EasyChair Preprint

№ 7625

Guardian Angel Project

Shuang Li

March 28, 2022

Content list:

1. Introduction

This project design report introduces a system that can solve the difficult problem of obtaining evidence in all kinds of violent cases, and the related technologies that were applied in all its subsystems.

2. Project statement

Imagine that you are an elementary school student. On your way home from school, some students surround you and demand that you hand over all your pocket money or they will rob you of everything you own and punch you. At this moment, you can't ask the teacher for help, and you can't run away. In that case, even if you have a cell phone, there's no way to call for help without being noticed. Even if you give up on revolt temporarily and seek help from teachers or the police after giving them all your money, you may not be able to bring them to justice because of the lack of evidence.

Similarly, if you suffer domestic violence at home, you don't have enough time to call for help. Even reporting it to the police after the incident is over is often doomed by insufficient evidence.

Unfortunately, the above examples illustrate very common and very possible scenarios. It is easy to see that the persistence of these two cases is due to the victim's inability to seek help in time and to provide sufficient evidence to the police after the assault.

In recent years, the incidence of campus violence and domestic violence increased, and this kind of violence has become a social phenomenon that cannot be ignored. According to the Work Report of the Supreme People's Procuratorate in 2020, procuratorial organs across China prosecuted 62,948 people for crimes against minors in 2019, up 24.1 percent year on year. In addition, School Violence and Bullying: Global Status and Trends, Drivers and Consequences report, which was published by UNESCO in 2019, shows that one in three students around the

world have experienced bullying [1]. The situation of domestic violence is even worse. Domestic violence is found in 30% of Chinese families, and it takes an average of 35 times for victims to report it to the police, according to the survey [1].

At a time of frequent violence, few products on the market can solve this problem. Common mobile alarm apps cannot work when danger is already on the way. There was not enough time for victims to open the phone, unlock the screen, tap the app and activate its functions. Whether it's school violence or domestic violence, the abuser can interrupt their operation before they call the police successfully. And in order to deal with school violence, some schools install alarm devices on campus. But such devices are too large and expensive to cover every corner of campus, so they cannot cope with the randomness of school violence.

In order to solve the above problems, we designed the "Guardian Angel" violent incident solving system. It has small and exquisite terminals, efficient information processing capacity, powerful storage capacity, perfect privacy protection system, as well as precision authority management system. The system will aim to minimize the time it takes on the help-seeking operation and can respond to all types of sudden violence. In addition, its access management system and privacy protection system enable it to provide necessary evidence to the police while protecting privacy.

The project consists of two parts, the terminal layer and the platform layer, and the huge information management system supporting the operation of the platform layer is the core part of the project. Help terminal by the button, microphone, positioning chip, and communication module highly integrated, with positioning, radio, and communication functions. The thickness of the product is 3-4mm, which looks like a card and is portable and easy to hide. In that case, in the event of violence, it is not easy to be found and damaged.

When the user is assaulted, users only need to click the button three times in a row (designed to prevent accidental press) to activate the device and upload real-time recording and location

information to the server. When the system receives a new connection request, it will immediately monitor the synchronous upload of the recording, using artificial intelligence and natural language recognition technology to identify its content. During this period, if the system determines that a violent incident is occurring or that the terminal is forcibly damaged (the transmission signal is suddenly interrupted, the judgment method is as follows), the system will synchronize all contents to the corresponding public security organs, competent authorities or rights authorities according to its location, and ask them to respond immediately. On the other hand, if the system does not determine that the voice content is involved in a violent crime, the related data will be packaged and stored.

If the data stored in the server is not called by any user within seven days, the data will be permanently erased. The data acquisition authority is not open to all subjects or individuals, but the system will determine the data attribution according to the terminal identification code and location information. Only the Ministry of Public Security has the authority to obtain all the information, and all other organizations and organs of power can only obtain the information and relevant data within the authorized scope.

For example, schools distribute terminals to students at risk of violence, and each terminal is verified by their real names. Once violence occurs, the subsystem of the school will receive instructions and relevant information distributed by the system, and make timely response to relevant incidents. If the judicial investigation needs to retrieve relevant evidence, the local public security bureau or school can log in to the system through their exclusive USB Key and retrieve relevant data within their authority. In particular, face recognition is required when logging in to the system, and access information is recorded.

The product features evidence collection and evidence storage, an accurate and secure rights management system, and natural language recognition and analysis capabilities. These functions make it possible to prevent violent acts in time, and to a great extent solve the problems of obtaining evidence and determining responsibility.

3. Project overview

This project focus on the software behind the violence concerning the problem statement. Our goal is to provide a system that can detect and stop violence promptly, and solve the problem of obtaining evidence of violence cases.

In this project, the core of the terminal equipment is the integrated circuit board, which takes the NBIOT communication module as the core and integrates the recording device and positioning module. The main reason for using the NBIOT communication protocol is its low power consumption, which can greatly prolong the battery standby time of terminal devices. While the device is running, all information collected by the radio and location module will be uploaded in real-time via NBIOT.

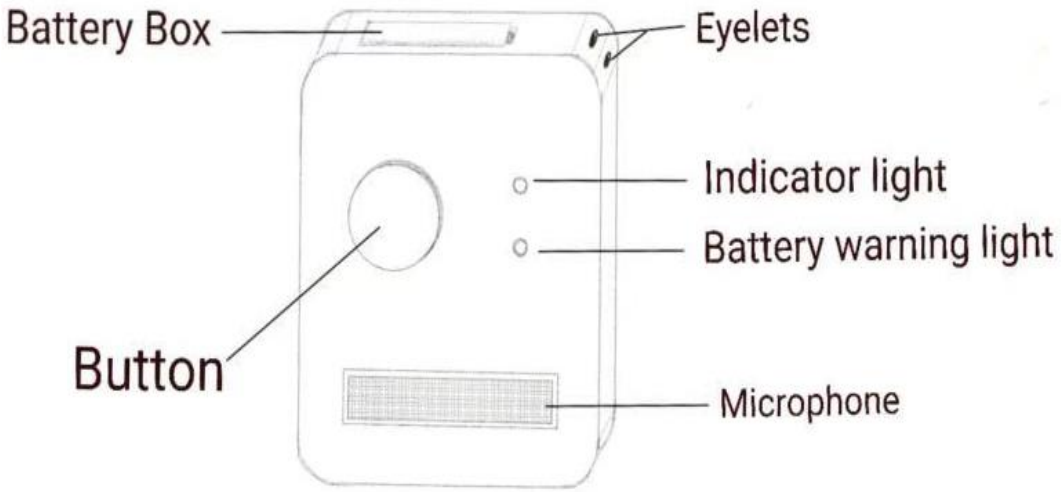

Fig.1 The model of terminal device

The terminal works for a maximum of 60 minutes at a time. After 60 minutes, the terminal automatically enters the standby state. Before entering the standby state, the system sends five consecutive confirmation JSON packages to the server. If the platform loses contact with the terminal without receiving any confirmation packet, it would consider that the terminal is damaged by violence and send an alarm.

The cloud platform is the heart of the whole system because data is meaningful only after it has been analyzed. When new data is uploaded to the server, it is processed using natural language recognition technology. After examining the recordings with specific features and meanings, emergency measures should be initiated in time. At the same time, the system will automatically correlate all surveillance footage from the vicinity of the place.

Collecting recordings can have privacy implications. Because the relevant privacy information is stolen or abused, it will cause serious consequences. Therefore, the authority distribution system is very important, all subjects with authority to view or call the data within their authority need to use an exclusive USB Key to verify their identity, and then do facial recognition to record login information.

4. Business goals and Objectives

The main goal of our project is to stop violence in time and solve the problem of obtaining related evidence. In order to achieve this goal, our project needs to meet the following conditions:

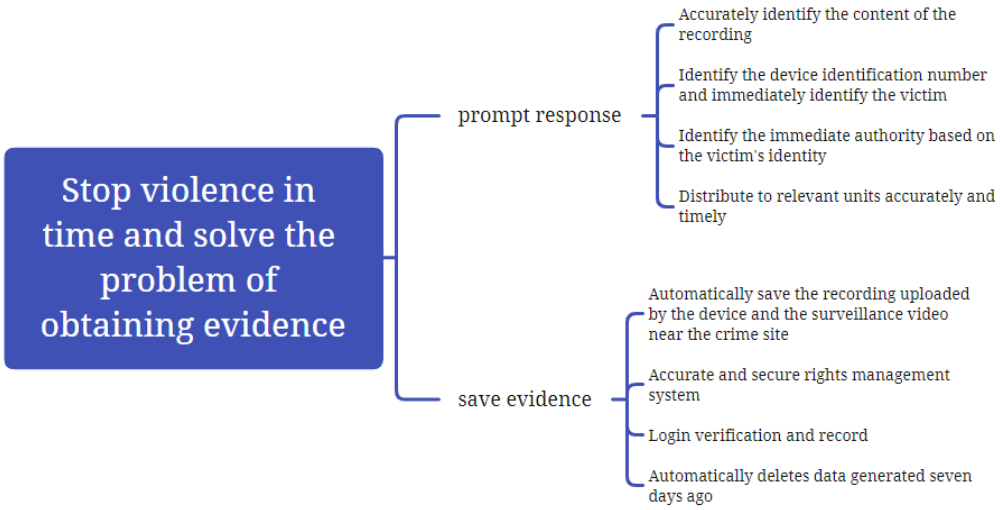

Fig.2 Business goals

5. Requirement analysis

5.1 Functional requirements

Req. Identifier	Priority	Requirement
REQ-1	5	Terminal devices can upload real-time recording and location information to the cloud via NBIOT
REQ-2	5	The system can accurately identify recordings of violent incidents
REQ-3	5	The system can automatically retrieve the surveillance video near the accident site and save it together with the recording file.
REQ-4	5	The system can accurately identify each terminal device and confirm the real name of the holder
REQ-5	5	The system can timely and accurately distribute the police information to the nearest authorities and related management agencies
REQ-6	4	Specify account permissions accurately
REQ-7	5	You need to verify the digital certificate when logging in to the system, which is stored in the
REQ-8	5	Users can only invoke data and content within their permissions
REQ-9	4	Log login and browsing information
REQ-10	3	The highest authority can manage the permissions of all accounts and audit data requests
REQ-11	4	The system can generate and distribute digital certificates for accounts with different permissions

5.2 non-functional requirements

Req. Identifier	Priority	Requirement
REQ-12	4	The system should provide a desktop and mobile-friendly

		web application to view and manage.
REQ-13	5	The content displayed on the web page varies according to permissions
REQ-14	3	The web application should be quick and easy to access and log into.
REQ-15	3	The web interface should be intuitive and user-friendly.
REQ-16	5	Identity-Verifying process should be accurate and fast
REQ-17	5	The system can send SMS messages to mobile phones that were bounded to corresponding accounts when distributing cases
REQ-18	4	The first page of your account should display a list of related cases.
		The system continuously sends SMS messages to bounded mobile phones until confirmation is received. If the confirmation is not received for a long time, the system sends a notification to their upper-level accounts.

5.3 User-interface requirements

Req. Identifier	Priority	Requirement
REQ-19	5	The web app shall have a login page for managers to access and configure their digital certification.
REQ-20	5	The Web app shall have a verification page to verify The identity of the user.
REQ-21	4	The "History Cases" page should list all cases within the authority of all accounts
REQ-22	5	The "Access Application" page guides users to retrieve data and relevant cases
REQ-23	5	The account Management page of the account with the highest permission allows you to manage the permissions

		of each account

Here are some hand-drawn sketches of the web pages and some related interaction below.

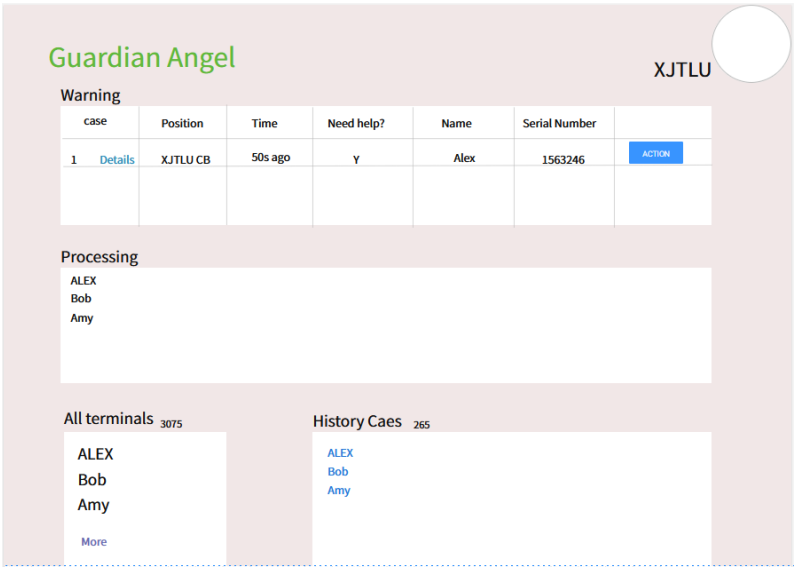

Fig.3 the sample user account of XJTLU

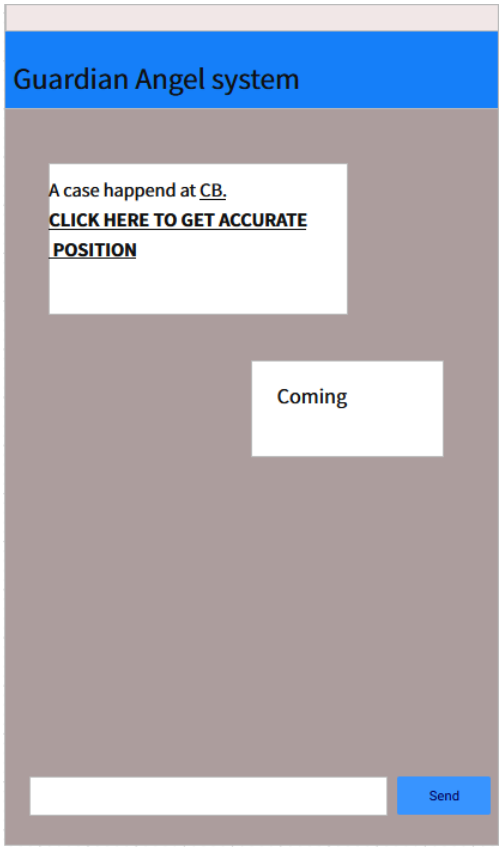

Fig.4 Message alert for the manager of XJTLU account

6. System architecture and system Design

6.1 Design and Design Limitations

The system is web-based, with all content stored on dedicated servers and different accounts having different access to the data. Only public security organs, schools, and committees can have accounts and e-certificates. All data uploaded by the terminal will be received and processed by the system.

Even though the system is powerful, some limitations cannot be ignored. The first is the security of digital certificates. Although digital certificates are used in conjunction with facial recognition to authenticate identities, they are still at risk of being stolen, which directly leads to large amounts of data being stolen or destroyed.

Second, the server will store all data uploaded by the terminal within seven days. The data size is hard to estimate. If the remaining storage space is not enough, the data stored on the server may overflow, which leads to system lag or even failure, resulting in serious consequences.

In addition, ensure that the compatibility of the system is high enough to be compatible with different login devices. The bandwidth of the server is also important, as hundreds of terminals across the country may be uploading data to the system at the same time. In this case, the speed at which the system processes data may be affected, latency may increase, and instructions may not be issued promptly.

6.2 Design Goals and guidelines

The most important principle that should be followed by the software of Web application is the KISS principle. For example, we can divide the system into many separated parts, which can help us to complete the project faster. Apart from that, its maintenance will be easier; and the system can be amended freely [2].

The core of the project is storing. In that case, the storage of the server should be as large as possible, which is the basis of its function. If there is not enough space to accommodate data, the system cannot complete any function.

The design of the terminal device should follow the principle that it is portable and thin, which makes it difficult to be discovered by the batterer.

6.3 Architectural styles

In general, this system will adapt the Model-View-Controller framework [3]. The frontend of the system enables users to interact with it. When users do the operation, the frontend would send HTTP requests to the backend. The database was stored in servers. When the user retrieves the data within his authority, the front end will send a HTTP request to the back end, and the back end will request the corresponding data to the database for it.

The web application adapts the CS architecture style. After users' identity was confirmed, the HTML/CSS/JavaScript related to the page will be transmitted to the users' computer from the server. Nowadays, a lot of web servers follow the same model. It is quite concise and can save resources.

All backend data will be stored in the database. The database contains all data relevant to user accounts (who are they) and the data that they can access (the owner of the terminal device, associated serial numbers, and data files).

The software of terminal devices utilizes an Event-driven architecture [4]. As the name indicates, this system detects and reacts to events, which is pressing the button three times. In this structure, it has event emitters, which are used to upload the audio-recordings and location information, and event consumers.

Peer-to-peer communication is used to transfer various data from the device to the platform client. In this project, the file transmission between the platform and terminal device will use

NBIOT.

6.4 Identifying subsystems

There are many subsystems, which allow the system to realize all its functions.

- The first subsystem is the terminal – Terminal Device. It can upload all the data it collects to the server. Each terminal device has its unique serial number.
- The second subsystem is the server (Database) – It can store data and analyze data that is uploaded by terminal devices. Also, it can communicate with the Web application and reply to data requests from Web Apps.
- Web Application is another subsystem – Users can request data from the server through it. It can also send messages when emergency cases happen.
-

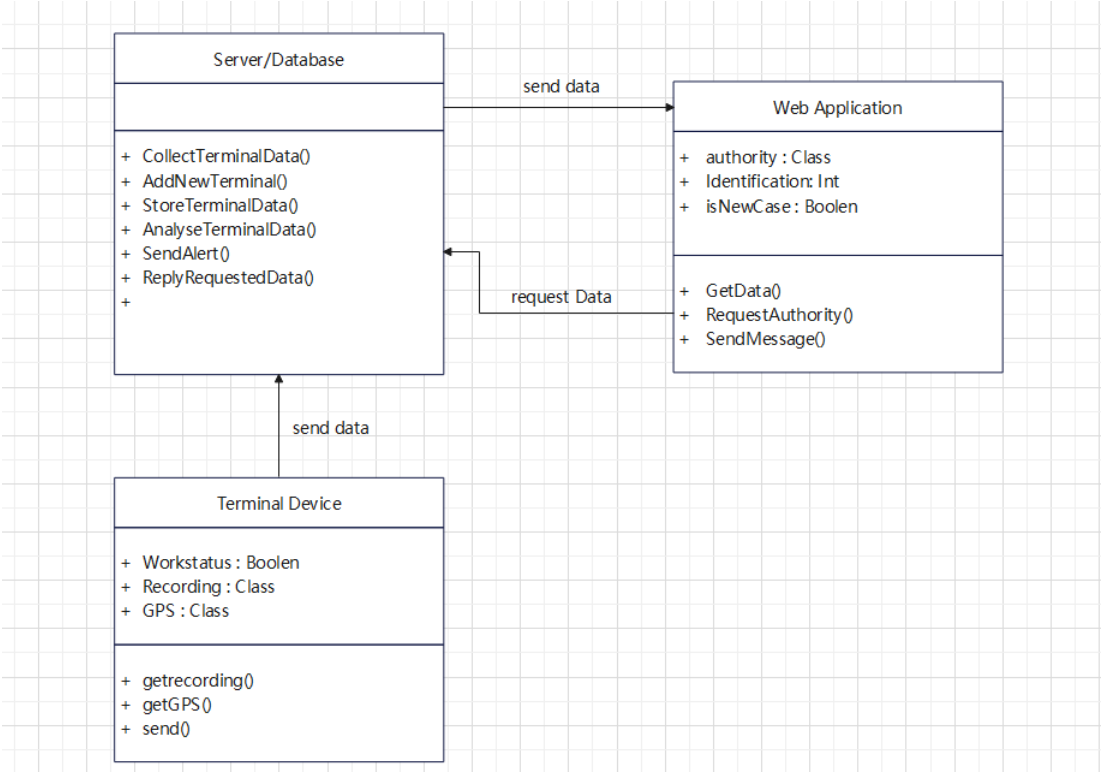

Fig.5 UML package diagram

6.5 Mapping subsystems to hardware

Subsystem: Terminal device

The terminal device consists of a local processor, a microphone, a GPS module, and an NBIOT

communication module.

Subsystem: REST API

The REST API runs on the server, which interfaces between the database and the web app.

Subsystem: Web App

The Web App is a host on personal computers, which enables users to request data from the server and manage the related terminal device.

6.6 Network protocol

To realize the communication between the central server and the web app, the project will use REST HTTP calls and use JSON for all communication. HTTP protocol will also be used for live streaming and the transmission of all kinds of data between the server and web app. The difference is that communication between terminal devices and platforms will use UDP and JSON.

6.6.1 HTTP

HTTP is a protocol that was used in the application layer [5]. It uses many areas of redundancy to lower the error rate and package loss. URLs are the identification of HTTP framework, which is one of the most important parts of HTTP. Data in HTML is represented by JSON format, which is easy to encode into HTTP format.

The reason why I design this application with HTTP protocol is that the data transferred between server and client is private and significant information, which needs to be well protected. Apart from that, its correctness must be guaranteed which means no package loss and error bits are acceptable. Therefore, HTTP is the best choice in the data-request process [5].

6.6.2 TCP

TCP is a connection-oriented, reliable, byte stream-based transport-layer communication protocol [6]. It is the basis of HTTP protocol. It is the reason why HTTP is reliable. It can reduce the error rate and package loss during the transferring process greatly, which is the main factor of using it in web applications.

6.6.3 UDP

Compared to TCP, UDP is a connectionless transport layer protocol that provides simple, transaction-oriented transport of unreliable information [7]. UDP transmits data quickly and does not require high quality of network communication. In our product, this protocol is applied in the process of the terminal device uploading information to the platform. UDP occupies far fewer resources than TCP, so it is more suitable for terminals with limited resources. In addition, the transmission rate of NBIOT is slow. If TCP protocol is adopted, a high-quality TCP connection cannot be guaranteed, and invalid transmission and high delay will occur so that the system cannot timely respond to cases.

7. Security and privacy

The recording and location information stored in the server of the project is private and could lead to serious consequences if leaked. Therefore, we use a variety of ways to keep private data secure.

First, users need to use the digital certificate distributed by the system to log in to the Web app. For security purposes, the digital certificate is distributed in the form of a USB key, which ensures the security of the digital certificate distribution to a large extent [8]. In addition, after the USB key authentication is passed, face recognition and registration are required for the logging process.

In addition to limiting access to the list of defenses listed above, you can also secure the server itself. First, convert all the disk partitions on the server where the data is stored to NTFS format. Second, install antivirus software to protect server security and install system patches in a

timely manner.

In addition to the safeguards mentioned above, having a data storage mechanism is also a good way to protect privacy. For example, automatically delete data uploaded seven days ago that has not been tagged and retrieved.

8. Hardware requirements

8.1 terminal device

- plastic card-like shell: it is easy to carry and can protect the sensor and circuit in it.
- Signal light: After the button is pressed 3 times, the signal light will be activated, which indicates that the device is working.
- NBIOT communication module: it can send the recording data and location information.
- Microphone: it can record sounds and save them.
- GPS module: it can

8.2 server

- dedicated server
- Storage: No less than 500TB. This will provide room for uploaded data. However, its size needs to be expanded as the number of terminal devices increases.
- Bandwidth: 500mbps upload and download. It is hard to estimate, which may be changed by many factors.

9. Project size estimation

It will take around 35 days to complete the project by a team of four people. The detailed allocation of the tasks would be displayed in the following Gantt chart.

	Task Name	Duration	Start	Finish	Predecessors	Resource Names
1	Buy components	5 days	'22 Mar 12	'22 Mar 17		member 1
2	Devise the terminal device	20 days	'22 Mar 18	'22 Apr 14	1	member 1
3	Develop Web App	20 days	'22 Mar 12	'22 Apr 7		member 3,member 4
4	Buy and deploy the server	25 days	'22 Mar 12	'22 Apr 14		Member 2
5	test the Web App	5 days	'22 Apr 8	'22 Apr 14	3	member 4,member 3
6	conncet three subsystem	5 days	'22 Apr 15	'22 Apr 21	2,3,4,5	member 1,Member 2, member 3,member 4

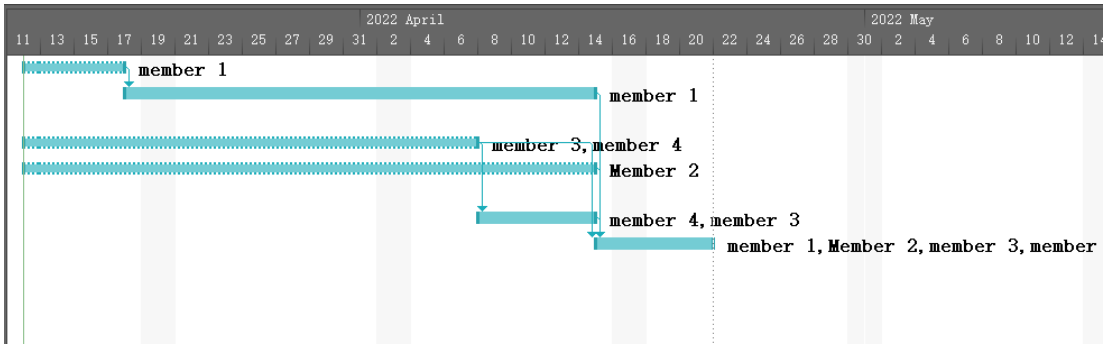

Fig.6 The Gantt Chart

10. Library and tools

During the development of the project, we adopt lots of libraries and tools, some of them are listed below.

Raknet - Raknet is a C++ network library based on UDP network transport protocol

CoAP - Based on the UDP protocol, a CoAP protocol can be implemented to meet the needs of transmission stability.

Libcurl - Libcurl is a free client URL transfer library that supports HTTP.

NodeJS - A JavaScript Runtime environment that is used in the development of the frontend of the Web App.

MySQL - An open-source relational database management system

SQL - A domain-specific programming language used for designing and managing relevant databases

Computer – it is used to access data from the server.

11. Reference

[1] R. MM, "Bullying victimization and adverse health behaviors among school-going adolescents in South Asia: Findings from the global school-based student health survey.," Wiley Country of Publication, 2020.

[2] V. R. Gibson, "System structure and software maintenance performance," Communications of ACM, vol. 32, no. 3, pp. 347-358, 1989.

[3] D. Guaman, "Classifying Model-View-Controller Software Applications Using Self-Organizing Maps," IEEE Access, 2021.

[4] Z. Wang, "A Software-Defined Always-On System With 57–75-nW Wake-Up Function Using Asynchronous Clock-Free Pipelined Event-Driven Architecture and Time-Shielding Level-Crossing ADC," IEEE Journal of Solid-State Circuits , 2021.

[5] S. X. zhu, Tu jie HTTP, Beijing: Ren min you dian chu ban she, 2014.

[6] D. Comer, Internetworking with TCP/IP, Pearson Education, 2014.

[7] A. Faisal, "A secure architecture for TCP/UDP-based cloud communications," International Journal of Information Security, vol. 20, no. 2, pp. 161-179, 2021.

[8] N. Varshney, "Security protocol for VANET by using digital certification to provide security with low bandwidth," in 2014 International Conference on Communication and Signal Processing Communications and Signal Processing, 2014.