Deepanshu Sharma et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Special Issue: Recent Innovation in Science, Engineering & Management, May 2022, pp. 110-121

Role of Quantum Computing in Fast Computation Systems

Deepanshu Sharma [*], **AkhandPratap Singh** [*], **Gaurav Kumar** [*], **Keshav Singh**[*], **Dr. Parli B. Hari**[**]

*Student, BCA VI Semester, DPGITM, Gurugram, Haryana (India)
**Associate Professor, Computer Science, DPGITM, Gurugram, Haryana (India)

Abstract: **Quantum Computing is a very new and exciting field in IT industry which intersects mathematics, Computer Science and Physics Quantum Computing still needed to be grown to a great extent because it can give us a lot of achievements for our better future. Computer systems built on the principle of Quantum Mechanics can perform difficult calculations very easily which seems to be unachievable for any classic computer system, as those calculations requires more memory space and time. In our research paper, we will show an overview and the past history of quantum computing, will discuss different algorithmic mechanisms and explores all its suggestions for Cryptography, innovations, power structures and day to day life uses.**

Keywords: Bitcoin, Artificial Intelligence, Machine Learning, Cryptography

I. INTRODUCTION

Basically, to understand the working of quantum computers, firstly we must understand the underlying "**Principles**" upon which quantum computing is built (i.e., Quantum Mechanics).

"I think I can safely say that nobody understands quantum mechanics".

-Feynman

In **1982**, Feynman proposed, the idea of creating machines on base of laws of quantum mechanics inspite of the laws of classical physics.

In **1985,** "**David Deutsch**" – He developed the quantum turing machine, showing that quantum circuits are universal.

In **1994**, "**Peter Shor**" came up with a "**Quantum algorithm**" to factor very large numbers in **polynomial time**. At last in **1994, Peter Shor**proved that quantum computing could crack crypto systems in polynomial time (e.g., **RSA**).

In **1997**, A time comes when "**LOV GROVER**" develops a quantum search algorithm with 0 (√n) complexities.

In our today's life, we can say that Quantum Computing is one of the most important topics in the technology sector for the best working in future. Many technical fields like cryptography, chemistry, quantum simulation, optimization and machine learning have been developed to a great level by using quantum computing. D-wave, has taken a distinctly different approach in building "Gated" quantum computer systems. "D-wave" used a different term to describe quantum computing (i.e. Quantum Annealing). Since this is the case bottleneck today, many entities are focused on developing quantum computing hardware. Again, this includes both the listed technology giants and relatively new start-ups like QC wave, Rigetti, IonQ, and Quantum Circuits.

Challenges	Phenomena	Advantages
QC algorithms involve advanced Discrete Mathematics	Linear superposition	Inherent parallelism (p.3)
	Entanglement	
Physical QC systems must control for little understood quantum mechanics (p.5)	Tunnelling	Physical solution to a mathematical problem (p.4)

II. Fundamentals of Quantum Computing

Some terms, like "**Super Position**" and "**Entanglement**" are what make quantum computer, so great and different from ordinary computers. Ordinary computer transmits information through bits which can be represented by a string of (1's and 0's).

However, Quantum Computers, use **qubits**those are for memory storage which can easily hold a linear superposition of both states (i.e. a1, a0, or even a **Superposition of those two states**).

Superposition	States
δ	$\|(1,1)>$
γ	$\|(0,1)>$
β	$\|(1,0)>$
α	$\|(0,0)>$

• Here, 2 - binary digits can determine the state of a 2 - bit digital system.

• Whereas, normalized 4 coefficients:, $\beta, \gamma, \delta$are required to determine the state of a 2 – bit digital system.

• N-qubits contain $2N$ units of classical information.

Since a single qubit can be of (two value) at once, qubits are exponentially, more powerful then classical bits. Such that, the value stored in qubits exponentially increases with each addition '**quit**'.

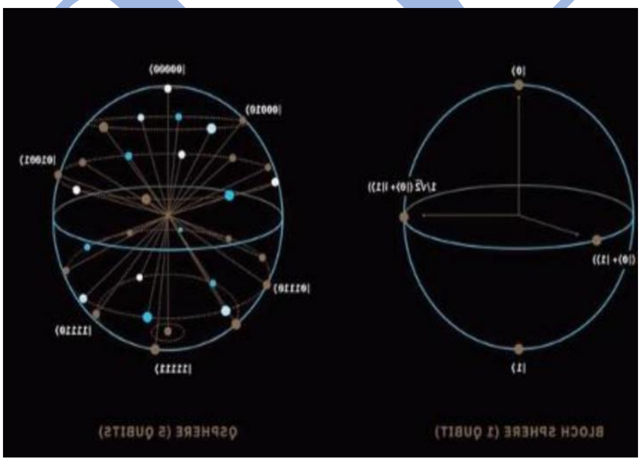
Another, best point of quantum computing is its use of "**Entanglement**". By using this feature of quantum computing (i.e., entanglement), quantum computers can create a larger state than possible with any classical bits (used in classical computers). Quantum computing uses quantum "**Entanglement**" to make another feature (i.e., Quantum Parallelism). Whereas quantum parallelism is it's a huge discussion. In discrete quantum world, Let's assume you have 3 qubits initially.

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

After operating the (H gate) on the three qubits, the result is: -

$$\frac{1}{\sqrt{2}}^3(|0\rangle + |1\rangle)^3 = \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + \ldots + |111\rangle).$$

Then applying any operator on the entangled 3- qubit state means applying the operator on eight state |000>, ……, |111>. Simultaneously, which will lead to an exponential speedup to a large extent. Entangling two quantum states means multiplying their dimension that, they do not simply add like combined classical bits.



With "**two qubits**" we get combination like:

a|00>+b|01+c|10>+d|11>

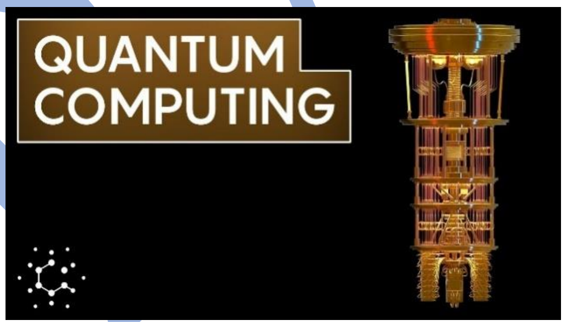
Where, (|01) means that the first qubit we have store 0's value (|0>) and the second stores 1's value (|1>).

A, b, c and d are complex numbers and $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$

If two or more of the a, b, c and d are not zero, and that reason we cannot separate the qubits, it simply signifies that they are entangled with perfect correlation and are no longer independent.

Can we say Quantum Computing is real?

Usually no can easily believe that this computing approach is real without having efficient knowledge about the quantum computing, or atleast some think that this concept cannot be possible at the moment. Different famous companies have worked a lot to develop a computer that operates using quantum principles. However, this approach is not valid everywhere but only in enough problems.



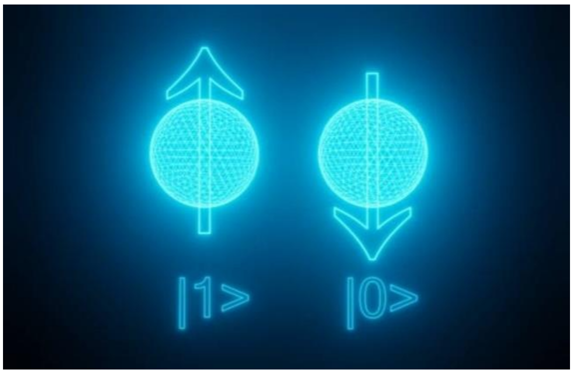
How can quantum computing bring a beneficial change to thus world?

Use of demonstration can make it easy to explain its benefits. Quantum computing can simulate real life situations. Hence, many scientists created a virtual laboratory where one can get the prediction about what will happen in the real laboratory.

Here we can see various implications to the development of human civilization:

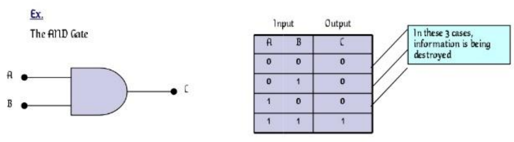
1. R&D like main process about a good can be occurred in a virtual lab, therefore, people can easily produce goods at much lower costs.
2. It shortens the time requirement to create urgent innovations.
3. Every type of failures can be detected, before manufacturing items by the developers and so can work on its solutions.
4. Now more tenable and eco-friendly is the manufacturing process.

III. OPERATIONS ON QUBITS – [Reversible Logic]



Due to nature of Quantum Physics, those laws of physics for quantum mechanics, the destruction information in a gate will cause heat to be evolved which will definitely destroy the Superposition of qubits.

For example: -



This type of gate cannot be used. We must use ***Quantum Gates***.

Quantum Gates are clearly different from any classical logic gate, as we lose the original value of an input after using a classical gate.

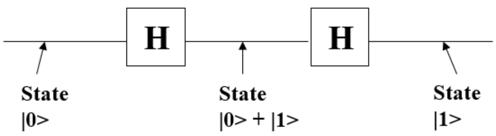
Whereas, Quantum logic gates are reversible. It is possible to perform classical computing using only "**Reversible**" gates.

Various Operations on Data

Basically, a deterministic computation can only be performed if the quantum computer is reversible. Providentially, it has been proven that any deterministic computation can be made reversible. **[Charles Bennet 1973].**

Logical gate in quantum computation (Hadamard)

The simplest Hadamard gate is a single-qubit operation that maps the basis state **|0> to |0>+|1>/2 and** |1> **to** |0>-|1>/2, it is also known as a square root of NOT Gate and this is the reason of superposition can be occurred of the two basis states.

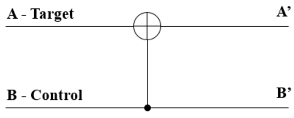


Note:NOT gate can be formed by using two Hadamard gates.

Quantum Gates –

1. Controlled NOT

Controlled-NOT (CN) Gate is used to operate two qubits at time. Let us assume the bit on the control line is 1 then it will invert the bit on the target line.



Input		Output	
A	B	A'	B'
0	0	0	0
0	1	1	1
1	0	1	0
1	1	0	1

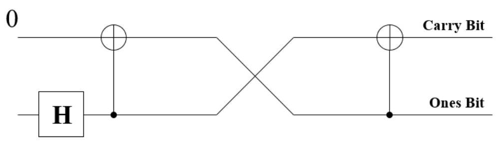
Note: With some extra information, the CN gate can behave like reversible as it is almost similar to the XOR gate.

Example-

Multiplication by 2

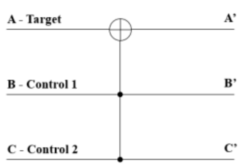
- CN Gates can be used to build reversible logic circuit to calculate multiplication by two.

Input		Output	
Carry Bit	Ones Bit	Carry Bit	Ones Bit
0	0	0	0
0	1	1	0



2. ControlledControlled NOT (CCN)

Controlled Controlled NOT (CCN) Gate is used to operate three qubits at a time. Let us assume the bit on the both of the control lines is 1 then the target bit inverted.



Input			Output		
A	B	C	A'	B'	C'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	0	1	1

IV. Shor's Algorithm

The algorithm is based on:

- Modular Arithmetic
- Quantum Parallelism

- Quantum Fourier Transform

Shor's Algorithm – Periodicity

An important result from Number Theory is:

F (a) = x^a modN is a periodic function

Choose N (assumption) = 15 and x = 7 and by solving mod we got the following:

7^0mod 15 = 1

7^1mod 15 = 7

7^2mod 15 = 4

7^3 mod 15 = 13

7^4mod 15 = 1

.

.

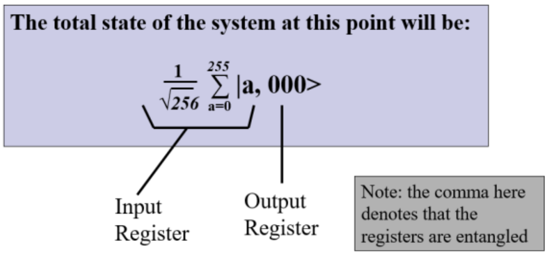
Depth Analyzing of Shor's Algorithm

Process to find out factor of an odd integer N (Let's choose 15):

1. We will choose an integer qwhereN <q< 2N **suppose the number is 256**.
2. Now we will choose a random integer xwhere GCD(x, N) = 1 **suppose the number is 7.**
3. Now we have to create two quantum registers which are entangled.
   - Input register: it containslarge number of qubits to represent large number as q-1. i.e.**up to 255, so we need 8 qubits in total.**
   - Output register: it must contain large number of qubits to represent numbers as large as N-1. **up to 14, so we need 4 qubits**

Shor's Algorithm - Preparing Data

4. **We will load the input register with an equally weighted superposition of all integers from 0 to q-1. 0 to 255**
5. **Now we have to load the output register with all zeros.**



Shor's Algorithm - Modular Arithmetic

6. We have to apply transformation x mod N to every no. in the input register and have to store the result in output register.

Input Register	7^a Mod 15	Output Register
|0>	7^0 Mod 15	1
|1>	7^1 Mod 15	7
|2>	7^2 Mod 15	4
|3>	7^3 Mod 15	13
|4>	7^4 Mod 15	1
|5>	7^5 Mod 15	7
|6>	7^6 Mod 15	4
|7>	7^7 Mod 15	13

Shor's Algorithm - Superposition Collapse

7. Measure the output register. This will collapse the superposition and represent a sample result of the transformation, let it be c.

Our output register will collapse to represent one of the following:

|1>, |4>, |7>, or |13

For sake of example, lets choose |1>

Shor's Algorithm – Entanglement

8. **After entangling two registers, if we measure the output register, it will have the effect of partially collapsing the input register into an equal superposition of each state between 0 and q-1 that yielded c.**

Since the output register collapsed to |1>, the input register will partially collapse to:

$$\frac{1}{\sqrt{64}}|0> + \frac{1}{\sqrt{64}}|4> + \frac{1}{\sqrt{64}}|8> + \frac{1}{\sqrt{64}}|12>, \ldots$$

The probabilities in this case are $\frac{1}{\sqrt{64}}$ since our register is now in an equal superposition of 64 values (0, 4, 8, . . . 252)

Shor's Algorithm – QFT

9. Quantum Fourier transform have to be applied on the resultant input register. AFourier transform can take the state |a> and transform it into new a state given by:

$$\frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} |c\rangle * e^{2\pi iac/q}$$

$$\frac{1}{\sqrt{64}} \sum_{a \in A} |a\rangle, |1\rangle \longrightarrow \frac{1}{\sqrt{256}} \sum_{c=0}^{255} |c\rangle * e^{2\pi iac/256}$$

Note: A is the set of all values that $7^a \bmod 15$ yielded 1. In our case A = {0, 4, 8, …, 252}

So the final state of the input register after the QFT is:

$$\frac{1}{\sqrt{64}} \sum_{a \in A} \frac{1}{\sqrt{256}} \sum_{c=0}^{255} |c\rangle * e^{2\pi iac/256} \; |1\rangle$$

The Factors of Shor's Algorithm -

10. Now we will determine the factors of N by taking the greatest common divisor of N w.r.tx ^ (P/2) + 1 and x ^ (P/2) - 1.

We compute:

$\text{Gcd}(7^{4/2} + 1, 15) = \mathbf{5}$

$\text{Gcd}(7^{4/2} - 1, 15) = \mathbf{3}$

We have successfully factored 15!

Problems withShor's Algorithm –

- The QFT is short and disclose the wrong period. The probability in real dependenton q's value. Value of correct probability depends on larger value of q.
- The period of the series results in a odd number.

V. HISTORY OF QUANTUM COMPUTNG

In 2000,The Los Alamos National Laboratory developed the first working quantum computer. In the next year, Stamford University success in the Shor's algorithm to factor the no. using 7 qubits and identical modules.

In 2004,In china the University of Science and Technology develop the five-photon entanglement and Oxford University develop the first five states NMR Quantum Computer.

In 2011,System like D-wave system claimed to have developed the first commercially available quantum computer, but still remains under dispute. Many people agree that the d-wave one can perform quantum calculations, these calculations can be done on a classical computer at same speed.

In 2016,IBM released the Quantum Experience. In the last year Google released a **72qubit** chip is called "**Bristlecone**" and Intel released a **49 qubit** chip called "**Tangle Lake**" and this year IBM released the first commercial quantum computer and the name of computer is **Q System One.**

VI. ADVANTAGES

1). Faster Computations: - These computers can perform computation at a much faster than normal computers. Quantum Computers have higher computation power than the supercomputers. They can process the data at 1000 times faster. The quantum algorithm computer all possible inputs at the same time.

2). Best for Simulation: - Quantum Computing are best for doing data simulation computing. There are many algorithms created that can simulate various things like, chemical simulation, weather forecasting.

3).Medicine Creation: -The healthcare industry, quantum computing could enable range of disruptive uses cases providers and health plans by accelerating diagnoses, personalising medicine and optimising pricing. They can also detect the disease and create a formula for medicine.

4).Google Search: -Quantum Computers are used by google to refine searches. Now every search on google can speed up by using these computers. Most relevant results can be populated using quantum computing.

5).Used in Radar Making: -A Quantum Radar can be seen as a device working in the Microwave range, which exploits quantum nature from its point of view of the radiation source and the output detection, and is able to outperform a classical counterpart. The accuracy of radar weapons can be improved by using the technology.

VII. DISADVANTAGES

1).Algorithm Creation: - For every type of computation, it needs to write a new algorithm. Quantum Computing cannot work as classical computers; they need special algorithms to perform tasks in their environment.

2).Low Temperature Needed: - As the processing ii these computers are done very deeply, so it needs a temperature of negative 460^0 F. This is the lowest temperature of the universe and it is very difficult to maintain that temperature.

3).Internet Security: - It is assumed by the scientist that if a quantum computer is implemented in the best way then whole internet security breaks. This is due to the facts that these computers can decrypt all the codes on the internet.

VIII. Applications of Quantum Computation: Quantum Machine Learning

Bitcoin and Quantum Computing

In 21st century, when we are using Cryptocurrency on a large scale, rules of Cryptocurrency are not quantum computer proof.Evidences can be shown that attacks on bitcoin using quantum computers are not feasible if economic costs are considered. The simple reason is that organizations have invested a big amount ofmoney to develop solutions to these undemonstrated problems.

Expert developers of Bitcoin have been using the unreliability around a non-existent quantum code cracking system to persuade users to change to substitutes of cryptographic primates that suit the implementation of Sidechains. They have been emphasizing the user to use**Lamport signatures** stating that **"while large, are secure against quantum computers".** The reason for the change to Lamport signatures is not quantum hardening; it is to enable the adoption of Sidechains. One unimaginable reality is that there is nothing to fear as Bitcoin uses a double hashing algorithm. Any unused bitcoin address will not be reversible to the public key.

Bitcoin Mining

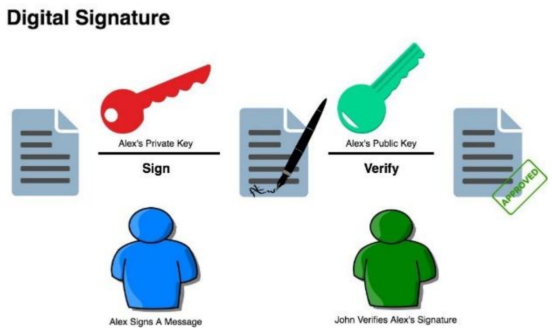
Quantum computers can solve the algorithms faster than solving hash. Therefore, a minerdoesn't get any economic benefit to use Quantum Computers for solving hash puzzles as they would solve only few hashes. Qubits are slower to process than bits. As a result,the miner who was to deploy a Quantum computer for the mining of Bitcoin, would be at an economic disadvantage. The Bitcoin protocol helpspeople and firms to use unused bitcoin addresses by moving money to them. We can prevent use of multiple bitcoin addresses by having single key reused addresses which has public keys are also exposed.

From Pre-Quantum to Post-Quantum Blockchain

A. Blockchain Public-Key Security

- Bits-of-security level is used to find the strength of Public-key cryptosystems.

- An asymmetric cryptosystem has a 1024-bit security and the effort required to attack it with a classical computer is equalto brute-force attack on a 1024-bit cryptographic key.



D. Blockchain Post-Quantum Schemes-Characteristics

Blockchains should have following features:

- Devices usingblockchainshould use small public and private keys so as to reduce the storage space that it requires. As small keys involve less complex operations while performing addition, it is important for blockchainswhich interacts with Internet of Things (IoT) end-devices, which have grown significantly in today's time.But still,IoT devices are facing challenges regarding security.

- Hash length and short signature:User signatures and block hashes are stored by blockchain. As a result, blockchain size will increase with the increase in signature or hash length.

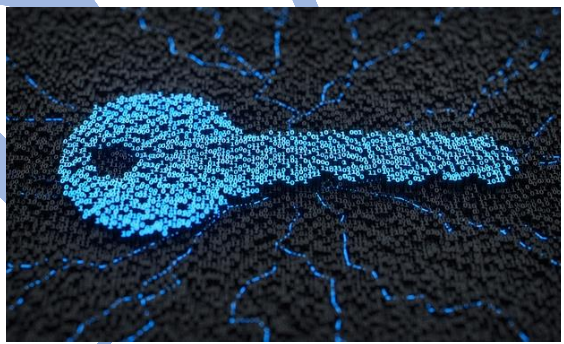
- Fast execution. If a large amount of transactions per second, post-quantum schemes need to be quick to allow a blockchain to process. Low computational complexityresultsin fast execution which is essentialto avoid exclusion of resource-constrained devices from blockchain transactions.

- Low computational complexity: fast execution with specific hardware does not state that the post-quantum cryptosystem is computationally simple. For example, Intel microprocessors can execute some schemes fast but the same schemes may be qualified as slow when executed on ARM-based microcontrollers. So we should focus on trade-off between computational complexity, execution time and supported hardware devices.

- Low energy consumption:We have assumed that Bitcoin are power hungry mainly due to the energy required to execute its consensus protocol. Other factors that impact power consumption, are used hardware, the amount of performed communications transactions and implemented security schemes.

A New Field is born: Quantum Cryptography

Even in the time of Caesar, Cryptography was used as a basic way to transfer data secretly. Let's take a look on that technique, in which one assigns a number value to each letter of the alphabet (i.e. "a" is 1, "b" is 2, "c" is 3, etc.) and sends a message entirely composed of these coded numbers. Only the recipient of the code can decode it easily based on his or her knowledge of the coded letter values. And nowadays we named that type of encoding and decoding as private key cryptography, in which basically two parties decide wisely for a key that encodes and decodes the secret messages. That method will only avoid interception by a third party but only if the two parties can keep the key completely private.



That is definitely a difficult task, since the two parties must somehow communicate the key without being intercepted. Public key cryptography, is the other main branch of cryptography. In public key cryptography, each party publishes a key to encode a message, but withholds the key to decode the message. For a particular example, if Person A wants to send a message to Person B secretly, then Person A has to simply look up for Person B's public encoding key, encode the secret message, and send the message to Person B. Person B then simply decodes the encoded message using his or her secret "**decryption key**". Declaring the encoding key public seems **contradictory**, especially since many decoding keys can be predicted by reversing the encoding key. Whereas the Public key cryptography seems to be very secure method of communication, however, if one takes advantage of one-way mathematical operations. The reason of its security, operations (encoding or decoding) are simple to do forward but very burdensome to do in reverse. For example, taking a cube of a number is a lot easier than getting the cube root of a number. More convoluted one-way mathematical operations form the basis of public key cryptography. Factoring large integers is one of those one-way mathematical operations. While it is elementary to multiply several prime numbers, it is much more complex to do this process in reverse by finding the factors of a very large number. We have got the most popular encryption technique based on factorization is the **Rivest-Shamir-Adleman (RSA)** technique as most expensive gift. Until recently, this method has been very secure because the classical computer is enable to factor large numbers efficiently. In light of, quantum computation and **Shor's** factoring algorithm, cryptographers are hectically searching for an encryption method that can hold out against attacks from quantum computers. The only solution lies in writing quantum algorithms for encryption and decryption, thus creating "**quantum cryptography**". Besides this so common protecting information from quantum hackers, the use of quantum computers in cryptography provides innumerable advantages. Networking quantum computers require exponentially less communication to solve problems in Compare of classical computers. To secure cryptosystem an efficient computer communication is must. Quantum laws such as the no-cloning theorem and uncertainty principle also provide extra security against internet hackers.

CONCLUSION:

Many of researchers and developers, have got their interest provoked by the recent progress on quantum computing who have worked with DLTs like blockchain, where public key cryptography and hash function were essential. This article inspected the impact of quantum computing attacks on blockchain and clarified how post-quantum cryptosystems can be implemented to minimize these attacks. We analysed the application of post quantum schemes to the blockchain and reviewed these schemes and their challenges in detail. For post-quantum public-key encryption and digital-signature schemes, sizeable comparisons were done on is characteristics and performance. Quantum threat on blockchain is extensively explained and useful guidelines for the researchers and developers of the next-generation of quantum-resistant blockchains are also provided.

REFERENCES

[1]. Dalal, S., Poongodi, M., Lilhore, U. K., Dahan, F., Vaiyapuri, T., Keshta, I., ... & Simaiya, S. Optimized LightGBM model for security and privacy issues in cyber-physical systems. Transactions on Emerging Telecommunications Technologies, e4771.

[2]. Dalal, S., Manoharan, P., Lilhore, U. K., Seth, B., Simaiya, S., Hamdi, M., & Raahemifar, K. (2023). Extremely boosted neural network for more accurate multi-stage Cyber attack prediction in cloud computing environment. Journal of Cloud Computing, 12(1), 1-22.

[3]. Malik, A., Onyema, E. M., Dalal, S., Kumar, U., Anand, D., Sharma, A., & Simaiya, S. (2023). Forecasting students' adaptability in online entrepreneurship education using modified ensemble machine learning model. Array, 100303.

[4]. Shetty, S., & Dalal, S. (2022, December). Bi-Directional Long Short-Term Memory Neural Networks for Music Composition. In 2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT) (pp. 1-6). IEEE.

[5]. Dalal, S. (2023, April). The Smart Analysis of Poisson Distribution Pattern Based Industrial Automation in Industry 4.0. In 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1-6). IEEE.

[6]. Dalal, S., Seth, B., Radulescu, M., Cilan, T. F., & Serbanescu, L. (2023). Optimized Deep Learning with Learning without Forgetting (LwF) for Weather Classification for Sustainable Transportation and Traffic Safety. Sustainability, 15(7), 6070.

[7]. Onyema, E. M., Lilhore, U. K., Saurabh, P., Dalal, S., Nwaeze, A. S., Chijindu, A. T., ... & Simaiya, S. (2023). Evaluation of IoT-Enabled hybrid model for genome sequence analysis of patients in healthcare 4.0. Measurement: Sensors, 26, 100679.

[8]. Dalal, S., Manoharan, P., Lilhore, U. K., Seth, B., Simaiya, S., Hamdi, M., & Raahemifar, K. (2023). Extremely boosted neural network for more accurate multi-stage Cyber attack prediction in cloud computing environment. Journal of Cloud Computing, 12(1), 1-22.

[9]. Dalal, S., Goel, P., Onyema, E. M., Alharbi, A., Mahmoud, A., Algarni, M. A., & Awal, H. (2023). Application of Machine Learning for Cardiovascular Disease Risk Prediction. Computational Intelligence and Neuroscience, 2023.

[10]. Dalal, S., Seth, B., Radulescu, M., Secara, C., & Tolea, C. (2022). Predicting Fraud in Financial Payment Services through Optimized Hyper-Parameter-Tuned XGBoost Model. Mathematics, 10(24), 4679.

[11]. Dalal, S., Onyema, E. M., & Malik, A. (2022). Hybrid XGBoost model with hyperparameter tuning for prediction of liver disease with better accuracy. World Journal of Gastroenterology, 28(46), 6551-6563.

[12]. Edeh, M. O., Dalal, S., Obagbuwa, I. C., Prasad, B. V. V., Ninoria, S. Z., Wajid, M. A., & Adesina, A. O. (2022). Bootstrapping random forest and CHAID for prediction of white spot disease among shrimp farmers. Scientific Reports, 12(1), 1-12.

[13]. Zaki, J., Nayyar, A., Dalal, S., & Ali, Z. H. (2022). House price prediction using hedonic pricing model and machine learning techniques. Concurrency and Computation: Practice and Experience, 34(27), e7342.

[14]. Dalal, S., Onyema, E., Romero, C., Ndufeiya-Kumasi, L., Maryann, D., Nnedimkpa, A. & Bhatia, T. (2022). Machine learning-based forecasting of potability of drinking water through adaptive

boosting model. Open Chemistry, 20(1), 816-828. https://doi.org/10.1515/chem-2022-0187

[15]. Onyema, E. M., Dalal, S., Romero, C. A. T., Seth, B., Young, P., & Wajid, M. A. (2022). Design of Intrusion Detection System based on Cyborg intelligence for security of Cloud Network Traffic of Smart Cities. Journal of Cloud Computing, 11(1), 1-20.

[16]. Dalal, S., Onyema, E. M., Kumar, P., Maryann, D. C., Roselyn, A. O., & Obichili, M. I. (2022). A Hybrid machine learning model for timely prediction of breast cancer. International Journal of Modeling, Simulation, and Scientific Computing, 2023, 1-21.

[17]. Dalal, S., Seth, B., Jaglan, V., Malik, M., Dahiya, N., Rani, U., ... & Hu, Y. C. (2022). An adaptive traffic routing approach toward load balancing and congestion control in Cloud–MANET ad hoc networks. Soft Computing, 26(11), 5377-5388.

[18]. Edeh, M. O., Dalal, S., Dhaou, I. B., Agubosim, C. C., Umoke, C. C., Richard-Nnabu, N. E., & Dahiya, N. (2022). Artificial Intelligence-Based Ensemble Learning Model for Prediction of Hepatitis C Disease. Frontiers in Public Health, 847.

[19]. Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2022). Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies, 33(4), e4108.

[20]. Malik, M., Nandal, R., Dalal, S., Maan, U., & Le, D. N. An efficient driver behavioral pattern analysis based on fuzzy logical feature selection and classification in big data analysis. Journal of Intelligent & Fuzzy Systems, 43(3), 3283-3292.

[21]. Malik, M., Nandal, R., Dalal, S., Jalglan, V., & Le, D. N. (2022). Deriving driver behavioral pattern analysis and performance using neural network approaches. Intelligent Automation & Soft Computing, 32(1), 87-99.

[22]. Shetty, S., & Dalal, S. (2022, December). Bi-Directional Long Short-Term Memory Neural Networks for Music Composition. In 2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT) (pp. 1-6). IEEE.

[23]. Onyema, E. M., Shukla, P. K., Dalal, S., Mathur, M. N., Zakariah, M., & Tiwari, B. (2021). Enhancement of patient facial recognition through deep learning algorithm: ConvNet. Journal of Healthcare Engineering, 2021.

[24]. Dalal, S., & Khalaf, O. I. (2021). Prediction of occupation stress by implementing convolutional neural network techniques. Journal of Cases on Information Technology (JCIT), 23(3), 27-42.

[25]. Dalal, S., Jaglan, V., & Le, D.-N. (Eds.). (2021). Green Internet of Things for Smart Cities: Concepts, Implications, and Challenges (1st ed.). CRC Press. https://doi.org/10.1201/9781003032397.

[26]. Dahiya, N., Dalal, S., & Jaglan, V. (2021). 8 Mobility in Green Management IoT. Green Internet of Things for Smart Cities: Concepts, Implications, and Challenges, 125.

[27]. Dahiya, N., Dalal, S., & Jaglan, V. (2021). 7 Efficient Green Solution. Green Internet of Things for Smart Cities: Concepts, Implications, and Challenges, 113.

[28]. Seth, B., Dalal, S., & Dahiya, N. (2021). 4 Practical Implications. Green Internet of Things for Smart Cities: Concepts, Implications, and Challenges, 61.

[29]. Malik, M., Nandal, R., Dalal, S., Jalglan, V., & Le, D. N. (2021). Driving pattern profiling and classification using deep learning. Intelligent Automation & Soft Computing, 28(3), 887-906.

[30]. Jindal, U., Dalal, S., Rajesh, G., Sama, N. U., Jhanjhi, N. Z., & Humayun, M. (2021). An integrated approach on verification of signatures using multiple classifiers (SVM and Decision Tree): A multi-classification approach.

[31]. Seth, B., Dalal, S., Le, D. N., Jaglan, V., Dahiya, N., Agrawal, A., ... & Verma, K. D. (2021). Secure Cloud Data Storage System Using Hybrid Paillier–Blowfish Algorithm. Computers, Materials & Continua, 67(1), 779-798.

[32]. Vijarania, M., Dahiya, N., Dalal, S., & Jaglan, V. (2021). WSN Based Efficient Multi-Metric Routing for IoT Networks. In Green Internet of Things for Smart Cities (pp. 249-262). CRC Press.

[33]. Goel, M., Hayat, A., Husain, A., & Dalal, S. (2021). Green-IoT (G-IoT) Architectures and Their Applications in the Smart City. In Green Internet of Things for Smart Cities (pp. 47-59). CRC Press.

[34]. Chawla, N., & Dalal, S. (2021). Edge AI with Wearable IoT: A Review on Leveraging Edge Intelligence in Wearables for Smart Healthcare. Green Internet of Things for Smart Cities, 205-231.

[35]. Dahiya, N., Dalal, S., & Jaglan, V. (2021). Efficient Green Solution for a Balanced Energy Consumption and Delay in the IoT-Fog-Cloud Computing. In Green Internet of Things for Smart Cities (pp. 113-123). CRC Press.

[36]. Dahiya, N., Dalal, S., & Jaglan, V. (2021). Mobility Management in Green IoT. In Green Internet of Things for Smart Cities (pp. 125-134). CRC Press.

[37]. Seth, B., Dalal, S., & Dahiya, N. (2021). Practical Implications of Green Internet of Things (G-IoT) for Smart Cities. In Green Internet of Things for Smart Cities (pp. 61-81). CRC Press.

[38]. Dalal, S., Agrawal, A., Dahiya, N., & Verma, J. (2020, July). Software Process Improvement Assessment for Cloud Application Based on Fuzzy Analytical Hierarchy Process Method. In International Conference on Computational Science and Its Applications (pp. 989-1001). Springer, Cham.

[39]. Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2020). Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies.

[40]. Hooda, M., & Shravankumar Bachu, P. (2020). Artificial Intelligence Technique for Detecting Bone Irregularity Using Fastai. In International Conference on Industrial Engineering and Operations Management Dubai, UAE (pp. 2392-2399).

[41]. Arora, S., & Dalal, S. (2019). An optimized cloud architecture for integrity verification. Journal of Computational and Theoretical Nanoscience, 16(12), 5067-5072.

[42]. Arora, S., & Dalal, S. (2019). Trust Evaluation Factors in Cloud Computing with Open Stack. Journal of Computational and Theoretical Nanoscience, 16(12), 5073-5077.

[43]. Shakti Arora, S. (2019). DDoS Attacks Simulation in Cloud Computing Environment. International Journal of Innovative Technology and Exploring Engineering, 9(1), 414-417.

[44]. Shakti Arora, S. (2019). Integrity Verification Mechanisms Adopted in Cloud Environment. International Journal of Engineering and Advanced Technology (IJEAT), 8, 1713-1717.

[45]. Sudha, B., Dalal, S., & Srinivasan, K. (2019). Early Detection of Glaucoma Disease in Retinal Fundus Images Using Spatial FCM with Level Set Segmentation. International Journal of Engineering and Advanced Technology (IJEAT), 8(5C), 1342-1349.

[46]. Sikri, A., Dalal, S., Singh, N. P., & Le, D. N. (2019). Mapping of e-Wallets With Features. Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies, 245-261.

[47]. Seth, B., Dalal, S., & Kumar, R. (2019). Hybrid homomorphic encryption scheme for secure cloud data storage. In Recent Advances in Computational Intelligence (pp. 71-92). Springer, Cham.

[48]. Seth, B., Dalal, S., & Kumar, R. (2019). Securing bioinformatics cloud for big data: Budding buzzword or a glance of the future. In Recent advances in computational intelligence (pp. 121-147). Springer, Cham.

[49]. Jindal, U., & Dalal, S. (2019). A hybrid approach to authentication of signature using DTSVM. In Emerging Trends in Expert Applications and Security (pp. 327-335). Springer, Singapore.

[50]. Le, D. N., Seth, B., & Dalal, S. (2018). A hybrid approach of secret sharing with fragmentation and encryption in cloud environment for securing outsourced medical database: a revolutionary approach. Journal of Cyber Security and Mobility, 7(4), 379-408.

[51]. Sikri, A., Dalal, S., Singh, N. P., & Dahiya, N. (2018). Data Mining and its Various Concepts. Kalpa Publications in Engineering, 2, 95-102.

[52]. Sameer Nagpal, S. (2018). Analysis of LrMu Power Algorithm in the Cloud Computing Environment using CloudSim Toolkit. International Journal of Research in Electronics and Computer Engineering (IJRECE), 6(3), 1175-1177.

[53]. Nagpal, S., Dahiya, N., & Dalal, S. (2018). Comparative Analysis of the Power Consumption Techniques in the Cloud Computing Environment. Journal Homepage: http://www. ijmra.us, 8(8), 1.

[54]. Kumar, N., Dalal, S., & Dahiya, N. (2018). Approach of Lion Optimization Algorithm for Efficient Load Balancing in Cloud Computing. Journal Homepage: http://www. ijmra.us, 8(8), 1.

[55]. Sameer Nagpal, S. (2018). Comparison of Task Scheduling in Cloud Computing Using various Optimization Algorithms. Journal of Computational Information Systems, 14(4), 43-57.

[56]. Arora, S., & Dalal, S. (2018). Hybrid algorithm designed for handling remote integrity check mechanism over dynamic cloud environment. International Journal of Engineering & Technology, 7(2.4), 161-164.

[57]. Kukreja, S., & Dalal, S. (2018). Modified drosophila optimization algorithm for managing re-sources in cloud environment. International Journal of Engineering & Technology, 7(2.4), 165-169.

[58]. Jindal, U., Dalal, S., & Dahiya, N. (2018). A combine approach of preprocessing in integrated signature verification (ISV). International Journal of Engineering & Technology, 7(1.2), 155-159.

[59]. Nagpal, S., Dahiya, N., & Dalal, S. (2018). Comparison of Task Scheduling in Cloud Computing Using various Optimization Algorithms. Journal of Computational Information Systems ISSN, 1553-9105.

[60]. Jindal, U., Dalal, S., & Dahiya, N. (2018). A combine approach of preprocessing in integrated signature verification (ISV). International Journal of Engineering & Technology, 7(1.2), 155-159

[61]. Shakti Arora, S. (2018). Resolving problem of Trust context in Cloud Computing. International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), 5(1), 138-142.

[62]. Dalal, S., Dahiya, N., & Jaglan, V. (2018). Efficient tuning of COCOMO model cost drivers through generalized reduced gradient (GRG) nonlinear optimization with best-fit analysis. In Progress in Advanced Computing and Intelligent Engineering (pp. 347-354). Springer, Singapore

[63]. Seth, B., & Dalal, S. (2018). Analytical assessment of security mechanisms of cloud environment. In Progress in Advanced Computing and Intelligent Engineering (pp. 211-220). Springer, Singapore.

[64]. Kukreja, S., & Dalal, S. (2018). Performance analysis of cloud resource provisioning algorithms. In Progress in Advanced Computing and Intelligent Engineering (pp. 593-602). Springer, Singapore.

[65]. Rani, U., Dalal, S., & Kumar, J. (2018). Optimizing performance of fuzzy decision support system with multiple parameter dependency for cloud provider evaluation. Int. J. Eng. Technol, 7(1.2), 61-65.

[66]. Dahiya, N., Dalal, S., & Khatri, S. (2017). An Enhanced Bat Algorithm for Data Clustering Problems. International Journal of Advanced Research in Computer Science, 8(3).

[67]. Dahiya, N., Dalal, S., & Khatri, S. (2017). Data clustering and its Application to numerical function optimization algorithm. International Journal of Advanced Research in Computer Science, 8(1).

[68]. Arora, S., & Dalal, S. (2017). Adaptive Model For Integrity Verification In Cloud Computing System. International Journal of Advanced Research in Computer Science, 8(1), 233-236.

[69]. Neeraj Dahiya, S. (2017). Numerical Function Optimization: Model, Procedure And Uses. International Journal of Engineering Science and Technology (IJEST), 9(4), 266-270.

[70]. Dahiya, N., Dalal, S., & Khatri, S. (2016). Refinement with Image clustering using Self-Organizing Map and Numerical Function Optimization. International Journal of Computer Science and Information Security, 14(11), 909.

[71]. Neeraj Dahiya, S. (2016). A Review on Numerical function optimization Algorithm and its Applications to Data Clustering & Classification. International Journal of Recent Research Aspects, 3(3), 115-121.

[72]. Arora, S., & Dalal, S. (2016). Novel Approach of Integrity Verification in Dynamic Cloud Environment. International Journal of Computer Science and Information Security, 14(8), 207.

[73]. Dalal, S., & Kukreja, S. (2016). Genetic Algorithm based Novel approach for Load Balancing problem in Cloud environment. International Journal of computer science and information security, 14(7), 88.

[74]. Arora, S., & Dalal, S. (2016). Study of Integrity Based Algorithm in Decentralized Cloud Computing Environment. International Journal of Institutional & Industrial Research, 1(1), 15-17.

[75]. Vishakha, S. D. (2016). Performance Analysis of Cloud Load Balancing Algorithms. International Journal of Institutional and Industrial Research, 1(01), 1-5.

[76]. Dalal, S., & Jindal, U. (2016, March). Performance of integrated signature verification approach. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 3369-3373). IEEE.

[77]. Dahiya, N., Dalal, S., & Tanwar, G. (2016, March). Refining of image using self-organizing map with clustering. In AIP Conference Proceedings (Vol. 1715, No. 1, p. 020064). AIP Publishing LLC.

[78]. Dahiya, N., Dalal, S., & Khatri, S. (2016). A Review on Numerical function optimization Algorithm and its Applications to Data Clustering & Classification. International Journal of Recent Research Aspects, 3(3), 111-115.

[79]. Arora, S., & Dalal, S. (2016). Enhanced Privacy Preserving Access Control in the Cloud. International Journal of Recent Research Aspects, 3(4), 66-70.

[80]. Dahiya, N., Dalal, S., Khatri, S., & Kumar, Y. (2016). Cat Swarm Optimization: Applications And Experimental Illustrations To Data Clustering. International Journal of Control Theory and Applications, 9(41), 759-765.

[81]. Rani, U., & Dalal, S. (2016). Neural Network Applications in Design Process of Decision Support System. International Journal of Recent Research Aspects, 4(2), 40-44.

[82]. Seth, B., & Dalal, S. (2016). Designing Hybrid Security Architecture in Multi Cloud System. International Journal of Control Theory and Applications, 9(41), 767-776.

[83]. Seth, B., & Dalal, S. (2016). Analysis of cryptographic approaches. International Journal of Recent Research Aspect, 3(1), 21-24.

[84]. Jindal, U., & Dalal, S. (2016). Survey on Signature verification and recognition using SIFT and its variant. International Journal of Recent Research Aspects, 3(3), 26-29.

[85]. Sharma, P., & Dalal, S. (2014). Reviewing MANET Network Security Threats. identity, 25-30.

[86]. Sharma, D., Dalal, S., & Sharma, K. K. (2014). Evaluating Heuristic based Load Balancing Algorithm through Ant Colony Optimization. environment, 5-9.

[87]. Sharma, D., Sharma, K., & Dalal, S. (2014). Optimized load balancing in grid computing using tentative ant colony algorithm. International Journal of Recent Research Aspects, 1(1), 35-39.

[88]. Jindal, K., Dalal, S., & Sharma, K. K. (2014, February). Analyzing spoofing attacks in wireless networks. In 2014 Fourth International Conference on Advanced Computing & Communication Technologies (pp. 398-402). IEEE.

[89]. Dalal, Surjeet & Srinivasan, S, Approach of multi agent system in controlling bullwhip effect of supply chain management system using case based reasoning, Department of Computer Science, Suresh Gyan Vihar University, 20/01/2014, http://hdl.handle.net/10603/36464

[90]. Sharma, S., & Dalal, S. (2014). Recognition and identification schemes for the development of Eigen feature extraction based iris recognition system. International Journal of Recent Research Aspects ISSN, 2349-7688.

[91]. Sharma, P., Sharma, K., & Dalal, S. (2014). Preventing Sybil Attack in MANET using Super nodes approach. International Journal of Recent Research Aspects, 1(1), 30-34.

[92]. Simi Gupta, D., & Dalal, S. (2014). Efficient broker scheduling in Cloud Computing. International Journal of Recent Research Aspects, 1(2), 74-77.

[93]. Sharma, S., & Dalal, S. (2014). Feature Recognition from Histogram and Eigen Algorithm in Digital Image Processing.

[94]. Gupta, S., Sharma, K. K., & Dalal, S. (2014). Multi objective parameters for real time scheduling in cloud computing.

[95]. Mittal, A., & Dalal, S. (2014). Implying p-Cure algorithm in case retrieval stage of the case-based reasoning. International Journal of Recent Research Aspects, 3(3), 91-98.

[96]. Mittal, A., Sharma, K. K., & Dalal, S. (2014). Approach of BPEL in supply chain activities for managing bullwhip effect of SCM system. Int. J. Res. Asp. Eng. Manag, 1(2), 26-30.

[97]. Sharma, P., & Dalal, S. (2014). Shortest Path Algorithms Technique for Nearly Acyclic Graphs. International Journal of Recent Research Aspects, 3(3), 36-39.

[98]. Dalal, S., Jaglan, V., & Sharma, K. K. (2014). Designing architecture of demand forecasting tool using multi-agent system. International Journal of Advanced Research in Engineering and Applied Sciences, 3(1), 11-20.

[99]. Sheikh, M., Sharma, K., & Dalal, S. (2014). Efficient method for WiMAX soft handover in VOIP and IPTV. International Journal of Research Aspects of Engineering & Management, 1(2), 5-48.

[100]. Kumar, S., & Dalal, S. (2014). Optimizing Intrusion Detection System using Genetic Algorithm. International Journal of Research Aspects of Engineering and Management ISSN, 2348-6627.

[101]. Mittal, A., Sharma, K. K., & Dalal, S. (2014). Applying clustering algorithm in case retrieval phase of the case-based reasoning. International Journal of Research Aspects of Engineering and Management, 1(2), 14-16.

[102]. Dalal, S., Jaglan, V., & Sharma, K. K. (2014). Integrating Multi-case-base-reasoning with Distributed case-based reasoning. International Journal of Advanced Research in IT and Engineering ISSN, 2278-6244.

[103]. Saini, A., Sharma, K. K., & Dalal, S. (2014). A survey on outlier detection in WSN. International Journal of Research Aspects of Engineering and Management ISSN, 2348-6627.

[104]. Sharma, P., Sharma, D. K., & Dalal, S. (2014). Preventing Sybil Attack In MANET Using Super Node Using Approach. International Journal of Recent Research Aspects, ISSN, 2349-7688.

[105]. Chahar, P., & Dalal, S. (2013). Deadlock resolution techniques: an overview. International Journal of Scientific and Research Publications, 3(7), 1-5.

[106]. Dalal, Surjeet, Keshav Jindal, and Monika Nirwal. "Developing Flexible Decision Support Systems Using Case-Base Reasoning System." International Journal of Engineering and Management Research (IJEMR) 3.4 (2013): 13-17.

[107]. Dalal, S., & Sharma, K. K. (2013). Simulating supply chain activities in multi-agent based supply chain management system with plasma simulator. International journal of Computer Science & Communication, 4(1), 80-85.

[108]. Dalal, S., Tanwar, G., & Alhawat, N. (2013). Designing CBRBDI agent for implementing supply chain system. system, 3(1), 1288-1292.

[109]. Dalal, S., & Athavale, V. (2012). Challenging Bullwhip Effect of Supply Chain Through Case Based Multi Agent System: A Review. International Journal of Advanced Research in Computer Science and Software Engineering, 2(12), 267-272.

[110]. Dalal, S., Tanwar, G., & Jindal, K. (2012). Agent Oriented Programming In Trading System Automation. International Journal of Research in IT, Management and Engineering, 2(8), 51-59.

[111]. Dalal, Surjeet, and Vijay Athavale. "Analysing Supply Chain Strategy Using Case-Based Reasoning." Journal of Supply Chain Management Systems 1.3 (2012).

[112]. Jindal, K., Dalal, S., & Jaglan, V. (2012). Comparative Study On IEEE 802.11 Wireless Local Area Network Securities. International Journal of Advanced Research in Computer Science, 3(1).

[113]. Jindal, K., Dalal, S., & Tanwar, G. (2012). Congestion Control Framework in Ad-Hoc Wireless using Neural Networks in QoS. International Journal of Research in Computer Engineering and Electronics, ISSN, 15-18.

[114]. Dalal, S., Athavale, V., & Jindal, K. (2012). Designing Case-based reasoning applications with Colibri Studio. International Journal of Research in Computer Engineering and Electronics, 1(1), 15-18.

[115]. Jaglan, V., Dalal, S., & Srinivasan, S. (2011). Improving performance of business intelligence through case based reasoning. International Journal of Engineering Science and Technology, 3(4), 2880-2886.

[116]. Jaglan, V., Dalai, S., & Srinivasan, S. (2011). Enhancing security of agent-oriented techniques programs code using jar files. International Journal on Computer Science and Engineering, 3(4), 1627-1632.

[117]. Dalal, S., Athavale, V., & Jindal, K. (2011). Case retrieval optimization of Case-based reasoning through Knowledge-intensive Similarity measures. Int. J. Comput. Appl, 34(3), 12-18.

[118]. Surjeet Dalal, V., & Kumar, S. (2010). Designing of business tool using intelligent agent. In National Conference Advanced Computing & Communication tech ACCT (pp. 751-754).

