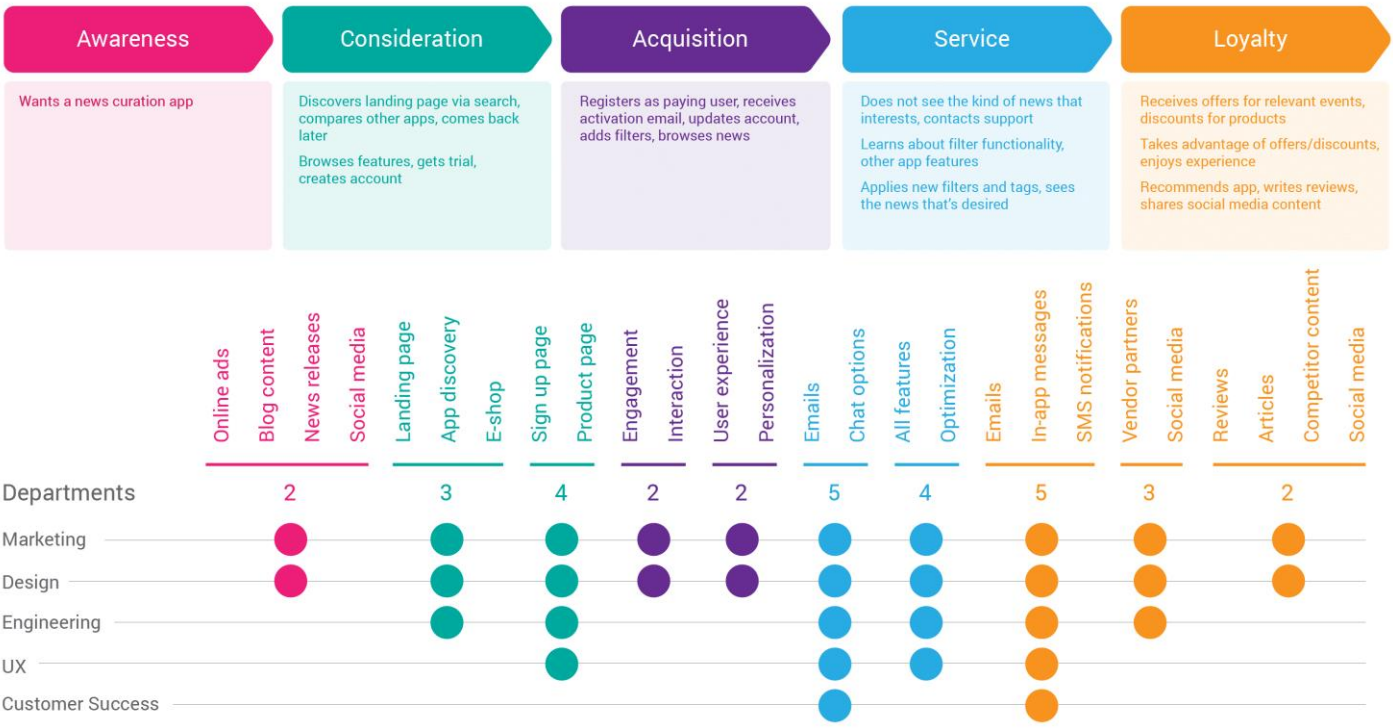
3. Requirement Analysis:

1.Customer Journey Map:



1. Awareness & Consideration:

- Phishing Risks: Online ads, blog content, and social media campaigns can be targeted by phishing attacks or fake links leading to malicious sites.
- Data Privacy: Collecting user data for targeted marketing requires compliance with privacy laws like GDPR.

2. Acquisition:

- Secure Sign-ups: Implementing multi-factor authentication (MFA) to secure account creation.
- Email Security: Activation emails should be protected against spoofing and phishing using SPF, DKIM, and DMARC.
- Data Encryption: Storing user credentials securely using hashing algorithms like bcrypt.

3. Service:

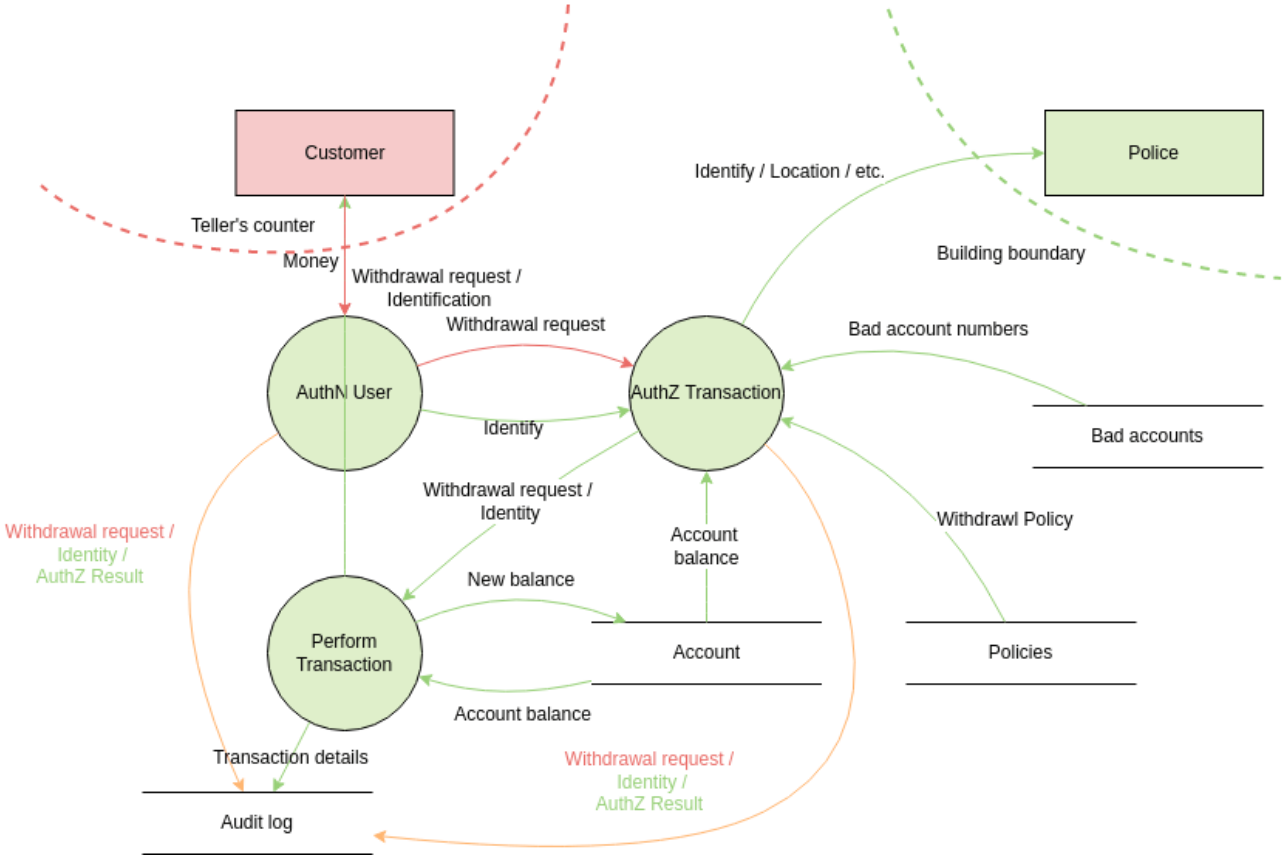
- User Authentication: Ensuring secure login mechanisms (OAuth, biometric authentication).

- Data Protection: Applying encryption for user preferences and filters.
- Secure Chat Options: Encrypting chat messages to prevent data leaks.

4. Loyalty:

- Fake Reviews & Social Engineering: Ensuring reviews are not manipulated or influenced by bots or fake accounts.
- Secure Vendor Partnerships: Ensuring vendors follow cybersecurity best practices to prevent data breaches.
- Content Security: Protecting against misinformation and fake articles by verifying sources.

2.Data flow Diagram:



1. Authentication & Authorization (AuthN & AuthZ)

- Authentication (AuthN): Verifying the identity of the user requesting a transaction.
    - Cybersecurity Risks: Weak authentication methods (e.g., simple passwords) can lead to unauthorized access.

    - Mitigation: Implement multi-factor authentication (MFA) for enhanced security.
- Authorization (AuthZ): Determining if the user has the right permissions to perform the transaction.
    - Cybersecurity Risks: Improper access control may allow unauthorized users to withdraw funds.
    - Mitigation: Role-based access control (RBAC) and least privilege principles should be enforced.

2. Transaction Security

- Account Balance Validation: Ensures sufficient funds are available before approving withdrawals.
- Withdrawal Policy Enforcement: Prevents excessive or suspicious transactions based on predefined rules.
    - Cybersecurity Risks: Policy bypassing through social engineering or insider threats.
    - Mitigation: AI-powered fraud detection and real-time monitoring.

3. Logging & Auditing

- Audit Logs: Store transaction details for later review and security analysis.
    - Cybersecurity Risks: If logs are not protected, attackers could tamper with records to hide fraud.
    - Mitigation: Use immutable logging techniques and monitor logs for anomalies.

4. Fraud & Anomaly Detection

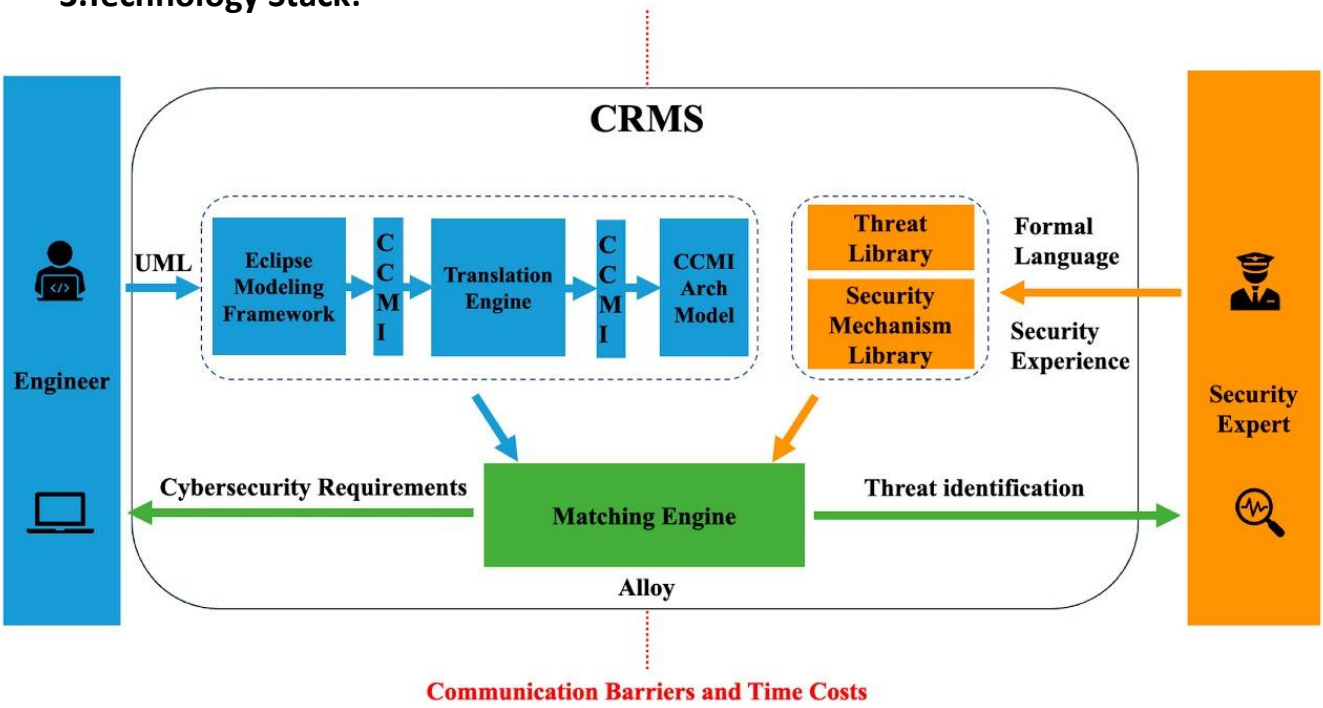
- Bad Account Detection: Identifies suspicious accounts based on patterns of fraud.
- Law Enforcement Reporting: Suspicious activities are flagged and sent to authorities when needed.
    - Cybersecurity Risks: Attackers may create fake accounts or use stolen identities.
    - Mitigation: Implement machine learning-based fraud detection and Know Your Customer (KYC) protocols.

5. Secure Communication & Data Protection

- Encryption: Protects transaction data while in transit and at rest.

- Secure APIs: Ensures that authentication and transaction authorization requests are protected from attacks like man-in-the-middle (MITM).
    - Cybersecurity Risks: Data interception or manipulation.
    - Mitigation: Use TLS encryption and token-based authentication (e.g., OAuth 2.0).

3.Technology Stack:



Key Components & Cybersecurity Relevance

1. **Engineer Input (UML & Cybersecurity Requirements)**
    - Engineers design system models using UML (Unified Modeling Language).
    - These models are processed through the Eclipse Modeling Framework and translated into cybersecurity-compliant architectures.
    - Cybersecurity Relevance: Engineers may lack deep security knowledge, so automating threat identification helps improve system security early in development.
2. **Translation & Threat Identification**
    - The Translation Engine converts UML models into security-compliant architecture models (CCMI Arch Model).
    - These are matched against a Threat Library and Security Mechanism Library.
    - Cybersecurity Relevance:
        - Threat Library: Identifies known cybersecurity vulnerabilities.

        - Security Mechanism Library: Suggests best practices to mitigate risks (e.g., encryption, access controls).

3. **Matching Engine (Core of CRMS)**
    - Uses Alloy (Formal Verification Tool) to match security requirements with threat models.
    - Helps engineers understand potential threats and select appropriate security mechanisms.
    - Cybersecurity Relevance: Helps automate compliance with security policies, reducing human error.
4. **Security Expert Involvement**
    - Security experts provide formal language-based security rules and expert knowledge to improve threat detection accuracy.
    - Cybersecurity Relevance:
        - Reduces dependency on security professionals for every small change.
        - Ensures compliance with cybersecurity standards (ISO 27001, NIST, etc.).

Challenges & Cybersecurity Insights

- Communication Barriers: Engineers and security experts often struggle to communicate due to different expertise areas.
- Time Costs: Manually identifying security threats is slow; automation improves efficiency.
- Cybersecurity Enhancement:
    - Integrating automated threat identification reduces security misconfigurations.
    - Using formal verification tools (like Alloy) ensures provable security compliance.