Jamie C Dance (PG/T – Computer Science)

URN: 6661320

MSc Dissertation

**The Relation between Neural Networks and Homomorphic Encryption**

A project supervised by Professor Liqun Chen



University of Surrey

Faculty of Engineering and Physical Sciences

# Abstract

# Acknowledgements

# Table of Contents

[Abstract 1](#_Toc80653469)

[Acknowledgements 2](#_Toc80653470)

[Table of Contents 3](#_Toc80653471)

[Part 1: START UP 5](#_Toc80653472)

[Chapter 1: 6](#_Toc80653473)

[1.1 Introduction 7](#_Toc80653474)

[1.2 Aims and Motivation 7](#_Toc80653475)

[1.3 Project Objectives 8](#_Toc80653476)

[1.4 Project Stakeholders? 8](#_Toc80653477)

[1.5 Project Scope and Context 8](#_Toc80653478)

[1.6 Resources and Resource Constraints 8](#_Toc80653479)

[1.7 Project Control and Risk Assessment 8](#_Toc80653480)

[1.8 Report Structure 9](#_Toc80653481)

[1.9 Measures of Project Success 9](#_Toc80653482)

[Chapter 2: Literature Review 10](#_Toc80653483)

[2.1 The Problem Background 11](#_Toc80653484)

[2.2 Recent Advances 11](#_Toc80653485)

[2.3 Related Work 12](#_Toc80653486)

[2.4 Summary of Part One 12](#_Toc80653487)

[References for Part One 13](#_Toc80653488)

[Part 2: Research 14](#_Toc80653489)

[Chapter 3: Research into Neural Networks and Homomorphic Encryption 15](#_Toc80653490)

[3.1 Research into Privacy-preserving neural networks with Homomorphic Encryption 16](#_Toc80653491)

[3.2 Homomorphic Encryption 16](#_Toc80653492)

[3.3 Fully Homomorphic Encryption 16](#_Toc80653493)

[3.4 Neural Networks 16](#_Toc80653494)

[3.5 Limitations 16](#_Toc80653495)

[3.6 Development Tools 16](#_Toc80653496)

[References for Part Two 16](#_Toc80653497)

[Part 3: Analysis, Design & Implementation 18](#_Toc80653498)

[Chapter 4: Analysis & Design 19](#_Toc80653499)

[4.1 20](#_Toc80653500)

[Chapter 5: Implementation 21](#_Toc80653501)

[References for Part Three 22](#_Toc80653502)

[PART 4: Closure 23](#_Toc80653503)

[Chapter 6: Evaluation & Testing 24](#_Toc80653504)

[6.1 25](#_Toc80653505)

[Chapter 7: Conclusion and future work 26](#_Toc80653506)

[7.1 27](#_Toc80653507)

[References for Part Four 28](#_Toc80653508)

# Part 1: START UP

Research

Analysis, Design & Implementation

* Introduction
* Literature Review

Start Up

* Research into Neural Networks & Homomorphic Encryption
* Analysis & Design
* Implementation

Closure

* Evaluation and Testing
* Conclusion and Future Work

## Chapter 1:

### 1.1 Introduction

We live in the age of algorithms, a term not so long ago that was surrounded by puzzlement. With the rise of Machine Learning they are in every nook and cranny of civilization. They’re not just a part of your cell phone, laptop or bank credit score, they are in your car, your house and even some of your fridges! Included within all that data can be very personal and sensitive data such as medical or financial data. So, in practice we have Data Scientists who are telling people to share their data to improve already existing mechanisms, whilst privacy experts are advising people to hide it or even delete it. This has led to the privacy dilemma: either sensitive user data must be revealed to the entity that evaluates the cognitive model (e.g, in the cloud), or the model itself must be revealed to the user so that the evaluation can take place locally REFERENCE - https://eprint.iacr.org/2017/1114.pdf. Applying machine learning to a problem that involves this data not only requires accurate predictions but also careful attention to maintaining data privacy and security.

This project will be focused on applying learned Neural Networks to encrypted data. This allows a data owner to send their data in an encrypted form to a cloud service that hosts the networks. The encryptions ensure the data remains confidential since the cloud does not have the means to decrypt it. Regardless, the cloud service will be capable of applying the neural networks to the encrypted data to make encrypted predictions that are then returned to the owner who can then decrypt them. That way the service provider does not gain any information about either the raw data or the predicted output.

The growing interest in Machine Learning As a Service (MLAS), where a marketplace of predictors is available on a pay-per-use basis, requires attention to the security and privacy of this model. Not all data types are sensitive but in certain areas such as medical, financial and marketing MLAS is becoming popular due to its versatility.

Neural networks are often built from pre-existing data. They are usually trained to solve a classification problem (definition of classification problem). In Neural Networks, non-linearities come from activation functions which are usually picked from a small set of non-linear functions of reference…

### 1.2 Aims and Motivation

As already mentioned in the previous section of this Chapter, this project aims to explore and potentially improve upon current existing methods of utilising neural networks upon encrypted data. The motivation for the project came from my desire to explore new modern methods of applying machine learning rather than researching older techniques I have previously conducted on past projects. Initially I wanted to investigate into a modern Machine Learning technique used with Big Data, but my Supervisor Professor Liqun Chen specialised in Cryptography and recommend looking into some link between Machine Learning and Cryptography. After some early research I discovered a new area of work involving using Neural Networks on Encrypted data by large organisations such as Microsoft and Amazon. Prof. Liqun Chen suggested I undertook this project and explore potential improvements and future work.

The **first aim** of this project is to research and explore some already existing methods of applying Neural Networks to Encrypted data that are available online such as Cryptonets, SageMaker and Discretized Neural Networks. This will help us build an understanding as to how developers are tackling this problem currently. In addition, it with provide us with some background that might help us to improve our own model in the future.

The **second aim** is to improve upon some these current concepts and try applying them to a new set of data of my choice. In our case the goal is to discuss the accuracy of these methods and identify the strengths and weaknesses associated with them. It is important to note that the methods explored may have different means of evaluation which could cause comparisons to be difficult.

The **third aim** is to…

### 1.3 Project Objectives

In the previous section we have discussed the motivations and the aims for the project. In this section we will list the objectives for this project:

1. Explore and understand some of the various elements within in the project such as Neural Networks, Encrypted data or more specifically homomorphic encrypted data.
2. Review Literature that is relevant to applying Neural Networks to encrypted data that already exist online.
3. Design, implement and test a new method of applying Neural Networks to encrypted data.
4. Evaluate the quality of the new implemented method.
5. Recommend improvements that can be made for the future.

### 1.4 Project Stakeholders?

The new methods implemented for the sake of this Project along with all its deliverables:

* Is the work of, and owned by Jamie Dance, student number 6661321. Jamie Dance is the Author of the Report and the developer of the new Applications of Neural Networks on Homomorphic Encrypted Data. Despite referencing throughout the project to a “We” this does not mean in any way that the Author had assistance or direct input by anyone other than himself or his supervisor.
* Is based on the work at…
* Is supervised by Professor Liqun Chen.

### 1.5 Project Scope and Context

In this section we will provide a better explanation of the overall scope of the project and we will discuss the importance of working with encrypted data.

Lots of work to do here.

### 1.6 Resources and Resource Constraints

TO BE COMPLETED AT THE END…

### 1.7 Project Control and Risk Assessment

In order to keep control over the project several measures were kept in place to ensure that the project was completed smoothly and successfully in time. Many separate documents that will not be included in this report were created and used to assist in the completion of the project such as a project plan, project schedule and project notes. In addition, when necessary these notes were shared with Professor Liqun Chen for approval.

Various threats and risks have been taken in consideration in order to ensure that the project is completed successfully. These threats are identified and outlined below:

* Very new topic, 2020/2021 so there isn’t a lot of content.

### 1.8 Report Structure

Inspiration for the structure of the report has been taken from one of the sample dissertations provided. The report was written by Marios Erodotou on the Automated detection and tracking of Mycobacterium Tuberculosis cells REFERENCE?. The structure of the report allows for a clear and pleasant way for the reader to navigate whilst simultaneously allowing the author to be aware of the current progress against the project schedule. Therefore, I have decided to also split the report into **four** different sections which each represented with a different theme. Within each section are a number of relevant chapters which have a number of subsections within that chapter. For example, the current section is located within “Chapter One: Introduction” which is within “Part One: Start Up”. I have decided to use a **colour** theme for Part One, thus any chapters or chapter subsections will follow this theme. For each section there will be a brief introduction to the chapters that will follow, and also a summary at the end to provide a brief conclusion that sums up everything important that was discussed within the section. For easier referencing I will also include an extra part at the end of each section that includes a list of corresponding references instead of one confusing block at the end of the report. A graphic will be included at the beginning of each section and will highlight the section and content that is to follow. Within each section of the graphic there is a summary of the significant chapters which allows to enhance the overall navigation and experience for the reader. The below graphic clearly illustrates the various sections and the lifecycle of this project:

Research

Analysis, Design & Implementation

* Introduction
* Literature Review

Start Up

* Research into Neural Networks & Homomorphic Encryption
* Analysis & Design
* Implementation

Closure

* Evaluation and Testing
* Conclusion and Future Work

The report contains a total of four sections and each section contains a number of chapters. Please find a brief description of each section below:

**Part One: Start Up.**

**Part Two: Research.**

**Part Three: Analysis, Design & Implementation.**

**Part Four: Closure.**

### 1.9 Measures of Project Success

## Chapter 2: Literature Review

### 2.1 The Problem Background

In this section, some insight will be given into some of the concepts included in this report in hopes of presenting a more detailed representation of what stage this current work is at and how it has developed over the years.

As mentioned in the Introduction, Machine Learning is a quickly developing and very powerful tool for people across the globe. But with growing success comes increasing issues and one of them issues is the topic of privacy and cybersecurity. Data scientists across the globe are encouraging people to share their sensitive material to create important developments into fields such as medicine although people aren’t prepared to share information that could be detrimental for themselves. Typically for one to analyse a set of data it is important to know the input, the output and the scope/aim of the data. That cannot be the case with encrypted data as it is not possible for the analyst to see the content of the data at all. By using homomorphic encryption, we can permit users to perform computations on encrypted data without decrypting it. Processing large amounts of encrypted data can be very difficult as the processing power needed to apply machine learning techniques is significantly higher.

### 2.2 Recent Advances

The combination of Neural Networks and more generally Machine learning with encrypted data is a modern-day concept.

In traditional cloud storage and computation solutions the cloud needs to have unencrypted access to the customers data to compute on it, necessarily exposing the data to the cloud operators. Customers need to trust the service provider to store and manage their data appropriately, e.g., not share it with third parties without the customers’ consent. As a result, data privacy relies on access control policies (such as an access control list) implemented by the cloud and trusted by the customer. With the advances in homomorphic encryption technology, it is possible to allow computations to be performed directly on encrypted data. In recent years, Fully Homomorphic Encryption development demonstrates remarkable progress. However, current literature in the homomorphic neural networks is almost exclusively addressed by practitioners looking for suitable implementations. It still lacks comprehensive and more thorough reviews. We will focus on the privacy-preserving homomorphic encryption cryptosystems targeted at neural networks identifying current solutions, open issues, challenges, opportunities, and potential research directions

The diagram below shows an example of a basic example of a traditional method of encryption (1) that requires the user to apply some function (addition in this example) to two numbers and then encrypt them. This is something that can be done with any encryption, but with Homomorphic Encryption you can go the other way around (2), you can first encrypt then apply some function. This can be done without knowing the value of or and without knowing the result. In this example we have used addition but the same can be done with multiplication and a multitude of functions.

add

add

encrypt

encrypt

1

2

### 2.3 Related Work

Homomorphic encryption schemes that are not

### 2.4 Summary of Part One

Part one has been constructed to serve as an informative introduction to the report that clearly lays out some of the initial key concepts of the report and creates a foundation to be developed upon further into the report. During this part we went through chapters One and Two which were composed of an introduction and a literature review. In the first chapter, an overview of the whole project was given that outlines all the key factors as to how the report was developed and what was intended to be provided to the reader by the author. This included the project’s aims, motivations, objectives and stakeholders. In addition, it listed the resources used and defined the measures of project success. In Chapter Two, a literature review was completed in which some initial conclusions were made as how to Neural Networks can be used with encrypted data. The conclusion was…

## References for Part One

# Part 2: Research

Research

Analysis, Design & Implementation

* Introduction
* Literature Review

Start Up

* Research into Neural Networks & Homomorphic Encryption
* Analysis & Design
* Implementation

Closure

* Evaluation and Testing
* Conclusion and Future Work

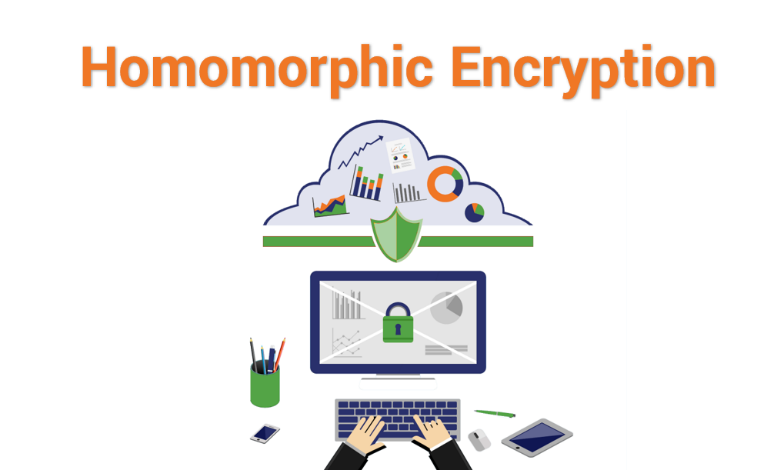
## Chapter 3: Research into Neural Networks and Homomorphic Encryption

### 3.1 Research into Privacy-preserving neural networks with Homomorphic Encryption

Modern encryption techniques ensure security and are considered as the best option to protect stored data and data in transit from an unauthorised third-party. However, a decryption process is necessary when the date must be processed and or analysed, falling into the initial problem of data vulnerability. Fully Homomorphic Encryption (FHE) is considered the holy grail of cryptography, an elusive goal that could solve cybersecurity problems [1-3]. Within this section we will discuss the fundamental concepts of Fully Homomorphic Encryption, practical implementations, state-of-the approaches, limitations, advantages, disadvantages, potential applications, and development tools focusing on neural networks.

Furthermore, this section is also meant to be used as a reference for the following chapters at the Design and Implementation phase of the project. This chapter is meant as more of a guidance or general explanation of some of the core concepts to avoid confusion and to allow the reader to have a grasp some of the algorithms used.

### 3.2 Homomorphic Encryption



### 3.3 Fully Homomorphic Encryption

### 3.4 Neural Networks

### 3.5 Limitations

### 3.6 Development Tools

## References for Part Two

1. Vaikuntanathan V (2011) Computing blindfolded: new developments in fully Homomorphic Encryption. In: 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science. Palm Springs, CA, pp 5–16. <https://doi.org/10.1109/FOCS.2011.98>
2. Gentry C (2009) A fully Homomorphic encryption scheme. In: Stanford University. Stanford, PhD Thesis
3. Gentry C, Halevi S (2011) Implementing gentry’s fully homomorphic encryption scheme. In: Paterson KG (ed) Advances in Cryptology – EUROCRYPT 2011. Lecture notes in computer science, vol 6632. Springer, Berlin, Heidelberg, pp 129–148. <https://doi.org/10.1007/978-3-642-20465-4_9>

Research on the 2/3 different developed methods (Microsoft, etc…)

# Part 3: Analysis, Design & Implementation

Research

Analysis, Design & Implementation

* Introduction
* Literature Review

Start Up

* Research into Neural Networks & Homomorphic Encryption
* Analysis & Design
* Implementation

Closure

* Evaluation and Testing
* Conclusion and Future Work

## Chapter 4: Analysis & Design

### 4.1

THIS IS WHERE MY PERSONAL IMPLEMENTATION ON A DATASET IS INCLUDED.

FOCUS IS ON THE METHODS NOT THE RESULTS.

TALK ABOUT PROGRAMMING LANGUAGE. USAGE/LIMITATIONS

<https://link.springer.com/content/pdf/10.1007/s12083-021-01076-8.pdf>

^ This has an example of an implementation but doesn’t provide the code.

## Chapter 5: Implementation

IMPLEMENTATION ON DATASET – TALK ABOUT THE WHOLE PROCESS, EVERY LITTLE THING

RESULTS ARE TALKED ABOUT IN THE NEXT SECTION

## References for Part Three

# Part 4: Closure

Research

Analysis, Design & Implementation

* Introduction
* Literature Review

Start Up

* Research into Neural Networks & Homomorphic Encryption
* Analysis & Design
* Implementation

Closure

* Evaluation and Testing
* Conclusion and Future Work

## Chapter 6: Evaluation & Testing

### 6.1

## Chapter 7: Conclusion and future work

### 7.1

## References for Part Four