Corrosion Management ISSN: 1355-5243
(https://corrosion-management.com/)
Volume 29, Issue 01–June 2019
SCOPUS

QUANTUM-RESISTANT AI ALGORITHM FOR CLOUD SECURITY

1st Rahul Vadisetty Electrical Engineering,)

Wayne State University) Detroit, MI, USA rahulvy91@gmail.com

Abstract:

Quantum quantum-resistant computer is a device used to solve complex problems by implementing rules of quantum mechanics. They are capable of solving complex issues before wasting any time. Quantum computers use quantum bits or qubits to store information. To extract information n qubits of quantum computers internally represent the entire span of n-bit numbers and perform calculations on all of them. For many problems, quantum algorithms are used to increase runtime complexity to speed up as compared to classical equipment. Shor's algorithm is a quantum-resistant algorithm that is used for integer factoring along with a runtime complexity.Quantum-resistant computers are beneficial for cloud security as they solve complex problems faster than other computers. AI algorithms can collect and analyze large amounts of data to detect threats which is beneficial for cloud security.

Key terms: Quantum resistant computer, AI Algorithm, Cloud Security, Computer, Techniques

1. Introduction:

A. Background:

Quantum resistant computer is a device that uses the rules of quantum mechanics to solve complex problems more efficiently. They can solve complex problems before wasting any time. They provide us with solutions to complex problems faster than other computers. Quantum computers use quantum bits or qubits to store information. Qubits are made by the spinning of an electron or proton. In recent two decades, qubits have been executed in a diversity of materials like atoms, liquids, semiconductors, and superconductors. Diamond Nitrogen-Vacancy Center has appeared as a main qubit candidate as it can be manipulated and measured with high fidelity at room temperature [1].

The system is measured by disintegrating the superposition to one basis state to extract information about the quantum computing state. To extract information n qubits of quantum computers internally represent the entire span of n-bit numbers and perform calculations on all of them but during the process of measuring state will subside to just one basis state and return only one result to the performed calculation. For these types of problems, quantum algorithms are used to expand basis states and probability for the basic structure of the problem. The obtained result will be repeatable and conclusive. For many issues, quantum algorithms are used to enhance runtime complexity to speed up in comparison to classical equipment. A system security position monitor called the Security Evolution Algorithm dynamically adjusts security measures according to the system's requirements and the state of the threat landscape. For optimal protection, it modifies security settings by applying reinforcement learning techniques and feedback loops.

Shor's algorithm is a quantum-resistant algorithm that is used for integer factoring along with a runtime complexity of $O((\log N)^2(\log\log N)(\log\log\log N))$. Shor's algorithm is considered a faster algorithm than all other algorithms. The problem of integer factorization is also reduced by finding the period of $f(x)=ax \bmod N$ where a is represented as a random integer and N is a factorized number. In Shor's algorithm, each basis state is created by connecting x with the value of f(x). When the f(x) is measured the superposition subsides by leaving one value v on the qubit while the qubits will be in a superposition of different x's with f(x)=v [2]. The use of artificial intelligence (AI) in cybersecurity is expanding due to the effectiveness of machine learning algorithms in identifying and removing threats. Two AI-driven security technologies that potentially enhance threat detection and response in cloud environments are deep learning and reinforcement learning.

B. Problem Statement:

Quantum-resistant computers are beneficial as they solve complex problems faster than other computers. Quantum-resistant computers allow us to solve complex problems but they also create problems for the existing cloud security infrastructure. Cryptography is the most essential support of cloud security. Cryptography refers to techniques derived from mathematical

concepts for the security of information and quantum-resistant computers can break all classical computer's cryptography which puts the cloud security of the international community at risk. The major problem is that the quantum-resistant computers in less than ten years could be advanced enough to endanger existing cryptography [3]. This report describes two possible solutions for above discussed problems:

Post-quantum resistant cryptography is standard code built on mathematical problems that can help us to withstand a quantum attack. Post-quantum resistant cryptography has the benefit that it works with existing classical software and hardware but its capability to withstand quantum attack depends on the imaginary mathematical hardness of the problem which can be difficult to anticipate. The quantum key distribution uses quantum channels to send or receive bits of details. Quantum key distribution can send details between short intervals and there is no need for mathematical suppositions of the firmness of the problem.

Organizations face several problems for cloud security due to existing technology of quantum-resistant AI Algorithms because quantum-resistant algorithms demand more resources as compared to traditional code techniques. Quantum-resistant AI Algorithms lead organizations to increased clarifying time and it also causes higher costs for suppliers and users of cloud service. The major challenge while using quantum-resistant AI algorithms is to balance the need for security with the logical use of resources. Techniques and solutions for using quantum-resistant AI Algorithms for cloud security are discussed in the next article [4].

C. Research Questions:

The research answers the following questions:

- How quantum-resistant AI algorithms are useful for cloud security?
- In what way does this technique contribute to cloud security?
- Quantum-resistant AI algorithms are useful but how do they manage to integrate in the context of cloud security?

Answers to these questions assist the researcher in analyzing existing trends related to Quantum-resistant AI algorithms and their applications in the real world. The research will identify the pros and cons of current developing strategies related to quantum-resistant AI algorithms and provide effective solutions to reduce the flaws of current trends to make the technology useful and effective.

D. Objectives:

The main objectives of the research are:

- Discuss the quantum-resistant AI algorithms for cloud security.
- It discusses the usefulness of quantum-resistant AI Algorithms for cloud security.
- It also discusses the recommendations for the effective usage of quantum-resistant AI algorithms in cloud security.

The objectives of the research are to command the quantum-resistant AI algorithms for cloud security. These objectives are orientated to present the existing techniques of quantum-resistant AI algorithms [5]. It also evaluates the applicability of these approaches in a cloud security context. The objectives roam on improving the framework of quantum-resistant AI algorithms for cloud security by examining previous studies.

E. Contribution of the study:

The research is critical for several reasons:

I. **Privacy issues:** Privacy is the major concern of the research that's why it covers several privacy considerations in the context of cloud security.

II. **Knowledge contribution:** Insights from previous studies gain the knowledge of the research in the context of quantum-resistant AI algorithms for cloud security.

III. **Security improvement:** Findings and results of the study enable the researcher to provide effective improved techniques for quantum-resistant AI algorithms for cloud security that can be used by industries, healthcare, finance, and government. The contribution of the study relies on improving the previous studies to make quantum-resistant AI algorithms more

secure for cloud security. The study involves various techniques to analyze the usefulness of quantum-resistant AI algorithms in a cloud security context. This will help to generate better and more efficient quantum-resistant AI algorithms for cloud security shortly.

F. Structure of the paper:

Chapter 2: Literature review provides valuable insights into the existing quantum-resistant AI algorithms for cloud security.

Chapter 3: Methodology- This chapter evaluates the methods and approaches for the existing techniques of quantum-resistant AI algorithms in a cloud security context.

Chapter 4: Result and Discussion includes an analysis of the findings and their implications.

Chapter 5: Conclusion and future work- This chapter includes a summary of the whole research, and what are its main contributions and future directions.

II. Literature Review:

1. 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 Resistant Barriers:

There are three types of quantum resistant machines which are quantum annealer which refers to D-wave systems. Quantum annealers do not exploit the qubits which means that they can do calculations with more than one thousand qubits and in this way, quantum annealers are used to solve complex problems. Quantum emulator is the second type which is related to analog systems. Quantum emulators study the quantum systems which are tough to study in the laboratory. Quantum emulators are used to identify insights about complex problems. Universal quantum computers can run different types of algorithms and identify patterns in data [6]. Quantum-resistant computers use different Quantum techniques to perform computations.

Quantum-resistant computers have different models but the Quantum circuit is the most common model of computation [7].

Quantum circuit model uses Quantum gates to transform the input qubit. Hadamard, CNOT(CX), and THE NOT(X) are the most used gates of Quantum computers. Quantum-resistant computers are more innovative than classical computers due to some barriers that prevent them from fully developing [8]. Quantum-resistant computers are stochastic machines, which means that they will provide accurate solutions with 100 possibilities in a single try-out but higher accuracy will be achieved after doing various try-outs of the same issue which reduces the speed of quantum-resistant computers. The environmental factor is the main barrier to the development of quantum-resistant computers because qubits can change by heat, and noise and to prevent their change qubits need to be isolated or placed at zero temperature. But when qubits are fully isolated they are difficult to control without involving the environment and noise. Errors that torture regular bits, and qubits are capable of changes in data like phase error which means that it can falsely flip the superposition cue and lead to errors in measurement.

B. AI Algorithms and Techniques for securing the cloud:

Data processing and data storage technologies have achieved great success in recent years. The success of these tech organizations in storage techniques has sanctioned a different computing model which is known as cloud computing. Artificial intelligence algorithms enable more accurate cloud system threats. AI algorithms can collect and analyze large amounts of data to detect the threat which is beneficial for cloud security. Algorithms collect information from dark web forums, and malware code to detect future attacks which can target the cloud environment. AI provides encryption techniques that are complex and difficult to crack for cloud security. Algorithms can easily manage encryption to ensure security and performance. AI algorithms protect cloud systems from threats and in the future, they will also be used to protect quantum computing attacks which will give a huge benefit to organizations [9].

AI algorithms can detect datasets, anomalies, and potential threats in very little time. By creating a baseline of normal behavior, AI systems can easily analyze anomalies or any changes in

network activities. It is very beneficial to identify the insider threat. AI algorithms can automate incident response which helps to respond to security incidents more rapidly [10]. As the data is transferred through the classical network and stored in the same server for many users it causes development in venomous programs and cloud security becomes an important problem. Hackers use different techniques to hack cloud systems. The following are the solutions for cloud security. The use of public key infrastructure is one of the solutions to prevent cloud security. Public key infrastructure interchange keys by using certificates through public channels for validation purposes. Public key infrastructure-built architecture works on Public key cryptography. Public key cryptography creates only computational security and by using Shor's algorithm with quantum-resistant computers it will be easy to crack the algorithms of public key cryptography but the public key infrastructure is very multiplex which is difficult to use [11]. Kerberos is another technique used for cloud security. Using Kerberos has many advantages as it allows the junctions to connect ends of different cloud networks. As compared to public key infrastructure Kerberos is easy to use and it allows the chances of Single Sign On.

C. Threats and solutions of Cloud security:

Cloud computing is gaining more attention because of the connection between the market and technology. The computing infrastructure of many organizations is changing due to rapid changes in business conditions. With the changing conditions of business new enterprise services are increasing and old enterprise services are being removed. Many financial companies are attracted to cloud computing but due to security reasons, they are not ready to adopt it properly. Cloud data security is the major issue as in 2014, accounts of 50 million users of Dropbox were hacked. It is very important to provide the same level of security as IT systems to see cloud computing as a workable option [12].

Cloud computing depends on virtualization and network infrastructure to work. Different technologies like Service-oriented architecture, and web services are used to give users access to their cloud resources. Anyone can access data from the cloud anywhere at any time which is easy for hackers to access and use other person's data without their consent. Data stealing and data

loss are the major problems in cloud computing. To resolve these issues cloud computing service providers have to ensure that user personal information should be well secured and that the data stored in cloud systems should remain confidential it should not be disclosed to unauthorized entities [13].

Summary:

This chapter offers a detailed explanation of the core concepts of quantum-resistant AI algorithms for cloud security from existing studies. It also includes the benefits and weaknesses of quantum-resistant AI algorithms in the context of cloud security. Analyzation of weakness provides effective strategies to overcome the weakness from the technique. This will enhance the productivity of quantum-resistant AI algorithms in a cloud security context.

III. Methodology

1. Introduction:

This chapter provides the methods and approaches used in the research to analyze the effectiveness and efficiency of quantum-resistant AI algorithms in a cloud security context. It highlights the ways through which data is collected and also mentions the techniques to analyze the reliability and validity of collected data. The methodology chapter also describes some ethical considerations that are essential to consider while collecting data. It strictly interprets that ethical norms should not be violated in the collection of data. It also demonstrates that if the study conducts useful methods and techniques then it will become beneficial for researchers to derive more accurate and useful quantum-resistant AI algorithms techniques.

2. Research design:

Research design is an approach that rules on research questions. This chapter uses mixed methodology by using both qualitative and quantitative methods for the research. Both these methods provide an effective outlook on the quantum-resistant AI algorithms in the cloud security context

A. Qualitative Method:

The study conducts qualitative data from various journals and online sources. It also conducts data from existing literature that helps to determine the existing studies related to quantum-resistant AI algorithms in a cloud security context [14]. A large number of existing studies were analyzed to gain comprehensive knowledge about the topic. Administrating questionnaires from professionals assists the researcher in gaining valuable insights from questionnaires.

B. Quantitative Method:

Experimental setup is arranged to analyze the quantitative data of the research which is also known as experimentalism. The experimental setup helps to examine the precision and validity of the techniques that assist in improving the quantum-resistant AI algorithms techniques for cloud security [15]. Therefore, the experimental setup of quantitative analysis provides rational methods and more effective ways in the field of quantum-resistant AI algorithms in a cloud security context.

3. Data collection method:

The gathering of data is a difficult process of the research. Data collection is the most essential part of the research. Primary and secondary sources are used to collect the data.

A. Literature review

The research gathered data from previous literature reviews that assist the researcher in enhancing an effective understanding of quantum-resistant AI algorithms for cloud security. The sources of the research are collected from academic journals, peer reviews, and research papers [16]. In the data collection, white papers and company reports became helpful and are used to evaluate the measures and current trends of quantum-resistant AI algorithms for cloud security.

B. Expert interviews

The research also conducts expert interviews to gain an effective understanding of the topic. Experts from the field of quantum-resistant AI algorithms are interviewed for valuable insights.

These interviews enable the researcher to identify the strengths of the quantum-resistant AI algorithms in a cloud security context [17].

C. Experimental data:

Data was also collected from statistical insights to attain numeric values of the data. Statistical analysis helps the researcher to thoroughly study the data.

4. Data analysis techniques:

Data analysis techniques involve the assessment and analysis of collected data. The data analysis technique is useful as it helps to interpret the reliability and validity of the data.

A. Qualitative data analysis:

Qualitative data was collected from existing literature, related journals, and peer reviews. For the analysis of qualitative data thematic analysis is used in the research. It provides various themes related to the research that helps to understand the credibility and reliability of the topic. Thematic analysis is very important in qualitative data analysis. Thematic analysis helps to analyze the patterns of data for effective recommendations. Narrative analysis also gains considerable importance in the research as it helps to narrate the numerical and statistical analysis in a narration form. Narrative analysis assists the research in properly narrating the data for readers' understanding [18].

B. Quantitative data analysis:

Quantitative data analysis is also important to analyze the experimental setup of the research. Quantitative analysis provides accuracy and clarity of the statistical data. Graphs and charts are used to analyze the quantitative data of experimental and statistics [19]. Furthermore, statistical analysis provides wise conclusions from data that help to make productive results of the chapter.

5. Experimental Setup:

Experimental setup used in the research as quantitative data. It covers various specifications like applications of quantum-resistant AI algorithms for cloud security and identification of effective

techniques like quantum-resistant AI algorithms technologies for cloud security. This will assist the research to effectively derive useful results for the research.

6. Evaluation metrics:

The effectiveness of quantum-resistant AI algorithms is influenced by some factors:

a) **Accuracy:** Accuracy is an important component as it aims at analyzing the proper forecasting of future trends. Higher accuracy means fewer mistakes which means that the higher the accuracy of the data higher the productiveness of the results.

b) **Efficiency**: Efficiency boosts the process of data collection and analysis. Efficiency refers in term of memory and time in this research. Less time consumption helps the researcher to complete the research on time. It also states that every collected source will be utilized properly to achieve the outcomes of the research.

c) **Scalability:** It is used to analyze the relation between collected data and required storage. Scalability is used for the resolution of problems in the research to smooth the operations.

d) **Privacy preservation**: Privacy feature is the main concern of the research. It determines that loss of information and data leakage should be minimized in AI and machine learning technologies for effective cyber threat detection.

e) Reliability and validity: Reliability and validity are also the major concerns of the research. For this concern, tests are conducted multiple times and if they generate the same value every time, this indication shows that they are reliable and valid [20].

f) Confusion Matrix: The confusion matrix provides more information about the accuracy of each class of data. It helps in determining the degree of correctness of the classification accomplished by various digits in the model. The study effectively demonstrates AI and machine learning in cyber threat detection. The results of the confusion matrix and ROC curves AI and machine learning in cyber threat detection. During the experiment, the accuracy and efficiency of the model were significantly high. Data protection can process huge amounts of data faster than data quality and analyze the detection of cyber threats. Additionally, they can detect vulnerabilities and predict threats with unprecedented accuracy. The graph as shown below in Fig 1 interprets that there is a visual

representation of the frequency of the correct and incorrect prediction by the model's performance. The confusion matrix is divided into two matrixs having high frequencies and low frequencies. Black shows the low frequency and blue shows the high frequency. It can be seen in Figure 1 that the gradient color scheme goes from low-frequency black to high-frequency blue.

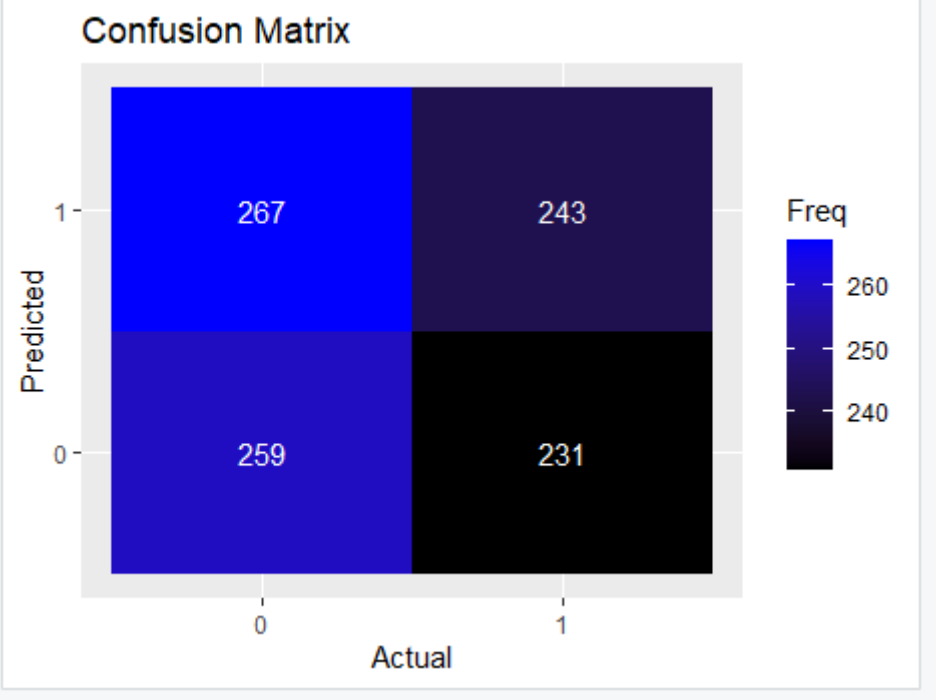

Figure 1. Confusion Matrix

***g). ROC Curve*:** The ROC Curve expresses the tradeoff between the true positive rate or sensitivity and the false positive rate or 1 specificity in terms of each class using ROC curves. This coefficient is suitable for comparing the results that the given model produced and here the predictive classification that has occurred is restricted only to two categories specificity and *sensitivity*. The ROC curve presented in Figure 2 shows the actual positive rate between cloud security systems of the quantum resistance in Artificial intelligence. The true positive rate is plotted as a function of the false positive rate for different cut-off points. A test with perfect discrimination has a ROC curve that passes through the upper left corner; the closer the ROC

curve is to the upper left corner, the higher the overall accuracy of the test. The ROC Curve as shown in the following Fig 2, shows the relationship between sensitivity and specificity. The curve as shown in the figure is plotted in blue which shows the model's performance in the Area Under the Curve. The value 0.5 suggests that the Area under the Curve assesses the performance of the model.

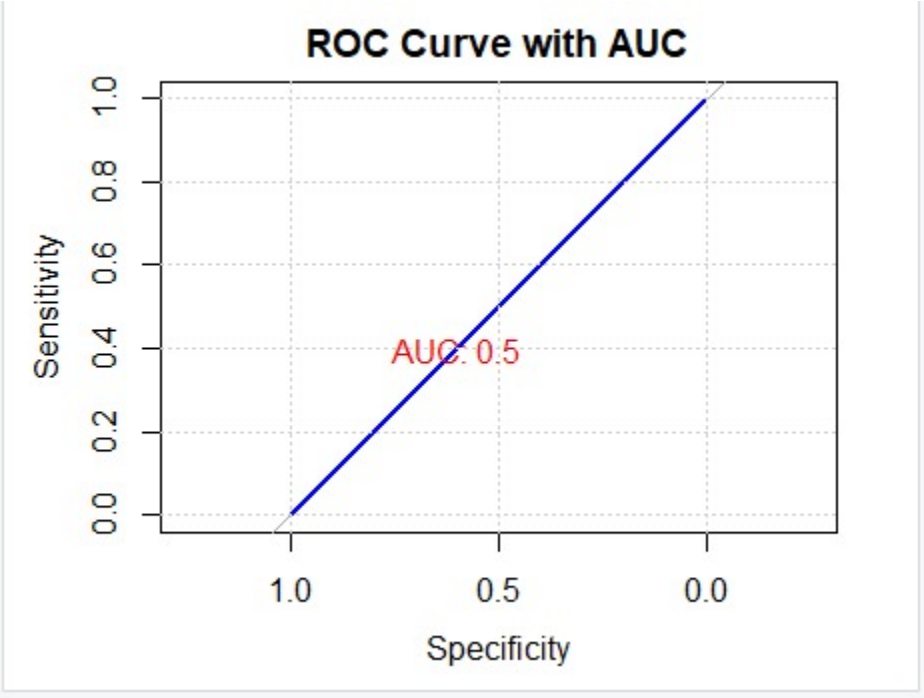

Figure 2. ROC Curve.

7. Summary:

The benefits and drawbacks of various cloud security frameworks were ascertained by a thorough examination of current technology. The graph makes it simple to evaluate the primary benefits and drawbacks of each framework by providing a clear and straightforward image of each one's relative efficacy. The data's visual representation is especially useful for pointing out areas that require more study and improvement as well as trends and patterns in the benefits and

drawbacks of different frameworks. Weighing the advantages and disadvantages of different cloud security frameworks.

8. Ethical considerations:

A. Data privacy: Data privacy is the major concern in the research. Proper storage of data is necessary to avoid data breaches. Collected data will only be used for information purposes. It will not include any ethical concerns [21].

B. Proper citation: The research conducts qualitative data from previous studies. Proper citation is necessary to give credit to the authors of previous studies. This will help the researcher to avoid any conflicts and mishaps in the completion of the research.

C. Informed consent: Informed consent is necessary for the participants of expert interviews. They will inform about the aims and goals of the research and where their information is going to be utilized. This assisted the research in fully engaging the participants in the research and made them aware of the use of data [22].

D. Conflict: The researcher should avoid those factors that can create conflicts in the research. Research obtained from the existing literature will be done smoothly and efficiently to achieve productive outcomes. The study will be conducted effectively by considering the factors to avoid conflicts in the research [23].

E. Consent: Participants are voluntary and free to respond to the study at any time without any hurry or obstacles. Participants were informed that their privacy would not be harmed. The participants were first fully informed of the information and data that was provided.

F. Free: Another important ethical consideration was that the participants who were involved in the survey were free to respond. The people who participated in the survey were not pressured and restricted.

G. Credit: In this paper, proper citation is given to give credit to the authors. Proper citation is necessary to avoid any ethical issues in the completion of the research. Proper information regarding previous authors assists the researcher in effectively conducting the research.

IV. Results and discussion:

1. Introduction:

In the chapter, the author assesses the aims that the researcher tends to find. In this chapter, it was highlighted what has been done, how it is done, and how it is useful in the future. It demonstrates the efforts used in the research for validation of the data. This chapter contains the results of the findings conducted in the article. It provides valuable insights to describe what the study has achieved in this article. 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 quantum-resistant AI algorithms for cloud security [24].

i. Data processing

The type of data used in the research is taken from the Kaggle dataset. In the Kaggle dataset, the data obtained is interpreted in the ROC curve graph and confusion matrix. The data set obtained from the data processing data will be further categorized into training and test data. This data set will help to perfectly evaluate the performance of the findings of resistance of quantum AI algorithm for cloud security.

ii. **Data set description:**

The research used data for the analysis is the Kaggle dataset which is a classic dataset in quantum-resistant AI algorithms for cloud security. The Kaggle dataset contains extensive material related to artificial intelligence for cloud security of quantum resistance. This dataset centers on various components to study the cloud security system of the quantum resistance in Artificial intelligence. The data set has been taken by Kaggle and then there is a description stated in the graphs of the ROC curve graph and confusion matrix as shown in figs and these graphs are interpreted.

iii. Data normalization:

The normalization step is crucial because it scales and arranges all the values of the article. In the research, the normalization of data is one of the crucial steps before processing collected data from the database. The range is used to manage the measurement of variables on different scales within the Kaggle dataset.

iv. Standardization:

All the steps used in the model of the Kaggle dataset, are for the accuracy and consistency of the research. This method enhances the convergence of the model and makes it faster than before.

2. Results

The research focuses on the level of accuracy of the model which is used to test the model that was the Kaggle dataset model. The test results show a quantum-resistant AI algorithm for cloud security. It can be seen that preparation and testing accuracy directly affect the effectiveness of the model. This reflects how quantum-resistant AI algorithms for cloud security. The results also show that the limitations of the model warrant expectations for the dataset used in the review.

3. Discussion:

The results help the author to evaluate quantum-resistant AI algorithms for cloud security. These results also support the author to solve problems like privacy and security by using the results. The results achieved with accurate formation enable the author to complete the research regarding cloud security reliably and validly.

V. Conclusion and Future work:

A. Conclusion:

The article is useful in understanding the current strategies and techniques of quantum-resistant AI algorithms for cloud security. It also provides methodological insights for quantum-resistant

AI algorithms for cloud security. The research describes that results conduct useful information that can be used by Organizations for effective implications of quantum-resistant AI algorithms for cloud security. It uses mixed methodology and analyzes the data through thematic and statistical analysis. The Kagel dataset was adopted for experiments that help to make graphs and charts. Therefore, the research is useful for useful implication of quantum-resistant AI algorithms in a cloud security context. In conclusion, the unparalleled difficulties that quantum computing presents for conventional encryption techniques necessitate the creation and application of quantum encryption algorithms. Quantum-resistant encryption is becoming more and more important for protecting sensitive data as organizations and governments get ready for the age of quantum computing. Case studies that demonstrate how quantum cryptography solutions are integrated offer important insights into the advantages and practical difficulties of the shift to quantum-resistant encryption. Moreover, quantum methods streamline AI procedures, facilitating quicker anomaly identification and stronger encryption. In an increasingly digital world, this combination offers strong resistance against sophisticated cyberattacks while guaranteeing data integrity and security.

B. Future work:

The research was conducted to examine the role of quantum-resistant AI algorithms in a cloud security context. The research conducts mixed methodology that is useful to derive effective results. In the future, the researcher can conduct more than one model to derive more accurate results for the research. Test results should be conducted more than one time to analyze the same value of the result every time. This helps the researcher to examine the effective nature of the collected data. It has also been observed that the research doesn't use any real-world data for detailed interpretation and explanation. In future work, more detailed and comprehensive information will assist the researcher in generating more accurate and clear results for quantum-resistant AI algorithms in a cloud security context. Further research will focus on enhancing quantum encryption, extending its use to domains such as the Internet of Things, and addressing secure communication aspects specific to humans. Quantum-cybersecurity systems must take into account ethical and legal considerations to ensure equitable access and compliance.

Bibliography

[1] J. R. Weber, W. F. Koehl, J. B. Varley, and D. D. Awschalom, "Quantum computing with defects," *PNAS*, 19 April 2010.

[2] I. Stewart, D. Ilie, A. Zamyatin, S. Werner, M. F. Torshizi and W. J. Knottenbelt, "Committing to quantum resistance: a slow defense for Bitcoin against a fast quantum computing attack," *ROYAL SOCIETY OPEN SCIENCE*, vol. 5, no. 6, 20 June 2018.

[3] S. Shoja, "A Quantum Future: Preparing Canada for the Potential Impacts of Quantum Computing," Toronto, Ontario, Canada, 2017.

[4] S. G. Gohwong, "The State of the Art of Cryptocurrencies," *Asian Administration & Management Review*, vol. 1, no. 2, p. 16, 2018.

[5] M. Farik and S. Ali, "The need for quantum-resistant cryptography in classical computers," *Academic edu*, vol. 5, no. 16, pp. 98-105, 2016.

[6] D. A. Herman and I. Friedson, "Quantum Computing: How to Address the National Security Risk," Hudson Institute, Washington, 2018.

[7] E. Cohen and B. Tamir, "D-Wave and predecessors: From simulated to quantum annealing," *International Journal of Quantum Information*, vol. 12, no. 3, 2014.

[8] Z. Kirsch, "Quantum Computing: The Risk to Existing Encryption Methods," *Computer Science 116*, vol. 116, p. 15, 15 December 2015.

[9] I. Stoica, D. Song, R. A. Popa, D. Patterson, M. W. Mahoney, R. Katz, A. D. Joseph, M. Jordan, J. M. Hellerstein, J. E. Gonzalez, K. Goldberg, A. Ghodsi, D. Culler and P. Abbeel, "A Berkeley View of Systems Challenges for AI," *arXiv*, 2017.

[10] N. Wirkuttis and H. Klein, "Artificial Intelligence in Cybersecurity," *Artificial_Intelligence_in_Cybersecurity-libre.pdf*, vol. 1, January 2017.

[11] M. Pandya, "Securing Cloud - The Quantum Way," *arXiv*, 7 December 2015.

[12] L. Coppolino, S. D'Antanio, G. Mazzeo and L. Ramano, "Cloud security: Emerging threats and current solutions," *Computers & Electrical Engineering*, vol. 59, pp. 126-140, 2017.

[13] S. Sridhar and Dr.S.Smys, "A Survey on Cloud Security Issues and Challenges with Possible Measures," *International Conference on Inventive Research in Engineering and Technology*, 2016.

[14] F. Rowe, "What literature review is not: diversity, boundaries, and recommendations," *Tandfo*, vol. 23, no. 3, pp. 241-255, 2014.

[15] V. L. Smith, "Theory and experiment: What are the questions?," *Science Direct*, vol. 73, no. 1, pp. 3-15, 2010.

[16] A. S. Denney and R. Tewksbury, "How to write a literature review," *Tandfo*, vol. 24, no. 2, pp. 218-234, 2013.

[17] B. Littig and F. Pöchhacker, "Socio-translational collaboration in qualitative inquiry: The case of expert interviews," *SAGE Publications*, vol. 20, no. 9, pp. 1085-1095, 2014.

[18] B. Smith, "Narrative analysis," *Academic edu*, vol. 2, pp. 202-221, 2016.

[19] L. Ferres, G. Lindgaard, L. Sumegi and B. Tsuji, "Evaluating a tool for improving accessibility to charts and graphs," *Swinburne Research Bank*, vol. 20, no. 5, pp. 1-32, 2013.

[20] R. Heale and A. Twycross, "Validity and reliability in quantitative studies," *Cross Mark*, vol. 18, no. 3, pp. 66-67, 2015.

[21] A. Mehmood, I. Natgunanathan, G. H. Yong Xiang and S. Guo, "Protection of big data privacy," *IEEE Explore*, vol. 4, pp. 1821-1834, 2016.

[22] A. M. Sobočan, T. Bertotti and K. Strom-Gottfried, "Ethical considerations in social work research," *European Journal of Social Work*, vol. 22, no. 5, pp. 805-818, 2018.

[23] J. Flaming and K. E.Zegwaard, "Methodologies, methods, and ethical considerations for conducting research in work-integrated learning," *Research Gate*, vol. 19, no. 3, pp. 205-213, 2018.

[24] B. Arslan, M. Ulker, S. Akleylek, and S. Sagiroglu, "A study on the use of quantum computers, risk assessment, and security problems," *IEEE Xplore*, 2018.