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](#_Toc80640430)

[Acknowledgements 2](#_Toc80640431)

[Table of Contents 3](#_Toc80640432)

[Part 1: START UP 5](#_Toc80640433)

[Chapter 1: 6](#_Toc80640434)

[1.1 Introduction 7](#_Toc80640435)

[1.2 Aims and Motivation 7](#_Toc80640436)

[1.3 Project Objectives 7](#_Toc80640437)

[1.4 Project Stakeholders? 7](#_Toc80640438)

[1.5 Project Scope and Context 7](#_Toc80640439)

[1.6 Resources and Resource Constraints 7](#_Toc80640440)

[1.7 Project Control and Risk Assessment 7](#_Toc80640441)

[1.8 Report Structure 7](#_Toc80640442)

[1.9 Measures of Project Success 7](#_Toc80640443)

[Chapter 2: Literature Review 8](#_Toc80640444)

[2.1 The Problem Background 9](#_Toc80640445)

[2.2 Recent Advances 9](#_Toc80640446)

[2.3 Related Work 9](#_Toc80640447)

[2.4 Summary of Part One 9](#_Toc80640448)

[2.5 References for Part One 9](#_Toc80640449)

[Part 2 Research: 10](#_Toc80640450)

[Chapter 3: Research into Neural Networks and Homomorphic Encryption 11](#_Toc80640451)

[3.1 Research into Privacy-preserving neural networks with Homomorphic Encryption 12](#_Toc80640452)

[3.2 Neural Networks 12](#_Toc80640453)

[3.3 Homomorphic Encryption 12](#_Toc80640454)

[Part 3: Analysis, Design & Implementation 13](#_Toc80640455)

[Chapter 4: Analysis & Design 14](#_Toc80640456)

[4.1 15](#_Toc80640457)

[Chapter 5: Implementation 16](#_Toc80640458)

[PART 4: Closure 17](#_Toc80640459)

[Chapter 6: Evaluation & Testing 18](#_Toc80640460)

[6.1 19](#_Toc80640461)

[Chapter 7: Conclusion and future work 20](#_Toc80640462)

[Project References 21](#_Toc80640463)

# 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:

### Introduction

### 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

### 1.3 Project Objectives

### 1.4 Project Stakeholders?

### 1.5 Project Scope and Context

### 1.6 Resources and Resource Constraints

### 1.7 Project Control and Risk Assessment

### 1.8 Report Structure

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

### 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 cant 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…

### 2.5 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

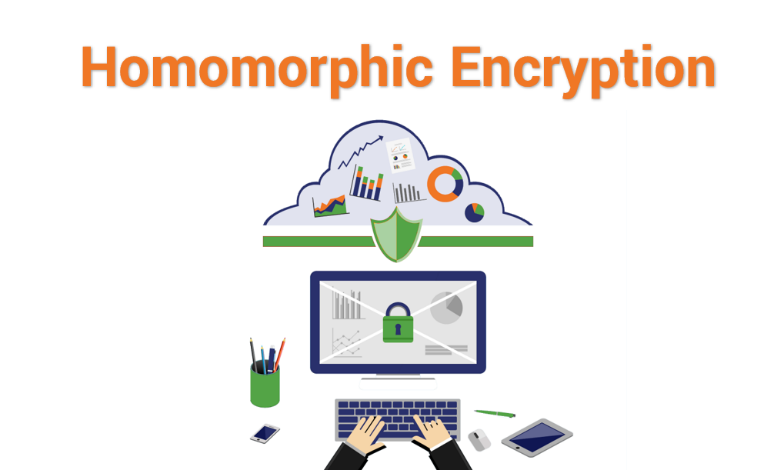
## Chapter 3: Research into Neural Networks and Homomorphic Encryption

### 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

### 3.6 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

## 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

# PART 4: Closure

## Chapter 6: Evaluation & Testing

### 6.1

## Chapter 7: Conclusion and future work

# Project References