**Name:Jawad Ahmad(020)**

**Name:Salahuddin(031)**

**Name:Yasar(193)**

**1.Introduction:**

Quantum computers have the ability and power to make innovations in many sectors, but will also increase the chances of cyber threats. Quantum computers can tackle big data that thousands of traditional computers can't do, so they are much more dominant in performing complicated tasks. Yet quantum computers are still in early stages to be not considered a cybersecurity threat. Quantum computing, conversely, will play a vital role in shifting the development of technology. Quantum computing is a downside for all sectors, like health, finance, and every crucial sector, like online currencies such as cryptocurrency. Quantum computing is not only hazardous for cybersecurity, but our passwords are not safe from this, so protective actions must be taken in advance.

Quantum computing has come with revolutionary strength to shift the pace of development in every field. Even so, this authority comes with cons, so we must check the worst side and take precautions. As we are discussing the power quantum computers hold, we must learn about encryption techniques and how we ensure data integrity accordingly. We'll discuss how quantum computing works and how it is hazardous for cybersecurity, determine the risks for encryption techniques, give solutions or protective measures we must consider, and talk about the pros and cons of quantum-resistant encryption.

In the early twentieth century, communication technology was limited to texting, calling, etc. But in the early twenty-first century, it is not only extended to that but also means control of industrial machines, money transfer in finance, autonomous vehicles, smart homes, etc. So, performing such a confidential task required that our communication be hardened and encrypted. Cyber risks are very dangerous for self-driving vehicles and smart cities. In the near future we can predict that self-driving vehicles will be used for transport and shipment, which are operating on communication technologies; a little error will result in life-threatening results. Moreover, modern wars are now fought with cyber attacks like jamming of radar systems, defence systems, and attacks on nuclear facilities. Cybersecurity actually means ensuring protective measures from cyber threats. So we need to cope with and tackle threats of quantum computing, which are more lethal than thousands of traditional computers.

Quantum computing is growing at a very fast pace, which creates new ways for innovation as well as poses a serious threat to already conventional cybersecurity techniques. Quantum computers work using qubits at very high speed; qubits represent zero and one states at the same time. Quantum computers hold the strength of cracking the encryption technique faster as compared to traditional computers. The most hazardous issue every sector is facing is because of quantum computing. Quantum computers can break down large numbers into their prime factors with exponential efficiency. The risk to confidential data and cyberattacks is gradually increasing for sectors where data integrity is needed, and they are facing these issues. So, one must take precautions by developing algorithms that can tackle quantum computing attacks or encryption techniques.

**2.Literature Review:**

Quantum computers are superior to supercomputers, due to which cybersecurity is at high risk. A quantum computer uses qubits, which are much faster than the traditional bits. It can break the high encryptions within seconds and become a severe danger for personal and financial data. as it uses advanced scientometric techniques like bibliometric analysis, which can help to study the map research activities and get through the technological process. Many researchers indicated that the advancements in quantum computers can demolish the building blocks of cybersecurity. Furthermore, various encryption methods, like robust, are in process to remove the vulnerabilities from encryption methods.[1]

Quantum computing has become one of the rising issues for cybersecurity in the current time. It is casting severe threats to the data security of various sectors. Consequently, RSA and ECC encryption methods are in great danger. The data in the soft form can be secured by using algorithms like Shor’s and Grover’s, which are very tense for data integrity and confidential data. Therefore, necessary steps should be taken to prevent these threats in advance to ensure data security.[2]

The advancing communication technology of the 21st century has made this world a global village, as well as the critical infrastructure and services that rely on it. Nevertheless, the emerging rate of cybersecurity threats may play a role in the cyber apocalypse in this regard, which can disrupt the traditional infrastructure. The current cryptography is in high danger due to Shor's algorithm, which allows the quantum computer to compromise the security of data and faster transactions. These flaws can lead the world to cyber apocalypses very soon as the advancements are included in the quantum computers. To prevent these vulnerabilities, two techniques are pursued. Quantum key distribution and post-quantum cryptography, which should be adapted to ensure data security.[3]

Quantum computers are making cybersecurity algorithms advanced, as by using quantum computing qubits, we can easily crack algorithms that a common computer takes thousands of years to solve. Many critical institutions like banking, health, and defence are under great threat because of quantum computing. In 2019, Google achieved a great breakthrough in quantum computing by using it to solve something impossible to solve in 200 seconds. Sectors just need to adopt quantum-resistant algorithms to ensure security and data integrity.[4]

Quantum computing is giving tough competition to already available cybersecurity algorithms, so it is necessary to make strong algorithms to face quantum computers. Today's encryption algorithms are at great risk of quantum, so we must take action to eradicate risks. All institutions must follow a well-planned strategy and keep records of all the algorithms so we can check pros and cons and develop strong security features accordingly. These steps for cybersecurity will ensure future threats of quantum computing and will guarantee data integrity.[5]

**3.Methodology:**

**4.Citations:**

[1]. https://www.sciencedirect.com/science/article/pii/S0160791X24001040

[2].https://cryptodeeptech.ru/doc/Quantum\_Computing\_and\_Cybersecurity\_Navigating\_Emerging\_Threats\_and\_Mitigation\_Strategies.pdf

[3]. https://ieeexplore.ieee.org/abstract/document/10551387#full-text-header

[4] .https://www.researchgate.net/profile/Shoeb-Ali-Syed/publication/390456241\_THE\_QUANTUM\_THREAT\_PREPARING\_FOR\_THE\_IMPENDING\_IMPACT\_ON\_CYBER\_SECURITY/links/67ee7a7a03b8d7280e1e4fd9/THE-QUANTUM-THREAT-PREPARING-FOR-THE-IMPENDING-IMPACT-ON-CYBER-SECURITY.pdf

[5].https://www.researchgate.net/publication/388732360\_Adapting\_Cybersecurity\_Risk\_Management\_for\_the\_Quantum\_Future