Sayansi Yathu Authentication Workflow

```
Start
  →
User opens login page
-Enter identifier + password
- Optional: remember device
- Device fingerprint captured
  →
Frontend POST
backend-php/auth/login.php
- identifier - password
- remember_device-
device_fingerprint
  →
Backend: Validate JSON
Check empty fields
Check account lock status
  →
Account locked?  --Yes→  Return error: "Too many attempts"  →  Security logs: login_failure user_id, IP, user_agent, fingerprint, timestamp  →  Redirect to login  →  End
  |
  No
  ↓
Identify user - If student_id: join students → users
- Else check email
- Else check username
  ↓
User found?  --No→  Return error: "Invalid credentials"
  |
  Yes
  ↓
Verify password
  ↓
Password correct?  --No→  Return error: "Invalid credentials"
  |
  Yes
  ↓
Successful login actions - Reset failed_attempts - Generate JWT (HS256, 30m) - Set sy_auth cookie - Prepare user profile - Select dashboard_route
  ↓
Security logs: login_success user_id, IP, user_agent, fingerprint, timestamp
  →
Return JSON: token, user data, dashboard_route, requires_verification=false
  →
Frontend: store JWT (localStorage)
-Store profile
-Redirect to dashboard_route
  →
Token exists?  --Yes→  Token valid?  --Yes→  Role matches page?  --Yes→  Protected page access
-Frontend sends JWT (Authorization)
-Backend check_auth.php validates token & role
  →  End

Process

Increment failed_attempts
-Lock if threshold reached
```