Scholars Journal of Engineering and Technology

OPEN ACCESS

Abbreviated Key Title: Sch J Eng Tech
ISSN 2347-9523 (Print) | ISSN 2321-435X (Online)
Journal homepage: https://saspublishers.com

Preparing AI-Powered Healthcare Security Systems to be Resilient Against Quantum Computing Threats

Gaurang Deshpande[1*]

[1]Software Developer, IBM, USA

DOI: 10.36347/sjet.2023.v11i12.004 | Received: 15.11.2023 | Accepted: 28.12.2023 | Published: 30.12.2023

*Corresponding author: Gaurang Deshpande
Software Developer, IBM, USA

Abstract **Original Research Article**

Healthcare powered by artificial intelligence is revolutionising the way patients are treated: AI helps diagnose intelligently and lets one manage data intelligently. Nevertheless, this is under threat with the emergence of quantum computing, which threatens to crack all established cryptographic protection in these systems. Currently, this study aims to explore how ready AI-powered healthcare security systems are to counter attacks based on quantum computing. It discusses present vulnerabilities, and considerations of post-quantum cryptographic protections and provides quantum resilience strategic measures. Based on secondary data analysis, literature review, and case studies, the study highlights the major gaps and offers a road map to make safe AI applications in healthcare. Research results underline the importance of implementing quantum-resistant technologies in the short term to maintain long-term data integrity and protection against the system.

Keywords: Artificial Intelligence, Healthcare Security, Quantum Computing, Post-Quantum Cryptography (PQC), Data Protection, AI Resilience.

I. INTRODUCTION

A. Background

AI technologies are becoming more and more popular in healthcare systems in terms of diagnostics, data about patients, and efficiency. Yet, it is also associated with a series of cybersecurity concerns. Quantum computing has rendered new crashes in the traditional means of cryptographic security that defend AI systems [1]. With quantum computers, most encryption methods used can be cracked in theory, and the data thus exposed has the potential to be sensitive healthcare data. Since medical records are very valuable and sensitive, there is a strong need to explore how ready AI-based healthcare systems are to confront quantum-based threats. Enhancement of cybersecurity systems to resist post-quantum exploits is a new prior concern to trust, privacy, and information integrity in healthcare processes.

B. Overview

This study investigates the adversity of healthcare security systems based on AI against the upcoming quantum computing threat [2]. It examines state-of-the-art AI-security specifications and measures how they resist quantum adversaries, and probes post-quantum cryptographic systems. This research will entail qualitative and secondary research techniques to carry out a structured resource on security preparedness. The results will advise the stakeholders to invest in quantum-resilient approaches to protecting patient data and ensuring the continuity of their operations as the cyber environment continues to change.

C. Aims and Objectives

The research aims to analyse and suggest efficient measures for equipping healthcare security systems with quantum computing developments using AI. The objectives of this research are: 1) To analyse current security architectures of AI-enabled healthcare systems. 2) To evaluate the possible effects of quantum computing on the present encryption measures. 3) To investigate post-quantum encryption systems that can be used in the protection of healthcare data. 4) To suggest strategic methods to place quantum-resistant technologies in AI medical systems.

D. Problem Statement

Although AI has enhanced the effective delivery of healthcare, it has also presented various security threats and risks, more so when pitted against equally powerful quantum computing. Existing security measures in the current AI systems cannot withstand quantum decryption potentials [3]. This presents a serious vulnerability in readiness, with the chances of the privacy of health records being exposed and manipulation of the system. Unless actively implemented, the quantum-resistant security models can be easily violated by sophisticated threats, putting the patient's safety and privacy in jeopardy at an unprecedented scale.

E. Scope and Significance

This study focuses on AI-enabled security networks in healthcare settings, especially those involved in processing sensitive information including medical records (electronic health records or EHRs), diagnostics, and treatment plans [4]. It also puts focus on the vulnerability of such systems to quantum-brought cyber risks. This study is important because the issue of healthcare breaches extends globally beyond the prospects of financial and legal solutions as well as ethical and life-threatening responses. Healthcare systems need to move on to an encryption system that can handle quantum computing advances as the computing approaches practical usage [5]. The study provides societal and scientific insight into the work, as it proposes a futuristic view of AI cybersecurity. It will seek to help policymakers, IT managers, and AI developers in healthcare to broadly anticipate how risks will grow and develop healthcare data and systems with effective scalable protective measures.

II. LITERATURE REVIEW

A. Current Security Architectures in AI-enabled Healthcare Systems

The authors note that AI in the healthcare sector is also becoming more dependent on cloud-based environments that protect their informational content with standard encryption, such as AES and RSA [6]. However, at the same time, they fail to ensure the security of their content in the face of quantum-based nightmare attacks. They substantiate that the existing architectures are focusing on efficiency instead of being future-proof, a factor that might leave systems vulnerable to arising vulnerabilities. The author also focuses on the dependence on centralised data systems, although, despite facilitating and ensuring real-time diagnostics and predictive analytics, they contain an unacceptable risk of single points of failure [7]. An example is the 2020 ransomware attack on the *University Hospital Düsseldorf (UKD)* in Germany, which was a reminder that unprepared healthcare AI infrastructure poses a threat to patient safety. Comprising these authors, there is a need to implement the gradual development of AI security frameworks to suit the intelligence and delicateness of healthcare applications.

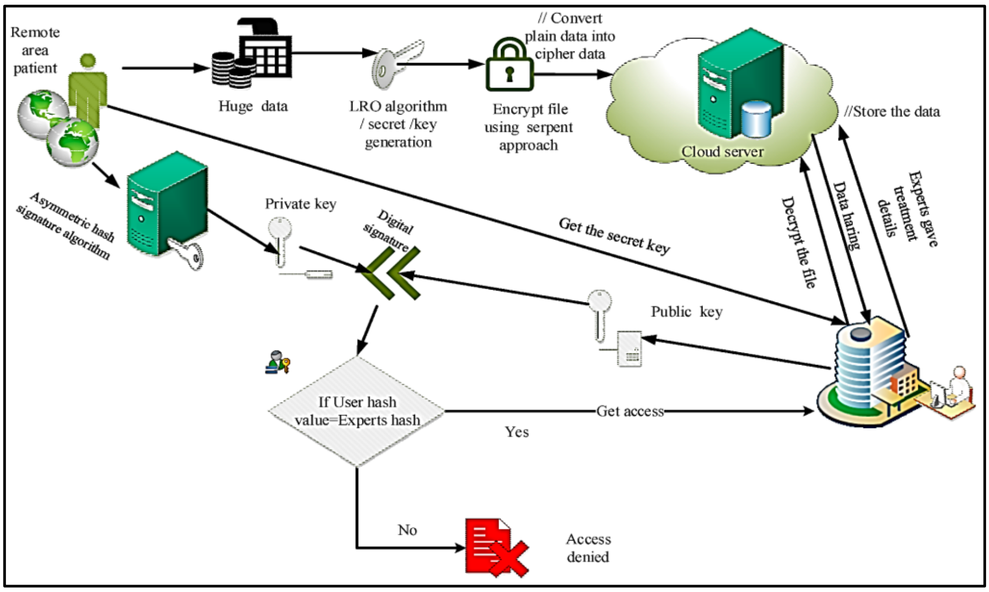
Remote area patient
Huge data
LRO algorithm / secret /key generation
// Convert plain data into cipher data
Encrypt file using serpent approach
Cloud server
//Store the data
Asymmetric hash signature algorithm
Private key
Digital signature
Get the secret key
Decrypt the file
Data haring
Experts gave treatment details
Public key
If User hash value=Experts hash
Get access
Yes
No
Access denied

Figure 1: Managing Security of Healthcare Data for a Modern Healthcare System [7]

B. Impact of Quantum Computing on Existing Cryptographic Methods

The threat to digital security was realised through a post which showed that quantum computers could crack RSA encryption, and ECC encryption fairly easily; it did show QCs could crack RSA and ECC encryption using a polynomial-time algorithm [8]. Expanding on this point, the author notes the so-called quantum risk timeline, whereby information goes encrypted these days but can be harvested and then decrypted in the future when quantum computers have grown sufficiently. Such a threat of harvest now and decrypting later is particularly significant to healthcare, in which patient information is long-term sensitive [9]. In a specific case, it can be stated that hospitals with RSA-encrypted EHRs are in danger of retrospective attacks after quantum capabilities are implemented. These views reinforce the fact that the current encryption systems, which are quite robust in the current setting, cannot provide the same security promises in the post-quantum era and therefore, AI-based healthcare systems will need a proactive move towards post-quantum cryptography.

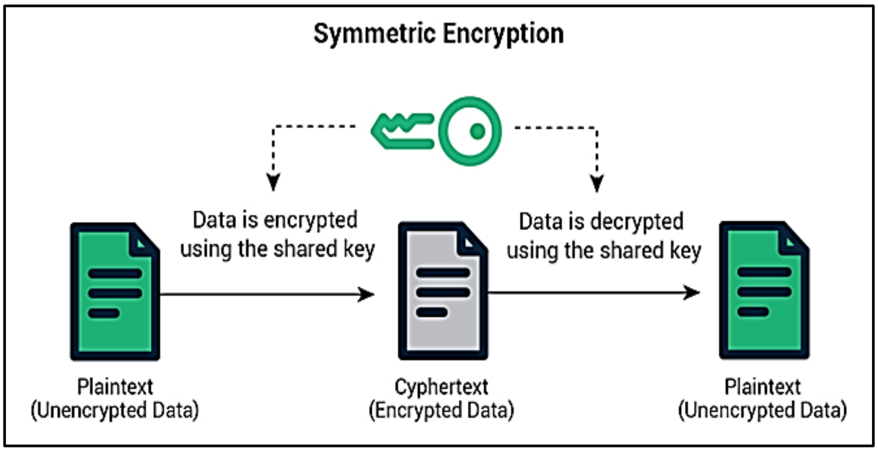
Symmetric Encryption
Data is encrypted using the shared key
Data is decrypted using the shared key
Plaintext (Unencrypted Data)
Cyphertext (Encrypted Data)
Plaintext (Unencrypted Data)

Figure 2: Quantum-Safe Cryptography and Encryption
[9]

C. Exploration of Post-Quantum Cryptographic Solutions for Healthcare Systems

In their report on NIST, the authors have broken down the post-quantum cryptographic (PQC) solutions into three groups that include lattice-based, hash-based, and multivariate cryptosystems with the lattice-based systems (e.g., CRYSTALS-Kyber) being promising because they are highly secure and fast [10]. They indicate that they are appropriate in health care as they have a low computational burden. Likewise, the author introduces NewHope (based on lattices) into consideration and shows that the protocol exhibits better results on embedded devices, which is of interest to applications of AI-powered IoT of the medical sort [11]. As an example, securing the patient's vitals with PQC on wearable sensors may store information securely in the long term, even when the data falls into the wrong hands at the time of interception. Both authors believe that the early adoption and integration of PQC into AI processes will make healthcare systems future-proof without compromising the efficiency and integrity of their systems.

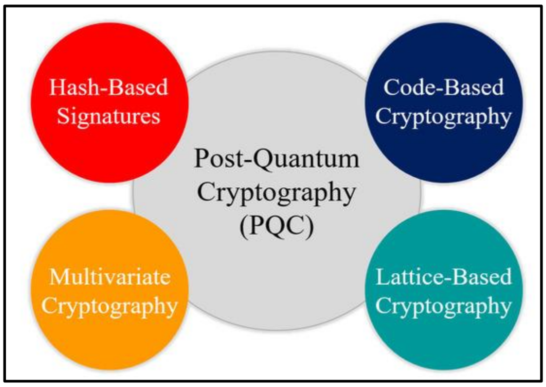
Hash-Based Signatures
Code-Based Cryptography
Post-Quantum Cryptography (PQC)
Multivariate Cryptography
Lattice-Based Cryptography

Figure 3: Post-Quantum Cryptosystems
[10]

D. Strategic Recommendations for Enhancing Quantum-Resilience in AI Healthcare Security

The author sustains that quantum resilience should become a strategic priority, and suggests hybrid encryption schemes, where classical and post-quantum algorithms are mixed in the transition phase [12]. They pay attention to internal preparedness that involves staff training and infrastructure checks. The author also witnessed a phased approach to integration, observing that quantum upgrades should be consistent with larger system plans for modernisation to reduce disruption [13]. As an illustration, seamless expansion can be guaranteed by implanting QR-API on AI diagnostic instruments when they are undergoing regular software updates. Both authors believe in the need for cooperation across sectors, governments, providers of technologies and healthcare institutions, to promote standardisation and attract funding. These views highlight the importance of the fact that the technical issues cannot be fully resolved to achieve quantum-immune AI healthcare assistants; planning, regulation, and overall systemwide coordination are crucial to long-term development.

III. METHODOLOGY

A. Research Design

The *explanatory* research design is used in this research study to explore how AI-driven healthcare systems may be shielded against threats posed by quantum computing. It is aimed at discussing the connections between new quantum abilities and the existing weak spots of AI-based healthcare infrastructure. The research will also suggest adequate mitigation measures by identifying these interconnections. Post-quantum cryptography, vulnerabilities of the system architecture, and possible solutions can be systematically studied based on conceptual frameworks, academic sources, and practice with the use of the explanatory approach.

B. Data Collection

In this study, *secondary* research involving both *quantitative and qualitative data* will be used to collect data. In the case of qualitative data, academic journals, white papers, government reports, and cybersecurity frameworks are used. Quantitative data extracted through the existing charts and graphs of industry surveys, breach statistics, and benchmarking authors to study the level of encryption standards and AI applications in healthcare. This combination of methods gives a clear idea of how and what is vulnerable, how it is prepared, and how it is expected to be impacted by quantum computing to present an evidence-based and balanced analysis of the situation.

C. Case Studies/Examples

Case Study 1: IBM Cleveland Clinic Partnership

The relationship between IBM and Cleveland Clinic is aiming at the combination of quantum computing and AI to enhance biomedical research [14]. Although it has the innovation potential, it puts new security threats on AI systems. This case demonstrates how the topic of post-quantum cryptography should be integrated into the work of future AI healthcare at an early stage to prevent possible data leakage in the event of quantum cryptography cracking.

Case Study 2: NHS Digital Data Security Centre (UK)

The security structure of NHS Digital uses the concept of AI to identify any occurrence of a cyber-threat within the UK health sector [15]. Current systems however use classical encryption, and this might be vulnerable to quantum attacks. The case demonstrates the importance of NHS and other comparable organisations shifting towards quantum-resistant cryptographic programs around the availability of medical data to patients.

D. Evaluation Metrics

The research uses some critical evaluation criteria to determine how well AI-assisted security systems in healthcare are equipped to handle quantum threats. These are encryption strength scores that assess the capability of the cryptographic algorithm resistant environments to quantum attacks and system vulnerability index, a measure of susceptibility to future quantum-based compromise [16]. The integration of post-quantum cryptography (PQC) is measured by the adoption level. Moreover, the levels of data breaches in terms of the extent and prevalence are considered to grasp the weaknesses in the past. Lastly, the policy and compliance readiness is evaluated to ascertain compliance with the emerging cybersecurity regulations. The combination of these metrics will allow one to have a full picture of how the system is resilient to the quantum threat and where it can be enhanced.

IV. RESULTS

A. Data Presentation

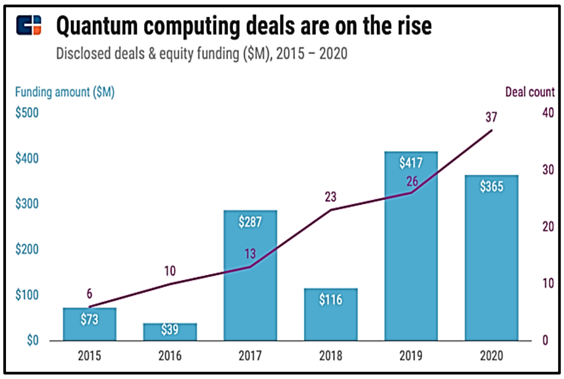

Figure 4: Dealings of quantum computing
[17]

According to the graph shown above, the number of deals and the sum of funding in quantum computing have gone up drastically from 2015 up to the year 2020. The amount of funding increased as compared to 2015 when it was only $73M to reach its peak level of $417M in 2019 and slightly declined in 2020 to the amount of $365M [17]. The number of deals doubled to 37 in 2020 when compared to 2015 where there were 6 deals. This price increase indicates the increased commercial interest and investor confidence in quantum technologies showing the closeness of real-world applications of quantum technologies. This means the great need to have AI-healthcare systems ready to face quantum threats.

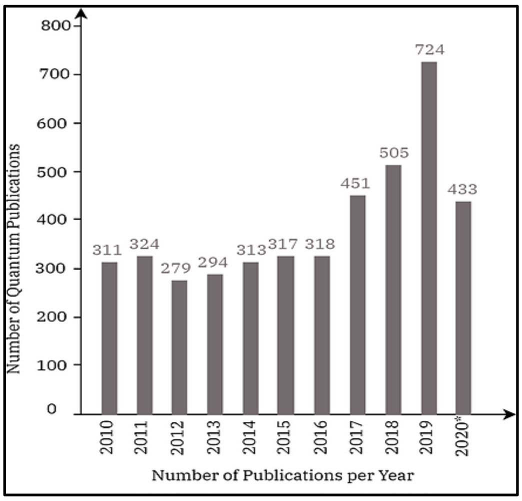

Figure 5: Present landscape of quantum computing [18]

The chart shown above presents a stable increasing trend in the number of publications related to quantum reaching up to 724 in 2019. The number of published figures was 279 to 324 per year between 2010 and 2016 [18]. There was a drastic increase after 2017, which is a hallmark of greater research focus and innovations in semantics. Although the number slightly decreased in 2020 (433 publications), the steady amount of publications is a testament to the academic concern over the development of the quantum domain around the world [18]. This solidifies the importance of post-quantum security course action in risky areas such as the pursuit of healthcare with the majority of healthcare AI innovations.

B. Findings

In this research, the findings from the graphs reveal a sharp growth in the number of investments in quantum computing and the publishing of academic articles growth between 2015 and 2020 [17]. Business investment in the quantum deals had tripled showing an increased industry interest and the reality that it is drawing nearer. At the same time, there is a similarly sharp increase in the output of publications related to quantum issues, which indicates an increasing academic interest and technical development [18]. According to these trends, quantum computing is evolving quicker than expected, and controversies are already posing risks to industries requiring conventional cryptography, such as healthcare. The results demonstrate the urgency of healthcare systems powered by AI to implement post-quantum cryptographic protection of sensitive information before the quantum-based threats are well-built and fully operational to crack the current security systems.

C. Case Study Outcomes

Case Study	Outcome Summary
IBM–Cleveland Clinic	Highlighted early-stage integration of quantum and AI, showing promise but security vulnerability [14].
NHS Digital (UK)	Demonstrated advanced AI use but lacked post-quantum security measures, indicating urgent upgrade needs [15].

The case study table above presents practical learning lessons for healthcare organisations, showing the potential security needs and the existing security gaps of AI systems in front of emerging quantum threats.

D. Comparative Analysis

Authors	Aspects of Literature Review	Focus	Key Findings	Gaps Identified
[6]	Data encryption in healthcare	Combined DNA computing with AES for image security	Multi-layer encryption enhances protection [6]	Lacks post-quantum resilience consideration

Authors	Aspects of Literature Review	Focus	Key Findings	Gaps Identified
[7]	Diagnostic technology in healthcare	A REASSURED diagnostic framework for health systems	Improves decision-making and patient care	There is no emphasis on cybersecurity in AI frameworks [7]
[8]	Quantum threats in blockchain	Post-quantum defence in cryptocurrency	Quantum resistance needs long-term planning [8]	Application in healthcare security not explored
[9]	HIPAA and healthcare data compliance	Data protection using mobile computing	Reinforces the importance of legal compliance	No technical countermeasures for quantum threats [9]
[10]	Lattice-based cryptography	Evaluation of NIST PQC algorithms	Identifies secure algorithms for PQ era	Needs integration study with AI healthcare systems [10]
[11]	Hardware for PQC	Sapphire crypto-processor for lattice protocols	Hardware can support efficient PQ encryption	Not tested in real healthcare environments [11]
[12]	Impact of Quantum Supremacy	Threats to traditional encryption in finance	A strong case for immediate PQC shift	Lacks focus on healthcare-specific AI systems [12]
[13]	Software modernisation	Adapting legacy systems for quantum tech	Advocates quantum-readiness in design [13]	No healthcare-specific implementation strategies

The comparative analysis table above summarises important findings of the literature on encryption, quantum risks and healthcare data security and defines critical gaps in research on post-quantum cryptography integration to AI-driven healthcare infrastructures.

V. DISCUSSION

A. Interpretation of Results

The findings closely correlate with the literature research and case studies showing an overall rush to quantum computing around the world. With increased amounts of research and money, AI-driven healthcare systems are poorly positioned. Other works by authors emphasise the threats posed by trusting classical forms of encryption and case studies reveal real-world lapses in system preparedness [9, 10]. The NHS experience demonstrates the application of operational AI but aged security systems, which further demonstrates the necessity to switch to quantum-resistant models [15]. The partnership between IBM and the Cleveland Clinic is both promising and serves as a reminder of the fact that innovation needs to go hand in hand with active encryption initiatives [14]. To be resilient against new quantum risks, the healthcare system should therefore implement hybrid encryption, focus more on post-quantum training, and match with the international cybersecurity standards.

B. Practical Implications

The study highlights why healthcare providers must future-proof their AI systems in a bid to keep them quantum-ready. Post-quantum cryptography (PQC) adoption will keep data secrets safe and make it compliant in the future. Medical information technology departments should deploy quantum-resistant algorithms to the current AI platform, which does not affect the real-time aspect. [19] Partnerships of the vendors, also, must focus on quantum-secure APIs and encryption frameworks. The results sensitise policymakers, IT workers, and cybersecurity companies that there is an urgent need to invest in training, system and country-wide standardisation of healthcare encryption models.

C. Challenges and Limitations

The uncertainty of when quantum supremacy will take place is another critical problem that may make it hard to establish a priority of funding by healthcare institutions [20]. In addition, there is a shortage of standardised post-quantum algorithms to implement. Most AI systems are coupled with legacy infrastructure hence upgrades are very costly and cumbersome [21]. Secondary data also has been used as a foundation of the study, and it does not completely show real-time development and region-based vulnerability. The use of case studies may not allow generalisation because they apply to a small number of institutions. Nevertheless, the study can offer a strategic basis upon which quantum-resilient security planning can be moderated in an AI-empowered attractive healthcare setting.

D. Recommendations

Healthcare systems need to start classical and post-quantum hybrid integration now. To determine weak legacy systems, stakeholders should focus on staff training and frequent audits. Strategic alliances with quantum research centres and cybersecurity companies are needed to keep abreast with the changing cryptographic standards [19]. Governments ought to stimulate quantum-safe upgrades through funding and control. Quantum resiliency should be implemented by AI developers in system design. Mixed-method research should be used in future research to compute the research results using empirical data as opposed to secondary studies as was done in this research.

VI. CONCLUSION & FUTURE WORK

Quantum investment research plays a significant role in advancing quantum capabilities, meaning that quantum attacks against AI-based healthcare systems are no longer hypothetical but tangible. Healthcare data are extremely insecure with the present status of classical encryption being used. Using literature analysis, case studies and data trends, and this study provides a strong basis for the necessity of the urgent implementation of post-quantum cryptography and planning. In the future, collecting primary data should be involved in audits of healthcare IT and interviews with quantum security consultants. Moreover, it may be useful to test post-quantum cryptographic algorithms on live healthcare AI systems in real time to gain practical experience. The observance of global quantum progress and interdisciplinary cooperation will remain central in the effort to realise sound, quantum-resistant healthcare safety in the era of AI.

REFERENCES

1. Varma, R., Melville, C., Pinello, C. and Sahai, T., 2021. Post-quantum secures command and control of mobile agents inserting quantum-resistant encryption schemes in the secure robot operating system. *International Journal of Semantic Computing*, *15*(03), pp.359-379.
2. Jimmy, F., 2021. Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defences. *Valley International Journal Digital Library*, *1*, pp.564-74.
3. Batista, E., Moncusi, M.A., López-Aguilar, P., Martínez-Ballesté, A. and Solanas, A., 2021. Sensors for context-aware smart healthcare: A security perspective. *Sensors*, *21*(20), p.6886.
4. Das, J., 2020. Leveraging Cloud Computing for Medical AI: Scalable Infrastructure and Data Security for Advanced Healthcare Solutions. *INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS*, *7*, pp.504-514.
5. Ndiaye, F., 2021. The Role of Quantum Computing in Shaping the Future of Advanced Computational Systems. *Journal of Advanced Computing Systems*, *1*(8), pp.1-9.
6. Madhloom, J.K., Abd Ghani, M.K. and Baharon, M.R., 2021. Enhancement to the patient's health care image encryption system, using several layers of DNA computing and AES (MLAESDNA). *Periodicals of Engineering and Natural Sciences (PEN)*, *9*(4), pp.928-947.
7. Land, K.J., Boeras, D.I., Chen, X.S., Ramsay, A.R. and Peeling, R.W., 2019. REASSURED diagnostics to inform disease control strategies, strengthen health systems and improve patient outcomes. *Nature Microbiology*, *4*(1), pp.46-54.
8. Stewart, I., Ilie, D., Zamyatin, A., Werner, S., Torshizi, M.F. and Knottenbelt, W.J., 2018. Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack. *Royal Society Open Science*, *5*(6), p.180410.
9. Mbonihankuye, S., Nkunzimana, A. and Ndagijimana, A., 2019. Healthcare data security technology: HIPAA compliance. *Wireless communications and mobile computing*, *2019*(1), p.1927495.
10. Imran, M., Abideen, Z.U. and Pagliarini, S., 2020. An experimental study of building blocks of lattice-based NIST post-quantum cryptographic algorithms. *Electronics*, *9*(11), p.1953.
11. Banerjee, U., Ukyab, T.S. and Chandrakasan, A.P., 2019. Sapphire: A configurable crypto-processor for post-quantum lattice-based protocols. *arXiv preprint arXiv:1910.07557*.
12. Sachin, D., 2020. The Impact of Quantum Supremacy on Cryptography: Implications for Secure Financial Transactions. *Int J Sci Res CSE & IT, 6*(4), p.611-637.
13. Pérez-Castillo, R., Serrano, M.A. and Piattini, M., 2021. Software modernization to embrace quantum technology. *Advances in Engineering Software*, *151*, p.102933.
14. Ibm.com, 2021. *Cleveland Clinic and IBM Unveil Landmark 10-Year...* Available at: https://newsroom.ibm.com/2021-03-30-Cleveland-Clinic-and-IBM-Unveil-Landmark-10-Year-Partnership-to-Accelerate-Discovery-in-Healthcare-and-Life-Sciences (Accessed On: 10th July 2022)
15. Nhs.uk, 2022. *Data Security Centre assurance.* Available at: https://digital.nhs.uk/coronavirus/vaccinations/data-security-centre-assurance (Accessed On: 10th July 2022)
16. Dommari, S., 2021. Exploring the Security Implications of Quantum Computing on Current Encryption Techniques. *Available at SSRN 5259341*.
17. Cbinsights.com, 2021. *What does the quantum computing landscape look like?* Available at: https://www.cbinsights.com/research/report/quantum-computing/ (Accessed On: 15th September 2022)
18. Wiley.com, 2020. *The present landscape of quantum computing.* Available at: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-qtc.2020.0027 (Accessed On: 15th September 2022)
19. Bremner, M., Clark, R., Bartlett, S. and Lam, P.K., 2021. The impact of quantum technologies on secure communications.
20. Aartsma-Rus, A., Dooms, M. and Le Cam, Y., 2021. Orphan medicine incentives: how to address the unmet needs of rare disease patients by optimizing the European orphan medicinal product landscape guiding principles and policy proposals by the European expert group for orphan drug incentives (OD expert group). *Frontiers in pharmacology*, *12*, p.744532.

21. Konda, R. End-to-End Observability in API-Driven Architecture using MuleSoft and Prometheus.
22. Chintale P: Optimizing data governance and privacy in Fintech: leveraging Microsoft Azure hybrid cloud solutions. Int J Innov Eng Res. 2022, 11:
23. Crawford, K., 2021. *The atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.
24. Goli, S. R., & Goli, A. K. R. (2022). Strengthening Data Governance and Privacy: Utilizing Amazon AWS Cloud Solutions for Optimal Results. *Available at SSRN 5317148*.
25. Goli, Arun Kumar Reddy. "DEVOPS METRICS THAT MATTER: BUSINESS IMPACT OF DORA AND SRE RELIABILITY INDICATORS."