|  |
| --- |
| Open Source Security |
| Security System |
|  |

|  |
| --- |
|  |

Contents

[Introduction 2](#_Toc152064062)

[Background Research 2](#_Toc152064063)

[What is a distributed system? 2](#_Toc152064064)

[Mechanisms of a Distributed System 2](#_Toc152064065)

[Zookeeper 2](#_Toc152064066)

[Mesh 2](#_Toc152064067)

[Dynamo 2](#_Toc152064068)

[Communication Methods 2](#_Toc152064069)

[I2C 2](#_Toc152064070)

[Wi-Fi 2](#_Toc152064071)

[UART 2](#_Toc152064072)

[GPIO 2](#_Toc152064073)

[Project Proposal 3](#_Toc152064074)

[Control Node – Keypad 3](#_Toc152064075)

[Function Overview 3](#_Toc152064076)

[Unlocking 3](#_Toc152064077)

[Locking 5](#_Toc152064078)

[Alarm Test 5](#_Toc152064079)

[Support 6](#_Toc152064080)

[Bugs 6](#_Toc152064081)

[Testing 7](#_Toc152064082)

[Limitations 7](#_Toc152064083)

[Application 7](#_Toc152064084)

[Dashboard 8](#_Toc152064085)

[New Nodes 8](#_Toc152064086)

[Communication System 9](#_Toc152064087)

[Jewelry Box Node 9](#_Toc152064088)

[Safe Node 9](#_Toc152064089)

[Bug Testing and Critical Reflections during integrations 9](#_Toc152064090)

# Introduction

Block diagrams

# Background Research

## What is a distributed system?

A distributed system “is one which component located at networked computers communicate and coordinates their actions only by passing messages” \*, this suggests the idea that distinct computing systems will need to communicate with one another in order to perceive what actions they need to do, and thus creating what is known as a distributed system.

Distributed systems are created from nodes, which are the fundamental building blocks of the distributed system, each node contains a constituent part of the overall system and contributes towards the goal of the system. Each node will contain primary code, which is specific to itself and then secondary code, which may also be referred to as middleware, this code is common across the entire system and is what allows the distributed system to communicate with one another.

Each node within a distributed system communicates with one another through the use of messages. Messages are segments of information that is passed between each node that instructs specific nodes or all nodes to complete a specific task, messages can also contain information which allows for the distributed system to keep all of its nodes up to date with one another.

## Formats of a Distributed System

There are many different formats in which a distributed system can occur in, in this section only two formats have been discussed, as they were the proposed formats for this project.

### Zookeeper

Zookeeper, as the name suggests, has a master node, ‘the zookeeper’, and slave nodes, ‘the animals’. The master node is in place to ensure that all the information within the distributed system is kept up to date, and that each node knows what it is doing. It has strong consistency; this is because the master node will ensure that all the nodes are constantly up to date.

The master node will control everything, but as previously stated, every slave node will have a copy of the master node, for the purpose of portioning, if it occurs. Partitioning will occur in the case of the project if the master node or any of the slave nodes go down, if it is the master node that goes down, then the slave nodes need to select a new master node, and to be able to do this each node must have a copy of everything on itself, which is again known as the middleware.

### Mesh

A mesh is a leaderless system, in which every node communicates with every other node within the system. It is highly effective as it does not require a master, therefore if any of the nodes go down then the other nodes will be able to continue as if nothing has happened. An advantage to a leaderless system, is that every node does not need to be connected to the master, and there can be chains of nodes within a mesh system, which allows for greater range of the distributed system.

Meshes fully support partitioning as well, as every node will contain middleware which allows it to dynamically communicate with other nodes in the network. Finally, there is eventual consistency between each node within the mesh distributed system, as it will take a couple of clock cycles for all of the information to be replicated across the entire network.

## Communication Methods

To be able to send information from each node within a distributed system to one another, there has to be standardized methods of communication, for the purposes of our project, this comes in the form of I2C, Wi-Fi, UART and GPIO pins. Each of the communication methods used are discussed below and the reasonings to why they have been used.

### I2C

Inter-Interconnected Communication is a communication standard, which is commonly used in electronics to communicate between peripherals and the microcontroller. It is effective as it is bidirectional, meaning that the master can receive and transmit information between slave devices. This communication protocol also only contains 2 connections, with being the System Clock and System Data connections. This method is synchronous, meaning that the data has to be times correctly otherwise it may not be read or transmitted correctly.

### Wi-Fi

Wireless Fidelity or Wi-Fi for short, is used to interconnect electronics between one another without a wired connection, it is primarily used to interface with the internet, however, can also be used to create a local network, or mesh, as seen within this project.

### UART

Universal Asynchronous Receive Transmit, is another older communication standard which is commonly used in electronics to upload code to boards. It is asynchronous meaning that there is no need for clocks to synchronize the information, instead this protocol employs buffers to contain the information until it is suitable for the microcontroller to receive it, e.g. on a clock edge. This means that information can be received at any point in time and it wont be affected by not being received on a clock edge.

### GPIO

This is the most basic form of communication method. GPIO stands for General Purpose Input Output, and is used to send and receive information, e.g., PWM, analogue and Digital On/Off signals. It is used in this project to notify the 5V logic level system of on off signals that cannot be send back through the voltage divider from the 3.3V logic level system within node 1. It is also within various nodes to receive information from sensors that do not employ any other communication protocol.

# Project Proposal

# Control Node – Keypad

## Function Overview

A close-up of a computer

Description automatically generatedNode 1 is one of the main interfaces between the end user and the system. The main function of this node is to provide a terminal that the user can input a code to disarm the system, so it doesn’t go off in the day when you’re just walking around the area. This node has a 16 key keypad and a display screen for inputs and visual prompts, these prompts are the unlocking function to disarm, a locking function when unlocked to rearm the system, an alarm sound test to make sure the systems alarm is working, a network function to test if it is connected to the other nodes, and a help function that shows a website and a phone number to contact for help.

### Unlocking

A computer screen with wires and a keypad

Description automatically generatedWhen the system is wanted to be unlocked the user can go to the terminal as seen in the photo below. The system will show text asking for a password to be inputted, this password can be a mix of numbers 0-9 and letters A-D, for the testing the password was ‘123A’ but the password can be any number of characters long.

A small electronic device with a blue screen

Description automatically generatedA small electronic device with a blue screen

Description automatically generatedA close up of a circuit board

Description automatically generatedIf the password is inputted correctly then a welcome screen is shown followed by the menu for further actions, shown below. These actions allow for further control and testing of the system.

A finger on a finger pressing a blue screen

Description automatically generatedA finger pressing a keypad on a small rectangular device

Description automatically generatedA finger touching a small rectangular device

Description automatically generatedOn the other hand, if the password is inputted incorrectly, the system will tell you this and tell you then there are 2 more attempts allowed. If the password is correct on any of these other attempts, the system carries on as normal. But if the password is inputted in wrong 3 times in a row, the system will go into warning mode. As seen in the image below, this means there is a countdown that gives the chance for one more attempt of the password, but if the password is wrong again, or the timer runs out, then the alarm sounds, a code is sent to the cloud to alert it something is wrong, and the keypad system locks up.

### Locking

A small green electronic device with a blue screen

Description automatically generatedOnce unlocked the user has the option to relock the system with one button press. As seen in the image below, the option on the menu shows up as ‘Lock’ press it and the system goes back to asking or a password. This function allowed the user to easily arm the space that its installed in, protecting the building and themselves. The system is built to be more problematic to unlock than lock, for security reasons.

### Alarm Test

A finger on a computer screen

Description automatically generatedIncluded in the menu is an alarm test, much like a smoke alarm, every now and then you’ll want to test if the alarm is working. It sounds the alarm for a few seconds, enough to know it works, then turns off.

### Support

A close up of a computer

Description automatically generatedThe last option on the menu list is simply a help page with the website link on it and a phone number to contact a help line for the system.

## Bugs

For Bugs for integration, see Bug Testing and Critical Reflections section.

For Node 1 there were many bugs that needed to be fixed, as show in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| Node | Problem | Description | Solution |
|  | A-B Password Ending | If the password ended in either A or B, the corresponding option would be selected in the proceeding menu. | Clear the key pressed queue after unlocking. |
|  | Debounce | A single press of a key would result in ~30 inputs of the pressed key. | A delay was added after every button press to avoid multiple inputs being received. |
|  | Infinite locking loop | Locking the system would result in an infinite loop if the password ended in A. | Solved when the previous bug-fixes were introduced, as the combination of them resulted in the first menu option (Lock) always being selected. |
| Control Pad (1) | Alarm spam | Pressing enough keys would eventually stop the alarm. | The inputs would act as another attempt on password, when 3 attempts were made, the timer reset. |
|  | Fake timer (display) | During/after the lockdown timer, password attempts could still be seen on the LCD. | Introducing a full lockdown mechanism disabled the keypad, not allowing any further inputs during alarm phase. |
|  | Fake timer (function) | Entering the correct password after the alarm started would unlock the system. | After Lockdown has initiated, the only method to stop is using an external device (cloud). |
|  | Alarm crash | Introducing a second timer during the alarm phase would crash the system. | While not confirmed, it is believed either the testing board only had one timer, or the library only allowed for one timer.  Code was re-developed to only require one timer. |

## Testing

MAKE A TESTING TABLE

Vigorous testing was performed on the node to make sure all functioned as well as expected.

We tested getting the password wrong many times, to get the security alarm to go off.

We tested getting the password wrong, but getting it correct at each step-in order. Once the wrong password section was done, we tested getting the password right, then locking the system and then getting it wrong again to check that the system did work as intended and still alarmed once locked.

We tested the menu system, to make sure each option worked as intended, that the lock option locked and the help option showed the information.

We tested that the C and D keys moved the menu around.

We tested the alarm test.

## Limitations

# ~~Application~~

~~This section of the documentation describes the purpose of Application. The Application (“App”), is a fundamental part of the distributed system, providing a crucial way of monitoring and controlling the security system from a remote location. The App is split into three main sections: Dashboard, New Nodes, and Information.~~

## ~~Dashboard~~

~~A screenshot of a computer

Description automatically generated~~

~~<Figure Caption>~~

~~The above figure demonstrates the overview that is seen on the dashboard. The main component of this page is the table which displays if the node is active, the Node Name, addresses and if the Node Alarm is active. The Update button allows the consumer to effectively update the node list to check if there are any changes to the node, the list will only update automatically when the Node alarm changes from “Neutral” to “Active”.~~

## ~~New Nodes~~

~~A screenshot of a computer

Description automatically generated~~

~~<Figure Caption>~~

~~This section works by entering the details of the node, and then submitting them, to create the node, deleting them, to delete the node, or Update node, to update the node. How this works is explained in more detail in the communication system section of this documentation.~~

# Communication System

This section of the project is not easily seen when viewing the security system, it is effectively the middleware of the project, this is because it is found on all the devices but is not easily seen when looked at.

As with every node within this project, the solution did not come easy, the original proposal was to have multiple nodes communicating with the cloud and communicating with one another, via a zookeeper system. The cloud system was able to be connected to but took up a lot of the processing power and storage space on the ESP boards.

The zookeeper system would have used the Wi-Fi to also communicate with one another, however this bought on problems as well, such as not being able to know the IP addresses of each node before they connect, meaning that they did not know what the IP address of the master would be. The problem was attempted to be solved using nRF chips, which would connect to one another without the need for a known IP address, which is only dynamically created on connection, instead it was a static address, which could be hard coded in beforehand, theoretically allowing for the communication between each of the nodes. However, the nRF chips were difficult to communicate with for unknown reasons. Therefore, it was chosen to abandon the zookeeper system for the time being and instead use a mesh network, which gave a few advantages of:

* Not needing an IP address and instead using the Wi-Fi chipset’s static MAC address.
* Not needing additional hardware as the ESP’s already had Wi-Fi chips on them.
* Being a format of distributed system, meaning that the zookeeper was additional none needed work.

Finally, it was also decided to not connect the network to the cloud, as the cloud expired and would lead to security risks if it was to be used in a real-world environment. Once the project had got the wireless communication mesh working, through the use of libraries such as PainlessMesh. The next major problem was communicating between the boards, as PainlessMesh was an ESP only library at the time, it meant that the project could not use the Arduino Uno R4 WiFi as a communication point, instead the project had to employ another route, which included connecting the Arduino Uno to an ESP board. This gave problems due to the fact that they do not use the same logic level, this being the Uno is on 5V, and the ESP being on 3.3V. The initial idea was to use a Logic Level shifter, which did not work at the time, therefore it was instead decided to use a voltage divider with a 2k2 and 1k resistor. The communication, however, did not work still. This was later found to be due to using Serial.write() instead of Serial.println() and trying to use Serial.swap() on the ESP board. After changing both sides to SoftwareSerial and changing the Serial.write() to Serial.println() the boards started communicating with one another. To communicate back to the 5V Arduino from the 3.3V ESP, the project had to employ a clever route of using the digital Out pins on the ESP and reading the Digital signal through the Arduino’s Analogue pins, as they would be able to read voltages less than 5V. Once a level had been set the boards were able to communicate with one another and generate pulses to turn on and off the alarm system.

A mesh network has different topologies, depending on the arrangement in space and additional factors such as traffic patterns. In the case of the project, the topology of the mesh network will be a ‘Full mesh topology’, in this format, all of the nodes are connected to every other node, which increases stability and if one of the nodes go down, it does not affect the other nodes, this would be more likely to occur in a ‘partial mesh topology’ due to the fact that every node is not connected to every other nodes, and instead chains are created, this would occur if the network was spread out in a line and all of the nodes were not close to one another. This has the risk of cutting off entire sections of the node network, if one or more nodes that connected a section the rest of the node network went down.

# Jewelry Box Node

# Safe Node

# Bug Testing and Critical Reflections during integrations