**aMAZE-RT: Secure Management for OpenWRT**

|  |
| --- |
| A Project Report Presented to  The Faculty of the College of Engineering |
| San Jose State University In Partial Fulfillment Of the Requirements for the Degree  **Master of Science in Software Engineering** |
| By |
| Ginto George, Binu Jose, Sandeep Panakkal, Nabin Thomas |
| December/2020 |

|  |
| --- |
| Copyright © 2020 |
| Ginto George, Binu Jose, Sandeep Panakkal, Nabin Thomas |
| ALL RIGHTS RESERVED |

|  |
| --- |
| **APPROVED** |
|  |
| Prof. Kaikai Liu, Project Advisor |
|  |
| [Program Director’s Name], Director, MS Software Engineering |
|  |
| [Department Chair’s Name], Department Chair |

ABSTRACT

aMAZE-RT: Secure Management for OpenWRT

By Ginto George, Binu Jose, Sandeep Panakkal, Nabin Thomas

A router is a device that helps to interconnect two or more networks, by forwarding data packets between them [1]. Home and Small office networks typically connect to the internet via consumer-level Wi-Fi routers, which provide wireless access points to the devices at home and route packets to the modem.

Typical consumer routers have locked firmware which restricts the functionality to whatever the device manufacturer decides to include. Open Source software stack like OpenWRT (Open Wireless Router) can be used to enhance the functionality and device security of consumer and custom Wi-Fi routers. Management of OpenWRT based devices is done using a browser or command-line interface. While this may work for the tech-savvy, a large majority of users may not be comfortable managing their devices this way. Some consumer-level devices have moved towards mobile app-based management, but OpenWRT lacks a mobile app-based router management functionality.

In this project, we plan to develop an end-to-end secure software to manage routers using a mobile application, with a customized version of OpenWRT, a mobile app as the front end, and an optional cloud-based management system for communication. The app provides features like monitoring and managing connection attempts with the notification on the mobile app via the cloud. Mobile App shall manage router connection attempts as an additional authentication factor on top of the Wi-Fi user authentication, enabling Multi-Factor Authentication. We also plan to port the major features of the LuCI web-based management tool for OpenWRT to the App, such as Access Control, package management, real-time monitoring, etc.

|  |
| --- |
| **Acknowledgments** |
| The authors are deeply indebted to Professor Michael Tjebban and Advisor Professor Kaikai Liu for their invaluable comments and assistance in the preparation for this project. |

**Table of Contents**

[Chapter 1. Project Overview 1](#_Toc56542778)

[Introduction 1](#_Toc56542779)

[Proposed Areas of Study and Academic Contribution 2](#_Toc56542780)

[Current State of the Art 2](#_Toc56542781)

[State-of-the-Art Summary 5](#_Toc56542782)

[Project Justification 5](#_Toc56542783)

[Chapter 2. Project Architecture 7](#_Toc56542784)

[Introduction 7](#_Toc56542785)

[Architecture Subsystems 7](#_Toc56542786)

[Chapter 3. Technology Descriptions 9](#_Toc56542787)

[Client Technologies 9](#_Toc56542788)

[Mobile App 9](#_Toc56542789)

[I. Android SDK 9](#_Toc56542790)

[II. JSCH 9](#_Toc56542791)

[AmazeRT Agent 9](#_Toc56542792)

[Python with Websockets 10](#_Toc56542793)

[UUID 10](#_Toc56542794)

[Middle-Tier Technologies 11](#_Toc56542795)

[App Engine 11](#_Toc56542796)

[Cloud Function 12](#_Toc56542797)

[Websockets with TLS for security for device to App Engine communication 12](#_Toc56542798)

[Data-Tier Technologies 12](#_Toc56542799)

[Secure Data Storage 12](#_Toc56542800)

[FireBase RealTime Database 12](#_Toc56542801)

[File Encryption for App data storage 13](#_Toc56542802)

[Chapter 4. Project Design 14](#_Toc56542803)

[Mobile App 14](#_Toc56542804)

[App Login UI 14](#_Toc56542805)

[Device Registration UI 14](#_Toc56542806)

[Device Settings UI 14](#_Toc56542807)

[Device Status UI 14](#_Toc56542808)

[OpenWRT device software 14](#_Toc56542809)

[Registration and Installation 14](#_Toc56542810)

[Heartbeats 14](#_Toc56542811)

[Status Updates 14](#_Toc56542812)

[Device Configuration Management 14](#_Toc56542813)

[Failure Handling 15](#_Toc56542814)

[Business Logic 15](#_Toc56542815)

[Websocket 15](#_Toc56542816)

[AppEngine 15](#_Toc56542817)

[Cloud function 15](#_Toc56542818)

[Secure Data Storage 15](#_Toc56542819)

[Shared Configuration Database 15](#_Toc56542820)

[Device Registration data on Mobile app 15](#_Toc56542821)

[Chapter 5. Project Implementation 16](#_Toc56542822)

[Mobile App 16](#_Toc56542823)

[App Login UI 16](#_Toc56542824)

[Device Registration UI 16](#_Toc56542825)

[Device Settings UI 16](#_Toc56542826)

[Device Status UI 16](#_Toc56542827)

[OpenWRT device software 16](#_Toc56542828)

[Registration and Installation 16](#_Toc56542829)

[Heartbeats 16](#_Toc56542830)

[Status Updates 16](#_Toc56542831)

[Device Configuration Management 16](#_Toc56542832)

[Failure Handling 16](#_Toc56542833)

[Business Logic 16](#_Toc56542834)

[Websocket 16](#_Toc56542835)

[AppEngine 16](#_Toc56542836)

[Cloud functions 16](#_Toc56542837)

[Secure Data Storage 17](#_Toc56542838)

[Shared Configuration Database 17](#_Toc56542839)

[Device Registration data on Mobile app 17](#_Toc56542840)

[Hardware platform 17](#_Toc56542841)

[Chapter 6. Testing and Verification 18](#_Toc56542842)

[Testing Process 18](#_Toc56542843)

[Mobile App 18](#_Toc56542844)

[OpenWRT Device Software 18](#_Toc56542845)

[Business Logic 18](#_Toc56542846)

[Database testing 18](#_Toc56542847)

[Test results 18](#_Toc56542848)

[Chapter 7. Performance and Benchmarks 19](#_Toc56542849)

[Scalability 19](#_Toc56542850)

[Throughput 19](#_Toc56542851)

[Reliability 19](#_Toc56542852)

[Feature Parity 19](#_Toc56542853)

[Chapter 8. Deployment, Operations, Maintenance 20](#_Toc56542854)

[Business Logic 20](#_Toc56542855)

[Cloud Functions 20](#_Toc56542856)

[App Engine 20](#_Toc56542857)

[Android App and Device software 20](#_Toc56542858)

[Android App Stores 20](#_Toc56542859)

[Packaging device software 20](#_Toc56542860)

[Secure Database operations 20](#_Toc56542861)

[Firebase Realtime Database 20](#_Toc56542862)

[Local App database 20](#_Toc56542863)

[Device data storage 20](#_Toc56542864)

[Github repository 21](#_Toc56542865)

[Chapter 9. Summary, Conclusions, and Recommendations 22](#_Toc56542866)

[Summary 22](#_Toc56542867)

[Conclusions 22](#_Toc56542868)

[Recommendations for Further Research 22](#_Toc56542869)

[Glossary 24](#_Toc56542870)

[References 25](#_Toc56542871)

[Appendices 26](#_Toc56542872)

**List of Figures**

[Figure 1 Typical Configuration of Home Network 1](#_Toc56540852)

[Figure 2 LuCL Web App UI – 1 3](#_Toc56540853)

[Figure 3 LuCL Web App UI – 2 4](#_Toc56540854)

[Figure 4 LuCL Web App UI - 3 4](#_Toc56540855)

[Figure 5 Project Architecture 7](#_Toc56540856)

[Figure 6 Cloud Architecture 11](file:///C:\Users\bjose\Documents\binu\MSPRJ\amazert\Learn\PrjReport\CMPE_295B_Final_Project_Report.docx#_Toc56540857)

**List of Tables**

[Table 1 Glossary 22](#_Toc55386090)

# Project Overview

## Introduction

* + 1. A router is a device that interconnects two or more networks, by forwarding data packets between them [1]. Routers can interconnect multiple public networks on the internet, such as the ones used in the internet backbone and interconnections between internet service providers [1]. Internet access in small offices and home environments typically is done via a broadband modem that connects to the public internet via the Internet Service provider. On the internal network, multiple devices may share the internet connection by using a wireless router, which interconnects the local network to the public network via the broadband modem. Figure 1 - Typical Configuration of Home Network shows how a typical home network connects to the internet using a wireless router.
  1. **Diagram

     Description automatically generated**

Figure Typical Configuration of Home Network

The consumer router market comes with a plethora of brands and models supporting varying hardware and software features. They often restrict the user with locked firmware limiting the features and functionality to a subset of possible features, as conceived by the device manufacturer. Like in the case of many commercial software products, Open Source software stacks provide an alternate option to enhance the functionality and security of consumer routers. OpenWRT is such an Open Source Linux based Wireless router firmware. OpenWRT supports a wide range of hardware. There are many commercial products available based on OpenWRT. Customers can add packages to enhance the functionality of the router. OpenWRT devices provide web-based administration that provides very advanced configuration and management functionality. This would not work for a large majority of novice users who would find it hard and technically demanding to manage their devices this way. There are only a handful of consumer-oriented devices that have ventured towards mobile application-based device management. This is one area that OpenWRT falls behind and even a basic mobile application-based router management functionality will benefit all the consumers in a big way. The trend towards using mobile apps for everything has made routers with mobile App based management more appealing for a large group of users, who would otherwise not even bother to configure the router with the web-based management tools [2].

## Proposed Areas of Study and Academic Contribution

Need to add relevant information here.

## Current State of the Art

OpenWRT firmware is based on the Linux operating system. The system provides a shell (ash shell) for running commands for making configuration changes. The fact that this is based on Linux makes it easy for extending the functionality, unlike other firmware options. OpenWRT provides a standardized way of implementing enhancements, called packages [3]. Each package is analogous to an application that can be installed on the device, extending its functionality. OpenWRT community also develops and maintains a list of around 3500 packages [4]. A Web-based management interface is provided which can be installed as a package on the device [2]. like art is currently supported in a wide range of router hardware. OpenWRT provides LuCI Web-based user interface for router administration and monitoring [5]. The UI is a bit complex to manage and operate for most of the home consumer router users. The following figures give a glimpse of the complex UI from OpenWRT

* 1. Graphical user interface

     Description automatically generated

Figure LuCL Web App UI – 1

* 1. A picture containing graphical user interface

     Description automatically generated

Figure LuCL Web App UI – 2

* 1. Graphical user interface, application

     Description automatically generated

Figure LuCL Web App UI - 3

For the not so tech-savvy end-user, management via a Web-based UI can be an uninteresting task when it involves remembering the IP Address, requiring login every time an administration or monitoring task needs to be done. This also has a negative impact on the security aspect of the router, since the users are mostly unknown about who is connected to their network, or what apps are using most data. There exist some hobby projects that provide basic mobile app functionality, but they are limited to basic management functions, and do not have any cloud support.

### State-of-the-Art Summary

There is no doubt that OpenWRT is an excellent open-source alternative for router firmware, providing one of the richest sets of management and security tools. However, having only a command line or web-based management and monitoring interface is a deterrent for most consumers in the era of mobile apps.

## Project Justification

OpenWRT is a feature-rich open-source wireless router firmware. It has a rich set of features and together with the active community support and contribution makes it a leader in its arena. The OpenWRT software stack is well adopted by a wide range of hardware vendors. Despite the rich feature set and much-desired hardware adoption, there is one much-desired improvement to the software stack, a mobile management app. When it comes to management and monitoring interfaces, the lack of a mobile app for continuous monitoring and configuration management is the Achilles heel of the system. No matter how advanced the available web interface features are, their usage mandates a browser and logging in every time something needs to be checked. Mobile app-based configuration and monitoring can solve this drawback by providing a simple user-friendly management and monitoring interface. In this era of mobile apps for everything, the availability of an average mobile application-based interface would cater to most of the internet users of the world. OpenWRT lacks in this area with no serious mobile application-based management and monitoring solutions being developed.

The project aims to improve the user adaptability and adoption rate of the OpenWRT stack. This will be done by adding a mobile application-based interface to manage and monitor the OpenWRT router. Cloud-based support for real-time monitoring and management of the router will be added to further enhance the adoption rate and user-friendliness of the software stack. The result will be an OpenWRT based software stack that supports mobile app-based management and monitoring of OpenWRT routers.

# Project Architecture

## Introduction

Include introductory text plus a diagram.

Diagram

Description automatically generated

Figure Project Architecture

TODO: Redo the Diagram as vector

## Architecture Subsystems

The entire project is divided into 3 major architectural subsystems as below.

1. The Mobile App used to provide the front-end functionality
2. The software that runs on the OpenWRT providing status updates and handling configuration changes
3. The business logic to manage and handle communication between OpenWRT device and Mobile App, which runs on Google Cloud Platform
4. The Secure Shared Database which keeps track of the device settings and provides real-time notifications to Mobile App about configuration changes

# Technology Descriptions

Assume you audience is a skilled computer scientist that has some familiarity with technologies taught in the client/server program. The topics below are for a typical MS Software Engineering project. Adjust the topics in this chapter to meet the needs of your project.

## Client Technologies

### Mobile App

Android App on the mobile device side. The front-end app to configure and control the OpenWRT device. The functionalities include device registration, configuration, status update and notification handling.

1. Android SDK
2. JSCH

Android library used to securely copy files to and from the OpenWRT device and mobile app. Same library used to securely execute commands on the OpenWRT device from mobile app.

## AmazeRT Agent

AmazeRT Agent is part of the AmazeRT software that runs on the OpenWRT router device. This is installed during the initial setup and will continue to run in the background, handling communication with the Cloud Backend.

### Python with Websockets

Since OpenWRT Stack can run on a variety of hardware architectures, keeping the AmazeRT Agent independent of the underlying CPU architecture was required. To handle this, we chose to implement it using Python programming language. The AmazeRT Agent software's primary purpose is to handle the communication with the Cloud backend and process the requests forwarded to it from the Mobile App Client. This required a persistent communication channel to talk to the Cloud backend. For communicating with the Cloud Backend, websockets library was chosen since it provided a good infrastructure to handle custom communication protocols on top of the secure TLS layer.

Python also has extensive set of libraries that helps with rapid prototyping of the software, letting us focus on the actual functionality, rather than spending effort on the Lower-level libraries and utility functions. Though OpenWRT SDK provides more low-level libraries and frameworks for developing native applications for OpenWRT based devices, handling different CPU architectures required a lot more effort from developer's side. For the purpose of prototyping, we did not need such low level access to the OpenWRT stack. Due to these reasons, we chose not to use the OpenWRT SDK for the prototyping.

### UUID

Every device that is managed by the AmazeRT system will need to be uniquely identified. A UUID was chosen as an identifier for the device. UUID is a 128-bit number, that can be generated to be uniquely without a central database of all generated Ids [6]. AmazerRT agent also uses UUID to generate a secret password that is shared between the device and mobile app, for securing and validating sensitive data sent across them.

## Middle-Tier Technologies

WebSocket

[…]

Cloud

App Engine

Cloud functions

Figure Cloud Architecture

### App Engine

App Engine is an platform as service infrastructure provided by Google to host an application with out worrying about instance management, scaling, resource allocation etc. It is a Linux container hosted in google public cloud. In this project App Engine instance is used as middle tire facilitating the communication between the Amaze RT device and the mobile application. App Engine takes care of authentication and authorization between Amaze RT device and Firebase Database.

For the communication between WRT device and mobile App an AppEngine (a cloud linux container instance) instance with public websockets is used. WRT devices can connect to this well-known websocket urls to asynchronously talk to the app. This architecture gives the flexibility that, even if the mobile app is not running at that time the WRT device can establish a connection to the websocket and push its message.

### Cloud Function

Cloud functions are serverless computing infrastructures which can be used to invoke a function for a specific event or a trigger. It is used to publish database modifications to App Engine websockets which in turn push the message to corresponding WRT device.

### Websockets with TLS for security for device to App Engine communication

## Data-Tier Technologies

### Secure Data Storage

Mobile App will utilize local device data storage for device specific information.

### FireBase RealTime Database

Firebase RealTime Database is used to implement the cloud-based device state and event management across managed openWrt devices and their managing applications. The Firebase infrastructure provides User authentication and authorization for appropriate access control. It also provides event trigger and registration mechanisms to help implement the business logic.

### File Encryption for App data storage

The device registration data from the OpenWRT device are encrypted and saved locally on the mobile app.

# Project Design

## Mobile App

### App Login UI

Mobile App login will use the standard Android Auth library support.

### Device Registration UI

Mobile App initial device registration logic

### Device Settings UI

Mobile App provides support for managed openWrt device settings configuration.

### Device Status UI

Mobile App provides support for user to view current device status.

## OpenWRT device software

### Registration and Installation

Device registration and installation

### Heartbeats

Send and receive heartbeats

### Status Updates

Update device status

### Device Configuration Management

Manage device configuration

### Failure Handling

Handle failure conditions

## Business Logic

### Websocket

### AppEngine

### Cloud function

## Secure Data Storage

### Shared Configuration Database

Firebase Realtime Database used for openWrt router to Mobile App communication including router settings and status notification.

### Device Registration data on Mobile app

Mobile device local storage will be used as secure store for persistence and retrieval of openWrt device registration and authenticated user details.

# Project Implementation

## Mobile App

### App Login UI

### Device Registration UI

### Device Settings UI

### Device Status UI

## OpenWRT device software

### Registration and Installation

### Heartbeats

### Status Updates

### Device Configuration Management

### Failure Handling

## Business Logic

### Websocket

### AppEngine

### Cloud functions

## Secure Data Storage

### Shared Configuration Database

### Device Registration data on Mobile app

## Hardware platform

Raspberry Pi 4 was chosen as the HW platform for implementing the router side of software for ease of debugging and availability of enough RAM for running debug tools as needed. For the Android App side, a simulator running Pixel 2 was chosen as the base hardware for prototype testing.

# Testing and Verification

Describe your test strategy, process, and results for verifying the functionality of your project.

## Testing Process

### Mobile App

### OpenWRT Device Software

### Business Logic

### Database testing

## Test results

# Performance and Benchmarks

Describe any performance and benchmarking criteria you used for your project. In addition, describe any benchmarking results you observed in your project.

## Scalability

## Throughput

## Reliability

## Feature Parity

# Deployment, Operations, Maintenance

## Business Logic

### Cloud Functions

Cloud function is deployed in google cloud. When the cloud function is upgraded with new features google cloud updates it reliably without down time.

### App Engine

App Engine is deployed in google cloud as a compute instance. It provides a public IP and a persistent websockets based connection to the managed devices.

## Android App and Device software

Deployed on mobile per device, used for managing the device.

### Android App Stores

### Packaging device software

## Secure Database operations

### Firebase Realtime Database

Firebase RealTime database is used for the AmazeRT device to Mobile App communication.

### Local App database

### Device data storage

## Github repository

Contains all project artifacts.

# Summary, Conclusions, and Recommendations

## Summary

TODO: Reformat the content

Our original design was to use a Custom Linux server running on AWS for the Business logic processing. This changed to use a Google App Engine, Firebase and Cloud functions

With the updated design we could avoid the requirement of a public IP Address and an open port for listening for control requests from the server

The original scope for this project was too big to be completed within the timeframe we had, but we were able to trim down the set of features supported and make the end to end flow working. A framework was implemented to add new settings support with minimal change from the Device software. The UI would require more changes but can be redesigned to make it more data driven.

## Conclusions

1.Achieved all the revised project goals and implemented some of the stretch goals as well.

## Recommendations for Further Research

TODO: Reformat the content

Enhancement of this infrastructure to support device management for Edge computing devices, using Mobile app and the framework provided by the AmazeRT cloud and device management modules

* Extend with IOS application support with SwiftUI for User interface development
* Moving from Firebase to Firestore for the database
* Moving to Android Jetpack compose to design modern scalable UI.
* Redesigning the Android app for generating configuration and status screens using a data driven mechanism so that new features can be added with minimal efforts.
* Integrating this entire software suite with the open source OpenWRT codebase and making this a default install option for all OpenWRT devices.

# Glossary

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| API | Application Programming Interface |
| JSON | JavaScript Object Notation. JSON is a lightweight data-interchange format. It is easy for humans to read and write as well as for machines to parse and generate. |
| XML | Extensible Markup Language. |

Table Glossary

# References

[1]     "Router (computing)", *En.wikipedia.org*, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Router\_(computing). [Accessed: 05- May- 2020]

[2]  Instructables.com, 2020. [Online]. Available: https://www.instructables.com/id/AndroidiOS-App-to-Access-Your-OpenWrt-Router-Remot/. [Accessed: 30- Apr- 2020]

[3]   "OpenWrt Project: Packages", *Openwrt.org*, 2020. [Online]. Available: https://openwrt.org/packages/start. [Accessed: 01- May- 2020]

[4] "OpenWRT Packages", 2020. [Online]. Available: https://openwrt.org/packages/table/start. [Accessed: 05- May- 2020]

[5]"OpenWrt Project: Use SSH to connect to the internet and install Luci Web interface", *Openwrt.org*, 2020. [Online]. Available: https://openwrt.org/docs/guide-quick-start/ssh\_connect\_to\_the\_internet\_and\_install\_luci. [Accessed: 02- May- 2020]

[6] “Universally unique identifier”. https://en.wikipedia.org/wiki/Universally\_unique\_identifier, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Universally\_unique\_identifier [Accessed: 02-Nov-2020]

# Appendices