The administration of justice combines maximum security imperatives with evidentiary reliability standards and constitutional privacy protections, making it an ideal lens through which to examine the practical implementation of AI and quantum technologies in mission-critical communication systems [7]. The legal

*Address correspondence to this author at the Department of Biotechnology, College of Life Sciences and Biotechnology, Korea University, Seoul 02841, Republic of Korea; E-mail: saekomi5@korea.ac.kr

Received on 31-12-2025 Accepted on 02-02-2026 Published on 01-03-2026

E-ISSN: 2979-1081/26

profession currently faces a dual disruption driven by the simultaneous maturation of generative AI and the accelerating development of QC.

The administration of justice has historically relied on two foundational pillars which are the epistemological reliability of evidence and the ontological security of information [8]. For centuries these pillars were maintained through human testimony and physical custody chains but the third decade of the 21st century has introduced radical discontinuity [9]. The legal profession currently faces a dual disruption driven by the simultaneous maturation of generative AI)and the accelerating development of QC [10-12]. Generative AI has introduced a regime of probabilistic truth where the generation of legal texts and evidentiary media is no longer strictly deterministic but constitutes the output of statistical correlations within vast datasets [13-15]. This shift has precipitated an immediate crisis characterized by the proliferation of hallucinated case law and the weaponization of synthetic media [16]. Parallel to this epistemological disruption is the ontological threat posed by QC [17]. Unlike the probabilistic emulation of intelligence seen in AI systems, QC harnesses superposition and entanglement to perform computations intractable for classical binary systems. While Generative AI challenges the content of legal files, QC challenges the container or the cryptographic locks securing sensitive criminal justice data [18]. The looming reality of Cryptographically Relevant Quantum Computers (CRQCs) has given rise to the Harvest Now Decrypt Later (HNDL) strategy where adversaries intercept encrypted data today to decrypt it in a post-quantum future [19]. This review synthesizes these divergent yet interconnected threads by analyzing the breakdown of truth in recent litigation, the regulatory divergence in AI governance, and the mechanics of the quantum threat to digital forensics.

2. COMMUNICATION INFRASTRUCTURES AND SECURITY FRAMEWORK

Modern communication systems require comprehensive security frameworks that address both classical threats and emerging quantum vulnerabilities while maintaining the performance necessary for real-time AI-driven applications [20]. The integration of artificial intelligence and quantum computing in communication networks necessitates a multi-layered approach encompassing secure protocols, resilient architectures, and efficient data processing pipelines that can operate across distributed environments [2].

The foundation of secure communication rests on robust cryptographic protocols, with traditional Transport Layer Security (TLS) and Secure Sockets Layer (SSL) mechanisms remaining essential for contemporary systems [21]. However, the impending threat of cryptographically relevant quantum computers has accelerated adoption of post-quantum cryptography (PQC) [22]. In August 2024, NIST released the first three PQC standards including Kyber for encryption and Dilithium and Falcon for digital signatures, marking a critical transition toward quantum-resistant security [23]. Organizations are implementing hybrid cryptographic approaches that combine classical algorithms with quantum-resistant alternatives, ensuring protection even if quantum breakthroughs occur unexpectedly. Major technology companies have deployed hybrid key exchange mechanisms for internal networks, while standards bodies develop specifications for widespread enterprise adoption across VPN appliances, databases, and cloud services [23].

Quantum Key Distribution (QKD) represents the next generation of secure communication, providing provably secure channels based on quantum mechanical principles rather than mathematical hardness assumptions [24]. Unlike PQC, QKD offers unconditional security by detecting eavesdropping attempts through quantum state disturbance. Commercial QKD networks are beginning deployment in data centers, critical infrastructure, and even consumer devices [24]. The European Commission's 2024 recommendations emphasize that quantum computing advances will enable adversaries to decrypt current encryption unless systems are upgraded, driving regulatory momentum for quantum-safe transitions globally [25]. Zero-trust architecture principles complement these cryptographic measures by requiring continuous verification of all network participants regardless of location. Multi-factor authentication enhanced with AI-driven behavioral analysis identifies anomalous access patterns while maintaining usability, and role-based access control ensures granular permission management across complex distributed systems [25].

Privacy-preserving techniques enable secure computation without exposing sensitive data [26]. Homomorphic encryption allows processing on encrypted data without decryption, critical for AI model training across organizational boundaries [26]. Secure multi-party computation protocols enable collaborative analytics while keeping individual inputs private, and differential privacy mechanisms protect individual data points while preserving statistical utility for large-scale analysis [27]. These technologies are essential for healthcare, finance, and government applications where regulatory compliance demands stringent data protection.

Network security architecture must address threats across multiple layers through AI-driven detection mechanisms and quantum-resistant cryptography [28]. Machine learning-based intrusion detection systems (IDS) achieve significant improvements in anomaly detection accuracy while reducing false positives through intelligent traffic analysis [29]. Deep learning architectures including CNNs, RNNs, and LSTM networks demonstrate high accuracy in detecting complex attacks such as DDoS, advanced persistent threats, and zero-day exploits by identifying spatial and temporal patterns in network traffic [29]. Ensemble approaches combining multiple models, particularly Random Forest algorithms, provide optimal performance with efficient inference times that enable real-time threat response within small packet windows [30, 31].

Federated learning enables collaborative intrusion detection across distributed networks without centralizing sensitive data, preserving privacy while improving threat intelligence sharing [30]. Modern frameworks can process hundreds of thousands of network inputs within seconds using distributed computing resources. Integration with Software-Defined Networking enables dynamic resource allocation in response to detected threats, automatically adjusting bandwidth, isolating compromised segments, and redistributing resources among legitimate users [31]. Multi-agent systems provide another architectural approach where intelligent agents operate autonomously across network segments, coordinating responses to provide hierarchical distributed security working in conjunction with firewalls and network management systems [32].

The quantum computing threat demands urgent quantum-safe infrastructure implementation. In October 2024, methods to attack RSA encryption using quantum systems indicates quantum cryptanalysis is transitioning from theory to reality [33]. QCs leveraging Shor's algorithm can break RSA and Elliptic Curve Cryptography, jeopardizing global communication security [33, 34]. Predictions suggest quantum computers could crack RSA-2048 within the next decade, requiring organizations to implement PQC while maintaining backward compatibility through hybrid classical-quantum security models [34]. Legislative frameworks are accelerating adoption of quantum-resistant algorithms, while the concept of cryptographic agility has become a core requirement for resilient security architectures [35].

Efficient data processing architectures balancing low latency with comprehensive analytics capabilities are essential for AI-driven systems. Edge computing brings computation closer to data sources, dramatically reducing latency compared to centralized cloud architectures [36]. This proximity enables real-time decision-making critical for autonomous vehicles, industrial IoT, and smart cities where millisecond response times are safety critical [37]. Market analysis predicts the most enterprise data will be processed outside traditional data centers by 2025, reflecting cloud computing's limitations for latency-sensitive applications [37]. Edge devices now possess significant computational capabilities for preprocessing, filtering, and machine learning inference previously exclusive to data centers [38]. By processing data locally and transmitting only relevant insights, edge architectures dramatically reduce bandwidth consumption, particularly valuable in bandwidth-constrained environments.

Hybrid edge-cloud architectures leverage complementary strengths of both paradigms. Cloud computing provides unlimited scalable storage and computational resources for comprehensive analytics, large-scale model training, and long-term data retention, excelling at batch processing and complex analytics [39]. Edge computing delivers immediate insights and rapid response to time-sensitive events through local processing [40]. This distribution achieves both real-time operational responsiveness and deep analytical insights, with organizations reporting substantial savings in latency-sensitive operations [41]. Distributed computing frameworks enable seamless workload orchestration, dynamically placing tasks based on latency requirements, data locality, computational complexity, and available resources [42]. Stream processing architectures using message queuing systems like Kafka and RabbitMQ facilitate reliable data streaming with durability guarantees and exactly-once processing semantics, enabling continuous analysis for real-time threat detection and system optimization [43].

AI model deployment in distributed environments requires specialized microservices architectures where each model operates independently, enabling scaling and updates without affecting other components [44]. API gateways manage secure access with rate limiting, authentication, request routing, and protocol translation [45]. Container technologies combined with orchestration platforms like Kubernetes facilitate scalable serving with automated failover, ensuring availability during node failures while enabling dynamic scaling based on demand [46]. Federated learning represents an emerging paradigm for training models across decentralized devices while preserving privacy, with each device maintaining local data and sharing only model updates [47]. This approach is valuable for sensitive applications where privacy regulations prevent data centralization, incorporating differential privacy and secure aggregation for mathematical privacy guarantees.

Data privacy and regulatory compliance remain paramount in distributed architecture. Processing sensitive data at edge nodes minimizes transmission to centralized servers, reducing exposure and aligning with GDPR, HIPAA, and industry-specific regulations [48]. Edge computing supports data minimization by processing raw data locally and transmitting only derived insights or aggregate statistics [40]. However, distributed nature introduces security considerations as edge devices may be physically accessible to attackers [49]. Hardware-based security mechanisms including trusted execution environments and secure enclaves protect cryptographic keys and sensitive computations even if host systems are compromised, while device attestation protocols verify integrity before allowing network participation [50].

This communication infrastructure and security framework provides the essential foundation for deploying AI and quantum technologies in high-security domains. The convergence of quantum-resistant cryptography, AI-driven threat detection, and hybrid edge-cloud architecture creates resilient systems capable of addressing current threats while adapting to emerging challenges [51]. As demonstrated in subsequent sections, criminal justice systems exemplify the most demanding applications of these frameworks, where evidentiary integrity and constitutional privacy protections require absolute security guarantees alongside real-time processing capabilities.

3. AI IN CRIMINAL LAW AND THE EPISTEMOLOGICAL CRISIS

The integration of Generative AI into the legal profession has precipitated an epistemological crisis regarding the veracity of legal citations and the integrity of evidence. While initially heralded for its potential to democratize access to legal services, the deployment of Large Language Models (LLMs) has exposed severe vulnerabilities in the judicial process [52]. These vulnerabilities manifest primarily through the phenomenon of hallucination where probabilistic token generation masquerades as authoritative legal precedent and through the fabrication of synthetic evidence which threatens the foundational trust required for criminal adjudication [53].

The most consequential inflection points in this reckoning occurred with the *Mata v. Avianca* litigation adjudicated in the Southern District of New York [54]. This case serves as a paradigmatic example of the risks associated with unverified reliance on algorithmic text generation. The counsel for the plaintiff submitted a brief citing multiple judicial precedents including *Varghese v. China Southern Airlines* which were subsequently revealed to be entirely fictitious constructs generated by ChatGPT [55]. The mechanism of this failure lies in the architecture of the Transformer model which functions as a probabilistic engine predicting plausible token sequences rather than retrieving semantic truth [56]. This incident exposed the danger of automation bias where human operators disproportionately trust automated outputs. The ruling emphasized that while technology can assist in legal work the ultimate responsibility for accuracy remains a non-delegable duty of the human officer. Consequently, the court imposed a $5,000 fine on the attorneys involved and mandated remedial legal education [55], setting a concrete precedent for algorithmic negligence. Despite high-profile sanctions, the submission of hallucinated content has persisted into 2024 and 2025 in cases such as *Park v. Kim* and *Kruse v. Karlan* which suggests a fundamental gap in technological competence within the legal profession [57].

Parallel to textual hallucinations, the proliferation of AI-generated synthetic media presents a dual threat: it catalyzes novel forms of criminal conduct while simultaneously destabilizing established evidentiary standards. The democratization of generative adversarial networks (GANs) and diffusion models has lowered the technical barrier for creating hyper-realistic fabrications [56]. This capability has been weaponized particularly in the creation of Non-Consensual Intimate Imagery (NCII) and Child Sexual Abuse Material (CSAM) [58]. Reports indicate that the volume of AI-generated abuse material actioned by authorities doubled between 2024 and 2025 with the severity of content intensifying significantly [59]. The legal system has struggled to adapt because the velocity of deepfake dissemination outpaces traditional legislative processes, leaving victims with limited recourse [60]. To bridge this regulatory gap, the United States enacted the TAKE IT DOWN Act in May 2025 to criminalize the non-consensual publication of intimate digital forgeries while states like Pennsylvania and Washington have classified malicious deepfake creation as a felony [61]. In criminal trials the silent witness theory relies on the assumption that a photograph accurately depicts reality, but Generative AI shatters this assumption. Defense attorneys increasingly invoke the liar's dividend strategy where the mere existence of deepfake technology is used to cast doubt on authentic video evidence [62].

Governance of these technologies has coalesced around divergent regulatory frameworks. The Artificial Intelligence Act (EU AI Act) of the European Union finalized in 2024 adopts a risk-based approach that explicitly prohibits certain law enforcement applications [62]. Article 5 of the Act bans predictive policing systems that assess risk based solely on profiling or personality traits rather than objective facts [62, 63]. This prohibition reflects concerns that algorithmic bias may entrench historical injustices. Furthermore, the Act places strict limitations on Real-Time Remote Biometric Identification (RBI) in publicly accessible spaces permitting its use only for strictly defined exigencies such as preventing imminent terrorist threats [64]. This contrasts with the approach in China, where the judiciary has aggressively integrated AI to enforce judicial standardization under the principle of 'Same Case, Same Judgment' [65]. The Chinese court system employs AI-driven recommendation engines to mitigate human disparity in sentencing. However, strict utilitarian application is evolving; recent rulings like the 2024 Guangzhou Internet Court decision have established liability for AI platform providers, indicating that algorithmic efficiency must coexist with legal accountability [66].

Ultimately, whether adopting the EU's risk-based restrictions or China's integrationist strategy, all legal systems share a common fundamental challenge: the urgent need to construct procedural safeguards that prevent the erosion of judicial integrity by algorithmic probabilities.

4. QC AND THE CRISIS OF CRYPTOGRAPHIC SECURITY

While Generative AI presents immediate challenges to legal content, the maturation of QC poses a fundamental ontological threat to the security infrastructure underpinning the criminal justice system [73]. This threat is encapsulated by the HNDL strategy [74]. This doctrine involves the interception and storage of currently encrypted data by adversarial actors with the intent of decrypting it once a cryptographically relevant QC becomes available. For the legal sector, which handles data with long-term confidentiality requirements such as grand jury testimonies and national security evidence, the implications are catastrophic.

The security of modern digital communications relies predominantly on public-key cryptography schemes such as the Rivest–Shamir–Adleman (RSA) algorithm and Elliptic Curve Cryptography (ECC) [75]. These systems function as digital locks, deriving their security from the extreme computational difficulty of solving specific mathematical problems, such as integer factorization [76]. However, this assumption of security is negated by Shor's algorithm. Unlike classical methods, Shor's algorithm provides a quantum-mechanical shortcut that theoretically allows a computer with sufficient quotes to solve these problems in polynomial time, effectively shattering the cryptographic shield of current legal infrastructures [77]. The HNDL threat is an active operational reality driven by a dangerous chronological imbalance. Adversarial actors are incentivized to intercept encrypted traffic today because the required secrecy duration of sensitive legal data such as national security evidence or sealed testimonies often extends far beyond the timeline projected for the arrival of fault-tolerant quantum hardware. If law enforcement agencies transmit sensitive case files over standard connections today that data is effectively compromised relative to a future quantum adversary. Once the encryption algorithm is broken in the future, the adversary can retroactively decrypt the data harvested today, exposing secrets that were intended to remain confidential for decades. A secondary threat vector

Table 1: Chronology of AI Regulation and Case Law in Criminal Justice (2016–2025)

Year	Event or Legislation	Jurisdiction	Key Impact or Provision
2016	**ProPublica Analysis of COMPAS**	USA	Demonstrated that the COMPAS recidivism algorithm exhibited systematic racial bias against black defendants through higher false positive rates [67].
2019	**Justice Reform Act Article 33**	France	Criminalized the use of litigation analytics to predict the behavior of specific judges to preserve judicial independence and prevent judge profiling [68].
2020	**Clearview AI Data Scraping Scandal**	Global	Investigations revealed Clearview AI scrapped billions of images from social media for law enforcement use violating platform terms and privacy expectations [69].
2021	**Clearview AI Declared Illegal**	Canada/EU	Privacy authorities declared the scraping of facial images by Clearview AI illegal and established precedents against untargeted mass biometric surveillance [70].
2023	***Mata v. Avianca***	USA (SDNY)	Landmark sanctions against attorneys for submitting AI-hallucinated case citations establishing the non-delegable duty of verification [71].
2024	**EU AI Act Finalization**	EU	Established comprehensive prohibitions on predictive policing based on profiling and restricted real-time remote biometric identification under Article 5 [72].
2025	**TAKE IT DOWN Act**	USA	Federal statute criminalizing the non-consensual publication of intimate deepfakes and mandating platform removal mechanisms [61].

known as Harvest Now Forge Later (HNFL) poses risks to digital evidence integrity [78]. If adversaries recover private signing keys, they could forge digital signatures on evidence files devastating the chain of custody by making fabricated evidence appear mathematically authentic.

In response to this threat the National Institute of Standards and Technology (NIST) in the United States has led a global effort to standardize Post-Quantum Cryptography (PQC) [79]. In August 2024 NIST officially released the first three finalized standards comprising FIPS 203, FIPS 204, and FIPS 205 [80, 81]. FIPS 203 specifies the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) derived from CRYSTALS-Kyber which relies on the hardness of the Module Learning with Errors problem [80]. FIPS 204 and 205 specify algorithms for digital signatures essential for identity authentication [80, 81]. The transition to these standards represents a logistical undertaking of immense complexity. The US federal government through National Security Memorandum has mandated a migration timeline requiring National Security Systems (NSS) to transition to quantum-resistant algorithms by 2035 [82]. For law enforcement agencies this involves re-architecting Public Key Infrastructures (PKI) that have been in place for decades [83].

The impact of QC extends to digital forensics and the preservation of evidence. Digital signatures verify that a file has not been altered since collection [84]. If the underlying algorithms protecting these signatures are broken the legal validity of decades of digital evidence could be challenged. Defense attorneys could argue that evidence cannot be authenticated because the digital signature could have been forged by a quantum-enabled actor [85]. Digital forensic analysts and cybersecurity experts are exploring crypto-agility and quantum-resistant hash functions to mitigate this risk. The concept of Mosca's Theorem illustrates this urgency through a simple inequality [86]. If the time required to migrate to quantum-safe encryption (x) plus the duration for which data must remain secret (y) exceeds the time until a quantum threat arrives (z), then the system is technically already compromised (x+y>z). In other words, if it takes 10 years to upgrade systems and the data must be kept secret for 20 years, but a quantum computer arrives in 15 years, the data is currently defenseless against the future threat. For capital offense records and national security files requiring indefinite retention, this inequality confirms that the risk is active today [86].

5. QUANTUM MACHINE LEARNING AND THE EVOLUTION OF DIGITAL FORENSICS

Beyond the threat of encryption, QC offers transformative potential through Quantum Machine Learning (QML) particularly in the detection of complex financial crimes [87]. As criminal networks utilize sophisticated digital laundering techniques classical machine learning models often struggle with the high dimensionality and sparse data inherent in fraud detection. QML utilizes superposition and entanglement to process information in high-dimensional Hilbert spaces and offers a computational advantage in identifying subtle patterns of illicit activity [15, 17].

From a forensic standpoint, the efficacy of QML in identifying these patterns is fundamentally derived from the quantum kernel trick, which enables the mapping of evidentiary data into a 2^n-dimensional Hilbert space [17]. While classical models are often constrained by the computational cost of processing high-dimensional

Table 2: Timeline of QC and Cryptographic Milestones (2019–2035)

Year	Milestone	Entity	Significance
2019	**Quantum Supremacy Demonstration**	Google	The Sycamore processor performed a calculation faster than a classical supercomputer and validated the potential for quantum acceleration [90].
2022	**Quantum Cybersecurity Preparedness Act**	USA	Legislation mandated federal agencies inventing cryptographic systems and prepare for migration to post-quantum standards [74].
2023	**Second Quantum Revolution Report**	Europol	Analysis of the dual-use nature of quantum technologies identifying HNDL as a primary threat to law enforcement [91].
2024	**Logical Qubit Breakthrough**	Microsoft	Demonstration of reliable logical qubits with error rates 800 times lower than physical qubits moving toward fault tolerance [92].
2024	**NIST PQC Standards Finalization**	NIST	Official release of FIPS 203, 204, and 205 standards for quantum-resistant encryption and digital signatures [80].
2025	**EU PQC Implementation Roadmap**	EU	Publication of a coordinated roadmap requiring member states to transition critical infrastructure to post-quantum cryptography by 2030 [81].
2035	**Projected CNSA 2.0 Compliance**	NSA	Target deadline for full transition of National Security Systems to quantum-resistant algorithms anticipating the arrival of CRQCs [93].

feature spaces, which often result in the omission of subtle yet critical probative information, the quantum approach utilizes a parameterized quantum circuit to directly measure the fidelity between quantum states [88]. This mechanism effectively performs inner product calculations in a feature space that is exponentially larger than what is accessible to classical systems, thereby facilitating the linear separation of sophisticated criminal patterns. Consequently, this allows the judicial system to identify and verify intricate, non-linear correlations in financial crimes and criminal networks that would otherwise remain legally and technically indiscernible under current digital forensic standards [89].

One promising application is the use of Quantum Support Vector Machines (QSVM) for anomaly detection [94]. In financial datasets fraudulent transactions are rare outliers. Classical Support Vector Machines (CSVM) become computationally expensive when processing high-dimensional feature spaces [12]. QSVM utilizes a quantum kernel trick where data is mapped into an exponentially large quantum Hilbert space using a parameterized quantum circuit. In this space complex correlations invisible in classical dimensions can become linearly separable. Research conducted in 2024 and 2025 demonstrated that these models can achieve high precision in fraud classification with some studies reporting F1 scores of 0.98 [95, 96]. Quantum Principal Component Analysis (QPCA) further allows for dimensionality reduction in large datasets enabling investigators to isolate relevant features of criminal behavior [97].

In addition to fraud detection QC is being applied to the Topological Data Analysis (TDA) of criminal networks [98]. Criminal organizations operate as complex networks with specific structural characteristics. Understanding the topology of these networks is essential for identifying vulnerabilities. Quantum algorithms enhance TDA by allowing analysts to compute Betti numbers more efficiently than classical methods [99]. By analyzing the shape of the data these methods can identify critical nodes and vulnerabilities within a criminal network that are not apparent through standard centrality measures. Recent studies indicate that topological features remain robust even with incomplete data which makes this a valuable tool for intelligence analysis where data is often fragmentary.

Despite the transformative potential of QSVM and TDA in forensic science, their practical deployment remains constrained by the noise of NISQ devices. A primary theoretical hurdle in scaling these models is the Barren Plateau problem. This phenomenon refers to the tendency of the cost function landscape in Variational Quantum Algorithms (VQAs) to become exponentially flat as the number of qubits increases [100]. In a barren plateau, the gradients of the cost function vanish exponentially, making it impossible for the optimizer to determine the direction of improvement [101]. This issue is analogous to the vanishing gradient problem in classical deep learning but is more severe due to the geometry of the Hilbert space. Addressing this problem through strategies like local cost functions and identity block initialization is critical for the viability of Quantum Neural Networks (QNNs) in analyzing complex legal data [101].

6. CONCLUSION

The intersection of Generative AI and QC represents a critical juncture for the criminal justice

Table 3: Developments in Quantum Machine Learning for Forensics and Security (2018–2025)

Year	Research or Technological Development	Focus Area	Key Finding or Application
2018	**Barren Plateaus in QNNs**	Theory	McClean *et al.* identified the gradient vanishing problem in parameterized quantum circuits which poses a scaling challenge for QML [102].
2019	**Quantum-Enhanced Feature Spaces**	QML	Havlicek *et al.* demonstrated that quantum kernels can separate data that is classically hard to classify, laying the groundwork for QSVM [103].
2021	**Quantum Face Recognition Protocol**	Biometrics	Proposal for combining QPCA with Ghost Imaging to identify suspects in low-light environments [104].
2023	**Quantum Anomaly Detection for AML**	Finance	Collaboration between Rigetti and HSBC to develop quantum algorithms for detecting complex money laundering patterns [105].
2024	**Quantum Federated Learning**	Privacy	Development of privacy-preserving forensic analysis methods that allow decentralized training on sensitive criminal data [106].
2025	**Quorum Unsupervised Detection**	Anomaly Detection	Introduction of an unsupervised framework using quantum autoencoders to detect anomalies without labeled training data [107].
2025	**Quantum Graph Neural Networks (QGNN)**	Network Analysis	Application of QGNNs to identify synthetic identities and long-range dependencies in financial transaction graphs with high precision [108].

system characterized by a dual disruption that challenges both the methods of ascertaining truth and the means of securing it. The legal profession must fortify procedural defenses against the influx of AI-generated misinformation. The lessons of *Mata v. Avianca* underscore that while AI can augment legal intellect it cannot replace the ethical duty of verification. Legislative mandates such as the EU AI Act represent necessary steps in establishing a governance framework that prioritizes judicial integrity. Simultaneously, the justice system must prepare for the silent threat of quantum decryption. The Harvest Now Decrypt Later strategy ensures that the window for action is already open. The migration to NIST Post-Quantum Cryptography standards is a fundamental requirement for the preservation of justice and national security. Failure to secure the chain of custody against quantum forgery could lead to a retrospective collapse of evidentiary validity. The convergence of these technologies presents a paradox where AI offers to synthesize vast amounts of legal data while QC threatens to unravel the cryptographic trust securing that data. Resolution requires a justice system that is technologically literate and steadfast in its commitment to the verification of truth.

ACKNOWLEDGEMENTS

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

CONFLICT OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] Suganthi N, Sakila VS, Devika M, Mishra S, Regin R, Jayaprakash J: The Role of Wireless Sensor Networks in Contemporary Communication and Impact: The Next Steps for 5G. In: Machine Learning, Predictive Analytics, and Optimization in Complex Systems. IGI Global Scientific Publishing; 2026: 307-322. https://doi.org/10.4018/979-8-3373-5203-9.ch016

[2] Bala I: Quantum Computing in 5G Communication and Networks. In: From Bits to Qubits: The Quantum Transformation of Computing: The Power of Quantum Computing. Springer; 2026: 31-53. https://doi.org/10.1007/978-3-032-00586-1_2

[3] Raza R, Aadil F: A comprehensive survey on FANET-IoT-IoV interactions: challenges, opportunities, and future directions in 6G-enabled smart cities. Computing 2026, 108(1): 10. https://doi.org/10.1007/s00607-025-01602-z

[4] Morshedi R, Mojtaba Matinkhah S: Cybersecurity Challenges and Solutions in Unmanned Aerial Vehicles (UAVs). Journal of Field Robotics 2026, 43(1): 314-329. https://doi.org/10.1002/rob.70040

[5] Das C, Das B, Bose A, Mandal A, Mishra AK, Raghuvanshi C: Machine Learning-Driven Social IoT: Advancing Inter-Connectivity, Intelligence, and Autonomous Systems. In: Social Internet of Things (SIoT) and Machine Learning—Enhancing Interconnectivity and Intelligence. Springer; 2026: 189-209. https://doi.org/10.1007/978-3-032-10122-8_10

[6] Feng Y, Cheng Y, Yan X: Legal response to facial recognition technologies in China: still seeking the balance. Computer Law & Security Review 2026, 60: 106250. https://doi.org/10.1016/j.clsr.2025.106250

[7] Chen X, Dai M: Dilemmas of Facial Recognition Technology in Chinese Digital Policing: A Qualitative Exploration. Asian Journal of Criminology 2026, 21(1): 2. https://doi.org/10.1007/s11417-025-09473-1

[8] Mitzen J: Ontological security in world politics: State identity and the security dilemma. European journal of international relations 2006, 12(3): 341-370. https://doi.org/10.1177/1354066106067346

[9] Maschi T, Killian ML: The evolution of forensic social work in the United States: Implications for 21st century practice. Journal of Forensic Social Work 2011, 1(1): 8-36. https://doi.org/10.1080/1936928X.2011.541198

[10] Kang SJ, Shin H: Biophysical mechanisms of spider-silk constituting element-induced stick-slip behavior and hydrogen bond regeneration for high toughness in silk fibers. Int J Biol Macromol 2025, 322(Pt 4): 147027. https://doi.org/10.1016/j.ijbiomac.2025.147027

[11] Shin H, Yoon T, Yoon S: Fatigue life predictor: predicting fatigue life of metallic material using LSTM with a contextual attention model. RSC Adv 2025, 15(20): 15781-15795. https://doi.org/10.1039/D5RA01578B

[12] Shin H, Yoon T, You J, Na S: A study of forecasting the Nephila clavipes silk fiber's ultimate tensile strength using machine learning strategies. J Mech Behav Biomed Mater 2024, 157: 106643. https://doi.org/10.1016/j.jmbbm.2024.106643

[13] Shin H, Yoon T, Yoon S: Closed-form physics-informed extension of Griffith's law for HDPEC-retarded crack growth. Modern Physics Letters B 2026, 40(02): 2550272. https://doi.org/10.1142/S0217984925502720

[14] Yoon T, Shin H, Park W, Kim Y, Na S: Biochemical mechanism involved in the enhancement of the Young's modulus of silk by the SpiCE protein. J Mech Behav Biomed Mater 2023, 143: 105878. https://doi.org/10.1016/j.jmbbm.2023.105878

[15] Cho HH, Kim TH, Hwang SG, Shin H: AI and Quantum Computing for Advanced Materials Design. Journal of AI-Driven Communication Engineering 2025, 1: 8-17.

[16] Phillips J, Toltzis A, Fanous V, Lalsinghani G: The Darwinian Effect: The Weaponization of Artificial Intelligence by Cyber Criminals. Cal WL Rev 2024, 61: 43.

[17] Kang SJ, Shin H: Amino acid sequence-based IDR classification using ensemble machine learning and quantum neural networks. Comput Biol Chem 2025, 118: 108480. https://doi.org/10.1016/j.compbiolchem.2025.108480

[18] Mthembu L, Smith A: Impacts of Quantum Computing on Cryptographic Algorithms: Challenges and the Future of Cybersecurity. Global Research Perspectives on Cybersecurity Governance, Policy, and Management 2024, 8(12): 12-23.

[19] Olutimehin AT, Joseph S, Ajayi AJ, Metibemu OC, Balogun AY, Olaniyi OO: Future-proofing data: Assessing the feasibility of post-quantum cryptographic algorithms to mitigate 'harvest now, decrypt later'attacks. Decrypt Later'Attacks (February 17, 2025) 2025. https://doi.org/10.2139/ssrn.5141513

[20] Thayalan S, Radhakrishnan N, Ramana T, Devarajan GG, Karuppiah M, Al Dabel MM: Real-Time Threat Detection and AI-Driven Predictive Security for Consumer Applications. IEEE Transactions on Consumer Electronics 2025. https://doi.org/10.1109/TCE.2025.3554589

[21] Ambedkar BR: Efficient Exploration of Secure Socket Layer at Transport Layer Security. Knowledgeable Research A Multidisciplinary Journal 2025, 3(06): 1-6.

[22] Singh M, Sood SK, Bhatia M: Post-quantum cryptography: a review on cryptographic solutions for the era of quantum computing. Archives of Computational Methods in Engineering 2025: 1-42. https://doi.org/10.1007/s11831-025-10412-7

[23] Ahmed N, Zhang L, Gangopadhyay A: A survey of post-quantum cryptography support in cryptographic libraries. In: 2025 IEEE International Conference on Quantum Computing and Engineering (QCE): 2025. IEEE: 906-917. https://doi.org/10.1109/QCE65121.2025.00102

[24] Mummadi S, Fathima S: A Comprehensive Study on Quantum Key Distribution Protocols. In: 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT): 2024. IEEE: 1-8. https://doi.org/10.1109/ICCCNT61001.2024.10726153

[25] Arslan R, Özseven T, Aydın MM: Transforming European Cybersecurity: AI-Powered Threat Analysis, Quantum Age, Blockchain/Crypto Risks, and Regulatory Strategies. International Journal of Engineering and Applied Sciences 2025, 17(2): 81-93. https://doi.org/10.24107/ijeas.1619600

[26] Zhang J, Xiao X, Ren W, Zhang Y: Privacy-preserving feature extraction for medical images based on fully homomorphic encryption. Journal of Advanced Computing Systems 2024, 4(2): 15-28. https://doi.org/10.1051/sands/2024012

[27] Khan S: Secure Multi-Party Computation for Privacy Preservation in Big Data Analytics. Journal of Big Data Privacy Management 2024, 2(02): 168-179.

[28] Biswas S, Raj MWZ: Quantum-Resistant Cryptographic Protocols Integrated with AI for Securing Cloud and IOT Environments. International Journal of Business and Economics Insights 2024, 4(4): 60-90. https://doi.org/10.63125/dryw3b96

[29] Nagarajan J, Mansourian P, Shahid MA, Jaekel A, Saini I, Zhang N, Kneppers M: Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey. Peer-to-Peer Networking and Applications 2023, 16(5): 2153-2185. https://doi.org/10.1007/s12083-023-01508-7

[30] Shin, H., Park, Y., Yeom, J., Na, S., & Yoon, T. (2026). Systematic Evaluation of Attention Mechanisms in Transformer Models for De Novo UTS-Driven Silk Protein Sequence Design. Journal of Computational Design and Engineering, qwag002. https://doi.org/10.1093/jcde/qwag002

[31] Shin, H., Yoon, T., Park, W., You, J., & Na, S. (2024). Unraveling the Mechanical Property Decrease of Electrospun Spider Silk: A Molecular Dynamics Simulation Study. ACS Applied Bio Materials, 7(3), 1968-1975. https://doi.org/10.1021/acsabm.4c00046

[32] Sarhan M, Layeghy S, Moustafa N, Portmann M: Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. Journal of Network and Systems Management 2023, 31(1): 3. https://doi.org/10.1007/s10922-022-09691-3

[33] Alomari AH, Subramaniam SK, Samian N, Latip R, Zukarnain ZA: Dual-phase resource allocation algorithm in software-defined network SDN-enabled cloud. IEEE Access 2023, 11: 102301-102315. https://doi.org/10.1109/ACCESS.2023.3315856

[34] Nezamoddini N, Gholami A: A survey of adaptive multi-agent networks and their applications in smart cities. Smart Cities 2022, 5(1): 318-347. https://doi.org/10.3390/smartcities5010019

[35] Wang C, Yu J, Pei Z, Wang Q, Hong C: A first successful factorization of RSA-2048 integer by D-Wave quantum computer. Tsinghua Science and Technology 2024, 30(3): 1270-1282. https://doi.org/10.26599/TST.2024.9010028

[36] Kute S, Desai C, Jadhav M: Analysis of RSA and Shor's algorithm for cryptography: A quantum perspective. In: AIP Conference Proceedings: 2024. AIP Publishing LLC: 040004. https://doi.org/10.1063/5.0227773

[37] Ahmed F: Quantum-resistant cryptography for national security: A policy and implementation roadmap. Int J Multidisciplinary on Science and Management 2024, 1(4): 54-65.

[38] Caiazza C, Giordano S, Luconi V, Vecchio A: Edge computing vs centralized cloud: Impact of communication latency on the energy consumption of LTE terminal nodes. Computer Communications 2022, 194: 213-225. https://doi.org/10.1016/j.comcom.2022.07.026

[39] Infant DD, Priyanka E: Enabling Smart Cities: A Comprehensive Study of IoT and IIoT Integration in Diverse Industries. In: Deep Learning and Blockchain Technology for Smart and Sustainable Cities. Auerbach Publications: 89-114. https://doi.org/10.1201/9781003476047-6

[40] Mukherjee S, Gupta S, Rawlley O, Jain S: Leveraging big data analytics in 5G-enabled IoT and industrial IoT for the development of sustainable smart cities. Transactions on Emerging Telecommunications Technologies 2022, 33(12): e4618. https://doi.org/10.1002/ett.4618

[41] Demirbaga Ü, Aujla GS, Jindal A, Kalyon O: Cloud computing for big data analytics. In: Big data analytics: Theory, techniques, platforms, and applications. Springer; 2024: 43-77. https://doi.org/10.1007/978-3-031-55639-5_4

[42] Bablu TA, Rashid MT: Edge computing and its impact on real-time data processing for IoT-driven applications. Journal of advanced computing systems 2025, 5(1): 26-43.

[43] Jonnalagadda AMC: Integrating AI and Cloud Technologies for Scalable, Low-Latency Edge Computing in Enterprise Workloads. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM) 2025, 8(3): 12110-12120.

[44] Rajesh SC, Goel L: Architecting Distributed Systems for Real-Time Data Processing in Multi-Cloud Environments. Int J Emerg Technol Innov Res 2025, 12: b623-b640.

[45] Bux R, Shenoy GS: Performance analysis of RESTFUL web services and RABBITMQ for microservices based systems on cloud environment. In: 2024 3rd International Conference for Innovation in Technology (INOCON): 2024. IEEE: 1-6. https://doi.org/10.1109/INOCON60754.2024.10511747

[46] Al-Doghman F, Moustafa N, Khalil I, Sohrabi N, Tari Z, Zomaya AY: AI-enabled secure microservices in edge computing: Opportunities and challenges. IEEE Transactions on Services Computing 2022, 16(2): 1485-1504. https://doi.org/10.1109/TSC.2022.3155447

[47] Hindka M: Securing the Digital Backbone: An In-depth Insights into API Security Patterns and Practices. Computer Science and Engineering 2024, 14(2): 35-41. https://doi.org/10.5923/j.computer.20241402.02

[48] Aruna K, Gurunathan P: Enhancing Edge Environment Scalability: Leveraging Kubernetes for Container Orchestration and Optimization. Concurrency and Computation: Practice and Experience 2024, 36(28): e8303. https://doi.org/10.1002/cpe.8303

[49] Beltrán ETM, Pérez MQ, Sánchez PMS, Bernal SL, Bovet G, Pérez MG, Pérez GM, Celdrán AH: Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges. IEEE Communications Surveys & Tutorials 2023, 25(4): 2983-3013. https://doi.org/10.1109/COMST.2023.3315746

[50] Ahmed A, Shahzad A, Naseem A, Ali S, Ahmad I: Evaluating the effectiveness of data governance frameworks in ensuring security and privacy of healthcare data: A quantitative analysis of ISO standards, GDPR, and HIPAA in blockchain technology. PLoS One 2025, 20(5): e0324285. https://doi.org/10.1371/journal.pone.0324285

[51] Ferrag MA, Friha O, Kantarci B, Tihanyi N, Cordeiro L, Debbah M, Hamouda D, Al-Hawawreh M, Choo K-KR: Edge learning for 6G-enabled Internet of Things: A comprehensive survey of vulnerabilities, datasets, and defenses. IEEE Communications Surveys & Tutorials 2023, 25(4): 2654-2713. https://doi.org/10.1109/COMST.2023.3317242

[52] Arshad A, Shaan M, Ahmed HM, Iqbal M: Exploring Secure Processing Architecture: A Comprehensive Review. Dialogue Social Science Review (DSSR) 2025, 3(1): 476-491.

[53] Ofili BT, Obasuyi OT, Akano TD: Edge Computing, 5G, and Cloud Security Convergence: Strengthening USA's Critical Infrastructure Resilience. Int J Comput Appl Technol Res 2023, 12(9): 17-31.

[54] Becher S, Alarie B: LexOptima: The promise of AI-enabled legal systems. University of Toronto Law Journal 2025, 75(1): 73-121. https://doi.org/10.3138/utlj-2024-0002

[55] Quevedo E, Salazar JY, Koerner R, Rivas P, Cerny T: Detecting hallucinations in large language model generation: A token probability approach. In: World Congress in Computer Science, Computer Engineering & Applied Computing: 2024. Springer: 154-173. https://doi.org/10.1007/978-3-031-86623-4_13

[56] Loftus ME: Am I Allowed to Use Artificial Intelligence?: Federal Courts, State Bars, and the Department of Justice on Generative Artificial Intelligence. Dep't of Just J Fed L & Prac 2025, 73: 139.

[57] Roscoe L: Contrasting AI and Human Hallucinations. Berkeley Scientific Journal 2025, 29(2). https://doi.org/10.5070/BS329265614

[58] Nayak DSK, Das R, Sahoo SK, Swarnkar T: ARGai 1.0: A GAN augmented in silico approach for identifying resistant genes and strains in E. coli using vision transformer. Comput Biol Chem 2025, 115: 108342. https://doi.org/10.1016/j.compbiolchem.2025.108342

[59] Browning JG: The Dawn of the" AI Judge"? Generative Artificial Intelligence and its Impact on Appellate Courts. J App Prac & Process 2025, 25: 341.

https://doi.org/10.1201/9781003621454-22

[60] Valentine D, d'Auvergne M: Combatting non-consensual intimate imagery in the Commonwealth Caribbean: Overcoming Legislative Gaps with Creative Approaches. The UWI St Augustine Law Journal 2024, 2(1): 42-55.

[61] ROCHMAN A: "Unwilling Avatars" revisited: A technical, legal, and social analysis of AI-generated nonconsensual intimate imagery. 2025.

[62] Whyte C: Deepfake news: AI-enabled disinformation as a multi-level public policy challenge. Journal of cyber policy 2020, 5(2): 199-217. https://doi.org/10.1080/23738871.2020.1797135

[63] Grimmelmann J: Deconstructing the Take It Down Act. Communications of the ACM 2025, 68(8): 28-30. https://doi.org/10.1145/3747203

[64] Apolo Y, Michael K: Beyond a reasonable doubt? Audiovisual evidence, AI manipulation, deepfakes, and the law. IEEE Transactions on Technology and Society 2024, 5(2): 156-168. https://doi.org/10.1109/TTS.2024.3427816

[65] Kalodanis K, Rizomiliotis P, Anagnostopoulos D: European artificial intelligence act: an AI security approach. Information & Computer Security 2024, 32(3): 265-281. https://doi.org/10.1108/ICS-10-2022-0165

[66] Kieslich K, Lünich M: Regulating ai-based remote biometric identification. investigating the public demand for bans, audits, and public database registrations. In: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency: 2024. 173-185. https://doi.org/10.1145/3630106.3658548

[67] Liu N: A Vulnerable Justice: Finality of Civil Judgments in China. Colum J Asian L 1999, 13: 35.

[68] Peng Y, Yan W: Embracing AI in Arbitration: Chinese Prospect–Navigating Challenges and Forging Pathways. International Journal of Digital Law and Governance 2025(0). https://doi.org/10.1515/ijdlg-2025-0017

[69] Washington AL: How to argue with an algorithm: Lessons from the COMPAS-ProPublica debate. Colo Tech LJ 2018, 17: 131.

[70] Ciuriak D, Rodionova V: Trading AI: Economic interests, societal choices and multilateral rules. Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration," Cambridge University Press (forthcoming) 2020. https://doi.org/10.1017/9781108954006.005

[71] Lala F: Data collection via web scraping: privacy and facial recognition after Clearview. i-lex 2023, 16(2): 34-45.

[72] Jung WK, Kwon HY: Privacy and data protection regulations for AI using publicly available data: Clearview AI case. In: Proceedings of the 17th International Conference on Theory and Practice of Electronic Governance: 2024. 48-55. https://doi.org/10.1145/3680127.3680200

[73] Norton CA, Rapoport NB: Doubling Down on Dumb: Lessons from Mata v. Avianca Inc. American Bankruptcy Institute Journal 2023, 42(8): 24-61.

[74] Kilian R, Jäck L, Ebel D: European ai standards–technical standardisation and implementation challenges under the eu ai act. European Journal of Risk Regulation 2025, 16(3): 1038-1062. https://doi.org/10.1017/err.2025.10032

[75] Shafik W: Quantum Computing and Generative Adversarial Networks (GANs): Ethics, Privacy, and Security. In: Quantum AI and its Applications in Blockchain Technology. IGI Global Scientific Publishing; 2025: 111-156. https://doi.org/10.4018/979-8-3373-1657-4.ch007

[76] Erol V: The Strategic Imperative of Quantum Readiness: A Comprehensive Review of Post-Quantum Cryptography. 2025. https://doi.org/10.20944/preprints202509.1720.v1

[77] Barrett P: Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor. In: Conference on the Theory and Application of Cryptographic Techniques: 1986. Springer: 311-323. https://doi.org/10.1007/3-540-47721-7_24

[78] Rushdi AMA, Zagzoog SS: Design of a digital circuit for integer factorization via solving the inverse problem of logic. Journal of Advances in Mathematics and Computer Science 2018, 26(3): 1-14. https://doi.org/10.9734/JAMCS/2018/39285

[79] Monz T, Nigg D, Martinez EA, Brandl MF, Schindler P, Rines R, Wang SX, Chuang IL, Blatt R: Realization of a scalable Shor algorithm. Science 2016, 351(6277): 1068-1070. https://doi.org/10.1126/science.aad9480

[80] Kao L: Quantum-Adversary-Resilient Evidence Structures and Migration Strategies for Regulated AI Audit Trails. arXiv preprint arXiv: 251200110 2025.

[81] Moody D, Alagic G, Alperin-Sheriff J, Apon D, Cooper D, Dang Q, Liu Y-K, Miller C, Peralta R, Perlner R: Status report on the first round of the nist post-quantum cryptography standardization process. In.: Technical report, National Institute of Standards and Technology; 2019. https://doi.org/10.6028/NIST.IR.8240

[82] Marmebro A, Stenbom K: Investigation of Post-Quantum Cryptography (FIPS 203 & 204) Compared to Legacy Cryptosystems, and Implementation in Large Corporations. In.; 2024.

[83] Lee Y-S, Tso R: Post-Quantum Cryptography (PQC) Migration Guide for Financial Institutions. Communications of the CCISA 2025, 31(1): 45-55.

[84] Jung E: The Impact of Quantum Information Science and Technology on National Security. Purdue University; 2024.

[85] Ellison C, Schneier B: Ten risks of PKI: What you're not being told about public key infrastructure. Comput Secur J 2000, 16(1): 1-7.

[86] Shatha A, Khaled E, Abdelrahman E: Digital Forensics of Quantum Computing: The Role of Quantum Entanglement in Digital Forensics—Current Status and Future Directions. Quantum Reports 2025, 7(4): 44. https://doi.org/10.3390/quantum7040044

[87] Uphoff RJ, Wood PB: The allocation of decisionmaking between defense counsel and criminal defendant: an empirical study of attorney-client decisionmaking. U Kan L Rev 1998, 47: 1.

[88] Kiviharju M: Refining Mosca's Theorem: Risk Management Model for the Quantum Threat Applied to IoT Protocol Security. In: Cyber Security: Critical Infrastructure Protection. Springer; 2022: 369-401. https://doi.org/10.1007/978-3-030-91293-2_16

[89] Cardaioli M, Marangoni L, Martini G, Mazzolin F, Pajola L, Parodi AF, Saitta A, Vernillo MC: FD4QC: Application of Classical and Quantum-Hybrid Machine Learning for Financial Fraud Detection A Technical Report. arXiv preprint arXiv: 250719402 2025.

[90] Benedetti M, Lloyd E, Sack S, Fiorentini M: Parameterized quantum circuits as machine learning models. Quantum science and technology 2019, 4(4): 043001. https://doi.org/10.1088/2058-9565/ab4eb5

[91] Dahbur K, Muscarello T: Classification system for serial criminal patterns. Artificial Intelligence and Law 2003, 11(4): 251-269. https://doi.org/10.1023/B:ARTI.0000045994.96685.21

[92] Arute F, Arya K, Babbush R, Bacon D, Bardin JC, Barends R, Biswas R, Boixo S, Brandao FG, Buell DA: Quantum supremacy using a programmable superconducting processor. Nature 2019, 574(7779): 505-510. https://doi.org/10.1038/s41586-019-1666-5

[93] Macci F: The Use of Quantum-Based Technologies for Secure Satellite Communications in Support of European Union Space Security and Defence. 2023.

[94] Paetznick A, da Silva M, Ryan-Anderson C, Bello-Rivas J, Campora III J, Chernoguzov A, Dreiling J, Foltz C, Frachon F, Gaebler J: Demonstration of logical qubits and repeated error correction with better-than-physical error rates. arXiv preprint arXiv: 240402280 2024.

[95] Campbell R: The Next-Generation Security Triad: Unifying PQC, ZTA, and AI Security through a Shared Modernization Substrate. 2025. https://doi.org/10.20944/preprints202512.0653.v1

[96] Rebentrost P, Mohseni M, Lloyd S: Quantum support vector machine for big data classification. arXiv preprint arXiv: 13070471 2013. https://doi.org/10.1103/PhysRevLett.113.130503

[97] Al-Maari A-A, Abdulnabi M, Nathan Y, Ali A, Ali U, Khan M: Optimized Credit Card Fraud Detection Leveraging Ensemble Machine Learning Methods. Engineering, Technology & Applied Science Research 2025, 15(3): 22287-22294. https://doi.org/10.48084/etasr.10287

[98] Reams TS, Carter A: Machine Learning in Finance: Evidence from Risk, Fraud, and Sentiment. Authorea Preprints 2025. https://doi.org/10.36227/techrxiv.175979238.85120535/v1

[99] Lloyd S, Mohseni M, Rebentrost P: Quantum principal component analysis. Nature physics 2014, 10(9): 631-633. https://doi.org/10.1038/nphys3029

[100] Gyurik C, Cade C, Dunjko V: Towards quantum advantage via topological data analysis. Quantum 2022, 6: 855. https://doi.org/10.22331/q-2022-11-10-855

[101] Friedman J: Computing Betti numbers via combinatorial Laplacians. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing: 1996. 386-391. https://doi.org/10.1145/237814.237985

[102] Cerezo M, Arrasmith A, Babbush R, Benjamin SC, Endo S, Fujii K, McClean JR, Mitarai K, Yuan X, Cincio L: Variational quantum algorithms. Nature Reviews Physics 2021, 3(9): 625-644. https://doi.org/10.1038/s42254-021-00348-9

[103] Qi H, Wang L, Zhu H, Gani A, Gong C: The barren plateaus of quantum neural networks: review, taxonomy and trends. Quantum Information Processing 2023, 22(12). https://doi.org/10.1007/s11128-023-04188-7

[104] McClean JR, Boixo S, Smelyanskiy VN, Babbush R, Neven H: Barren plateaus in quantum neural network training landscapes. Nature communications 2018, 9(1): 4812. https://doi.org/10.1038/s41467-018-07090-4

[105] Havlíček V, Córcoles AD, Temme K, Harrow AW, Kandala A, Chow JM, Gambetta JM: Supervised learning with quantum-enhanced feature spaces. Nature 2019, 567(7747): 209-212. https://doi.org/10.1038/s41586-019-0980-2

[106] Zhu Z, Yang X, Lu R, Shen T, Zhang T, Wang S: Ghost imaging in the dark: A multi-illumination estimation network for low-light image enhancement. IEEE Transactions on Circuits and Systems for Video Technology 2024. https://doi.org/10.1109/TCSVT.2024.3472278

[107] Mercadier M: Quantum-enhanced versus classical Support Vector Machine: An application to stock index forecasting. Available at SSRN 4630419 2023. https://doi.org/10.2139/ssrn.4630419

[108] Iyengar S, Nabavirazavi S, Hariprasad Y, HB P, Mohan CK: Privacy-Preserving AI (Federated Learning) for Digital Forensics. In: Artificial Intelligence in Practice: Theory and Application for Cyber Security and Forensics. Springer; 2025: 161-176. https://doi.org/10.1007/978-3-031-89327-8_5

[109] Ludmir JZ, Rebello S, Ruiz J, Patel T: Quorum: Zero-Training Unsupervised Anomaly Detection using Quantum Autoencoders. arXiv preprint arXiv: 250413113 2025. https://doi.org/10.1109/DAC63849.2025.11132860

[110] Basa AN: The Role of Quantum Neural Networks in Fraud Detection: Opportunities and Challenges.

https://doi.org/10.31875/2979-1081.2026.02.01