IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

Enhancing Cyber Security Using Quantum Computing and Artificial Intelligence: A Review

Shoumya Singh[1] and Deepak Kumar[2]
orcid.org/0009-0001-9541-6177 and orcid.org/0009-0009-2137-0864
Department of Computer Science, San Francisco Bay University, CA, USA[1]
Department of Information Technology, University of the Cumberlands, KY, USA[2]

Abstract: *This article examines the transformative potential of quantum computing in addressing the growing challenge of cyber threats. With traditional encryption methods becoming increasingly ineffective against sophisticated cyber attacks, quantum computing emerges as a promising solution, offering unparalleled computational capabilities for enhancing cyber security. This technology is poised to revolutionize how we protect sensitive data by developing quantum-resistant encryption algorithms and quantum-based machine learning modules to safeguard critical infrastructures. By exploring the intersection between quantum computing and cyber security, this article highlights the opportunities, challenges, and prospects of leveraging quantum advancements to strengthen our defenses against the evolving landscape of cyber threats.*

Keywords: Quantum Computing, Cyber Security, Machine Learning, Artificial Intelligence

I. INTRODUCTION

The current cybersecurity landscape presents numerous challenges that call for reevaluating traditional approaches. One of the foremost concerns is the susceptibility of current encryption protocols to quantum computing-based attacks(NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers, 2023). With the continuous advancement of quantum computers, the risk of decrypting sensitive data encrypted using conventional methods grows significantly. This impending threat emphasizes the need for the development of quantum-resistant encryption techniques. Another major challenge in cybersecurity is the persistence and evolution of sophisticated cyber attacks. From ransomware and phishing scams to state-sponsored cyber warfare, these threats are becoming increasingly intricate and complex to thwart using traditional security measures(Yalçın et al., 2024). With its unparalleled computational power, Quantum computing has the potential to provide advanced threat detection and mitigation capabilities that surpass the limitations of classical computing.Furthermore, the interconnected nature of modern technology infrastructures amplifies cyber-attacks impact, posing risks to critical sectors such as finance, healthcare, and energy. Quantum computing offers an opportunity to bolster the resilience of these infrastructures by enabling the development of robust cryptographic protocols and enhancing the security of interconnected systems(Rehman, 2024).As we navigate these challenges, it becomes clear that integrating quantum computing into cybersecurity strategies presents a proactive and necessary approach to ensure comprehensive protection against emerging threats. The following sections will explore the opportunities and implications of harnessing quantum computing to effectively address these pressing cybersecurity challenges.

II. IMPORTANCE OF DEVELOPING ADVANCED CYBERSECURITY MEASURES

Given the increasing cyber threats, the significance of enhancing advanced cybersecurity measures cannot be emphasized enough. With the rise of interconnected devices and the digitization of critical infrastructures, the potential impact of cyber-attacks has reached unparalleled levels(Microsoft, 2024). Therefore, it is crucial to prioritize the development of solid cybersecurity measures that can effectively protect sensitive data, secure essential services, and reduce the risk of disruptive cyber incidents(EBR, 2024). As we observe the swift evolution of cyber threats, the necessity for advanced cybersecurity measures becomes even more compelling. Traditional security protocols and encryption techniques are increasingly susceptible to sophisticated attacks, requiring a shift towards quantum-resistant

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

algorithms and innovative security solutions(Pereira, 2024). By embracing quantum computing and utilizing its computational power, developing advanced cybersecurity measures can significantly improve digital systems andinfrastructure resilience(NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers, 2023).Moreover, cyber attack's economic and societal consequences emphasize the urgency of advancing cybersecurity measures. The potential financial losses, damage to reputation, and disruption of critical services resulting from cyber incidents underscore robust cybersecurity's crucial role in safeguarding the digital ecosystem's stability and integrity(Aurangzeb et al., 2024).

Additionally, developing advanced cybersecurity measures is of utmost importance to mitigate evolving cyber threats and ensure the security and resilience of digital systems(A.I. Technology is Invaluable for Cybersecurity, 2023). By leveraging the potential of quantum computing and advancing encryption techniques, proactive measures can be implemented to strengthen cyber defenses and stay ahead of emerging threats. This proactive approach is essential for fostering a secure and trustworthy digital environment in the face of relentless cyber challenges.

Quantum Computing Principles:

Quantum computing applies the principles of quantum mechanics to solve intricate calculations and computational problems that exceed the capabilities of classical computers. Unlike classical bits, Quantum computing uses quantum bits or qubits, which can exist in multiple states simultaneously due to superposition(Conversation, 2023). This unique feature enables quantum computers to process and analyze vast amounts of data concurrently, resulting in exponential increases in computing power for specific problem types(IBM Says It's Made a Big Breakthrough in Quantum Computing, 2023). Entanglement, another fundamental principle of quantum computing, happens when the quantum states of multiple qubits become interdependent, allowing the correlation of information across different qubits(Bei, 2023). This characteristic enables quantum computers to efficiently handle complex algorithms and factor large numbers at speeds that surpass classical computers, making them particularly suitable for cryptographic applications(Hoefler et al., 2023). Figure 1 shows the architecture of Quantum Computing (B.Shodi, 2018).

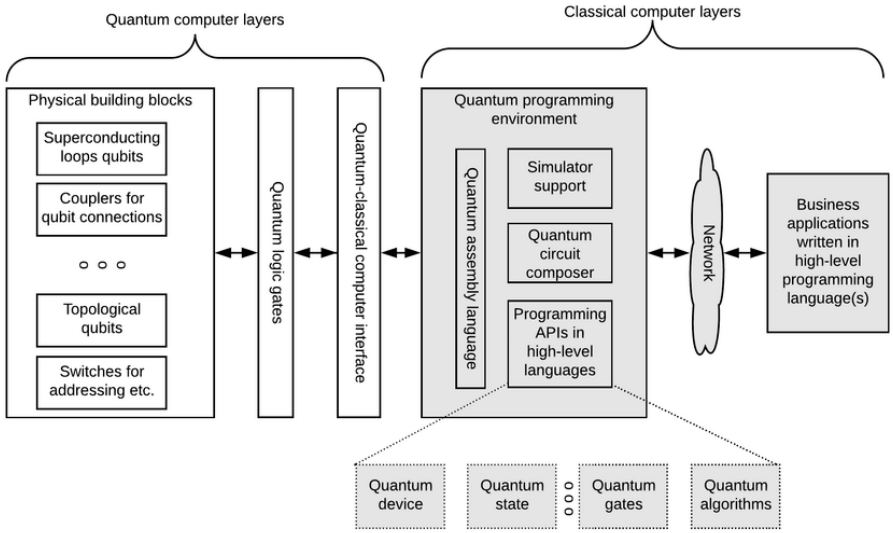

Figure 1: Architecture of Quantum Computing

Quantum computing also employs the concept of quantum interference, where quantum algorithms manipulate the probability amplitudes of qubits to enhance desired outcomes and suppress unwanted results(Nourbakhsh et al., 2022). This distinct property enables quantum computers to execute operations remarkably efficiently, offering a potential advantage in solving optimization and search problems relevant to cybersecurity.The potential of quantum computing to revolutionize various fields, including cybersecurity, is significant. Its ability to process and analyze vast amounts of data in parallel, along with its potential to advance encryption techniques, opens up new frontiers in cybersecurity(NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers, 2023). By leveraging the unique

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

properties of quantum computing, such as superposition and entanglement, it becomes possible to address existing vulnerabilities and fortify the resilience of encryption methods in the face of advancing cyber threats(Rehman, 2024)

Quantum Computing in Cryptography:

The emergence of quantum computing has significant implications for cybersecurity, especially in cryptography. Traditional cryptographic techniques, such as RSA and ECC, rely on the difficulty of factoring large numbers for security. However, quantum computers can efficiently factor large numbers using algorithms like Shor's algorithm, which presents a substantial risk to the security of encrypted data(NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers, 2023). In response to this threat, the cybersecurity community has been focused on developing post-quantum cryptographic algorithms that can resist quantum-based attacks. Post-quantum cryptography encompasses many encryption techniques, including lattice-based cryptography, code-based cryptography, and multivariate cryptography. These methods are designed to withstand the computational power of quantum computers, thereby reducing the risk posed by quantum-based attacks on traditional cryptographic systems(Yalamuri et al., 2022). Artificial Intelligence-based algorithms can manage and optimize these quantum keys, adapting to security needs in real-time and ensuring that data transmission between parties is impenetrably secure (Gonaygunta, H. et al.2024).Adopting post-quantum cryptographic algorithms is expected to enhance cybersecurity by offering robust protection against potential threats from quantum computing. Following is the sudo code for data encryption and decryption based on Quantum Computing.

```
Generate_keypair(public_key, private_key)
function Encrypt(plaintext, public_key)
    Initialize quantum_resistant_algorithm(parameters)
    ciphertext = quantum_resistant_algorithm.encrypt(plaintext, public_key)
    return ciphertext
function Decrypt(ciphertext, private_key)
    Initialize quantum_resistant_algorithm(parameters)
    plaintext = quantum_resistant_algorithm.decrypt(ciphertext, private_key)
    return plaintext
End
```

Quantum Computing for Threat Detection and Mitigation:

Apart from its impact on encryption, quantum computing shows promise for improving threat detection and mitigation in cybersecurity. The exceptional computational power of quantum computers allows for efficient analysis of large-scale data sets and rapid identification of patterns that indicate cyber threats(Baker, 2024). By harnessing quantum computing's processing power, Artificial Intelligence can automate complex security protocols that are impractical with classical computing. This includes the dynamic adaptation of encryption algorithms based on threat level analysis, enhancing the robustness of cyber defenses.This potential for accelerated data processing and pattern recognition aligns with the changing landscape of cyber-attacks, where quick detection and response are crucial for mitigating the impact of security breaches(com, 2023). Moreover, quantum computing's ability to solve optimization problems can be used to enhance cybersecurity measures(Jadhav et al., 2023). Tasks such as network optimization, resource allocation, and vulnerability assessment can benefit from the computational efficiency of quantum algorithms, leading to more effective and proactive security strategies.Figure 2 shows the uses of Quantum computing in cyber security, while Figure 3 shows the complete flow diagram of Threat detection and mitigation using Quantum Computing.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

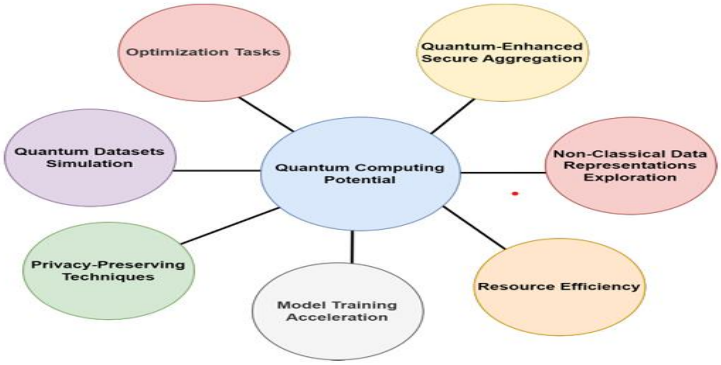

Figure 2: Quantum Computing &AI Use in Cyber Security

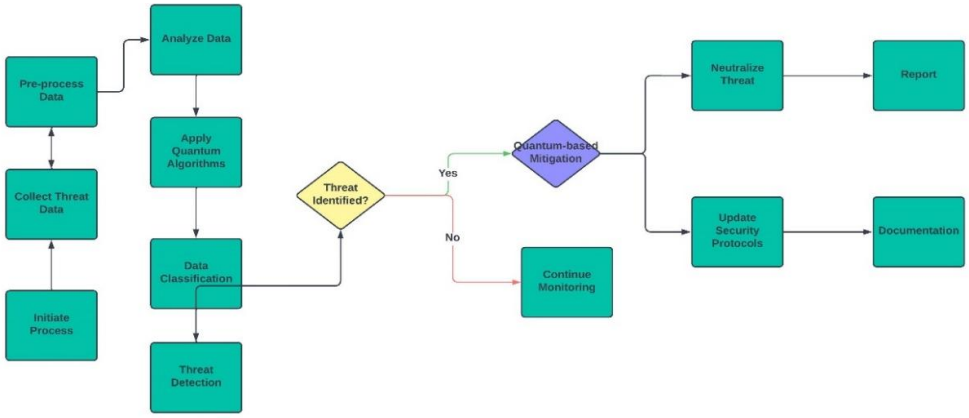

Figure 3: Flow diagram of threat detection using Quantum Computing

Quantum-Enhanced Security Protocols:

Quantum Random Number Generators: It provide true randomness for cryptographic security, leveraging quantum phenomena to generate unpredictable and unbiased random numbers. This enhances the robustness of cryptographic protocols(Renner & Wolf, 2023).

Quantum Secure Communication: The advancement of secure communication protocols utilizing quantum mechanics is a significant breakthrough in cybersecurity. Quantum secure communication leverages the principles of quantum key distribution to establish secure and inherently unhackable communication channels(Tobias, 2024).Quantum key distribution (QKD) uses quantum properties such as the Heisenberg uncertainty principle to facilitate the secure exchange of encryption keys between communicators(Renner & Wolf, 2023). By transmitting quantum states, any attempt to intercept or eavesdrop on the communication would disrupt the quantum nature of the transmitted information, thus alerting the communicating parties to the presence of an intrusion. This innovative approach to secure communication shows great potential in protecting sensitive information against unauthorized access and interception, making it a valuable asset in cybersecurity measures.

III. QUANTUM THREATS USE CASE AND ETHICAL & REGULATORY CONSIDERATION

The rapid advancement of quantum computing presents unprecedented challenges for traditional cryptographic methods. Quantum computers have the potential to efficiently factor large numbers using algorithms like Shor's algorithm, posing a significant risk to the security of encrypted data. In response to these quantum threats, the cybersecurity community focuses on developing post-quantum cryptographic algorithms that resist quantum-based attacks. Various post-quantum cryptographic techniques have been proposed, including lattice-based cryptography, code-based cryptography, and multivariate cryptography. These encryption schemes aim to withstand the computational

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

power of quantum computers, ensuring that data remains secure in the quantum computing era. As organizations and governments prepare for the era of quantum computing, integrating post-quantum cryptographic algorithms is essential for fortifying the foundations of cybersecurity and safeguarding sensitive information from potential quantum-based attacks.

Quantum-Resistant Encryption in Government and Enterprise Systems:

As the looming quantum threat poses a risk to current cryptographic systems, government agencies and enterprises increasingly prioritize adopting quantum-resistant encryption to protect their sensitive information(Yalçın et al., 2024). Case studies that showcase the integration of post-quantum cryptographic solutions in government and enterprise systems can provide valuable insights into the practical challenges and advantages of transitioning to quantum-resistant encryption(Yalamuri et al., 2022). Exploring the experiences of organizations incorporating post-quantum cryptographic algorithms in their security protocols can offer valuable insights into the operational impact, performance considerations, and best practices for deploying quantum-resistant encryption(Nouri, 2023). These case studies serve as valuable resources for organizations looking to strengthen their cybersecurity defenses in preparation for the quantum computing era. By examining the real-world applications of quantum-resistant encryption in government and enterprise environments, we can gain valuable insights into the feasibility and effectiveness of post-quantum cryptographic solutions in various operational settings(NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers, 2023).

Future Prospects and Research Directions

As quantum computing progresses, it is set to revolutionize the cybersecurity landscape, necessitating significant evolution in encryption methods. Quantum cybersecurity research explores enhancements in quantum encryption and novel approaches surpassing traditional cryptographic methods(Davies, 2024). A pivotal area of focus is the development of quantum-resistant algorithms designed to counteract the superior computational capabilities of quantum computers, ensuring long-term data security against quantum threats(Frank, 2024).Combining quantum encryption with security protocols offers a promising research trajectory. This involves leveraging quantum communication and cryptography to strengthen cybersecurity frameworks by integrating conventional encryption techniques(Davies, 2024). The application of quantum-resistant encryption in burgeoning fields like the Internet of Things (IoT) and cloud computing is also gaining attention(Raja, 2024). This seeks to secure the increasingly interconnected and distributed digital infrastructure, addressing contemporary security challenges.Research is not limited to technological advancements but also encompasses the human and behavioral dimensions of secure communication, focusing on quantum encryption's usability and user experience to facilitate broader adoption and practical implementation(Davies, 2024).Future research will likely delve into optimizing these hybrid models to harness quantum advantages fully(G, 2024). Areas of interest may include the design of more efficient quantum circuits tailored for specific machine learning tasks, exploring noise-resistant quantum algorithms to cope with the limitations of Noisy Intermediate Scale Quantum technology, and developing novel quantum-classical data encoding methods.

Additionally, extensive testing and benchmarking against classical models will be critical in assessing the practical superiority of quantum-inspired models (GonayguntaH, et al. 2024). Furthermore, as quantum hardware evolves, machine learning applications will likely benefit from increased qubit counts, improved coherence times, and quantum error correction, driving the field towards realizing quantum advantage in practical cybersecurity applications(Aurangzeb et al., 2024).

Emphasizing collaboration between quantum physicists, machine learning experts, and cybersecurity professionals will also advance this interdisciplinary field(Yalçın et al., 2024). Through these combined efforts, machine learning with quantum computing is positioned to play a significant role in future cybersecurity solutions.

Lastly, the future of quantum cybersecurity research is inherently multidisciplinary, blending scientific, technological, and human-centric studies to enhance encryption resilience and effectiveness in the quantum computing age, safeguarding sensitive information against new threats.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

Ethical and Regulatory Considerations in Quantum-Cybersecurity:

The intersection of quantum technology and cybersecurity raises various ethical and regulatory considerations that require thorough examination. As we embrace the potential of quantum computing to transform encryption methods, it is essential to carefully navigate the ethical dimensions of utilizing quantum cybersecurity solutions responsibly(Cybersecurity of Quantum Computing: A New Frontier, 2023).One of the primary ethical considerations revolves around the implications of quantum computing for data privacy and security. As quantum-resistant encryption methods become essential for safeguarding sensitive information, assessing the ethical implications of potential variations in data security capabilities across different sectors and regions is crucial(Aurangzeb et al., 2024). Ethical frameworks that advocate for equity and fairness in implementing quantum-cybersecurity solutions are crucial in ensuring that the advantages of enhanced encryption are accessible to everyone(Yalamuri et al., 2022)

Additionally, regulatory considerations are critical in shaping the adoption and deployment of quantum-cybersecurity solutions. As quantum-resistant encryption methods evolve, regulatory frameworks must adapt to address the unique characteristics of quantum technology and its implications for data protection(Securing Data for a Post-Quantum World, 2023). Balancing innovation with regulatory compliance is a complex yet essential endeavor in establishing a secure and regulated environment for quantum-cybersecurity advancements. The intersection of quantum technology and cybersecurity raises various ethical and regulatory considerations that require thorough examination. As we embrace the potential of quantum computing to transform encryption methods, it is essential to carefully navigate the ethical dimensions of utilizing quantum cybersecurity solutions responsibly.

IV. CONCLUSION

In conclusion, quantum computing poses unprecedented challenges to traditional cryptographic methods, necessitating the development and integration of post-quantum cryptographic algorithms. As organizations and governments prepare for the quantum computing era, quantum-resistant encryption is increasingly prioritized to protect sensitive information. Case studies showcasing the integration of post-quantum cryptographic solutions provide valuable insights into the practical challenges and advantages of transitioning to quantum-resistant encryption. Quantum algorithms also optimize Artificial Intelligence processes, enabling more robust encryption and rapid anomaly detection. This synergy promises robust protection against sophisticated cyberattacks, ensuring data integrity and security in an increasingly digital world. Future research is focused on enhancing quantum encryption, extending its applications to fields like the Internet of Things, and addressing the human-centric aspects of secure communication. Ethical and regulatory considerations are crucial in ensuring equitable access and compliance when implementing quantum-cybersecurity solutions.

REFERENCES

[1] A.I. Technology is Invaluable for Cybersecurity. (2023, October 26). https://www.smartdatacollective.com/ai-technology-is-invaluable-for-cybersecurity/

[2] Aurangzeb, M., Wang, Y., Iqbal, S., Naveed, A., Ahmed, Z., Alenezi, M., & Shouran, M. (2024, June 1). Enhancing cybersecurity in smart grids: Deep black box adversarial attacks and quantum voting ensemble models for blockchain privacy-preserving storage. https://doi.org/10.1016/j.egyr.2024.02.010

[3] B. Sodhi, "Quality attributes on quantum computing platforms," ArXiv, vol.abs/1803.07407, 2018

[4] Baker, B. (2024, March 27). Quantum A.I. Model Improves Early Cyber Threat Detection. https://aibusiness.com/quantum-computing/quantum-ai-model-improves-early-cyber-threat-detection

[5] Bei, F G L D L J X T Z. (2023, October 13). Quantum computing: principles and applications. https://arxiv.org/abs/2310.09386

[6] Com, C. (2023, January 1). Cyber Security Assessment Services. https://cybersecop.com/cybersecurity-assessment-services

[7] Conversation, T. (2023, November 24). A computer scientist explains how quantum advantage could change the world. https://www.fastcompany.com/90987214/a-computer-scientist-explains-how-quantum-advantage-could-change-the-world

[8] Cybersecurity of Quantum Computing: A New Frontier. (2023, April 10). https://doi.org/10.58012/rzmt-m258.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

[9] Davies, B. (2024, April 11). Quantum Encryption: Pioneering Cybersecurity Advancements. https://www.azoquantum.com/Article.aspx
[10] EBR, E. (2024, February 9). Securing Critical Infrastructure: Protecting Vital Systems from Cyber Threats - The European Business Review. https://www.europeanbusinessreview.com/securing-critical-infrastructure-protecting-vital-systems-from-cyber-threats/
[11] Frank, B J L. (2024, May 20). Post-Quantum Security: Origin, Fundamentals, and Adoption. https://arxiv.org/abs/2405.11885
[12] G, C C H L D M A M B K A D. (2024, May 17). Resource-Efficient Hybrid Quantum-Classical Simulation Algorithm. https://arxiv.org/abs/2405.10528
[13] Gil-Fuster, E., Eisert, J., & Bravo-Prieto, C. (2024, March 13). Understanding quantum machine learning also requires rethinking generalization. https://doi.org/10.1038/s41467-024-45882-z
[14] Gonaygunta, H., Nadella, G. S., Pramod Pawar, P., & Kumar, D. (2024). Enhancing cybersecurity: The development of a flexible deep learning model for enhanced anomaly detection. 2024 Systems and Information Engineering Design Symposium (SIEDS). https://doi.org/10.1109/sieds61124.2024.10534661
[15] Gonaygunta, H., Nadella, G. S., Pawar, P. P., & Kumar, D. (2024). Study on empowering cyber security by using Adaptive Machine Learning Methods. 2024 Systems and Information Engineering Design Symposium (SIEDS). https://doi.org/10.1109/sieds61124.2024.10534694
[16] Hoefler, T., Häner, T., & Troyer, M. (2023, April 21). Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage. https://doi.org/10.1145/3571725
[17] IBM Says It's Made a Big Breakthrough in Quantum Computing. (2023, June 16). https://futurism.com/ibm-breakthrough-quantum-computing
[18] J, C M V G H H C L C P. (2023, March 16). Challenges and Opportunities in Quantum Machine Learning. https://arxiv.org/abs/2303.09491
[19] Jadhav, A., Rasool, A., & Gyanchandani, M. (2023, January 1). Quantum Machine Learning: Scope for real-world problems. https://doi.org/10.1016/j.procs.2023.01.235
[20] Microsoft, C B. (2024, May 3). Prioritizing security above all else. https://blogs.microsoft.com/blog/2024/05/03/prioritizing-security-above-all-else/
[21] NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers. (2023, August 24). https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers
[22] Nourbakhsh, A., Jones, M N., Kristjuhan, K., Carberry, D., Karon, J., Beenfeldt, C., Shahriari, K., Andersson, M., Jadidi, M., & Mansouri, S S. (2022, January 1). Quantum Computing: Fundamentals, Trends and Perspectives for Chemical and Biochemical Engineers. https://doi.org/10.48550/arxiv.2201.02823
[23] Nouri, N N W A W O A. (2023, January 11). Managing the Migration to Post-Quantum-Cryptography. https://arxiv.org/abs/2301.04491
[24] Pereira, D. (2024, April 4). Quantum Day (aka "Q-Day") is a Gray Rhino Stridently Galloping Straight at Your Organization. https://www.oodaloop.com/archive/2024/04/04/quantum-day-aka-q-day-is-a-gray-rhino-stridently-galloping-straight-at-your-organization/
[25] Raja, L T R G J. (2024, January 31). Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization. https://arxiv.org/abs/2401.17538
[26] Rehman, M U. (2024, February 1). Quantum-enhanced chaotic image encryption: Strengthening digital data security with 1-D sine-based chaotic maps and quantum coding. https://doi.org/10.1016/j.jksuci.2024.101980
[27] Renner, R., & Wolf, R. (2023, May 1). Quantum Advantage in Cryptography. https://doi.org/10.2514/1.j062267
[28] Securing Data for a Post-Quantum World. (2023, March 8). https://www.gao.gov/products/gao-23-106559
[29] Tobias, J N C H N D H A A E L H N N L B E A U L G. (2024, February 29). Future proofing network encryption technology (and securing critical infrastructure data) with continuous-variable quantum key distribution. https://arxiv.org/abs/2402.18881
[30] Yalamuri, G., Honnavalli, P B., & Eswaran, S. (2022, January 1). A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats. https://doi.org/10.1016/j.procs.2022.12.086

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

[31] Yalçın, H., Daim, T., Moughari, M M., & Mermoud, A. (2024, April 1). Supercomputers and Quantum Computing on the Axis of Cyber Security. https://doi.org/10.1016/j.techsoc.2024.102556

BIOGRAPHY

Dr. Deepak Kumar completed a B.E from Visvesvaraya Technological University, Karnataka, India 2008, an M. S in Computer Science from San Francisco Bay University, CA, USA, in 2016, and a Doctor of Philosophy in Information Technology from the University of the Cumberlands, KY, USA, in 2022. He has ten years of experience in software development, where he worked with different technologies like Java, Python, SQL, Big Data, Real-time ingestion systems, visualization tools, etc. Currently, he works for the most prominent social media company, where he deals with Petabyte of data, privacy, security, compliances, data warehouse, data migration, visualization, and development of end-to-end data ingestion pipelines to secure and move data across the globe. He has multiple certifications in data privacy and security, software tools,and technologies. He has experience in different domains like airlines, banking, FMCG, social media, transportation, etc. As a researcher, he is interested in IoT, Big Data, Machine Learning, AI, Blockchain, Cyber Security, etc.

Shoumya Singh completed a B.E from Mumbai University, Maharastra, India, in 2013, an M.E in Information Technology from SRH Hochschule, Heidelberg, Germany, in 2017, and an M.S. in Computer Science from the San Francisco Bay University, CA, USA, in 2022. She has seven years of experience in software and hardware development and has worked with different technologies like Java, Python, C, Matlab, Web Development, Hardware in Loop, Robotics, etc. She was associated with Siemens, BMW, and Fraunhofer IPA. Her areas of interest are machine learning, AI, and more.