Project of a secure network infrastructure

By

Muhammad Faizan

Contents

Access Control System Details:

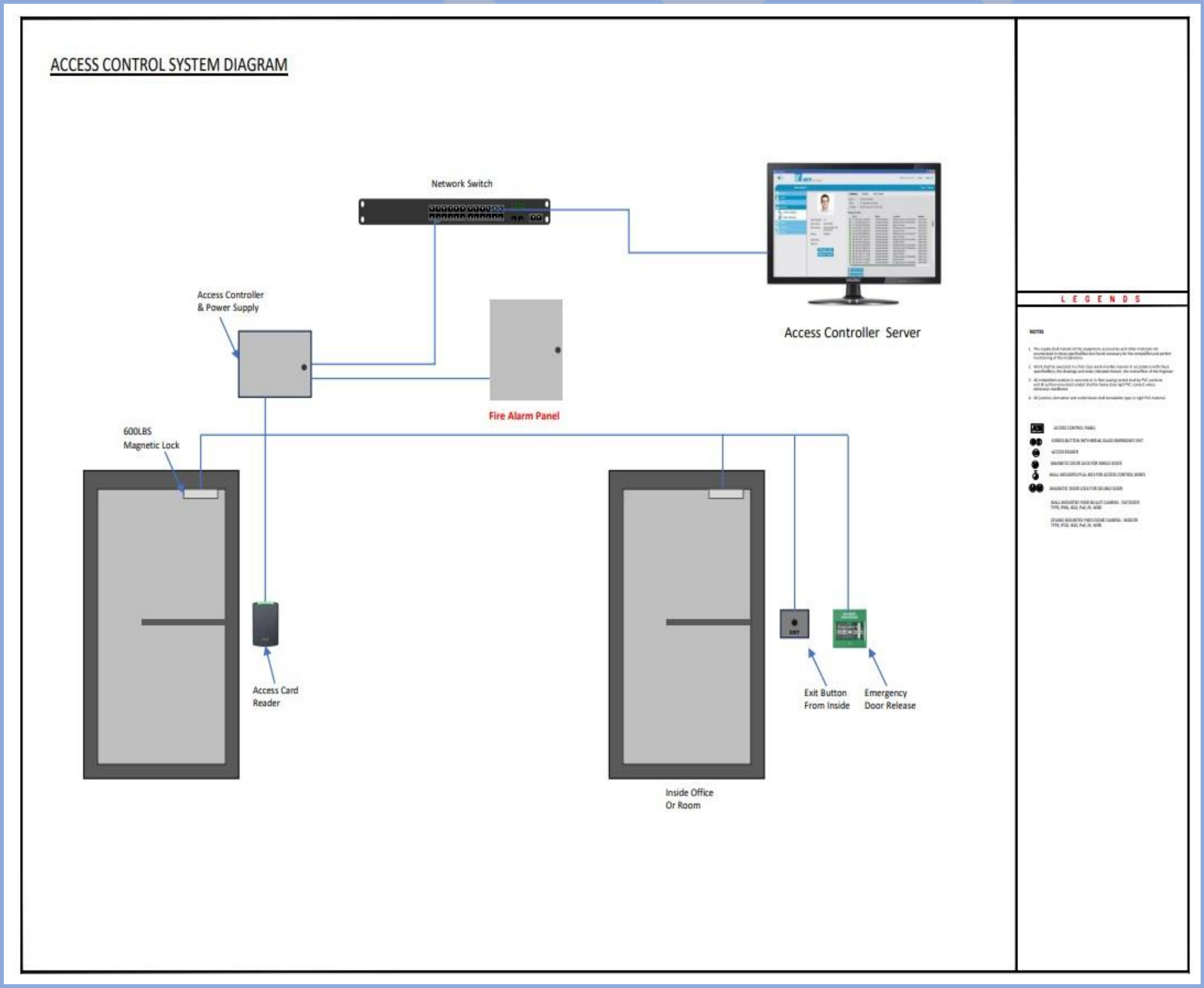
We have installed the Access Control System described through the process consisted of 8 stages.

1. **600LBS Magnetic Lock Door Entry:**
    - A 600LBS magnetic lock is installed on the entry door, providing secure access control.
2. **Access Controller & Power Supply:**
    - An Access Controller is integrated with the system to manage access permissions.
    - A dedicated Power Supply unit is installed to provide power to the access control components.
    - Power Supply integrated with the Access Controller to ensure continuous operation.
    - Backup power systems, such as uninterruptible power supplies (UPS), may be considered for critical components.
3. **Access Card Reader and Fire Alarm Panel:**
    - An Access Card Reader is connected to the Access Controller to facilitate authorized access using access cards.
    - The Access Controller is integrated with a Fire Alarm Panel to ensure coordination with the fire safety system.
4. **Network Switch:**
    - A Network Switch is connected to the Access Controller Server to enable communication and network integration.
    - This allows for centralized control and monitoring of the access control system.
5. **Exit Button:**
    - Inside the office or room, an exit button is installed. This button allows individuals inside the secured area to exit without requiring an access card.
    - This contributes to the overall ease of movement within the controlled space.
6. **Emergency Button:**
    - An Emergency Button is installed, providing a quick and easily accessible means to trigger emergency protocols.
    - This button might be linked to the building's overall emergency response system.
7. **Functionality:**
    - The Access Controller manages access permissions and interfaces with the Access Card Reader, Fire Alarm Panel, Exit Button, and Emergency Button.

- The Magnetic Lock secures the door entry point and is controlled by the Access Controller.
- Access Card Reader authenticates users based on presented access cards.
- Fire Alarm Panel is integrated to trigger alarms or responses in case of fire emergencies.
- Exit Button allows occupants to exit from the inside without using access cards.
- Emergency Button provides a quick response option in emergency situations.

8. Integration:

- Access Controller and Power Supply are integrated components managing the access system.
- Access Controller is connected to the Network Switch for centralized control and monitoring.
- Fire Alarm Panel is integrated for enhanced safety and rapid response during fire incidents.



Access Door:

We have many types of doors list the following every step through the process consisted of 14 stages

1. **M-TOIL (Main Toilets):**
    - Likely contains multiple toilet stalls, sinks, and possibly shower facilities.
    - Provides the primary restroom facilities for the building.
2. **ELE. ROOM (Electrical Room):**
    - Dedicated to housing electrical equipment such as switchboards, panels, and other electrical infrastructure.
    - May include backup power systems like generators or uninterruptible power supplies (UPS).
3. **MEETING ROOM:**
    - Designed for conducting meetings, discussions, presentations, and collaborative work.
    - May contain a conference table, chairs, audio-visual equipment, and whiteboards.
4. **IDF-SEC (Intermediate Distribution Frame - Security):**
    - Functions as a hub for network and security equipment.
    - Likely houses servers, network switches, and security systems such as CCTV cameras, access control panels, and related infrastructure.
5. **ACS-GF-OFF (Access Control System - Ground Floor Office):**
    - Ground floor office dedicated to the Access Control System.
    - Controls and monitors access to different parts of the building.
6. **PRAYER ROOM:**
    - A dedicated space for individuals to pray or meditate.
    - May include prayer mats, religious texts, and other amenities to accommodate religious practices.
7. **Boller Shiner Door:**
    - The purpose is unclear from the provided diagram.
    - It may refer to a specific door with a special function or security feature.
8. **WORK SHOP:**
    - Designated for workshop activities, possibly for hands-on projects, repairs, or maintenance.

- May include workbenches, tools, and equipment relevant to the type of workshop.

9. **FLAMMABLE STORAGE:**
    - Specifically designed for the safe storage of flammable materials.
    - Likely equipped with safety measures such as fire-resistant cabinets and proper ventilation.

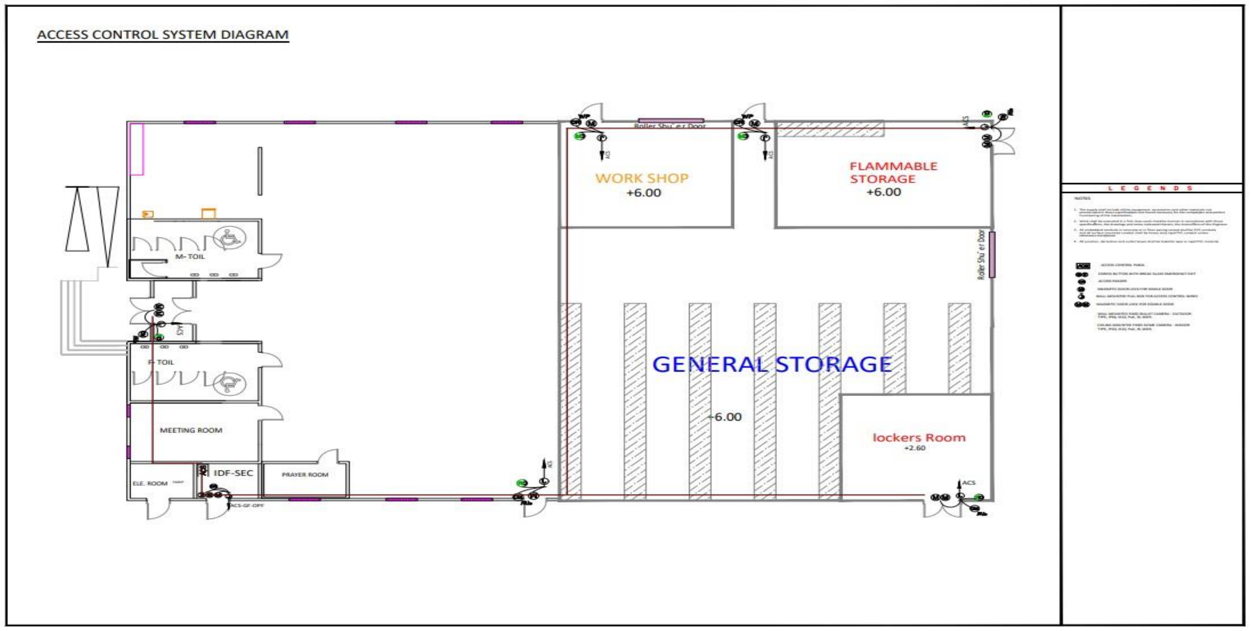
10. **APPLY STORAGE:**
    - The purpose is unclear from the provided diagram.
    - It may be a storage area for items related to applications or specific to a certain process.

11. **GENERAL STORAGE:**
    - A generic storage area for general items not covered by other specialized storage rooms.

12. **LOCKERS ROOM:**
    - Contains lockers for individuals to store personal belongings securely.
    - Common in workplaces for employees to store items like bags, coats, and personal items.

13. **GENDS (Gender-specific restrooms):**
    - Separate restrooms for different genders, providing privacy and comfort.

14. **NOTES 1:0.03:**
    - Possibly a room for documentation or note-keeping, though the purpose is not entirely clear from the provided information.



Wi-Fi Installation in Different Areas:

Wi-Fi installation details would depend on the organization's policies, the building's infrastructure, and technology standards at the time of installation as well as the total number of Wi-Fi network is having 5 in the room the following every steps

1. **MEETING ROOM:**

   - The Meeting Room typically requires robust Wi-Fi connectivity to support presentations, collaborative work, and teleconferencing.
   - Installation might include dual-band Wi-Fi routers capable of both 2.4 GHz and 5 GHz frequencies for flexibility and performance.

2. **WORK SHOP:**

   - In a WORK SHOP, Wi-Fi might be installed to support wireless tools, equipment, and enable connectivity for workshop-related activities.
   - The choice between 2.4 GHz and 5 GHz would depend on the specific requirements and potential interference in the area.

3. **FLAMMABLE STORAGE:**

   - Flammable storage areas might have limitations on electronic equipment due to safety concerns.
   - Wi-Fi installation would need to comply with safety regulations and may not be applicable in some cases.

4. **APPLY STORAGE:**

   - Similar to FLAMMABLE STORAGE, Wi-Fi installation might be limited in certain storage areas based on safety requirements.

5. **LOCKERS ROOM:**

   - Wi-Fi installation in a LOCKERS ROOM might be provided for convenience, allowing individuals to access online services or check messages while using lockers.
   - Dual-band routers could be used to accommodate various devices.

6. **GENDS (Gender-specific restrooms):**

   - Wi-Fi installation in restrooms is less common but could be provided for convenience.
   - Privacy and security considerations would be important in such installations.

Wi-Fi Frequency Options:

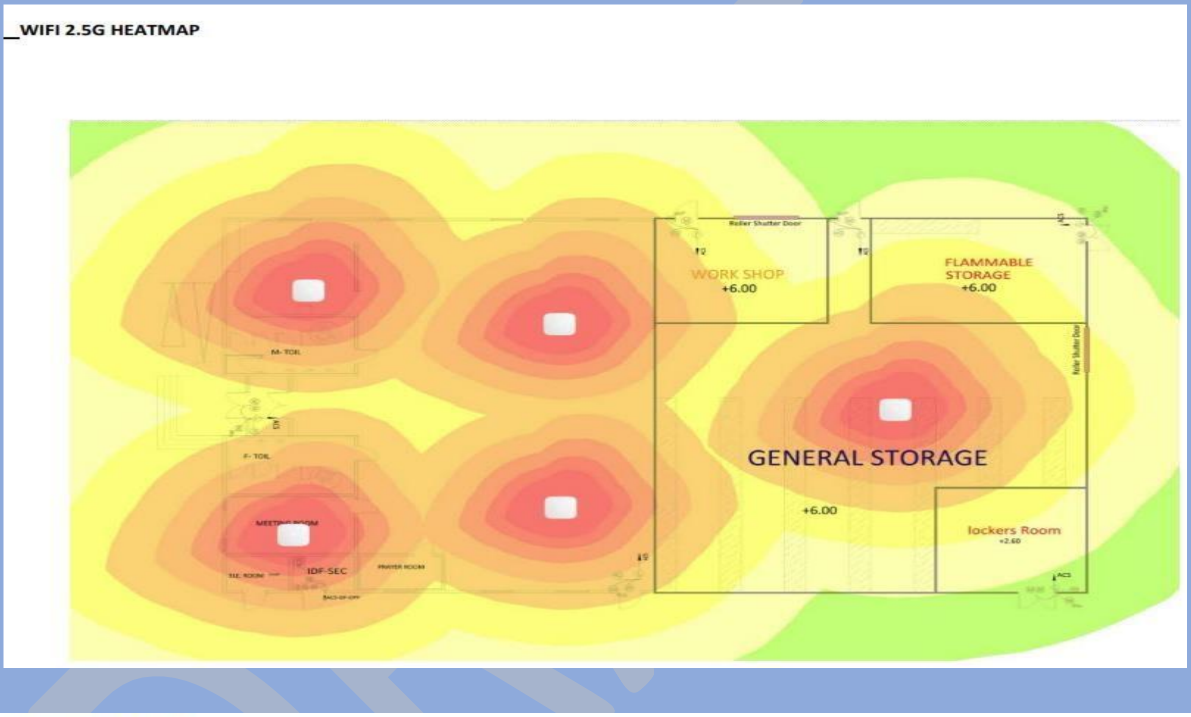
- **2.4 GHz:**

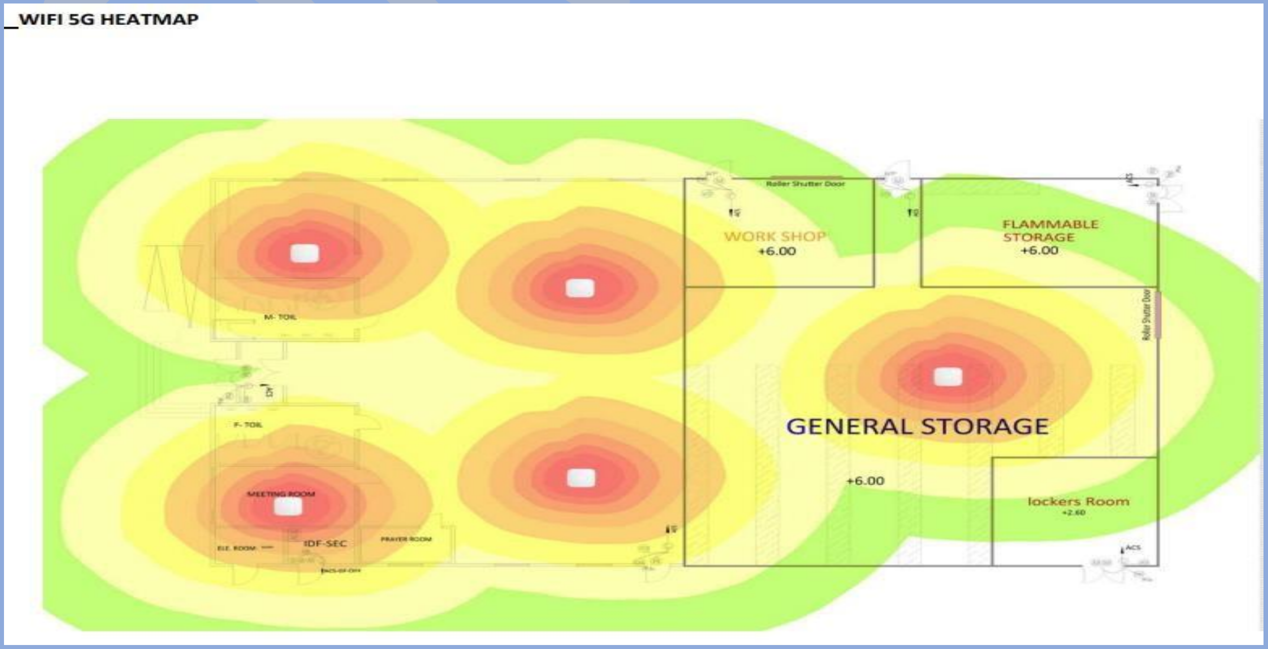
  - Offers longer range and better penetration through walls.

    - Can be more susceptible to interference from other devices using the same frequency.

- **5 GHz:**
    - Provides higher data rates and is less crowded than the 2.4 GHz band.
    - Shorter range compared to 2.4 GHz but less susceptible to interference.

The decision to use 2.4 GHz or 5 GHz would depend on factors like the density of devices, the need for high data rates, and the specific requirements of each area.





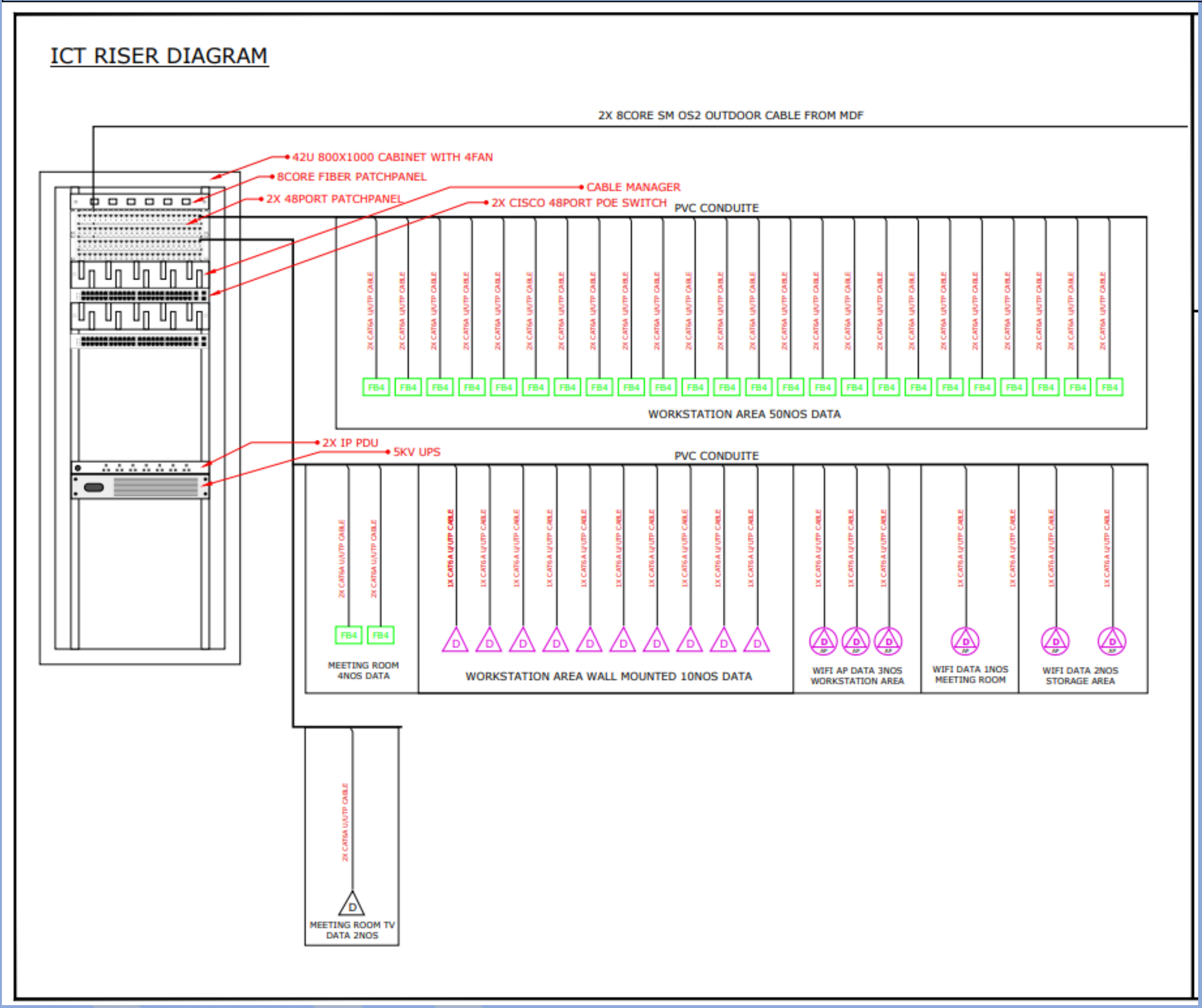
Server Room:

Our network infrastructure comprises multiple switches, firewalls, and patch panels.

Core Switch

1st Switch				
Switch Model	**Port Status**	**Vlan Tag**	**Uplink Ports**	**Uplink Port Status**
Switch 3750 24P UTS(WAN-DMZ)	**23 Used Ports (**1-8,10-24) **1 Free Ports** (8)	**Vlan102** – Ports(1-16) **Vlan194** – Ports(17-24)	Port 27-28 – **SFP Module** Port 25-26 – **SFP Module**	UTS-WAN DMZ-UTI
2nd Switch				
Switch 3560 48P UTS(LAN-DMZ)	**36 Used Ports (**1-10,12-18,21,23,25,28,30-33,36,39-48) **12 Free Ports** (11,19-20,22,24,26-27,29,34-35,37-38)	**Vlan193** – Ports(1-36) **Vlan1** – Ports(37-48)	Port 49 – **SFP Module** Port 51 – **SFP Module**	UTS-DMZ UTS-LAN
MicroTik Router				
3rd Switch				
Switch 3750 24P DMZ (SPI)	**17 Used Ports (**1-6,8,13-14,17-24) **7 Free Ports** (7,9-12,15-16)	**Vlan191** – Ports(1-24)	Port 25 – **SFP Module**	SPI-DMZ
4th Switch				
Switch 3750 48P UIC-WAN UIC-WAN-DMZ UIC LAN	**30 Used Ports (**3-5,10,12-15,18-23,25,29-30,32-33,35-36,38,40-41,43-48) **18 Free Ports** (1-2,6-9,11,16-17,24,26-28,31,34,37,39,42)	**Vlan100** – Ports(1-5) **Vlan192** – Ports(6-40) **Vlan10** – Ports(41-48)	Port 49 – **SFP Module** Port 51 – **SFP Module**	UIC UIC

Fortinet Firewall 200E


ICT RISER DIAGRAM
2X 8CORE SM OS2 OUTDOOR CABLE FROM MDF
42U 800X1000 CABINET WITH 4FAN
8CORE FIBER PATCHPANEL
2X 48PORT PATCHPANEL
CABLE MANAGER
2X CISCO 48PORT POE SWITCH
PVC CONDUITE
2X CAT6A U/UTP CABLE
FB4
WORKSTATION AREA 50NOS DATA
2X IP PDU
5KV UPS
PVC CONDUITE
2X CAT6A U/UTP CABLE
FB4
MEETING ROOM 4NOS DATA
1X CAT6 A U/UTP CABLE
D
WORKSTATION AREA WALL MOUNTED 10NOS DATA
D
AP
WIFI AP DATA 3NOS WORKSTATION AREA
WIFI DATA 1NOS MEETING ROOM
WIFI DATA 2NOS STORAGE AREA
2X CAT6A U/UTP CABLE
D
MEETING ROOM TV DATA 2NOS

ICT Rack Configuration:

1. **Rack Type:**
    - Utilize a standard 19-inch server rack to accommodate all the ICT equipment.
2. **Rack Location:**
    - Place the ICT rack in a designated server room or data center with proper environmental controls.
3. **Fiber Uplink (MDF to IDF):**
    - Install an 8-core fiber optic cable for high-speed connectivity between the Main Distribution Frame (MDF) and Intermediate Distribution Frame (IDF) for ICT.
4. **Switches:**
    - Install two 48-port switches for Data and Wireless connectivity.

- Ensure these switches support the required network protocols and PoE (Power over Ethernet) for APs.

5. **Access Points (APs):**

    - Deploy a total of 5 Access Points distributed strategically across the covered area based on the heatmap analysis.
    - Configure the APs to provide seamless and reliable wireless connectivity.

6. **IP PDUs:**

    - Install 2 IP Power Distribution Units (PDUs) on the rack to manage power distribution and monitor power consumption remotely.

7. **UPS (Uninterruptible Power Supply):**

    - Connect a 5KV UPS to each rack to ensure continuous power supply and protect against power fluctuations or outages.
    - Size the UPS units to provide sufficient runtime for graceful shutdowns in case of extended power outages.

8. **HLD (High-Level Design) & LLD (Low-Level Design) Diagrams:**

    - Develop comprehensive High-Level Design (HLD) and Low-Level Design (LLD) diagrams detailing the architecture, connectivity, and specifications of the ICT rack setup.
    - Include information on network topology, device configurations, cabling, and power distribution.

9. **Commissioning Process:**

    - Plan and document the commissioning process for the devices in the rack.
    - Include steps for initial setup, configuration, and testing to ensure all components function as intended.

10. **Collaboration with Neom IT Team:**

    - Coordinate closely with the Neom IT Team to synchronize any further changes or updates to the ICT rack setup.
    - Document change management processes to ensure smooth integration with existing IT infrastructure.

11. **Environmental Considerations:**

    - Ensure proper ventilation and cooling within the server room to maintain optimal operating temperatures for ICT equipment.

12. **Security Measures:**

- Implement physical security measures, such as restricted access to the server room and rack, to safeguard critical infrastructure.

13. Monitoring and Management:

- Set up monitoring systems for real-time tracking of network performance, power usage, and environmental conditions within the server room.

14. Documentation:

- Maintain detailed documentation for the entire setup, including equipment specifications, configurations, and any changes made during the lifecycle.

ELV Rack Configuration

Connectivity:

1. **Fiber Uplink (MDF to IDF):**

    - Utilize an 8-core fiber optic cable for a robust and high-speed uplink between the Main Distribution Frame (MDF) and the ELV Intermediate Distribution Frame (IDF) rack.

CCTV and Access Control System (ACS):

2. **Network Video Recorder (NVR):**

    - Install the NVR in the existing CCTV control room to centrally manage and store video feeds from surveillance cameras.

3. **Switch for CCTV and ACS:**

    - Implement a 48-port switch dedicated to handling both Closed-Circuit Television (CCTV) and Access Control System (ACS) devices.

    - Ensure the switch supports Power over Ethernet (PoE) for easy deployment of IP cameras and ACS devices.

4. **ACS Control Panel:**

    - Install the ACS control panel in the IDF room to centrally manage access control permissions and events.

    - Connect the ACS control panel to the switch for seamless integration with other ELV components.

5. **Integration with Fire Alarm:**

    - Establish connectivity between the ACS and the fire alarm module for coordinated response during security and emergency situations.

Public Address (PA) System:

6. **PA System on ICT Rack:**

    - Integrate the Public Address (PA) system into the Information and Communication Technology (ICT) rack for centralized audio management.

    - Connect PA system components to the network for remote control and monitoring.

Power Distribution:

7. **IP PDUs (Power Distribution Units):**

    - Install two IP PDUs on the ELV rack to efficiently manage power distribution, monitor consumption, and remotely control power outlets.

8. **Uninterruptible Power Supply (UPS):**

- Deploy a 3KV UPS on the ELV rack to ensure continuous power supply, protecting critical ELV components from power disruptions.
- Size the UPS to provide sufficient runtime during power outages.

Collaboration with Neom IT Team:

9. **Synchronization with IT Team:**

   - Coordinate closely with the Neom IT Team for any further changes or updates to the ELV rack setup.
   - Establish a streamlined communication process to ensure seamless integration with existing IT infrastructure.

Documentation and Planning:

10. **Detailed Documentation:**

    - Develop detailed High-Level Design (HLD) and Low-Level Design (LLD) diagrams outlining the architecture, connectivity, and specifications of the ELV rack setup.
    - Maintain comprehensive documentation for all ELV components, configurations, and connectivity details.

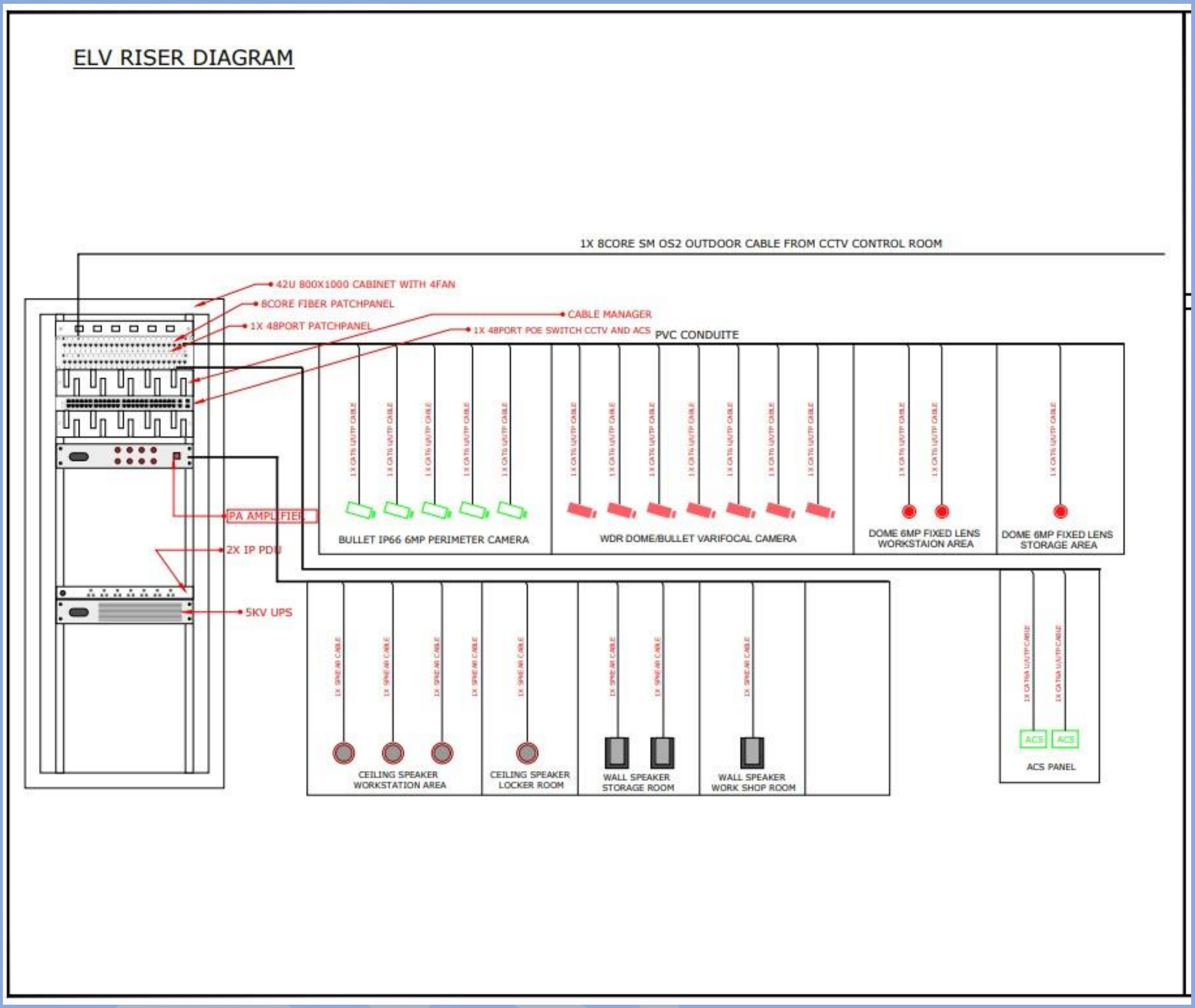
11. **Testing and Commissioning:**

    - Plan for thorough testing and commissioning of the ELV rack to validate the functionality of each component.
    - Conduct tests to ensure proper integration with other systems and adherence to security protocols.

Security and Safety:

12. **Security Measures:**

    - Implement access controls and monitoring systems to secure the ELV rack against unauthorized access.
    - Consider environmental monitoring to safeguard equipment against temperature and humidity fluctuations.



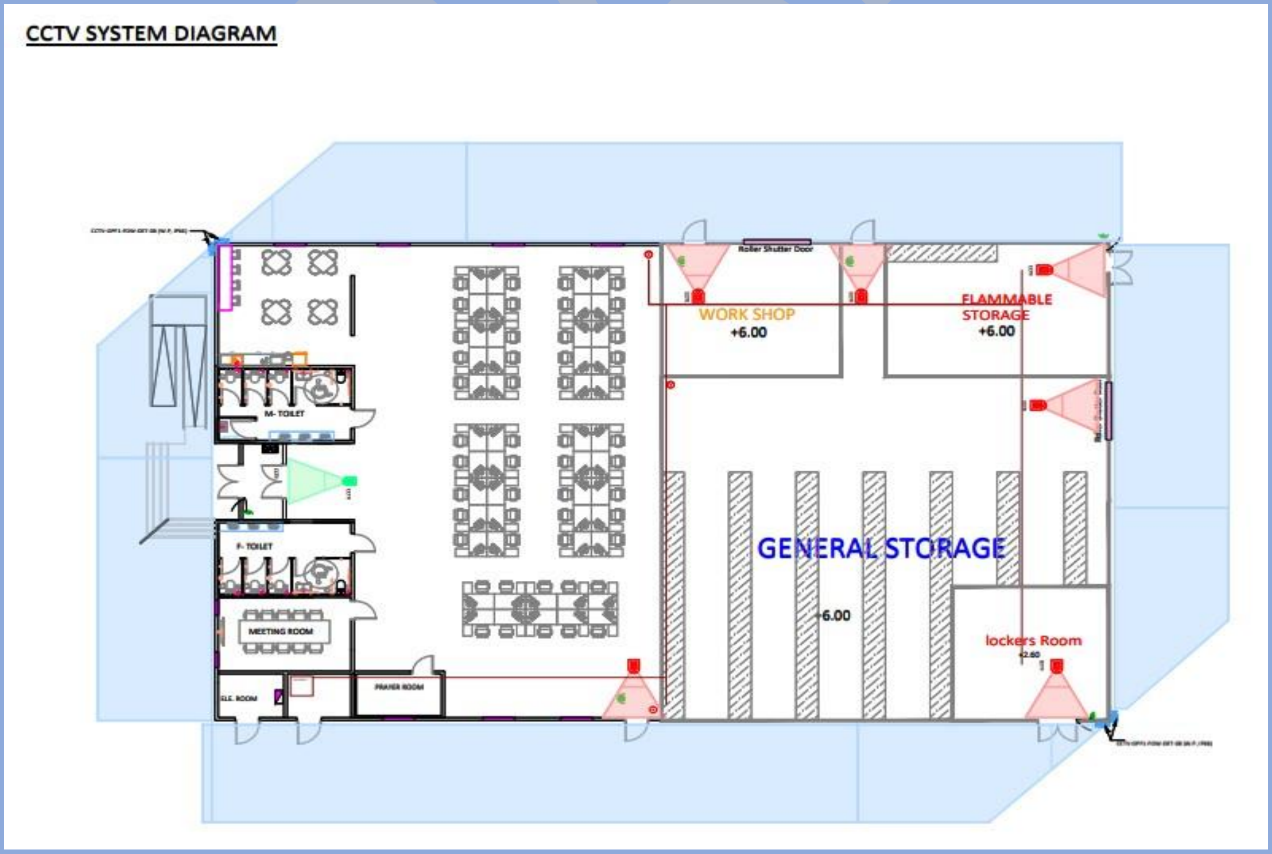
INSTALLATION OF CCTV:

The installation of CCTV in these areas the total number of CCTV cameras is having 13.

- **CCTV in Meeting Room:**
  - Typically, CCTV cameras may be installed at strategic locations to monitor activities within and around the meeting room.
  - Provides security and oversight during meetings.
- **CCTV at Boller Shiner Door:**
  - If the purpose of the door involves security or restricted access, 4 CCTV cameras may be installed to monitor and record activity around the door.
- **CCTV in Work Shop:**
  - 1 Dome cameras may be installed to enhance security in the workshop area, monitor tools and equipment, and ensure safety.

- **CCTV in Flammable Storage:**
    - Critical for safety and compliance, CCTV cameras may monitor the storage of flammable materials to prevent unauthorized access and ensure adherence to safety protocols.
- **CCTV in Lockers Room:**
    - Commonly installed to enhance security and monitor access to lockers, ensuring the safety of personal belongings.
- **CCTV in GENDS (Restrooms):**
    - While CCTV in restrooms raises privacy concerns, it is generally not recommended. Privacy laws often prohibit the installation of cameras in such areas.
- **CCTV in General Storage:**
    - 1 Dome Camera may be installed to monitor access to general storage areas.
    - Helps prevent theft, unauthorized access, and ensures the security of stored items.

The installation of CCTV should be done with careful consideration of privacy, legal regulations, and the specific security needs of each area. It's important to strike a balance between security measures and respecting the privacy of individuals within the facility.

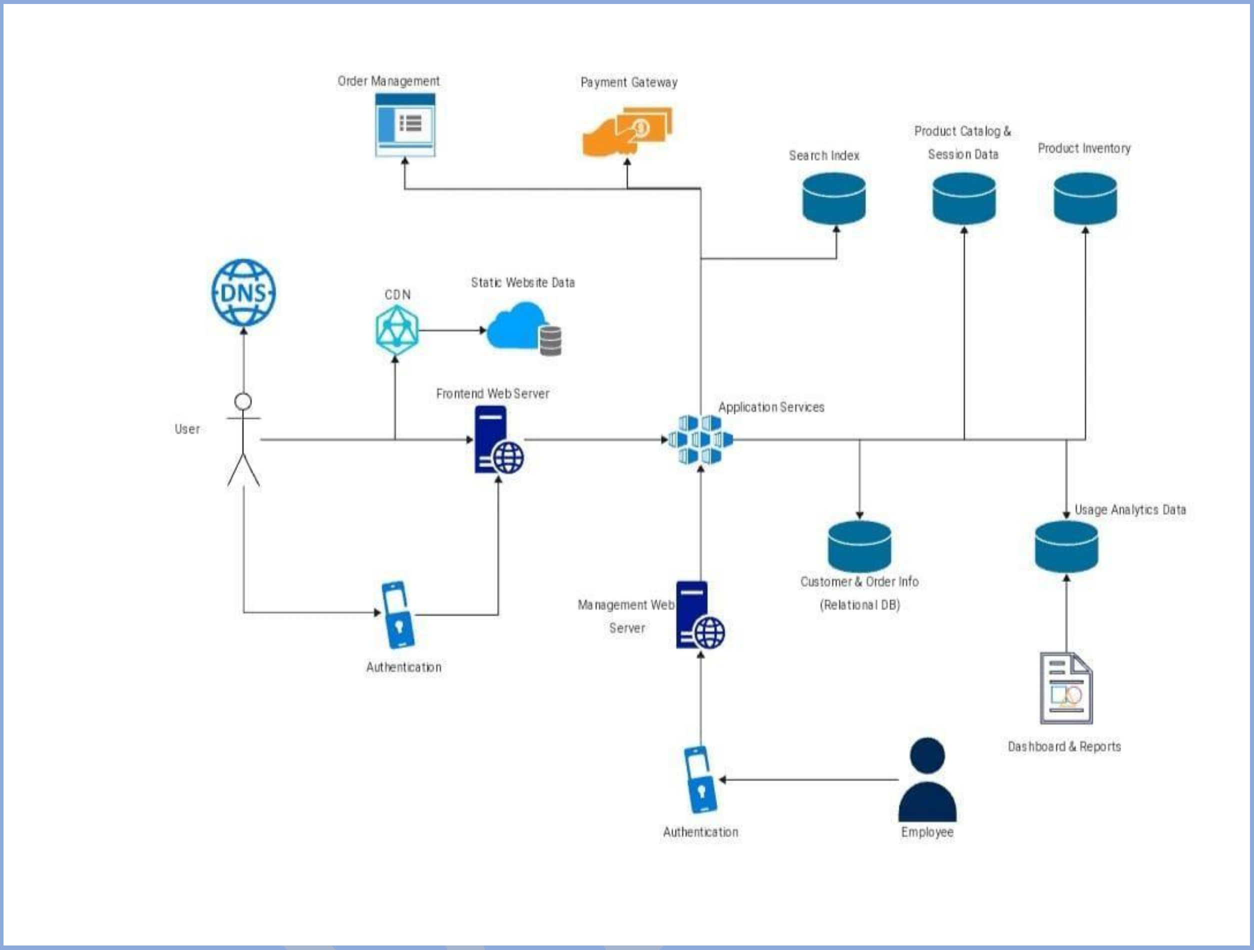

CCTV SYSTEM DIAGRAM

High-Level Design (HLD):

1. **Overview:**
    - **Purpose:**
        - Define the purpose of the system architecture to provide a clear understanding of its goals.
    - **Scope:**
        - Identify specific aspects of the system's functionality and non-functional characteristics.
2. **Key Components:**
    - **Modules or Subsystems:**
        - Provide a detailed breakdown of each module, specifying their responsibilities and interactions.
    - **Interfaces:**
        - Define input/output interfaces for each module, including data formats and communication protocols.
    - **Data Flow:**
        - Present a comprehensive view of how data traverses the system, considering inputs, transformations, and outputs.
3. **Architectural Patterns:**
    - **Architecture Type:**
        - Justify the chosen architectural pattern and explain how it aligns with the project requirements.
    - **Deployment Diagrams:**
        - Offer visual representations of how the system components will be deployed across various environments.
4. **Technology Stack:**
    - **Programming Languages and Frameworks:**
        - Specify versions and justify the choice of programming languages and frameworks.
    - **Database Systems:**
        - Detail the database systems, their configurations, and how data will be managed.

- **External APIs:**
    - Enumerate external APIs and elucidate their roles in the system.

5. **Security Considerations:**
    - **Authentication and Authorization:**
        - Detail the authentication mechanisms and authorization workflows.
    - **Data Encryption:**
        - Specify encryption algorithms, key management, and secure data transmission methods.
6. **Scalability and Performance:**
    - **Scalability Plan:**
        - Provide a roadmap for scaling the system horizontally or vertically.
    - **Performance Metrics:**
        - Establish benchmarks and performance expectations for critical functions.
7. **Error Handling and Logging:**
    - **Error Handling Strategy:**
        - Define a robust strategy for handling errors, including user feedback and system alerts.
    - **Logging Mechanism:**
        - Detail how logs will be generated, stored, and monitored.
8. **Integration Points:**
    - **Third-Party Integrations:**
        - Detail the protocols and data formats for third-party integrations.
    - **API Contracts:**
        - Provide a contract for each API, specifying endpoints, methods, and expected responses.



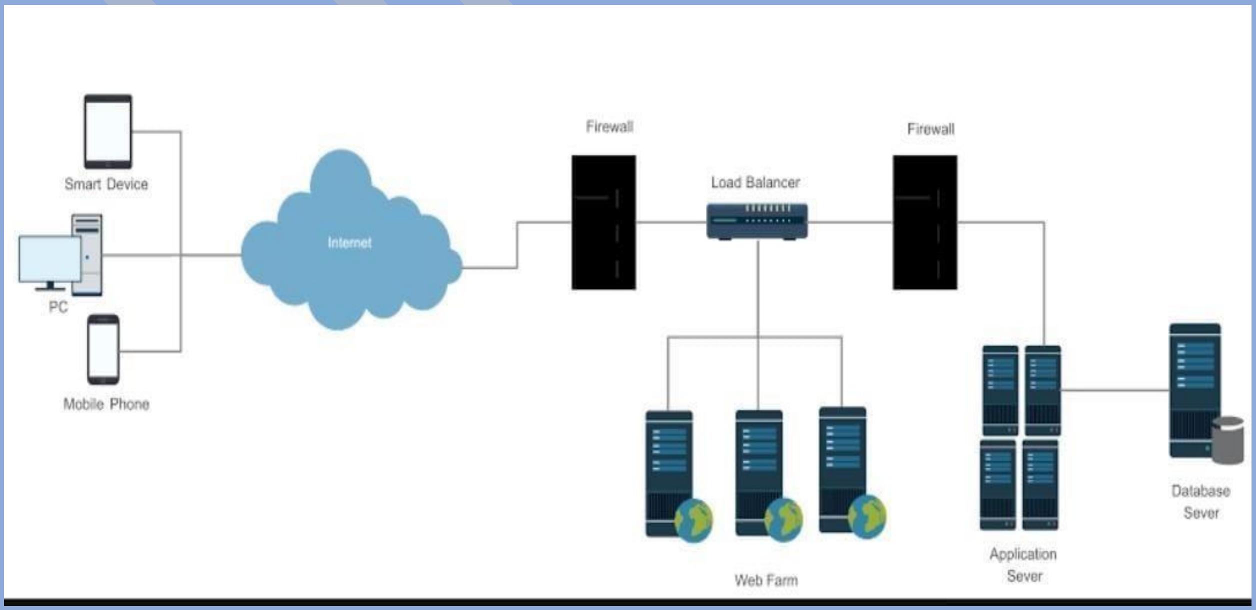
Low-Level Design (LLD):

1. **Detailed Component Design:**
    - **Module-Level Design:**
        - Break down each module into classes or components, specifying their roles and relationships.
    - **Class and Function Definitions:**
        - Provide detailed specifications for each class, method, and function, including input parameters and return values.
2. **Data Structures and Algorithms:**
    - **Data Structures:**
        - Enumerate and justify the choice of data structures for each critical aspect of the system.
    - **Algorithms:**

        - Specify algorithms for core functionalities, emphasizing efficiency and scalability.

3. **Database Schema:**
    - **Database Tables and Relationships:**
        - Detail tables, their relationships, primary/foreign keys, and constraints.
    - Query Optimization:
        - Consider indexing strategies and other optimizations for database queries.
4. **Detailed Interface Design:**
    - **API Endpoints:**
        - Specify each API endpoint, including the structure of requests and responses.
    - **User Interface Components:**
        - If applicable, describe the design and interactions of user interface components.
5. **Error Handling and Recovery:**
    - **Error Codes and Messages:**
        - Provide a comprehensive list of error codes and corresponding user-friendly error messages.
    - **Recovery Mechanisms:**
        - Detail recovery strategies, including automatic recovery and manual interventions.
6. **Concurrency and Multithreading:**
    - **Concurrency Controls:**
        - Specify mechanisms for handling concurrent access to shared resources.
    - **Thread Management:**
        - If applicable, detail how multithreading is managed, considering thread safety.
7. **Security Implementation:**
    - **Data Encryption Mechanisms:**
        - Specify encryption protocols and implementations for data at rest and in transit.
    - **Access Controls:**
        - Define access control lists and mechanisms for enforcing security at various levels.

8. **Testing and Quality Assurance:**
    - **Test Cases:**
        - Develop detailed test cases, covering unit tests, integration tests, and system tests.
    - **Quality Metrics:**
        - Establish metrics for measuring code quality, including code coverage and performance metrics.
9. **Deployment Plan:**
    - **Deployment Scripts:**
        - Provide scripts for deploying the system, including version control and rollback procedures.
    - **Configuration Management:**
        - Outline how configurations will be managed across development, testing, and production environments.
10. **Documentation:**
    - **Code Documentation:**
        - Embed comments within the code, explaining complex algorithms, assumptions, and design decisions.
    - **User Manuals:**
        - If applicable, create user manuals to guide end-users on system usage and troubleshooting.


Smart Device
PC
Mobile Phone
Internet
Firewall
Load Balancer
Firewall
Web Farm
Application
Sever
Database
Sever