Australian National University

Network System Design for Diabetes Management and Security Evaluation

COMP 6340 Networked Information Systems Group Assignment

Zihan Meng	u7354208	u7354208@anu.edu.au
NaiSheng Liang	u6356745	u6356745@anu.edu.au
Lingchao Zhang	u7368778	u7368778@anu.edu.au
Peilin Song	u6225932	u6225932@anu.edu.au
Ethan Yifan Zhu	u7560434	u7560434@anu.edu.au

The Australian National University

College of Engineering, Computing and Cybernetics

Table of Contents

Abstract

Diabetes is a chronic disease with high blood glucose levels that, if left untreated, can seriously harm the body. The main problem is the increasing prevalence of diabetes leading to healthcare disparities and high mortality rates. However, with the development of the network system, there are lots of systems that are designed to help diabetes management, but some of which are not updated and comprehensive. Here we show an approach to designing a network system that involves user requirement analysis through stakeholder evaluation and user story mapping. It also incorporates improvements based on existing systems, such as applying related contexts for network device characteristics design and adopting Unified Theories of Acceptance and Use of Technology (UTAUT) and Value-Sensitive Design (VSD) principles. Additionally, network security analysis is performed based on risk assessment criteria. The main result of this study is that we propose the design of a mobile application for diabetes management that provides comprehensive functions like viewing blood glucose data, receiving alerts and advice, and interacting with healthcare providers. The data transfer between sensor devices and user devices is facilitated through Bluetooth and ZigBee protocols. Data transmission between user devices and servers is secured using HTTPS and OAuth 2.0 protocols. Healthcare providers can remotely access data on the server through a Virtual Private Network (VPN) for secure transmission. We aim to design a secure and user-friendly network system for diabetes management, which can have broader implications for addressing healthcare disparities in other populations as well.

Keywords: diabetes management, network system, wearable devices, network security, healthcare

Executive summary to Professor Russell Gruen, Dean of The ANU College of Health and Medicine

This executive summary provides an overview of a proposed network system for diabetes management. The system aims to address healthcare disparities and high mortality rates associated with diabetes. It utilizes wearable sensors connected to a database for data collection and analysis by healthcare practitioners. The study focuses on meeting user requirements, improving existing systems, and assessing network security risks. Stakeholder needs, including healthcare providers, individuals with diabetes, and educational institutions, are considered. The design incorporates models such as UTAUT and VSD, with an emphasis on a mobile application for diabetes management. Data transfer within the network system is secured through Bluetooth, ZigBee, HTTPS, TCP, and IP protocols. Data privacy and integrity are ensured through VPN and layer-by-layer analysis of network technologies. This study contributes to the development of an efficient, secure, and user-centric network system for diabetes management, providing valuable insights and recommendations for implementation.

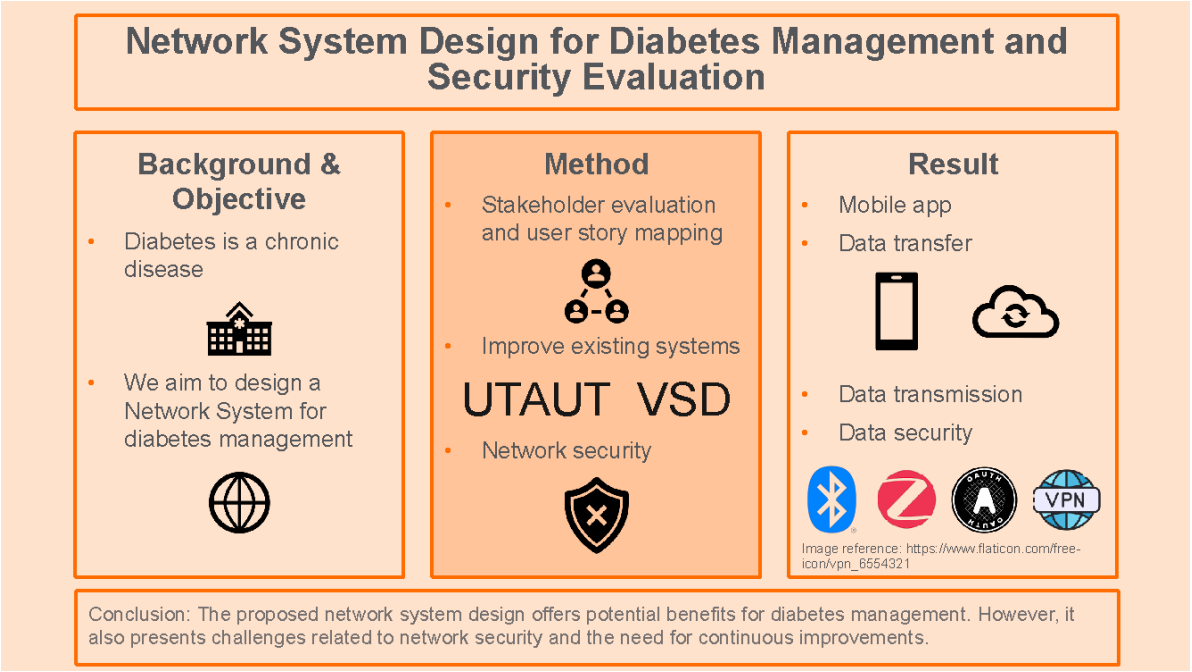
Advice to School Principals with a Duty of Care for Children with Diabetes at Their Schools

1. School administrators have a responsibility under the law to protect the health and safety of students with diabetes who attend their institutions.

2. To achieve efficient diabetes control in schools, proper communication and collaboration with parents, healthcare professionals, and school employees are essential.

3. The head of a school should make sure that kids with diabetes are not subjected to prejudice or denied participation in any activities because of their illness.

Graphical Abstract



Presentation Slides
(https://anu365-my.sharepoint.com/:b:/g/personal/u7560434_anu_edu_au/Ef9P1MKCSt9Nnu-dSZ1HehcBSJkPpihhbLIb_5k3NkqIng?e=dj2Mbd)

Presentation Video
(https://anu365-my.sharepoint.com/:v:/g/personal/u7560434_anu_edu_au/EXtBt2YFRNdFhIPtM4qYRhABes_d7zI70X00YE0U_wkVtw?e=7dL4o4)

1 Introduction

Diabetes has become more common among the Indigenous population, which has resulted in healthcare disparities and high mortality rates. The establishment of a network system linking wearable sensors with a database for data collecting and analytics by healthcare practitioners is one possible strategy for addressing this difficulty. However, using sensors to collect data via network systems involves several risks that should be carefully evaluated and addressed.

This essay aims to contribute to the development of an effective and secure network system for diabetes management. The objectives are to meet user requirements, analyze stakeholder interests and power, improve upon existing systems, and assess network security risks.

Our essay is structured into several sections. First, the network design will be developed based on user requirements in various scenarios. Then, a comparison will be made between the newly designed system and existing networked information systems for diabetes to identify areas for improvement. Network security issues will also be discussed, considering the risks and assessing the impact areas related to safety, legality, productivity, and reputation. Furthermore, we will explore the application of the designed system by analyzing the needs of stakeholders, such as healthcare providers, individuals with diabetes, and educational institutions.

To enhance the network design, the study will draw upon existing models and research, such as the qualitative study on young people living with type 1 diabetes. By applying relevant theories and concepts, including Unified Theories of Acceptance and Use of Technology (UTAUT) and Value-Sensitive Design (VSD), the study aims to improve the performance, user experience, accessibility, trust, and privacy of the network system.

Additionally, our essay discusses the design of a mobile application for diabetes management, considering factors such as patient and healthcare worker needs, data accuracy and security, device compatibility, and application usability. The application will be optimized for various devices, including smartphones, tablets, and smartwatches, and will provide comprehensive diabetes management features.

Data transfer within the network system will be facilitated through Bluetooth and ZigBee protocols, ensuring reliable and secure communication between sensor devices and user devices. The connection between user devices and servers will utilize HTTPS for secure transmission, TCP for data integrity, and IP for packet routing. The network system architecture and data communication are illustrated in a diagram to provide a clear understanding of the data flow.

Furthermore, our essay highlights the importance of data security and the use of a Virtual Private Network (VPN) for remote access to the server by healthcare providers. The layer-by-layer analysis of the network protocols and technologies employed in the system demonstrates the commitment to ensuring data privacy, integrity, and secure transmission.

Overall, we aim to contribute to the development of an efficient, secure, and user-centric network system for diabetes management in Indigenous populations. By addressing user requirements, analyzing stakeholder interests, improving upon existing systems, and ensuring network security, the study seeks to provide valuable insights and recommendations for the successful implementation of such a system.

2 Methods

2.1 Study Design and Objectives

As it is mentioned in the background information, the rising prevalence and healthcare inequality are the main reasons for diabetes in the Indigenous population. Under the current circumstances, the high rates of chronic disease cause high mortality rates which is a challenge that demands prompt solution. This network design aims to seek possible methods to establish the system between wearable sensors and database storage through network connectivity. Furthermore, the data collection can be used for analytics by the healthcare provider. Moreover, the threats of applying sensors to collect data through network systems are worth considering making further improvements.

To implement our network system, there are three main perspectives. First and foremost, the network design will be developed based on the user requirements in various scenarios based on our assumptions mentioned before. And then referring to the networked information systems for diabetes in 2023, it is critical to compare with our newly designed system to find out the pros and cons for making further improvements. Last but not least, the network security issues will be discussed according to the risks assessment to analyze our network system design.

2.2 User requirement analysis for the system

2.2.1 Stakeholder analysis

By extracting all the possible stakeholders from the background information, it is clear to assign their importance based on their interests(concerns) and power(influence). To set three indicators (High, Medium, Low) to their importance, it is necessary to evaluate their interests and power to the network systems. For these stakeholders who have high influence and interests such as Healthcare Providers and Technology Developer, they have the top priority to be involved in network system design and implementation. We need to consider how to apply their expertise to ensure technologies can realize clinical needs. And for stakeholders who have strong interests but lack influence, such as individuals with diabetes or potentially, it is also crucial to identify and satisfy their needs and prospects to improve user experience.

When the network system has been designed, it also needs to satisfy Ethical considerations and policy approvement, due to the government and authorities being stakeholders playing an active role in impacting the project. More detailed information can be found in the following table.

Stakeholder	Interest/Concern	Influence/Power	Importance
Individuals with Diabetes	Access to non-invasive monitoring, improved disease management	Low to Medium	High
Healthcare Providers	Accurate and timely data for diagnosis and treatment	High	High
Researchers and Scientists	Access to large-scale data for medical research	Medium	Medium
Technology Developers and Manufacturers	Successful adoption and utilization of their products	High	High
Government and Regulatory Bodies	Ensuring data privacy, security, and ethical practices	High	High
Educational Institutions	Supporting student health and well-being	Medium	Medium

FIGURE 2.1 Diabetes monitor project stakeholder matrix

2.2.2 User stories matching

From the highest importance, we can generate the following user story mapping.

For the healthcare provider, the non-invasive and continuous monitoring of diabetes based on the wearable sensor and reliable network is necessary to diagnose and manage diabetes effectively. Individuals with diabetes or potentially, want to access the affordable and scalable monitoring system in their everyday routines in school. Their health conditions can be easily monitored and receive timely interventions to improve their health outcomes. For the educational institution, they need to develop an integrated network system with wearable sensors in school routines. The network system needs to have network security and sustainable maintenance to support long-term diabetes monitoring.

2.3 Improvement based on the existing system

By researching the relevant topics, it is effective to design our network based on existing models and make improvements to them. For example, the recommended article *Toward diabetes device development that is mindful of the needs of young people living with type 1 diabetes: A data- and theory-driven qualitative study* (Brew-Sam et al., 2023), which provided their research on young people's and their caregivers' experiences with diabetes technologies. Based on the data analysis and conclusion, we can find out how to apply the related contexts for our network device characteristic design and implementation to meet the needs of young people.

According to the results part generated from the article, there are various Unified Theories of Acceptance and Use of Technology (UTAUT) and Value-Sensitive Design (VSD) which can be used for network device characteristics design, such as Performance Expectancy, user experience, accessibility, trust and privacy (Brew-Sam et al., 2023). From different perspectives, we can apply these concerns to improve our network design, and discuss the benefits, issues, and debates of networked information systems for diabetes in 2023 in the following parts.

3 Result

3.1 Application

Designing a mobile application for diabetes management for patients is also an important part of the overall system. A variety of factors need to be considered, including patient and healthcare worker needs, device compatibility, data accuracy and security, and application ease of use and accessibility.

- **Mobile application**

In the mobile app, we will provide complete diabetes management functions. Users can view real-time blood sugar data, analyze historical data, receive alerts and advice, and interact with healthcare workers.

The user interface (UI) will have an intuitive design, using bright colours and clear fonts. We use charts and graphs to visualize blood sugar data so that users can see the trend at a glance.

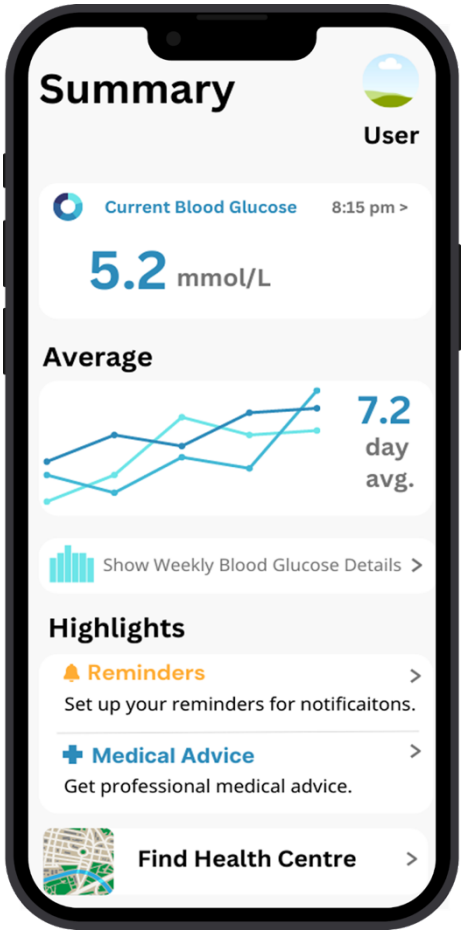


FIGURE 3.1 User interface of a mobile application

- **Watch app**

In the watch app, we will provide simplified diabetes management features. Users can view real-time blood glucose data, receive reminders and suggestions, as well as respond quickly with simple gesture operations.

Applications will connect to diabetes sensor devices using Bluetooth or ZigBee protocols to collect and display real-time blood glucose data. The application will also connect to our data server via Wi-Fi or cellular data, upload the collected data to the server, and download analysis results and recommendations from the server.

Our application will use the OAuth 2.0 protocol for authentication and authorization. According to (Okta, 2023), OAuth 2.0 is an industry-standard protocol to securely authorize third-party applications to access a user's data without sharing a password. The following diagram shows the flow of OAuth 2.0.

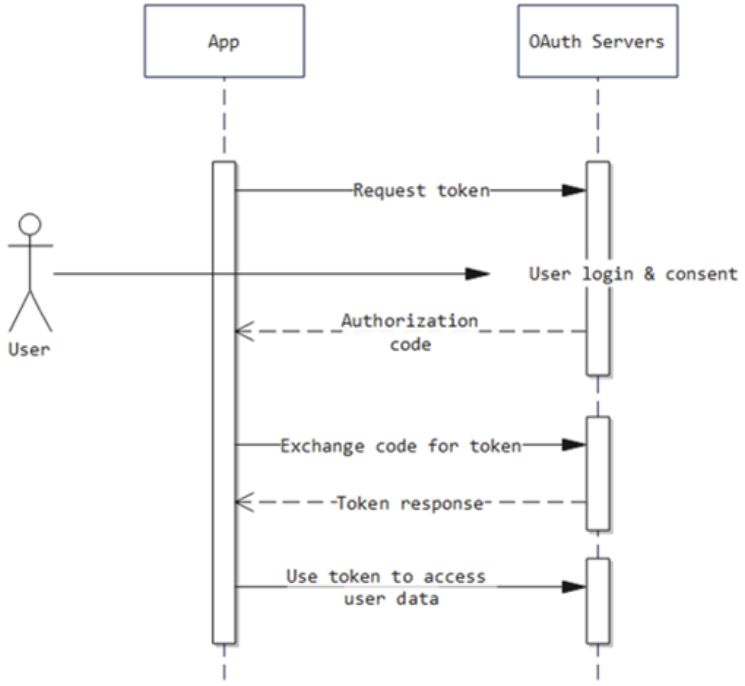


FIGURE 3.2 The flow of OAuth 2.0

- **Sensor Design**

Sensors are devices used to monitor blood glucose levels and convert these data into electrical signals. Based on the description of the case, there is a need to test for diabetes in a non-invasive manner. At the same time, it is important to note that the technology involved should be friendly to educators and young diabetic patients who are not supervised by trained medical experts in schools and should also be new and trustworthy. Moving away from invasive methods of measuring blood glucose, there are two main non-invasive methods, Namely, Non-invasive optical glucose monitors and Non-invasive fluid sampling glucose monitoring (Shang et al., 2021).

3.2 Network System Design

The case mentioned that testing the technology designed in this paper for detecting diabetes could be part of the routine work of schools,

The measurement results will be connected to the central data storage and analysis server via the university's network.

The below diagram shows the architecture of the network designed by us. Each component in the network system will be detailed and introduced in the following paragraphs.

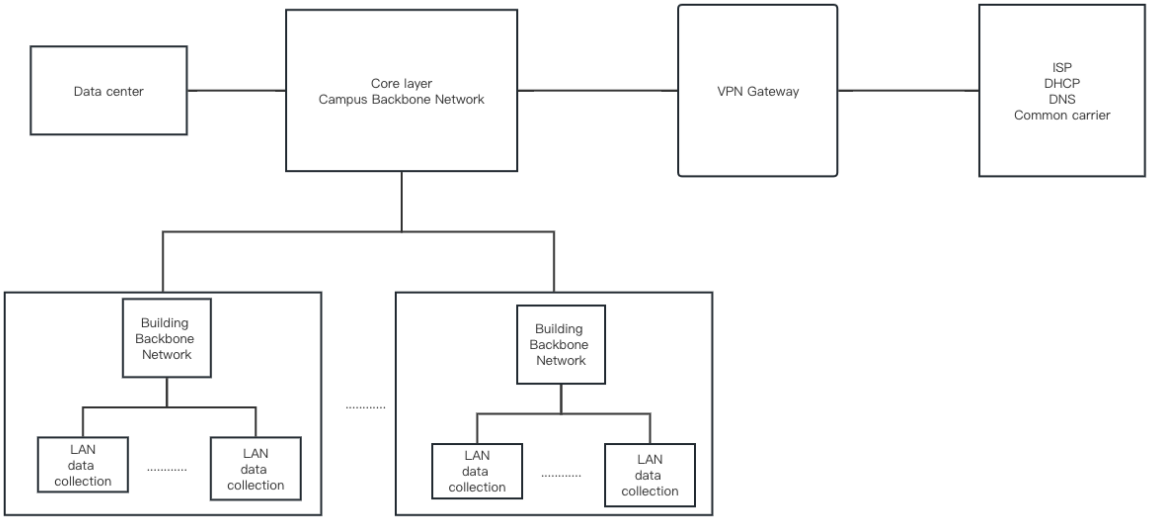


FIGURE 3.3 Network System Architecture

3.2.1 Local area network (LAN)

LAN enables diabetic patients to access the network. Each LAN consists of sensors, user devices, Bluetooth 5.0, Zigbee gateway, Access Points and switches. Sensors will collect health information from patients based on settings and send data to mobile devices through Bluetooth or a Zigbee gateway through Zigbee.

The following diagram illustrates the LAN architecture.

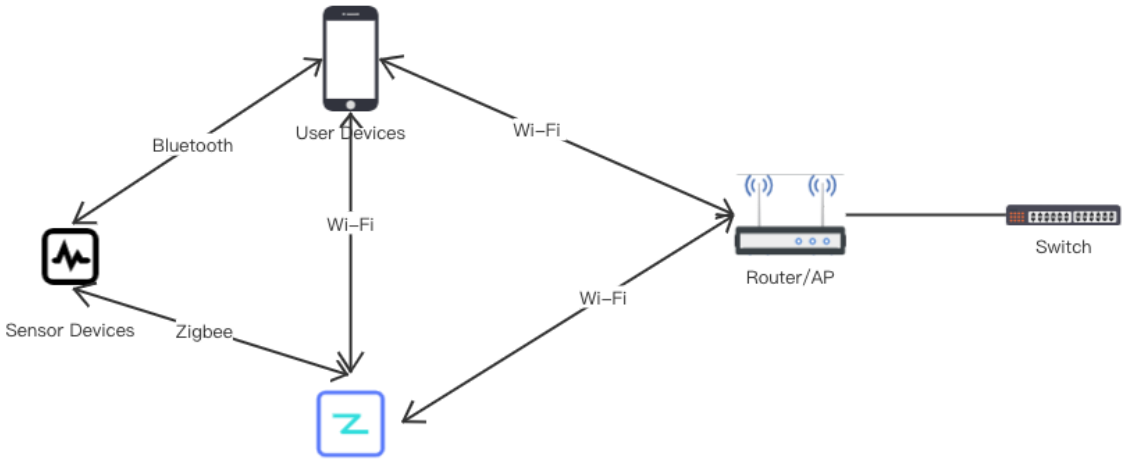


FIGURE 3.4 LAN Architecture

In 2016, the Bluetooth 5.0 protocol which inherited the advantages of BLE was officially released. Compared with WIFI and ZigBee, Bluetooth Low Energy technology has the lowest power consumption, so it is very suitable for carrying on the sensor device with a small battery capacity.

The energy consumption of ZigBee technology can be controlled at a lower level so it can run stably for a long time.

If the sensor sends data using Zigbee protocol and the user device doesn't support Zigbee protocol, then a Zigbee gateway is required. The Zigbee gateway receives Zigbee signals from sensors and converts them into IP packets to be sent to the user's device over Wi-Fi. Similarly, when the user device needs to send a command to the sensor, the Zigbee gateway also converts the IP packet into a Zigbee signal.

Wi-Fi 6 is a wireless network protocol that provides higher data rates and better connection quality.

3.2.2 Building Backbone Network

Building backbone network distributes network traffic to and from the LANs. In the distribution layer, we compose LAN with a proper switch that supports dealing with all data transmitted from LANs. Additionally, switches implemented here are faster than those in LANs. For instance, Juniper

Networks EX Series Switches which has 48 ports and 10 Gbps transmitting speed is adapted to the situation.

The following diagram illustrates the building BN architecture.

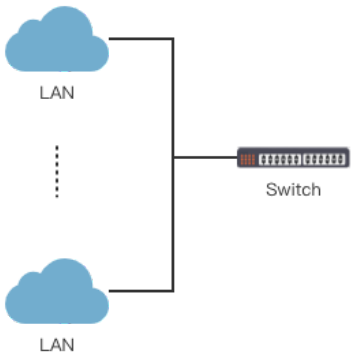


FIGURE 3.4 Building BN Architecture

3.2.3 Campus Backbone Network

All building backbone networks are connected to a layer 3 switch in the core layer, hence a much more powerful switch is necessary for the campus backbone network. The Cisco Catalyst 3850 series switches provide 1000 Ethernet ports and four optional 1G or 10G uplink ports which support an extremely fast data transmission speed.

The following diagram illustrates the campus backbone network architecture.

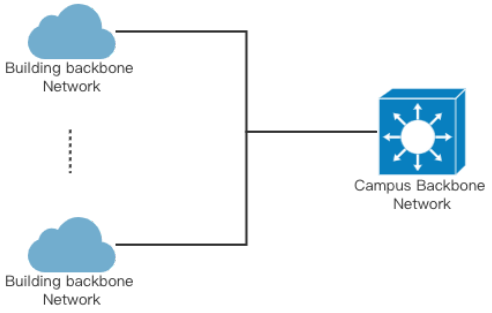


FIGURE 3.5 Campus Backbone Network Architecture

3.2.4 Data Centre, Wide Area Network (WAN) and Internet Access

The data centre is also in the centre of campus which performs the storage and analysis of data mainly. It only connects the core layer, thus it is also considered as a LAN internally.

The following diagram illustrates the all components connected to the core layer.

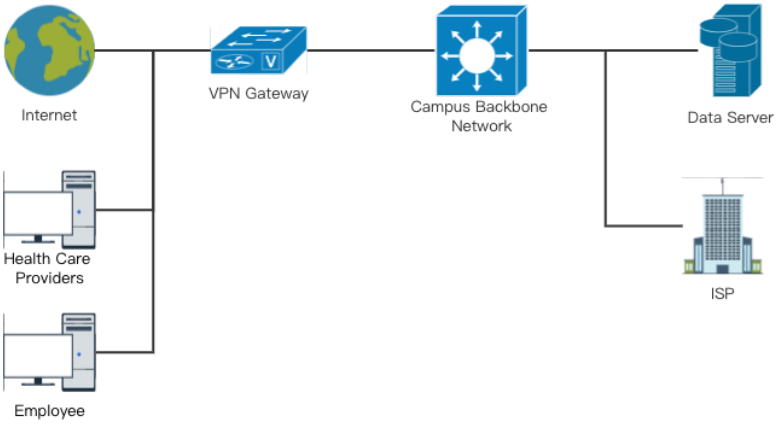


FIGURE 3.6 All components connected to the core layer

Healthcare providers and employees may need remote access to data on the server. In this case, they can use a Virtual Private Network (VPN) to securely access the server.

VPN is an encrypted connection from a device to the network over the Internet. It prevents unauthorized people from eavesdropping on traffic and allows users to do remote work (Cisco, 2019).

HTTPS is an application layer protocol that is a secure version of the HTTP protocol, which adds an SSL/TLS encryption layer between HTTP and TCP to protect data privacy and integrity. In this context, we chose HTTPS because it can provide secure end-to-end communication, preventing data interception and tampering while in transit.

TCP is a reliable, connection-oriented transport protocol that provides in-order transmission of data and error recovery. In this case, we choose TCP because we need to guarantee data integrity and reliability.

IP protocol is responsible for sending packets from the source address to the destination address. In this case, we chose IP because it is the underlying protocol on the Internet and can support a variety of different network environments and devices.

By combining these protocols and technologies, we can create a secure and reliable way to communicate data over the Internet. This approach not only meets the needs of medical service providers for data access but also protects the data security of patients.

4 Discussion

4.1 Pros and Cons

How our designed system can solve the problem?

First, we will discuss how our designed system can solve the problem. As we mentioned in the methodology section, our system should meet the following requirements: it is affordable, scalable and can be accessed by diabetes patients in school routine life, it can monitor health conditions easily and provide timely interventions for patients and it provides network security and sustainable maintenance.

For the first requirement, WLAN(especially Zigbee), mobile app and mesh topology implemented in our designed system can solve it. WLAN which covers the whole campus and mobile apps can ensure all patients can access the system everywhere. Mesh topology provides scalability and Zigbee offers low cost (Yang, Yao and Yang, 2007).

To meet the second demand, we applied watches and WLAN to the system. Watches provide convenience to monitor health conditions and give interventions to patients. WLAN can ensure patients can receive messages timely. Typically, Zigbee offers short delay and excellent stability which can promise timeliness (Yang, Yao and Yang, 2007).

The purpose of using OAuth 2.0, Bluetooth Low Energy technology, VPN, firewall and Bluetooth 5.0 is to satisfy the third requirement. By using OAuth 2.0, the system can ensure that only authorized applications can access a user's data. An encrypted connection supported by VPN and firewall also supply network security. Furthermore, Bluetooth Low Energy technology and the Mesh networking supported by Bluetooth 5.0(Jabra, 2020) can ensure sustainability by providing the lowest power consumption and improved network coverage.

Pros and Cons

- **Advantages**

  First, the university Intranet employed in the system only allows users inside the university to access the data hence providing privacy and security. Besides, the mesh topology furnishes robustness and scalability. The full-duplex supported by it improves the efficiency and timeliness of transmission. Apart from these, OAuth 2.0(Auth0, n.d.) supplies authentication and authorization to enhance security. What's more, the low power consumption and high data security of Bluetooth and Zigbee benefit our system and it is relatively simple to implement them. Especially, Zigbee can work independently without user devices so it delivers flexibility (Yang, Yao and Yang, 2007). Furthermore, the firewall can block untrusted accessibility hence granting security and privacy (Cisco, 2023). VPN contributes to security and the ability to access remotely to our system. Last but not least, Bluetooth 5.0 and Zigbee offer a longer transmission distance with the same power consumption, enhanced throughput, significantly improved network coverage and more capability to transmit data (Jabra, 2020).

- **Drawbacks**

  Since we utilized many technologies in our system, it will bring high costs and is hard to manage and maintain. Besides, mesh topology can cause latency issues which will harm the timeliness of the system. It also needs high costs to establish and manage. More importantly, our system must use advanced VPNs to ensure high-speed and reliable security and privacy, this will also need considerable costs.

4.2 Risk Assessment

To establish a trustworthy and secure network, risk assessment is essential and necessary. In this section, we will perform the risk assessment according to the framework proposed by FitzGerald and Dennis (2007). There will five subsections which start from developing the risk measurement criteria, and then we discuss about the IT assets and existing common threats. After that we also propose the methods of risk control and approaches for ensuring business continuity.

4.2.1 Risk Measurement Criteria

In this first step, we create a sample risk measurement criterion for this OHIOH project with respect to wireless technology. Below is the form:

TABLE 4.1 A sample of risk measurement criteria

Impact Area	Priority	Low Impact	Medium Impact	High Impact
Safety	High	Proportion of Injures is less than 3%	Proportion of Injures is from 3% to 10%	Proportion of Injures is more than 10%
Reputation	High	Decrease in number of customer by less than 3%	Decrease in number of customer from 3% to 8%	Decrease in number of customer by more than 8%
Productivity	Medium	Annual operating expenses increase by less than 2%	Annual operating expenses increase by from 2% to 4%	Annual operating expenses increase by more than 4%
Legal	Medium	Incurring fines or legal fees less than $5,000	Incurring fines or legal fees from $5,000 to $30,000	Incurring fines or legal fees more than $30,000
Financial	Low	Sales drop by less than 2%	Sales drop by 2%–10%	Sales drop by more than 10%

4.2.2 Inventory IT Assets

Identifying IT assets is also important for evaluating the risk of a networked information system. Hence we list two tables of types of assets involved in the system and also the inventory of assets specifically. We also assume that there is a Chief Information Officer (CIO) and network manager in the project.

TABLE 4.2 Types of IT assets

Hardware	Physical servers for different purposes such as web servers, DNS servers, DHCP servers, LAN file servers, BN file servers, WAN file servers. Mobile devices and sensors with built-in Bluetooth and wireless function Data transmission devices such as switches and routers
Circuits	Wireless circuits between users' mobiles and sensors Leased locally operated circuits of Backbone Network and LAN Leased contracted circuits of WAN circuits Internet access circuits
Network software	Operating systems and settings on all servers such as Windows 10, Ubuntu Linux and MacOS Web applications which consist of multiple functions such as data transmission, analysis and storage.
Client software	Operating systems and settings on all mobile devices such as Windows 10, Ubuntu Linux and MacOS Web applications which consist of multiple functions such as data identification, collection and transmission.
Organizational data	Databases with organizational records on the cloud servers
Mission-critical applications	Data transferring and analysis application

TABLE 4.3 Inventory of IT assets

Asset	Importance	Most Important Security Requirement	Description	Owner(s)
Web server	High	•Confidentiality •Integrity •Availability	This supports the data collected from customers can be transmitted and storaged correctly and efficiently	Network manager
Customer database	High	•Confidentiality •Integrity •Availability	This is the database which consists of users' privacy and necessary information. It also can perform the analysis and filters automatically based on the settings	CIO
Sensors	High	•Confidentiality •Integrity •Availability	The sensors are attached to mobile devices which are used to collect the body information from users in real-time	Customers
Financial records	Medium	•Confidentiality •Integrity •Availability	These records are maintained by financial department which can be used in financial evaluation.	CFO
Employees' computers	Medium	•Confidentiality •Integrity •Availability	Each employee is assigned a desktop computer which are allowed to access the customers' database. Employees provide customer service and support for our product using these computers.	Division directors

4.2.3 Identify Threats & Risk Control

After we analyzed all IT assets involved in the OHIOH project, we can identify what threats may possibly occur and how we control the risks from several different perspectives.

We evaluate all potential threats and choose five of them which are most likely happened to each of our IT assets: Malicious virus attack, Natural disaster, Theft of information, Intrusion and Spear fishing attack. More

specifically, the two major threats among them are malicious virus attack and intrusion. Malicious attack is considered as a kind of destruction which refers to the damage that can destroy the system, network and data thoroughly. The damage cannot be recovered easily that may cause a significant loss and failure for our product. Intrusion normally refers that external hackers access the internal information system secretly and manipulate data which may cause unexpected loss. All private and sensitive data may be leaked and spread through the internet which must be treated seriously as a major threat.

To analyze these threats in details, we perform five tables which contains the specific descriptions, risk scores and the approaches that are effective on controlling these threats.

TABLE 4.4 Malicious virus attack on Web server

Asset	Webserver		
Asset Importance	High		
Threat	Malicious virus attack		
Description	The virus can invade any devices including servers and do harm to systems which may make the system crash and data loss or damage and all customers cannot access the product.		
Likelihood	Medium(2)		
Impact on	_____ Confidentiality _____ Integrity ___✓__ Availability		
Impact Area	Priority	Impact	Score
Safety	High(3)	High(3)	9
Reputation	High(3)	Medium(2)	6
Productivity	Medium(2)	High(3)	6
Legal	Medium(2)	Low(1)	2
Financial	Low(1)	High(3)	3
		Impact Score	26
Risk Score (Likelihood × Impact Score)	52		
Adequacy of Existing Controls	Medium		
Risk Control Strategy	_____ Accept ___✓__ Mitigate _____ Share _____ Defer		
Risk Mitigation Controls	Measurements		
Antivirus software	Install reputable antivirus software on all systems to detect and block known viruses and malware.		
Educate and train employees	Provide comprehensive cybersecurity awareness training to employees, teaching them how to recognize and avoid potential virus threats, such as suspicious email attachments or malicious websites.		
Enable firewall protection	Configure firewalls on network devices and individual systems to filter incoming and outgoing network traffic, helping to block unauthorized access and the spread of viruses.		
Regularly back up data	Perform frequent backups of important data and verify the backups for integrity. Store backups in a separate location or use cloud-based backup solutions to ensure data can be restored in case of a virus attack.		

TABLE 4.5 Natural disaster on customer database

Asset	Customer database		
Asset Importance	High		
Threat	Natural disaster		
Description	The database containing customers' information can be hit by the hill fire and destroyed physically.		
Likelihood	Low(1)		
Impact on	_____ Confidentiality _____ Integrity ___✓__ Availability		
Impact Area	Priority	Impact	Score
Safety	High(3)	Low(1)	3
Reputation	High(3)	Low(1)	3
Productivity	Medium(2)	Medium(2)	4
Legal	Medium(2)	Low(1)	2
Financial	Low(1)	High(3)	3
		Impact Score	15
Risk Score (Likelihood × Impact Score)	15		
Adequacy of Existing Controls	High		
Risk Control Strategy	_____ Accept ___✓__ Mitigate _____ Share _____ Defer		
Risk Mitigation Controls	Measurements		
Regularly back up data	Perform frequent backups of important data and verify the backups for integrity. Store backups in a separate location or use cloud-based backup solutions to ensure data can be restored in case of a virus attack.		
Geographically diverse data centers	If possible, consider hosting the customer database in data centers located in different geographic regions. This helps mitigate the risk of a single natural disaster impacting all data centers simultaneously.		
Regular maintenance and inspection	Conduct regular maintenance and inspection of data center facilities and infrastructure to identify and address any potential vulnerabilities or risks that could impact the customer database during a natural disaster.		

TABLE 4.6 Theft of information on Sensors

Asset	Sensors		
Asset Importance	High		
Threat	Theft of information		
Description	External hackers may block and eavesdrop the customers' data when it is being transmitted. The destination of transmission may also be modified.		
Likelihood	Low(1)		
Impact on	__✓___ Confidentiality __✓___ Integrity _____ Availability		
Impact Area	Priority	Impact	Score
Safety	High(3)	High(3)	9
Reputation	High(3)	High(3)	9
Productivity	Medium(2)	Medium(2)	4
Legal	Medium(2)	Low(1)	2
Financial	Low(1)	Medium(2)	2
		Impact Score	26
Risk Score (Likelihood × Impact Score)	26		
Adequacy of Existing Controls	Medium		
Risk Control Strategy	_____ Accept ___✓__ Mitigate _____ Share _____ Defer		
Risk Mitigation Controls	Measurements		
Encryption	Implement strong encryption mechanisms to protect customer sensor data both in transit and at rest. This ensures that even if the data is intercepted or stolen, it remains unreadable and unusable without the encryption keys.		
Secure communication channels	Utilize secure communication protocols, such as HTTPS or VPNs, when transmitting customer sensor data. This protects the data from interception and ensures its integrity during transmission.		
Monitoring and auditing	Implement robust monitoring and auditing mechanisms to track and log access to customer sensor data. Regularly review logs for any suspicious activities or unauthorized access attempts, enabling timely detection and response.		

TABLE 4.7 Intrusion on Financial records

Asset	Financial records		
Asset Importance	Medium		
Threat	Intrusion		
Description	External hackers use unauthorized access or entry to get into a computer system, network, or device. It involves an individual or entity gaining access to resources, data, or functionalities without proper authorization.		
Likelihood	Medium(2)		
Impact on	_____ Confidentiality _____ Integrity ___✓__ Availability		
Impact Area	Priority	Impact	Score
Safety	High(3)	Medium(2)	6
Reputation	High(3)	Medium(2)	6
Productivity	Medium(2)	Low(1)	2
Legal	Medium(2)	Low(1)	2
Financial	Low(1)	High(3)	3
		Impact Score	19
Risk Score (Likelihood × Impact Score)	38		
Adequacy of Existing Controls	Medium		
Risk Control Strategy	_____ Accept ___✓__ Mitigate _____ Share _____ Defer		
Risk Mitigation Controls	Measurements		
Encryption	Utilize encryption to protect financial records both in transit and at rest. Encrypt sensitive data using strong encryption algorithms to ensure that even if the data is compromised, it remains unreadable and unusable without the encryption keys.		
Intrusion detection and prevention systems	Deploy intrusion detection and prevention systems (IDPS) to monitor network traffic and detect suspicious or unauthorized activity. These systems can automatically respond to potential intrusions by blocking or alerting administrators.		
Network segmentation	Implement network segmentation to isolate financial records and systems from other parts of the network. This reduces the attack surface and limits the potential impact of an intrusion.		

TABLE 4.8 Spear fishing attack on Employ's computers

Asset	Employees' computers		
Asset Importance	Medium		
Threat	Spear fishing attack		
Description	External hackers may send personalized and highly tailored fraudulent emails or messages to our internal employees to get access to the system and do harm to our product.		
Likelihood	Medium(2)		
Impact on	__✓___ Confidentiality _____ Integrity _____ Availability		
Impact Area	Priority	Impact	Score
Safety	High(3)	High(3)	9
Reputation	High(3)	High(3)	9
Productivity	Medium(2)	Low(1)	2
Legal	Medium(2)	Low(1)	2
Financial	Low(1)	Medium(2)	2
		Impact Score	15
Risk Score (Likelihood × Impact Score)	30		
Adequacy of Existing Controls	Medium		
Risk Control Strategy	_____ Accept ___✓__ Mitigate _____ Share _____ Defer		
Risk Mitigation Controls	Measurements		
Security Awareness Training	Provide regular security awareness training to employees to educate them about the risks of spear phishing attacks, how to recognize suspicious emails, and best practices for handling and reporting them.		
Email Filtering and Anti-Spam Measures	Implement robust email filtering and anti-spam solutions that can detect and block suspicious emails, including those with known phishing indicators.		
Multi-Factor Authentication	Enable multi-factor authentication for email accounts and other critical systems. This adds an extra layer of security and makes it more difficult for attackers to gain unauthorized access.		

4.2.4 Business Continuity

Business continuity is typically defined as the ability of an enterprise to maintain its operations in the event of a disaster or failure. The basic requirement for business continuity is to keep mission-critical functions running during an undesired event and to recover in the shortest possible downtime. Therefore, we suggest to establish the continuous monitoring and threat intelligence system to ensure the business continuity.

Continuous monitoring shall involve real time monitoring of critical systems, networks and applications for the detection and immediate responses to possible security incidents. This is typically carried out with security information and event management systems, intrusion detection systems, intruder control systems, log analysis tools or other monitoring solutions. Organisations can discover and address threats, such as unauthorised access attempts, unusual network behaviour or suspected activities through continuous tracking of networks traffic, system logs and user activity. Moreover, continuous monitoring and intelligence on threats gives organisations the ability to identify and correct security gaps, vulnerabilities or weaknesses in their systems and networks without delay. In this context, it assists in identifying patterns, trends and indicators of compromise which may be missed by a proactive monitoring approach. Organisations can ensure the priority of their security activities, efficient allocation of resources and improved overall safety posture through use of threat intelligence.

- **Benefits**

According to the result of the connectivity of networked information systems for diabetes evaluated by Brew-Sam and his colleagues, some of them have data sharing function while others have suspended when low function (Brew-Sam et al., 2023). Apart from this, some systems can share patient data with the healthcare team or within patients' family automatically.

- **Issues**

Although all systems either can share data or have the function to suspend when low, none of them has both data sharing function and suspend when low function(Brew-Sam et al., 2023). Additionally, some of the systems don't have the ability to upload data automatically. They still need to upload the

data to the cloud and share them with the healthcare team. Worsely, as claimed by Britton and Britton-Colonnese, the systems don't have control to collect, store and use patient data.

- **Debates**

In accordance with the result of interviews made by Brew-Sam and his colleagues, most young people don't want to share data with their parents while parents want to keep on sharing data (Brew-Sam et al., 2023).

- **Challenge**

A big challenge will be the privacy of patient data since more and more patients have concerns about emerging diabetes techniques. CGM data may be considered as a risk to privacy in the future hence it is very essential to focus more on privacy and improve the privacy of the systems as much possible as they can.

- **Future**

Furthermore, many patients expected to use fully automatized systems in order to enable normality when they were asked about their wishes about the systems in the interview (Brew-Sam et al., 2023).

Group Description

Our group has five members, Peilin Song, Naisheng Liang, Zihan Meng, Ethan Yifan Zhu and Lingchao Zhang.

Zihan has studied human-computer interaction courses and has interned as a product manager. He also has some experience with design prototypes and believed this experience would be useful for this assignment.

Peilin is a master of computing with data science specialization. Apart from these, he has plentiful project experience in web server development and network design. Therefore, he wants to take charge of the methodology part of the team.

Naisheng is currently doing a master degree in computing and also got bachelor's degree from ANU too. He expertises in programming languages and has a relatively good research background. As a part of this assignment, he focused on secure assessment and business continuity and also structured the design for this network system design.

Ethan is pursuing his second semester of Master of Computing. He had experience designing systems for an industry before and is willing to learn more. He is mainly responsible for summarizing and arranging the report.

Lingchao is hard-working and willing to undertake any task. His subject is Master of Computing. He enjoys challenging himself. He has some knowledge about network design methodologies, network technologies like Network Package Broker, protocols and cyber security such as encryption.

Contribution Statement

All group members discussed the network system design.

Zihan completed the holistic network system architecture. He was also responsible for describing the sensors and mobile applications connected to the system as well as illustrating the whole process of data transmission.

Peilin worked on researching the methodology of network system design. He did stakeholder and user requirements analysis. He also analyzed network security. He was also responsible for the executive summary part.

Naisheng did the risk assessment. He also did risk control by recording risk assessment and corresponding resolutions. He researched threats to our system, assessed security and made some defensive approaches.

Ethan worked on the abstract and introduction. He reviewed all of our work and proposed a few amendments. He also typeset the paper and made it consistent.

Lingchao worked on the discussion part. He researched how our designed system can solve the problem along with the advantages and drawbacks. He recorded the group description and contribution statement.

Reflection

The problem-solving strategies are mainly reflective of this team project.

Firstly, as a team, it is efficient to allocate the tasks for different team members according to their expertise and interests. Part of the team did research on relevant topics for network technologies and others started from user requirements to apply relevant content to the network projects. Secondly, the network design for diabetes monitoring systems is a new field to get learn more information about individuals with diabetes. We need to find out how can help them to improve health outcomes affordably and convincingly.

From previous knowledge, a good way to start the project is to find out the stakeholders and list the user story maps. Every time we define the problems, we will think about the connection between the use scenario to network layers. When we established the network architecture, we also made improvements based on the previous patterns provided in the textbook or journal articles. It is critical to analyse pros and cons to fit our model in practical ways,

In conclusion, we can practice all the design thinking in our network design. All of our team members can take charge of the corresponding part and we share our work to make sure every team member can understand what others doing and provide feedback.

Reference

Brew-Sam, N. *et al.* (2023) 'Toward diabetes device development that is mindful to the needs of young people living with type 1 diabetes: A data- and theory-driven qualitative study', *JMIR Diabetes*, 8. doi:10.2196/43377.

Cisco (2019). *What Is a VPN? - Virtual Private Network*. [online] Cisco. Available at: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html.

Cisco (2023). *What is a Firewall?* Available at: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html (Accessed: 15 May 2023).

FitzGerald, J., & Dennis, A. (2007). *Business data communications and networking*. John Wiley & Sons.

Jabra (2020). *Bluetooth 5.0 headsets: Should you get one? · Jabra Blog*. [online] Jabra Blog. Available at: https://www.jabra.com/blog/bluetooth-5-headsets/#:~:text=Higher%20bandwidth%3A%20While%20Bluetooth%204.2 [Accessed 28 Mar. 2023].

Okta (2023). OAuth 2.0 Authorization Framework. [online] Auth0 Docs. Available at: https://auth0.com/docs/authenticate/protocols/oauth#:~:text=The%20OAuth%202.0%20authorization%20framework [Accessed 14 May 2023].

Shang, T., Zhang, J.Y., Thomas, A., Arnold, M.A., Vetter, B.N., Heinemann, L. and Klonoff, D.C. (2021). Products for Monitoring Glucose Levels in the Human Body with Noninvasive Optical, Noninvasive Fluid Sampling, or Minimally Invasive Technologies. *Journal of Diabetes Science and Technology*, [online] p.193229682110072. doi:https://doi.org/10.1177/19322968211007212.

Yang, H., Yao, F. and Yang, S.-H. (2007). *Zigbee enabled radio frequency identification system*. [online] *repository.lboro.ac.uk*. Loughborough University. Available at: https://repository.lboro.ac.uk/articles/conference_contribution/Zigbee_enabled_radio_frequency_identification_system/9404108 [Accessed 15 May 2023].