EasyChair Preprint

№ 9913

Quantum Web-Based Health Analytics System

K Pradheep Kumar and Acm Dhinakaran. K.

March 31, 2023

Quantum Web-Based Health Analytics System

K. Pradheep Kumar[1],Dhinakaran K[2]

[1*]Assistant Professor, Department of Computer Science and Engineering, BITS Pilani, India.

[2]Assistant Professor, Department of Artificial Intelligence and Data Science, Dhanalakshmi College of Engineering, Chennai, India.

K.Pradheep Kumar* E-mail(s): pradjourn@gmail.com;
Contributingauthors:maildhina.k@gmail.com;

Abstract

In this work, a quantum web-based health analytics system has been proposed. The system uses a Neuro-Fuzzy algorithm which uses a selective rule-based strategy to process data sets. When a query is being raised, the datasets required are identified and processed to formulate inference for a knowledge repository. The knowledge repository is decentralized and ensure authentic access for a particular query. The quantum block chain algorithm reduces processing time and memory consumed by 24% and 28%, compared to the conventional block chain approach.

Keywords: Quantum Block chain, Neuro Fuzzy, Rule Strength, Hyperledger, Qubits, Web 3, Shy computing

1 Introduction

In today's world several diseases occur as pandemics which result in disasters. To overcome the same, it is essential for everybody to have awareness in the healthdomain.

The information available should be authentic and reliable. Hence a security system is required to ensure that no unauthorized access is attempted on the data. This is possible only if we have a decentralized distributed database system where users are restricted to access only a particular subset of datasets. Such a decentralized web known as Web 3 is designed which permits execution on datasets to provide inferences.

In this model datasets are stored in several clouds hosted by multiple service providers. Each service provider has a separate Service Level Agreement. When data is being accessed from a particular cloud environment several challenges such as authorized access, latency, etc are associated. To overcome the same, it becomes essential to have a sky computing model where access is provided to multiple cloud providers without any breach to the service level agreement. Also optimizing the network latency by an appropriate virtualization strategy to facilitate the storage is mandatory.

Each cloud computing source is identified by a tag to identify its source. A query might require several datasets to provide an inference. Further in several cases a query may not require a complete dataset, it might require a partial dataset which is a subset of a dataset. It may also require a simultaneous data mining on partial datasets. This may require extensive processing of the data sets. Such extensive processing may consume large amount of memory resource. This is because inferences are required in a timely manner to avoid any disaster.

A block chain is constructed with inferences which are essential for a query set to provide a required diagnosis for a patient. A quantum computing algorithm is executed on all the nodes of the block chain to provide a diagnosis.

This is accomplished by formulating a rule base for the chosen data sets for each query. A query set comprising of relevant queries is created. A one-to-one mapping exists between the query set and the data sets.

Based on the inferences obtained a diagnosis for a patient is obtained. The quantum block chain algorithm reduces processing time and memory consumed by 24% and 28%, compared to the conventional block chain approach.

The paper is organized as follows: Section 2 reports the literature analyzed in this domain. Section 3 explains the proposed model. It also highlights the salient features of the architecture and the algorithm. Section 4 discusses the simulation results in detail. Section 5 concludes the work and highlights the future directions of extension of work.

2 Literature Review

A quantum block chain is one which has multiple nodes which are in consensus. The consensus problem with Byzantine Agreement has been discussed by Chuntang et al in [1]. Different data frameworks and health records for various health records have been discussed by Rehab et al in [2]. The mapping of cloud computing data as block chains has also been illustrated with different data frameworks. Different digital signature algorithms and use of qTESLA for extracting public key using basic operations of lattices has been explained by Zhang et al in [3]. Digital Signature algorithms and hash checking has also been explained in [3]. Quantum Resistant Cryptographic algorithm particularly using Lattices which has additional features compared to RSA, ECDSA, etc has been discussed by Mohammed and Askar in [4].

Several Blockchain schemes based on code and Lattice for extraction of public key has been explained by Teodora et al in [5]. The Hash based

digital schemes have also been emphasized with reference to the public key cryptography have been illustrated in [5]. A quantum network protocol with quantum repeaters with emphasis on the Network Layer Architecture has been discussed by Kozlowski et el in [6]. A quantum key distribution protocol for Decoherence-free subspace by formulating special quantum error correcting codes in Hilbert Space have been explained by Qianqian et al in [7]. The vulnerabilities in a block chain network have been illustrated and Post Quantum Certificates by LACChain nodes have been explained by Allende et al in [8]. The vulnerabilities have been rated based on their severity level as discussed by Kearney et al in [9]. The various security primitives, Hash functions. Quantum Cryptosystems have also been classified as Multivariate cryptosystems and Lattice cryptosystems have been explained by Fernandez and Paula in [10].

Proposed model

For providing diagnosis for any disease a set of inferences need to be analysed from a knowledge repository. These inferences require extensive processing of datasets, partial datasets, and combined processing of multiple partial datasets.

The proposed model has two stages:

1. Identification of Required datasets
2. Processing of the Required datasets

2.1 Identification of Required datasets

The datasets reside on multiple cloud servers in multiple clusters. The first step is to identify the required datasets. To accomplish the same when a query is raised the same is decomposed into multiple query components. These query components are modelled as query points. Using the metadata information from the cloud the required data sets are collected by making an assessment from the sources. Each source has a Tag and a lookup table is created with a Tag id and the required dataset. Datasets from multiple clouds are linked to a dataset identifier for extraction and then mapped with the query points as shown in Fig 1.

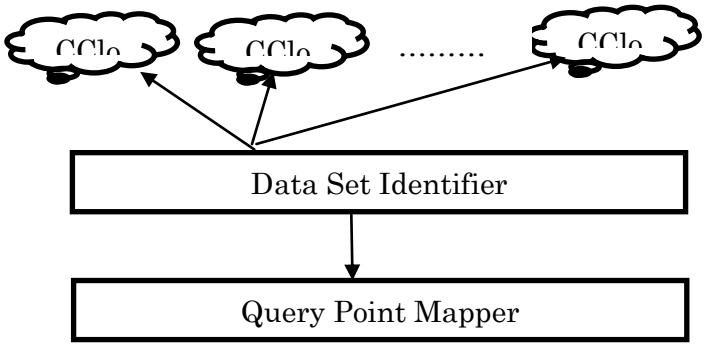

Fig. 1 Block Diagram showing mapping operation of query points with datasets

2.2 Processing of Required Datasets

For each query a rule base is formulated and a threshold for the same is computed based on the rule strength.
The rule strength is computed using the following expression:

$$RS(i) = \sum_{i=1}^{i=n} (Wt(i) * Lingval(i) \quad \text{----------} \quad (1)$$

Where Wt(i) is the attribute significance for the query component and Lingval(i) is the mid value of the linguistic fuzzy variable
The Threshold of the Rule base is computed using the following expression:

$$T = \frac{\sum_{i=1}^{i=n} (Rid * RS(i))}{\sum_{i=1}^{i=n} Rid} \quad \text{----------} \quad (2)$$

Where Rid is the rule number and RS(i) is the rule Strength.
Rules whose rule strength is less than the threshold is chosen and only those rules are packed as qubits. Each qubit would handle 2^n rules. The qubits then process the datasets identified.

2.2.1 Creation of Quantum Block Chain:

The output of each qubit which is an inference is stored as a block in the quantum block chain. The block chain used here is a Hyperledger type without a wallet. Finally a Hadamard gate operation is applied to the quantum block chain by aggregating the outputs of each qubit. The Hadamard gate operation analyses all combinations of qubits and optimizes the same. It then provides the diagnosis. The quantum block chain with qubits processing the datasets has been illustrated in Fig 2

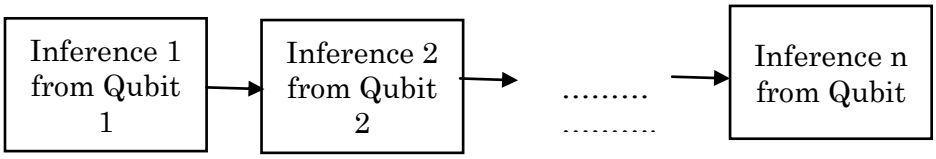

Fig. 2 Quantum Block chain

The Hadamard Gate processing on the quantum block chain to provide the diagnosis is shown in fig 3.

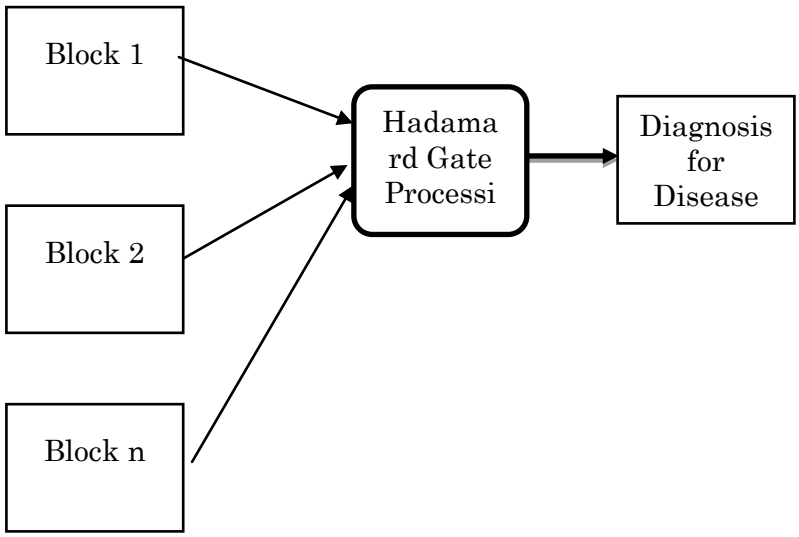

Fig. 3 Block diagram processing of quantum block chain

Algorithm

- Fetch a Query Set
- For each query in set
- Decompose the query into query components
- For each Query Component identify the required datasets
- For each query point create a Rule base
- Compute the Rule Strength and Threshold for the Rule base
- Choose Rules whose Rule Strength is less than the Threshold
- Decide on the number of qubits
- Each qubit would store 2^n rules where n is the number of rules
- Map each qubit to the required datasets to process
- Aggregate Results of all query points of a particular query.
- Store results of each query as a node in the quantum block chain
- Repeat the above step for all queries in the set.
- Apply Hadamard gate processing for all blocks in the block chain to obtain the diagnosis for a patient.

3 Stimulation Results:

The algorithm was implemented using CIRQ to convert JSON objects to Qubits. It was tested for 1,00,000 data sets across 3 Cloud Provider Platforms namely Google, Amazon and Azure. The performance of the algorithm was assessed based on the following metrics:

- Processing Time
- Memory Consumption

3.1 Processing Time:

The Processing Time is the total time duration to decompose a query into query components, fetch the required datasets and process the same. It is the time involved for the entire query set after applying the Hadamard gate operation on quantum block chain.

Table 1 Query Processing Times (Conventional Block Chain Vs Quantum Block Chain Approach)

No. of. Data sets	Processing Time		Reduction(%)
	Conventional Blockchain Approach (secs)	Quantum Blockchain Approach (secs)	
10000	15.78	12.41	21.36
20000	23.45	18.65	20.47
30000	34.56	24.51	29.08
40000	47.51	35.65	24.96
50000	57.87	43.56	24.73
60000	65.67	52.34	20.30
70000	75.67	56.54	25.28
80000	86.57	66.54	23.14
90000	94.56	72.34	23.50
100000	98.65	75.47	23.50
Average	**60.63**	**45.80**	**23.63**

It could be observed that the average reduction of processing time which is 24% could be obtained for 50,000 data sets compared to the conventional approach and maximum reduction of processing time which is 29% is obtained for 30,000 datasets as shown in Table 1 and illustrated in Fig 4 and 5.

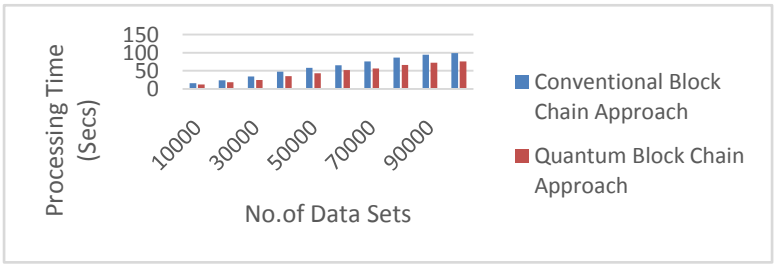

Fig 4. Plot Comparing Processing Times (Conventional Block Chain Approach Vs Quantum Block Chain Approach)

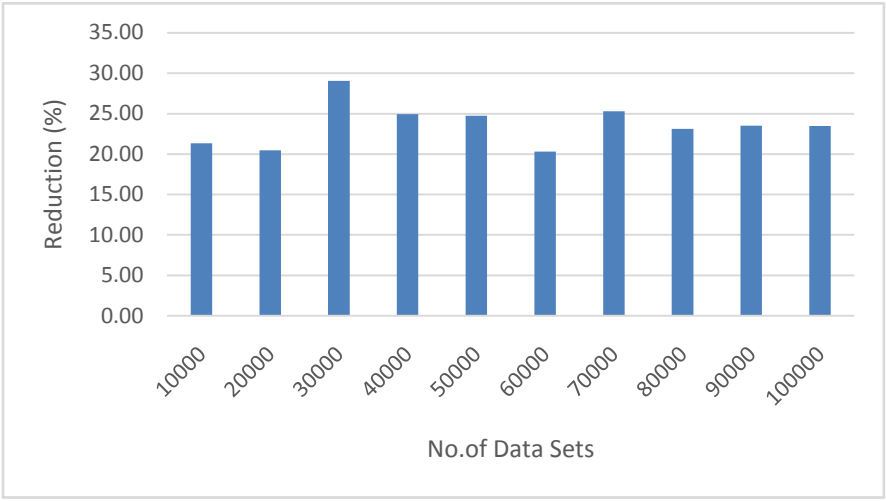

Fig 5. Plot showing Reduction of Processing Time using Quantum Block Chain Approach

3.2 Memory Consumption:

The memory resource consumed store the entire quantum block chain which is the aggregate of all the nodes in the quantum block chain.

The memory resource consumed by the quantum block chain and conventional block chain approach has been tabulated in Table 2.

Table 2 Resource Consumption (Conventional Block Chain Vs Quantum Block Chain Approach)

No. of. Data sets	Processing Time		Reduction(%)
	Conventional Blockchain Approach (secs)	Quantum Blockchain Approach (secs)	
10000	11.45	8.75	23.58
20000	18.67	12.67	32.14
30000	29.45	19.54	33.65
40000	36.76	23.45	36.21
50000	47.54	32.54	31.55
60000	56.76	41.43	27.01
70000	65.43	49.87	23.78
80000	74.34	57.65	22.45
90000	84.42	63.45	24.84
100000	96.46	72.34	25.01
Average	**52.128**	**38.17**	**28.02**

It could be observed that the average reduction of memory resource which is 28% could be obtained for 60,000 data sets compared to the conventional approach and maximum reduction of memory resource which is 36% is obtained for 40,000 datasets as shown in Table 2 and illustrated in Fig 6 and 7.

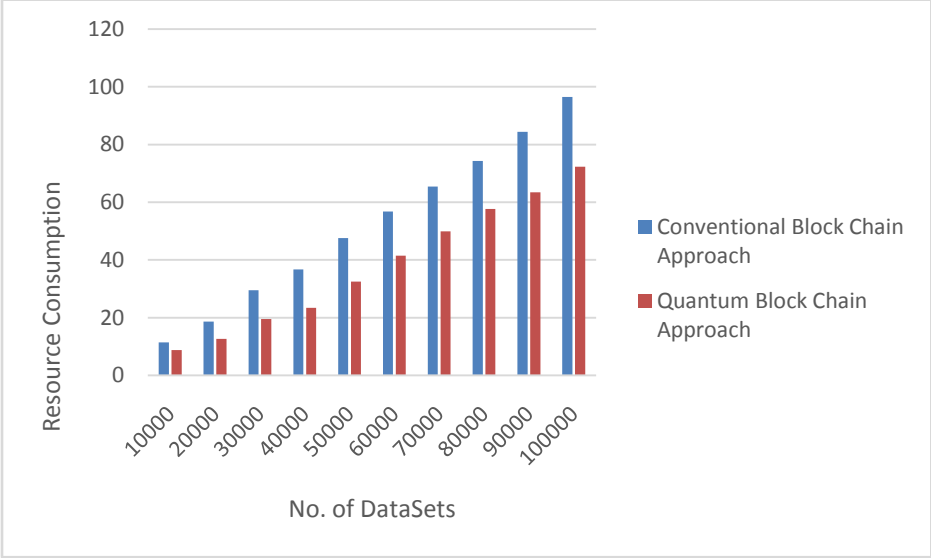

Fig 6. Plot Comparing Processing Times (Conventional Block Chain approach Vs Quantum Block Chain Approach)

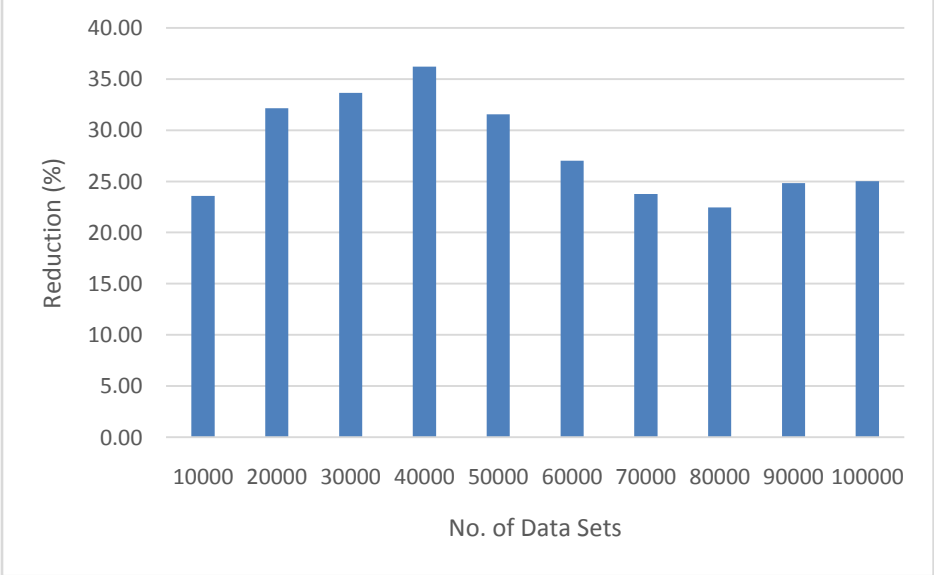

Fig 7. Plot showing Reduction of Memory Consumed using Quantum Block Chain Approach

4 Conclusion

In this work a Quantum Block Chain network has been proposed for a Web 3 architecture. The work attempts to enhance security and achieve high speed dataset processing. The quantum block chain algorithm reduces processing time and memory consumed by 24% and 28%, compared to the conventional block chain approach.

5 Future Work

The Quantum Block chain network could be ported in Web 3 platform to create a Quantum Internet. Additional security protocols could be incorporated to add more security and provide reliable diagnosis for patients.

6 Reference

[1] Chuntang Li, YinSong Xu, Jiahao Tang and Wenjie Liu. "Quantum Blockchain: A Decentralized, Encrypted and Distributed Database Based on Quantum Mechanics", Journal of Quantum Computing, Vol 1, No.2, pp 49-63, 2019.

[2] Rehab A. Rayan, Imran Zafar and Christos Tsagkaris. "Blockchain Technology for Healthcare Cloud-Based Data Privacy and Security", Book: Integration of WSN into Internet of Things, pp 336-349, 2021.

[3] Peijun Zhang, Lianhai Wang, Wei Wang, Kunlun Fu and Jinpeng Wang. "A Blockchain System Based on Quantum-Resistant Digital Signature".

[4] Zhwan Mohammed Khalid and Shavan Askar. "Resistant Blockchain Cryptography to Quantum Computing Attacks", International Journal of Science and Business, pp 116-125, 2021.

[5] Andrada-Teodora Ciulei, Marian-CodrinCretu and Emil Simion. "Preparation for Post-Quantum Era: a survey about blockchain schemes from a post-quantum perspective", pp 0-37, Jan, 2022.

[6] Wojciech Kozlowski, Axel Dahlberg and Stephanie Wehner. "Designing a Quantum Network Protocol", ACM, pp 1-16, 2021.

[7] Qianqian Hu, Tianzi Sun, Bao Feng and Wei Jia. "A quantum key distribution scheme based on quantum error-avoiding code in decoherence-free subspace", pp 1-35,ACM, May 2019.

[8] Marcos Allende, Diego Lopez, Sergio Ceron, Antonio Leal, Adrian Pareja, Marcelo Da Silva, Alejandro Pardo, Duncan Jones, David Worrall, Ben Merriman, Jonathan Gilmore, Nick Kitchener, Salvador E.Venegas-Andraca. "Quantum-Resistance in Blockchain Networks", ITE Department, IDB Lab, pp 1-30, Jun 2021.

[9] Joseph J.Kearney, Carlos.A, Perez Delgado. “Vulnerability of Blockchain Technologies to Quantum Attacks”, pp 1-10, Apr 2021.

[10] Tiago M.Fernandez-Carames and Paula Fraga-Lamas. “ Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks”, IEEE Access, Vol 1, 2020.