PriMera Scientific Engineering
Volume 6 Issue 5 May 2025
DOI: 10.56831/PSEN-06-196
ISSN: 2834-2550

PriMera Scientific Publications

Leveraging Artificial Intelligence and Cybersecurity Lessons Learned to Improve Federal Quantum Computing Adoption Outcomes

Type: Research Article
Received: April 19, 2025
Published: April 22, 2025

Citation:
James Hornage. "Leveraging Artificial Intelligence and Cybersecurity Lessons Learned to Improve Federal Quantum Computing Adoption Outcomes". PriMera Scientific Engineering 6.5 (2025): 13-18.

Copyright:
© 2025 James Hornage. This is an open-access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

James Hornage*

Capitol Technology University, United States of America

***Corresponding Author:** James Hornage, Capitol Technology University, PSC 78 Box 579, APO, AP, 96326, United States of America.

Abstract

The U.S. Federal Government is currently engaged in multiple major modernization initiatives. Cloud computing is largely implemented across the federal government, but artificial intelligence (machine learning), cybersecurity, and quantum computing are all competing for resources and management attention. Artificial intelligence adoption is further along than quantum computing and can serve as a framework for predicting and preventing quantum adoption issues. This paper provides an analysis of the federal government's implementation history for the four major technology areas. It outlines an approach for leveraging artificial intelligence adoption in the federal government to help predict quantum adoption challenges, including the creation of a time series analysis to leverage the Federal Government's AI investment, progress, and challenges to help predict federal quantum adoption challenges.

Keywords: quantum; quantum computing; quantum computing adoption; artificial intelligence; machine learning; cybersecurity; enterprise modernization; federal adoption

Abbreviations

AI: Artificial Intelligence.
DARPA: Defense Advanced Research Projects Agency.
NIST: National Institute of Standards and Technology.
R&D: Research and Development.
GAO: U.S. Government Accountability Office.

Introduction

The federal government is investing billions of dollars annually to accelerate quantum technology. Quantum technologies have entered the commercial marketplace, and the federal government is actively evaluating many solutions for potential adoption. The federal government has a vast range of agencies and technology requirements, and it has struggled with adoption of modern technologies. The current approach to accelerating quantum adoption mirrors other troubled technological implementations. Prior research [1] outlined a three-phase approach, as presented in Figure 1, to developing a research-based, federal quantum computing adoption framework and methodology.

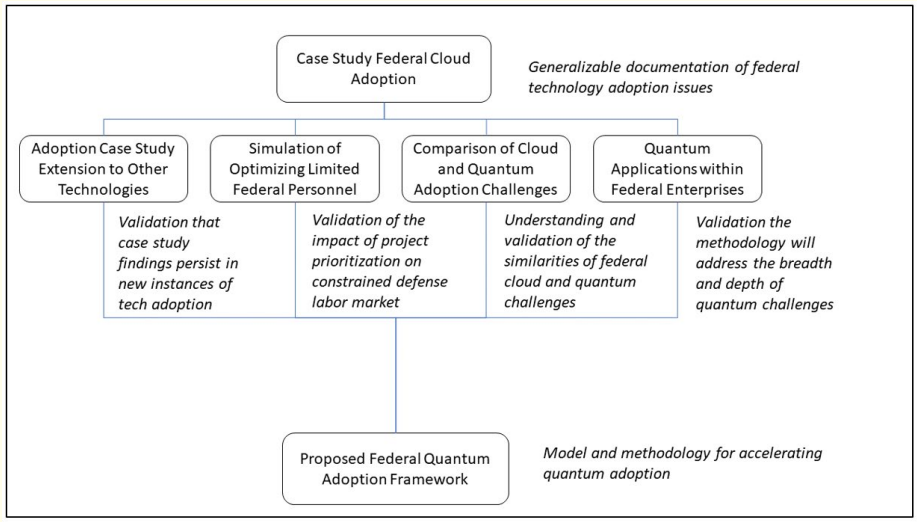

Figure 1: Framework for Study to Develop Methodology and Model for Accelerating Quantum Adoption.

This paper addresses "Adoption Case Study Extension to Other Technologies" by examining the extent to which federal adoption of artificial intelligence (AI) and cybersecurity can be leveraged to support the development of the proposed federal quantum adoption framework.

Background

The federal government is currently in the process of adopting four major technological advances. Cloud computing, cybersecurity, AI, and quantum computing are all in various stages of federal adoption. There have been documented challenges with the adoption of cloud computing [2], cybersecurity, and AI. Federal investment in key technologies has reduced research and development (R&D) timelines, but inefficiencies within federal adoption have led to decades-long delays in incorporating these technologies and improving outcomes for the federal government. Quantum computing adoption is in the earliest phases, and the government could benefit from addressing key lessons learned to speed up adoption of this critical technology.

The federal government has designated cloud computing, AI, cybersecurity, and quantum computing as critical technologies. The government outlines its prioritization of these technologies through a range of mechanisms such as increased funding, implementation guidance, policies and standards, white papers, and presidential directives.

Cloud computing

The National Institute of Standards and Technology, or NIST, defines cloud computing [3] as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

It is the evolution of virtualization and other enterprise computing services to a self-service and often outsourced model. The federal government leverages cloud computing to increase speed, efficiency, and resiliency for its computing requirements. Numerous agencies have reported the ability to reduce personnel and data centers as they migrate to cloud computing. Prior research found [2] that despite more than 15 years of focus on cloud computing as a critical enabler, cloud adoption goals still have not been met.

AI

NIST has adopted the ANSI definition of AI [4] as "a branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement".

Federal investment in machine learning and AI dates to the 1950s. The first major national AI policy, The National Artificial Intelligence Research and Development Strategic Plan, was issued in October 2016 by the National Science and Technology Council [5]. The government had spent over $1B on unclassified research the prior year, and the plan outlined seven priorities for federally funded AI research. Since then, additional guidance [6-10] has been issued across multiple administrations, with two memorandums covering the use and acquisition of AI released in May 2025 [11].

In 2023 [12], the U.S. Government Accountability Office (GAO) found wide disparities in artificial intelligence adoption, which was driven in part by a lack of "government-wide guidance on how agencies should acquire and use AI. " AI is gaining traction within the government, but the lack of a comprehensive framework is causing adoption challenges. The lack of specific government guidance was also identified as a challenge in cloud computing adoption [2], which provides an indication that similar problems may occur for future (quantum) technology adoption.

Cybersecurity

NIST defines cybersecurity [13] as "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation".

The first national cyber policy was issued as a Presidential Directive [14] on May 22, 1998. It has been updated over successive presidential administrations in 2003 as The National Strategy to Secure Cyberspace [15], the 2009 Cyberspace Policy Review [16], the 2018 National Cyber Strategy [17], and the 2023 National Cybersecurity Strategy [18]. Each administration has outlined the value of cybersecurity and directed investments and specific actions to drive increased protections. Despite more than 25 years of investment, a 2024 GAO report [19] found that nearly half of the recommendations for 1) establishing a comprehensive cybersecurity strategy and performing effective oversight, 2) protecting critical infrastructure, and 3) protecting privacy and sensitive data have not been implemented. This makes cybersecurity an ongoing federal technology adoption area to derive lessons learned and inform future quantum adoption.

Quantum computing

NIST does not have a published definition of the broader field of quantum computing, but they do offer explanations [20] of quantum computation and quantum information. This is consistent with the timeline for NIST's prior technology definitions, which were not published for cloud and AI until they had matured further. IBM defines quantum computing [21] as "an emergent field of cutting-edge computer science harnessing the unique qualities of quantum mechanics to solve problems beyond the ability of even the most powerful classical computers. The field of quantum computing contains a range of disciplines, including quantum hardware and quantum algorithms".

The National Quantum Initiative Act was passed in 2018 [22]. It established the National Quantum Coordination Office, which has overseen and collated more than 50 strategy and technical documents [23] covering topics such as quantum sensors, quantum networks, quantum information science, and quantum cryptography, as well as issues related to workforce development.

Defense Advanced Research Projects Agency (DARPA) is leading the Quantum Benchmarking Initiative [24], which "is designed to rigorously verify and validate whether any quantum computing approach can achieve utility-scale operation — meaning its computational value exceeds its cost — by the year 2033". IBM's roadmap [25] for quantum computing anticipates error correction at initial scale in 2029 with its Starling platform and expanding that scale to 2000 qubits with the Blue Jay platform in 2033 and beyond.

These projections highlight the fact that quantum computing is in its infancy and there is still time before solutions that operate at scale are available. This provides an opportunity to identify a methodology and framework to better prepare for large-scale adoption.

Strong Relationships Among Technology Areas

Cloud, cybersecurity, AI and quantum technologies are all related to each other. Cloud computing provides the computing power that drives AI and cybersecurity solutions, and in some cases, it provides access to quantum computing technologies. Cybersecurity protects cloud computing resources, artificial intelligence solutions, and quantum computing solutions. Artificial intelligence is an enabling technology for automation in cloud computing and for logging and monitoring solutions in cybersecurity, and the field of quantum machine learning combines quantum computing and AI solutions. Quantum computing is being made accessible via cloud interfaces to enable future classical-quantum hybrid solutions. Its potential impact on encryption has forced cybersecurity professionals to plan for a post-quantum environment, and complex AI solutions may soon be implemented via quantum machine learning.

Materials and Methods

There is limited published research on improving federal technology adoption. The analysis relied on review of government documents related to high-level policy, strategy, standards, technical implementation, and programmatic reviews. Industry documents covering major industry trends, technology roadmaps, and technical implementation were also reviewed.

Prior research into the history of federal cloud computing adoption [2] provides a strong baseline to understand potential quantum computing adoption challenges. While the federal government has not fully achieved its desired adoption targets yet, the process for achieving the desired adoption levels is now only a function of time and resources. Thus, it should be considered a static baseline.

Since cloud computing has already been established as a static baseline, the analysis focused on the extent to which AI and cybersecurity could serve as dynamic baselines to inform quantum adoption planning. Significant changes are under way within the federal government, and a quantum adoption framework would benefit from having a dynamic technology baseline to complement the static cloud computing baseline.

The analysis considered the similarity to quantum computing, level of prioritization, notional implementation timelines, and current adoption levels. It also evaluated the availability of robust data sources to understand the potential to conduct a time-series analysis to develop a predictive analytic to improve adoption understanding.

Results and Discussion

The analysis found that cloud, cybersecurity, artificial intelligence and quantum computing are all likely to face similar adoption challenges within the federal government. Prior research into cloud computing adoption challenges identified a range of issues, and there is sufficient cloud adoption to provide a static baseline. Cloud computing currently provides the most insight into future quantum adoption challenges.

Artificial intelligence adoption is still in its relative infancy, and there is enough similarity between AI and quantum in the federal government to research its challenges and monitor adoption progress over the next decade. Thus, artificial intelligence can serve as a dynamic baseline and an ongoing vehicle for extracting lessons learned and predicting federal quantum adoption challenges. Further, ongoing monitoring of artificial intelligence adoption data could support time series analysis as a powerful predictive analytic. Monitoring AI adoption can also improve the eventual adoption of quantum machine learning.

Cybersecurity adoption has been ongoing for more than 25 years, and it has had to respond to the advent of cloud, AI and quantum solutions. For example, as quantum computing solutions began to emerge, cybersecurity needed to respond to threats to encryption posed by a post-quantum environment [26]. Federal cybersecurity adoption differs from the other three major technologies because while the other three technologies serve to enable solutions, cybersecurity is primarily concerned with sustaining availability of sys-

tems and protecting the integrity of their data. Cloud, AI, and quantum technologies should all achieve desired adoption levels, but cybersecurity's adoption challenges will be ongoing. In fact, if a framework for federal quantum computing adoption is successfully created, it may be able to help inform cybersecurity's adoption of the solutions required to project the next major technology area.

Cloud computing provides a strong static baseline, artificial intelligence provides the best opportunity for a dynamic baseline, and cybersecurity can provide valuable insights but has significant differences that may hinder using it as a baseline.

Conclusion

There are several additional research questions that can be derived from the analysis and findings. What are the specific similarities and differences between the likely federal adoption pathways for artificial intelligence and quantum computing? What are the most critical factors and data to consider in the development of a time series analysis and predictive analytics? What lessons can be learned from cybersecurity adoption challenges for each major technological advance? How will competition for resources by each of the four major technological thrusts impact each other?

There is ongoing research aimed at completing the second phase of research as outlined in Figure 1 to enable the development of a research-based framework for federal quantum computing adoption.

References

1. Hornage J. "Methodology to Accelerate Federal Agency Adoption of Quantum Technologies". Grid, Cloud, and Cluster Computing; Quantum Technologies; and Modeling, Simulation and Visualization Methods. CSCE 2024. Communications in Computer and Information Science, Springer, Cham 2257 (2025).
2. Hornage J. "Federal Cloud Computing Adoption Case Study: A Retrospective Analysis as a Precursor to Optimized Quantum Adoption Methodologies". Grid, Cloud, and Cluster Computing; Quantum Technologies; and Modeling, Simulation and Visualization Methods. CSCE 2024. Communications in Computer and Information Science, Springer, Cham 2257 (2025).
3. NIST. NIST SP 800-145: The NIST Definition of Cloud Computing (2011).
4. NIST. U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools 25 (2019).
5. National Science and Technology Council, Networking and Information Technology Research and Development Subcommittee. "The National Artificial Intelligence Research and Development Strategic Plan". (2016).
6. National Science & Technology Council. "The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update". (2019).
7. 116th Congress. H.R.6216 - National Artificial Intelligence Initiative Act of 2020 (2020).
8. Congressional Research Service. "Artificial Intelligence: Background, Selected Issues, and Policy Considerations". (2021).
9. National Security Commission on Artificial Intelligence. "The Final Report". (2021).
10. The White House. "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence". (2023).
11. The White House. "White House Releases New Policies on Federal Agency AI Use and Procurement". (2025).
12. GAO. GAO-24-105980. "Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements".
13. NIST. NIST Special Publication 800-53, Rev 5: Security and Privacy Controls for Information Systems and Organizations (2020): 401.
14. Presidential Decision Directive/NSC-63 22 (1998).
15. The National Strategy to Secure Cyberspace (2003).
16. Cyberspace Policy Review (2009).
17. National Cyber Strategy (2018).
18. National Cybersecurity Strategy (2023).
19. GAO-24-107231. High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation (2024).
20. NIST. "Quantum Computing Explained". (2025).

21. IBM. “What is Quantum Computing”. (2025).
22. 115th Congress. “National Quantum Initiative Act”. (2018).
23. National Quantum Coordination Office Website. “Publication Library”.
24. DARPA. “DARPA Announces Stage A Quantum Benchmarking Initiative Participants”. (2025).
25. IBM. “Expanding the IBM Quantum roadmap to anticipate the future of quantum-centric supercomputing”.
26. NIST. NIST CSWP 15. “Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms”. (2021).