A PRELIMINARY REPORT
ON

Neural Networks Based Message Concealment Scheme

SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE
IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE

OF

BACHELOR OF ENGINEERING (COMPUTER)

SUBMITTED BY

STUDENT NAME	EXAM NO:
Prasann Shimpi	**71922822M**
Sanket Halake	**71922556G**
Shivam Dharmshetti	**71922510J**
Shashank Singh	**71922816G**

DEPARTMENT OF COMPUTER ENGINEERING
DR. D.Y.PATIL INSTITUTE OF ENGINEERING, MANAGEMENT & RESEARCH
AKURDI, PUNE 411044

SAVITRIBAI PHULE PUNE UNIVERSITY

2021 -2022

CERTIFICATE

This is to certify that the project report entitles

“NEURAL NETWORKS BASED KEY CONCEALMENT SCHEME”

Submitted by

STUDENT NAME	**EXAM NO:**
Prasann Shimpi	**71922822M**
Sanket Halake	**71922556G**
Shivam Dharmshetti	**71922510J**
Shashank Singh	**71922816G**

is a bonafide student of this institute and the work has been carried out by him/her under the supervision of **Dr. Amol Dhakne** and it is approved for the partial fulfilment of the requirement of Savitribai Phule Pune University, for the award of the degree of **Bachelor of Engineering** (Computer Engineering).

Dr. Amol Dhakane
Guide
Department of Computer Engineering

Prof. P.P.Shevatekar
Head,
Department of Computer Engineering

Dr. Anupama V. Patil
Principal,
Dr.D.Y.Patil Institute of Engineering,Management & Research Akurdi Pune – 41

Place : Pune
Date :

ACKNOWLEDGEMENT

It gives us great pleasure in presenting the preliminary project report on ‘Neural Network based message concealment scheme’.

I would like to take this opportunity to thank my internal guide Dr. Amol Dhakane for giving me all the help and guidance I needed. I am really grateful to them for their kind support. Their valuable suggestions were very helpful.

I am also grateful to Prof. P.P. Shevtekar, Head of Computer Engineering Department, Dr. D. Y. Patil Institute of Engineering, Management & Research for his indispensable support, suggestions.

In the end our special thanks to Dr. Amol Dhakane for providing various resources such as laboratory with all needed software platforms, continuous guidance, for Our Project.

Prasanna Shimpi	**71922822M**
Sanket Halake	**71922556G**
Shivam Dharmshetti	**71922510J**
Shashank Singh	**71922816G**

(BE Computer Engineering)

ABSTRACT

The goal of cryptography is to make it impossible to take a cipher and reproduce the original plain text without the proper key. With good cryptography, your messages are encrypted in such a way that brute force attacks against the algorithm or key are almost impossible. Good cryptography keeps you safe by using incredibly long keys and using encryption algorithms resistant to other attacks. The neural network application is a form of the next development in good cryptography. This project is about the use of neural networks in cryptography, for example, the design of a neural network that is practically used in the field of cryptography.

Neural cryptography is a new field aimed at combining cryptography and neural networks for cryptanalysis and cryptography applications. This project shows that neural networks can perform symmetric cryptography in a hostile environment to improve the known literature on this topic. It also shows that neural networks can detect known unencrypted communications by playing well-known cryptographic games based on ciphertext**.**

In this project, we study the problem of key exchange using Artificial Neural Network. The purpose of this project is to examine the feasibility and performance of Artificial Intellegence in cryptography. We compare the performance and reliability of traditional key exchange against key exchange using ANNs. The Neural Network is trained in an adversarial fashion with distinct constructions for loss. The Accuracy of the performance of the neural network is compared using various out of sample performance measures.

[P3]

TABLE OF CONTENTS

Appendix A: Problem statement feasibility assessment using, satisfiability analysis and NP Hard,NP-Complete or P type using modern algebra and relevant mathematical models.

Appendix B: Details of the papers referred in IEEE format (given earlier) Summary of the above paper in not more than 3-4 lines. Here you should write the seed idea of the papers you had referred for preparation of this project report in the following format.
Example:
Thomas Noltey, Hans Hanssony, Lucia Lo Belloz,"Communication Buses for Automotive Applications" In *Proceedings of the* 3rd *Information Survivability Workshop (ISW-2007),* Boston, Massachusetts, USA, October 2007. IEEE Computer Society.

Appendix C: Plagiarism Report

References

LIST OF ABBREVATIONS

ABBREVIATION	ILLUSTRATION
HTTP	Hyper Text Transfer Protocol
MQTT	Message Query Telemetry Transport
ANN	Artificial Neural Networks
CNN	Convolutional Neural Networks

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1 OVERVIEW

Nowadays, we live in a data-driven world, and in most use cases, businesses collect and store sensitive personal and non-personal information, which can be exploited by cyber criminals.

Good cryptography keeps you safe by using incredibly long keys and using encryption algorithms resistant to other attacks. The neural network application is a form of the next development in good cryptography. This project is about the use of neural networks in cryptography, for example, the design of a neural network that is practically used in the field of cryptography. To demonstrate an application of ANNs in the field of cyber security, we create three neural networks: Alice, Bob and Eve. Two of these participate in a message exchange using symmetric encryption and the third acts as an adversary and observe the rate of success.

1.2 MOTIVATION

Cryptography is a method that enables a method of decrypting secrets, and is a function that transforms information into information that is not explicitly understood. The basic idea of encryption is the ability to send information between participants in a way that no one else can read. There are many number-theoretic cryptographic methods available, but they have the disadvantage of requiring a great deal of computational power, complexity, and wasting time. To overcome these shortcomings, artificial neural networks (ANNs) have been used to solve many problems. ANN has many characteristics such as learning, generalization, reduced data requirements, fast computing, easy implementation, software and hardware availability, and is very attractive to many applications.

Work on artificial neural network has been motivated right from its inception by the recognition that the human brain computes in an entirely different way from the conventional digital computer. With the growth of the Internet, social networks, and online social interactions, getting daily user predictions is feasible job. Thus, our motivation is to successfully incorporate artificial intelligence in order to make the cyber space safe that will benefit everyone.

1.3 PROBLEM STATEMENT AND OBJECTIVE

1.3.1 Problem Statement:

To demonstrate the current progress of implementing Artificial Intelligence in Cryptography and see how it performs against traditional methods. The project is based in the demonstration using three artificial neural networks that will generate and exchange keys for symmetric encryption while the third acts as an adversary. This will not only help test the strength of the encryption and key exchange algorithm but also supersede the need of a human adversary. When executed via the right strategies, cryptography helps you safeguard this sensitive information, preventing it from falling prey to cyber threats and threat actors.

1.3.2 Objectives:

- To ensure data integrity through hashing algorithms and message digests. By providing digital codes and keys to ensure that what is received is genuine and originates from the intended sender, the recipient can ensure that the data received has not been tampered with in transit
- To test key exchange between two neural networks in presence of an adversary.

1.4 PROJECT SCOPE

1.4.1 Project Scope:

Symmetric Key encryption using artificial intelligence will be useful to safeguard internet exchanges and to defend against man-in-middle attacks.

2. LITERATURE SURVEY

Table 1. Literature Survery

Sr. No	Paper Title	Authors & Published on	Methodology
1	Deep Neural Networks based key concealment schemes	Taehyuk Kim, Tae Young Youn 04 Nov 2020	In this paper, we propose a new DNNs-based key concealment scheme for concealing cryptographic keys within DNNs.
2	A Neural Network based Approach for Cryptographic Function Detection	Li Jia, Anmin Zhou, Peng Jia, Luping Liu, Yan Wang, Liang Liu 2020	This paper proposed a novel approach for cryptographic function detection in malware.
3	Neural Cryptography based on Complex Valued Neural Networks	Tao Dong,Tingwen Huang 2019	This paper took a complex value based parity machine (CVTPM) approach to neural cryptography.
4	Neural Cryptography Based on Topology Evolving Neural Networks	Yuetong Zhu, Danilo Vasconcellos Vargas, Kouichi Sakurai 2018	This paper suggested a neural network architecture to learn neural cryptography.
5	Neural Cryptography: From symmetric encryption to Adverarial Steganography	Dylan Modesitt, Tim Henry, Jon Coden, and Rachel Lathe 2018	This paper discussed various research in the field of neural cryptography from symmetric encryption to steganography.

6	Use of Neural Networks in Cryptography: A Review	Pranita P. Hadke, Swati G. Kale 2016	This paper gave a review of the current usage and possibilities of the utilisation of neural networks in cryptography.
7	Neural Network based Cryptography	Apdullah Yayik,, Yapik Kutlu 2014	This paper discussed the iteration of ANNs in cryptography and their advantages over other methods (symmetric encryption).
8	Cryptography based on Neural Networks	Eva Volna, Michael Janosek, Martin Kotyrba 2014	This paper brought into light the method of practical implementation of neural cryptography in real world applications.
9	Cryptography using Artificial Neural Networks	Vikas Gujral, Satish Pradhan 2009	This paper represented a comparative study between different neural network architectures for a adder and discussed their possible applications in cryptography.
10	Neural Cryptography	Wolfgang Kiesel, Ido Kanter. 2002	This paper discussed the first iteration of ANNs in cryptography and their advantages over other methods (symmetric encryption).

3. SOFTWARE REQUIREMENT SPECIFICATION

3.1 INTRODUCTION

3.1.1 PROJECT SCOPE

- The proposed system will help to strengthen the traditional key exchange.
- The given system will create secret key and transfuses this secret key using several convolution layers.

3.1.2 USE CLASSES AND CHARACTERISTICS

Our system is divided into two class/modules:

1) adversary

2) participants (sender and receiver)

3.1.3 ASSUMPTIONS AND DEPENDENCIES

1. User must have the knowledge of web based application.
2. User must have the knowledge of English.
3. User must have all required software to run the application.

3.1.4 MATHEMATICAL MODELING OF AN ARTIFICIAL NEURAL NETWORK

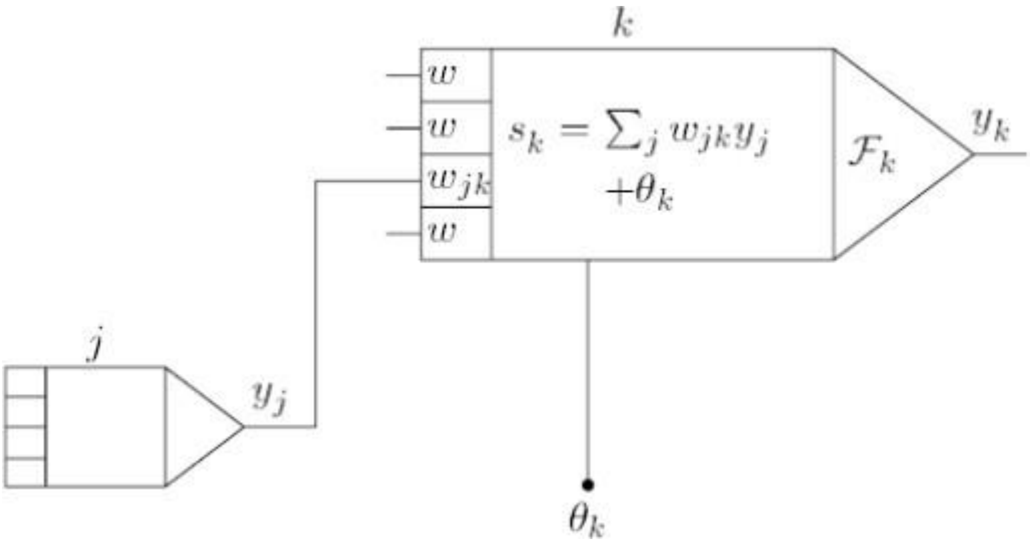

Figure 1. ANN block diagram

An artificial neural network consists of a pool of simple processing units which communicate by sending signals to each other over a large number of weighted connections. A set of major aspects of ANN are:

A state of activation yk for every unit, which equivalent to the output of the unit;

Connections between the units. Generally each connection is defined by a weight wjk which determines the effect which the signal of unit j has on unit k;

A propagation rule, which determines the effective input sk of a unit from its external inputs;

An activation function Fk, which determines the new level of activation based on the effective input sk(t) and the current activation yk(t) (i.e., the update);

An external input (aka bias, offset) θk for each unit;

Connections between units

$$s_k(t) = \sum_j w_{jk}(t)\, y_j(t) + \theta_k(t).$$

$$s_k(t) = \sum_j w_{jk}(t) \prod_m y_{j_m}(t) + \theta_k(t).$$

Activation and the output rules

$$y_k = \mathcal{F}(s_k) = \frac{1}{1 + e^{-s_k}}$$

$$y_k(t+1) = \mathcal{F}_k(y_k(t), s_k(t)).$$

$$y_k(t+1) = \mathcal{F}_k(s_k(t)) = \mathcal{F}_k\left(\sum_j w_{jk}(t)\, y_j(t) + \theta_k(t)\right),$$

Equation No. 1

Failures:

1. Data packet loss during the transmission within the network
2. Hardware failure.
3. Software failure.

Success:

1. Decrypt the message without compromising integrity of data.
2. Encryption is done very fast so is the decryption

Space Complexity:

The space complexity depends on Presentation and visualization of discovered patterns. More the storage of data more is the space complexity.

Time Complexity:

Check No. of patterns available in the datasets= n

If (n>1) then retrieving of information can be time consuming. So the time complexity of this algorithm is O$(n^n)(n^n)$.

3.2 FUNCTIONAL REQUIRMENTS

- It should be able to encrypt and decrypt the data
- It shouldn’t be able to cracked easily.
- Performance of the functions and every module must be well. The overall performance of the algorithm will enable the users to rely with respect to security.
- The system is designed in modules where errors can be detected and fixed easily. This makes it easier to install and update new functionality if required.

3.3 EXTERNAL INTERFACE REQUIREMENTS

3.3.1 USER INTERFACES

The requirements section of hardware includes minimum of 180 GB hard disk and 4 GB RAM with 2 GHz or higher speed. The primary requirements include a memory of 4GB for the Android Application development and MySQL.

3.4 HARDWARE INTERFACES

As this is an online application for product management we are not enabling or installing any hardware components for user interface.

It’s not an embedded system

- Processor - Pentium IV 2.4 GHZ
- Speed - 1.5 Ghz and Above
- RAM - 4 GB (min)
- Hard Disk - 220 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse

SOFTWARE INTERFACES

This is the software configuration in which the project was shaped. The programming language used, tools used, etc are described here.

●	Operating System	: Windows
●	Front End	: html,css,boostrap,javascript
●	Tool	: pycharm,Keras
●	Database	: MySQL

3.5 COMMUNICATION INTERFACES

- Standard internet connection is required.
- TCP/UDP connection will be required.

3.4 NON-FUNCTIONAL REQUIREMENTS

3.4.1 PERFORMANCE REQUIREMENTS

- High Speed:

System should process requested task in parallel for various action to give quick response. Then system must wait for process completion.

- Accuracy:

System should correctly execute process, display the result accurately. System output should be in user required format.

3.4.2 SAFETY REQUIREMENTS

The data safety must be ensured by arranging for a secure and reliable transmission media. The source and destination information must be entered correctly to avoid any misuse or malfunctioning..

3.4.3 SECURITY REQUIREMENTS

Secure access of confidential data (user's details).

- Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.
- The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

3.4.4 SOFTWARE QUALITY ASSURANCE

- Availability [related to Reliability]
- Modifiability [includes portability, reusability, scalability]
- Performance

- Security

- Testability
- Usability[includes self-adaptability and user adaptability]

3.5 SYSTEM REQUIREMENTS

3.5.1 DATABASE REQUIREMENTS

MySQL : MySQL is an open-source relational database management system (RDBMS). Its name is a combination of “My”, the name of co-founder Michael Widenius’s daughter, and “SQL”, the abbreviation for Structured Query Language.

MySQL is free and open-source software under the terms of the GNU General Public License, and is also available under a variety of proprietary licenses. MySQL was owned and sponsored by the Swedish company MySQL AB, which was bought by Sun Microsystems (now Oracle Corporation). In 2010, when Oracle acquired Sun, Widenius forked the open-source MySQL project to create MariaDB.

MySQL is a component of the LAMP web application software stack (and others), which is an acronym for Linux, Apache, MySQL, Perl/PHP/Python. MySQL is used by many database-driven web applications, including Drupal, Joomla, phpBB, and WordPress. MySQL is also used by many popular websites, including Facebook, Flickr, MediaWiki, Twitter, and YouTube.

3.5.2 SOFTWARE REQUIREMENTS Operating

system : Windows 7 and above.Coding

Language : Python,

IDE : Pycharm, Atom

3.5.3 HARDWARE REQUIREMENTS

System : Intel I3 Processor and above.

Hard Disk	:	5 GB.
Monitor	:	15 VGA Color.
Ram	:	4 GB.

3.6 ANALYSIS MODELS : SDLC MODEL TO BE APPLIED

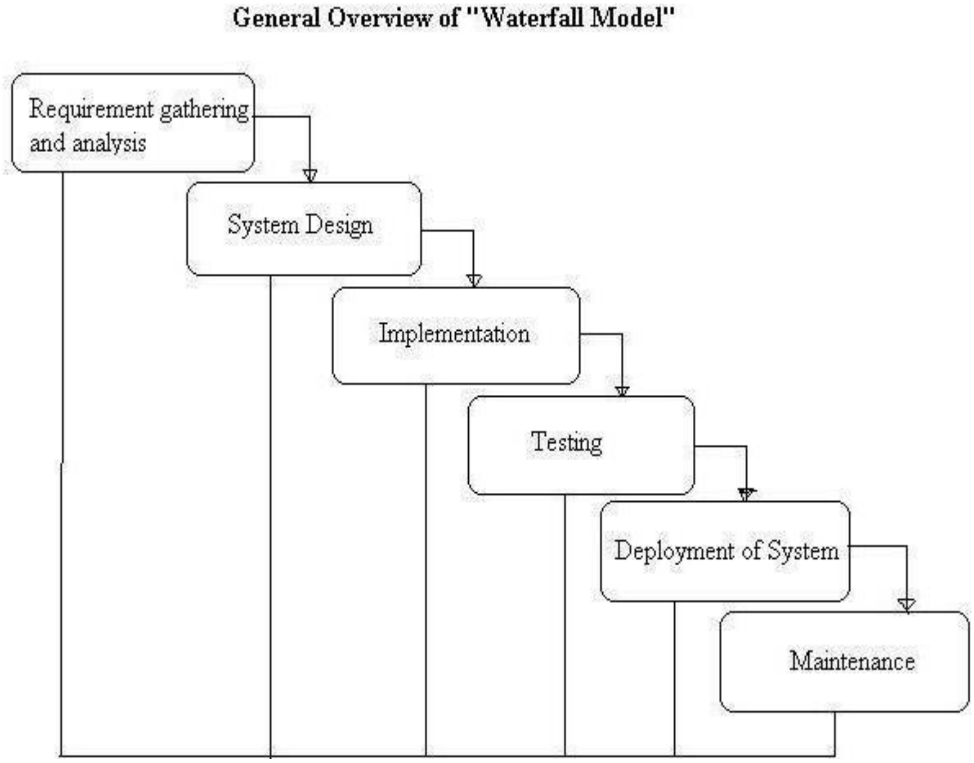
General Overview of "Waterfall Model"
Requirement gathering and analysis
System Design
Implementation
Testing
Deployment of System
Maintenance

Figure 2. Waterfall Model

3.7 SYSTEM IMPLEMENTION PLAN

1. Requirement gathering and analysis:

In this step of waterfall we identify what are various requirements are need for our project such are software and hardware required, database, and interfaces.

2. System Design:

In this system design phase we design the system which is easily understood for end user i.e. user friendly.

We design some UML diagrams and data flow diagram to understand the system flow and system module and sequence of execution.

3. Implementation:

In implementation phase of our project we have implemented various module required of successfully getting expected outcome at the different module levels.

With inputs from system design, the system is first developed in small programs called units, which are integrated in the next phase. Each unit is developed and tested for its functionality which is referred to as Unit Testing.

4. Testing:

The different test cases are performed to test whether the project module are giving expected outcome in assumed time.

All the units developed in the implementation phase are integrated into a system after testing of each unit. Post integration the entire system is tested for any faults and failures.

5. Deployment of System:

Once the functional and nonfunctional testing is done, the product is deployed in the customer environment or released into the market.

6. Maintenance:

There are some issues which come up in the client environment. To fix those issues patches are released. Also to enhance the product some better versions are released. Maintenance is done to deliver these changes in the customer environment.

All these phases are cascaded to each other in which progress is seen as flowing steadily downwards like a waterfall through the phases. The next phase is started only after the defined set of goals are achieved for previous phase and it is signed off, so the name “Waterfall Model”. In this model phases do not overlap.

4.SYSTEM DESIGN

4.1. SYSTEM ARCHITECTURE

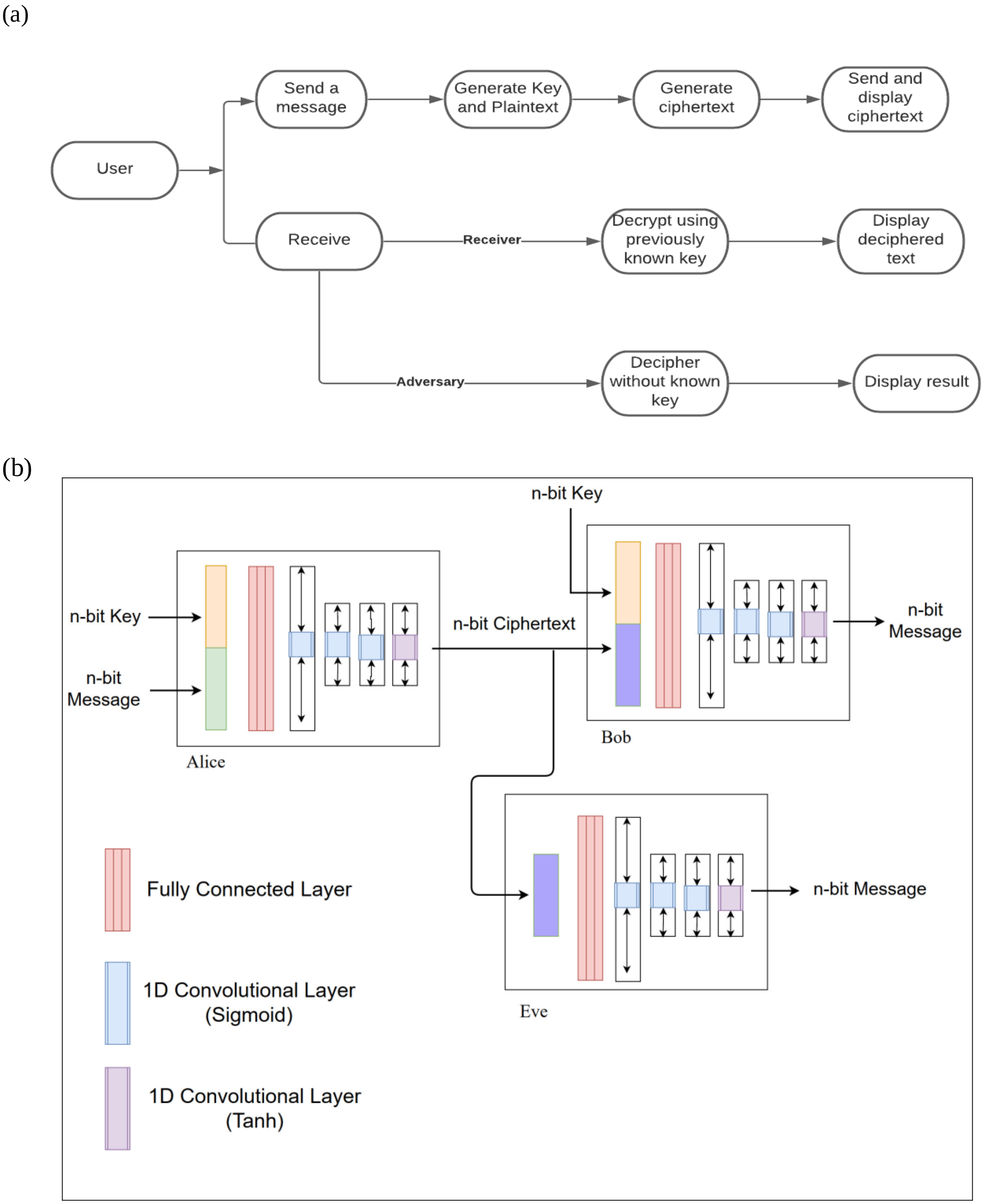

Figure 3.(a) System Architecture (b) Convolutional Model

4.2. DATA FLOW DIAGRAM

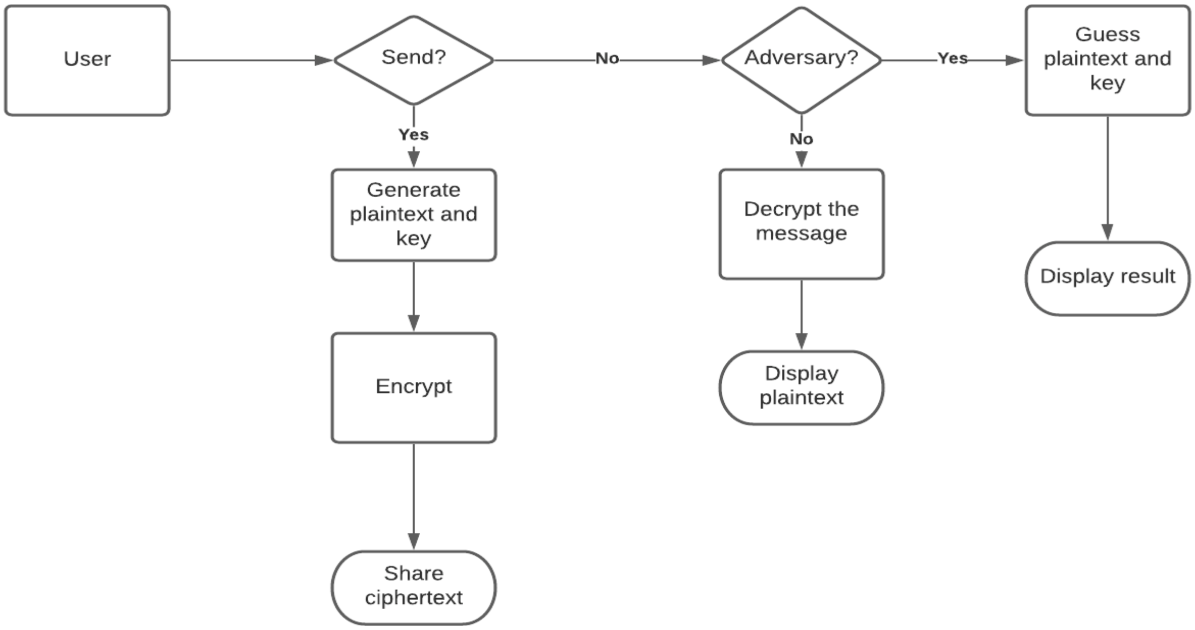

Figure 4 Dataflow Diagram

4.3. ENTITY RELATIONSHIP DIAGRAM

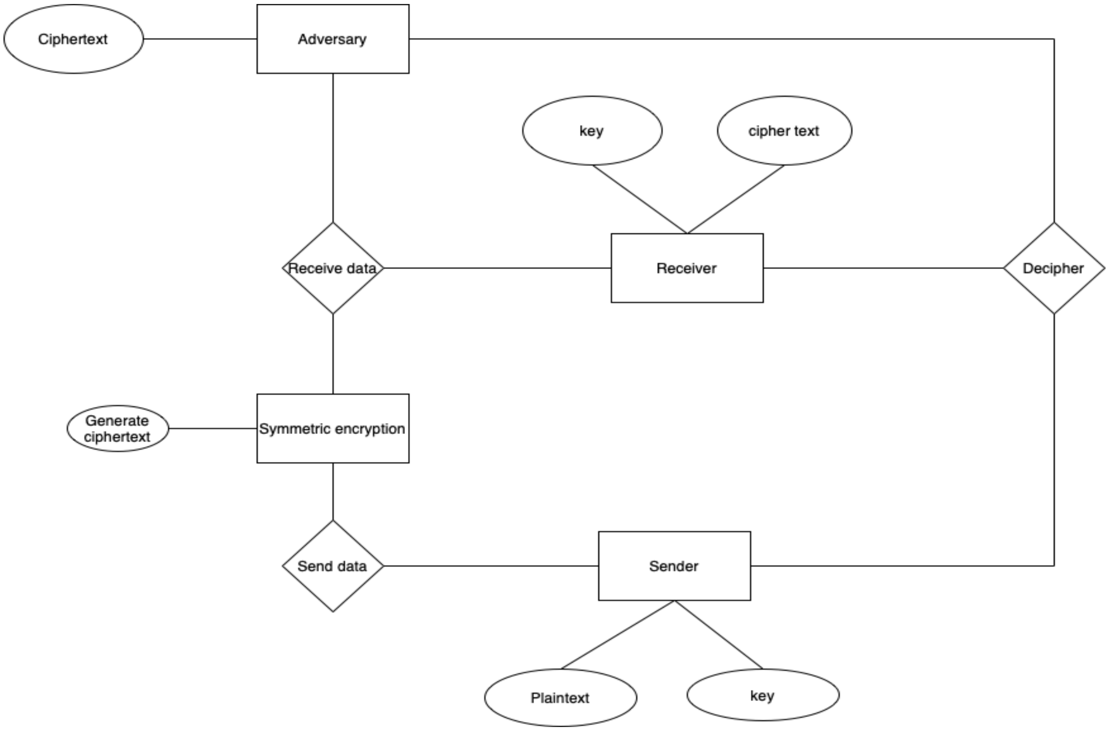

Figure 5. Entity Relationship Diagram

4.4. UML DIAGRAMS

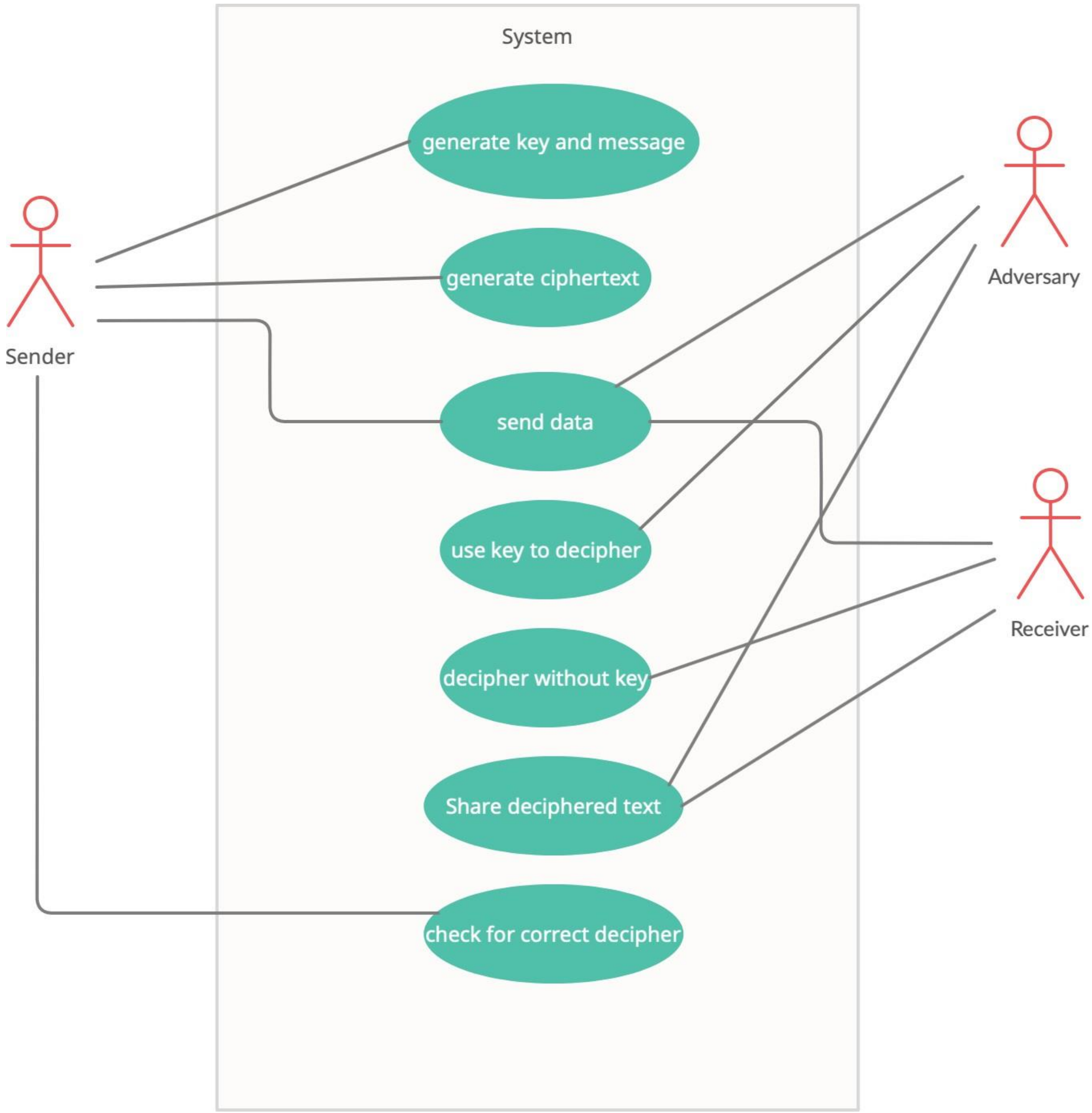

Figure 6. UML Diagram

SEQUENCE DIAGRAM

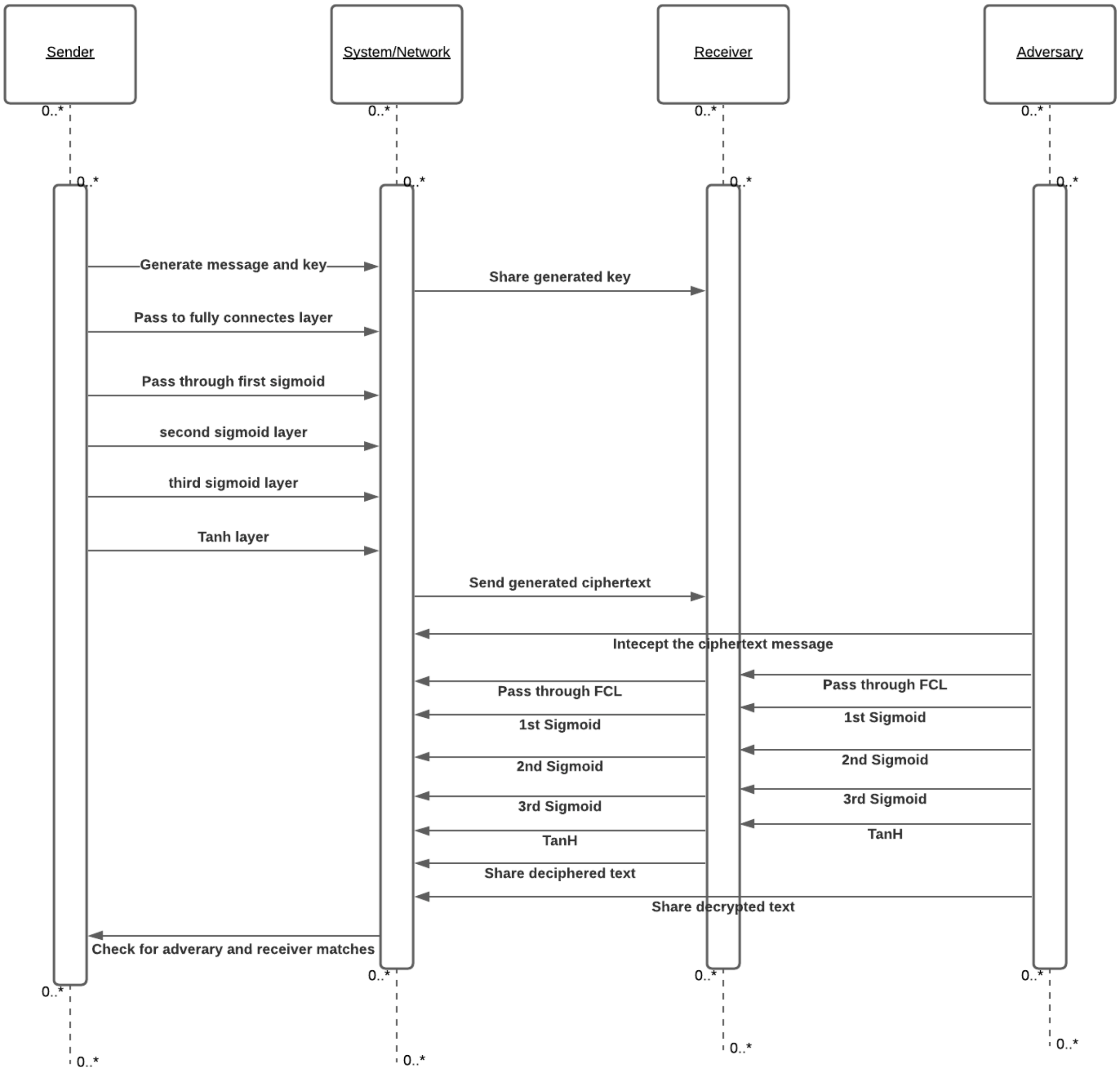

Figure 7. Sequence Diagram

ACTIVITY DIAGRAM

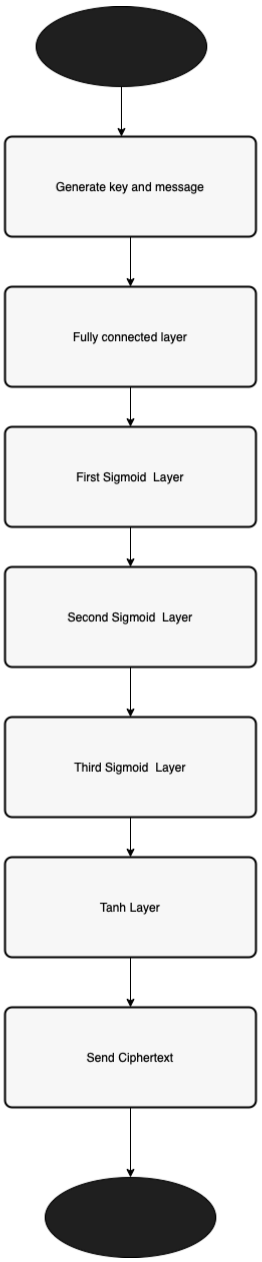

Figure 8 . Activity Diagram

5. OTHER SPECIFICATION

5.1 ADVANTAGES

- Encrypts the data such a way it doesn't get compromised easily
- Effective cryptographic technique
- Confirming those infected is essential to manage and contain the virus successfully. Without reliable testing, it would be hard to determine the actual rates of cases. Thus, it is vital to identify what these available tests can and can't do to use them appropriately**.**
- Secure and efficient system

5.2 LIMITATIONS

1. User must have the knowledge of English.
2. User must have all required software to run the application.
3. It required internet connection must.
4. User behavior cannot be controlled, hence they might be victim of phishing.

6. CONCLUSION & FUTURE WORK

6.1 Conclusion:

Artificial neural networks are a simple yet powerful technique that can emulate highly complex computing machines. In this project, we used this technique to build a simple combinatorial logic and sequential machine using the backpropagation algorithm. Comparative studies have been conducted between two different architectures of the neural network, and their strengths / weaknesses are mentioned. ANN can be used to implement complex combinational and sequential circuits.

6.2 Future scope:

This project tries to use artificial neural networks for cryptography, doing so ensures integrity of data during transmission, and also strengthen data sharing through network.

Future scope for the project to do obfuscation as the next step of the encryption and hide the key within the encrypted data, that is neural steganography. That will be an optimization of the neural cryptography.

Helps in knowing the number growing cyber attacks, will enforce security protocols.

References:

1) Taehyuk Kim, Tae Young Youn, Dooho Choi, Deep Neural Networks based Key Concealment Scheme, November 4, 2020
2) Li Jia, Anmin Zhou, Peng Jia, Luping Liu, Yan Wang, Liang Liu, A Neural Network based Approach for Cryptographic Function Detection, 2020
3) Tao Dong, Tingwen Huang, Neural Cryptography based on Complex Valued Neural Networks, 2019
4) Yuetong Zhu, Danilo Vasconcellos Vargas, Kouichi Sakura, Neural Cryptography Based on Topology Evolving Neural Networks, 2018
5) Dylan Modesitt, Tim Henry, Jon Coden, and Rachel Lathe, Neural Cryptography: From symmetric encryption to Adverarial Steganography, 2018.
6) Pranita P. Hadke, Swati G. Kale, Use of Neural Networks in Cryptography: A Review, 2016
7) Deep Neural Networks based key concealment schemes Taehyuk Kim, Tae Young Youn 04 Nov 2020

8) A Neural Network based Approach for Cryptographic Function Detection Li Jia, Anmin Zhou, Peng Jia, Luping Liu, Yan Wang, Liang Liu 2020

9) Neural Cryptography based on Complex Valued Neural Networks Tao Dong,Tingwen Huang 2019

10) Neural Cryptography Based on Topology Evolving Neural Networks Yuetong Zhu, Danilo Vasconcellos Vargas, Kouichi Sakurai 2018

11) Cryptography using Artificial Neural Networks Vikas Gujral, Satish Pradhan 2009

12) Neural Cryptography Wolfgang Kiesel, Ido Kanter.2002