Corrosion Management **ISSN: 1355-5243**

(https://corrosion-management.com/)

Volume32, Issue 01–June 2022

SCOPUS

AI Algorithms for Quantum Computing: Enhancing Cybersecurity

1 st Rahul Vadisetty Electrical Engineering,)

Wayne state university) Detroit, MI, USA rahulvy91@gmail.com

***Abstract*—**Artificial intelligence refers to a set of Algorithms that has shown unbelievable success in the analysis of large datasets. The study focuses on the effectiveness of AI algorithms and quantum computing to increase the protection and security of data. They can also provide us with solutions to various problems without wasting any time but due to the limited practicality of quantum computers, they cannot fully replace classical computers so future computers may be a combination of both types. The research conducted qualitative and quantitative research approaches to analyses the effectiveness of AI models. Quantum computers are very important in cybersecurity. Machine learning and simulation indicate that AI and quantum models can protect data from threats. The results indicate that the trained model of AI and Quantum computing maintains strong performance and protects the privacy of data. The research also provides future suggestions to improve data concerns. Future research will focus on advancing quantum technology to further protect data security**.**

***Index Terms— Quantum computers, cyber security, AI Algorithms, Encryption, classical computers*.**

I. Introduction

A. Background

Artificial intelligence refers to an extensive set of algorithms that have been the center of attraction for the last decade and it has shown unbelievable success in the analysis of large datasets. These algorithms are often dependent on a computational model known as a Neural Network. Neutral Network belongs to differential programming techniques. Trainability is the main reason for the success of Neural Network Programs. If trained properly, they should be able to predict well on new data. Neural Network has three layers, the input layer that receives the input information in the forms of numbers and text, Hidden layers that perform several types of mathematical computation, and the output layers that we obtain through rigorous computations. [1].

Corrosion Management ISSN: 1355-5243

(https://corrosion-management.com/)

Volume32, Issue 01–June 2022

SCOPUS

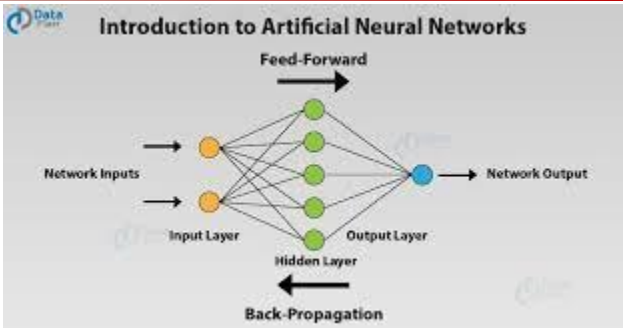

Figure 1 Artificial Neural Networks for Machine Learning [2]

A Quantum computer is a device that efficiently simulates a realizable physical system. They are advanced systems that use quantum bits or the properties of quantum physics to store information. They can solve complex problems much faster than any other computer as they have the skills to perform these complex calculations. Classical computers encode information in binary "bits" while quantum computers encode information in quantum bits or qubits. Qubits are made by the spinning of an electron or a photon. There are situations where Classical computers perform well as compared to quantum ones so the future computers may be a combination of both types [3].

Quantum computers can approach the input and output with complexity because quantum computers use quantum bits instead of binary systems. These quantum bits are also called qubits which are in the superposition state of both 0 and 1. While classical computers can calculate 0 and 1 individually. Quantum bits involve values of 00,01,10 and 11. They use cryptography techniques for encryption. Due to the limited practicality of quantum computers, they are not able to fully replace classical computers

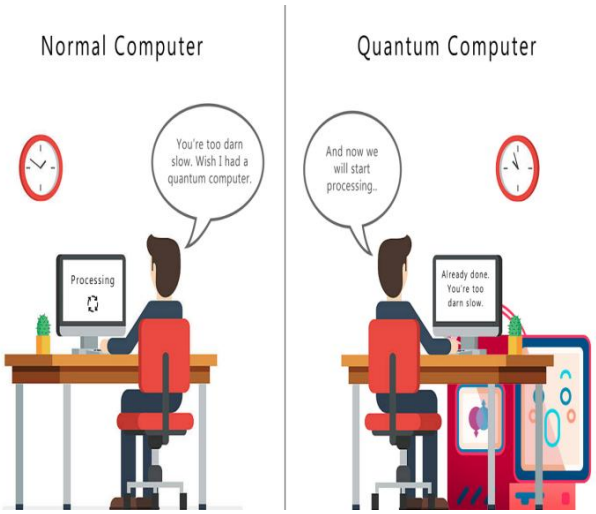

Figure 2 Quantum Computing explained simply and how Quantum Computers work [4].

Corrosion Management ISSN: 1355-5243
(https://corrosion-management.com/)
Volume32, Issue 01–June 2022
SCOPUS

B. Problem Statement

One of the main problems of using AI algorithms in quantum computing is ensuring security. Encryption techniques are used to ensure security for corporate data. To ensure security, advanced Encryption standard algorithms are used against brute-force attacks for file encryption/decryption. Quantum computing is now ready to take current information to a new level based on strong security. Advanced Encryption standards use quantum gates for security. Advanced encryption standards use the same keys for encryption and it can have 128 bits, 192 bits, and 256 bits with encryption keys. Algorithm reliability is an important factor when using AI algorithms in quantum computing. Quantum computing introduces various challenges that can affect the reliability and accuracy of data.

Another challenge while using AI algorithms in quantum computing is reliability and accuracy. Quantum computers operate based on principles which can cause errors. While using quantum computers, the main problem is quantum attack which refers to techniques that are used to attack quantum computers. To enhance the security of the data organizations can use quantum-resistant encryption techniques. Quantum computing faces challenges of limitations of resources which means that quantum computers require specific software and hardware to perform their functions. Quantum computers can cause errors due to noise and de-coherence because of this it requires additional computer techniques for error correction [5].

Computational complexity is another problem that we face while using AI algorithms in quantum computing. AI algorithms often involve vast search spaces for their task which can lead to long processing to Quantum algorithms follow new techniques to tackle these challenges by creating the unique properties of quantum mechanics. These techniques can lead to significant speed-ups in dealing with certain types of problems and make algorithms attractive for AI applications. Different techniques like developing quantum error correction codes, and noise resilient quantum algorithms to overcome the problems that arise during the use of AI algorithms in quantum computing.

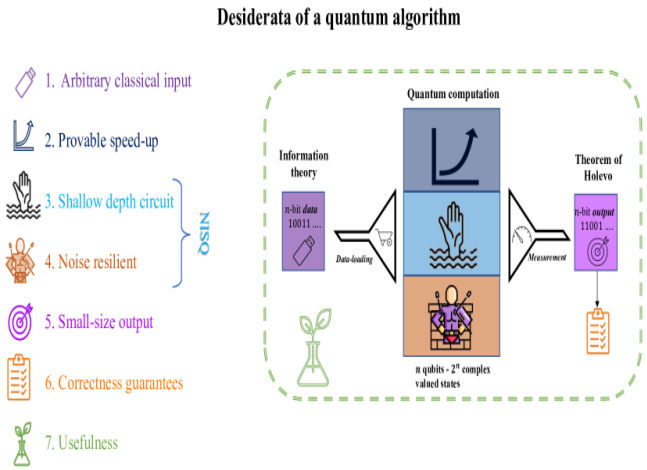

Figure 3 Towards Quantum Advantage on noisy quantum computers [6].

C. Objectives

The research focuses on AI algorithms for quantum computing to enhance cyber security. The main objectives are the role of quantum computers in cybersecurity, and investigating the implementation of AI algorithms in quantum computers to strengthen cyber security measures. We also seek the advantage of collaboration between quantum computer experts and cyber security professionals. While using AI algorithms, raising awareness about the accuracy and reliability of data used in quantum computers. Our main objective is to raise awareness about how technologies like algorithms, quantum computers, and cyber security can work together to develop more security solutions. Moreover, we focus on the benefits, challenges, and plans of using AI algorithms in quantum computers for enhancing cyber security.

D. Research Questions

This study aims to answer the following questions:

1. How can the collaboration between Quantum computer experts and cyber security professionals develop innovation in quantum platforms?
2. How do AI algorithms for quantum computers enhance cyber security?
3. How can quantum computers affect the performance of AI algorithms for cyber security?
4. How quantum computers are better than classic computers in the context of cyber security?
5. What problems might arise while using AI algorithms in quantum computers to enhance cyber security?

Answering these questions will help to improve cybersecurity, the difficulties we may face in using quantum computers for cybersecurity, and techniques to deal with the difficulties.

E. Contribution of the Study

The research is vital for several reasons:

AI algorithms:

Considering AI algorithms in Quantum computing as a primary discussion of the article, several techniques for Quantum computing, the impact of quantum computing in AI algorithms, and problems of AI algorithms are discussed in the context of quantum computing systems.

Knowledge contribution:

Understandings from existing literature add Knowledge to the content of AI algorithms in quantum computing enhancing cyber security

Security improvements:

The findings, discussions, and results of the article provide valuable insights to improve cyber security in quantum computing while using AI algorithms, which can be safely used by companies and individuals.

F. Structure of the Paper

The paper is organized as follows:

Chapter 1: Introduction that focuses on discussing background information, Problem statement and research questions.

Chapter 2: Literature review, a detailed examination of existing studies on AI Algorithms, Quantum computing, the use of AI algorithms in quantum computing to enhance cyber security, and the Intersection of quantum computing and AI.

Chapter 3: Methodology, The methods and techniques are used to enhance cyber security while using AI algorithms in quantum computers.

Chapter 4: Results and discussion, an analysis of the findings and their implications.

Chapter 5: Conclusion and future framework, a summary of the research, its contributions and future direction.

II. Literature Review

A. Introduction

In this chapter, we have discussed the solutions to related problems and how we can solve the problems by following these solutions. Our goal is to discuss related and modern approaches and their drawbacks to create the theoretical background.

A. Quantum Computing

Quantum computing is a field that uses Quantum mechanics concepts to perform computations. It is connected with the fields like mathematics, physics, and computer science. The research on quantum computers is still ongoing and its practical use is zero so it's impossible to predict its future. There is hope that the quantum systems will start showing practical applications like machine learning, and cryptography. As of now, large companies such as Google, Microsoft, and startups like Rigetti, and Xanadu have built quantum. Organizations developed a software development kit that involves cloud services that enable people to experiment and run their code on a quantum computer. The Qubits |0} and |1} are often called computational bases and they can be a superposition of these computational bases [7].

Corrosion Management ISSN: 1355-5243
(https://corrosion-management.com/)
Volume32, Issue 01–June 2022
SCOPUS

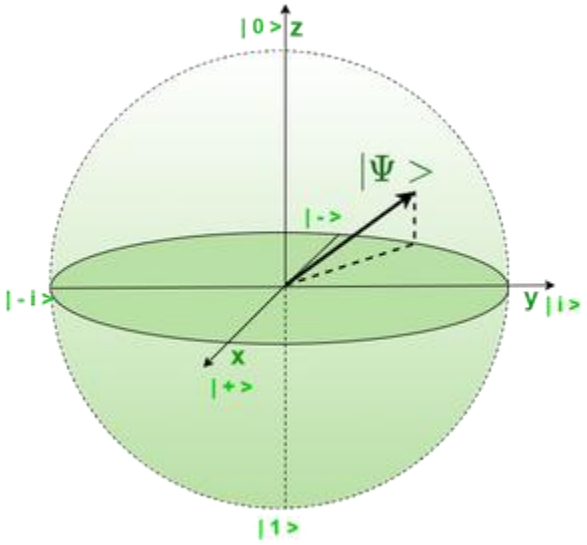

Figure 4 Qubit Representation [8].

Adiabatic quantum computers, Quantum Turing machines, and quantum circuits are the models of computation but the quantum circuit is the most common model of computation. Similar to a classical computer, the Quantum circuit model has quantum gates that are used to transform the input qubit. These quantum gates are used to perform complex computations. The most common gates are The NOT (X), Hadamard, and CNOT(CX). The NOT gate is used to transform |0}, |1} and vice versa, while in the Hadamard gate, the qubit's probability collapses to either |0} or |1}.

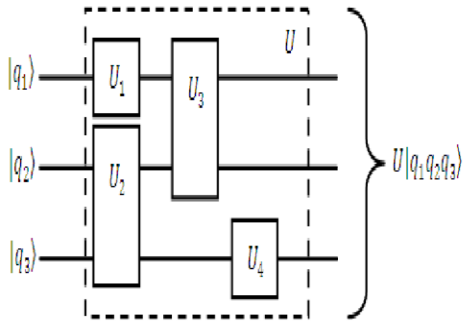

Figure 5 Quantum Circuit Example [9].

Corrosion Management ISSN: 1355-5243
(https://corrosion-management.com/)
Volume32, Issue 01–June 2022
SCOPUS

B. Importance of Quantum AI Algorithm

Quantum computing and AI represent important factors in computational capabilities. Quantum AI algorithms are attached to the unique belongings of quantum computing to increase the performance of AI systems. These algorithms have skills to solve complex problems more rapidly than classical systems. Quantum algorithms can provide various solutions without wasting time in the fields of logistics, and Finance. Quantum algorithms can also process large datasets in machine learning. But these progressions can also have their consequences. Quantum AI algorithms can lead to advancements in drug discovery areas by pretending molecular interactions with unique accuracy, they can break traditional encryption techniques to develop new quantum-resistant methods.

Quantum gates are building blocks for quantum circuits that are capable of operating on qubits and analyzing various quantum operations. Quantum gates are different from classical gates as they are reversible which means that they can transform qubit states without losing any useful information. Some quantum gates are:

Hadamard Gate: which can transform qubit from $|0\rangle$ to $(|0\rangle + |1\rangle)/\sqrt{2}$ and from $|1\rangle$ to $(|0\rangle — |1\rangle)/\sqrt{2}$.

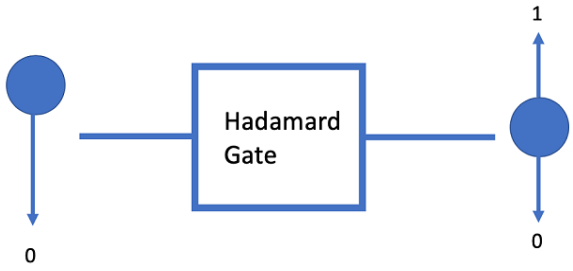

Figure 6 All about Hadamard Gate [10]

Pauli-X Gate:

This gate can flip the state of a qubit.

Controlled-Not Gate:

It is an important gate where the control qubit decides whether to flip the target qubit. These gates are arranged to build quantum circuits to perform complex operations.

C. Types of Problems

Following are the four categories of problems where quantum computers can be significantly advantageous.

- **Combinatorial optimization:**

  It refers to finding the shortest total space between a given set of points. But if we perform these types of problems on a classical computer, a brute-force search is not tractable

- **Problems based on linear algebra:**

Linear algebra is an interrelated field of mathematics that has vectors, and matrices. It acts as a fundamental pillar of machine learning.

- **Problems involving differential equations:**

It relates to one or more functions and their products. It can be used to enhance the behavior of complex systems by applying fundamental laws of physics.

- **Factorization:**

It refers to the transmission of an expression into a product.

D. Quantum Cybersecurity

Quantum computing is considered as most important factor in detecting cyberattacks. It detects the attack before any damage is done. It will provide stronger protections for data by developing strong cryptographic standards. Quantum computers can handle vast amounts of data which means that they can offer more computational power. Because of this benefit, organizations will able to optimize data management by applying quantum mechanism. Algorithms are known as pseudo-random number generators as they cannot create random encryption numbers because they always follow a pattern but quantum Algorithms can act as truly random number generators because of quantum physics and computational power. Quantum systems can also provide us with data security of the highest possible standards by offering randomization. Quantum-protected communications will also use resilient encryption keys on their channels to avoid the entrance of external parties in the future [11]

E. Summary

This chapter describes how quantum computing is an important factor in the field of cyber security as it detects the attack before any damage is done. They can easily handle vast amounts of data and can provide us with solutions to any problem without wasting any time. Quantum AI Algorithms have many benefits as it has properties of quantum computing which increase the performance of AI systems. Quantum gates are also very beneficial as they are capable of operating on qubits and they can easily analyze various quantum operations. Quantum computers are much faster than classical computers as classical computers encode information in binary "bits" while quantum computers encode information in quantum bits or qubits.

Quantum computers can also cause problems when dealing with algorithms. Because Algorithms act as instructions for solving complex problems. One of the biggest challenges for cybercriminals is to acquire encrypted data. Every piece of information is of no use until the data is in incomprehensible form, as it is protected by encryption algorithms.

III. Methodology

A. Introduction

The methodology section outlines the research methods employed in the study to examine the role of AI algorithms for quantum computation in increasing cybersecurity. The sub-section of the methodology chapter justifies data collection and analysis techniques that ensure the study's

reliability and validity. The chapter also focuses on the ethical considerations to ensure the credibility of the research.

A. B. Research Design

The research design is the strategy used by the study to rule out the objectives and questions highlighted in Chapter 1. A mixed research design such as qualitative and quantitative is used in the study to examine the role of AI algorithms in increasing cybersecurity.

In the quantitative approach, the study collects data through surveys and experiments [12]. The research conducts simulations and compares the effectiveness of AI from previous studies. The quantitative method provides rational techniques for analysing the result of the simulation. Furthermore, it also focuses on the effectiveness of the usage of quantum computing to increase cybersecurity [13].

The research employs a qualitative approach to collect data from previous literature. The study collects data from previous journals, articles, publications, and other documents [14]. The research also interacted with other scholars and experts. It enables the study to gather large literature on the topic.

B. Data Collection Methods

The research collects data through qualitative and quantitative approaches which align with the research questions and objectives of the study. In this context, the data was collected through both primary and secondary sources.

The data was gathered through various previous studies and articles. It enables the study to develop a literature review. The study focuses on understanding the concept and information related to AI algorithms and cybersecurity [12]. The sources of the study encompass academic journals, professional research papers, and peer-reviewed papers. Furthermore, the interviews from experts were also conducted in the study to analyses the role of AI in data protection.

The research collects experimental data from surveys and case studies related to quantum computing and data protection. The surveys and case studies are used to collect data from organizations' experience with AI and quantum computing and data protection.

C. Data Analysis Techniques

The research analyses collected data through primary and secondary data. It describes the approach to analysing qualitative and quantitative data and allows conclusions to be drawn by fully evaluating all the information collected.

The data was obtained through previous literature and expert interviews on cyber security and quantum computing. Thematic analysis is used to analyses the collected data. In the thematic analysis, the study analyses patterns and trends in the data and makes possible recommendations [15].

The quantitative data was collected through experiments and simulation of computing of data protection. In this context, the experiment and case study are processed through Quantum computing techniques. This technique ensures the accuracy, efficiency, and privacy of the data. To evaluate techniques, the statistical analysis was conducted and demonstrated with the help of charts and graphs.

D. Evaluation Metrics

The role and effectiveness of AI algorithms were evaluated through various metrics. It includes accuracy, efficiency, scalability, and privacy preservation [16]. These metrics evaluate the effectiveness of AI algorithms in quantum computing, focusing on their ability to improve cybersecurity. The results are compared with established standards to determine the practical applicability and impact of the algorithms on the protection of data from cyberattacks.

E. Experimental Setup

The experimental setup involves creating a quantum computing environment using machine learning techniques and simulation. Popular datasets related to machine learning and AI are selected to apply different techniques. In this environment, AI algorithms such as quantum-enhanced machine learning models are implemented [17]. The focus of the research is on testing the ability of the algorithms to detect and prevent cyber threats such as quantum-based attacks or breaking encryption. The software and hardware are required to implement the experiment process.

F. Reliability and Validity

The research focuses on reliability and validity to ensure credibility and overcome the challenges. The problems associated with AI algorithms for quantum computing in cybersecurity. It enables the study to protect data from cyberattacks and enhance effectiveness.

The study achieved reliability by performing experiments and simulations several times and formulating the results. In this way, the results of several experiments were compared if the values were the same which means the reliability of the study is high [18].

To ensure validity, the study used standard criteria to evaluate the results of different experiments and simulations and confirm the effectiveness of AI on data protection.

G. Ethical Considerations

The study follows ethical considerations to ensure data privacy which is a critical element for the research.

The data gathered from previous literature, surveys, interviews, and experiments was protected in the system. The third party has no right to access the collected data for the study.

The study ensures that participants or interviewers are informed about the purpose of the research. The aim and subject of the study were informed to them in detail [19]. The study ensured that participants were fully aware of the purpose of the study and the usage of their data.

H. Summary

This chapter focuses on the mixed research methodology. The research provides a detailed research methodology through which the study collects and analyses the effectiveness of AI. The methodology section provides knowledge of machine learning and simulation techniques to gather accurate and reliable findings. The next chapter of the research provides the results of experiments and simulations in detail and concludes in the last chapter.

IV. Results and Discussions

A. A. Overview

The results and discussion chapter of the study focuses on the experiment and simulation of the collected data. This section presents the results of the research and details related to the effectiveness of AI and quantum on data protection.

B. Dataset Description

The research used data for the analysis is the Kaggle dataset which is a classic dataset in machine learning research. The Kaggle dataset contains extensive material related to artificial intelligence computing and online secured quantum processing. This dataset centres on various components to study the feasibility of artificial intelligence. It contains system logs, risk indicators and garbled information. Furthermore, this dataset is suitable for preparing and evaluating artificial consciousness models. It can be seen that this data set aims to upgrade network security and protect sensitive information.

C. Data Normalization

In the research, the normalization of data is one of the crucial steps before processing collected data from the database. It aimed to ensure the contribution of training of the model equally. The data from the dataset were normalized in the standard range which is typically from 0 to 1. Furthermore, the range is used to manage the measurement of variables on different scales.

D. Results

The research focuses on the level of accuracy of the model which is used to test the model. The test results show that the established artificial intelligence and quantum recording models maintain their advantages. It can be seen that preparation and testing accuracy directly affect the effectiveness of the model. This reflects that artificial intelligence and quantum processing models can maintain accuracy to protect information security [21]. The results also show that the limitations of the model warrant expectations for the dataset used in the review. The prepared

model demonstrated high accuracy and precision in identifying digital hazards, a huge improvement over traditional techniques.

A. ROC Curves

The ROC curve focuses on determining the error and utility of a classifier for organizing categories and represents the degree of separability. The ROC curve represents the true positive rate and false positive rate, as well as the relationship between them, and is suitable for comparing results in simulation models. The ROC curves in the artificial intelligence and data protection simulation results indicate that individuals are concerned about the protection and security of data in artificial intelligence and quantum computing. Simulation models show that data protection performance, accessibility and accuracy help protect data from threats.

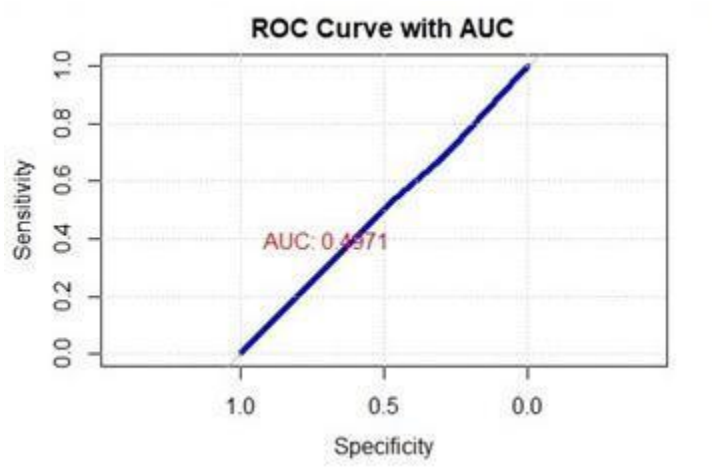

Figure 7: ROC Curve

The ROC curve presented in Figure 7 shows the actual positive rate between categories within the quantum computing and cybersecurity frameworks. This also shows that the AI model effectively reduces network security risks and protects data privacy. From the above simulation model curve, it can be seen that the true positive rate increases and the false positive rate decreases. The AUC value of the ROC curve varies depending on the category. The curve slopes toward the upper left corner, indicating that the model has a higher true positive rate and a lower false positive rate, representing better performance. The ROC curve proves the reliability of the model in accurately detecting and classifying network security threats in a quantum computing environment and supports its practical application to improve network security measures.

B. Confusion Matrix

The confusion matrix provides more precise data and information about each data category in the dataset. This is a machine learning assessment tool that summarizes positive and negative numbers shown in the material. This detailed classification helps to focus on specific categories that were correctly identified and misclassified in the research dataset. The confusion matrix plot

Corrosion Management ISSN: 1355-5243
(https://corrosion-management.com/)
Volume32, Issue 01–June 2022
SCOPUS

shows the detailed performance of the artificial intelligence model used in the study to calculate data security. The matrix results show that artificial intelligence and quantum computing models can effectively reduce network security threats and protect data from leaks. This matrix shows the true positive values for each model class. The frequencies of the matrix shown in Figure 1 indicate that the AI model can enhance cybersecurity and ensure data protection.

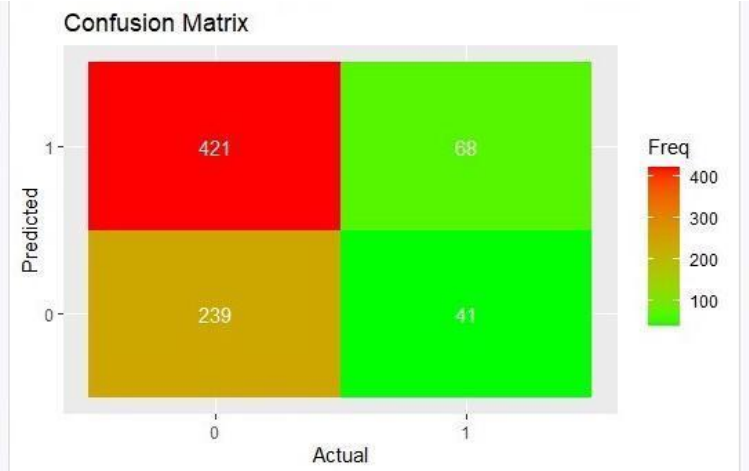

Figure 8: Confusion Matrix

The study effectively demonstrates data protection through machine learning and simulation models. The results of the confusion matrix and ROC curves show that AI algorithms and quantum computing are capable of protecting data and maintaining model performance. During the experiment, the accuracy and efficiency of the model were significantly high. Quantum algorithms can process huge amounts of data faster than traditional algorithms. Additionally, they can detect vulnerabilities and predict threats with unprecedented accuracy [20].

V. Conclusion and Future Work

A. Conclusion

The research focuses on the feasibility of artificial consciousness computations and quantum numbers to protect information from cyberattacks and threats. Artificial intelligence is being used in various areas and the importance of information security is becoming increasingly important. The research evaluates AI and quantum models to ensure information security. The research focuses on integrating protection with AI using Kaggle datasets. The research shows that artificial consciousness plays an important role in monitoring information protection. Quantum figuration techniques offer extraordinary possibilities in the field of artificial consciousness. ROC curves and matrixes show that AI and quantum models are effective and promote individual security concerns. Quantum computation improves computer-aided reasoning cycles by increasing encryption strength and speeding up the location of irregularities. This arrangement increases security against complex cyberattacks and increases the reliability and

security of information. The combination of quantum computing and artificial intelligence promises better protection against evolving digital threats.

B. Future Work

Data protection in the digital environment is becoming increasingly important for key development. Future research will focus on developing quantum encryption technology to better protect communications and data security. It plans to extend these encryption methods to new areas such as the Internet of Things (IoT). In this context, strong security of devices through technology is becoming increasingly important. In addition, special attention is paid to the human aspects of secure communication. It covers user behaviour, interface design, and the impact of quantum encryption on daily practices and privacy issues.

REFERENCES

[1]	S. Mangini, F. Tacchino, D. Gerace, D. Bajoni and C. Macchiavello, "Quantum computing models for artificial neural networks," *A LETTERS JOURNAL EXPLORING THE FRONTIERS OF PHYSICS*, 2021.
[2]	Data Flair, "Artificial Neural Networks for Machine Learning – Every aspect you need to know about," 2021. [Online]. Available: https://data-flair.training/blogs/artificial-neural-networks-for-machine-learning/.
[3]	U. Alvarez-Rodriguez, L. L. M. Sanz and E. Solano, "Quantum Artificial Life in an IBM Quantum Computer," *Scientific Reports*, 4 october 2018.
[4]	TecHindustan, "Quantum Computing Explained Simply And How Actually Quantum Computers Work," 18 may 2018. [Online]. Available: https://medium.com/@techindustan/quantum-computing-explained-simply-and-how-actually-quantum-computers-work-c6e0667f3468.

[5]	K.-K. Ko and E.-S. Jung, "Development of Cybersecurity Technology and Algorithm Based on Quantum Computing," *MDPI*, vol. 11, no. 19, September 2021.
[6]	I. Y. Akhalwaya, S. Ubaru, K. L. Clarkson, M. S. Squillante and V. Jejjala, "Towards Quantum Advantage on Noisy Quantum Computers," *ArXiv*, vol. 1, no. 1, pp. 1-10, 2021.
[7]	V. C. Vikas Hassija, V. Saxena, V. Chanana, P. Parashari, S. Mumtaz and M. Guizani, "Present landscape of quantum computing," *The Institute of Engineering and Technology*, vol. 1, no. 2, pp. 42-48, 2 december 2020.
[8]	Geeksforgeeks, "Qubit Representation," 23 November 2020. [Online]. Available: https://www.geeksforgeeks.org/qubit-representation/.
[9]	M. Elhoushi, "Quantum circuit example.," 2011. [Online]. Available: https://www.researchgate.net/figure/Quantum-circuit-example_fig8_263928386.
[10]	M. Publications, "All about Hadamard Gates," 2020. [Online]. Available: https://manningbooks.medium.com/all-about-hadamard-gates-f36110cd14a0.
[11]	S. S. Gill, A. Kumar, H. Singh, M. Singh, K. Kaur, M. Usman and R. Buyya, "Quantum computing: A taxonomy, systematic review and future directions," *WILEY*, vol. 52, no. 1, pp. 66-114, 2021.
[12]	E. A. A. Abuhamda, I. A. Ismail and T. R. K. Bsharat, "Understanding quantitative and qualitative research methods: A theoretical perspective for young researchers," *International*

	Journal of Research, vol. 8, no. 2, pp. 71-87, 2021.
[13]	K.-K. Ko and E.-S. Jung, "Development of Cybersecurity Technology and Algorithm Based on Quantum Computing," *Applied Science,* vol. 11, no. 19, p. 9085, 2021.
[14]	M. Borgstede and M. Scholz, "Quantitative and Qualitative Approaches to Generalization and Replication–A Representationalist View," *Frontiers in Psychology,* vol. 12, no. 1, p. e20, 2021.
[15]	D. Byrne, "A worked example of Braun and Clarke's approach to reflexive thematic analysis," *Quality & Quantity,* vol. 56, no. 1, pp. 1391-1421, 2021.
[16]	G. S. Handelman, H. K. Kok, R. V. Chandra, A. H. Razavi, S. Huang, M. Brooks and M. J. Lee, "Peering Into the Black Box of Artificial Intelligence: Evaluation Metrics of Machine Learning Methods," *American Journal of Roentgenology,* vol. 212, no. 2, pp. 38-43, 2018.
[17]	S. Zeadally, E. Adi, Z. Baig and I. A. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," *IEEE Access,* vol. 8, no. 1, pp. 23817-23837, 2020.
[18]	R. Gupta, S. Tanwar, S. Tyagi and N. Kumar, "Machine Learning Models for Secure Data Analytics: A taxonomy and threat model," *Computer Communications,* vol. 153, no. 1, pp. 406-440, 2020.
[19]	S. R. M. Arifin, "Ethical Considerations in Qualitative Study," *International Journal of Care Scholar,* vol. 1, no. 2, pp. 30-33, 2018.

[20]	E. Payares and J. C. M. Santos, "Quantum machine learning for intrusion detection of distributed denial of service attacks: A comparative overview," in *SPIE OPTO 2021–Quantum Computing, Communication, and Simulation*, 2021.