HOMOMORPHIC ENCRYPTION FOR NEURAL NETWORKS

Project Proposal Pitch

PRESENT BY Nam, Kim, Diyon, Aurora, Brendon

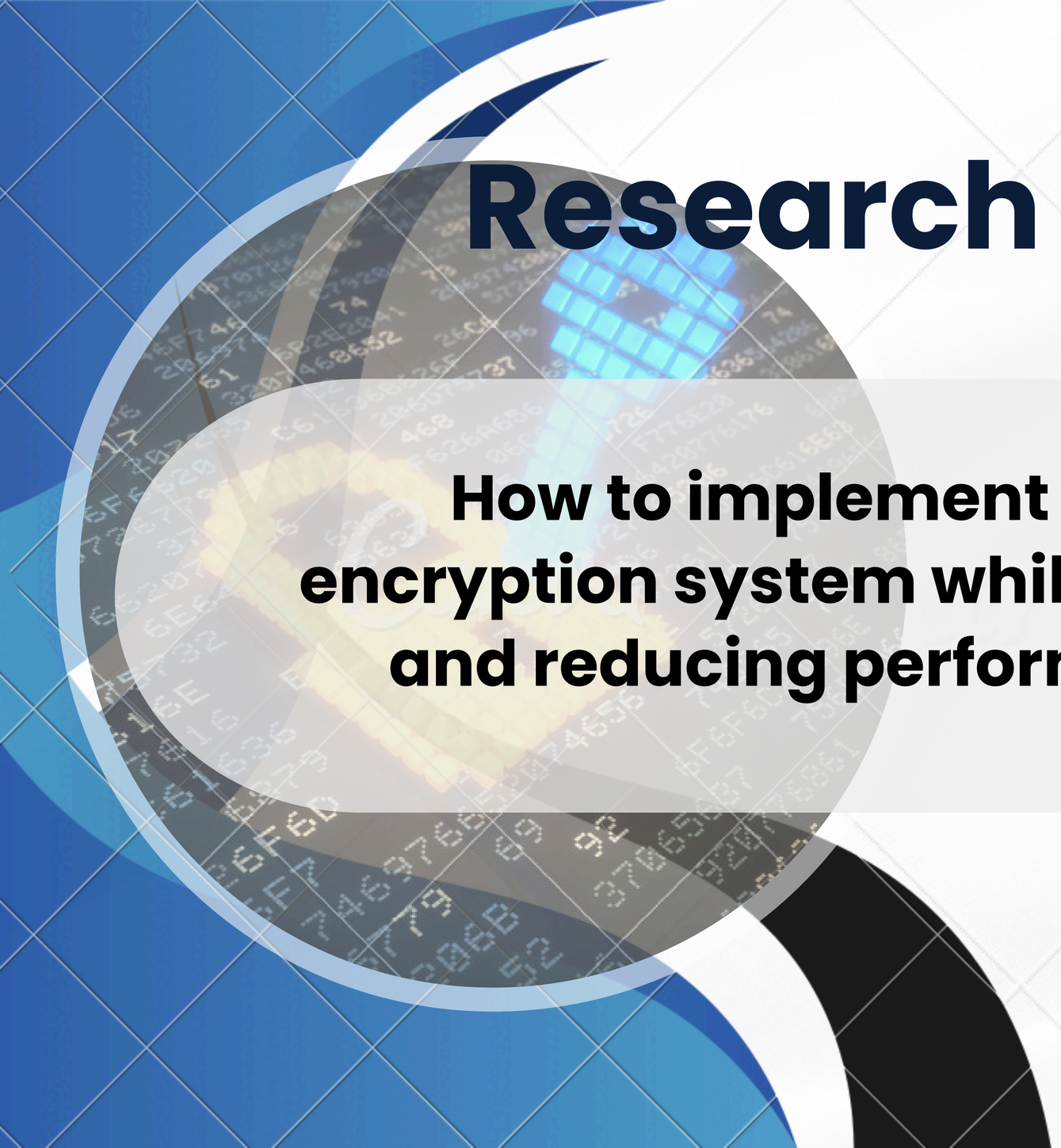
Background & Context of the Research Problem

Think --> How can we keep our private information safe when it's all getting stored and moved around on the internet?

Definition:

Homomorphic encryption is a form of encryption that permits users to perform computations on its encrypted data without first decrypting it (Gillis, 2022).

Research Question



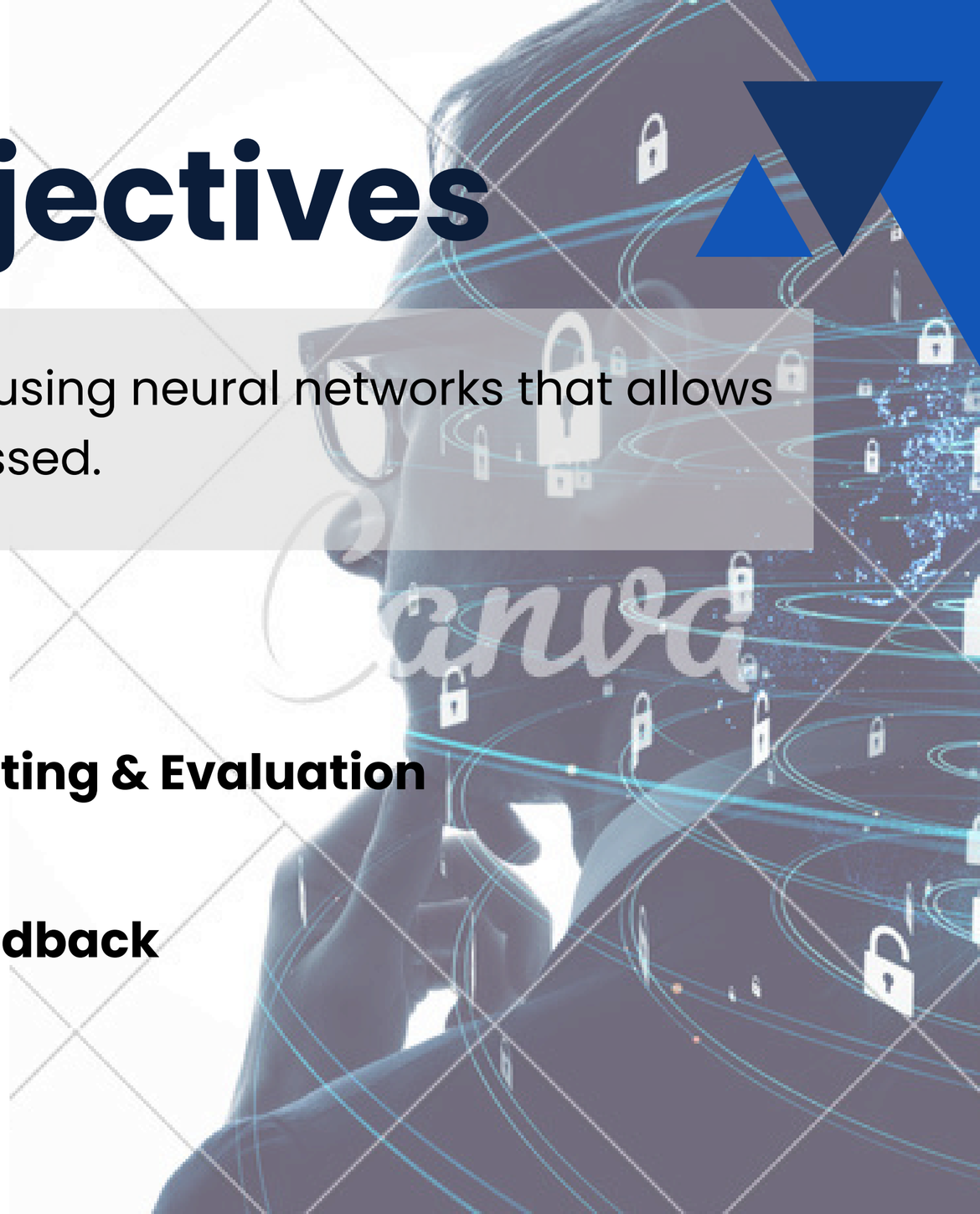
How to implement a homomorphic encryption system while preserving privacy and reducing performance overhead ?

Aims & Objectives

Develop a homomorphic encryption system using neural networks that allows data to remain encrypted while being processed.

OBJECTIVES

1. **Research & Design**
2. **Implementation**
3. **Optimization**
4. **Testing & Evaluation**
5. **Feedback**



Impact of the Research

- **Privacy preservation :** A beacon of hope in an era of frequent data breaches.
- **Performance Improvement :** Making algorithms light and fast.
- **Sector Revolution :** Impact on healthcare, finance, and government.

Literature Review

Key generation [edit]

1. Choose two large prime numbers p and q randomly and independently of each other such that $\gcd(pq, (p-1)(q-1)) = 1$. This property is assured if both primes are of equal length.[1]
2. Compute $n = pq$ and $\lambda = \operatorname{lcm}(p-1, q-1)$.
3. Select random integer g where $g \in \mathbb{Z}^*_{n^2}$
4. Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse: $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$,

where function L is defined as $L(x) = \dfrac{x-1}{n}$.

Note that the notation $\dfrac{a}{b}$ does not denote the modular multiplication of a times the modular multiplicative inverse of b but rather the quotient of a divided by b, i.e., the largest integer value $v \geq 0$ to satisfy the relation $a \geq vb$.

- The public (encryption) key is (n, g).
- The private (decryption) key is (λ, μ).

If using p,q of equivalent length, a simpler variant of the above key generation steps would be to set $g = n + 1, \lambda = \varphi(n)$, and $\mu = \varphi(n)^{-1} \bmod n$, where $\varphi(n) = (p-1)(q-1)$.[1]

Encryption [edit]

1. Let m be a message to be encrypted where $0 \leq m < n$
2. Select random r where $0 \leq r < n$
3. Compute ciphertext as: $c = g^m \cdot r^n \bmod n^2$

Decryption [edit]

1. Let c be the ciphertext to decrypt, where $c \in \mathbb{Z}^*_{n^2}$
2. Compute the plaintext message as: $m = L(c^\lambda \bmod n^2) \cdot \mu \bmod n$

Paillier Scheme algorithm (Paillier 1999)

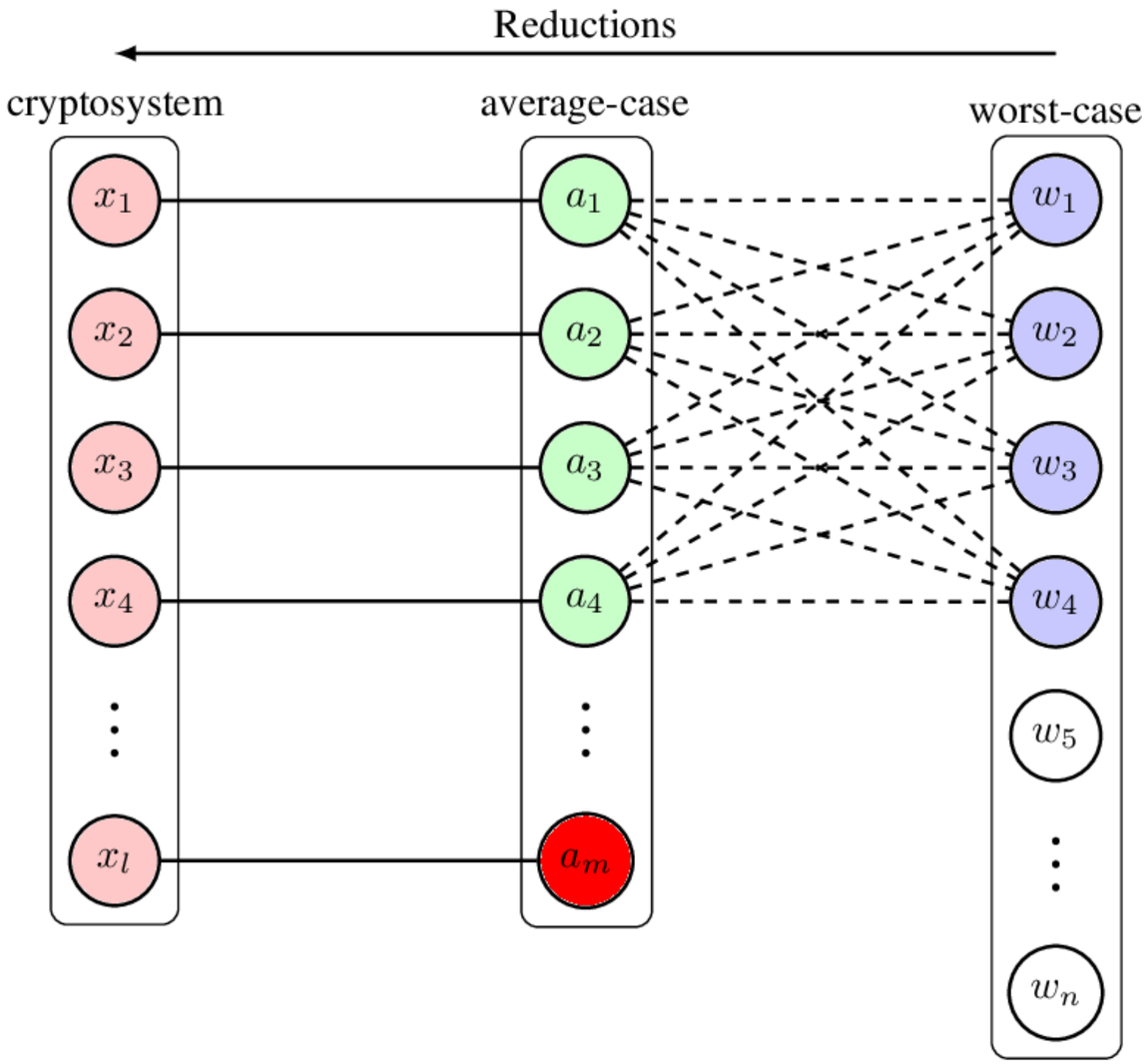
Partial vs Full homomorphism

Partial	Full
Allow for add or multiply between ciphertexts	Allow for add and multiply between ciphertexts
Can still multiply with constants	Can still multiply with constants
Allow for less overhead	Expensive

(‘Types of Homomorphic Encryption - IEEE Digital Privacy’ n.d.)

$$Z \neq R$$

Paillier Scheme algorithm (Paillier 1999)



Lattices for homomorphic encryption (Li, Ng & Purcell 2022)

Fixed point encoding : Storing a fixed number of fractional bits along with integer part (Goyal et al. n.d.)

Example encoding

5 -> 101 in binary

0.625 -> 0.101 in binary

5.625 is 101.101

Remove the .

101101 -> 45

Remember the number of bits in the mantissa (fractional bits)

Methodology

Research Design

Quantitative

- Aims to **measure**
- Focus on benchmarking, quantifiable statistics, and measurement
- Larger sample sizes
- Examples include online surveys and computer-assisted telephone interviewing (CATI)

Quantitative aspects focus on performance metrics such as the accuracy, F1 score, and computational efficiency of neural networks trained to be compatible with homomorphic encryption

Qualitative aspects could involve the evaluation of the practicality and scalability of such systems in real-world scenarios.

Qualitative

- Aims to **explore**
- Focus on diving deep, asking why, and exploring mindsets with great detail
- Smaller sample sizes
- Examples include focus groups and in-depth interviews

Data Collection

In this project, we aim to collect the datasets for our training and testing step for the neural net work optimization

kaggle

Use platforms like Kaggle for publicly available datasets relevant to the domains where homomorphic encryption could be applied, such as healthcare and finance

Using MNIST dataset to validate the effectiveness and efficiency of the neural network-based homomorphic encryption system in processing image data

Enhancing Data Analysis Through Advanced Methodologies

Step 1

- Model Training and Validation
- Performance Metrics

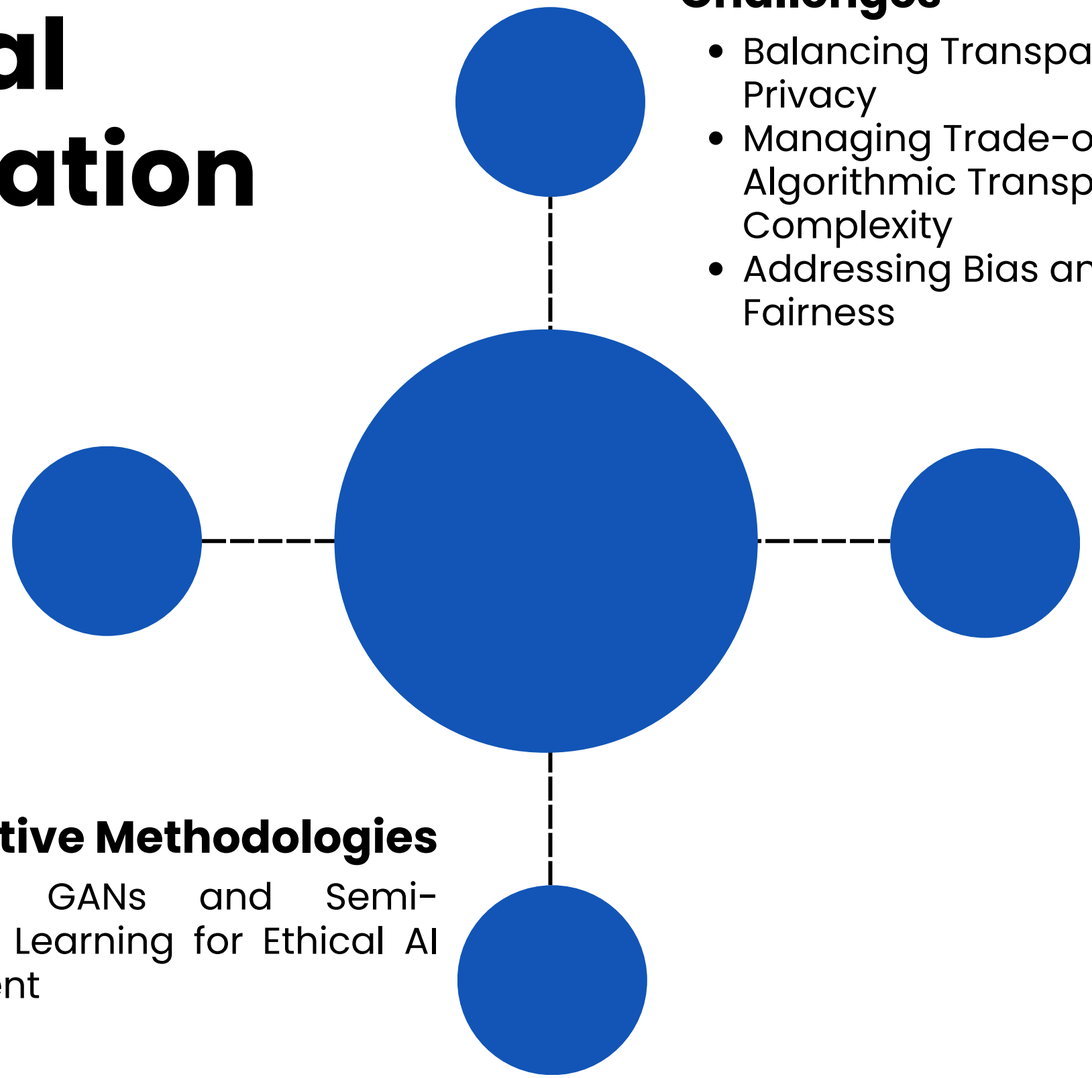
Step 2

- Model Optimization
- Security Assessment

Step 3

- Comparative Analysis
- Real-world Application Testing

Ethical Consideration



Challenges

- Balancing Transparency and Privacy
- Managing Trade-offs: Algorithmic Transparency vs. Complexity
- Addressing Bias and Ensuring Fairness

Core Ethical Principles

Beneficence, Non-maleficence, Autonomy, Justice, Explicability.

Solution

- Inherent Model Interpretability
- Ethical Audits and Accountability Measures

Innovative Methodologies

Leveraging GANs and Semi-Supervised Learning for Ethical AI Development

Expected Results

Anticipated outcomes

Our research aims to provide a suitable real world solution to the performance and security risks of encyrpting and decrypting data

Efficiency

Our research aims to demonstrate a quantitive increase in efficiency versus current state of the art methods through a reduction or maintenance in time efficiency

Security Preservation

Homomorphic encryption algorithms allow obscuration of private data whilst maintaining the ability to perform operations.

Interopability

Integration and standardisation of data encryption across platform domains and communication across technologies

Scalability

Our research aims to develop homomorphic encryption algorithms that are suitable for extremely large data sets

Potential Limitations

Security and Vulnerability detection

The practical adaptation of homomorphic encryption can have a vast array of potentially unknown vulnerabilities that are very difficult to anticipate.

Practical Adaptation

The Complexity of homomorphic encryption can leave this method as unviable to the general public. Lack of ecosystem tools and resources may also impact adoption.

Diversity of data types and operations

Homomorphic encryption can be potentially difficult to apply to the wide variety of data formats. Support for advanced data operations above simple mathematical computations may be challenging to implement.
With continuous advancements in technology and cryptographic research, we aim to increase the versatility of homomorphic encryption.

Challenges

Budget

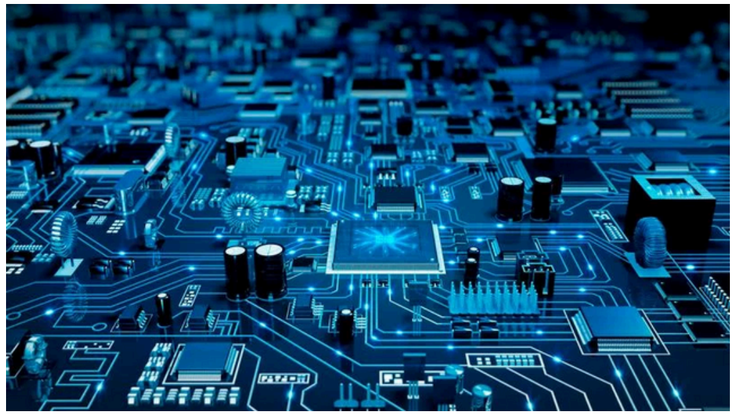
Considering the budgetary limitations of our research our research may be influenced through our choice of research methods and ability to conduct experiments

Ethical considerations

Our proposed solutions and implementations must comply to regulatory laws and engage in socially responsible considerations to ensure we contribute positively to the community and environment around us.

Australian Government
Australian Signals Directorate

ACSC
Australian Cyber Security Centre

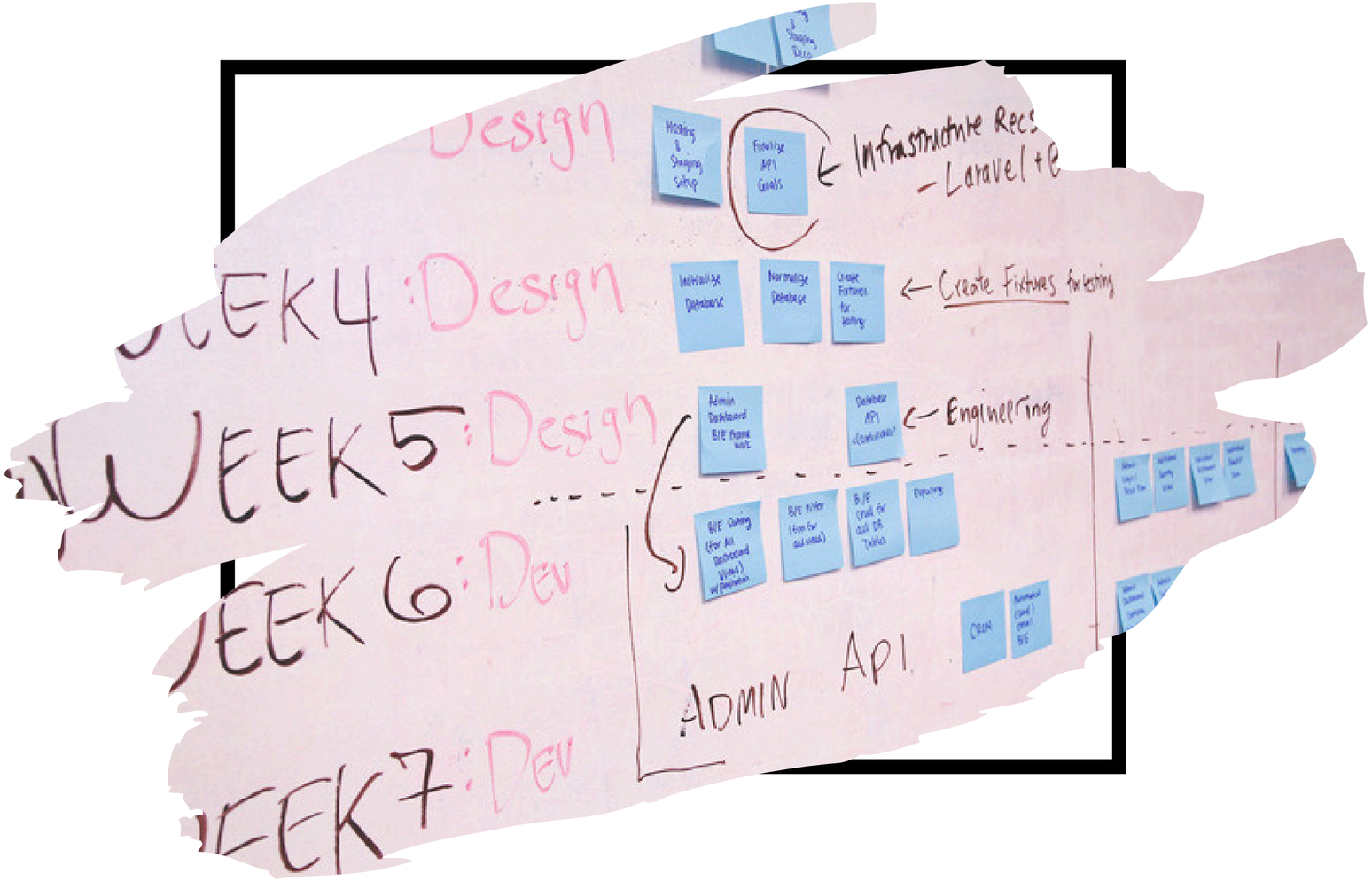


Data sets and hardware

Securing appropriate data sets and suitable hardware for the research may significantly impact our methodology and research.
It is crucial to carefully select the data sets that align with the objectives of the research to ensure the accuracy and reliability of the findings. Additionally, having the right hardware and technological tools can streamline the data collection and analysis process.

Timeline & Schedules

Schedules for achieving goals in each of the phases.
Weekly Saturday Meeting (Optional: online or in-person).
Continuous online discussions.



Schedules for each phase of the research project

Homomorphic Encryption using Neural Networks	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week	Week 9	Week 10	Week 11	Week 12
Phase 1: Research and Design	Define projec and objective	Conduct research resources among	Initiation on implementing									
Phase 2: Implementation			Implementing projec		Monitor pro	Review and make adjustments						
Phase 3: Optimization					Review and optimising		Make nessisary adjustments					
Phase 4: Testing Evaluation and Finalising									Conduct testing /Gather feedback		Analyze the result	Finalise

Role and Responsibilities

1

Paillier Encryption

c++ implementation of paillier encryption

Team members: Nam, Brendan, Aurora

2

Machine Learning

Using Python

Team member: Diyon and Jayce

Feasibility Study

Estimate cost for conducting the research and allocation of resources.

Feasibility Overview

Estimate Cost

- Development, Implementation and Maintenance cost.

- Equipment and Supply
- Other expenses

Allocation of resources

- The team leader, Nam is responsible for resource allocation.

- Team members request the resources needed from the team leader.

Thank You!

References

Li, Y., Ng, K. & Purcell, M. 2022, A TUTORIAL INTRODUCTION TO LATTICE-BASED CRYPTOGRAPHY AND HOMOMORPHIC ENCRYPTION A PREPRINT, viewed 11 March 2024.

Paillier, P. 1999, ‘Public-Key Cryptosystems Based on Composite Degree Residuosity Classes’, LNCS, vol. 1592, pp. 223–38, viewed 9 March 2024, <https://link.springer.com/content/pdf/10.1007/3-540-48910-X_16.pdf>.

Pathak, V. 2022, Notes on Lattices, Homomorphic Encryption, and CKKS, viewed 9 March 2024, <https://arxiv.org/pdf/2205.03511.pdf>

Gillis, A. S. (2022, August 24). What is homomorphic encryption?. Security. https://www.techtarget.com/searchsecurity/definition/homomorphic-encryption#:~:text=Homomorphic%20encryption%20enables%20complex%20mathematical,between%20elements%20in%20both%20sets

‘Types of Homomorphic Encryption - IEEE Digital Privacy’ n.d., digitalprivacy.ieee.org, viewed <https://digitalprivacy.ieee.org/publications/topics/types-of-homomorphic-encryption>.

Goyal, R., Vanschoren, J., Van Acht, V. & Nijssen, S. n.d., Fixed-point Quantization of Convolutional Neural Networks for Quantized Inference on Embedded Platforms.

.

Diyon : Introduction

Nam : Literature Review

Thai : Methodology

Brendan : Expected Results

Aurora : Timeline and Feasibility