**Research Proposal**

# on

# Post Quantum Security Enhancement Scheme in Blockchain Embedded Smart Technologies

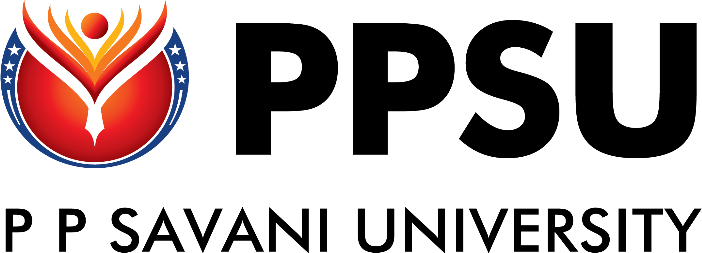
# In the field of

# Computer Science Engineering

# Submitted by

# Mr Raviraj Chauhan

# Submitted to



# Admission Batch: July 2023

## INTRODUCTION

Blockchain has emerged as an efficient digital ledger, decentralized technology in managing transactions. A collection of IoT devices connected in a blockchain framework to jointly manage the database that records and maintains various transaction details. This leads to the transactions being managed simultaneously by all the IoT devices, and not a particular central authority [1]. Information that is held on a blockchain exists as a shared and continually coordinated database. The blockchain database isn't stored in any single location but is distributed among various systems over the network. The information is hosted by multiple IoT devices simultaneously, its data is accessible to anyone on the internet. Due to the decentralization of the information among multiple systems, the adversary cannot overload a particular node using the Distributed Denial of Service attack [2]. This prevents individual nodes from getting overloaded, hence providing higher security and better accessibility for the users. The blockchain framework becomes more user friendly as anyone can access the recent and updated data at any time. Blockchain is an emerging technology that ensures that there are no missed transactions due to an overload on server, or machine error, or human error or even due to an exchange that was not done without the consent of the parties involved [3]. Blockchain uses various hashing functions and digital signatures to ensure the authenticity of the transaction. Blockchain provides transparency by letting the users know about the status of their transactions as discussed by [4]. It sounds like a fool proof technology but one feature that blockchain lacks is in-built confidentiality. It does not provide the facility of encrypting private data before sharing it on the blockchain. Several private blockchain framework have started implementing several traditional public key encryption algorithms like RSA to solve the confidentiality loop-hole [5]. But the security of the classical cryptographic algorithm mostly depends on the intractability of the elliptic curve discrete logarithm problem and the integer factorization problem. The quantum computers can have powerful parallel computing ability which might become a great threat to classical cryptographic algorithms as proposed by Shor. On the contrary, genetic algorithm is a method for solving both constrained and unconstrained optimization problems that is based on natural selection, the process that drives biological evolution [6]. The genetic algorithm repeatedly modifies a population for individual solutions. Thus, making it independent of Shor’s factorization. Genetic approach can act as a key to protect our private information in the quantum era. In this research work we combined blockchain with genetic approach and developed a double crossover security framework to enhance security in several applications of smart technologies [7]. The rest of the sections of this work briefly explain the related work in this domain followed by our contribution in the field of security of smart technology. Furthermore, this work includes the brief overview of the applications on which we have tested our algorithm. Finally, the work concludes with the strength testing of the proposed framework using various security parameters like information entropy analysis, chi-square test analysis of cipher image, correlation analysis, plaintext and key sensitivity test, time complexity analysis, noise and data losses.

## RELATED WORK

#### [5] and other NASA scientists demonstrated the possibility of the generation of virtual quantum computers in the real-world scenario. They proposed several technical advances that pave the way towards error correction. They developed fast and high-performing gates that would be executed simultaneously across two-dimensional quantum bits arrays. They benchmarked the processor at component and system level using a cross-entropy technique. Then, they used component-level fidelities to accurately calculate the performance of the whole system. [6] realized that Feynman’s vision of quantum computers poses significant experimental and theoretical challenges. A quantum system needs to be engineered to perform massive computations with a minimized error rate to provide a quantum speedup. Keeping in mind that the methodology should be np-hard for a classical computer but can be solved in polynomial time by a quantum computer. By computing a novel benchmark task on a superconducting quantum bits processor, [7] tackled both of these. [8] have discussed the quantum computing attack. To handle the security of IoT devices connected in a blockchain framework, the authors defined Post Quantum Blockchain (PQB) and proposed a secure cryptocurrency approach based on lattice cryptography, which is capable of resisting quantum computing attacks. [18] discussed entanglement-based quantum cryptography to tackle the issue of quantum computing attack. [19] used quantum key distribution to provide security in the field of medical science by protecting patients’ privacy. [9] worked on intellectualization of smart automobiles. [10] concluded that the amalgamation of blockchain infrastructure and the intellectual vehicular industry provides answers for the most clutching issues, particularly those identified with unwavering quality and security of communication. The blockchain would have the befitting course of action to embellish information streams from programmers with the most elevated accessible degree of security [11]. In the vehicular innovation pursuit, the utilization of sequestrated records can guarantee that counterfeit scrap cannot be embedded into the pliant genuine fraction, which is undertaken by straightforwardness in the suave chain for creation, conveyance, and providers. Moreover, in the vehicle-blockchain combo business, perspicacious agreements can be implanted underway blockchain to consequently give information requests at specific phases of the creation cycle. In the world of smart grids as well, the use of blockchain shows promising prospects. Lately, many organizations have been working together to recompute the utilization of power sources and mitigate the energy extremity [12]. The entire global framework relies on electricity apparatus build traditionally; this is resulting in exceeding ineffectiveness. Currently, in the existing electricity grid structure, resources are utilized blindly to meet the societal requirements [13]. Extravagant use of resources and energy leads to excessive release of carbon dioxide into the atmosphere, which is the major cause of global temperature rise. A thorough arrangement of Smart Grid with renewables would be a major step to address environmental crashes [14]. The worldwide organizations are now coordinating together to develop a grid that is efficient and productive. Controlling authorities are effectively teaming up on inventive ways to deal with the making of Smart-Grid [15]. Furthermore, research shows that private buyers will pay more to reduce the half-life span of ozone-depleting substances [17].

## RESEARCH GAP & OBJECTIVE OF THE STUDY UNDERTAKEN

#### From the related work we observed that the security of the futuristic smart technology is the major concern. Quantum computers can easily break the traditional cryptographic approaches according to Shor’s hypothesis. During the course of the present research, following primary objectives are assumed to be fulfilled.

#### Securitization of the applications of smart vehicles, smart grids, smart healthcare, smart education and smart currency in quantum era.

#### Develop a quantum resistant algorithm to provide high range avalanche effect.

#### Develop an algorithm which can perform the task in polynomial time.

#### Develop an algorithm to avoid data loses after decryption of the ciphertext.

#### Develop an algorithm to provide high entropy to the encrypted data.

#### Develop an algorithm to avoid correlation between plaintext and ciphertext.

## PROPOSED METHODOLOGY

#### In this work, we propose a post quantum security enhancement scheme in blockchain infrastructure. Firstly, the data is fetched and prepared. Data consists of road condition images in smart vehicles application; or electricity consumption data in smart grids application; or medical images like COVID infected lungs image in smart healthcare application; or students’ facial expression image during online class in smart education application; or transaction amount in smart currency application. Depending on the application, the data varies. This data is concatenated with any other personal data. This concatenated data is then XORed with key generated from a pseudorandom bit generator. After this substitution and permutation operations are performed as described in the following equations.

The data is collected using IoT devices. Filtering and cleaning of the collected data are performed. Later the consumption data is encrypted. To provide authentication, the hash value is computed and appended with the data. Then it is shared on the blockchain framework. We devised a security framework for the securitization of smart grids. In the proposed flow, the consumption data is calculated using gamma function Γ(𝑧). It helps in modeling scenarios with uncertainty and continuous changes. Then gaussian integral is used to calculate the consumption data 𝐶𝑑 over a particular time duration 𝑡. To generate key, in the following equations, is Personal Data; is type of usage; is random number generated; is the hexadecimal number from Substitution box; is power consumption; is auxiliary power consumed by the meter or sensor etc.; is the power wastage rate due to the deterioration of panel or grid with passing time.

After calculating the consumption data, padding is performed between consumption data, personal data, and type of consumption. Personal data is padded on the most significant side of the consumption data. The type of consumption is padded on the least significant side of the same.

Thereafter, perform XOR operation between the resulting padded data and pseudo-random number generated from the random number generator.

The least significant half of the XORed data is stored as an integer in and the most significant half of the same is stored in .

## APPLICATIONS OF PROPOSED RESEARCH

**Smart Vehicles**

Conduction of this demonstrative investigation is done using Udacity’s open-source smart vehicle simulation framework [28]. The model training is fulfilled scrupulously using the nano degree program for 10 minutes of drive, 10 times leading to an aggregate of 100 minutes total drive time. The car is accoutered with three additional homogeneous camcorders on it’s exterior to snap lane images from three different angles. The following three screencaps exemplify the lane images snapped by the camcorders.

**Smart Grids**

Smart grid simulation is performed using OpenDSS and Anaconda-Jupyter. In OpenDSS, we have taken phase lines and buses to simulate the electric grid. The following lines show the phases, buses, line code, and length of the phase line. The phase line connectivity of the grid is demonstrated in subsequent figures.

## SELECTED REFERENCES:

1. Biswas, R., Jiang, Z., Kechezhi, K., Knysh, S., Mandrà, S., O’Gorman, B. Wang, Z. (2017). A NASA perspective on quantum computing: Opportunities and challenges. Parallel Computing, 64, 81–98. doi: 10.1016/j.parco.2016.11.002
2. Badr, S., Gomaa, I., & Abd-Elrahman, E. (2018). Multi-tier Blockchain Framework for IoT-EHRs Systems. Procedia Computer Science, 141, 159–166. doi: 10.1016/j.procs.2018.10.162
3. Rieffel , E. G. (2019). Quantum Supremacy Using a Programmable Superconducting Processor. NASA Ames Research Center. doi: NASA/TP-2019-220319
4. Song, J. C., Demir, M. A., Prevost, J. J., & Rad, P. (2018). Blockchain Design for Trusted Decentralized IoT Networks. 2018 13th Annual Conference on System of Systems Engineering (SoSE). doi: 10.1109/sysose.2018.8428720
5. Banerjee, M., Lee, J., & Choo, K.-K. R. (2018). A blockchain future for internet of things security: a position paper. Digital Communications and Networks, 4(3), 149–160. doi: 10.1016/j.dcan.2017.10.006
6. Cheng, C., Lu, R., Petzoldt, A., & Takagi, T. (2017). Securing the Internet of Things in a Quantum World. IEEE Communications Magazine, 55(2), 116–120. doi: 10.1109/mcom.2017.1600522cm
7. Yan, J., Wang, L., Dong, M., Yang, Y., & Yao, W. (2015). Identity-based signcryption from lattices. Security and Communication Networks, 8(18), 3751–3770. doi: 10.1002/sec.1297
8. Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., Fedorov, A. K. (2018). Quantum-secured blockchain. Quantum Science and Technology, 3(3), 035004. doi: 10.1088/2058-9565/aabc6b
9. Biswas, K., & Muthukkumarasamy, V. (2016). Securing Smart Cities Using Blockchain Technology. 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS). doi: 10.1109/hpcc-smartcity-dss.2016.0198
10. Biswas, K., Muthukkumarasamy, V., Singh, K., 2014, An encryption scheme using chaotic map and genetic operations for wireless sensor networks, IEEE Sensors Journal, 2801-2809.