PROBLEM IDENTIFICATION & STAKEHOLDER ANALYSIS

Team FabFive

MAIN CC Portal

Prepared by:

Praval Pattam
Theenesh Potluri
Mayank Jhawer
Pranav Sai Sarvepalli
Koka Sai Abhishek

Problem statement:

The current system for computer servers and campus Wi-Fi authentication at NIT Calicut is **inefficient and unreliable**, causing significant disruptions for students, faculty, and researchers. Key pain points include:

1. **Server Management Issues**:
    - **Lack of Transparency**: No visibility into server maintenance schedules, leading to unexpected downtimes.
    - **Access Management**: No centralized system to view server access details (IP addresses, credentials).
    - **Communication Issues**: Reliance on emails for requests (server access, VPN, issue reporting), resulting in delays.
    - **Data Loss**: Difficulty reporting server downtimes/data loss, risking academic/research work.
2. **Campus Wi-Fi Authentication Issues**:
    - **Single Device Limitation**: Users can only log in on one device; manual logouts are cumbersome.
    - **Automatic Disconnections**: Frequent Wi-Fi drop-offs requiring re-authentication.
    - **Inefficient Resolution**: Users must call CNC for help, causing delays.

Evidence of the Problem:

- **Surveys**: Widespread dissatisfaction with email-based systems and Wi-Fi authentication.
- **Interviews**: Frequent complaints about server access delays and Wi-Fi issues.

Stakeholder Identification:

Stakeholder Group	Roles & Interests
Primary Users	
Students	Need reliable server/Wi-Fi access for coursework, projects, and research.
Faculty	Depend on servers for teaching, research, and administrative tasks.

Stakeholder Group	**Roles & Interests**
Researchers	Require uninterrupted server access for simulations, data analysis, and experiments.
Secondary Users	
IT Administrators	Manage server access, maintenance, and user permissions.
CNC Staff	Handle Wi-Fi authentication and troubleshoot connectivity issues.
Decision-Makers	
Head of CNC	Approve systems balancing cost, security, and compliance.
College Administration	Allocate budget and resources for IT infrastructure.
Regulators	
Data Security Officer	Ensure compliance with data privacy laws (e.g., institutional security protocols).

Interview Questions:

1. How often do you use the servers and Wi-Fi at NIT Calicut for your academic or research work?
2. What challenges do you face with the current server management system and Wi-Fi authentication?
3. How do server downtimes and Wi-Fi issues affect your work or research?
4. What features would you like to see in a new server management and Wi-Fi authentication system?
5. How do you currently handle server access requests, issue reporting, or Wi-Fi authentication problems? What are the pain points in this process?

Interview with a Stakeholder: Student

https://youtu.be/YDTCX5KebkM

Initial Requirements

Functional Requirements

1. **Inputs the System Should Accept**:
   - User requests (server access, VPN, Wi-Fi logout).
   - Administrative actions (approvals, maintenance updates).
   - Authentication data (credentials, device details).
2. **Outputs the System Should Produce**:
   - Confirmation emails/SMS for submitted requests.
   - Real-time status updates and maintenance notifications.
   - Dashboards and reports for admins.
3. **Data the System Should Store**:
   - User profiles, server metadata, Wi-Fi session logs, issue reports.
   - Shared data for security systems (audit logs) and resource allocation systems (usage trends).
4. **Computations the System Should Perform**:
   - Validate credentials, prioritize issues, encrypt sensitive data.
   - Calculate SLA compliance metrics and predict maintenance needs.
5. **Timing and Synchronization**:
   - Real-time alerts for critical issues.
   - Scheduled tasks (e.g., maintenance notifications, monthly reports).
   - Synchronization with external systems (e.g., CNC database).

Non-Functional Requirements

1. **Security**:
   - Encrypt user credentials and comply with data protection laws.
2. **Reliability**:
   - 99.9% uptime for servers and Wi-Fi authentication.
3. **Usability**:
   - Intuitive interface for non-technical users (students, faculty).
4. **Scalability**:
   - Support 100+ simultaneous users and future growth.

Specifications:

- **Web-Based Platform**: Accessible via desktop/mobile.
- **Automated Alerts**: Notify users of maintenance schedules via SMS/email.
- **Audit Logs**: Track server access and Wi-Fi authentication for security reviews.

Value Proposition

- **For Users**: Save time, reduce frustration, and ensure continuity in academic/research work.
- **For IT/CNC Staff**: Streamline workflows, reduce manual tasks, and improve response times.
- **For Institution**: Enhance productivity, data security, and compliance.