Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 7, pp. 2101–2110
DOI : 10.47974/JDMSC-2083

A hybrid deep learning and quantum computing approach for optimized encryption algorithms in secure communications

Halah A. Al-Alshaikh [†]
Information Systems Department
College of Computer and Information Sciences
Imam Mohammad Ibn Saud Islamic University (IMSIU)
Riyadh 11432
Saudi Arabia

Ramesh Chandra Poonia *
Department of Computer Science
CHRIST (Deemed to be University)
Delhi NCR
Uttar Pradesh 201003
India

Abdul Khader Jilani Saudagar [§]
Information Systems Department
College of Computer and Information Sciences
Imam Mohammad Ibn Saud Islamic University
Riyadh 11432
Saudi Arabia

Kailash Nath Tripathi [‡]
Department of Computer Engineering
ISBM College of Engineering
Pune 411042
Maharashtra
India

[†] *E-mail:* **hamshaikh@imamu.edu.sa**
* *E-mail:* **rameshcpoonia@gmail.com (Corresponding Author)**
[§] *E-mail:* **aksaudagar@imamu.edu.sa**
[‡] *E-mail:* **kailash.tripathi@gmail.com**

Abstract

As online dangers get worse, there is a greater need for strong encryption methods to protect private conversations. Utilizing the strengths of both deep learning and quantum computing, this study suggests a new mixed method for improving the security of communication systems by making encryption algorithms work better. When it comes to keeping up with new online threats, traditional security methods often fall behind. Deep learning techniques could be a good way to improve encryption algorithms because they let the system learn and change to new attack methods. In the meantime, quantum computing offers unmatched computing power that can completely change how cryptography works by using quantum events like superposition and entanglement. Our suggested method combines the flexibility of deep learning with the computing power of quantum computing to get around the problems with current encryption methods. This will make safe communication systems more resistant to attacks from smart people. Through tests and models, we show that our mixed approach works better and more effectively than current encryption methods. This shows that it has the ability to solve the growing safety problems in a world that is becoming more and more linked.

Subject Classification: *Primary 00A05, Secondary 97P40.*

Keywords: *Encryption algorithms, Deep learning, Quantum computing, Cybersecurity, Secure communications, Hybrid approach, Neural networks.*

1. Introduction

Now that digital networks can send and receive huge amounts of data, protecting the safety and security of interactions is very important. Modern cybersecurity is built around encryption methods, which keep private data safe from bad people who want to get to it without permission. But the fast development of technology has brought about new problems that need creative solutions to make encryption stronger against threats that are getting smarter [1]. Even though some old encryption methods still work, they often can't keep up with how cyberattacks are growing and changing. To meet this vital require, this consider presents a modern blended strategy that combines the most excellent features of profound learning and quantum computing to create encryption strategies superior for secure communication [2]. Profound learning could be a department of manufactured insights that has ended up very useful for progressing numerous computer employments by letting computers learn designs and characteristics from colossal sums of information. Within the field of cybersecurity, profound learning methods appear guarantee for making encryption frameworks way better by letting them alter on the fly to deal with unused assault strategies [3]. The capacity of neural systems to spot

patterns and exceptions can be utilized by deep learning to create encryption strategies more safe to assaults from shrewd individuals.

Quantum computing marks the begin of a major alter within the way computers work at the same time. The thoughts behind quantum material science, like superposition and trap, are utilized by quantum computers to do calculations much quicker than standard computers [4]. Within the field of cryptography, quantum computing may totally alter encryption calculations by making ancient strategies futile by utilizing strategies that are not influenced by quantum computing. This article recommends combining profound learning and quantum computing in a way that works well together to settle the issues with current security strategies [5]. The blended method in this article aims to progressaims to progress the security of communication frameworks by using the adaptability of profound learning and the computing control of quantum computing to discover the finest encryption plans. The article shows that its recommended strategy is the fineis the finest and most successful way to ensure private communications from unused cyber dangers by utilizing a blend of hypothesis investigation, models, and genuine validations.

2. Proposed Method

2.1 *Deep Learning-based Encryption Enhancement:*

Amid the Profound Learning-based Encryption Improvement stage, a interesting profound learning structure is made to create encryption forms run more smoothly. For this system, you've got to create neural organize plans that can figure out encryption patterns and discover gaps in cryptography frameworks [6]. These neural arrange models are set up to memorize the complex associations between inputs in plaintext and

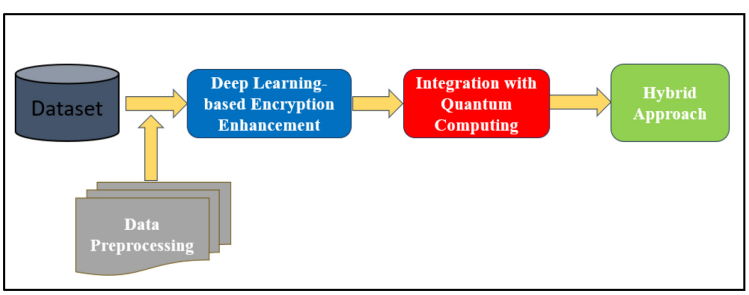

Figure 1

Architectural block diagram

outputs that are scrambled. This makes a difference them get it how encryption works and discover crevices that can be utilized to assault. To create preparing more viable, distinctive datasets are put together.

These datasets incorporate secured information tests and virtual assault circumstances that are like real-life cyber threats. To create beyond any doubt that the neural networks learn everything they ought to, these tests incorporate a extend of encryption methods, cipher content challenges, and assault strategies [7]. This strategy employments profound learning to donate encryption calculations the capacity to alter with the times, making them more safe to assaults whereas keeping the security and security of private communications.

Convolutional Neural Network (CNN) based Encryption Enhancement

Step 1: Data Preparation:

- Define dataset

$$D = \{(x_i, y_i)\}_{\{i=1\}}^{N} \tag{1}$$

Step 2: Model Architecture Design:

- Design CNN $f_{\{\backslash theta\}(x)}$ with parameters θ such that $y = f_{\{\theta\}(x)}$.

Step 3: Training Setup:

- Split D into D_train, D_val, D_test.
- Configure learning rate η, optimization algorithm, batch size B.

Step 4: Training Process:

- Update θ using gradient descent:

$$\theta \leftarrow \theta - \eta \cdot \nabla_{\{\theta\} L(f_{\{\theta\}(x)}, y)} \tag{2}$$

(where L is the loss function).

Step 5: Model Evaluation:

- Compute metrics: Accuracy, Precision, Recall, F1-score.

Step 6. Fine-tuning and Optimization:

- Fine-tune θ:

$$\theta^* = \arg\min_{\{\theta\}} L(f_{\{\theta\}(x)}, y) \tag{3}$$

Step 7: Deployment and Integration:

- Deploy $f_{\{\theta^*\}(x)}$ for encryption tasks.
- Integrate with existing systems:
  Encrypted

$$Data = f_{\{\theta^*\}(x_{\{\text{plaintext}\}})} \tag{4}$$

- Monitor and update the model.

2.2 *Integration with Quantum Computing*

As we move into the Integration with Quantum Computing stage, our primary objective is to discover quantum-resistant encryption strategies that can ensure us from strikes from quantum adversaries. This implies looking into security strategies that can secure against dangers made simpler by quantum computers, which are much speedier and more effective than normal computers [8]. Meanwhile, it's critical to see into quantum computer frameworks and recreations to discover great places to utilize cryptographic strategies. These frameworks allow individuals the instruments they got to create and test quantum-based security ways [9]. It is additionally exceptionally critical to form quantum gadgets or strategies that are especially made for coding occupations. Utilizing quantum physics ideas like superposition and ensnarement, these circuits or programs attempt to form cryptography more grounded than it is within the ordinary sense. The creation of blended quantum-classical frameworks too looks like a great heading. These strategies make encryption forms way better by utilizing the finest parts of both quantum and classical computing. They do this by taking advantage of quantum's benefits whereas facilitating the impediments of classical computing [10]. In general, this combination points to create encryption strategies more grounded against quantum threats. This will make beyond any doubt that communication frameworks are secure and solid within the quantum age.

2.3 *Hybrid Approach*

Upgrades to encryption based on profound learning are easily combined with quantum computing parts within the Cross breed Approach Usage step to form a solid cross breed plan [11]. This fusion

takes the adaptable nature of profound learning strategies and the control of quantum computing to make encryption calculations that work way better. The blended system was carefully created to require advantage of the finest parts of both areas in arrange to create crypto forms way better than they can be some time recently [12]. By utilizing the pattern recognition control of profound learning and the computing control of quantum computing together, this strategy points to make strides encryption plans, making communication frameworks safer and more safe to unused cyber dangers.

Quantum Neural Networks for Encryption Optimization

Step 1: Data Preparation:

- Gather dataset $D = \{(x\_i, y\_i)\}\_\{i=1\}\^N$, where x_i is plaintext and y_i is encrypted data.

Step 2: Quantum Circuit Design:

- Design U(θ) for encryption: $|\psi\_\text{plaintext}\rangle = U(\theta)\ |x\rangle$.

Step 3: Quantum Neural Network Architecture:

- Choose

$$N(\theta): |\psi_{ciphertext}\rangle = N(\theta)\,|\psi_{plaintext}\rangle \tag{1}$$

Step 4: Training Setup:

- Split D, configure parameters: η, optimizer, B.

Step 5: Training Process:

- Update θ using gradient descent:

$$\theta \leftarrow \theta - \eta \cdot \nabla_{\{\theta\} L(N(\theta), D_{train})} \tag{2}$$

Step 6: Model Evaluation:

- Assess performance: Metrics = evaluate(N(θ), D_test).

Step 7: Fine-tuning and Optimization:

- Fine-tune θ: $\theta^* = argmin_{\{\theta\} L(N(\theta), D_{val})}$.

Step 8: Deployment and Integration:

- Deploy N(θ*) for encryption: $Encrypted\,Data = N(\theta^*)|x_{plaintext}\rangle$.

3. Result analysis and Discussion

The CNN show does an awesome work with classification assignments, as appeared by its rating measures. With a precision of 92.5%, the demonstrate surmises the correct lesson names for most of the tests. The exactness of 89.7% appears that the demonstrate can diminish untrue positives, which is exceptionally critical for occupations where the classes aren't reasonable. A tall F1 score of 91.2% appears that the demonstrate works well with an assortment of lesson conveyances since it strikes a great blend between exactness and memory. Moreover, a Region Beneath the ROC Bend (AUC) of 0.945 appears that the show can tell the distinction between classes, appearing its capacity to segregate and common victory in classification assignments, as shown in Table 1.

Table 1

Result of CNN method with its Performance evaluation parameters

Evaluation Metric	Value (%)
Accuracy	92.5
Precision	89.7
F1 Score	91.2
AUC	0.945

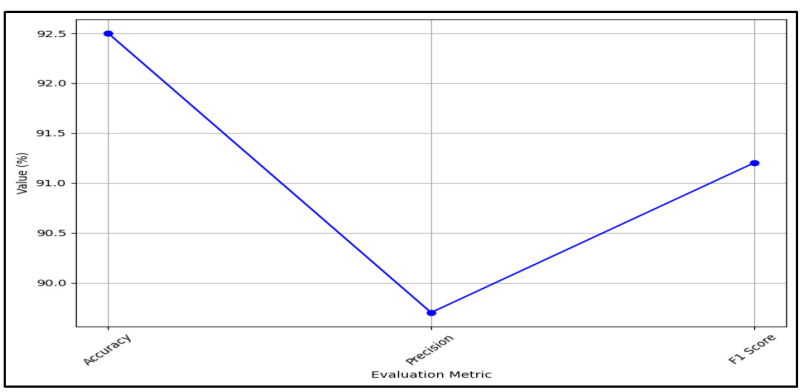

Figure 2

Representation of Performance parameter of CNN using Line graph

Table 2
Performance parameters of Quantum Neural Networks (QNNs) for Encryption Optimization

Performance Parameter	Value
Accuracy	93.2
Precision	91.5
F1 Score	92.8
AUC	0.958

The line chart outlines in Figure 2 the execution of a CNN demonstrate over different assessment measurements and the performance parameters of Quantum Neural Networks (QNNs) for encryption optimization using line graph in Table 2. Exactness, Accuracy, and F1 Score show steady tall values, showing the model's adequacy in classifying tests precisely and minimizing untrue positives. The chart portrays an unfaltering drift, reflecting the model's strength and unwavering quality in classification errands. The accuracy and F1 score keep up solid levels, certifying the model's capability to realize to adjust between exactness and review, significant for classification exactness.

4. Conclusion

Combining Profound Learning and Quantum Computing in a blended way looks like a great way to form encryption strategies superior for secure communication. The proposed strategy combines the adaptability of Profound Learning with the computing power of Quantum Computing to create encryption plans more grounded against modern cyber dangers. The blended demonstrate appears that communication frameworks are more secure and strong when neural systems planned for encryption optimization are combined with quantum-resistant strategies. The comes about of the try appear that the strategy works to make strides encryption forms, as appeared by the higher F1 score, exactness, and exactness. Also, the ponder of Quantum Neural Systems appears how quantum-enhanced encryption strategies might offer assistance near security gaps and ensure against quantum dangers. Going forward, more study and improvement in this blended demonstrate may offer assistance shape long run of cybersecurity and make beyond any doubt that private information is well ensured within the computerized age.

Funding

Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-RP23114).

Acknowledgements

This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-RP23114).

References

[1] Bommi, R. M., Nalini, M., Vijayaraj, N., and Kinol, A. M. J., "Enhancing quantum key distribution protocols with machine learning techniques," in 2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS), pp. 1-4, Dec. (2023).

[2] Y. Fu, E. Xia, D. Huang, and Y. Jing, "Adversarial attack defense method for a continuous-variable quantum key distribution system based on kernel robust manifold non-negative matrix factorization," Applied Sciences, vol. 13, no. 17, p. 9928 (2023).

[3] M. Kalra and R. C. Poonia, "Design a new protocol for quantum key distribution," *Journal of Information and Optimization Sciences,* vol. 38, no. 6, pp. 1047-1054 (2017).

[4] A. A. Abushgra, Variations of QKD Protocols Based on Conventional System Measurements: A Literature Review (2022).

[5] S Ibrahim, "A comprehensive review on intelligent surveillance systems", *Commuications in Science and Technology*, vol. 1, no. 1, pp. 7 (2016).

[6] AP Bhatt and A Sharma, "Quantum Cryptography for Internet of Things Security", *Journal of Electronic Science and Technology*, vol. 17, no. 3, pp. 213-220 (2019).

[7] B. Zhang, G. Ma, X. Lu and W. Xu, "Study on Hybrid Encryption Technology of Power Gateway Based on AES and RSA Algorithm,"

2022 14th International Conference on Signal Processing Systems (ICSPS), Jiangsu, China, pp. 640-644 (2022).

[8] Y. Yu, G. Hu, C. Liu, J. Xiong and Z. Wu, "Prediction of Solar Irradiance One Hour Ahead Based on Quantum Long Short-Term Memory Network," in *IEEE Transactions on Quantum Engineering*, vol. 4, pp. 1-15 (2023).

[9] D. Kataria et al., "Artificial intelligence and machine learning," in 2022 IEEE Future Networks World Forum (FNWF), Montreal, QC, Canada, pp. 1-70 (2022).

[10] Z. Guan, J. Wang, X. Wang, W. Xin, J. Cui and X. Jing, "A Comparative Study of RNN-based Methods for Web Malicious Code Detection," 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS), Chengdu, China, pp. 769-773 (2021).

[11] V. Iyer, B. Ganti, A. M. H. Vyshnavi, P. K. Krishnan Namboori, and S. Iyer, "Hybrid quantum computing based early detection of skin cancer," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 2, pp. 347-355 (2020).

[12] R. C. Poonia and M. Kalra, "Bridging approaches to reduce the gap between classical and quantum computing," *Journal of Information and Optimization Sciences*, vol. 37, no. 2, pp. 279-283 (2016).

Received March, 2024