Quantum Artificial Intelligence (AI) for Advanced Authentication Systems

***Dragan Korać**
University of Banja Luka,
*E-mail: dragan.korac@pmf.unibl.org

Cong Pu
Oklahoma State University, USA
cong.pu@outlook.com

Hamid R. Arabnia
University of Georgia, Athens, USA
hra@uga.edu

Abstract The advancement of Quantum Computing (QC) and Artificial Intelligence (AI) technologies, which together form a new transformative paradigm known as Quantum Artificial Intelligence (QAI), poses several challenges for authentication systems. To tackle these challenges, we first illustrate where the authentication process fits within the Quantum Identity Management (QIdM) framework. We then describe and clearly differentiate the key elements involved, such as quantum credentials, identifiers, and attributes. Next, we provide a detailed analysis of QAI influence on advanced authentication systems, highlighting key quantum transformation effects on AI technologies related to defensive strategies and attack vectors. Given that we present the mathematical foundations of quantum computational power, highlighting polynomial time complexity as a benchmarked advantage over exponential classical complexity; hence, we illustrate this comparison through a practical example showing how quantum algorithms scale more efficiently as problem size increases. We also provide a comparison between QAI and classical computing in authentication approaches, highlighting why quantum technologies with their unique quantum properties (e.g., superposition and entanglement) pose a potential threat to classical cryptography algorithm-enhanced multifactor authentication (MFA) solutions. Finally, we discuss the current QAI challenges and limitations in authentication approaches and outline future research directions with the aim of paving the path for fully exploiting quantum advantages in authentication systems.

Key words Quantum artificial intelligence (QAI), Authentication systems, Quantum attack vectors, Cybersecurity.

1. Introduction

In the era of modern digital transformations, quantum computing (QC) and artificial intelligence (AI), as two of the most dynamic and influential research intersection frontiers, have the potential to leverage breakthroughs from each domain, thereby inaugurating an entirely new computational paradigm known as quantum artificial intelligence (QAI) (Acampora et al., 2026). Advancements in QC have prompted the research community to reevaluate traditional authentication solutions in environments that are susceptible to quantum threat vectors (Pu et al., 2026). Given that QC and AI have distinct technological frontiers, their synergistic convergence within the intersectional domain of QAI has significant dual benefits (Klusch et al., 2024) as given in Figure 1. QAI has enormous potential to transform various sectors, including cybersecurity, healthcare, Internet of Things (IoT), and metaverse (Sharma et al., 2026; Sunki et al., 2025; Tuli et al., 2024). In communication networks, QAI brings a specific challenge associated with identity management systems (IdM), particularly with secure and efficient authentication processes (Ma et al., 2020, Xue et al., 2019).

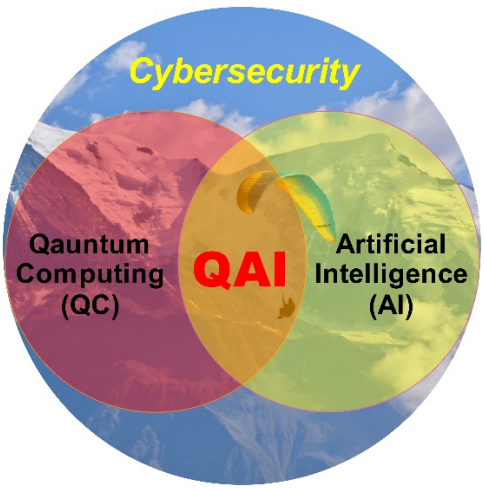

Fig. 1. Illustration of the synergistic convergence of QAI.

Authentication processes serve as a key element in protecting communication networks (Zhu et al., 2025), functioning as the first line of defense in cybersecurity strategies (Ghaemi et al., 2024). Besides security, there are many other user priorities (e.g., privacy, trust, safety, complexity, accessibility, convenience, complexity, etc.) that play a key role in the selection and development of authentication solutions (Stylios et al., 2021; Korać et al., 2022; Furnell & Helkala, 2022; Korać et al., 2025a). Today, numerous robust multifactor authentication (MFA) solutions are based on different frameworks, such as Public Key Infrastructure (PKI) that employs asymmetric cryptographic algorithms, including Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) (Buchmann et al., 2013). Although these conventional solutions demonstrate robustness against current attack vectors (e.g., brute-force, replay, man-in-the-middle (MiTM), and analytical attacks), they remain vulnerable to emerging threat vectors in QC environments (Kim and Park, 2025; Çakir and Tolga, 2026). The substantial reason is superior QC capabilities based on discrete mathematical logarithms and factorization (Alzahrani, 2025; Wang et al., 2025; Kasse and Mboup, 2025).

Table 1 The list of acronyms

Acronyms	Explanation	Acronyms	Explanation
AES	*Advanced Encryption Standard*	*PKI*	*Public Key Infrastructure*
AI	*Artificial Intelligence*	*PQC*	*Post-Quantum Cryptographic*
ECC	*Elliptic Curve Cryptosystem*	*QAI*	*Quantum Artificial Intelligence*
IdM	*Identity Management*	*QAOA*	*Quantum Approximate Optimization Algorithm*
IoD	*Internet of Drone,*	*QC*	*Quantum computing*
IoHT	*Internet of Health Thing*	*QIdM*	*Quantum Identity Management*
IoT	*Internet of Thing*	*QKD*	*Quantum Key Distribution*
IoTD	*IoT Device*	*Q-PUF*	*Quantum Physical Unclonable Function*
IoV	*IoT Vehicle*	*QRNG*	*Quantum Random Number Generation.*
MFA	*Multifactor Authentication*	*RSA*	*Rivest-Shamir-Adleman*
MiTM	*Man-in-The-Middle*	*SSO*	*Single Sign-On*
OTP	*One Time Password*	*VQE*	*Variational Quantum Eigensolver*

Nevertheless, the enormous computational power of QAI not only raises security challenges but also ethical issues related to bias, fairness, transparency, and sustainability (Rodríguez-Pérez et al., 2021). As the rapid technological evolution underlying QAI has exposed fundamental limitations in existing methodological frameworks for addressing ethical and security concerns; hence, there is a critical need for interdisciplinary collaboration to systematically integrate ethical principles into QAI development while promoting transparency, inclusivity, and equitable global access (Bano et al., 2025). The power and development of QAI represent not only a significant theoretical issue but also a significant practical authentication challenge. Despite rapid advancements in QC and AI technologies, their enduring influence on cybersecurity remains undetermined (de Jong, 2022). The importance and urgency of research into QAI-enhanced cybersecurity have been highlighted as a key priority in combating emerging vector-based threats (Wang et al., 2025; Tandel and Nasriwala, 2025; Balasubramanian et al., 2025). The list of key acronyms used in this research is given in Table 1. In summary, we present the following key contributions:

- Present an overview and description of QAI, highlighting its current significance in the authentication approaches as an unexplored area.
- Give an overview of the Quantum Identity Management (QIDM) framework and the role of AI in authentication approaches, illustrating the positioning of authentication processes within the IdM system.
- Provide a mathematical representation of QAI with a unique computational complexity benchmark.
- Compare QC and classical computing in authentication approaches, highlighting their key transformative effects.
- Discuss the challenges and limitations of QAI in authentication systems, providing clearly defined future research directions.

The remaining part of this work is structured as presented in Figure 1. Section 2 describes related work, while Section 3 illustrates the preliminary background, highlighting the overview of the basics of the QIdM framework and the AI role as well. Section 4 provides a mathematical representation of QAI and a computational complexity benchmark. The comparison of QC and classical computing in authentication approaches, along with the transformative effects of QAI, is presented in Section 5. Discussion, including QAI challenges and limitations and future work, is given in the two last sections.

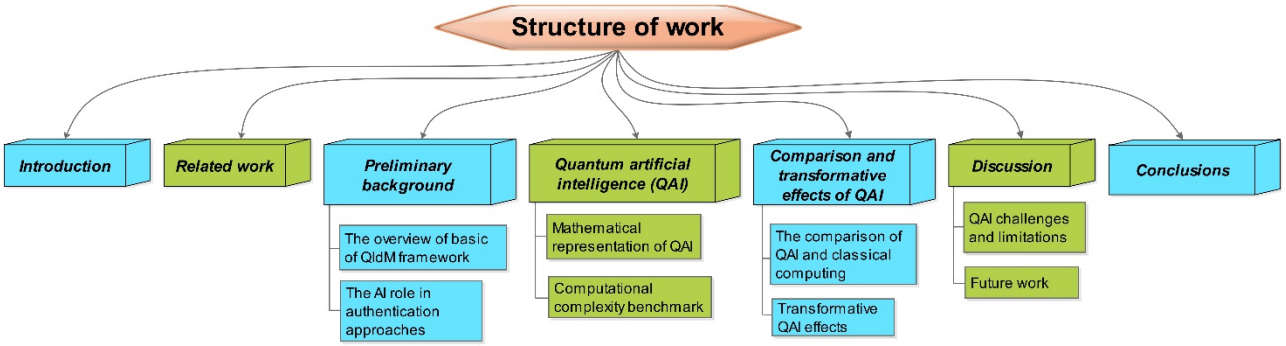

Fig. 2. Structure of this work.

2. Related work

Even though QAI technologies are relatively new, their roles and significance in authentication approaches have been extensively studied in recent years. There have also been attempts to explore QAI in cybersecurity by introducing frameworks tailored to specific contexts. For example, Aragona and Acampa, (2026); Illiano et al., (2022); Pirandola and Braunstein, (2016); Wu et al., (2025); Radanliev (2024) studied the concept of convergence of QC and AI through identifying key vulnerabilities and recommending integrated ethical and security strategies in national security and critical infrastructure (like quantum internet). Also, Alzahrani, 2025 presented an integrated framework for QC and AI with the aim of improving security in IoT environments. Singh and Kumar 2024; Paul et al. 2025; Rawat et al. 2022 addressed security risks and ethical trade-offs related to QC, highlighting the vulnerabilities of classical cryptographic algorithms. Sood and Chauhan, (2024) explored key technical challenges in QC, including quantum processors, qubit coherence, hardware stability, and error correction. Alexeev et al., (2025) addressed the development of quantum supercomputers, focusing on fault-tolerant quantum hardware. Ahmad and Srirangan, (2025) examined vulnerabilities of quantum attacks in the Internet of Health Things (IoHT), proposing a blockchain-driven mutual authentication scheme that removes the need for classical cryptographic algorithms such as RSA and ECC.

There have been numerous studies primarily focused on developing protocols based on mutual authentication in different fields (e.g., Internet of Drones (IoD), Internet of Things (IoT), and IoT Devices (IoTDs) and Internet of vehicle (IoV)). For example, in the works of Pu et al., (2026a); Nasajpour et al., (2020); Pu et al., (2022); Korać et al., (2025); Yazdinejad et al., (2019); Bhattarai et al., (2024); Li et al., (2022); Ma et al., (2019); Korać and Simić, (2019); Wu et al., (2021), the authors developed specific authentication protocols in which, besides vulnerability issues, they analyzed the other issues related to computation and communication costs. Moreover, there have also been research efforts to investigate AI as a primary task in cybersecurity. For example, Kaur et al., (2023) investigated how AI contributes to task automation, faster identification of threat vectors, and enhanced accuracy in cybersecurity defense. Hoffmann and Flother 2024; Umbrello 2024 addressed QAI through the prism of ethical issues responsible governance, and inclusion. In works of Kop et al., (2023) and Albusays et al., (2021), authors investigated issues of QAI algorithmic bias, fairness, and transparency, while Biamonte et al. (2017) presented the impact of QC on AI, focusing on the analysis and processing of massive volumes of information. Sarkar (2024) focused on the bias issue in QAI models through using training datasets, while Shams et al., (2023) explored QAI through issues of explainability and auditability.

Literature analysis showed that the previous works highlighted key contributions to QAI in cybersecurity, each aiming to address specific issues from its own perspective; however, there remains a unique need for a comprehensive exploration of the significance and importance of QAI in authentication approaches, which is the main focus of this research.

3. Preliminary background

This section provides the overview of the QIdM framework and the AI role in authentication approaches.

3.1. The overview of the QIdM framework

This subsection provides an overview of the QIdM framework (as illustrated in Figure 3), with the aim of illustrating QC-enhanced authentication processes as a key tool for connection between entity and system within authentication systems. The QIdM processes highlight the close relationship between authentication and identification, despite the fact

that they are fundamentally different processes: identification occurs before authentication, while authorization takes place after authentication. Specifically, authentication systems within the QIdM framework are responsible for verifying the entities (e.g., users, devices, or services) by leveraging quantum-based principles alongside classical authentication methods. Given that QIdM exploits quantum properties (e.g., superposition, entanglement, and the no-cloning theorem) to enhance authentication processes between entities and systems; thereby, it enables the creation of more resilient systems against various attack vectors (e.g., impersonation, replay attacks, and eavesdropping). Within the QIdM framework, authentication typically involves quantum key distribution (QKD), quantum challenge/response protocols, or hybrid quantum-classical authentication methods to ensure secure, tamper-proof identity validation.

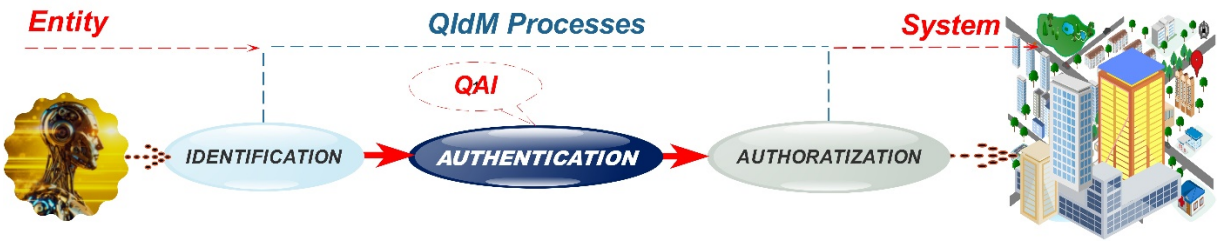

Fig. 3. Illustration of the QIdM framework.

The basic elements in QIdM processes (illustrated in Figure 4) include quantum credentials, identifiers, and attributes, each serving a distinct purpose within authentication systems. Quantum credentials, as a shared critical resource across entities and systems, represent a primary target for cyber attackers aiming to change, corrupt, or exfiltrate sensitive information. The motivations behind such attacks are diverse, encompassing financial gain, reputational damage and unauthorized access to digital assets, dissemination of fake information, and the manipulation of public or political opinion (Korać et al., 2022a). It is important to point out that the identification and authentication processes use quantum credentials, but the key point is that both processes are fundamentally different and should not be used interchangeably. QKD provides a theoretically unbreakable method for secure communication by enabling the trustworthy exchange of cryptographic keys between entities and systems (Kish et al., 2026; Parihar et al., 2025).

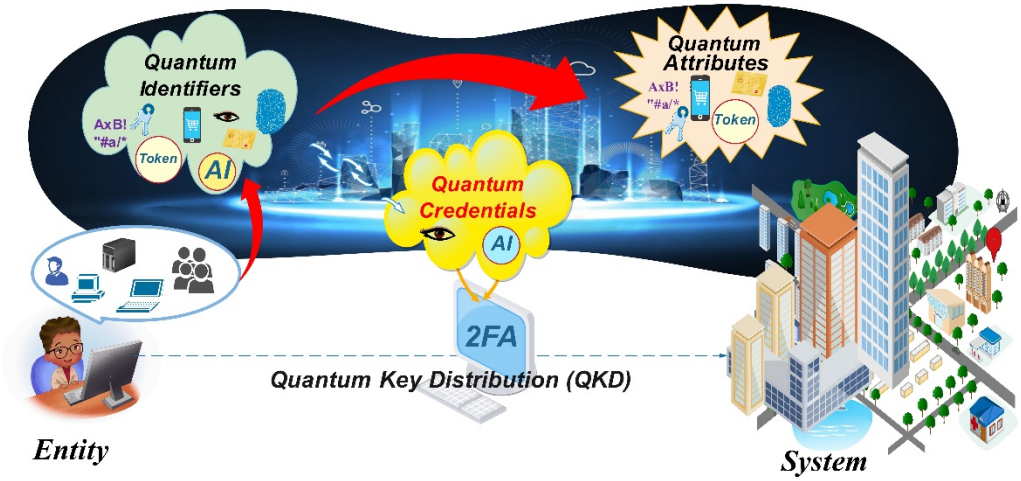

Fig. 4. Illustration of the entity elements.

3.2. The AI role in authentication approaches

AI can play multiple roles in authentication approaches, either as quantum credentials (as shown in Figure 4) or through algorithms. These algorithms provide features such as information collection, processing, monitoring, and decision-making, affording this technology numerous advantages against all other technologies. First of all, the AI capability to collect, process, combine, and predict future outcomes is a key feature for its application in authentication approaches (Wani et al., 2024). Furthermore, AI algorithms have a specific power to analyze large amounts of information, enabling the discovery of potential attack vectors in real time without relying on conventional methods (Thakkar and Lohiya, 2022). AI has a special role in authentication systems through the training processes, including iterative pre-training steps (Zha et al., 2023). However, there are two specific different processes related to the explainability and interpretability of decision-making. Explainability refers to the mechanisms and techniques used to clarify model processes of internal

logic, while interpretability, describes the extent to which a human observer understands a models behavior based on its input/output relationships (Arrieta et al., 2020).

4. Quantum artificial intelligence (QAI)

This section is organized into three subsections: the first provides a mathematical representation of QAI, outlining the benchmark and the comparison of polynomial time and exponential time; the second presents a comparison between quantum and classical computing related to user priorities (e.g., security, privacy, trust) and other ethical factors; and the third section presents transformative effects of QAI such as MFA solutions, Decision-making, vector threats, training processes, information privacy, information security awareness and behavior.

4.1. Mathematical representation of QAI

QAI represents the integration of quantum computing (QC) and artificial intelligence (AI), harnessing the strengths of both technologies in a synergistic approach to enhance performance. QC is a computational paradigm based on quantum mechanical phenomena (e.g., superposition, entanglement, and interference) (Viggiano and Brin, 2023) to efficiently tackle problems that are intractable for classical computers (Feynman, 1982; Preskill 2018). Unlike traditional computing based on binary logic as a basic unit (e.g., 0 or 1), QC has possibilities to manipulate entanglement and superposition states (Rieffel and Polak, 2000). The difference between these states is that the superposition enables quantum particles to be in two states at once, while entanglement links qubits so that changing one affects others even when physically separated (Rab et al., 2017). These unique properties known as quantum parallelism expand computing capabilities, giving quantum computers enormous processing power. Specifically, QC can solve certain problems in polynomial time, such as factoring integers with Shor's algorithm, offering exponential speedup compared to classical algorithms that require exponential time (Shor, 2002). Other algorithms like Grover's, Quantum Approximate Optimization Algorithm (QAOA), and Variational Quantum Eigensolver (VQE) offer quadratic or problem-dependent speedups but do not guarantee polynomial-time solutions for all complex problems. Thus, quantum features open new possibilities in cryptography, simulations, optimization, and improving the accuracy and efficiency of machine learning tasks (Schuld and Killoran 2019; Wang et al. 2023; Herman et al. 2023; Ho et al. 2024). For better mathematical understanding of the superposition phenomenon, the list of the used mathematical terms with key remarks is presented in Table 2.

Table 2. Description of mathematical notations.

Notations	***Meaning***	***Remarks***
$\boldsymbol{\psi}$	*The state vector*	*It completely describes the state of a quantum system*
$\boldsymbol{\alpha, \beta}$	*Probability amplitudes*	*Complex numbers weighting states*
n	*Number of qubits*	*Determines the size of the quantum system*
2^n	*Number of basis states*	*Total possible classical states*
x	*Index*	*Enumerates all basis states*
$\frac{\mathbf{1}}{\sqrt{\mathbf{2^n}}}$	*Normalization factor*	*Ensures total probability equals 1*
$T(n)$	*Time complexity function*	*Represents the number of computational steps an algorithm performs.*
n	*Input size*	*Size of problem instance*
$O(\cdot)$	*Big-O notation*	*Asymptotic upper bound*
k	*Polynomial degree*	*Fixed constant ≥ 1*
n^k	*Polynomial function*	*Grows moderately*
c	*Exponential base*	*Fixed constant > 1*
c^n	*Exponential function*	*Grows rapidly*
$\frac{\boldsymbol{n^k}}{\boldsymbol{c^n}}$	*Efficiency*	*Measures polynomial vs. exponential growth*

Superposition as phenomenon of single and multi-qubit superposition can be mathematically formulated as (Forcer et al., 2002):

- *Single-qubit superposition:* A qubit is a normalized vector in a two-dimensional complex Hilbert space and can be written as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{where} \quad \alpha, \beta \in \mathbb{C} \quad \wedge \quad |\alpha|^2 + |\beta|^2 = 1 \tag{1}$$

- *Multi-qubit superposition (all possible exponents):* An n-qubit system spans a state space of dimension 2^n. The uniform superposition over all classical states is

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \qquad \text{where} \qquad n \in \mathbb{N}_0 \tag{2}$$

$|x\rangle$ denotes a computational basis state corresponding to the binary representation of *x*.

- *Polynomial Time Complexity*: An algorithm runs in polynomial time if its time complexity can be mathematically expressed as:

$$T(n) = O(n^k) \qquad \text{where} \qquad (\exists\, \mathrm{k} \in \mathbb{N}) \tag{3}$$

- *Exponential time complexity*: An algorithm runs in exponential time if its time complexity grows as

$$T(n) = O(c^n) \qquad (\mathrm{c} > 1) \tag{4}$$

- *Exponential growth asymptotically dominates polynomial growth*:

$$\lim_{n\to\infty} \frac{n^k}{c^n} = 0 \qquad for \qquad \forall\, \mathrm{k} \geq 1 \quad \wedge \quad \forall\, \mathrm{c} > 1 \tag{5}$$

- It implies that

$$\exists\, N \in \mathbb{N} \;\; such\ that \;\; \forall\, n \geq N, \qquad \frac{n^k}{c^n} \leq 1 \quad \Leftrightarrow \quad c^n \geq n^k \tag{6}$$

4.2 Computational complexity benchmark

For the purpose of better understanding QC power in authentication approaches, we give a benchmark through a concrete practical comparative example as visible and tangible remarks associated with defensive cyber strategy. As this mathematical approach enables direct comparison between polynomial time and exponential time complexities; thereby allowing the results to be interpreted in relation to identified threat vectors and the corresponding levels of defense against them. Specifically, we present a comparison of polynomial-time and exponential-time complexities, using a benchmark as a reference framework, with three fixed parameter values defined in Table 3.

Table 3. Proposed parameter values.

S.No	***Parameter***	***Value***
1	*n*	*4, 8, 16, 32, 64, 128, 256, 512, 1024*
2	*k*	*2*
3	*c*	*3*

Taking into account the defined fixed parameters in Table 3, it is possible to calculate concrete practical numerical values. Specifically, the extra empirical work corresponding to Equations (3), (4), and (6) can be calculated for every benchmark scenario (Eqs. 7–32).

I Benchmark calculations for n=4:

$$n^k = 4^2 = 16 \tag{7}$$
$$c^n = 3^4 = 81 \tag{8}$$
$$\frac{n^k}{c^n} = \frac{16}{81} = 0.1975 \tag{8}$$

II Benchmark calculations for n=8:

$$n^k = 8^2 = 64 \tag{9}$$
$$c^n = 3^8 = 6561 \tag{10}$$
$$\frac{n^k}{c^n} = \frac{64}{6561} = 0.00976 \tag{11}$$

III Benchmark calculations for n=16:

$$n^k = 16^2 = 256 \quad (12)$$

$$c^n = 3^{16} = 43\,046\,721 \quad (13)$$

$$\frac{n^k}{c^n} = \frac{256}{43046721} = 5.95 \times 10^{-6} \quad (14)$$

IV Benchmark calculations for n=32:

$$n^k = 32^2 = 1\,024 \quad (15)$$

$$c^n = 3^{32} = 1.85 \times 10^{15} \quad (16)$$

$$\frac{n^k}{c^n} = \frac{1\,024}{1.85 \times 10^{15}} = 5.53 \times 10^{-13} \quad (17)$$

V Benchmark calculations for n=64:

$$n^k = 64^2 = 4\,096 \quad (18)$$

$$c^n = 3^{64} = 3.40 \times 10^{30} \quad (19)$$

$$\frac{n^k}{c^n} = \frac{4\,096}{3.40 \times 10^{30}} = 1.20 \times 10^{-27} \quad (20)$$

VI Benchmark calculations for n=128:

$$n^k = 128^2 = 16\,384 \quad (21)$$

$$c^n = 3^{128} = 1.16 \times 10^{61} \quad (22)$$

$$\frac{n^k}{c^n} = \frac{16\,384}{1.16 \times 10^{61}} = 1.41 \times 10^{-57} \quad (23)$$

VII Benchmark calculations for n=256:

$$n^k = 256^2 = 65\,536 \quad (24)$$

$$c^n = 3^{256} = 1.34 \times 10^{122} \quad (25)$$

$$\frac{n^k}{c^n} = \frac{65\,536}{1.34 \times 10^{122}} = 4.89 \times 10^{-118} \quad (26)$$

VIII Benchmark calculations for n=512:

$$n^k = 512^2 = 262\,144 \quad (27)$$

$$c^n = 3^{512} = 1.79 \times 10^{244} \quad (28)$$

$$\frac{n^k}{c^n} = \frac{262\,144}{1.79 \times 10^{244}} = 1.46 \times 10^{-239} \quad (29)$$

IX Benchmark calculations for n=1024:

$$n^k = 1024^2 = 1\,048\,576 \quad (30)$$

$$c^n = 3^{1024} = 3.20 \times 10^{488} \quad (31)$$

$$\frac{n^k}{c^n} = \frac{1\,048\,576}{3.20 \times 10^{488}} = 3.28 \times 10^{-482} \quad (32)$$

To better understand Eq. (5) and to interpret the computational results acquired from evaluating the efficiency of polynomial versus exponential growth, we provide a formal statistical comparison of the results (Eq. 33):

$$0.1975 > 0.00976 > 5.95 \times 10^{-6} > 5.53 \times 10^{-13} > 1.20 \times 10^{-27} > 1.41 \times 10^{-57} > 4.89 \times 10^{-118} > 1.46 \times 10^{-239} > 3.28 \times 10^{-482} \quad (33)$$

These comparative results clearly indicate that as the number of qubits increases proportionally toward infinity, the rate of efficiency of the measures (comparing polynomial and exponential growth) tends toward zero. The summary of all possible results from the benchmark calculations comparing efficiency between polynomial and exponential growth in benchmark scenarios is presented in Table 4. As Table 4 clearly shows a significant disparity between quantum algorithms (i.e., polynomial-time growth) and classical algorithms (i.e., exponential-time growth); thereby, it discovers the reason why exponential complexity is fundamental to modern cryptographic security. For small values of input size (e.g., algorithms from 4 to 16 bits), the polynomial term remains comparable to the exponential term, making systems vulnerable to brute-force and dictionary attacks.

Practically, QC has the capability to perform multivariable computations and resolve complex mathematical inquiries in microseconds, significantly faster than classical computing. However, as input size values increase (algorithms from 128 bits and above), the efficiency rapidly approaches zero, meaning the exponential space grows overwhelmingly faster than any feasible polynomial-time attack. It is the reason why authors like MacQuarrie et al., (2020); Mikkelsen et al., (2007)

point out speed as a specific QC feature. However, the key mathematical values (e.g., input size from 1024 bits) suggest that quantum algorithms (e.g., 1 048 576) are more efficient than classical algorithms (e.g., 3.20×10^{488}) due to their need for fewer computational steps. This efficiency reduces exponential-time processes in classical algorithms to polynomial-time or even faster steps with quantum algorithms.

Table 4. Efficiency comparison between polynomial and exponential growth in benchmark scenarios.

Benchmark scenario	n	n^k	c^n	n^k/c^n	*Remarks*
I	4	16	81	0.1975	Extremely weak; an attacker using brute-force guessing can break it instantly.
II	8	64	6 561	0.00976	Weak; feasible for a determined attacker using brute-force, dictionary as basic attack vectors.
III	16	256	43 046 721	5.95×10^{-6}	Moderate security; attacks using Brute-force dictionary possible with massive computing power.
IV	32	1 024	1.85×10^{15}	5.53×10^{-13}	Strong security; practically unbreakable for most attackers.
V	64	4 096	3.40×10^{30}	1.20×10^{-27}	Extremely secure; would require immense resources over many years.
VI	128	16 384	1.16×10^{61}	1.41×10^{-57}	Advanced Encryption Standard (AES)-level security; brute-force effectively impossible today.
VII	256	65 536	1.34×10^{122}	4.89×10^{-118}	Near-absolute security; only future tech could attempt this.
VIII	512	262 144	1.79×10^{244}	1.46×10^{-239}	Exponentially negligible chance; quantum attacks insufficient.
IX	1024	1 048 576	3.20×10^{488}	3.28×10^{-482}	Practically impossible; essentially unbreakable indefinitely.

This results in a sharp transition from weak and breakable security to practically unbreakable systems, even with massive classical or QC resources. In essence, the theoretical results highlight that increasing key input sizes does not merely improve security linearly but multiplies it exponentially, making attack vectors increasingly unrealistic as values of input size grow. Thus, due to the large key lengths, classical brute force attacks become practically infeasible because the number of possible keys increases exponentially. In contrast, quantum algorithms can search the key space in approximately polynomial time, which makes large keys more susceptible to quantum attacks than to classical attacks.

5. Comparison and transformative effects of QAI

This section discusses current cyber challenges and research opportunities in authentication systems, focusing on the critical need for continued investigation and innovation to fully leverage the potential of AI in enhancing cybersecurity.

5.1 The comparison of QC and classical computing

The above presented mathematical approach highlights the potential impact of integrating quantum technologies into existing threat vectors (e.g., brute-force attacks, MiTM, impersonation, cryptographic attacks, zero-day, replay attacks, and physical theft of devices) that significantly amplifies the vulnerabilities of classical authentication systems. For example, quantum algorithms that use Shor's algorithm to factorize large numbers in polynomial time can break RSA and ECC encryption that underpin most digital certificates. Furthermore, Single Sign-On (SSO) implementations based on cryptographic protocols are vulnerable to quantum attacks. Therefore, quantum attack vectors represent a threat to strong MFA solutions-based authentication systems in which protection of credentials is of the highest priority. Consequently, quantum technologies extend vulnerabilities across all IdM systems. On the other hand, the mathematical approach points out that the convergence of quantum and AI technologies has the potential to enhance quantum authentication systems in different ways, such as detecting different quantum attack vectors, improving the performance of authentication systems (e.g., enabling ultra-fast decision-making), and optimizing quantum random number generation (QRNG). In order to better understand the significance of QC compared to classical computing, a comparison between quantum and classical computing in authentication approaches is given in Table 4.

Table 4 shows the superior capabilities of QAI over traditional AI, particularly in terms of collecting and processing massive amounts of information in real time with rapid behavioral tracking, early detection of advanced threat vectors, and improved outcome prediction and decision-making. These superiors are based on leveraging quantum-secure encryption, QKD, and QRNG that offer a fundamentally stronger and more advanced authentication system than classical computing systems. They significantly improve resistance against both current and future quantum attack vectors that make vulnerable classical cryptography algorithms (such as RSA and ECC). Besides security, QC enhances privacy and credentials trustworthiness by minimizing sensitive information exposure and making credentials practically impossible

to predict or forge. On the other hand, the classical authentication systems remain constrained by computational limits and monitoring, reliance on pseudo-randomness, and cryptographic algorithms that are increasingly vulnerable in a post-quantum era. Their slower adaptability, limited transparency, and higher exposure to information breaches reduce long-term reliability.

Table 4. The comparison between quantum and classical computing in authentication approaches.

Features	***QC***	***Classical Computing***
Security	Supports quantum-secure encryption, QKD, and creating strong MFA.	Classical cryptography and MFA may be vulnerable to quantum-enabled attacks (e.g., Shor's algorithm breaking RSA/ECC).
Privacy	Enable privacy-preserving authentication, including quantum-secure ID verification, secure multiparty computations, and minimal data exposure.	Classical systems often rely on storing sensitive user data, making them more vulnerable to data breaches and correlation attack vectors.
Trustworthiness of credentials	Use QRNG and quantum-secure keys, making credentials inherently harder to forge or predict.	Rely on pseudo-random keys and classical cryptography that may be predictable.
Adaptive authentication	AI analyzes behavioral patterns, risk scores, and contextual information in real time, while quantum-enhanced computation enables faster large-scale analysis.	Classical AI, or rule-based systems, are slower at processing large behavioral datasets and have limited real-time adaptation.
Threat vector detection	Quantum-accelerated analytics enable the detection of subtle anomalies, advanced attack vectors, and MiTM attempts.	Limited to conventional monitoring and are slower at detecting sophisticated or large-scale attacks.
Transparency	AI-driven insights allow for explainable authentication decisions, improving both user and organizational trust.	Classical systems often act as black boxes; users and admins may not understand why access is granted or denied.

Thus, QAI-powered authentication systems represent a strategic evolution toward secure, privacy-preserving, and transparent identity verification, in which quantum technology guarantees integrity and unpredictability, and AI enables continuous authentication and dynamic adjustment of security levels in real time. However, the development of such authentication systems requires the implementation of comprehensive defensive strategies, including infrastructure of identity related to post-quantum cryptographic (PQC) algorithms (e.g., CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, and FALCON (NIST, 2022)), zero-trust architecture, strengthened identity governance, certificate authorities, and PKI (Marshall, 2025).

5.2. Transformative effects of QAI

QAI, with its inherent quantum features, is anticipated to significantly transform advanced authentication systems across several dimensions, such as the adoption of quantum cryptographic algorithms, the generation of truly unpredictable credentials via quantum random number generation (QRNG), and the enhancement of adaptive authentication through sophisticated AI-driven risk analysis. Specifically, QAI, by integrating QC with AI technologies, fundamentally reshapes authentication systems, enabling the deliver faster, more adaptive, and intelligent authentication mechanisms capable of countering post-quantum and large-scale cyber threat vectors. Given that the integration of quantum-resistant security mechanisms with real-time behavioral intelligence enables QAI-powered systems to enhance resilience against quantum-enabled attacks; thereby, it improves authentication accuracy, scalability, and responsiveness in complex, large-scale digital environments. Thus, QAI adoption in authentication approaches has strong transformative effects (as presented in Figure 5) in addressing the following aspects:

- Enhancing MFA solutions, including hash-based, lattice-based, or QKD-based keys.
- Improving decision-making.
- Identifying and mitigating potential attack vectors, including hacking and signal interception in satellite networks.
- Boosting the efficiency and speed of authentication processes through qubit features (e.g., superposition and entanglement).
- Accelerating and optimizing training processes.
- Strengthening post-quantum information privacy.
- Enhancing computation speed, reliability, sustainability, and secrecy.
- Promoting real-time information security awareness and adaptive, context-aware authentication behaviors.

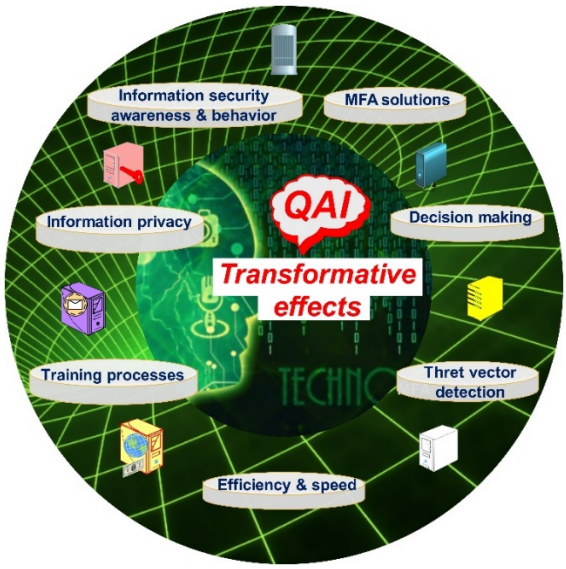

Fig. 5. Transformative QAI effects for advanced authentication systems.

6. Discussion

This section is structured into two subsections. First provides an overview of QAI challenges and limitations, highlighting QC potential in authentication approaches. The second presents future works, outlining the key quantum features that contribute to the future development of intelligent authentication systems.

6.1 QAI challenges and limitations

Quantum supremacy refers to the milestone at which a quantum computer outperforms a classical computer in solving a specific task, demonstrating the superior computational potential of quantum technology (Dixit & Jian, 2022). However, building large-scale quantum computers is challenging due to decoherence, where qubits lose their quantum state when interacting with the environment (Procopio et al., 2015; Youssefi et al., 2023; Oppenheim et al., 2023). Specifically, the QAI deployment encounters numerous implementation challenges despite its significant practical potential. As QAI represents an unprecedented advancement in the protection of authentication systems, offering virtually unbreakable quantum algorithms, real-time prevention of attack vectors, and AI-driven network optimization; however, QC is still in the early stages of development and implementation in authentication approaches. There are many issues associated with QAI in authentication approaches, including security validation and testing, scalability, hardware limitations, regulatory and compliance issues, privacy issues, sensitivity to disturbances, pricing issues, etc. The full implementation of QAI requires ultra-secure, low-latency 6G infrastructure with decentralized architectures, enabling secure cloud and edge computing and self-optimizing autonomous telecommunications networks. QC should be integrated with emerging technologies such as blockchain in order to mitigate quantum-related vulnerabilities. However, QAI raises specific concerns about algorithmic fairness and transparency because of its probabilistic nature. Given that probabilistic outputs obscure the traces of decision-making (often not even visible to programmers), making irreversible or high-impact consequences, hence, they can significantly contribute to challenges in training models and raise ethical concerns (e.g., transparency and auditability) due to the loss of meaningful human control. The probabilistic nature may introduce complex and hard-to-detect biases during training (Rodríguez-Pérez et al., 2021) that could result in bad predictive outcomes (Shams et al., 2023).

To mitigate these risks, ethical AI in the advanced authentication systems has to incorporate bias detection mechanisms tailored for QC, ensuring that decisions made by QAI remain interpretable and explainable. In addition, QAI introduces additional complexities in decision-making, extreme non-interpretability, power asymmetries, and diminished human oversight caused by quantum states (e.g., superposition, entanglement) that are fundamentally harder to explain than classical AI. QAI's ability to easily break classic traditional cryptographic algorithms represents a precedent in cybersecurity that inevitably raises numerous other questions related to user priorities in authentication approaches: Does large-scale QAI-supported network monitoring and real-time decryption irreversibly undermine user privacy? QAI can significantly strengthen authentication systems by introducing fundamentally stronger and more robust MFA solutions in IdM systems. But, this security challenge has to be addressed with other user priorities such as maintaining privacy,

usability, pricing, complexity, etc. The new old problem in authentication approaches related to the issue of balancing security and privacy remains a major problem.

6.2 Future work

The implementation of QC based on QKD and Q-PUFs in authentication systems can provide a better level of protection of device identities and verification channels from cloning and unauthorized access that comprehensively provides a high-level defensive strategy against future quantum attack vectors. Moreover, the convergence of AI and QC technologies represents symbiosis in which AI technology with all its algorithmic capabilities leverages quantum hardware infrastructure to increase its own capacities with the aim of building a stronger and more intelligent future generation of advanced authentication systems. AI algorithms in authentication approaches can process quantum signals, detect error patterns, and monitor user behavior in real time, effectively differentiating between legitimate anomalies and malicious activities. In the future, QAI may further enhance decision-making in authentication approaches by enabling rapid analysis of large datasets and dynamic adjustment of security levels. As the implementation of QC is on the threshold of its evolutionary development in authentication approaches, the question of ethical factors has emerged as the substantial imperative for future research directions.

7. Conclusions

Authentication systems are among the most time-sensitive targets for quantum security, as cyber attackers are likely to adopt QC technologies as quantum tools early. QC, by relying on polynomial time complexity, has the potential to significantly enhance the role of AI in authentication systems, particularly by enabling the analysis and processing of massive volumes of information at rates far exceeding those of with classical computing. Polynomial time complexity ensures efficiency, while exponential time complexity ensures security by making exhaustive attacks (e.g., brute force and quantum attacks) impractical. Exponential-time algorithms scale fundamentally worse than polynomial-time algorithms, because exponential growth eventually overwhelms any polynomial growth. In addition, QAI facilitates integration with other emerging technologies, such as blockchain, for supporting the development of more robust and resilient MFA solutions. QAI-enhanced advanced authentication systems as the first line of defensive cyber strategy have a domino effect directly improving all other systems of society, such as economy, industrial automation & robotics, chemical, nuclear, cyber-physical systems, and many others. While QAI promises breakthroughs in authentication approaches, especially in security, optimization, and decision-making, it also introduces profound ethical challenges associated with monitoring issues that will shape the future of responsible QAI.

References

1. Acampora, G., Chiatto, A., Schiattarella, R., Autilia Vitiello, A. (2026). Quantum artificial intelligence: A survey, Computer Science Review, 59, 2026, 100807.
2. Ahmad, A., Srirangan, J., (2025). Quantum-safe mutual authentication scheme for IoHT using blockchain, Results in Engineering, 28, 106945.
3. Albusays, K., et al.: The diversity crisis in software development. IEEE Soft. 38(2), 19–25 (2021).
4. Alexeev, Y., Farag, M.H., Patti, T.L. *et al.* Artificial intelligence for quantum computing. *Nat Commun* 16, 10829 (2025). https://doi.org/10.1038/s41467-025-65836-3-
5. Alzahrani, A.I.A. Exploring AI and quantum computing synergies in holographic counterpart frameworks for IoT security and privacy. *J Supercomput* 81, 1194 (2025). https://doi.org/10.1007/s11227-025-07682-0.
6. Aragona, B., Acampa, S. (2026). Definitions of artificial intelligence and quantum technologies: A comparative thematic analysis of the strategic documents of 29 European countries, Futures, 175, 103722.
7. Arrieta, A.B., et al., (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," Information Fusion, vol. 58, pp. 82–115, Jun. 2020.
8. Arute, F., Arya, K., Babbush, R., Bacon, D., et al. Quantum supremacy using a programmable superconducting processor Nature, 574 (2019), pp. 505-510.
9. Balasubramanian, P., Liyana, S., Sankaran, H. *et al.* Generative AI for cyber threat intelligence: applications, challenges, and analysis of real-world case studies. *Artif Intell Rev* 58, 336 (2025). https://doi.org/10.1007/s10462-025-11338-z.
10. Bano, M., Ali, S. & Zowghi, D. Envisioning responsible quantum software engineering and quantum artificial intelligence. Autom Softw Eng 32, 69 (2025). https://doi.org/10.1007/s10515-025-00541-5.
11. Bhattarai, I. Pu, C. Choo K.K.R. and Korać, D. (2024). A Lightweight and Anonymous Application-Aware Authentication and Key Agreement Protocol for the Internet of Drones, in IEEE Internet of Things Journal, 11(11), 19790-19803. doi: 10.1109/JIOT.2024.3367799.
12. Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., Lloyd, S. Quantum machine learning, Nature, 549 (2017),

pp. 195-202.
13. Buchmann, J.A., Karatsiolis, E.G., Wiesmaier, A. Introduction to Public Key Infrastructures, Springer, Berlin Heidelberg, 2013.
14. Çakir, E., Tolga, A.Ç. (2026). A Review of Artificial Intelligence's Impact on Cybersecurity in the Big Data Era. In: Gervasi, O., et al. Computational Science and Its Applications – ICCSA 2025 Workshops. ICCSA 2025. Lecture Notes in Computer Science, vol 15886. Springer, Cham. https://doi.org/10.1007/978-3-031-97576-9_12.
15. Dixit, V., Jian, S. Quantum Fourier transform to estimate drive cycles Sci. Rep., 12 (2022), p. 654.
16. Feynman, R.P., (1982). Simulating physics with computers, Internat. J. Theoret. Phys., 21 (6–7), 467-488.
17. Forcer, T.M., Hey, A.J., Ross, D., Smith, P.G. (2002). Superposition, entanglement and quantum computation. Quantum Inf. Process., 2 (2), 97-116.
18. Furnell, S., Helkala, K., Woods, N., 2022. Accessible authentication: Assessing the applicability for users with disabilities, Computers & Security, 113 10256.
19. Ghaemi, H., Abbasinezhad-Mood, D., Ostad-Sharif, A., and Alizadehsani, Z., (2024). Novel blockchain-assisted fault-tolerant roaming authentication protocol for mobility networks without home agent entanglement, Journal of Network and Computer Applications, 224 103843.
20. Herman, D., et al.: Quantum computing for finance. Nat. Rev. Phys. 5(8), 450–465 (2023).
21. Ho, K.T.M., Chen et al.: Quantum computing for climate resilience and sustainability challenges. In: 2024 IEEE international conference on quantum computing and engineering (QCE), vol. 2, pp. 262–267 (2024). IEEE
22. Hoffmann, C.H., Flother, F.F.: Why business adoption of quantum and ai technology must be ethical. Res. Director: Quantum Technol. 2, 4 (2024). https://doi.org/10.1017/qut.2024.5.
23. Illiano, J., Caleffi, M., Manzalini, A., Cacciapuoti, A.S., (2022). Quantum internet protocol stack: a comprehensive survey Comput. Netw., 213 (2022), Article 109092.
24. Jafri, R., Arabnia, H., (2009). A Survey of Face Recognition Techniques, Journal of Information Processing Systems 5(2), 41-68.
25. Jong, E.: Own the unknown: an anticipatory approach to prepare society for the quantum age. Digital Soc. 1(2), 15 (2022.
26. Kasse, M.C., Mboup, E.H.M. Post-quantum secure authentication protocol based on OTP and TEE. *J Supercomput* 81, 1532 (2025). https://doi.org/10.1007/s11227-025-08029-5.
27. Kaur R, Gabrijelčič D, Klobučar T (2023) Artificial intelligence for cybersecurity: literature review and future research directions. Inform Fusion 97, 101804.
28. Kim, M., Park, J.H. Quantum-resilient security for 6G networks: a comprehensive survey on challenges, solutions, and research opportunities. *J Supercomput* 81, 1086 (2025). https://doi.org/10.1007/s11227-025-07544-9.
29. Kish, S., Pieprzyk, J., Camtepe, S. (2026). Trends in Quantum Key Distribution (QKD). In: Jang-Jaccard, J., Caroff, P., Blezinger, E., Mulder, V., Mermoud, A., Lenders, V. (eds) Quantum Technologies. Springer, Cham. https://doi.org/10.1007/978-3-031-90727-2_12.
30. Klusch, M., Lässig, J., Müssig, D. et al. Quantum Artificial Intelligence: A Brief Survey. Künstl Intell 38, 257–276 (2024). https://doi.org/10.1007/s13218-024-00871-8.
31. Kop, M., et al.: 10 principles for responsible quantum innovation. SSRN Electronic Journal. (2023). https://doi.org/10.2139/ssrn.4475556.
32. Korać, D., Čvokić, D. and Simić, D. 2025a. Computational Engineering Approach-Based Modeling of Safety and Security Boundaries: A Review, Novel Model, and Comparison. Arch Computat Methods Eng. https://doi.org/10.1007/s11831-025-10352-2
33. Korać, D., Damjanović, B. & Simić, D. (2022a). A model of digital identity for better information security in e-learning systems. J Supercomput, 78, 3355.
34. Korać, D., Damjanović, B., Simić, D., and Pu, C., 2025. Management of evaluation processes and creation of authentication metrics: Artificial intelligence-based fusion framework, Information Processing & Management, 62 (6) 104233.
35. Korać, D., Damjanović, B., Simić, D., Choo, K.K.R. (2022). A hybrid XSS attack (HYXSSA) based on fusion approach: Challenges, threats and implications in cybersecurity. Journal of King Saud University - Computer and Information Sciences, 34 (10), Part B, 9284-9300.
36. Korać, D., Simić, D., 2019. Fishbone Model and Universal Authentication Framework for Evaluation of Multifactor Authentication in Mobile Environment, Computers & Security, 85, 313-332.
37. Li, X., Chen, T., Cheng, Q., Ma, J. An efficient and authenticated key establishment scheme based on fog computing for healthcare system, Front. Comput. Sci. 16 (2022) 1–12.
38. Ma, M., He, D., Wang, H., Kumar, N., Choo, K.K.R. (2019). An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks, IEEE Internet Things J. 6 (2019) 8065–8075.
39. Ma, R., Cao, J., Feng, D. et al., LAA: Lattice-based access authentication scheme for IoT in space information networks, IEEE Internet Things J. 7 (4) (2020) 2791–2805.
40. MacQuarrie, E.R., Simon, C., Simmons, S., Maine, E., The emerging commercial landscape of quantum computing, Nat. Rev. Phys., 2 (2020), pp. 596-598.
41. Marshall, M., (2025), Quantum-Safe Authentication: Preparing Your Enterprise for the Post-Quantum Era. https://www.avatier.com/blog/quantum-safe-authentication/. (Accessed December 25, 2026).

42. Mikkelsen, M., Berezovsky, J., Stoltz, N., Coldren, L., Awschalom, D. Optically detected coherent spin dynamics of a single electron in a quantum dot Nat. Phys., 3 (2007), pp. 770-773.
43. Nasajpour, M., Pouriyeh, S., Parizi, R.M. Dorodchi, M., Valero, M., & Hamid R. Arabnia, H.A., Internet of Things for Current COVID-19 and Future Pandemics: an Exploratory Study. J Healthc Inform Res 4, 325–364 (2020). https://doi.org/10.1007/s41666-020-00080-6.
44. NIST, (2022). NIST Announces First Four Quantum-Resistant Cryptographic Algorithms, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms. (Accessed January 25, 2026).
45. Oppenheim, J., Sparaciari, C., Šoda, B., Weller-Davies, Z. Gravitationally induced decoherence vs space-time diffusion: testing the quantum nature of gravity, Nat. Commun., 14 (2023), p. 7910.
46. Parihar, A.S. A secure communication in distributed system using quantum key distribution. J Supercomput 81, 1468 (2025). https://doi.org/10.1007/s11227-025-07964-7.
47. Paul, S., et al.: Integration of ai and quantum computing in cybersecurity: A comprehensive review. In: Integration of AI, quantum computing, and semiconductor technology, pp. 287–308 (2025).
48. Pirandola, S., Braunstein, S.L., Physics: unite to build a quantum internet, Nature, 532 (2016), pp. 169-171.
49. Preskill, J.: Quantum computing in the low era and beyond. Quantum. 2, 79 (2018).
50. Procopio, L.M., Moqanaki, A., Araújo, M. et al. Experimental superposition of orders of quantum gates Nat. Commun., 6 (2015), p. 7913.
51. Pu, C., Seol, J., Park, N., and, Korać, D., Authenticated Key Agreement Protocol for Device-to-Gateway Communication in IoT," in *IEEE Consumer Communications & Networking Conference (IEEE CCNC 2026)*, 2026.
52. Pu, C., Bilal, M., Lim, S.., Quantum-Safe and Cross-Layer Authentication and Key Agreement Protocol for Smart Grid Communications, in *IEEE Consumer Communications & Networking Conference (IEEE CCNC 2026)*, 2026a.
53. Pu, C., Wall, A., Choo, K.-K.R., Ahmed, I., and Lim, S., 2022. A Lightweight and Privacy-Preserving Mutual Authentication and Key Agreement Protocol for Internet of Drones Environment, in IEEE Internet of Things Journal, 9 (12), 9918-9933.
54. Rab, A.S., Polino, E., Man, Z.X., Ba, N. An, et al. (2017). Entanglement of photons in their dual wave-particle nature Nat. Commun., 8, p. 915.
55. Radanliev, P. Artificial intelligence and quantum cryptography. J Anal Sci Technol 15, 4 (2024). https://doi.org/10.1186/s40543-024-00416-6.
56. Rawat, B., et al.: Quantum computing and ai: Impacts & possibilities. ADI J. Recent Innov. 3(2), 202–207 (2022).
57. Rieffel, E., Polak, W., (2000). An introduction to quantum computing for non-physicists, ACM Comput. Surv., 32 (3) (2000), pp. 300-335.
58. Rodríguez-Pérez, G., Nadri, R., Nagappan, M.: Perceived diversity in software engineering: a systematic literature review. Empire. Soft. Eng. 26, 1–38 (2021).
59. Sarkar, A. Automated quantum software engineering. Autom Softw Eng 31, 36 (2024). https://doi.org/10.1007/s10515-024-00436-x.
60. Schuld, M., Killoran, N.: Quantum machine learning in feature hilbert spaces. Phys. Rev. Lett. 122(4), 040504 (2019).
61. Shams, R.A., Zowghi, D., Bano, M.: AI and the quest for diversity and inclusion: A systematic literature review. AI and Ethics, pp. 1–28 (2023).
62. Shams, R.A., Zowghi, D., Bano, M.: AI and the quest for diversity and inclusion: A systematic literature review. AI and Ethics, pp. 1–28 (2023).
63. Sharma, S., Sharma, L., Gandhi, T.K. (2026). Integration of quantum artificial intelligence in disease diagnosis: A review of methods and applications, Computer Methods and Programs in Biomedicine, 274, 109175.
64. Shor, P.W.: Introduction to quantum algorithms. In: Proceedings of Symposia in Applied Mathematics, vol. 58, pp. 143–160 (2002).
65. Singh, S., Kumar, D.: Enhancing cyber security using quantum computing and artificial intelligence: A review. In: algorithms. 4(3) (2024).
66. Sood, V., Chauhan, R.P.: Archives of quantum computing: research progress and challenges. Arch. Comput. Methods Eng. 31(1), 73–91 (2024).
67. Stylios, I., Kokolakis, S., Thanou, O., Chatzis, S., 2021. Behavioral biometrics & continuous user authentication on mobile devices: A survey, Information Fusion, 66 76-99.
68. Sunki, K., Reddy, C.K.K., Reddy, D.M.K., Doss, S. (2025). The Role of Quantum Artificial Intelligence in Healthcare Advancements. In: Gunjan, V.K., Senatore, S., Kumar, A. (eds) Cybernetics, Human Cognition, and Machine Learning in Communicative Applications. Cognitive Science and Technology. Springer, Singapore. https://doi.org/10.1007/978-981-97-8533-9_10.
69. Tandel, P., Nasriwala, J. Secure authentication framework for IoT applications using a hash-based post-quantum signature scheme. *SOCA* 19, 251–262 (2025). https://doi.org/10.1007/s11761-024-00414-x.
70. Thakkar, A., Lohiya, R. (2022). A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. Artif Intell Rev 55, 453–563. https://doi.org/10.1007/
71. Tuli, E. ., Lee, JM. & Kim, DS. Leveraging quantum blockchain for secure multiparty space sharing and authentication on specialized metaverse platform. Sci Rep 14, 25776 (2024). https://doi.org/10.1038/s41598-024-74213-x.

72. Umbrello, S.: Ethics of quantum technologies: A scoping review. Int. J. Appl. Phil. (2024).
73. Umbrello, S.: Ethics of quantum technologies: A scoping review. Int. J. Appl. Phil. (2024).
74. Viggiano, G., Brin, D.: Convergence: artificial intelligence and quantum computing: social, economic, and policy impacts. In: Wiley, (2023). ISBN: 978-1394174102.
75. Wang, M., Guo, J., Zhang, W., Long, G.L., (2025). Efficient access authentication for quantum communication network with digital certificates, Fundamental Research, online 11 November 2025. https://doi.org/10.1016/j.fmre.2025.10.014.
76. Wang, P.-H., et al.: Recent advances in quantum computing for drug discovery and development. IEEE Nanotechnol. Mag. 17(2), 26–30 (2023).
77. Wang, S., Zhao, G., Xu, C. *et al.* LPQAA: a lightweight post-quantum access authentication scheme for satellite network. *J Supercomput* 81, 233 (2025). https://doi.org/10.1007/s11227-024-06687-5.
78. Wani, N.A., Kumar, R., Mamta, Bedi, J., Rida, I. (2024). Explainable AI-driven IoMT fusion: Unravelling techniques, opportunities, and challenges with Explainable AI in healthcare, Information Fusion, 110, (2024) 102472.
79. Wu, F., Zhou, B., Song, J. *et al.* Quantum-resistant blockchain and performance analysis. *J Supercomput* 81, 498 (2025). https://doi.org/10.1007/s11227-025-07018-y.
80. Wu, T.Y., Guo, X., Yang, L., Meng, Q., Chen, C.M. A lightweight authenticated key agreement protocol using fog nodes in social Internet of vehicles, Mob. Inf. Syst. 2021 (2021) 3277113.
81. Xue, K., Meng, W., Li, S.et al., A secure and efficient access and handover authentication protocol for internet of things in space information networks, IEEE Internet Things J. 6 (3) (2019) 5485–5499.
82. Yazdinejad A, Parizi RM, Dehghantanha A, Choo K.K.R., (2019) Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5g networks. IEEE Transactions on Network Science and Engineering 1–1.
83. Youssefi, A., Kono, S., Chegnizadeh, M., Kippenberg, T.J. A squeezed mechanical oscillator with millisecond quantum decoherence Nat. Phys., 19 (2023), pp. 1697-1702.
84. Zha, D., Bhat, Z.P., Lai, K-H., et al., (2023). Data-centric Artificial Intelligence: A Survey, ACM Computing Surveys, Volume 57, Issue 5, Article No.: 129, 2025, Pages 1 - 42, https://doi.org/10.1145/3711118.
85. Zhu, T., Chen, J., Ma, M., Chen, T., Lv, M., and Weng. Z. (2025) "GANDACOG: Implicit Mobile User Authentication in Multi Environments With Scarce Data," in IEEE Internet of Things Journal, vol. 12, no. 14, pp. 28074-28091, 15 July15, 2025.