

American International University-Bangladesh (AIUB)  
**Department of Computer Science  
Faculty of Science & Technology (FST)**

**Project Title:   
Integrated Application Usage Tracking & Parental Control System**

**Supervised by:**

TONNY SHEKHA KAR

A Software Engineering Project Submitted

By

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Semester: Summer\_23\_24** | | **Section: H** | **Group Number: 09** | |
| SN | Student Name | Student ID | Contribution (CO3+CO4) | Individual Marks |
| 1 | A. F. M. RAFIUL HASSAN | 22-47048-1 |  |  |
| 2 | MD. ASHIKUZZAMAN ABIR | 22-47006-1 |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# FUNCTIONAL REQUIREMENTS

**1. Software Registration**

**1.1** The user should provide a valid email address for registration.

* **Priority Level**: High
* **Precondition**: None

**1.2** The user should provide a valid phone number for registration.

* **Priority Level**: High
* **Precondition**: None

**1.3** The user should provide a valid and unique username at registration.

* **Priority Level**: High
* **Precondition**: None

**1.4** The user should provide their date of birth during registration.

* **Priority Level**: High
* **Precondition**: None

**1.5** The user should provide a valid password of at least 6 characters, including a mixture of uppercase letters, lowercase letters, and numbers during registration.

* **Priority Level**: High
* **Precondition**: None

**1.6** The user should confirm the provided password.

* **Priority Level**: High
* **Precondition**: The user entered the password same as the provided password

**2. Software Login**

**2.1** The software shall allow users to log in with their given username and password.

* **Priority Level**: High
* **Precondition**: The user has a valid username and password.

**2.2** The email address and password shall be verified with database records.

* **Priority Level**: High
* **Precondition**: The user has entered login credentials.

**2.3** If the login is successful, the home page of the user account shall be displayed.

* **Priority Level**: High
* **Precondition**: The user has entered valid login credentials.

**2.4** If the email address and/or password are incorrect, the system shall prompt the user to enter the correct email address and password and retry login.

* **Priority Level**: High
* **Precondition**: The user has entered incorrect login credentials.

**2.5** If the number of login attempts exceeds its limit (3 times), the system shall block the user account login for 24 hours.

* **Priority Level**: Medium
* **Precondition**: The user has attempted to log in with incorrect credentials more than 3 times.

**3. Authentication**

**3.1** Users shall enter their email address or phone number to verify their created account.

* **Priority Level**: High
* **Precondition**: The user has completed the registration process.

**3.2** An OTP shall be sent to the user's email address or phone number.

* **Priority Level**: High
* **Precondition**: The user has requested for account verification.

**3.3** If the OTP is sent successfully within 60 seconds, the user shall enter the OTP to verify.

* **Priority Level**: High
* **Precondition**: The OTP has been sent successfully.

**3.4** If the OTP is not sent successfully within 60 seconds, a new OTP shall be resent.

* **Priority Level**: High
* **Precondition**: The OTP sending process has failed.

**4. Usage Monitoring**

**4.1** The user and their parents shall be able to view device usage.

* **Priority Level**: Medium
* **Precondition**: The user has logged in.

**4.2** The system shall provide statistics of total screen time over the last 30 days.

* **Priority Level**: Medium
* **Precondition**: The user has logged in.

**4.3** The system shall provide details about which apps are used over the period and how much time they are used.

* **Priority Level**: Medium
* **Precondition**: The user has logged in.

**4.4** The user and their parents shall be informed about the visited websites.

* **Priority Level**: Medium
* **Precondition**: The user has logged in.

**4.5** The system shall show the list of locked and unlocked apps.

* **Priority Level**: Medium
* **Precondition**: The user has logged in.

**4.6** All the history mentioned above shall be displayed for the last 30 days, after which the history shall be deleted automatically.

* **Priority Level**: Medium
* **Precondition**: The user has logged in.

**5. App Blocking and Filtering**

**5.1** The system shall allow parents to block or restrict access to specific apps or websites deemed inappropriate or excessive.

* **Priority Level**: High
* **Precondition**: The parent has logged in.

**5.2** The system shall implement content filtering based on categories such as violence, adult content, gambling, etc.

* **Priority Level**: High
* **Precondition**: The parent has logged in.

**6. Screen Time Management**

**6.1** The user and parents shall have access to set time limits for device usage per day or app.

* **Priority Level**: High
* **Precondition**: The user or parent has logged in.

**6.2** The system shall allow scheduling of device usage time, such as allowing access only during certain hours like homework hours and bedtime.

* **Priority Level**: High
* **Precondition**: The user or parent has logged in.

**6.3** The system shall provide warnings or notifications as usage limits approach or when time is exceeded.

* **Priority Level**: High
* **Precondition**: The user or parent has logged in.

**6.4** After issuing a warning, the system shall automatically close the apps or systems when usage time is exceeded.

* **Priority Level**: High
* **Precondition**: The usage limit has been exceeded.

**7. Location Tracking and Geofencing**

**7.1** The parent shall have access to GPS tracking to locate the device and provide information about the child's location.

* **Priority Level**: High
* **Precondition**: The parent has logged in and has enabled location tracking.

**7.2** The system shall allow setting up geofences to receive alerts when the child enters or leaves specific locations such as home, school, or forbidden places.

* **Priority Level**: High
* **Precondition**: The parent has logged in and has set up geofences.

**8. Customizable Profiles and Settings**

**8.1** The system shall support multiple user profiles for different family members with individualized settings.

* **Priority Level**: Medium
* **Precondition**: The parent has logged in.

**8.2** The guardian shall be able to log in to the system from their device and control children's activities.

* **Priority Level**: Medium
* **Precondition**: The parent has logged in.

**8.3** The system shall allow customization of restrictions and permissions based on age or user preferences.

* **Priority Level**: Medium
* **Precondition**: The parent has logged in.

**9. Emergency Features**

**9.1** The system shall develop features to quickly alert parents or guardians in case of emergencies, such as panic buttons, emergency contacts, or automated notifications.

* **Priority Level**: High
* **Precondition**: The emergency feature is enabled.

**9.2** The system shall send an emergency notification if the child visits forbidden apps or websites.

* **Priority Level**: High
* **Precondition**: The emergency feature is enabled.

**9.3** The guardians shall be notified when the child starts searching any forbidden website.

* **Priority Level**: High
* **Precondition**: The emergency feature is enabled.

**10. Remote Management**

**10.1** The system shall implement APIs or protocols for remote management of devices and settings.

* **Priority Level**: High
* **Precondition**: The parent has logged in.

**10.2** The system shall allow parents to control and monitor their children's devices from anywhere with an internet connection.

* **Priority Level**: High
* **Precondition**: The parent has logged in and has an internet connection.

**11. Activity Insights and Recommendations**

**11.1** The system shall utilize machine learning and data analytics techniques to provide actionable insights and personalized recommendations for improving digital well-being and usage habits.

* **Priority Level**: Medium
* **Precondition**: The user has logged in.

**12. Data Privacy and Security**

**12.1** The system shall implement strong encryption methods to secure sensitive user data.

* **Priority Level**: High
* **Precondition**: The user has logged in.

**12.2** The system shall secure login information, personal information, and communication between devices.

* **Priority Level**: High
* **Precondition**: The user has logged in.

**13. Access Request for New App**

**13.1** For installing a new app, users (children) shall send an access request to the admin (parent).

* **Priority Level**: High
* **Precondition**: The child has logged in and attempting to install a new app.

**13.2** Only the admin (parent) shall have access to accept or reject the access request.

* **Priority Level**: High
* **Precondition**: The parent has logged in.

**14. Educational Resources**

**14.1** The system shall offer educational materials and resources for parents and children to promote digital literacy and responsible online behavior.

* **Priority Level**: Medium
* **Precondition**: The user has logged in.

**15. Live Screen Monitoring**

**15.1** Parents shall be able to monitor their children's phone screens in real-time.

* **Priority Level**: High
* **Precondition**: The parent has logged in and has enabled live screen monitoring.

**15.2** Children’s phones shall not be notified during the live screen monitoring.

* **Priority Level**: High
* **Precondition**: The parent has enabled live screen monitoring.

**16. Software Logout**

**16.1** Only the admin (parent) shall be able to sign out from this software at any time after a successful login.

* **Priority Level**: High
* **Precondition**: The parent has logged in.

# NON FUNCTIONAL REQUIREMENTS

### Usability

* **Ease of Registration:** A new user should be able to complete the registration process within an average of three minutes and a maximum of five minutes.
  + **Priority Level:** High
* **Login Efficiency:** A returning user should be able to log in within an average of two minutes, including the verification process if applicable.
  + **Priority Level:** High
* **User Interface:** The user interface shall be intuitive and easy to navigate, requiring no more than five clicks to access any major function.
  + **Priority Level:** Medium

### Performance

* **Response Time:** The system shall respond to all user actions, such as registration, login, and configuration changes, within two seconds under normal conditions.
* **Priority Level:** High
* **OTP Delivery:** The OTP for authentication shall be delivered within 60 seconds 95% of the time.
* **Priority Level:** High
* **Real-time Monitoring:** The live screen monitoring feature shall update every five seconds with minimal lag.
* **Priority Level:** Medium

### Availability

* **System Uptime:** The system shall have an uptime of 99.9%, allowing for no more than 8.76 hours of downtime annually.
* **Priority Level:** High
* **Disaster Recovery:** The system shall have a recovery time objective (RTO) of one hour and a recovery point objective (RPO) of 15 minutes.
* **Priority Level:** High

### Security

* **Data Encryption:** All sensitive data, including personal information, passwords, and usage logs, shall be encrypted at rest and in transit using AES-256 encryption.
* **Priority Level:** High
* **Access Control:** The system shall implement role-based access control (RBAC) to ensure only authorized users can perform administrative functions.
* **Priority Level:** High
* **Login Security:** The system shall support multi-factor authentication (MFA) for all accounts to enhance security.
* **Priority Level:** High

### Capacity

* **User Capacity:** The system shall support up to 100,000 registered users, with the capability to scale up to 1,000,000 users.
* **Priority Level:** Medium
* **Data Storage:** The system shall be capable of storing detailed usage data for at least one year for all users, with an automatic purge of data older than one year.
* **Priority Level:** Medium

### Maintainability

* **Modular Architecture:** The system shall be designed using a modular architecture to facilitate easy updates and maintenance.
* **Priority Level:** Medium
* **Code Documentation:** All code shall be thoroughly documented to ensure that future developers can understand and modify it with ease.
* **Priority Level:** Medium

### Documentation

* **User Documentation:** The system shall include comprehensive user manuals and FAQs to help users understand and use all features effectively.
* **Priority Level:** High
* **Technical Documentation:** Detailed technical documentation shall be provided for developers and administrators, including API documentation and system architecture diagrams.
* **Priority Level:** High

### Reliability

* **Error Handling:** The system shall handle errors gracefully, providing clear error messages and guidance for users to resolve issues.
* **Priority Level:** High
* **Retry Mechanism:** The system shall include retry mechanisms for transient failures, such as OTP delivery or network interruptions.
* **Priority Level:** Medium

### Compliance

* **Data Privacy:** The system shall comply with relevant data privacy regulations, such as GDPR and CCPA, ensuring user data is handled appropriately.
* **Priority Level:** High
* **Parental Consent:** The system shall include mechanisms for obtaining and verifying parental consent for child accounts, in compliance with COPPA.
* **Priority Level:** High

### Scalability

* **Load Handling:** The system shall be able to handle a load of up to 10,000 concurrent users without performance degradation.
* **Priority Level:** Medium
* **Elastic Scaling:** The system shall support elastic scaling to accommodate sudden spikes in usage, such as during new feature rollouts or marketing campaigns.
* **Priority Level:** Medium

### Support and Training

* **Customer Support:** The system shall provide 24/7 customer support to assist users with any issues or questions.
* **Priority Level:** Medium
* **Training Resources:** The system shall include training resources, such as video tutorials and webinars, to help users make the most of its features.
* **Priority Level:** Medium

1. **PROJECT DEVELOPMENT CONSTRAINTS**
2. **Budget Constraints:**
   * The project budget is limited to $500,000, which includes development, testing, deployment, and initial marketing efforts.
   * Any third-party services or APIs used must fit within this budget without compromising essential functionality.
3. **Time Constraints:**
   * The project must be completed within a 12-month timeframe, with the following milestones:

* Requirements Gathering and Planning: 2 months
* Design and Prototyping: 2 months
* Development: 5 months
* Testing and Quality Assurance: 2 months
* Deployment and Launch: 1 month

1. **Resource Constraints:**
   * The development team is limited to 10 members, including developers, testers, UX/UI designers, and project managers.
   * Access to external consultants and specialists is restricted and must be pre-approved based on budget allowances.
2. **Technology Constraints:**
   * The system must be developed using predefined technology stacks, including:
     + Frontend: React.js
     + Backend: Node.js with Express.js
     + Database: MongoDB
     + Mobile Platforms: Android and iOS using React Native
     + Cloud Services: AWS or Azure for hosting and storage
   * Compatibility with legacy systems or platforms outside these stacks is not guaranteed and may require additional resources.
3. **Regulatory Constraints:**
   * The system must comply with GDPR, CCPA, COPPA, and other relevant data protection and privacy regulations.
   * Any data storage and processing must meet local jurisdictional requirements, especially for storing sensitive data related to children.
4. **Quality Constraints:**
   * The system must pass all specified non-functional requirements related to performance, security, and usability before release.
   * All major features must achieve a minimum of 95% test coverage, and critical bugs must be resolved prior to deployment.
5. **Dependency Constraints:**
   * The project is dependent on timely delivery and integration of third-party services such as SMS/Email OTP providers, payment gateways, and map services for geofencing.
   * Delays in these services can impact the overall project timeline and must be managed accordingly.
6. **User and Stakeholder Constraints:**
   * Regular feedback must be incorporated from key stakeholders, including parents, children, educators, and security experts.
   * The system must support multilingual interfaces, at least for English, Spanish, and French, to cater to a broader user base.
7. **Operational Constraints:**
   * Post-launch support and maintenance must be planned within the budget, ensuring that the system operates smoothly and user issues are resolved promptly.
   * Regular updates and feature enhancements must be scheduled to keep the system competitive and secure.
8. **Ethical Constraints:**
   * The system must ensure the ethical use of monitoring and control features, respecting the privacy and autonomy of users, especially children.
   * Clear communication and consent processes must be in place to inform users about data collection and usage policies.