e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

A QUANTUM REVIEW: CYBER SECURITY AND EMERGING TECHNOLOGIES

Abhishek Agnihotri[*1], Ishika Pandya[*2]

[*1,2]Student, Computer Science, RMD School of Engineering, Pune, Maharashtra, India.

ABSTRACT

Cyber technologies have become a integrated part of lives, whether it's personal life, the socio-economic, Military or any other aspect of life. But the most important question arises, is it secured? and if it is then to what extent? Nowadays information is transferred in Computer Networks .This information or data can be business, military data, academic data, research data, etc. it is shared either on a public or a private network. Security in this transfer of data and the communication is increasing day by day. As the need and value of computational requirement increase the conventional approaches cease to give a promising and reliable solution. In the early 20th century as we all know the path of Physics was completely changed by the Theory of Relativity and then by the Theory of Quantum mechanics and this not only changed the physics but the whole technology , it created a whole new field of computation usually known as Quantum Computing . Quantum Computing and Communications has room for everything which was dreamed in the field of Computing and communications. Quantum technology is going to be the next step to make computers both faster and smarter. In this paper author gives a complete overview of How Quantum Technologies are changing the paradigms of Cyber Security and emerging technologies with it.

I. INTRODUCTION

As perfectly stated in a Max Planck quote," **A new scientific truth does not triumph by convincing its opponents and making them see the light, but rather because its opponents eventually die, and a new generation grows up that is familiar with it".** Quantum technologies are having exactly the same effect on today's technologies. Quantum Computing is going to be the latest and the most powerful tool for Computational requirements. Currently computer security is handled by using mathematical theories for encrypting and decrypting the data in communication between sender and receiver. Even after considering the high performance computer it would take exponentially long time to decrypt this information. But according to theory by using a quantum computer, an attacker can find a key and access the data in feasible amount of time. Quantum Computers can solve exponentially big mathematical problems in parallel in seconds. As mentioned above all the security techniques depend on the mathematical theories for encryption and decryption of data, now a serious question has been raised on these conventional data transfer techniques.. In the following paper author discusses what is Quantum computing and its effects on emerging technologies and mainly its effects on Cyber Security. The paper is divided in three sections. In which, the first section gives an introduction about Quantum computing Concepts and terminologies. Second Section provides the impact on Cyber Security and introduction about new technologies emerging with it and the third section concludes the paper.

Section-I

A Quantum Computer is a machine which uses quantum phenomenon for computation purposes. In last few decades, researchers have realized that in the way which quantum physics allows different phenomenon which can be harnessed for computational requirement. Quantum Computer can use the Quantum physics laws and perform computation in ways that are unimaginable for conventional computers. In a classical computer information is stored in bits in the form of 0 or 1 and only one value can be stored in it at a given point but in contrary a quantum computer can store both values at one time. Let's consider some of the basic quantum computing concepts which allow this magnificent possibility

1. **Superposition:** - A particle can exist in a combination of two different states at once. For example. A particle can act as If it is spinning in both clockwise and anti clockwise. Once it is measured by the observer it settles into single spin, it settles probabilistically either in one of the spin. Consider a physical system that can be in N different classical states. Suppose these states as |1 >, |2 >,…,|N >. Any pure quantum state is in superposition of classical states given as :-

$$|\varphi> = \alpha1|1> + \alpha2|2> + \cdots + \alpha N |N>$$

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

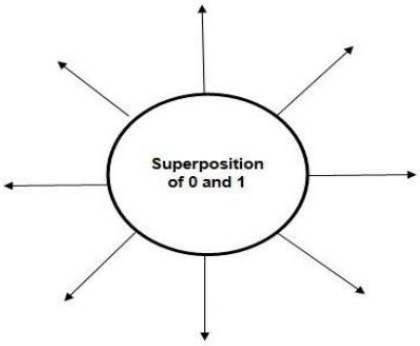

Fig. 1. Particle in superposition

2. **Entanglement:** - Two or more particles become connected or entangled as if they cannot be described as two different entities. It can also be put as measure of one of the particle determines the outcome of the other. This property is also true over a large distances.
3. **Qubits (Quantum bits):** - Now by using these properties of quantum physics a basic building block of a quantum computer is made 'qubit ' or quantum bit . A quantum computer would store the information in these qubits , which can be in both 0 and 1 states until the observation is made. This increases the storage capacity of a quantum computer exponentially

In case of a conventional computer or even the super computer are designed with silicon chips having billions of transistors fixed on them , with these transistors these conventional computer are getting more and more efficient but this has limitation . In contrary in case of a quantum computers they are made of more complex quantum mechanical system unlike transistor having only choice of either ON or OFF a quantum bit can be in ON , OFF , BOTH ON & OFF .Small particles like electrons or photons have properties like spin . This spin can be measured using magnetic field. For example electron can have a spin pointing up or low:

Fig. 2. Particle can have spin both UP and LOW

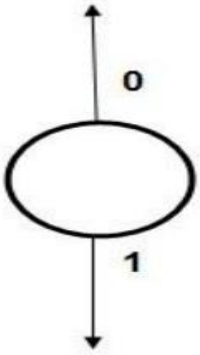

Fig 3. UP and LOW both spin simultaneously

Now let's consider the example of a 8 bit register, In case of a conventional computer a 8 bit register can store one and only one number from 0 to 255 at a time

1	0	1	0	1	0	0

Fig 4. 8-bit register containing 8 bits of data

Now for of a quantum computer , it can store all the values ranging from 0 to 255 as it is a qu-register of 8 entangled qubits. It can contain all the 2^8 i.e.(256) numbers simultaneously in a 8 bit by superposition .

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

1 AND	1 AND	1 AND	1 AND	1 AND	1 AND	1 AND	1 AND

Fig 5. 8 bit qu-register containing 2^8 numbers of 8-bit data

Section-II

1. **Cyber Security:** Potential vulnerability of digital information and its interaction with other technologies makes quantum technologies an important aspect in security world. It is asserted that being first in quantum technologies will surely provide an enormous strategic advantage not only this but political and economic benefits. Of course at the core of all this is the effect of quantum computing in cryptography. Highly important and huge amounts of data can be accessed using these technologies. This poses *significant* threat to existing technological infrastructure .To secure data and communication systems from these threats, the field Cryptography is used. In today's world, communication is secured by cryptography. It is a method of encrypting the data by algorithms and converting the input into encrypted form generally known as cipher text. Cryptography is categorized in two categories: - Symmetric Cryptography and Asymmetric Cryptography. Symmetric Cryptography uses single key for encryption and decryption of data in contrast Asymmetric Cryptography one key is used to encrypt while another key is used to decrypt the data. Most of these algorithms use mathematical problems for encryption e.g. factorization of huge number. But with the power of advanced computing, a quantum computer can break these algorithms in feasible amount of time. Quantum computer pose a significant threat to these commonly used cryptosystems. As a result the whole field of encryption comes in check, but not all of these algorithms are vulnerable to quantum computing, with some modification they can be used even in the quantum era. These are some encryption algorithms provided with the impact of quantum technologies on it

Names	Type	Purpose of algorithm	Impact of quantum stechnologies
AES	Symmetric key	Encryption	Large key sizes needed
SHA-2, SHA-3	…	Hash functions	Large output needed
RSA	Public key	Digital Signatures and key establishment	Not secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Digital Signatures and key exchange	Not secure

2. **Quantum Key Distribution (QKD):** Developments in communication technologies have resulted in faster and more convenient mode of exchange of information. Basically it is a method of communication using laws of quantum mechanics. In this the sender and receiver use a random secrete key to encrypt the messages between them. This key is sent to the other end of communication using a fiber optic key. Most important advantage of this is the communication can be done in secured manner. QKD provides the ability to the both parties to detect if any third party is present and if it is trying to obtain the key. This ability is given through the fundamental aspects of quantum physics. Result of highly sensitivity of a quantum system the any third party trying to measure the systems disturbs the system resulting in detectable irregularity. This provides the sender and receiver assured secured communication.
3. **Diagnostics:** Quantum Computing give a significant boost in A.I algorithms for prediction of a disease by optimizing the Machine Learning algorithms. It gives a ability to get high resolution MRI. By storing a huge amount of pre-recorded data and images we can improve the diagnostics through A.I based systems which needed a professional person, it allows to diagnose the disease without the patient having to go through long procedures.
4. **Drugs Development:** Drugs are invented using a method called Trial and error. Currently pharmaceutical companies use a method for comparison of the molecules for finding a perfect match to improve the positive effects and reduce the side effects. Quantum computer can provide a method for molecular comparison which will be significantly efficient, fast and powerful than any of the existing one.

5. **Financial Services:** In financial services Quantum computing can provide a highly secured system for financial transfers. Detection of fraudulent activities can be done by processing and auditing the patterns of transaction and requests of transactions. The processing cost can be reduced by using highly efficient systems for fast processing of transaction. In this way the financial services can take a giant leap through Quantum Technologies.
6. **Quantum Sensing:** Quantum Sensors have ability to us quantum states for the purpose of measurements .As the quantum states as highly sensitive. By manipulating the quantum states we can make these sensing systems highly immune to strongest sources of noise. Quantum sensing will definitely improve the precision of scientific devices, not only this but it has applications in self driving vehicles and underground mapping.
7. **Optimisation:** The use of quantum computer will solve many problems which are found to be not efficiently solved. For example "Travelling Salesman problem" and many more. This would result in optimization and high efficiency in every filed known to humanity.

II. CONCLUSION

The basics of quantum computing its application in cyber security and some emerging technologies with it have been reviewed. It is important that the reality of a practical Quantum Computer is still a future. But when it will come to reality the quantum computer will be able to do computations and solve problems which were unapproachable to any known supercomputer. Quantum computing has a significant role in emerging technologies and specifically cyber security .This field opens new opportunities in the fields of computation like diagnostics, drugs developments, financial services, networking, space communications, Artificial intelligence etc. It can take the technologies to new heights and will help us making our lives more easy and secure.

III. REFERENCES

[1] Quantum Computing and Communication Complexity Author : R.M. de Wolf
[2] Quantum Safe Cryptography and Security An introduction, benefits, enablers and challenges June 2015 ISBN No. 979-10-92620-03-0
[3] https://www.thehaguesecuritydelta.com/media/com_hsd/report/257/document/HSD-Rapport-Quantum.pdf
[4] https://www.academia.edu/18295176/QUANTUM_COMPUTING_THE_EMERGING_TECHNOLOGY
[5] COMPUTER NETWORK DEFENSE THROUGH RADIAL WAVE FUNCTIONS by Ian J. Malloy A Thesis Submitted to the Faculty of Utica College December, 2015 in Partial Fulfillment of the Requirements for the Degree of Master of Science in Cyber security.
[6] https://spectrum.ieee.org/tech-talk/computing/software/better-commuting-through-quantum-computing
[7] A Review on Quantum Cryptography Technology 1Premjeet Kumar, 2Yashpal Singh 1,2Department of Computer Science &Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, India. International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org NCETEMS-2015 Conference Proceedings
[8] https://www.raconteur.net/risk-management/five-ways-quantum-computing-will-change-cybersecurity-forever
[9] https://www.healthcareitnews.com/news/quantum-computing-could-turbocharge-healthcare-analytics-ai
[10] www.scientificamerican.com/article/new-encryption-systemprotects-data-from-quantum-computers/
[11] H. Bhatt and S. Gautam, "Quantum Computing: A New Era of Computer Science," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019, pp. 558-561.
[12] A. Narayanan, "Quantum computing for beginners," Proceedings of the 1999 Congress on Evolutionary Computation-CEC99 (Cat. No. 99TH8406), 1999, pp. 2231-2238 Vol. 3, doi: 10.1109/CEC.1999.785552.