Privacy-preserving quantum machine learning using differential privacy

Makhamisa Senekane[1], Mhlambululi Mafu[2] and Benedict Molibeli Taele[3]

***Abstract*— The advance of artificial intelligence in general and machine learning in particular has resulted in the need to pay more attention to the provision of privacy to the data being anlyzed. An example of sensitive data analysis might be in the analysis of individuals' medical records. In such a case, there might be a need to draw insights from data while at the same time maintaining privacy of the participants. Such cases have given birth to privacy-preserving data analyitics. Privacy is typically guaranteed by a differentially private mechanism. In this paper, we present a novel mechanism for privacy-preserving quantum machine learning. The mechanism is tested on the sensitive dataset that contains features and target labels for breast cancer prediction. The results obtained underline the utility of this mechanism.**

I. INTRODUCTION

Artificial intelligence is concerned with the ability of computing machines to perceive, reason and act; just like humans and other animals [1], [2], [3]. The field of artificial intelligence can be divided into different subfields, namely; expert systems, optimization, robotics, machine learning and natural language processing.

Machine learning is the subfield of artificial intelligence which is focused on the use of data to improve performance of an algorithm based on the previous experience (data) [2], [4], [5]. A key benefit of machine learning as opposed to a static program is that it (machine learning) is capable of efficiently making data-driven predictions. Machine learning can be deployed in applications such as spam filtering, customer segmentation, fraud detection, drug discovery, and bioinformatics.

Typically, machine learning algorithms are implemented on conventional (sometimes called classical) computers. However, modified versions of machine learning algorithms can still be implemented on quantum computers. The intersection of artificial intelligence and quantum computation is a field called quantum artificial intelligence, and quantum machine learning is a subfield of quantum artificial intelligence [6], [7], [8].

Data analytics involves the use of data in order to draw meaningful insights. In some case, that dataset that is to be analyzed can turn out to be very sensitive, thereby requiring the need to maintain privacy of the participants. In such cases, the need to mathematically guarantee security becomes profound. A mere anonymization of data would not be enough to guarantee security. A mechanism that is used to guarantee security in such cases is differential privacy [9], [10], [11]. When differential privacy is applied to machine learning algorithms, such resulting algorithms are called privacy-preserving machine learning algorithms [12].

In this paper, we introduce a privacy-preserving quantum machine learning mechanism for analysis of sensitive datasets on a quantum computer. The major contribution of our paper is in the application of differential privacy to quantum machine learning. The proposed mechanism is then applied to Wisconsin breast cancer dataset, in order to test the efficacy of the mechanism.

The remainder of this paper is structured as follows. The next section provides bacground information on machine learning and differential privacy. It is followed by Section III, which descibes a novel privacy-preserving quantum machine learning algorithm proposed in this paper. Section IV provides results and discussion of the results obtained. The last section concludes this paper.

II. BACKGROUND INFORMATION

A. Machine learning

Machine learning, which is also known as statistical learning, is the most successful subfield of artificial intelligence [5]. This is due to the fact that the application of machine learning is ubiquitous in almost every aspect of life. Machine learning involves the development of algorithms learn from past experience to make predictions.

Machine learnig can be broadly divided into two major categories. These categories are [4], [5]:

- Supervised learning: is used to generalize from known examples. The learning algorithm is provided with a pair of input attributes and outputs (targets). The role of the algorithm in such a case is to generalize what the output would be, given a certain input. Examples of supervised machine learning algorithms are naive Bayes, logistic regression, and artificial neural network.
- Unsupervised learning: unlike supervised learning, this category does not provide the algorithm with desired outputs; only inputs are provided. The task of the algorithm is to discover similarities in data inputs, and group data according to such similarities. Examples of unsupervised machine learning are clustering and dimensionality reduction.

Supervised machine learning is used to solve two classes of problems, namely regression and classification problems. A regression problem involves cases where target values are

[1]M. Senekane is with the Department of Physics and Electronics, National University of Lesotho, Roma, Lesotho Makhamisa12@gmail.com

[2]M. Mafu is with the Department of Physics and Astronomy, Botswana International University of Science and Technology, Palapye, Botswana mafum@biust.ac.bw

[3]B. M. Taele is with the Department of Physics and Electronics, National University of Lesotho, Roma, Lesotho bm.taele@nul.ls

978-1-5386-2775-4/17/$31.00 ©2017 IEEE

continuous. On the other hand, target values for classification problems are discrete.

B. Quantum Computation and Quantum Machine learning

A quantum computer uses makes use of quantum mechanical phenomena to increase performance of computation [13]. The unit of information for quantum computation is a qubit; which is analogous to a bit, which is used by conventional computers. However, unlike a bit, which exists in either one of two states, a qubit can exist in superposition of two states. A qubit is mathematically represented as [13]

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

where α and β are probability amplitudes. These amplitudes satisfy the condition

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2}$$

Just like conventional computers, which realize computation through the use of logic gates, quantum computers also realize computation through the use of quantum gates. Quantum gates use unitary operators for transformations of qubits from one state to another.

Quantum machine learning makes use of quantum computers for predictive data analysis. It is pursued in two key directions. The first direction involves transformations of classical datasets into quantum states, for statistical learning on the quantum computers [7]. The second direction involves the collection and statistical analysis of quantum data. In this approach, even the data collected is already a quantum data. The approach taken in this paper is the former, since classical dataset is used. Classical data is converted to quantum state such that for an instance $\overrightarrow{x_i}$ and number of instances N in the dataset [8]:

$$|\overrightarrow{x_i}\rangle = \frac{1}{|\overrightarrow{x_i}|}\sum_{j=1}^{N}(\overrightarrow{x_i})_j|j\rangle. \tag{3}$$

C. Differential Privacy and Privacy-preserving Machine Learning

Differential privacy is a mathematically strong definition of security [9], [10], [11], [12]. It mimimizes the risk of an individual being identified when they participate in a statistical database. Differential privacy is therefore useful for quantifying and bounding privacy loss [11].

Definition 1. *A randomized function* K *gives an* ϵ*-differential privacy if for all datasets* D_1 *and* D_2 *differing in at most one element, and all* S $\subseteq$ *Range(*K*) [12],*

$$P[\mathrm{K}(D_1) \in \mathrm{S}] \leq exp(\epsilon) \times P[\mathrm{K}(D_2) \in \mathrm{S}], \tag{4}$$

where $\epsilon \ll 1$.

Definition 2. *A randomized function* K *gives an* (ϵ, δ)*-differential privacy if for all datasets* D_1 *and* D_2 *differing in at most one element, and all* S $\subseteq$ *Range(*K*) [12],*

$$P[\mathrm{K}(D_1) \in \mathrm{S}] \leq exp(\epsilon) \times P[\mathrm{K}(D_2) \in \mathrm{S}] + \delta, \tag{5}$$

where $\epsilon \ll 1$ *and* δ *is cryptographically small.*

The key objective of statistical learning is to discover insights from the dataset while on the other hand, the objective of differential privacy is to minimize privacy loss of participants of a statistical database. Privacy-preserving machine learning fuses together machine learning and differential privacy. It is useful in the cases where data being explored for predictive analytics is very sensitive, and there is a need to maintain privacy of the participants.

In order to realize privacy-preserving machine learning, noise perturbation can be added in three different ways, namely:

- Input perturbation: where the noise is added to input dataset, before data could be fed to the machine learning model. This noise pertubation is the one used in the work presented in this paper.
- Objective perturbation: where the noise is introduced to the objective function of a machine learning model.
- Output pertubation: where the noise is added to the output of machine learning model.

III. PRIVACY-PRESERVING QUANTUM MACHINE LEARNING ALGORITHM

The algorithm proposed in this paper involves the addition of discrete Laplace noise to the dataset, followed by the transformation of data from classical representation to quantum representation. Conversion of data from classical state to quantum state is done in accordance with Eq. 3. Lastly, quantum logistic machine learning algorithm is then applied in order to model the transformed dataset. Therefore, in order to guarantee security using differential privacy, the noise mechanism is added to the input side of the privacy-preserving quantum machine learning algorithm.

The proposed privacy-preserving quantum machine learning algorithm is implemented using Python programming language [14], version 2.7.13. Python was chosen mainly due to its prominence in data analytics. Additionally, Python has a variety of very rich libraries for data analysis, data visualization and machine learning. Machine learning library that was used is Scikit-learn [15], version 0.18.1. This library is very prominent in machine learning applications. However, in order to implement quantum machine learning using scikit-learn, some of the algorithms have to be modified in order to cater for the quantumness of the data being analyzed.

The dataset that was used for analysis of the privacy-preserving quantum machine learning language is breast cancer Wisnconsin dataset. The dataset comes pre-loaded with scikit-learn, and is used for classification. Alternatively, the dataset can be obtained as a separate comma-separated values (CSV) file. This dataset consists of 569 instances (rows) and 30 features (attributes). There is also one column for target labels, which classify whether the tumor is malignant or benign.

In order to apply quantum machine learning on the dataset discussed in the previous paragraph, such a dataset then transformed to the quantum representation, where quantum logistic machine learning is applied. Since there is a possibility to bias the machine learning model, portion of data

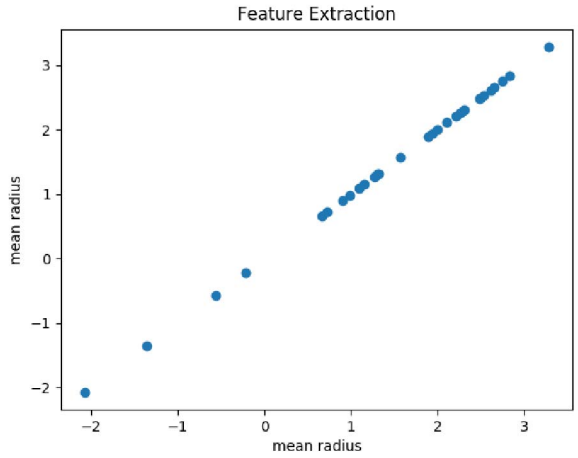

Fig. 1. A graph showing feature dependence of the dataset. Since the comparison is on the single feature, the graph is linear.

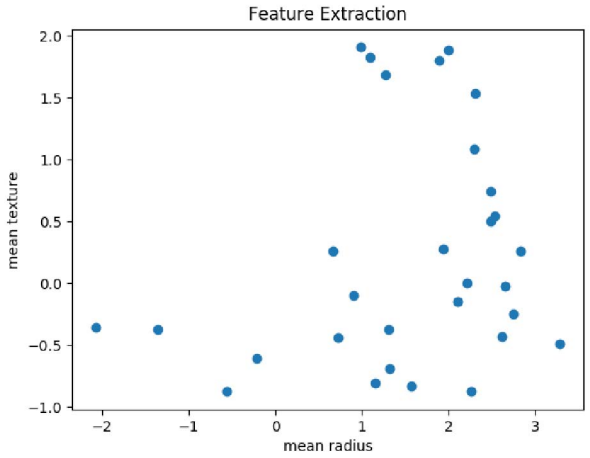

Fig. 2. A graph comparing dependence of **mean radius** and **mean texture** features. The non-linearity of the graph implies that the features are independent.

from the dataset (426 instances) is used to train the model, while the remaining portion (143 instances) is used to test the accuracy of the model. The results obtained are provided and discussed in the next section.

IV. RESULTS AND DISCUSSION

The first step after applying discrete Laplace noise was to preprocess the data to ensure that there is no dependence among features, so as to ensure that only informative features are used as predictors. In order to compare different features, feature scaling is required. Feature scaling ensures that all the features are normalized to be within the sam scale. After feature scaling, different features were compared to test for dependence. Feature dependence is demonstrated by feature graph with a linear curve, as shown in Fig. 1. On the other hand, feature independence is charactirized by a non-linear curve between the features, as shown in Fig. 2 and Fig. 3. All the features were found to be inndependent of one another, and hence they were all used as predictors, in order to improve the accuracy of the model.

After feature engineering step, data was split into training data both training data and test data. Training data was fitted to the model; in order to train it, while test data was used to test the accuracy of the model. The accuracy of the privacy-present quantum machine learning algorithm was found to be *98.6%*.

The detailed classification report is given in TABLE I. The table gives values for presicion, recall and F-1 score. All these metrics underline the utility of the privacy-preserving quantum machine learning proposed in this paper.

Finally, a confusion matrix of the mechanism was found to be

$$\begin{bmatrix} 52 & 2 \\ 0 & 89 \end{bmatrix}.$$

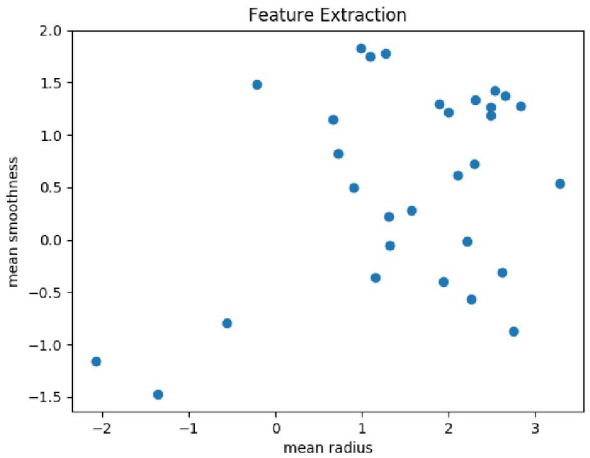

Fig. 3. A graph comparing dependence of **mean radius** and **mean smoothness** features. The non-linearity of the graph in this case also implies that the features are independent. This feature independence means that both features can be used as predictors.

V. CONCLUSION

We have demonstrated a novel privacy-preserving quantum logistic regression machine learning. This mechanism is then tested on the Wisconsin breast cancer dataset, which classifies whether the tumor is malignant or benign. The proposed mechanism uses discrete Laplace noise as a noise mechanism, and the noise perturbation takes place at the input. High performance of the mechanism is characterized by high accuracy, high precision, high recall, F-1 score close to unity, and confusion matrix with non-zero diagonals. This high performance underlines the utility of the privacy-preserving mechanism proposed in this paper.

Future work will focus on both objective and output noise perturbations. Additionally, different quantum machine learning algorithms will be explored in order to produce

TABLE I
CLASSIFICATION REPORT.

	Precision	Recall	F-1 Score	Support
malignant	1.00	0.96	0.98	54
benign	0.98	1.00	0.99	89
avg/total	0.99	0.99	0.99	143

more mechanisms for privacy-preserving quantum machine learning.

ACKNOWLEDGMENT

All the authors would like to thank their employers for affording them opportunity to work in this research endeavor. MS would like to thank the management and staff members at the National University of Lesotho, for their support. MM thanks his colleagues in the Department of Physics and Technology - Botswana International University of Science and Technology, for their motivation and stimulating academic engagements. BMT thanks all his colleagues in the Department of Physics and Electronics - National University of Lesotho, for their support. He particularly thanks his head of department for making funds and other resources available for this research.

REFERENCES

[1] P. H. winston, Artificial Intelligence, 3rd ed. New York: Addison-Wesley, 1992, ch. 1.
[2] S. Russell and P. Norvig, Artificial Intelligence - A Modern Approach. 3rd ed. New Jersey: Prentice Hall, 2010, ch. 1.
[3] D. Khemani, A First Course in Artificial Intelligence. New Delhi: McGraw-Hill, 2014, ch. 1.
[4] K. P. Murphy, Machine Learning - A Probabilistic Approach. Massachusetts: MIT Press, 2012.
[5] S. Marsland, Machine Learning - An Algorithmic Perspective. 2nd ed. Florida: CRC Press, 2015.
[6] A. Wichert, Principles of Quantum Artificial Intelligence. New Jersey: World Scientific, 2014.
[7] P. Wittek, Quantum Machine Learning - What Quantum Computing Means to Data Mining. Amsterdam: Elservier, 2014.
[8] M. Schuld, I. Sinayskiy and F. Petruccione, An Introduction to Quantum Machine Learning. Contemporary Physics, **56**, pp. 172-185, 2015.
[9] C. Dwork *et.al*, Our Data, Ourselves: Privacy via Distributed Noise Generation. EUROCRYPT 2006, LNCS 4004, pp. 486-503, 2006.
[10] C. Dwork and A. Smith, Differential Privacy for Statistics: What We Know and What We Want to Learn, Journal of Privacy and Confidentiality, **1**, Number 2, pp. 135-154, 2009.
[11] M. Senekane and F. Petruccione, A Mechanism for (ϵ, δ)-differential Privacy Using Student's t Distribution. IEEE Security & Privacy, submitted for publication, 2017.
[12] C. Dwork and A. Roth, The Algorithmic Foundations of Differential Privacy, Foundations and Trends in Theoretical Computer Science, Vol. 9, Nos. 3-4, pp. 211-407, 2014.
[13] I. Chuang and M. Nielsen, Quantum Computation and Quantum Information.10th Anniversary ed. Cambridge: Cambridge University Press, 2010.
[14] M. Lutz, Python Pocket Reference. 5th ed. California: O'Reilly Media, 2014.
[15] G. Hackeling, Mastering Machine Learning with Scikit-learn. Birmingham: Packt Publishing, 2014.