ST AUGUSTINE'S
COLLEGE - SYDNEY

# Nodepaths
# Project Portfolio - Task 1

*By Alex Greig*

*April 26, 2021*

# Contents

**1 Project Portfolio** **2**

1.1 Problem Definition . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2

1.2 Input, Output and Processes Diagram . . . . . . . . . . . . . . . . . . . 2

1.3 Context and Data-flow Diagrams . . . . . . . . . . . . . . . . . . . . . . 5

1.4 Algorithms . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

# 1 Project Portfolio

## 1.1 Problem Definition

The problem with today's internet is the control large corporations have over information transmission, enabling data to be lost, monetized, or given to the government, all without users knowing. Another problem of the internet is the inherent security flaws associated with centralised control; that is, its ability to be hacked. The final problem is the inequality of the internet as large populations throughout the world are unable to access the internet, with access they would be able to receive better educational resources, progressing humanity forward.

The application that I am creating is called Nodepaths, and it is important for the consumer market as it will provide high security to user's data and a network that is robust and resistant to problems allowing for secure data transfer between devices globally, solving the problems above. The application will have a significant effect on the way we use the internet and allow users to share, communicate and complete complex computational tasks efficiently and securely. The application will be a decentralised network that uses peer-to-peer architecture and mesh topology, allowing any machine capable of connecting to a network to join and become a "node". The application will also include the feature of Wi-Fi peer to peer transmission allowing for nodes to be connected by Wi-Fi radio waves eliminating costs of telecommunication services, however, if users cannot be connected by the mesh then cellular internet is available. This information will be encrypted, end to end. The mesh network will relay data and messages using a wireless ad-hoc network, where data is propagated along a path by hopping from node to node until it reaches its destination. The paths will be calculated based on the Ad-Hoc On Demand Vector Routing protocol (AODV), a routing protocol that determines and maintains routes whenever they are required.

The application that I am creating, Nodepaths, will have three main functions. First it will create an asymmetric key pair (public and private key using elliptic curve cryptography), a psuedo-random IPv4 Address and validate a username that has been entered by the user. The second function of Nodepaths is to transfer data, normally messages, over a wireless ad-hoc network to another node. The final main function of the application will be to give users the ability to add new nodes (friends) to the application allowing them to select friends that they want to text to. These three functions when integrated will provide the foundation for a user-friendly text messaging application that runs on a decentralised, distributed network. Although the functions may seem simple or basic the underlying backend behind a network of this caliber is complex; to function, innovative solutions are needed.

Future improvements and upgrades to the application will include the implementation of Blockchain technology to provide digital transactions and a cryptographic wallet on the application, eliminating the need for banks and other financial institutions. In the future, the application may also provide assistance to disadvantaged communities as it would give them communication without the cost of telecommunication services.

## 1.2 Input, Output and Processes Diagram

| Input | Processing | Output |
|---|---|---|
| The user opens the application for the first time, and they are asked to input a username. | The application calculates a pseudo-random number with a uniform distribution to create a IPv4 address in the range of 192.168.1.0 to 192.168.254.255. It then creates an asymmetric key pair, a private and public key that will be used for identification of nodes and end-to-end encryption of data transmissions. It then takes the username that was inputed and validates it, checking that the length is between 5 and 20 characters and doesn't contain any special characters. The username, the IPv4 address and the key pair are stored securely in the phone storage | If a username was inputted that doesn't meet the required validation then the user will be redirected to enter another username. A loading screen is displayed with text saying, "Setting up Profile and Configuration." This happens while waiting for operations to be complete, then welcome text appears when done and a main menu appears. |
| The user selects the option on the main menu, "Search for users on the network." | Using the mobile phone's API for peer-to-peer Wi-Fi connections it sends out a Wi-Fi signal and also listens for incoming Wi-Fi connections. It sends a data packet on the network containing the username and searches for users with the same name. If there are multiple users with the same username then the user can select the profile they want. The two nodes establish a connection and communication is available | The user is prompted with the different users that have the username they searched, it then displays the ability to add them. If they add a node as a friend, the text, "Successfully added [username] as a friend" will be displayed. |

| | | |
|---|---|---|
| The user scans a QR code of another user. | The QR code is a representation of the public key, IP address and username of a user and when it is scanned, it is saved onto the mobile phone’s storage | Display text, ”Successfully added [username] as a friend” |
| When in the chat section of the application the user selects a user to message, they then send a text to them. | The application, utilising the ad-hoc on-demand vector routing protocol will flood the network with Route Request Packets via UDP, if the route is found then a Route Reply packet will be sent, this contains the shortest path between users. When the path is created using TCP, the public keys will be exchanged. The message will be encrypted with the other user’s public key and transmitted across the network. The message will be validated to make sure the packet size isn’t larger than 100 MB. | Once the message has been sent, the message on the user’s screen goes blue, displaying to the user that the message has been transmitted. |
| Within the profile section of the application the user can select to add a photo to their profile. | The application will open the default picture viewing application on the phone and allow the user to select a picture. The user can scale the photo to fit inside a circle with diameter of 1000 pixels. | The default photo viewing application will be displayed, then the text, ”Successfully added the profile picture,” will be displayed once the picture is scaled and fitted to the profile picture template. |

### 1.3 Context and Data-flow Diagrams

Figure 1: Context Diagram

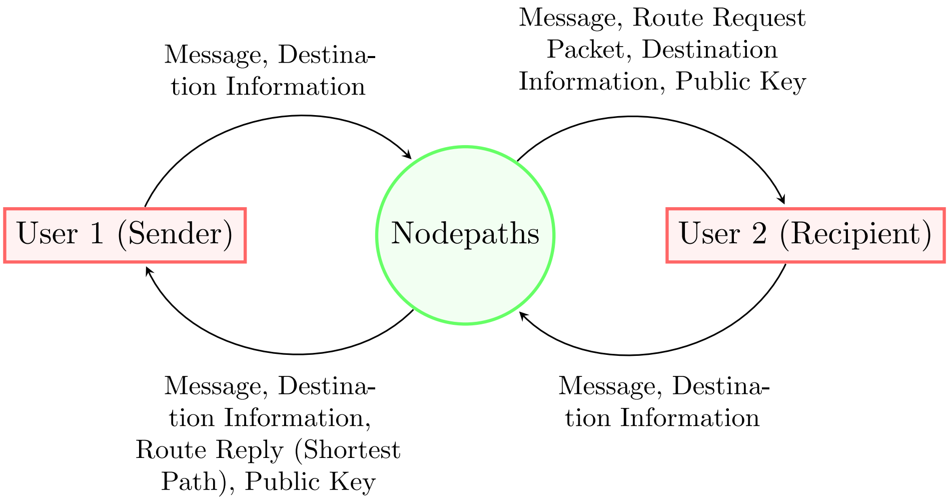
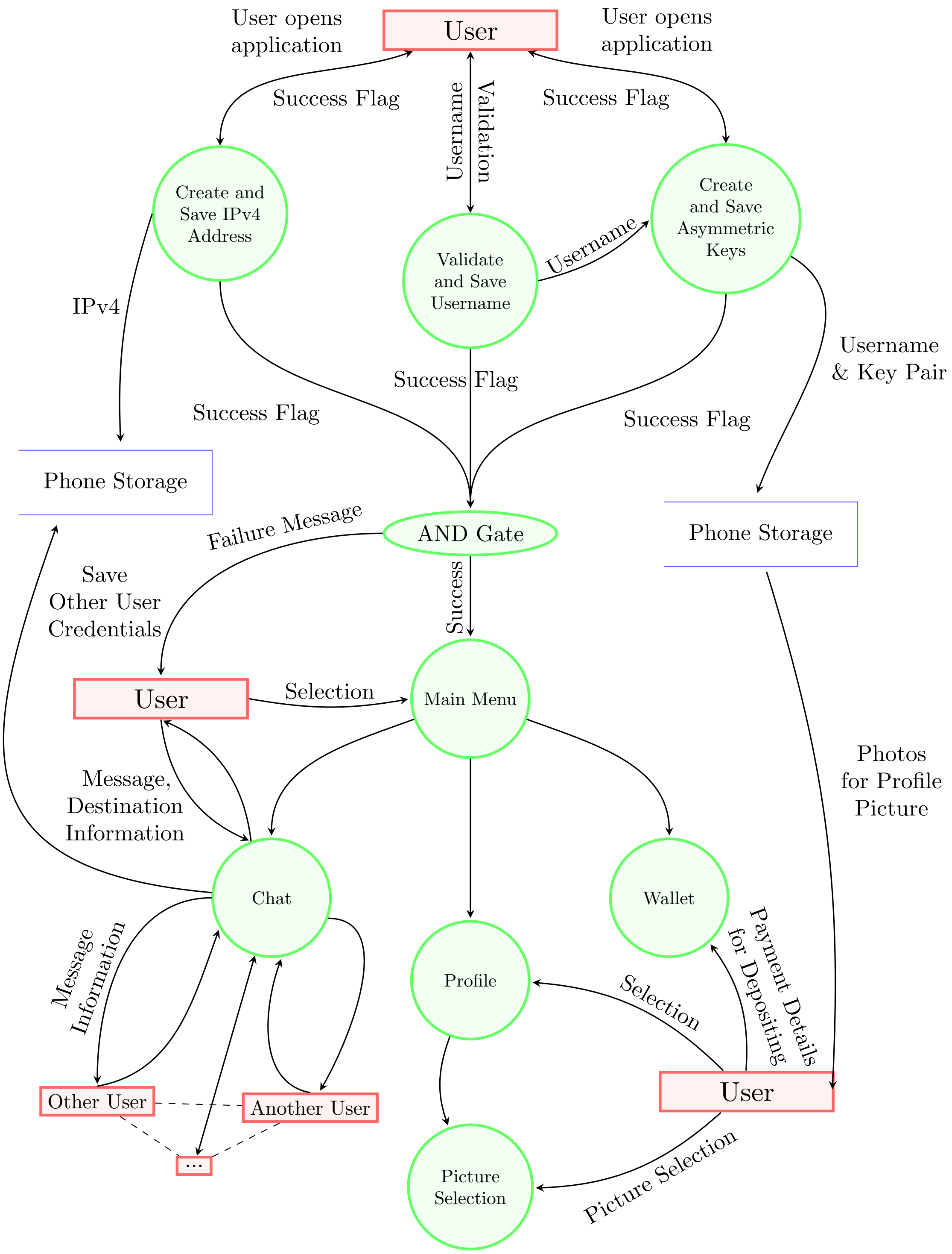

Message, Destination Information
Message, Route Request Packet, Destination Information, Public Key
User 1 (Sender)
Nodepaths
User 2 (Recipient)
Message, Destination Information, Route Reply (Shortest Path), Public Key
Message, Destination Information

Figure 2: Data Flow Diagram



### 1.4 Algorithms