

# CSCI 3172 Web-Centric Computing

## Milestone 2

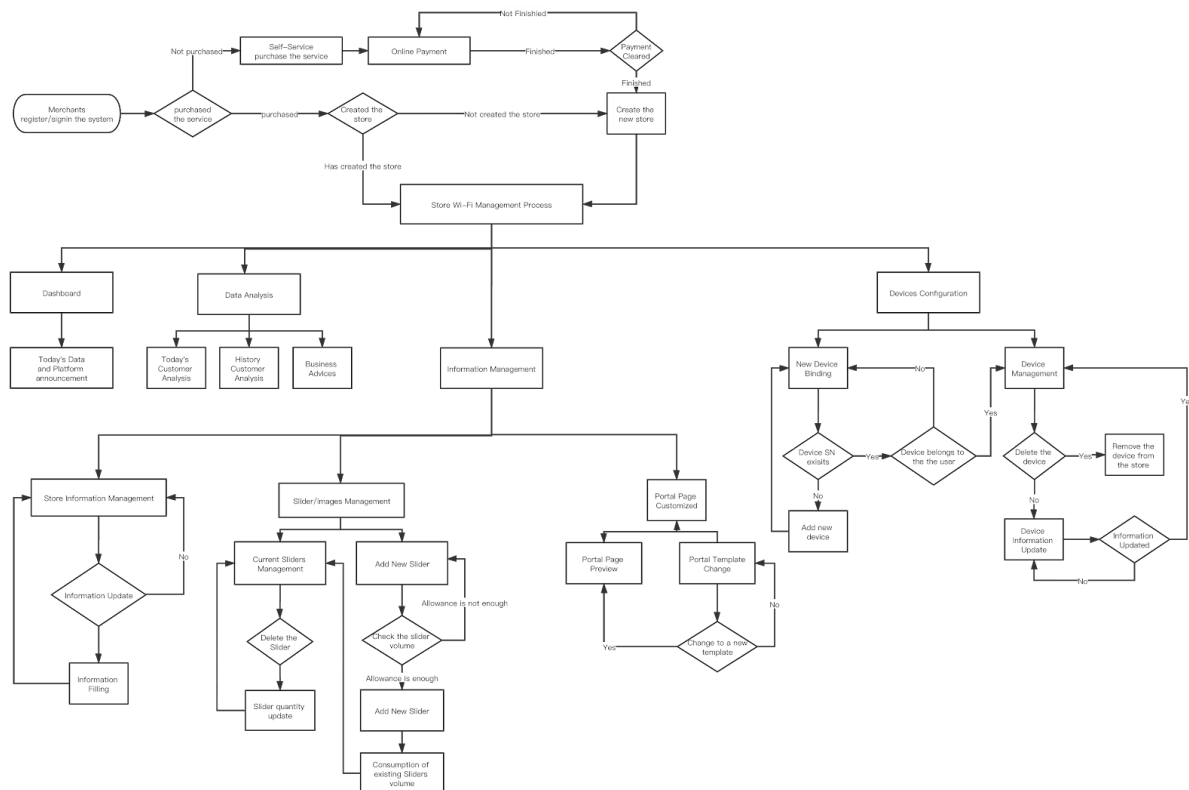
Guest Wi-Fi Management System

**Yanlin Zhu B00812966**

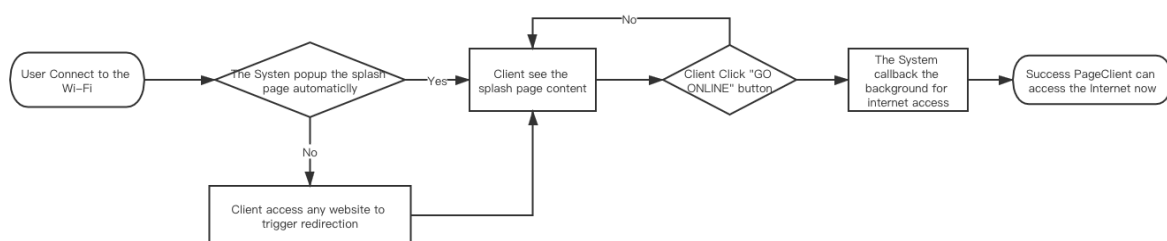
**Xinhai Cheng B00796386**

# Usability

## User Flow Chart



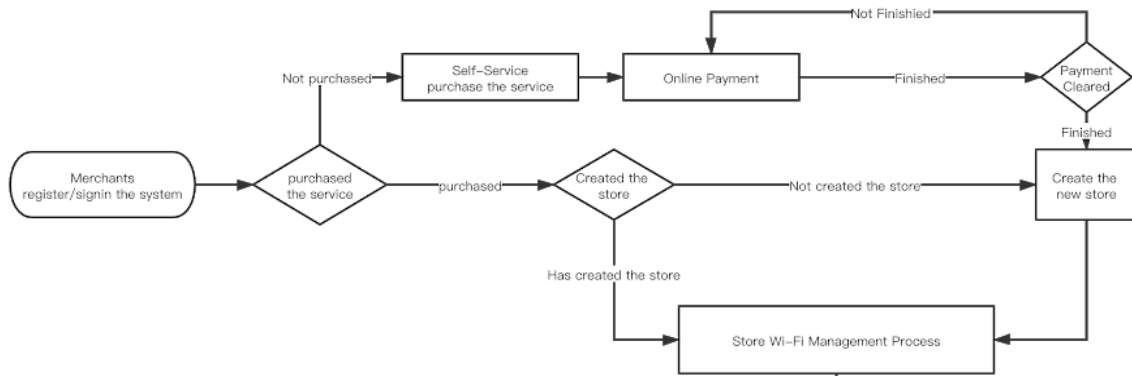
## Overview of our Application for Merchant Operation



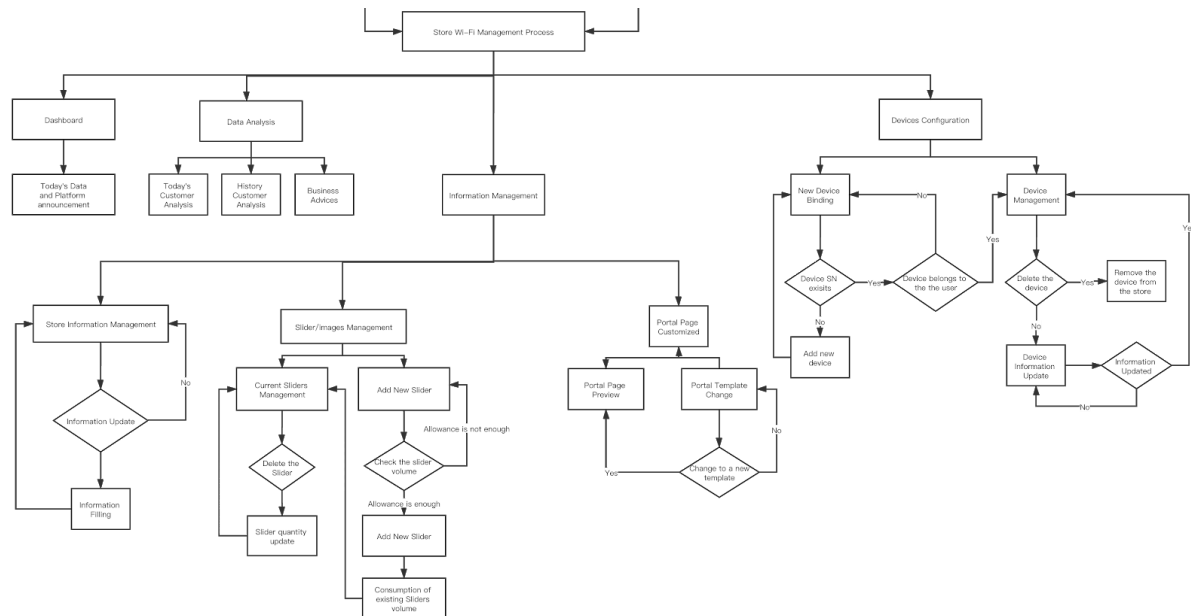
## Overview of our Application for Merchants' Customer WiFi Authentication

### Portal

## For a Vertical Customers (Merchants):

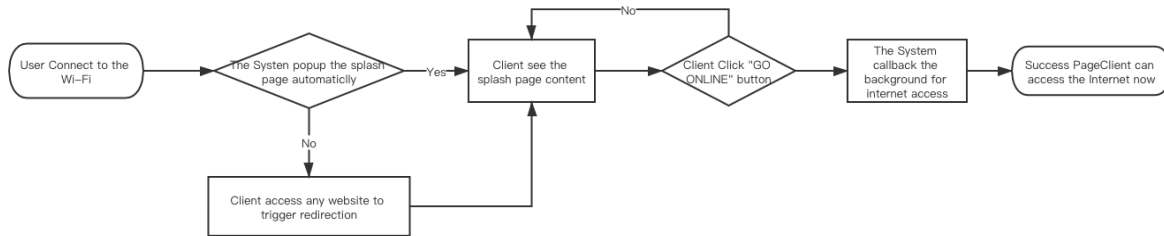


As shown in the figure, the first part is the user account and service packages check module. When the merchants complete the registration in the system, they can sign in to the merchant dashboard. The system will inquire the database to know whether the current user has the service purchase history or the store information that has been bound in the account. If this is the first time a merchant has registered or has not ordered any services, the system will automatically redirect the user to the service purchase page. The user selects the service plan they need and completes the payment through online payment. The system obtains the payment status of users through third-party payment platforms, such as Stripe or Paypal, and allocates corresponding packages for users. After the user opens the service package, the system will provide binding guidance for customers who are not bound to the store information, and help users fill in the store information and access the device by using Bring your own device (BYOD) method.



After completing the configuration of store information or equipment, users can use all the functions of the system. Users can view the latest announcements through the merchant dashboard to ensure that they can know the information and system status. At the same time, users can use the visitor data analysis function to view the big-data of current Wi-Fi visitors in real time. In addition, users can view the recent historical data and view the business optimization information given by the system. The information management function can help users to view and update the store information in real time. At the same time, users can also delete and upload pictures on Wi-Fi authentication pages to help merchants better promote their products. All information changes can be previewed through Portal page management, and templates can be switched through the Portal page management function.


## For a Horizontal Customers (Merchants' Customers):



When a horizontal customer (the merchant's customer) arrives at the merchant's store to consume and use the network, it will first turn on the device's Wi-Fi Settings, select and connect to the merchant's public wireless network. After connecting to the network, with hotspot protocol, the system will automatically pop up the splash page window. If the system does not have a pop-up window or the user accidentally closes it, the user needs to reconnect to Wi-Fi or open the browser to access any website to be redirected to the splash page. Once the users are redirected to the splash page, they can complete the Internet connection operation by clicking the "GO ONLINE" button on the page. After the user clicks the button, the system sends the authentication request to the back-end service, and the back-end service receives the request and forwards it to the device. Then the user will be redirected to the success page, so that can browse the Internet normally.

## Personas and Scenarios

### Persona 1

	<b>Name: Chang</b>	<b>Role: System Administrator</b>
<b>Demographics</b>	<ul style="list-style-type: none"> <li>· Age: 25 years old</li> <li>· Familiar with Web development and system maintenance</li> <li>· With bachelor's degree in CS</li> </ul>	
<b>Bio</b>	<p>Chang is a 25-year-old man who has a bachelor's degree in Computer Science. He started working for Store WiFi Management System Company as a system admin for 3 years after graduating from university.</p>	
<b>Responsibility</b>	<ul style="list-style-type: none"> <li>● Check if auto authentication for merchants works fine</li> <li>● Help new merchant install WiFi device</li> <li>● Solve merchants' problems on request</li> </ul>	


Chang is a 25-year-old man who has a bachelor's degree in Computer Science. He started working for Store WiFi Management System Company as a system admin for 3 years after graduating from university. His responsibility is to monitor the system status including checking auto authentication to those merchants who subscript our service and have made

payment in full, help merchants install our WiFi devices, solve merchants' problems on request.

### Scenario

After Chang started working, he checked the system status to make sure everything works fine and there is no error reported by the system. He noticed there is a new merchant who just subscribed our service yesterday and requested an install WiFi device service scheduled at 4 p.m. He went to the merchant's store on time and helped the merchant install a WiFi device and set the information on the user portal page.


### Persona 2

	<b>Name: Kim</b>	<b>Role: Owner of a restaurant</b>
<b>Demographics</b>	<ul style="list-style-type: none"> <li>· Age: 35 years old</li> <li>· Unfamiliar with any web or network technologies</li> </ul>	
<b>Bio</b>	<p>Kim is a 35-year-old man who owns a Korean restaurant. He was frequently asked by customers for WiFi password through he stuck a paper with password on the wall. Also, he wants to let people know what is recommended without asking during busy time. Therefore, he wants to use the WiFi authentication system.</p>	

<b>Goals</b>	<ul style="list-style-type: none"> <li>• Let users connect to WiFi by themselves without asking</li> <li>• Have a prompt on his recommended cuisine while users connecting to WiFi</li> <li>• Have some experts install and set up the WiFi system for him</li> </ul>
--------------	---

Kim is a 35-year-old man who owns a Korean restaurant. He is unfamiliar with technologies so he prefers to have some experts to help him handle technology related things. He was frequently asked by customers for WiFi password through he stuck a paper with password on the wall. Also, he wants to let people know what is recommended without asking during busy times. Therefore, he wants to use the WiFi authentication system.

### Persona 3

	<b>Name: Henry</b>	<b>Role: Customer of a restaurant</b>
<b>Demographics</b>	<ul style="list-style-type: none"> <li>· Age: 30 years old</li> <li>· Unfamiliar with any technologies</li> </ul>	
<b>Bio</b>	Henry is a 30-year-old man who just entered a restaurant that he is not familiar with technologies. He wants to ask for the WiFi	



	password but all the waiters are busy. He is not familiar with this restaurant so he wants to know what is recommended.
<b>Goals</b>	<ul style="list-style-type: none"><li>● Connect to WiFi without asking during busy time</li><li>● Know what is recommended for a unfamiliar restaurant</li><li>● WiFi authentication system is simple and easy to use</li></ul>

Henry is a 30-year-old man who just entered a restaurant that he is not familiar with. He wants to ask for the WiFi password but all the waiters are busy. He is not familiar with this restaurant so he wants to know what is recommended. He wants any technology implemented by the merchant is simple and easy to learn.

#### Scenario

Henry entered a new restaurant, He found this store has a WiFi authentication system that can let him connect to WiFi with his phone without asking for a password. He followed instructions on the portal page and connected to WiFi easily. Also, He found there is an image on the portal page showing what is recommended for this restaurant so he decided to try the recommended one.

## StoryBoards



### SCRIPT

1

Kim is a 35-year-old man who owns a Korean restaurant. He is unfamiliar with technologies so he prefers to have some experts to help him handle technology related things. He was frequently asked by customers for WiFi password through he stuck a paper with password on the wall. Also, he wants to let people know what is recommended without asking during busy times. Therefore, he wants to use the WiFi authentication system.

### ACTION

N/A



## SCRIPT

1

As Kim is not familiar with technology, he do not know how to install the WiFi device and how to config it. Therefore, he needs to call admin for help.

## ACTION

Kim subscribed service and called admin for help.



## SCRIPT

3

Chang is a 25-year-old man who has a bachelor's degree in Computer Science. He started working for Store WiFi Management System Company as a system admin for 3 years after graduating from university. His responsibility is to monitor the system status including checking auto authentication to those merchants who subscribe our service and have made payment in full, help merchants install our WiFi devices, solve merchants' problems on request.

## ACTION

Chang received a phone call from the new subscriber Kim that asked him to install WiFi devices



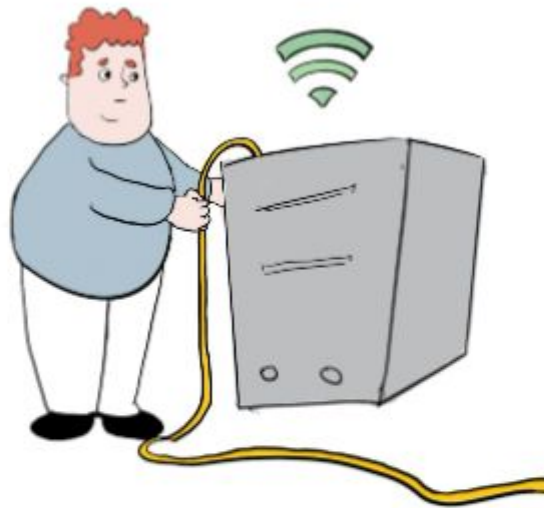
SCRIPT

N/A

4

ACTION

Chang went to Kim's restaurant and met him.



SCRIPT

N/A

5

ACTION

Chang was working on installing WiFi device



SCRIPT

N/A

6

ACTION

Chang was instructing Kim how to use their merchant dashboard to set up his WiFi portal page.



## SCRIPT

7

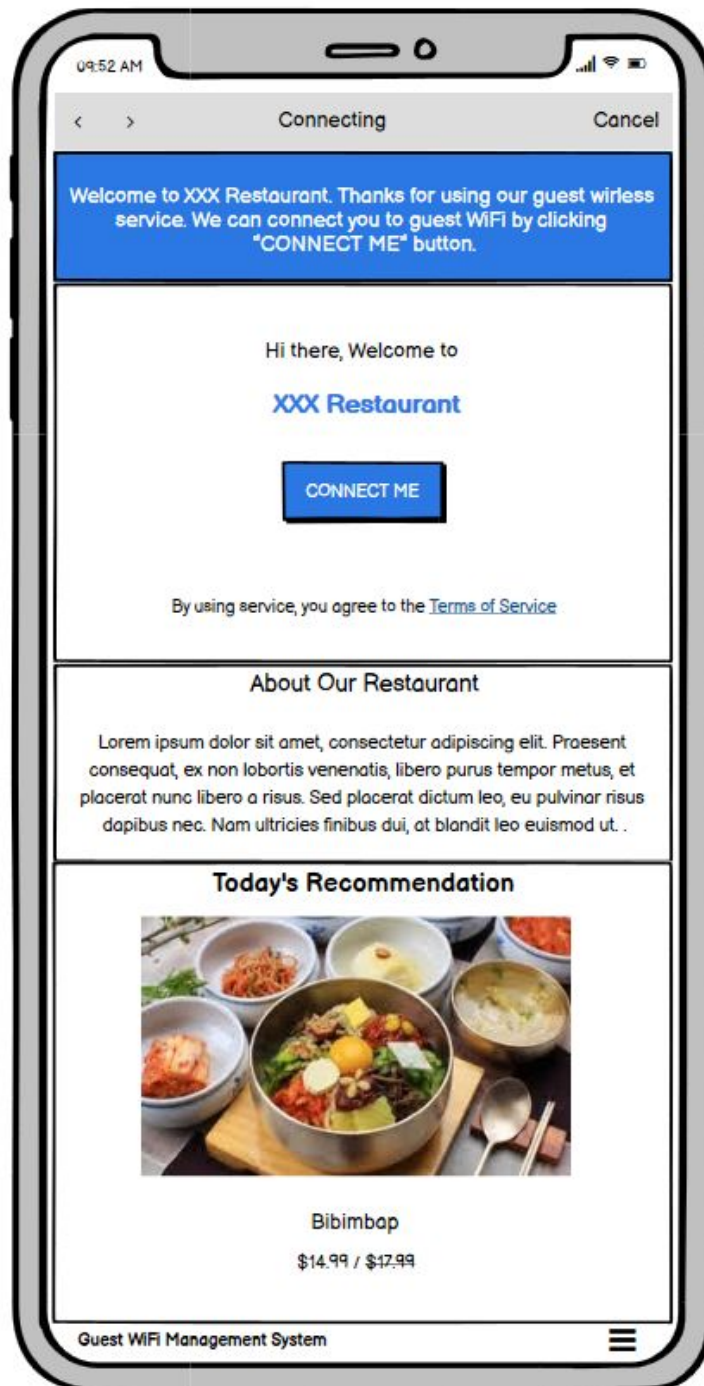
Henry is a 30-year-old man who just entered a restaurant that he is not familiar with. He wants to ask for the WiFi password but all the waiters are busy. He is not familiar with this restaurant so he wants to know what is recommended. He wants any technology implemented by the merchant is simple and easy to learn.

## ACTION

Henry went into Kim's restaurant and connected to WiFi via the new system.



## Prototypes



Source:  
<https://www.cnn.com/travel/article/best-korean-dishes/index.html>

Merchant's customer WiFi connection portal

**Guest WiFi Management System**
Hi, Admin

[Main](#)
[Data Analysis](#)
[Carousel Management](#)
[Store Info Management](#)
[WiFi Config](#)
[Admin Panel](#)

Your subscription is valid.  
All service is working successfully

0  
Devices have connected to WiFi today

327  
Devices have connected to WiFi so far

### New Announcement

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc in risus ut velit tristique tincidunt. Morbi eu libero volutpat, aliquet mauris eu, rhoncus sem. Fusce id porttitor lorem. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Etiam in tristique lacus. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus vel massa tincidunt, blandit lorem eu, semper odio. Cras at mauris malesuada, interdum neque vel, consequat justo.

Etiam auctor mollis lectus, nec tristique velit ornare ac. Praesent finibus, nulla sed sodales faucibus, mi nulla fermentum mauris, eu hendrerit sapien metus at tellus. Proin aliquet lacus id sem varius bibendum. Proin eget urna sodales, viverra nunc vel, tincidunt risus. Suspendisse iaculis vel nunc a tempus. Ut imperdiet felis arcu, ac lobortis libero tincidunt at. Nullam sem dui, blandit at efficitur vitae, congue vel elit. Praesent egestas interdum sapien a elementum. Quisque condimentum suscipit lectus, non imperdiet odio semper vitae. Nam id mauris ac ex rutrum vestibulum sit amet vitae mauris. Nunc sollicitudin felis nulla, sed lacinia purus bibendum in. Donec condimentum felis nunc, vel ornare est consequat quis. Donec tincidunt efficitur dolor.

Cras ut justo ut ligula venenatis ornare. Quisque hendrerit ex a eros eleifend, non semper ante placerat. Maecenas molestie justo metus, ac lobortis mi posuere eget. Duis quis suscipit ex, in aliquam orci. Interdum et malesuada fames ac ante ipsum primis in faucibus. Donec non pellentesque odio. Mauris vel dignissim erat, id tempor massa. Mauris auctor et lacus id aliquam. Sed vulputate eu nisi nec accumsan. Curabitur non lacinia quam, a molestie orci. Vestibulum a nibh eget urna consequat ultricies. Morbi sed dui faucibus, suscipit ligula id, iaculis urna. Maecenas faucibus elit vitae iaculis consequat. Donec ut orci vestibulum, pulvinar tortor nec, tincidunt nulla. Phasellus consequat commodo placerat. Suspendisse id diam mi.

Duis placerat tristique odio, sed imperdiet nunc molestie consectetur. Pellentesque imperdiet diam risus, vel vulputate dui ultricies posuere. Aliquam non molestie nunc. Nulla sit amet blandit elit. Praesent efficitur velit mauris, eu consequat dolor sagittis ac. Quisque dignissim maximus ipsum, molestie pharetra erat luctus non. Suspendisse non feugiat velit, eget congue sem. Proin aliquet dui at dui tincidunt vestibulum. Vivamus euismod pellentesque arcu, at auctor turpis molestie sit amet. Aenean vehicula varius libero, mollis ornare elit sagittis eget. Donec tellus ipsum, cursus non auctor ac, faucibus ut sapien. Fusce purus tellus, pellentesque id nunc varius, pellentesque commodo nisi.

Yours Sincerely,

Guest WiFi Management System Admin Group

2020.11.28

## Merchant Dashboard

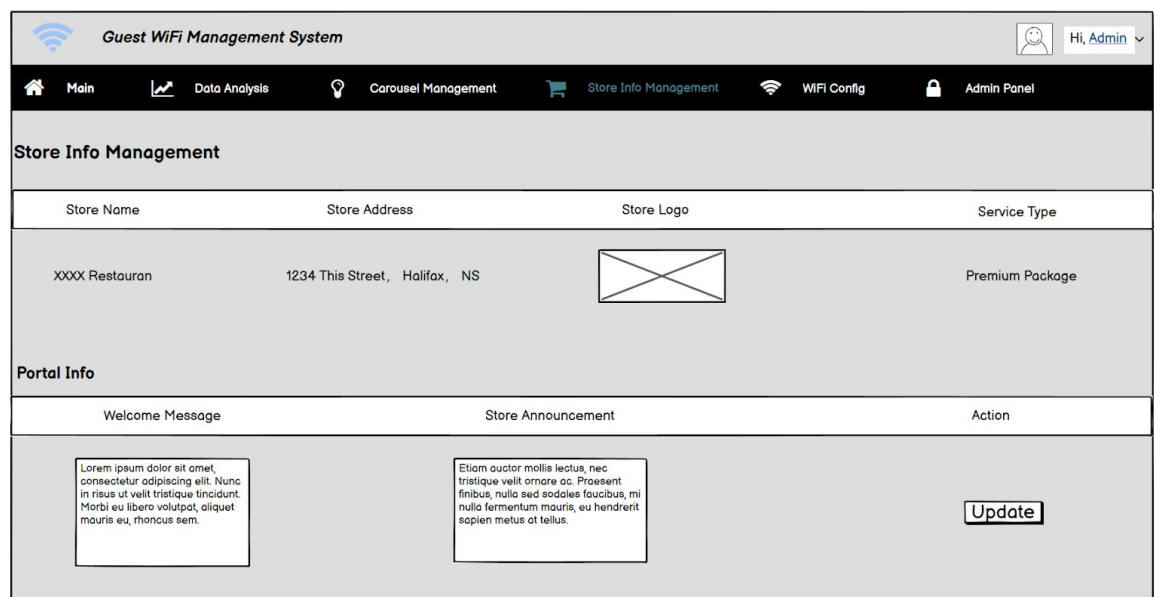
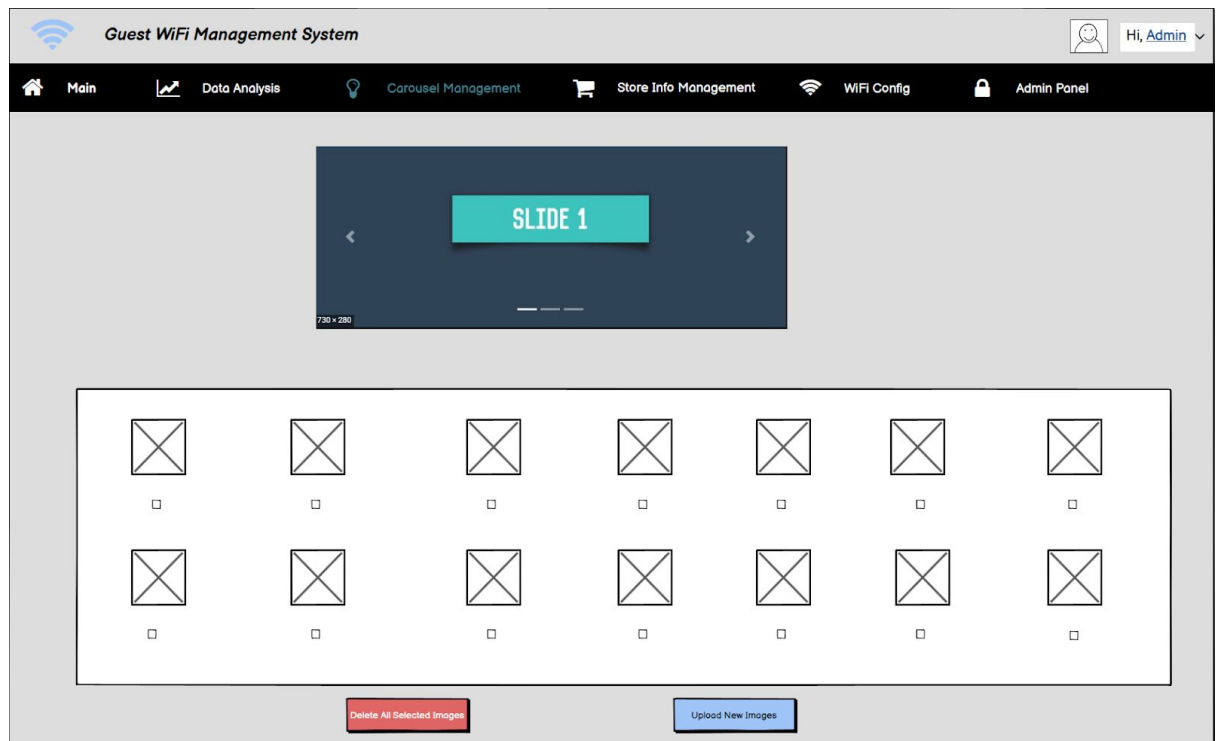
**Guest WiFi Management System**
Hi, Admin

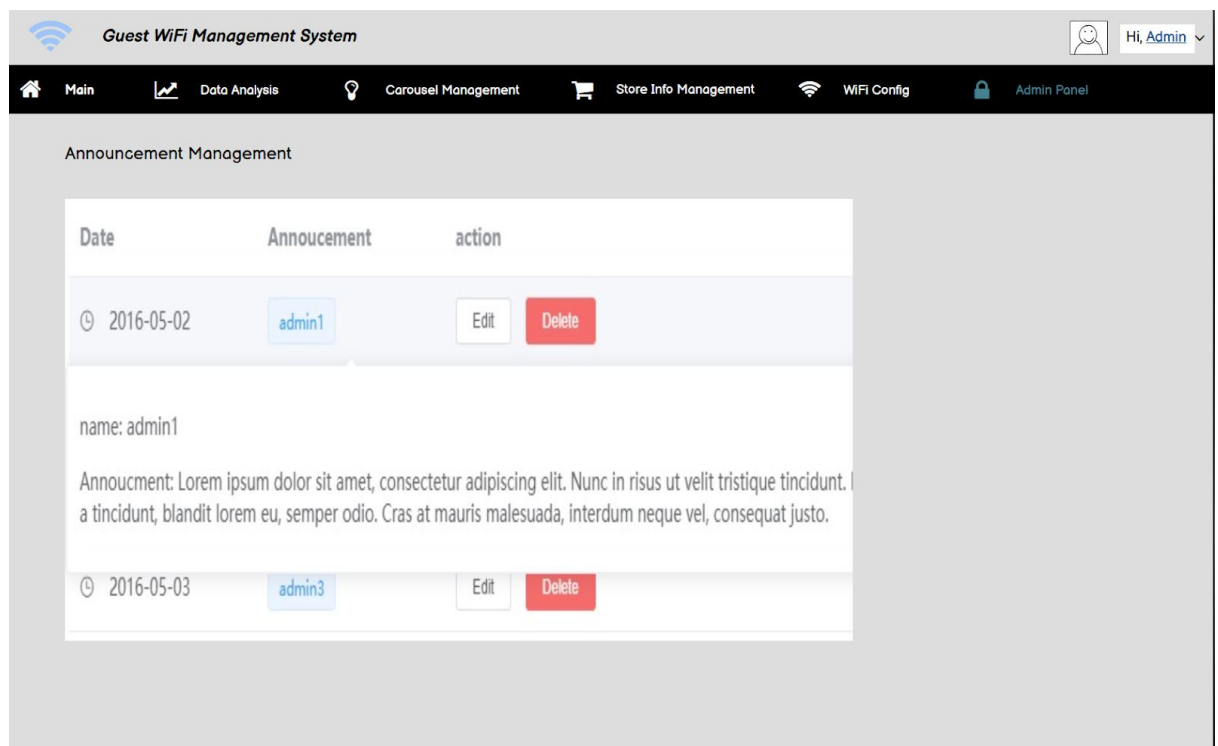
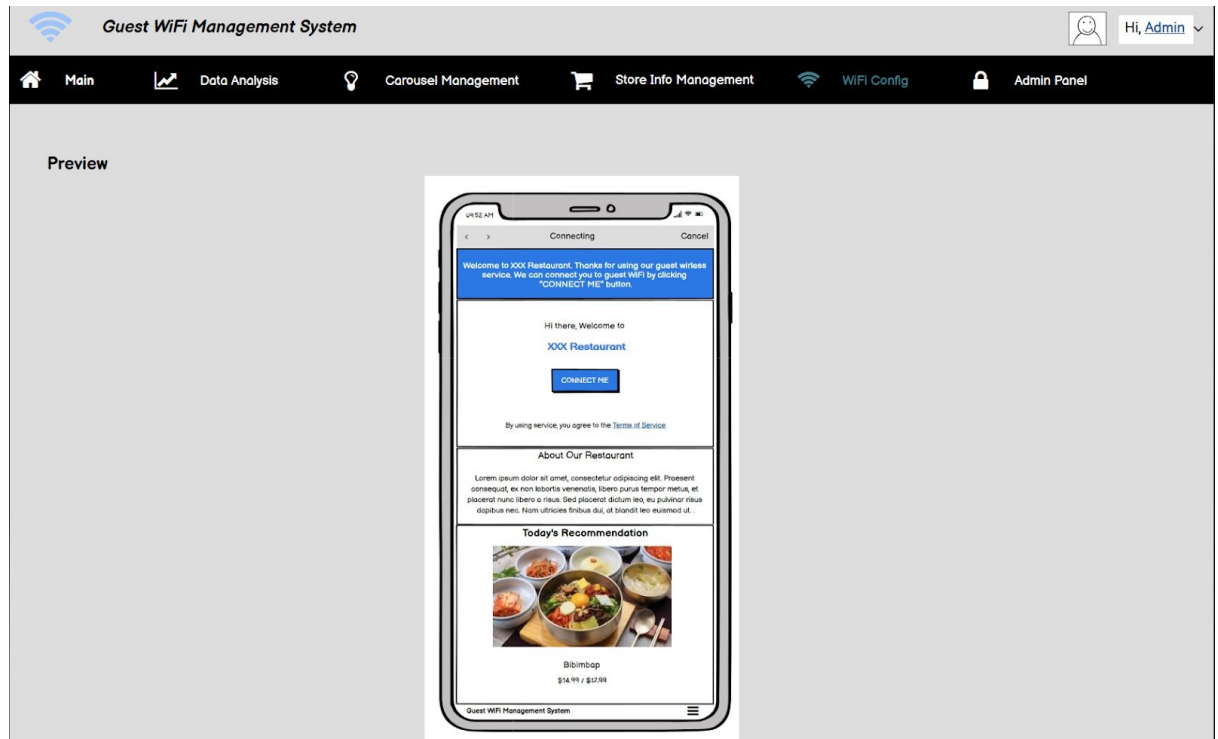
[Main](#)
[Data Analysis](#)
[Carousel Management](#)
[Store Info Management](#)
[WiFi Config](#)
[Admin Panel](#)

### Data analysis

### Detail

2020-12-01	2020-11-30	2020-11-29	2020-11-28
9 devices	47 devices	86 devices	75 devices
Total Authentications	Devices	Devices that authenticated more than twice	
69999	13456	7712	





## Security

Because our system needs to store, transmit, and process both vertical user (merchant) and horizontal customer (merchant's customer) data, data security is a significant design and implementation challenges. To address security challenges, we need to develop strategies for them. For this system's security policy, we will discuss data collection and processing, data transmission, and data storage.

The first is data collection and processing. For vertical customers, we need to collect their personal contact information, such as customer name, contact phone number, contact email, company name, company address, etc. Simultaneously, we also need to collect the necessary information of horizontal customers for the server authentication processing, such as the customer's IP address, Mac address, etc. According to the Privacy Laws in Canada, the information we collect above is personal and needs to be handled with extra care. Because any individual or company can not disclose personal privacy, disclosure of personal privacy is illegal. For the above user data collection, we will complete the HTTPS page after TLS (Transport Layer Security) encryption transmission to ensure that a third party will not intercept the user's data. According to Cloudflare (2020), TLS is a widely adopted security protocol designed to promote communications' privacy and data security over the Internet. The primary use case for TLS is to encrypt the communication between the Web application and the server (for example, a Web browser loading a Web site). And because TLS is asymmetrically encrypted, security is very high, and there is little chance of cracking.

Simultaneously, we will use a new, internal encryption algorithm to encrypt and process user data so that even if POST data is obtained by capturing packets or developer console, users' plaintext sensitive information cannot be directly seen. For this encryption algorithm, we will use Base64 to encrypt the user-submitted data and then generate a random number between 10-99 as the secret key for decryption. Finally, a loop is created, and the

encrypted ciphertext is obtained by replacing and shuffling the data previously encrypted through Base64 through PHP's substr function. Through TLS and our encryption algorithm, we can ensure that the user data from the input to the end of the processing are in a safe encryption state.

Besides, our system also needs to accept users' online payment to get the service, so sensitive information such as users' credit card information should have individual specific policies. Stripe, a third-party service provider, is used to collect, transmit, and process payment information. Stripe's SDK development framework is responsible for collecting and processing relevant information so that our system will never store and process any credit card data to ensure payment security.

The second is the data transfer phase, where our most significant challenge comes from the front-end and back-end interactions, which are mostly based on JSON strings, but because the JSON strings are plaintext, we need to do extra processing. As mentioned earlier, we will use TLS and our encryption algorithm to ensure that third parties will not intercept the content of the front and back end interactions. Even if POST data is obtained through the developer console or other means, the plaintext information will not be visible. Since our service consists of a wireless network management system (cloud platform) and hardware, we also need to deal with data transmission security between the system and the hardware. To ensure information transmission safety between the system and hardware, we use TOKEN authentication instead of sending complete service information. When a user initiates an authentication request from a mobile device browser, the front end will communicate with the back end and send information such as the user's phone's MAC address. After the back end completes processing, a temporary TOKEN will be generated and returned to the front end.

After the front end receives the TOKEN, it will send the TOKEN to the current network device, complete authentication by communicating with the Radius server and

back-end server. The device will release the internet access to the user after a valid TOKEN authentication is passed. In the whole authentication phase, the data transmission does not involve user information or any sensitive information, which greatly protects the data security.

Meanwhile, since the device and the Radius authentication server use Radius over TLS (RADSEC) to encrypt the transmission, any third party cannot listen to or decrypt the data. Through the above data encryption transmission scheme, even in the worst case, the hacker can only obtain user TOKEN, which cannot be reversely converted into useful information and cannot be used for a long time. Therefore, the above data transmission security policy is feasible and effective.

After data collection, processing, and transmission, we also need to store user data. How to store user data securely is also a great challenge for our system and the entire Internet industry. In terms of data storage security, we will adopt the MySQL remote dual live solution to deploy clusters in two or more different places. By deploying clusters in two or more different cities, business stability and data storage security can be significantly enhanced. Even in irreversible data corruption in one data center, the other data center provides stable and secure data backups that allow businesses to switch to the backup data center immediately. Simultaneously, in addition to storage security, the security of stored data is also worth our attention. We will apply strict authority management and SQL statement auditing platforms to each MySQL cluster to ensure that permissions are traceable and execution content traceable. As long as an authorized technician can access the database on loan from a jumper and its access rights are strictly limited, unauthorized data cannot be accessed across rights. At the same time, the database is only open to the specified IP access rights to ensure that the database can only be accessed and used by our internal systems.

In addition to the security policy we specify in the Wi-Fi management system's design and deployment, we can also use additional security protection systems to ensure the whole service system's security. We will deploy WAF (Web Application Firewall) to all Web-based services to filter for bad access and malicious attacks. WAF can block unauthorized access to our system, XSS or SQL injection attacks, DDoS attacks, etc., to maximize the system's security and stability. Even when the system appears vulnerable, there is still a certain degree of protection. At the same time, WAF can provide more flexible access control capability than traditional hardware firewalls. WAF can help us prevent unauthorized users from accessing sensitive information, such as blocking non-white list IP addresses, browser UA access to the system administrator dashboard. Not only that, WAF can prevent user privacy disclosure and the collection of malicious crawlers to protect the privacy security of users. Therefore, deploying WAF outside of our system is a layer of protection.

Through the development and deployment of the above security policies for the system, we can fully protect the security of the system from data acquisition, processing, transmission, and storage, and protect the privacy of customers from being disclosed.



## Development Plan

### 1. Login / Register

As we plan to use Laravel as our backend, we can easily implement user authentication and login/register function by using Laravel embed package `php artisan make:auth` and `$ php artisan migrate` to generate the login register function including user authentication. However, as we plan to use Vue as our front end, we can use the `Laravel/ui` package which is a very simple authentication scaffold built on top of the Bootstrap CSS framework. It also lets you choose between Vue/React presets. After installing the package using composer, we can use `php artisan ui vue --auth`. In this way, we can create the views in vue and render it on blade. However, as Laravel has updated to 8.0 version, the official recommended frontend scaffolding is jetstream. Jetstream provides a start point for application includes login, registration, email verification, two-factor authentication, session management. It is built on Tailwind CSS and offers a choice of Livewire or Inertia scaffolding. By selecting Inertia, we can still use vue for our development. As indicated in its official doc, Inertia is only required for its package, developers can ignore inertia if they are not familiar with it. As for our development, we will try to learn and use the latest tech which is the jetstream package option, if that way does not work out. We may switch to the `Laravel/ui` option. This part is assigned to Yanlin Zhu and should be included in Milestone 3. The test plan for this one should not be complex as it is not a part of our

core feature. We plan to test it by interacting with demo and test security by implementing SQL injection after completion.

## 2. Dashboard

The core and most significant challenge of the Wi-Fi network management system is the merchant Dashboard because this is the entry point where our vertical customers (merchants) can directly interact with the system and use the service. The whole service is entirely dependent on this Dashboard. After careful selection, we decided to use the open-source project Vue-element-Admin as the front-end framework for the entire Dashboard. Because Vue-Element-Admin is based on the Vue and Element-UI implementations, it uses the latest front-end technology stack, built-in i18N internationalization solution, dynamic routing, authorization verification, refined the typical business model, and provides a wealth of functional components. We were able to quickly implement our dashboard prototype using Vue-element-Admin, allowing us to focus more on the back end and combine the front and back in an API way. Simultaneously, Vue-element-Admin can provide a more user-friendly interface for our customers, reducing their learning and use costs, and improving user experience.

When the user has logged in through the Vue-Element-Admin front end, he can select the action he wants to take. For example, when the user wants to manage the wireless network of the opened store, by clicking the management button of the corresponding store in the front end, the front end will send a string containing the store ID, user ID, and the user's current login Token to the back end of Laravel through JSON. Laravel back-end receipt will be sent to you by parsing the JSON user

ID, store the information such as ID and Token, first verify the user Token. ID is valid, if practical, will be sent to you by the SQL statement to the MySQL database for information query, get the current user want to management shop information, and then converts the data to a JSON string sent to the front end. After the front end receives the corresponding JSON string from the back end, the related content is filled into the content template through parsing, enabling the user to complete the following operations. Due to our design of separating the front and rear ends, the dashboard front end is responsible for user interaction and interface rendering. All user operations will communicate and interact with the back end API through JSON.

## Production Environment:

Our wireless network management system is developed by Laravel and Vue, a standard LAMP/LNMP (Linux + Apache/Nginx + MySQL + PHP) architecture software, so that our cloud platform software part will be deployed in the Linux-based service operating system. Meanwhile, our team member Xinhai Cheng, a Red Hat Certified Architect advanced certification, is familiar with the Red Hat Enterprise Linux kernel and architecture. Therefore, we decided to use CentOS, an open-source community version of the operating system architected with Red Hat Enterprise Linux, as our server operating system to complete DevOps operations and deploy our services.

For the Web Server section, we did a lot of research and based on Xinhai's experience, we decided to use Nginx instead of Apache. Because Nginx practices the latest Epoll I/O model and the KQueue network model, it can achieve I/O multiplexing. Apache, on the other hand, uses the traditional Select model. Its stable Prefork mode is the multi-process

mode, requiring frequent descends of sub-processes, so it consumes much more CPU and other server resources than Nginx. Therefore, under the same resource constraints, Nginx has fewer resource requirements, more robust service capability, and more excellent stability than Apache. Since the wireless network management system will serve our vertical customers (merchants) and horizontal customers (merchants' customers) as the core business cloud platform, which will carry a large amount of concurrency and traffic, the choice of Nginx can also bring stronger performance and stability for the entire cloud platform service. Moreover, Nginx can also be selected as a reverse proxy server to achieve a highly available load balancing system through reasonable configuration and optimization. Combining with our MySQL multi-data center scheme, the remote multi-activity strategy can be performed to ensure the business's stable operation.

At the same time, we also made a lot of comparisons and investigations on selecting the MySQL version of the database. In the end, we decided to use MariaDB instead of MySQL, which was acquired by Oracle. Because MariaDB is open source software, it can be updated and maintained quickly and without charge, saving money for project deployment. MariaDB is a branch version of MySQL that is nearly 100% compatible with MySQL, and existing projects can seamlessly use MariaDB without additional updates. Second, MariaDB has made other optimizations for traditional MySQL applications that are faster and more secure. Therefore, we believe that by deploying MariaDB, we can bring new vitality to our system.

In addition to the database and Web Server, the choice of PHP version also requires special attention. Since Laravel 8 is adopted as the backend infrastructure framework in this system, our PHP version needs to be greater than or equal to 7.3. The latest stable PHP version is 7.4.x, and the latest Beta version is 8.0.x. To ensure maximum system compatibility and stability, we finally adopted PHP 7.4.x as our production deployment version. Since

Nginx is chosen as the Web server, we will use PHP-FPM(FastCGI Process Manager) as our service suite to work with Nginx.

To sum up, we will deploy and run the software part of our wireless network management system on the LNMP architecture and continuously optimize the business environment to ensure the business's stable and efficient operation.

## Reference

What is TLS (Transport Layer Security)?. Cloudflare (2020). Retrieved 1 December 2020, from  
<https://www.cloudflare.com/zh-cn/learning/ssl/transport-layer-security-tls/>