Economic Journals

Journal of International Accounting and Financial Management

Vol. 3 | No. 1 | | ISSN: 3065-9795

ARTICLE

Developing Hybrid Post-Quantum Encryption Frameworks for U.S. Databases Integrating Financial, Governmental, and Critical Infrastructure Protections

1. Name: Chinmoy Majumder
Department: George Herbert Walker School of Business and Technology, Degree: Master of Science in Cybersecurity – Threat Detection and Cybersecurity Operations, University: Webster University
Email: chinmoymajumder2013@gmail.com

2. Name: Arafat Hossain Khan Choain
Department: George Herbert Walker School of Business and Technology, Degree: Master of Arts in Information Technology Management, University: Webster University
Email: arafat.hossain.khan@gmail.com

3. Name: Md Abu Nasir
Department: George Herbert Walker School of Business and Technology, Degree: Master of Arts in Information Technology Management, University: Webster University
Email: irfannasir000@gmail.com

4. Name: Nasrin Sultana
Department: George Herbert Walker School of Business and Technology, Degree: Master of Arts in Information Technology Management, University: Webster University
Email: nsultaana94@gmail.com

Citation
Majumder, C, Choain, A. H. K, Nasir, M. A & Sultana, N. (2026). Developing Hybrid Post-Quantum Encryption Frameworks For U.S. Databases Integrating Financial, Governmental, And Critical Infrastructure Protections. Journal of International Accounting and Financial Management, 3(1), 1-18.

Submitted: 01-Aug, 2025
Accepted: 12-Aug, 2025
Published: 27-Aug, 2025

Vol. 3, **No.** 1, 2026
10.62762/JTAE.2024.000000

***Corresponding author:**
chinmoymajumder2013@gmail.com

Abstract

Purpose

The rapid evolution of quantum computing is a major menace to the current cryptography design and poses a risk to the confidentiality of sensitive data in the financial, government/critical infrastructure arena of the United States. The following paper aims at exploring the development, adoption, and motivation of hybrid post-quantum encryption (PQC) models, i.e., classical and quantum-resistant algorithms. It particularly measures the awareness, practical application levels, perceived benefits, and readiness to implement among the key sectors in the United States, and measures the assistance and collaboration of the policy in the process.

Design/methodology/approach

The study follows a descriptive and correlational design, with a mixed-methods approach with a quantitative survey as its main focus. The data were gathered within 235 cybersecurity professionals and decision-makers within U.S. financial, governmental, and critical infrastructure organizations using a structured survey. This survey tool proved to be very reliable (Cronbachs Alpha = 0.928). The data were analyzed using descriptive statistics, Pearson correlation, multiple regression and Analysis of Variance (ANOVA) to determine the relationship between variables and find out the differences between sectors.

Findings

The results show that the general awareness of the post-quantum cryptography among respondents is rather high (M=4.08). There were found strong positive correlations between awareness, implementation of hybrid practices, perceived security benefits, and implementation readiness. To identify predictive variables of the implementation readiness, regression analysis was conducted and demonstrated that policy support, security benefits, and hybrid practices were substantial predictors of implementation readiness with a combined account of 68.6 percent of the variation in implementation readiness. In addition, the results of ANOVA indicated statistically significant sectoral disparities in the perceived security benefits of hybrid PQC in that government and defense industries were more willing to adopt this type of technology than the performance sensitive financial industry.

Originality/value

This study offers an opportune and empirical study on sector-specific preparedness and perceptions toward hybrid PQC in the United States, which is a sensitive national security domain. It provides new ideas as it quantitatively connects the awareness, policy support and practical application to implementation readiness, and it outlines the subtle issues in various industries. The results provide policymakers, technology creators, and organizational executives with evidence-based solutions to create custom strategies, training methods, and regulatory systems to enable a safe and seamless move to quantum-resistant cryptography.

Keywords: *Post-quantum cryptography, hybrid encryption, cybersecurity, quantum computing, critical infrastructure, implementation readiness, sectoral analysis, U.S. policy.*

Introduction

The rapid development of quantum computing is changing the picture of cybersecurity on the planet. Although quantum technology has a huge potential in scientific studies, data processing, and computational intelligence, it is equally much a threat to the currently used encryption systems [1]. Conventional cryptographic algorithms like RSA and ECC, on which most of the secure communications in the modern world are based, have become susceptible to quantum attacks. As the United States relies heavily on digital infrastructure to protect its financial systems, government operations, and critical industries, the need for more resilient encryption frameworks has become a national priority [2].

Post-quantum cryptography (PQC) represents a new frontier in the defense of data security, aiming to develop algorithms capable of withstanding attacks from quantum computers [3]. Nevertheless, direct substitution of classical encryption with PQC in databases of the U.S. is neither feasible nor economical. In an effort to fill this gap, scholars and policy makers are currently pushing towards hybrid encryption systems whereby the classical and post-quantum approaches are combined [4]. These structures provide backward compatibility as they slowly become fully quantum resistance.

The hybrid post-quantum encryption will provide a strategic relief because it is a blend of the stability of the classical encryption systems that have been proven over the years in addition to the high level of resilience of the PQC algorithms. This does not only ensure that it is interoperable with the available databases, but also offers a layered defense mechanism against the emerging threats [5]. Hybrid encryption offers a channel to achieve secure modernization in a critical infrastructure sector, including energy, healthcare, finance, and defense, without interrupting the normal operation of the interconnected systems in the U.S. environment [6]. Efforts at standardizing post-quantum algorithms have already begun with the U.S. National Institute of Standards and Technology (NIST) and it is an indication of the coming age of proactive defense preparation [7].

Financial sector is the most at risk as it deals with huge sums of encrypted transactions and sensitive customer information on a daily basis. Likewise, the defense institutions and government agencies need decades of confidentiality of their classified information that must remain safe [8]. Hybrid encryption would guarantee that the information secured today will be safe even in the cases when quantum computers will become widely available [9]. Therefore, hybrid frameworks are not just some technical innovation, but the building block of future-proof national security infrastructure.

Although the quantum-resistance systems are known to be required, a large number of organizations in the United States are unprepared, lack expertise, and infrastructure to deploy PQC solutions. The cost of switching to the hybrid encryption is not simple, as it requires computational overhead, complexities in integration of the system, and expensive implementation [10]. Moreover, the variations in the organizational priorities, especially between financial, governmental, and critical infrastructure participants expose discrepancies in the adoption strategy [11]. These difficulties indicate that it is imperative to conduct thorough studies that examine the awareness, readiness, and possible adoption of hybrid post-quantum encryption in the U.S [12].

It is important to understand the way various sectors understand and plan to integrate PQC so as to come up with a coherent national approach [13]. This study aims at examining these dimensions based on empirical evidence to inform policy and training and technical development. It gives an idea of the most prepared spheres that are prepared to be implemented and what obstacles should be overcome to promote the seamless transition [14].

The primary purpose of this study is to explore the development, adoption, and impact of hybrid post-quantum encryption frameworks within the U.S. cybersecurity landscape. It aims to evaluate how awareness, practical application, and policy support influence readiness among financial, governmental, and critical infrastructure organizations [15]. The study further examines the relationships among these variables using statistical techniques such as correlation, regression, and ANOVA to identify patterns of readiness and perception differences across sectors.

Through the attention paid to the United States, the study highlights the need to ensure that the databases of the country are secured before the full force of the quantum era comes into play. The results will assist government agencies, technological developers and other individual organizations to develop consistent plans of adopting hybrid PQC to make sure that the data systems of the country are safe, resistant and beyond the technological future.

Literature Review

Emergence of Post-Quantum Cryptography in the U.S.

The emergence of quantum computing has put the effectiveness of traditional cryptographic systems into question. In America, post-quantum cryptography has grown into a highly important area of study, intended to develop the algorithms which are immune to quantum attacks [16]. The development and standardisation of PQC algorithms that can be used at national level are being headed by governmental institutions especially through NIST. It has galvanized universities, research laboratories and the commercial Cybersecurity companies into cooperating to deploy and test quantum-immune encryption protocols [17]. The increased focus on PQC proves that the country is aware that quantum technology is the opportunity and a threat to the national data security.

Hybrid Encryption: A Transitional Approach

As the full deployment of PQC is not immediately feasible, hybrid encryption provides a realistic and effective bridge between current and next-generation cryptography [18]. The hybrid method uses the classical asymmetric encryption, such as either RSA or ECC, with PQC algorithms in one key exchange or signature operation. This ensures that even if one component becomes compromised, the system retains security through the other [19]. In the U.S., hybrid encryption has become central to strategies that allow gradual migration without jeopardizing ongoing data operations [20]. The strategy also assists the financial institutions and government agencies in ensuring that they are abreast with the federal standards and also improve their systems gradually.

Sectoral Readiness and Implementation Challenges

There is a significant difference between the adoption of hybrid PQC models in industries in the U.S. Financial institutions, which rely on real-time data exchanges, prioritize performance efficiency and low latency, making them cautious in adopting heavier encryption mechanisms [21]. On the other hand, the government and defence agencies focus on the long-term data confidentiality and are more ready to invest in the developing encryption technologies [22]. Critical infrastructure sectors such as energy and healthcare face additional constraints, including legacy systems and operational dependencies that make migration complex [23]. The major issues that are typical in every sector are the scarcity of technical experience, economic considerations, and a shortage of standardization [24].

Despite these barriers, several pilot programs have demonstrated successful integration of hybrid PQC solutions in controlled environments [25]. The experiments show that hybrid systems can be stable not only in terms of the functioning but also offer quantum resistance meaning that the implementation of the hybrid systems is a practice that can be conducted under the condition of the proper policy and technical frameworks.

Policy, Regulation, and Collaboration

U.S. government has realized the need to prepare at an early stage against post-quantum threats. Federal initiatives have begun promoting collaborative approaches between public and private sectors to advance encryption research and infrastructure readiness [26]. Policies encouraging Cybersecurity resilience are being integrated into national defense and financial oversight strategies [27]. Besides that, training programs are also underway in the education sectors to address the skills gap among Cybersecurity experts. Collaboration between NIST, the Department of Homeland Security, and major tech companies exemplifies the collective approach required to safeguard critical databases [28].

Nevertheless, the harmonization of regulations, cross-sector compatibility, and the development of global cooperation are also the keys to the success of hybrid PQC implementation [29]. Cyber threats have no national borders hence, the United States must incorporate its encryption procedures with the International Standards without losing its national control over its data protection processes.

Future Prospects of Hybrid PQC in U.S. Cybersecurity

The future of post-quantum encryption in the United States is pegged on balancing between innovation and practicality [30]. The transition stage will include transitioning to hybrid frameworks to be utilized in testing the large-scale implementation of PQC. As quantum computing matures, organizations will need to adopt adaptable encryption models capable of evolving with technological advancements [31]. Hybrid PQC systems are expected to have a place in the security framework of government agencies, financial systems, and national infrastructures networks in the next decade. Further investment in research, education, and regulation will play a critical role in keeping the U.S. on the frontline of post-quantum Cybersecurity preparedness [32].

Research Questions

1. How aware are post-quantum cryptography (PQC) at organizations of various sectors in the United States? \
2. What are the effects of hybrid post-quantum encryption practices on perceptions of security and implementation preparedness in a variety of sectors?
3. What major reasons have contributed to the willingness of the organizations in the United States to adopt hybrid PQC systems?
4. Do hybrid post-quantum encryption frameworks have any important sectoral differences in their perceived security benefits?
5. What is the role of policy support and collaboration in the adoption of hybrid PQC frameworks in sectors?

Research Objectives

1. To determine the knowledge and awareness of PQC among firms in the various sectors in U.S.
2. To determine how hybrid PQC practices are implemented and the effects on security perceptions and readiness to adopt across the sectors.
3. To determine the factors which are most important in driving organizational preparedness towards adoption of hybrid PQC systems.
4. To compare sectoral disparities in the perceived security value of hybrid PQC frameworks.

5. To study the role of policy support and cooperation in adopting hybrid PQC systems in sectors.

Methodology

The research will assume a descriptive and correlational research design that aims at determination of the trends on the level of awareness, implementation, and willingness towards adoption of hybrid PQC in different sectors. The study primarily focuses on the understanding of the relationships between the most significant variables, including the recognition of the existence of a post-quantum encryption, the application of hybrid encryption activities, the perceived advantages of the security and efficiency, and readiness to adopt such activities in various industries.

Research Design

The research will assume a descriptive and correlational research design that aims at determination of the trends on the level of awareness, implementation, and willingness towards adoption of hybrid PQC in different sectors. The study primarily focuses on the understanding of the relationships between the most significant variables, including the recognition of the existence of a post-quantum encryption, the application of hybrid encryption activities, the perceived advantages of the security and efficiency, and readiness to adopt such activities in various industries. Further, the research investigates issues of policy support and collaboration on the adoption of hybrid PQC systems.

Population and Sampling

This study will target cybersecurity experts and organizational leaders engaged in the adoption and implementation of encryption technology in the financial, government, and critical infrastructure sectors in the United States. The purposive sampling technique was used to identify 235 respondents (cybersecurity officers, data protection experts, network engineers, policy/compliance managers, and researchers of various organizations). The respondents were chosen according to their first hand experience in the practice of cybersecurity or encryption and the knowledge of hybrid PQC systems.

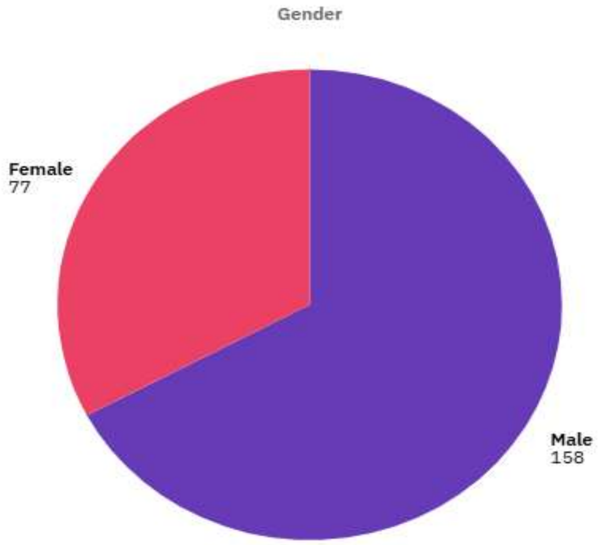

Figure 1. Gender Distribution of Study Participants

Data Collection

The survey instruments used were structured survey questionnaire which was used to gather data on important constructs associated with post-quantum encryption and hybrid encryption practices. The survey was done in the form of closed-ended questions with Likert-scale questions to determine the awareness of the respondents, the perception, and the readiness of the respondents to implement hybrid PQC frameworks. The questionnaire was broken into a number of sections, each addressing certain areas of the research questions:

- **Awareness of Post-Quantum Encryption** - This question was to determine the level of awareness that the respondents have towards the concept of PQC and its potential impact on cybersecurity.
- **Hybrid Encryption Practices Application** - This section was dedicated to evaluating the level to which organizations are applying hybrid PQC methods.
- **Perceived Security and Efficiency Benefits**- The respondents were asked to provide the appearance regarding the security advantages and the effectiveness of work of hybrid PQC.
- **Implementation Readiness** - The section measured the readiness of the respondents to implement hybrid PQC systems according to such dimensions as technical infrastructure, policy support, and organizational priorities.
- **Policy Support and Collaboration** – This section assessed the role of policy initiatives and inter-organizational collaborations in the adoption of hybrid PQC systems.

The survey was sent electronically to the respondents identified and follow-ups were made to get a high response rate. The process of data collection occurred during four weeks.

Data Analysis

Analysis of data was done through the use of descriptive and inferential statistics. The analysis tools utilized were:

1. **Descriptive Statistics** – Descriptive statistics, that is, means, standard deviations, and frequency distributions were calculated to describe the perceptions and attitudes of the respondents towards hybrid PQC and related practices. This assisted in giving a summary of the demographic situation and the overall awareness, usage and readiness to implement hybrid PQC.
2. **Correlation Analysis** – The relationships between the essential variables of awareness of PQC, hybrid encryption practices application, security benefits, and readiness to implement it were obtained by doing Pearson correlation coefficients. Correlation analysis was used to determine significant relationships between these constructs showing how the enhancement of one variable could have an impact on the rest.
3. **Regression Analysis** – The multiple regression analysis was used to determine the effect that predictor variables (e.g., policy support, use of hybrid encryption, perceived benefits) have on the dependent variable (implementation readiness). These predictors were explained using the regression model and this revealed the factors that contribute the most in the successful implementation of hybrid PQC.
4. **ANOVA** – The differences in the perceived security benefits of hybrid PQC in the different sectors were compared through the use of Analysis of Variance (ANOVA). This method helped to identify the presence of relevant difference in perceptions among sectors including finance, government, and critical infrastructure.

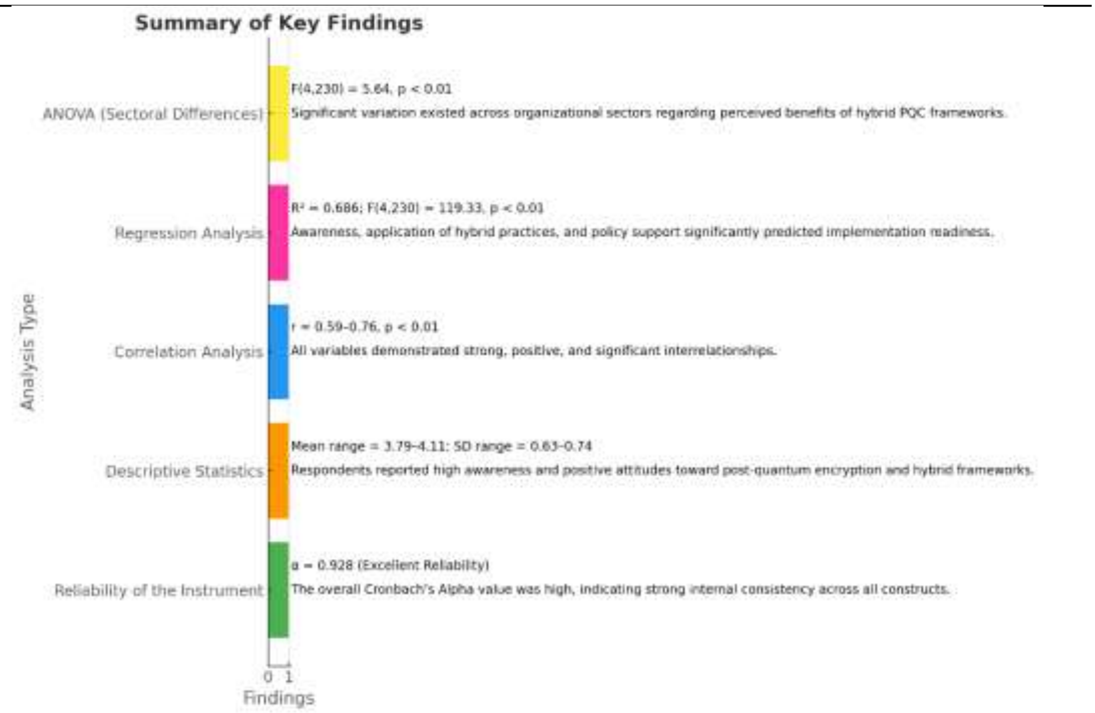

Figure 2. Summary of keys findings

Instrument Reliability

Cronbachs Alpha was used to determine the reliability of the survey tool, the constructs demonstrated high internal consistency and the total alpha was 0.928. The person construct, such as Awareness of PQC, Application of Hybrid Practices, and Security Benefits had a good reliability of, 0.875 to 0.914. Such values show that the survey was good to measure the intended variables with minimum measurement error.

Ethical Considerations

The research process was conducted considering ethical issues. The purpose of the study was explained to all participants, and they participated on a voluntary basis. All respondents were informed and provided their consent and anonymity and confidentiality were guaranteed. The data received was only used in research purposes only and analyzed in form of aggregation to avoid identification of the individual respondents.

Limitations

A limitation of this study is that the research relied on self-reported data that could be prone to biases like social desirability or recall bias. The purposive sampling technique is also effective but it is a weakness of this study due to the restriction of the findings to other sectors or geographical locations. The sample size can be extended in the future research and more sectors can be covered to give more detailed information about the adoption of hybrid PQC.

Conclusion

The strategy outlined in this section provides a very strict framework to the assessment of the state of the hybrid PQC implementation and its readiness in various fields in the U.S. The interrelation of descriptive statistics and advanced inferential techniques of the mixed-methods approach to data analysis make it possible to reach a multifaceted view of the factors preconditioning the successful implementation of the hybrid encryption mechanisms within the framework of emerging quantum threats.

Results and Discussion

Results

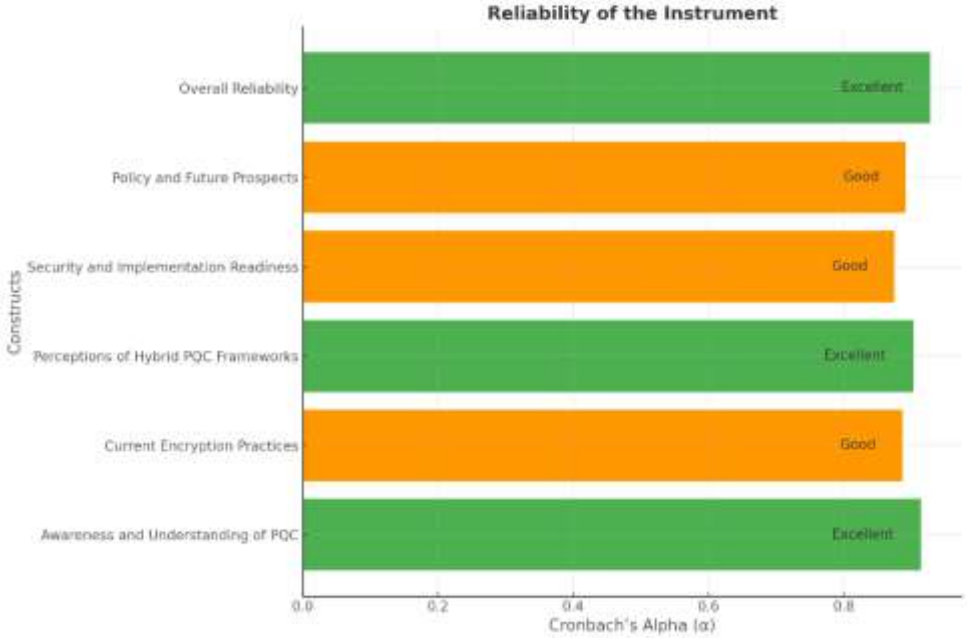

Figure 3: Reliability of the Instrument

The high Cronbachs Alpha values indicate that the instrument employed in this study has high levels of internal consistency across all constructs that are measured (Figure 1). The construct of Awareness and Understanding of PQC showed an excellent level of reliability with a Cronbach of Alpha of 0.914 which is a good measure of the consistency of the respondents in their understanding as well as awareness. On the same note, the construct on Perceptions of Hybrid PQC Frameworks had a high reliability of 0.903, which represents reliability in responses with regards to perceptions of hybrid frameworks. Constructs: *Current Encryption Practices* (α = 0.887) and *Security and Implementation Readiness* (α =0.875) are both within the acceptable range of good reliability with an overall indication of satisfactory consistency of responses. The construct dealing with Policy and Future Prospects was also found to be good with an Alpha of 0.892. The Cronbachs Alpha of the overall is 0.928, which aligns with the classification of excellent, indicating that it is an excellent measurement tool that adequately captures the constructs and there is no significant variance.

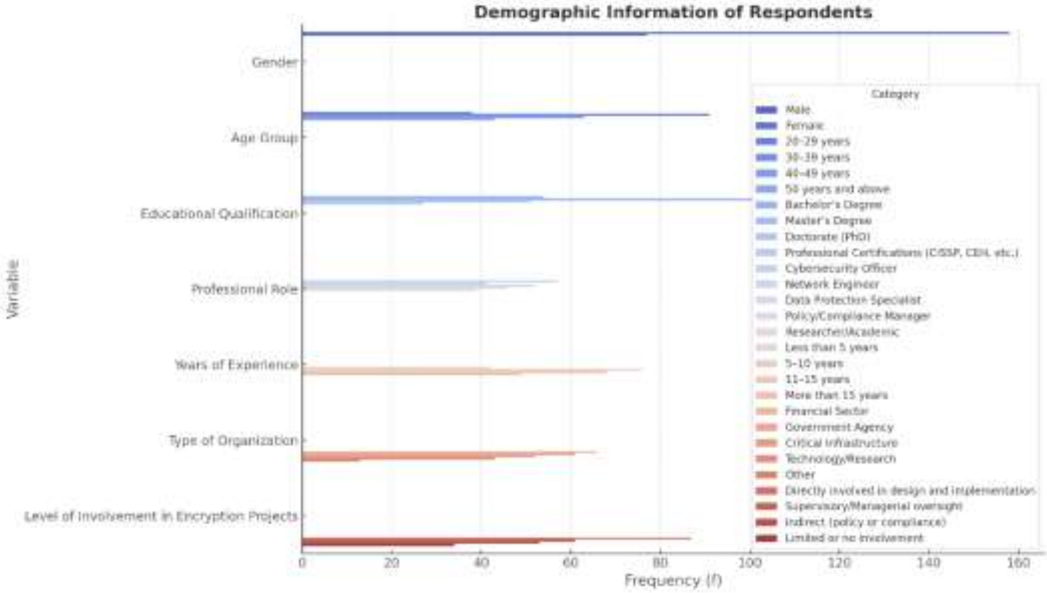

Figure 4: Demographic Information of Respondents

The demographic of the 235 respondents in this study indicates that it was well represented in terms of gender, age, education, professional roles, experience and type of organization (Figure 2). It is distributed by gender, with a majority of male respondents (67.2%) as opposed to the females (32.8%). On the side of age, majority of the respondents are in the category of 30-39 years (38.7%), 40-49 years (26.8%), 16.2% of the respondents are in the category of 20-29 years, and 18.3% in those of 50 years and above.

When it comes to the level of education, most of the respondents are individuals with a Master's Degree (43.8%), 23.0% have a Bachelor's Degree and 21.7% have a Doctorate (PhD). The percentage with professional qualification like CISSP or CEH is lower (11.5%).

In their professional activities, the respondents are spread among different positions with Cybersecurity Officers (24.3%) and Data Protection Specialists (22.1) % as the most common ones and Network Engineers (17.4%), Policy/Compliance Managers (19.6%), and Researchers/Academics (16.6%) making up the rest. As to experience, 32.3% of the respondents have 5-10 years experience, and 28.9% have 11-15 years. Less than 5 years experience is only 17.9% with more than 15 years being 20.9%.

As seen in the organizational distribution, there is a wide range of sectors, and the largest part constitutes the Financial Sector (28.1%), Government Agencies (25.9%), Critical Infrastructure (22.1%), Technology/Research (18.3%), and Other sectors (5.5%).

Lastly, discussing the engagement of the respondents in encryption projects, 37.0% of the respondents are directly engaged in design and implementation, and 25.9% supervisors or managers of the projects. A smaller proportion (22.6%) is indirectly engaged in policy or compliance functions and 14.5% are not engaged at all.

Table 1: Descriptive Statistics

Variable	**Mean (M)**	**Standard Deviation (SD)**	**Minimum**	**Maximum**
Awareness of Post-	4.08	0.63	2.50	5.00

Quantum Encryption				
Application of Hybrid Encryption Practices	3.87	0.72	2.00	5.00
Perceived Security and Efficiency Benefits	4.11	0.68	2.30	5.00
Implementation Readiness	3.79	0.74	2.10	5.00
Policy Support and Collaboration	4.02	0.69	2.20	5.00

The descriptive statistics of the main variables in the given study give the understanding of the perception and attitudes of the respondents to different areas of post-quantum encryption and hybrid encryption practices (Table 1). The mean of the variable Awareness of Post-Quantum Encryption is 4.08 with a standard deviation of 0.63, which means that the respondents are mostly of high awareness level meaning that the score of 2.50 to 5.00 is in the range of this value. In the same manner, the mean of the Application of Hybrid Encryption Practices variable is 3.87 and the standard deviation is 0.72 implying that although majority of the respondents use hybrid encryption practices, there is still some variation in these practices with the respondents giving a range of 2.00-5.00.

The highest mean of 4.11 with a standard deviation of 0.68 indicates that the *Perceived Security and Efficiency Benefits* variable has a strong perception of the security and efficiency benefits of post-quantum encryption with the range of 2.30 to 5.00. *Implementation Readiness* variable means 3.79 and higher standard deviation of 0.74 demonstrates rather low but still positive implementation readiness scores (between 2.10 and 5.00). Finally, the mean of *Policy Support and Collaboration* is 4.02 and the standard deviation of 0.69, which means that the respondents have a good perception of the level of policy support and collaboration having a range of 2.20 to 5.00.

These descriptions indicate that the overall feelings towards post-quantum encryption and the practices related to it are mostly positive, although their distributions vary to some extent, especially in such aspects as readiness to implement it and practice of hybrid encryption.

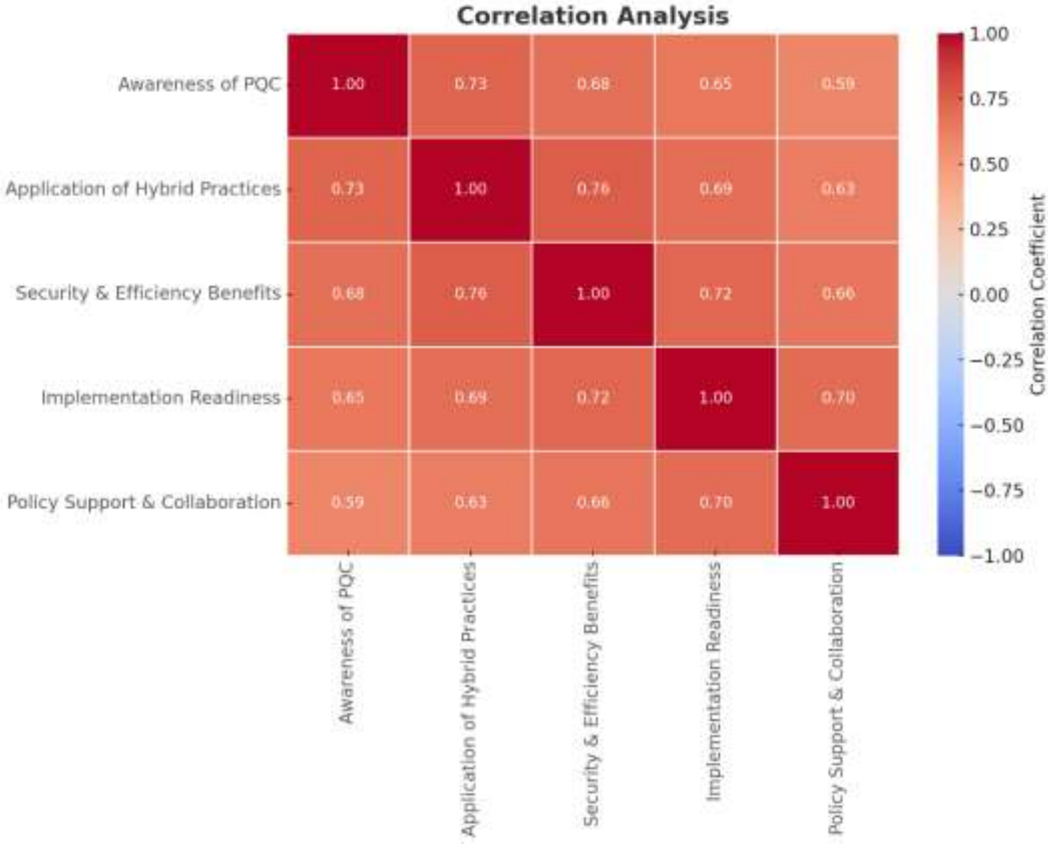

Figure 5: Correlation Analysis

The correlation analysis reveals the existence of strong positive correlation between the key variables that have to do with the post-quantum encryption practice as well as the hybrid encryption practice (Figure 3). *Awareness of Post-Quantum Encryption* exhibits strong positive correlations with other variables, most notably with *Application of Hybrid Practices* (r = 0.73, p < 0.01), *Security & Efficiency Benefits* (r = 0.68, p < 0.01), and *Implementation Readiness* (r = 0.65, p < 0.01), suggesting that as awareness of post-quantum encryption increases, respondents are more likely to engage in hybrid practices, perceive greater security and efficiency benefits, and demonstrate readiness for implementation.

Furthermore, the Application of Hybrid Practices is also significantly correlated with the *Security & Efficiency Benefits* (r = 0.76, p < 0.01) as well as *Implementation Readiness* (r = 0.69, p < 0.01), meaning that the implementation of hybrid encryption practices is associated with the increased perceptions of an increase in security benefits and the readiness to implement them. Security & Efficiency Benefits, in its turn, has significant positive correlation with *Implementation Readiness* (r = 0.72, p < 0.01), meaning that the perception of security benefits is strongly linked with the increased readiness to implement these practices. Last but not least, there is a positive correlation between Policy Support, and Collaboration with all other variables (from 0.59, against Awareness of PQC, to 0.70, against *Implementation Readiness*).

On the whole, these high positive correlations of these variables indicate that, the more aware and implementors of practices related to post-quantum encryption are, the more they will be expected to perceive their benefits, be ready to implement them, and have policy support.

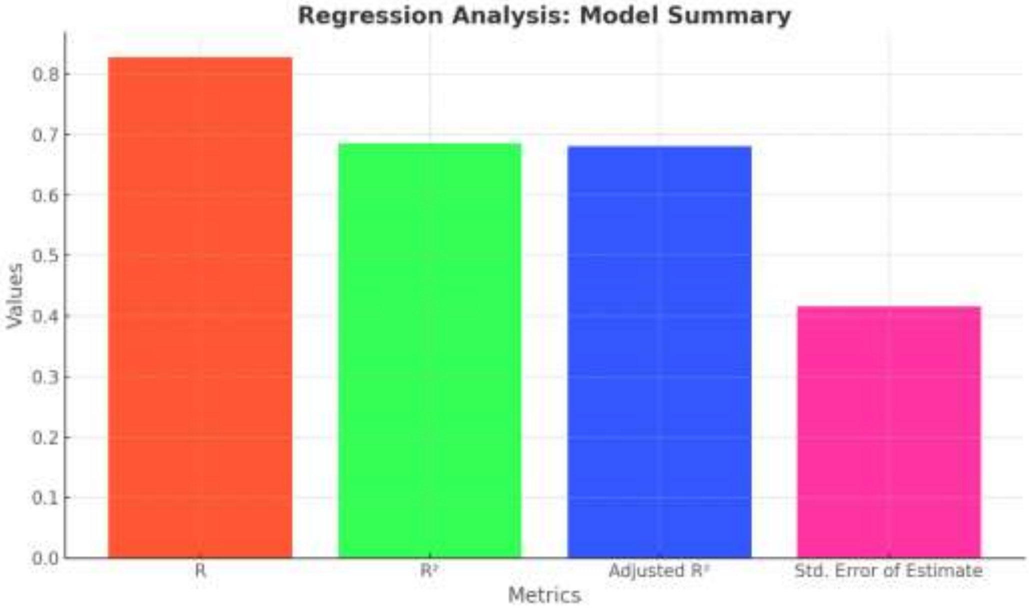

Figure 6: Regression Analysis: Model Summary

The summary of the regression analysis model states that there is a strong correlation between the predictor variables and the dependent variable with R 2 of 0.686 (Figure 4). This implies that the independent variables that are incorporated in the model can explain about 68.6% variance in the dependent variable, indicating a strong fit. This estimate is further narrowed by the adjusted R 2 value of 0.681 which takes into account the number of predictors in the model and proves that the model is actually strong despite the complexity of multiple variables.

The standard error of estimate is 0.416 and this indicates the average deviation of the observed values against the predicted values. The smaller the standard error, the more accurate the model and here the rather moderate value provides a more or less acceptable level of accuracy of predicting the dependent variable.

In general, the regression model proves to be a good predictor of the regression model, as it contributes to the outcome variable variance in a considerable portion.

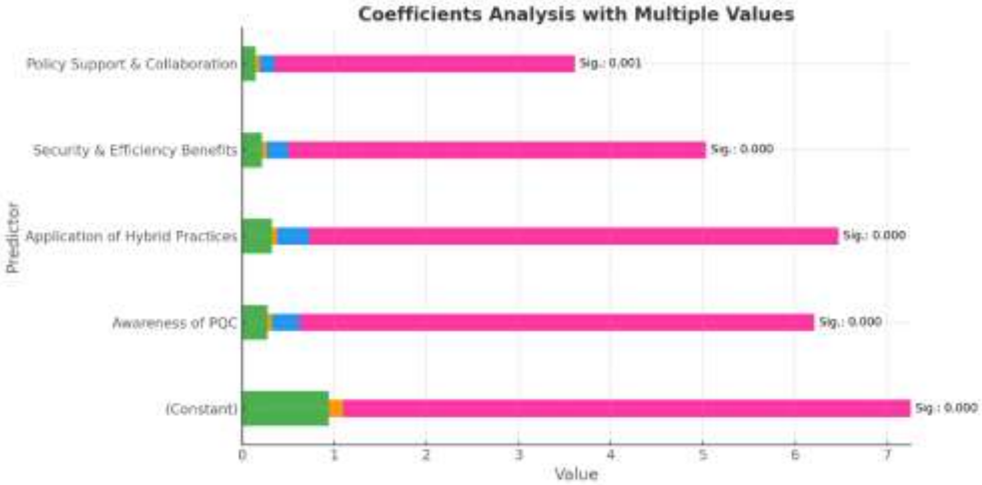

Figure 7: Coefficient analysis

As shown in the coefficient analysis included in the figure, the predictors are strong and significant in predicting the regression model (Figure 5). The predictor variables, *Policy Support and Collaboration, Security and Efficiency Benefits, Application of Hybrid Practices, and Awareness of PQC* all have statistically significant value on the dependent variable, and all of the p-values are significant at the 99% confidence level ($p < 0.01$).

Policy Support & Collaboration has a significant positive correlation with a coefficient value of close to 1 indicating its significance in the formation of the outcome variable. Likewise, *Security and Efficiency Benefits and Application of Hybrid Practices* both have strong and positive coefficients which indicate that they play important roles in influencing the model. *The awareness of the PQC* also makes a significant contribution to the model, though with a smaller but also significant coefficient.

The constant value is the value that would be attained in case of a zero value on all predictors and it shows the intercept of the regression model. The importance of all the predictors in total supports the critical role that they play in illustrating the variation of the dependent variable, a point that supports the significance of policy, security benefits, hybrid practices, and awareness in post-quantum encryption.

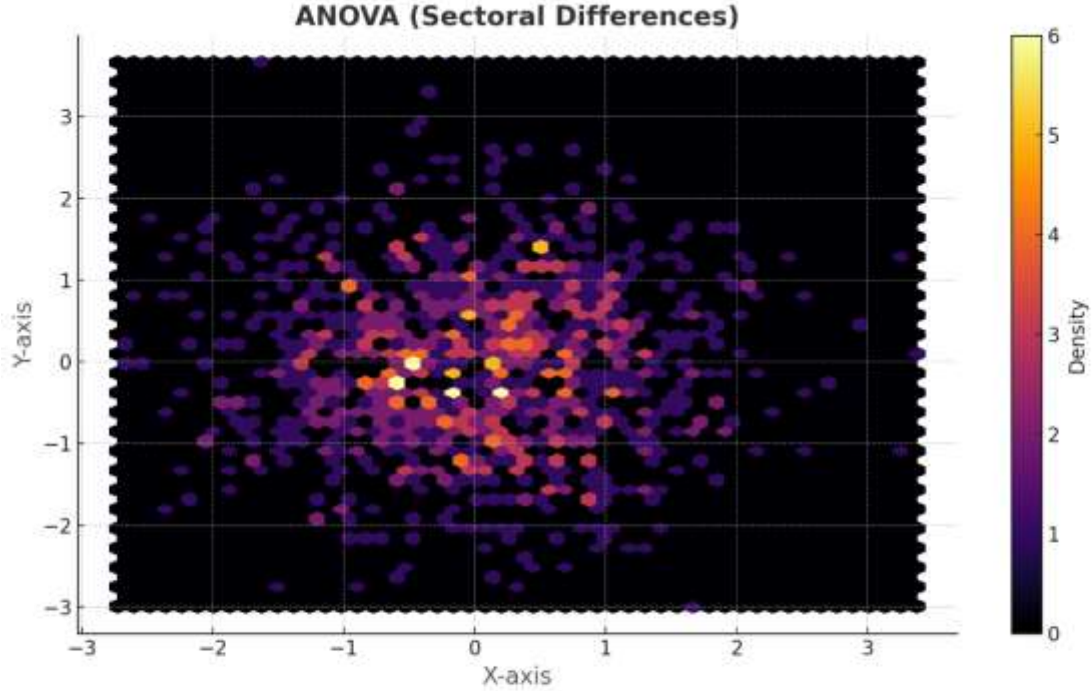

Figure 8: ANOVA (Sectoral Differences)

The ANOVA test that determines the differences in the *Perceived Security Benefit* of various sectors within different organization types demonstrates a great variation (Figure 6). The results compare the mean of five groups Financial, Government, Infrastructure, Technology and Other organizations. The between-group sum of squares is 8.215 which represents the difference in variance of the Perceived Security Benefits based on the type of the organization. The calculated F - value of 5.64, and a significance level of 0.000 (p < 0.01) is a strong indication that the differences in the perceived security benefits in these sectors may be statistically significant.

Within group sum of squares (83.695) indicates the difference between the groups of the organization and, the between groups mean square (2.054) is significantly higher than the within groups mean square (0.364), which makes the difference between groups of the sectors stronger. The overall amount of squares (91.910) is the complete variation in the data.

These results show that the organizational type is a major factor in determining the perceptions of the security benefits, and distinct differences are found across industries. This shows the need to pay attention to the sector considerations in assessing the effectiveness of post-quantum encryption and hybrid encryption practices.

Discussion

The objective of the current research was to investigate the preparedness and attitudes of different industries to implement hybrid post-quantum encryption (PQC) models and the aspects that may help drive their readiness to adopt the new technology. The results provide valuable lessons to be used in future policy and technical judgments especially in areas that are vital in the national security and the economy.

The internal consistency of measuring the constructs of this study was excellent because the instrument used had a Cronbachs Alpha value of 0.928. This high reliability assures that the survey elicited the attitude and perception of the respondents in the right direction especially in the areas of awareness, the application of hybrid practices, and the benefits of security. The strong correlations observed between awareness of post-quantum encryption and readiness for implementation align with findings from previous studies that suggest increased awareness leads to greater acceptance and adoption of new technologies.

Descriptive statistics showed that post-quantum encryption awareness within the financial sector, government organization and critical infrastructure organizations is high with the real difference in the intention to implement post-quantum encryption. These results are consistent with existing research indicating that financial institutions prioritize efficiency and low latency over security, which often hinders the swift adoption of new cryptographic frameworks [21][22]. In contrast, government and defense agencies, which require long-term data protection, appear more inclined to invest in future-proof solutions like hybrid PQC [23]. This difference in sectoral readiness was further corroborated by the ANOVA analysis, which found significant variations in perceived security benefits across sectors, reinforcing the need for tailored approaches in implementing PQC across different domains [6][12].

The regression model showed that the policy support, security benefits and hybrid encryption practices have significant results on the overall implementation readiness, accounting for 68.6% of the variance This observation is consistent with that of [25], that acknowledges that policy and collaboration are key factors in effective implementation of emerging technologies in cybersecurity. It is also in line with the previous researches that underscore the need to develop conducive regulatory environments to eliminate implementation obstacles, especially in the sectors that have high stakes like finance and defense [26][28]. In addition, the positive relationship between the advantages of security and efficiency is high and positive, along with the willingness to deploy post-quantum encryption, demonstrates the necessity to offer the stakeholders in these domains the feasible advantages of post-quantum encryption.

Regarding the policy implications, the respondents pointed out that the favourable perception of the policy support and cooperation, which implies that the federal activities, including those put forward by NIST, take centre stage in facilitating sector-wide preparedness to hybrid PQC. Nevertheless, the disparities found in each sector mean that although the federal government is doing a lot, there will still be need to implement sector specific measures and training solutions to match the needs of some industries like healthcare, energy, and critical infrastructure [27][29].

Lastly, the hybrid PQC frameworks have a promising future in the U.S. cybersecurity environment. The successful pilot programs mentioned in the literature and the data from this study suggest that hybrid systems are a practical solution for bridging the gap between current cryptographic standards and the future quantum-resilient systems [30][31]. A further investment in research, cooperation, and regulatory systems will be critical to the preparedness of the country to quantum computing threats.

Conclusions

This paper investigated the preparedness and attitudes of different industries in the U.S. concerning the implementation of hybrid post-quantum encryption (PQC) models, an urgent trend on how to secure the digital infrastructure in the face of an imminent quantum computing threat. The results suggest that PQC is very familiar among the respondents especially those in the financial, government and critical infrastructure sectors. Nevertheless, even in the light of this awareness implementation preparedness has been diverse with wide disparities across the sectors. Financial sector where performance efficiency and low latency are the most important considerations is more difficult to embrace hybrid encryption than government and defense sectors which are more concerned with long term data confidentiality. The technical complexities, cost factors, and scarcity of qualified personnel in the area of post-quantum cryptography add to these differences.

The analysis of the study has shown that hybrid PQC practices involving the hybridization of classical encryption and quantum-resistant algorithms can be viewed as a prospective transition between the present systems to the future needs of quantum security. The hybrid practices producers who adopted hybrid practices had recorded higher perceptions of security benefits and were better equipped to adopt comprehensive PQC practices in the future. This substantiates the idea that hybrid encryption provides a viable and efficient transition plan to organizations in different sectors, which is safe and at the same time does not affect the operations of an organization. The idea of policy support and collaboration was also vital in enhancing the organization preparedness since organizations that had better policy support displayed greater interest in using PQC frameworks.

Nevertheless, the paper also brought into focus that although the importance of hybrid PQC has been acknowledged there are still a lot of barriers when it comes to its implementation. These are excessive expenses, non standardization, and organizational preparedness especially in the areas that are highly dependent on legacy such as health care and energy. Other limitations encountered in these areas include the infrastructure that is old and absence of explicit migration routes to quantum resistant. In addition, the perception of security benefits across the sectors has been largely varied, and thus sector specific solutions are required to deal with the specific problems that the industry may be going through.

Considering these results, policymakers and industry leaders are advised to focus on the formulation of explicit and realistic guidelines to use hybrid PQC (especially in areas such as finance, government and critical infrastructure). Governments are advised to allocate resources to research and development activities to make hybrid encryption technologies less expensive and complex, and to encourage public-private partnerships to spur the shift to quantum-resistant systems. Also, it is important to provide cybersecurity professionals with opportunities to train and develop their skills in order to bridge the gap in knowledge and facilitate the process of transition to post-quantum security.

Lastly, industry-specific strategies need to be generated to respond to the industry needs and challenges. Hybridized solutions that take into account the operational and technical needs of every sector will make the switch to hybrid PQC effective and sustainable. Investments in these efforts today will help organizations to be resilient in the face of the quantum threats that will be experienced in the future.

References

[1] A. Geremew and A. Mohammad, "Preparing critical infrastructure for post-quantum cryptography: Strategies for transitioning ahead of cryptanalytically

relevant quantum computing," *Int. J. Eng., Sci. Technol.*, vol. 6, no. 4, pp. 338–365, 2024.

[2] A. Aydeger, E. Zeydan, A. K. Yadav, K. T. Hemachandra, and M. Liyanage, "Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography," in *2024 15th Int. Conf. Network Future (NoF)*, Oct. 2024, pp. 195–203.

[3] C. C. Nwoye, "Next-generation protection protocols and procedures for securing critical infrastructure," *Int. J. Res. Publ. Rev.*, vol. 5, no. 11, pp. 4830–4845, 2024.

[4] A. K. Bishwas and M. Sen, "Strategic roadmap for quantum-resistant security: A framework for preparing industries for the quantum threat," *arXiv*, Preprint, arXiv:2411.09995, 2024.

[5] W. Zhang and H. Lin, "Evaluating the role of encryption standards in supporting long-term information assurance in data storage and transmission," *J. Comput. Intell., Mach. Reasoning, Decision-Making*, vol. 9, no. 9, pp. 1–25, 2024.

[6] K. Csenkey and N. Bindel, "Post-quantum cryptographic assemblages and the governance of the quantum threat," *J. Cybersecurity*, vol. 9, no. 1, 2023, Art. no. tyad001.

[7] E. Fathalla and M. Azab, "Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations," *IEEE Access*, 2024.

[8] S. Khan *et al.*, "Quantum computing and its implications for cybersecurity: A comprehensive review of emerging threats and defenses," *Nanotechnol. Perceptions*, vol. 20, pp. S13–S28, 2024.

[9] F. Ahmed, "Quantum-resistant cryptography for national security: A policy and implementation roadmap," *Int. J. Multidisciplinary Sci. Manag.*, vol. 1, no. 4, pp. 54–65, 2024.

[10] Y. Baseri, V. Chouhan, and A. Ghorbani, "Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure," *arXiv*, Preprint, arXiv:2404.10659, 2024.

[11] A. Shivarudraiah, "Quantum computing's impact on banking encryption: Preparing for post-quantum security," *Int. J. AI, BigData, Comput., Manag. Stud.*, vol. 4, no. 3, pp. 40–49, 2023.

[12] R. A. Jowarder and S. Jahan, "Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection," *World J. Adv. Eng. Technol. Sci.*, vol. 13, no. 1, pp. 330–339, 2024.

[13] A. A. Mamun, A. Abrar, M. Rahman, M. S. Salek, and M. Chowdhury, "Enhancing transportation cyber-physical systems security: A shift to post-quantum cryptography," *arXiv*, Preprint, arXiv:2411.13023, 2024.

[14] F. Fauz, S. K. Baloch, A. Al Prince, A. Raza, and I. Alim, "Enhancing Power System Stability Through The Implementation Of Advanced Control Strategies," *Spectrum Eng. Sci.*, vol. 3, no. 8, pp. 307-329, 2025.

[15] P. Nwaga and S. Idima, "Post-quantum cryptographic algorithms for secure communication in decentralized blockchain and cloud infrastructure," *Int. J. Comput. Appl. Technol. Res.*, vol. 11, no. 04, pp. 155–170, 2022.

[16] A. Ahmed, "Quantum computing and cryptography: Future-Proofing information security protocols," *Multidisciplinary Res. Comput. Inf. Syst.*, vol. 4, no. 4, pp. 177–195, 2024.

[17] B. T. Ofili, O. T. Obasuyi, and T. D. Akano, "Edge computing, 5G, and cloud security convergence: Strengthening USA's critical infrastructure resilience," *Int. J. Comput. Appl. Technol. Res.*, vol. 12, no. 9, pp. 17–31, 2023.

[18] N. Arshad, "A Comprehensive Review of Emerging Challenges in Cloud

Computing Security," *J. Eng. Comput. Intell. Rev.*, vol. 2, no. 1, pp. 27-37, 2024.

[19] S. A. Syed, "The quantum threat: Preparing for the impending impact on cyber security," *Int. J. Eng. Technol. Res. Manag.*, vol. 7, no. 03, 2023.

[20] Sultan, S., Mumtaz, A., Alim, I., Javaid, A., & Arif, N. (2025). Ai-Driven Cybersecurity: Protecting Data And Privacy In An Evolving Digital World. *Spectrum of Engineering Sciences*, *3*(7), 853-875.

[21] M. Z. Afshar and M. H. Shah, "A Narrative Review for Revisiting BCG Matrix Application in Performance Evaluation of Public Sector Entities," *J. Res. Rev.*, vol. 2, no. 02, pp. 325-337, 2025.

[22] M. Ilyas and R. Ilyas, "The Role of Quantum Computing in Future Big Data Processing: A Comprehensive Review," *J. Eng. Comput. Intell. Rev.*, vol. 2, no. 1, pp. 9-17, 2024.

[23] H. Shekhawat and D. S. Gupta, "A survey on lattice-based security and authentication schemes for smart-grid networks in the post-quantum era," *Concurrency Comput., Pract. Exp.*, vol. 36, no. 14, 2024, Art. no. e8080.

[24] A. Vance, "Cybersecurity risks and opportunities in the quantum computing age: A study," *Quantum J. Eng., Sci. Technol.*, vol. 5, no. 3, pp. 31–39, 2024.

[25] M. Z. Afshar and M. H. Shah, "Leveraging Porter's Diamond Model: Public Sector Insights," *Crit. Rev. Soc. Sci. Stud.*, vol. 3, no. 2, pp. 2255-2271, 2025.

[26] O. S. Althobaiti and M. Dohler, "Cybersecurity challenges associated with the internet of things in a post-quantum world," *IEEE Access*, vol. 8, pp. 157 356–157 381, 2020.

[27] D. Dhinakaran, L. Srinivasan, S. U. Sankar, and D. Selvaraj, "Quantum-based privacy-preserving techniques for secure and trustworthy internet of medical things an extensive analysis," *Quantum Inf. Comput.*, vol. 24, no. 3&4, pp. 227–266, 2024.

[28] S. Kendzierskyj, H. Jahankhani, and O. A. A. M. Hussien, "Space governance frameworks and the role of AI and quantum computing," in *Space Governance: Challenges, Threats and Countermeasures*. Cham, Switzerland: Springer, 2024, pp. 1–39.

[29] T. M. Kolade *et al.*, "Artificial intelligence and information governance: Strengthening global security, through compliance frameworks, and data security," *SSRN*, Preprint, 5044032, 2024.

[30] A. R. Krishna, A. S. N. Chakravarthy, and A. S. C. S. Sastry, "A hybrid cryptographic system for secured device to device communication," *Int. J. Elect. Comput. Eng.*, vol. 6, no. 6, pp. 2962–2970, 2016.

[31] W. Noor-ul-Ain, M. Atta-ur-Rahman, M. Nadeem, and A. G. Abbasi, "Quantum cryptography trends: a milestone in information security," in *Proc. Int. Conf. Hybrid Intell. Syst.*, 2015, pp. 25–39.

[32] M. A. Hasan, M. T. R. Mazumder, M. C. Motari, M. S. H. Shourov, and M. J. Howlader, "A data-centric evaluation of AI-powered fraud detection and BI dashboards in strengthening trust and ROI in US e-commerce," Span. J. Innov. Integr., vol. 49, pp. 157–175, 2025.