

Master Thesis

On

Development and Implementation of Secure Cloud Based Digital Signage System

## Informatik und Ingenieurwissenschaften, Fachbereich 2

Author:

Sameer Soni

Supervisor Prof. Dr. Christian Baun Co-Supervisor Prof. Dr. Thomas Gabel

# **Affidavit**

I hereby declare that I have developed and written the enclosed master thesis entirely on my own and have not used outside sources without declaration in the text. Any concepts or quotations applicable to these sources are clearly attributed to them. This master thesis has not been submitted in the same or substantially similar version, not even in part, to any other authority for grading and has not been published elsewhere. I know a misstatement may have serious legal consequences.

Sameer Soni

5 December 2023

# 

# **Thanksgiving**

https://www.christianbaun.de/hilfe\_abschlussarbeit.html

# 

# **Abstract**

* Put up numbers why digital signage system is very important to get attention to important details also for marketing products
* How it helps for the businesses and can help universities to increase students participation in various activities
* Should discuss how this research and software and system design discussed in this paper tries to achieve and its intended audience

# 

# **Introduction**

Product marketing plays a very important role in success or failure of a product and in some cases for a company. With right marketing strategy and customer targeting methodologies, interesting products, its features and offers can be passed to the customers in effective way which converts into higher sales, enhancing brand image and promotions. This strategy in the marketing world is known as *Upselling* and digital signage system is one of the tools of this strategy.

*Digital signage System* is one of the methodologies which is used heavy all over the world to target consumers with interesting offers and products. This method usually includes a digital screen (televisions / monitors), a player device, a content scheduling and controlling application. In the case of smart television, players devices may be replaced by an application running on the smart television. Now a days, it is difficult to find a company which is in business to customer segment and not using digital signage system for its product promotions and offers. Be it Aldi, Rewe or Burger King everywhere one can see these systems deployed and running catchy promotions.

There are several companies in the market which are providing solutions for this requirement. Some are providing systems and products which can be deployed in company infrastructure, and some are providing subscription-based services which is bases on pay on use model. Some of these companies are *Yodeck, LobbySpace, Optisigns* etc.

# 

# 

# **State of The Art**

* Describe the current state of research and what has been established so far in the form of solutions and products. This motivates you why it makes sense at all for you to develop your solution and write this work. Something new is supposed to be created, and for that you need to know what has been done in the field so far and where there is still a need for research. This chapter is extremely important , because you are not writing a project report that is only about your solution , but a scientific thesis and the classification in the state of the art is important. Specifically, this chapter should include:
  + A description of the criteria (e.g. functionalities, acquisition costs, compatibility with specific platforms) that you use to examine existing solutions.
  + A list of existing solutions that partially or fully meet the required requirements.
  + An examination of the existing solutions against the criteria you set up. This investigation should make it clear why you used a certain solution for your work, or why you developed a new solution.
  + A brief description of the technologies you use (e.g. hardware components, programming languages, protocols).

Requirements:

1. Cloud Based

Existing Solutions:

Yodeck:

LobbySpace:

OptiSigns:

Solution Evaluation:

On features terms:

|  |  |  |  |
| --- | --- | --- | --- |
| Features of Available Solutions | [yodeck.com](http://yodeck.com) | LobbySpace | OptiSign |
| Central Admistration |  |  |  |
| Cloud Based System |  |  |  |
| On Premise Offering |  |  |  |
| Content Scheduling |  |  |  |
| Multiscreen Support |  |  |  |
| Multiuser Support |  |  |  |
| Location Based Display Allocation |  |  |  |
| Status Monitoring |  |  |  |
| Offline Playback |  |  |  |

On offering & investment required terms:

|  |  |  |  |
| --- | --- | --- | --- |
| Offerings in market | [Yodeck.com](http://yodeck.com/) | LobbySpace | OptiSigns |
| Player Hardware | Raspberry Pi |  |  |
| Player Cost | $79 |  |  |
| Business Model | Subscription Based |  |  |
| Cost (screen/month) | $87 |  |  |
| Management App | Cloud Web App |  |  |
|  |  |  |  |
|  |  |  |  |

˜

On security terms:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Security Aspects | TLS1.2/TLS1.3 Communication | Mutual Authentication based on TLS | Hardware Temper Detection | Cryptograpic Key Storage HSM | Storage Encryption | Data/File Inegreity check | Outbound traffic |
| OptiSigns |  |  |  |  |  |  |  |
| Yodek |  |  |  |  |  |  |  |
| LobbySpace |  |  |  |  |  |  |  |

Conclusion of evaluation:

**Technologies used in the solution:**

**Hardware:**

**Raspberry Pi:**

Raspberry Pi are series of single board computers which are developed by raspberry foundation in association with Broadcom. These small boards have everything one can expect in a computer, and they are exceptionally cheap and produced in bulk which makes them idea choice for learning, teaching, prototyping and in a lot of cases actual use in products. These boards support a wide range of additional hardware which can be connected in available GPIO pins to provide additional functionalities to the system.

Board features a Broadcom system on chip (SoC) with integrated ARM compatible central processing unit and on chip graphical processing unit. It also features GPIO, I2C, SPI, UART, Digital In/Out, +5V, GND pins in 40 J8 pins available on the board. Board also features Wi-Fi, ethernet port and four USB ports. Depending on the version of the boards, it comes with HDMI/micro-HDMI, micro or type-c USB power supply.

Since 2012, several versions of raspberry pi models are introduced in the market in which most recent one is raspberry pi 5 model B which in offered in different configurations (mainly in terms of RAM) and can be chosen as per the requirements.

Raspberry Pi Pico, Raspberry Pi Zero and Raspberry Pi Compute modules are also available in the market, but we are only considering Raspberry Pi 5 model B which is currently latest to this date.

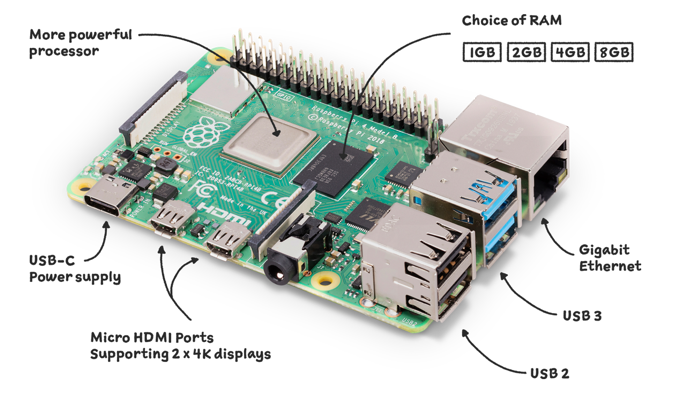
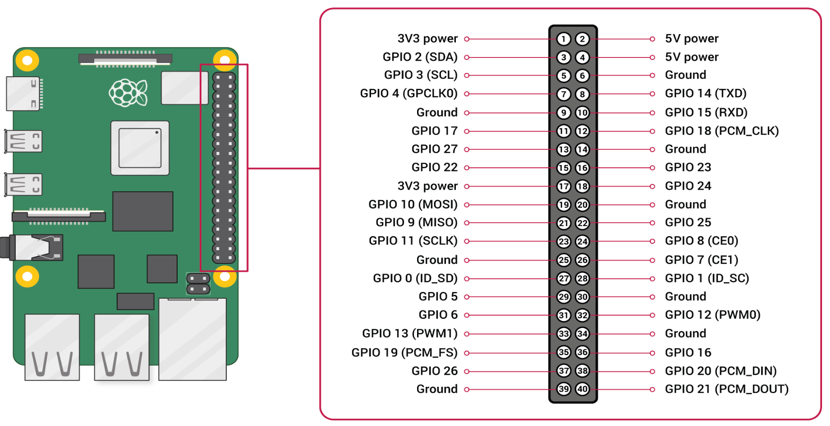


Image X: Raspberry Pi 5 Model B Image X: Raspberry Pi 5 Model B pin out diagram

Table X: Raspberry Pi 5 Model B Specification

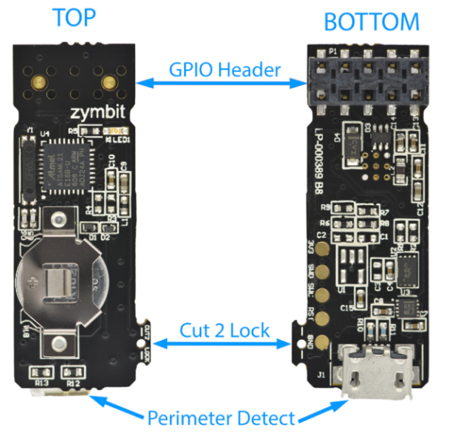
Model: Raspberry Pi 5 Model B

Processor: Broadcom ARM Cortex A76 64 Bit quad-code 2.4 GHz

RAM: 1 GB or 2 GB or 4 GB or 8 GB

Network: 802.11ac Wi-Fi, Gigabit Ethernet, BLE 5.0 low energy

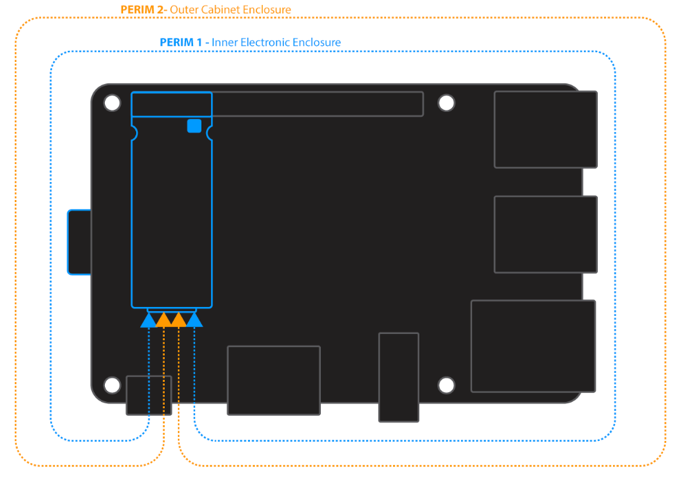
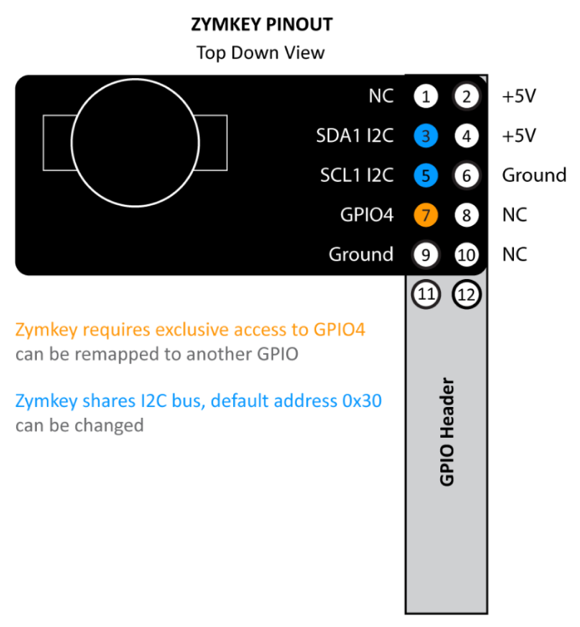
**Zymkey 4i**:

Zymkey 4i is a hardware security module for raspberry pi from Zymbit which provides several security features which are not available on raspberry pi by default. The main and most important feature is to provide hardware root of trust. Device is equipped with Atmel crypto engine for providing cryptographic services and key storage and generation capabilities. Below are main key features of the module.

Key Features:

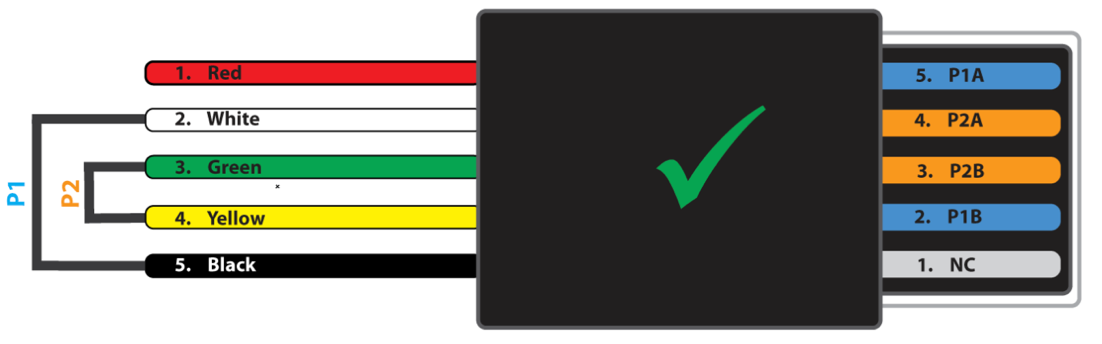
* Cryptographic engine
* Physical temper sensor
* File System Encryption
* Key Storage and Generation
* Real time clock

Device connects to the GPIO header of the SBC and uses the I2C bus and GPIO4 to communicate with the SBC CPU via an encrypted channel. This module is used in the solution described for crypto engine, private key storage, file system encryption and temper detection. So, this is very important system module.



**Micro USB extension cable:**

This is cable which is suitable and recommended to use with Zymkey 4i for perimeter tamper detection. This wire consists of five wires of which 4 are used for inner and outer detection. Image **x** shows how wires of this cable can be used for the perimeter detection.



**Monitor:**

**Software:**

*Programming Languages:*

***Golang:***

Golang is advanced statically typed, compiled high level open-source programming language, initially developed by Google, and has a big support and development community. Go syntax is like C/C++ and compiles to machine code and provides efficiency comparable to C/C++. It is considered easy to code, easy to understand and highly performant for networking and concurrent application. Golang has a lot of features which makes it an appropriate choice for development.

* Built-in support for concurrency and parallelism
* Garbage collection – automatic memory management, less risk of memory leaks
* Cross-Platform
* Statically typed.
* Highly scalable
* Faster development possible compared to C/C++

*Why Golang is chosen for implementation of described solution here?* The reasons are all above mentioned. Fast development of highly scalable concurrent servers was required which can support microservice architecture in case in future requirement arises. Also, I was important make code easy to read, understandable and modularized.

***Python:***

Python is a scripting, highly abstract programming language.

***ReactJS:***

ReactJS is popular open-source front end JavaScript framework for intuitive user interfaces used for website development. ReactJS is developed my Meta and maintained by Meta and community. Framework follows component-based architecture allowing developers for develop user interface based on components which modularize and allows reusability.

**Open-Source Software:**

**Nginx Web Server:**

Nginx is popular opensource web and application server for hosting web application. It is easy to configure product suit of several applications which comes in editions - community, and enterprise edition. Community edition is free and open-source suit which comes with web server, app server, reverse proxy, mail proxy modules. Web server is capable to handle mostly all kinds of internet protocols for example TLS/SSL, WebSocket, http, https, FastCGI or gRPC etc. Nginx async event driven architecture to handle request makes it exceptional performant and efficient and designed to handle concurrent connections keeping modern web requirements in mind. Below are some features of the web server.

* Ability to handle high simultaneous connections with memory footprint.
* Reverse proxy
* Load balancing
* TLS/SSL support via OpenSSL
* gRPC, HTTP1/2/3 support
* IPv6 Compatible

**CockroachDB Database:**

CockroachDB is opensource distributed SQL database which is built on a transactional and strongly consistent key-value pair. CockroachDB provide easy configuration and maintenance across multiple nodes across locations allowing automatic data replication and rebalancing which makes it resistant to disk, machine, datacenter crashes making it highly available and gives failover protection. CockroachDB provides SQL for structuring, maintaining and querying data. It is compatible to PostgreSQL database.

* Resiliency – distributed nature, automatic data replication, failover protection
* Scalability–Supports horizontal scalability by adding addition nodes on higher volumes.
* Geo-partitioning and multi region

**MinIO Object Storage:**

MinIO is open-source high performance object store. It is Amazon S3 compatible which can store unstructured data such as photos, videos, files etc. MinIO can be deployed on any kind of infrastructure for example public or private cloud, Kubernetes clusters, independent systems, or edge environments. Store also provides functionalities for active and multi-site replication for resiliency. Below are some features-

* Active-Active replication
* Identity and Access Management
* Encryption
* Monitoring

*Why MinIO is used in the solution?* It is appropriate open-source solution for storing content info files locally or on cloud. It is easy and quick to deploy and highly configurable.

**OpenSSL:**

OpenSSL is opensource library and software toolkit for general purpose cryptography and secure communication. It is widely used and trusted by applications communicating over internet. Library contains implementation for SSL and TLS protocols which essential for communications security.

**Visual Studio Code:**

Visual studio code, popularly known as VS code is free, open-source IDE from Microsoft available for MacOS, Windows, and Linux. It is one of the most popular easy to use tool for source code editing. It supports wide variety programming languages for example C, Cpp, Go, Python, and JS. VS code has built in run and debug features and supports extensions which allows community-based addition of features which is huge and has almost solution for every kind of needs.

**Libp11:**

Libp11 is an opensource library that provides a high-level interface to access PKCS#11 objects. Library provides standard API for cryptographic hardware devices such as hardware security modules and smart cards. It is used in applications which uses OpenSSL to access cryptographic keys from crypto engines following PKCS#11 standards.

**Protocols:**

**HTTPS:**

Hypertext Transfer Protocol Secure (HTTPS) is extension to HTTP protocol. It uses transport layer security encryption for secure communication over computer network. It is widely used protocol over internet to transfer data between web browser and web server. The main purpose of protocol is to provide protection of privacy and integrity of information traveling over network between two applications. This protection aspect is based on a trusted third party signing a digital certificate which is basis of authentication and encryption using public key cryptography.

**API:**

**RESTful:**

Device:

Raspberry pi based solution:

Physical device security:

Communication security:

Device data security:

Over-the-Air Firmware upgrade:

Over-the-Air OS upgrade:

Secure player enrollment:

Server:

Central display management:

Location based display allocation:

Content Scheduling:

Multi-Screen Display:

Media player monitoring:

On premise solution:

Cost of solution per screen:

Open source technologies:

Existing Solutions meeting criteria:

Drawbacks of existing solution:

# 

# **Design**

**Design Aspects:**

* Security
* Redundancy
* Availability
* Power Saving

**Requirements Analysis:**

1. User needs to display advertisement video on the monitors/televisions installed in its building across locations.
2. User should be able to control content displayed on monitor remotely.
3. User should be able to control schedule for content playback.
4. User should be able to monitor displays available in the locations.
5. System should be secure from physical as well as network attacks.

**Used Cases:**

**Solution Architecture:**

**Workflow:**

System workflow:

Factory or Tech Backoffice workflow:

This is where your personal contribution begins , and with it the main part of your work. Describe possible solutions and develop your solution. This also includes the reasoning why you developed your solution in this way and not in another way.

Features should be explored:

Secure boot

Physical device security

Drive encryption

Secure network communication

Firewall

Operation system upgrade

Firmware upgrade using docker containers

Outbound network

Workflows which can be included:

Pi based device factory production workflow

Device Installation and setup workflow

Device Registration workflow

Digital Signage System workflow

Device Deregistration workflow

Device decommissioning workflow

Also discuss current rinks to security and bottlenecks in the design

Factory Workflow:

This workflow can be used to produce raspberry pi based media players from back office or factory.

# 

# 

# Implementation

This is where you describe your implementation. Go into the important parts of your personal contribution. Longer (more than 1 page) source texts belong in the appendix.

Physical device security?

Disk security?

Communication security?

Application?

Build Your Own Certification Authority for Demonstration purpose:

# 

# Evaluation

This is where you evaluate the results of your work. Failures and their reasons are also results and you should describe them.

# <https://www.zymbit.com/zymkey/>

<https://docs.zymbit.com/getting-started/zymkey4/quickstart/#power-on-and-confirm-operation>

<https://docs.zymbit.com/tutorials/perimeter-detect/zymkey4/>

<https://www.nginx.com/products/>

<https://www.ibm.com/docs/en/linux-on-systems?topic=introduction-what-is-pkcs-11>

<https://github.com/OpenSC/libp11>

<https://en.wikipedia.org/wiki/OpenSSL>

<https://min.io/>

<https://en.wikipedia.org/wiki/MinIO>

<https://en.wikipedia.org/wiki/Visual_Studio_Code>

# Summary

# 

# Attachments