Team Details

a. **Team name:** CyberSentinel
b. **Team leader name:** Urvi Chaudhari
c. **Domain :** Security
d. **Problem Statement:** Real-Time Cyber Threat Detection and Alert System.

PROPOSED SOLUTION

- **Data Collection:** Monitor network traffic using tools (Wireshark, tcpdump) and collect logs from routers, firewalls, and endpoints.
- **Threat Detection:** Use signature-based detection (Snort) for known threats and ML algorithms (e.g., Random Forest) for anomalies.
- **Alert System:** Generate real-time alerts by severity (Critical, Warning, Info) and notify via Slack, email, or SMS.
- **Dashboard:** Use frameworks (React.js, Angular) to visualize traffic, threats, and historical data in real-time.
- **Infrastructure Integration:** Connect with SIEM systems (Splunk, ELK) for analytics and automate responses with SOAR tools (e.g., Cortex XSOAR).

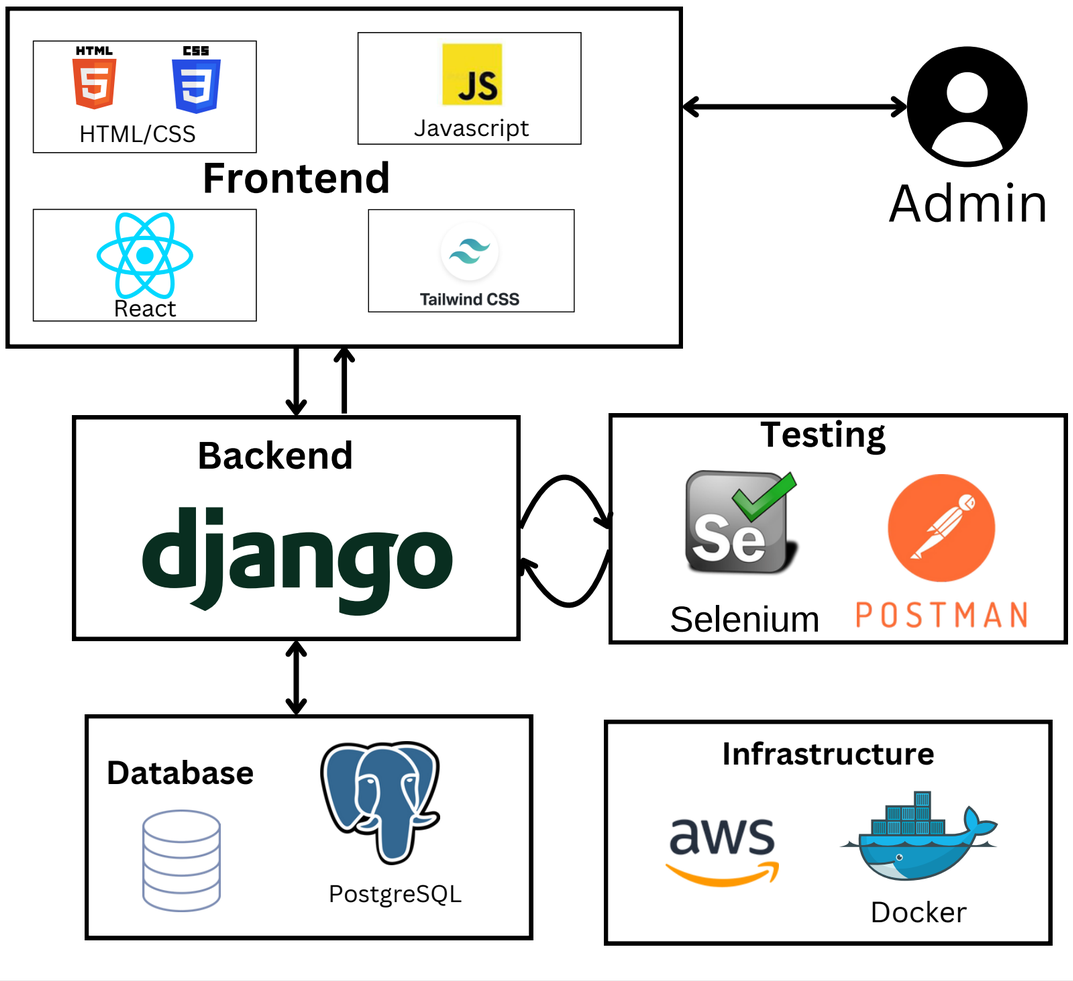
INNOVATIVENESS AND UNIQUENESS

- **Hybrid Detection:** Combines signature-based and ML-driven anomaly detection for comprehensive threat identification.
- **Severity-Based Alerts:** Real-time alerts (Critical, Warning, Info) sent via Slack, Email, or SMS for prioritized response.
- **System Integration**: Seamlessly integrates with SIEM (Splunk, ELK) and SOAR tools (Cortex XSOAR).
- **Visual Dashboard**: Real-time graphs and charts for intuitive threat analysis and network monitoring.
- **Automated Response**: SOAR-integrated playbooks enable rapid mitigation, such as IP blocking .

TECHNICAL APPROACH

- **Front-End:**
  - React.js: UI development
  - Chart.js/D3.js: Real-time data visualization
  - Socket.IO-client: Real-time communication
  - Tailwind CSS/Material-UI: Styling and responsive design
- **Back-End:**
  - Python (Django): Business logic, APIs, and threat detection
  - Django REST Framework (DRF): RESTful APIs
  - Django Channels: WebSocket support for real-time alerts
- **Real-Time Data Processing:**
  - Snort/Suricata/Zeek: Signature-based threat detection Database.
  - PostgreSQL: Stores network logs and threat data
  - Redis: Caching and real-time storage
- **Alert System:**
  - Twilio/SendGrid: SMS/email notifications
  - Push Notifications: Web alerts (optional)
- **Security:**
  - JWT: Secure authentication
  - SSL/TLS: Secure communication
- **Testing & Debugging:**
  - Postman: API testing
  - Selenium: End-to-end front-end testing (optional)

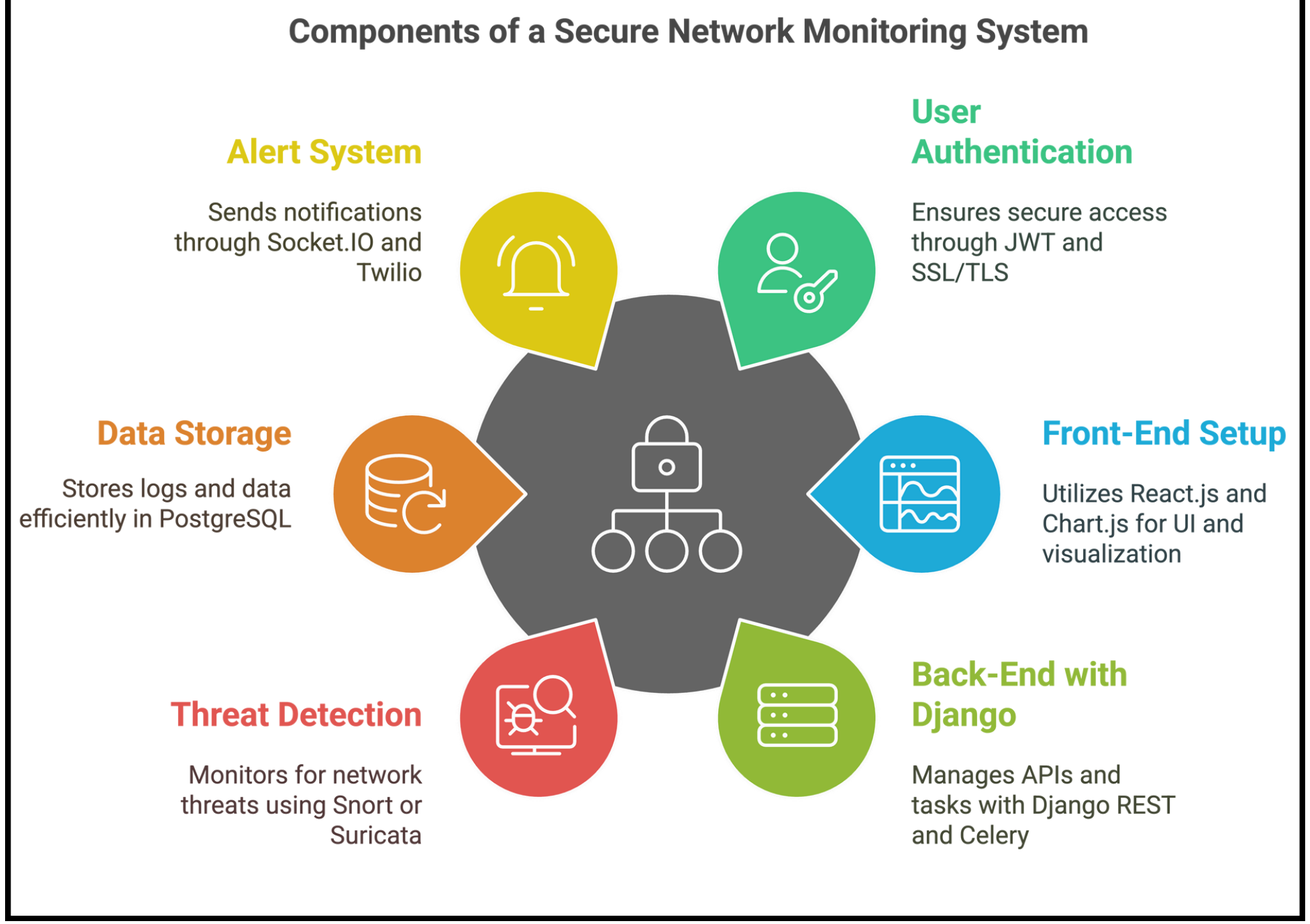
TECHNOLOGY USED



TECHNICAL APPROACH

Technology -

- **Authentication & Security:** JWT for login, SSL/TLS for secure communication.
- **Front-End:** React.js, Chart.js/D3.js for UI and real-time updates via Socket.IO.
- **Back-End:** Django REST for APIs, Celery for async tasks, Django Channels for real-time alerts.
- **Threat Detection:** Snort, Suricata, Zeek for network monitoring.
- **Storage:** PostgreSQL for data storage, Redis for caching.
- **Alerts:** Real-time via Socket.IO, notifications via Twilio/SendGrid.
- **Testing:** Postman for APIs, Selenium for front-end testing.



FEASIBILITY AND VIABILITY

1.Feasibility Analysis

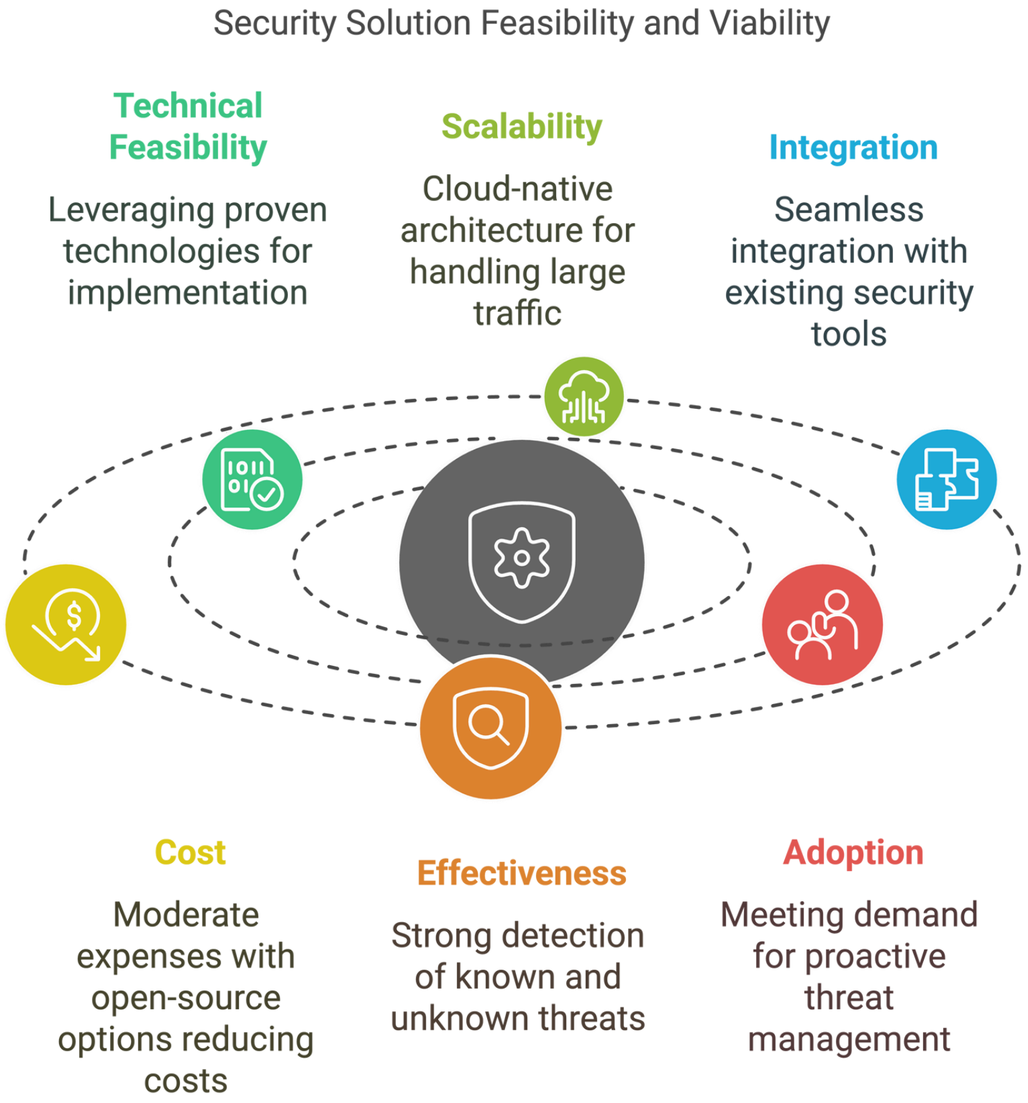
- Technical: Uses proven tools (Wireshark, Snort, Random Forest, Kubernetes).
- Scalability: Cloud-native with Docker & Kubernetes for easy scaling.
- Integration: Integrates smoothly with existing security tools (SIEM, SOAR).

2.Challenges and Risks

- Privacy Concerns: User reluctance to share sensitive data.
- Traffic Volume: Risk of rate limiting during peak times.
- Tool Compatibility: Integration challenges with varied platforms.
- Evolving Threats: Constantly changing attack techniques.

3.Strategies to Overcome Challenges

- Privacy Concerns: Anonymize and encrypt user data.
- Traffic Volume: Implement caching and optimize queries.
- Tool Compatibility: Ensure regular updates and support for multiple platforms.
- Evolving Threats: Continuously update detection algorithms and models.



Team Details

Harshvardhan Bhosale : Second Year (ENTC)
Email: hbhosale2004@gmail.com | Mobile: 8830752464

Sakshi Chougule : Second Year (Information Technology)
Email: chougulesakshi1311@gmail.com | Mobile: 8530853828

Kartik Sirsilla : Second Year (Information Technology)
Email: ksirsilla0908@gmail.com | Mobile : 9325562464

Urvi Chaudhari : Second Year (ENTC)
Email: urvi1655@gmail.com | Mobile: 8446155994