**SCAMSAFE SYSTEM SPECIFICATION**

**Name:** Tang Joyce

**Course:** CSC3150 System Design

Professor Andy

**Date:** June 3 2024



Table of Contents

[1. Executive Summary 3](#_Toc168323675)

[2. Introduction 3](#_Toc168323676)

[2.1. Problem Statement / Project Vision 4](#_Toc168323677)

[2.2. System Capabilities 4](#_Toc168323678)

[2.3. Non-functional Requirements and Design Constraints 5](#_Toc168323679)

[2.4. System Evolution 6](#_Toc168323680)

[2.5. Document Outline 7](#_Toc168323681)

[3. Structural Model 10](#_Toc168323682)

[3.1. Model Introduction 10](#_Toc168323683)

[3.2. Class Diagrams 10](#_Toc168323684)

[3.3. Metadata 10](#_Toc168323685)

[4. Architecture Design 18](#_Toc168323686)

[4.1. Architecture Overview 18](#_Toc168323687)

[4.2. Infrastructure Model 18](#_Toc168323688)

[4.2.1. Deployment Diagram 1 – Architecture Overview 19](#_Toc168323689)

[4.2.2. Deployment Diagram 2 – Nodes and Artifacts 20](#_Toc168323690)

[4.3. Hardware and Software Requirements 21](#_Toc168323691)

[4.3.1. Hardware Components 21](#_Toc168323692)

[4.3.2. Required Software Components 22](#_Toc168323693)

[4.4. Security Plan 22](#_Toc168323694)

[4.4.1. Security Overview 22](#_Toc168323695)

[4.4.2. Security Plan 23](#_Toc168323696)

[5. User-Interface 24](#_Toc168323697)

[5.1. User-Interface Requirements and Constraints 24](#_Toc168323698)

[5.2. Window/Screen Navigation Diagram 25](#_Toc168323699)

[5.3. UI Wireframes 26](#_Toc168323700)

[5.4 Reports: "Formal Output" Design 39](#_Toc168323701)

[6. Appendices 40](#_Toc168323702)

[6.1. Glossary 40](#_Toc168323703)

[6.2. References / Bibliography 40](#_Toc168323704)

# **Executive Summary**

ScamSafe is an innovative digital security platform designed to shield individuals and businesses from the complexities of modern digital threats. This summary outlines the significant progress in the development of ScamSafe and maps out the strategic direction for future enhancements. We aim to deliver a user-friendly platform with advanced security features, including real-time scam detection, robust data encryption, and proactive fraud prevention tools. While we have made considerable progress, our journey toward establishing ScamSafe as a leading solution in personal data security continues. Upcoming phases will focus on refining functionalities, integrating user feedback, and leveraging new technologies to elevate the user experience. This document will guide the development team, providing a robust framework upon which to build and ensuring a cohesive approach towards creating a trusted security solution.

# **Introduction**

ScamSafe represents a breakthrough in personal information security, specifically designed to combat the evolving threats in digital transactions. Unlike conventional security applications, ScamSafe offers enhanced protection mechanisms seamlessly integrated into an intuitive interface, such as real-time scam detection and comprehensive data encryption.

This document acts as a thorough technical guide for developers joining the project and serves as a vital reference for existing team members to maintain alignment in development objectives. It outlines the system’s core functionalities and the architectural strategies employed, ensuring that all team members have a common understanding of ScamSafe’s operational framework and development trajectory.

ScamSafe is characterized by several key components:

Security Enhancements

The application incorporates leading-edge security protocols to safeguard user data effectively.

User Interface

Designed with user experience in mind, the interface facilitates easy navigation and management of personal information.

Compliance and Standards

ScamSafe complies with relevant legal and regulatory standards, ensuring the platform meets global security benchmarks.

Developers should utilize this document to understand the architecture, process flows, and functional requirements of ScamSafe. It is structured to clarify the system's design and operational mechanics without cross-referencing the System Proposal directly. For comprehensive details on the project’s background, development context, and more granular specifications, team members should consult the project documentation repository or contact the project lead.

## **Problem Statement / Project Vision**

In the rapidly evolving digital landscape, the security of personal information is paramount, yet many existing solutions fail to protect users against modern cybercriminals' sophisticated techniques adequately. This gap in adequate security measures exposes consumers and financial institutions to heightened risks of fraud and data breaches. ScamSafe is designed to bridge this gap by enhancing the security infrastructure available to users, thereby significantly reducing the potential for fraud and unauthorized data access.

ScamSafe is committed to revolutionizing the way personal data is protected. Our vision encompasses the development of a highly secure platform that surpasses existing legal compliance standards and expectations for data protection. By integrating advanced security features such as real-time scam detection, end-to-end data encryption, and proactive fraud prevention tools, ScamSafe aims to not only defend against threats but also to advance the standard of digital security in personal and financial transactions. The intuitive user interface will ensure that these sophisticated security measures enhance, rather than complicate, the user experience.

The deployment of ScamSafe is expected to yield considerable benefits for all stakeholders involved. It offers end-users a more secure and streamlined method of managing personal and financial information, significantly reducing their vulnerability to cyber threats. Financial institutions will benefit from robust security measures that protect client data, support compliance with strict regulatory standards, and bolster their reputation as trustworthy stewards of sensitive information. Ultimately, ScamSafe seeks to restore and strengthen trust in digital ecosystems by providing a reliable and user-friendly platform that upholds the highest data security standards.

## **System Capabilities**

The functional requirements of ScamSafe are derived from the detailed analysis presented in Section 4 of the System Proposal and are illustrated through the use case diagrams and descriptions provided therein. Each requirement is designed to enhance the security and usability of the platform, ensuring it meets the needs of our users effectively. Below is a summary of these requirements, including their corresponding use case names and ID numbers.

User Registration and Authentication (UC-01)

Enables users to securely register and authenticate their accounts using multi-factor authentication to ensure data security.

Manage User Profile (UC-03)

Users can securely update and manage their personal profile information within the ScamSafe app.

Upload Documents (UC-04)

Users can upload necessary documents for verification, which are automatically checked for authenticity and compliance.

Perform Automatic Safety Checks (UC-05)

Automatically verify uploaded documents against legal and security standards to prevent fraud.

Monitor Transactions for Fraud (UC-06)

Continuously analyzes user transactions to detect and alert users of potentially fraudulent activities in real-time.

Receive Fraud Alerts (UC-07)

Provides real-time alerts to users about suspicious activities detected within their accounts.

Update Legal Standards (UC-08)

Ensures the system stays updated with the latest legal requirements and standards for data protection.

Generate Reports (UC-09)

Generates detailed reports on system usage, fraud detection, and compliance with legal standards.

Conduct Regular Security Updates (UC-10)

Regular system updates to incorporate the latest security patches and features.

Integrate with Financial Systems (UC-11)

Facilitates seamless integration with existing financial systems for enhanced data exchange and security.

Provide Customer Support (UC-12)

Offers comprehensive support and assistance to users through various channels such as live chat and email.

Promote the App (UC-13)

Engages in various marketing activities to promote ScamSafe to potential users and increase adoption.

For more detailed descriptions and additional context regarding these requirements, please refer to the **System Proposal** Section 4, which includes comprehensive discussions on each functionality and the expected impact on the user experience.

## **Non-functional Requirements and Design Constraints**

The non-functional requirements and design constraints for **ScamSafe** ensure that the system operates efficiently, securely, and within all regulatory boundaries. These requirements, as outlined in Sections 1 and 4 of the System Proposal, focus on performance, security, usability, and scalability. Each point is summarized below, with a reference to further details in the System Proposal:

Security

ScamSafe must comply with international cybersecurity standards, including GDPR and CCPA, ensuring data protection across all transactions (refer to Section 4).

Performance

The system should handle up to 10,000 concurrent users without degradation in performance, supporting high-traffic scenarios (Section 4).

Usability

The user interface is designed to be intuitive and accessible, enhancing user experience and facilitating more straightforward navigation and operation (Section 4).

Scalability

The architecture must support scaling to accommodate increasing user loads and data volume as the platform grows (Section 4).

Technical Constraints

Reliance on continuous internet connectivity is required for real-time data processing and updates, limiting offline capabilities (Section 1).

Advanced Security Technologies

Regular updates to security measures are required to protect against emerging threats, necessitating ongoing investment in state-of-the-art security technologies (Section 1).

Compliance Constraints

Rapid changes in privacy laws may necessitate quick system updates to remain compliant, introducing potential legal risks (Feasibility Assessment in Section 3).

Operational Constraints

Regular updates and maintenance are critical to ensure the system's effectiveness and compliance, which may increase operational costs and complexity (Section 1).

These summarized points are critical to the design and ongoing development of ScamSafe. For a more detailed explanation of how these requirements influence the system's architecture and functionality, please refer to the detailed discussions in the System Proposal, Sections 1 and 4.

## **System Evolution**

As Section 6 of the System Proposal outlines, ScamSafe is designed with a phased development approach, ensuring each platform version builds upon the foundational security and functionality established in previous releases. This evolution strategy allows us to continually enhance the system’s capabilities and address emerging security challenges and user needs.

**Version 1 (MVP)**

The initial release of ScamSafe will focus on establishing core functionalities such as User Registration and Authentication (UC-01), Document Upload and Verification (UC-04), and essential Fraud Detection (UC-06). This version will provide a robust foundation for personal data security, addressing the most critical needs of our users.

* + 1. **Version 2 Changes**

Enhanced Fraud Detection (UC-14)

Building on the initial fraud detection capabilities, Version 2 will introduce more sophisticated algorithms to detect and analyze fraud patterns using artificial intelligence, increasing the accuracy and response speed.

Automated Compliance Updates (UC-15)

To ensure ongoing legal compliance, ScamSafe will automatically update its systems in response to changes in data protection laws. This use case will streamline the integration of new legal standards without manual intervention.

User Behavior Analytics (UC-16)

This feature will analyze user behaviors to detect anomalies that may indicate fraudulent activities or potential security risks, enhancing the overall security posture of the platform.

* + 1. **Version 3 and beyond Changes**

Multi-Language Support (UC-17)

As ScamSafe expands globally, Version 3 will introduce multilingual support, making the platform accessible to a broader audience by accommodating various languages.

Advanced User Interface Customization (UC-18)

Future versions will allow users to customize the interface according to their preferences, enhancing usability and user satisfaction. This will include various themes and layout options to suit different user needs.

Blockchain Integration for Transaction Security (UC-19)

Integrating blockchain technology provides additional security and transparency for transactions processed through ScamSafe.

Cross-Platform Accessibility (UC-20)

Expanding accessibility by developing applications for multiple platforms, including iOS and Android, ensuring users can securely access their information on any device.

**Future Versions**

Subsequent updates will continue to build on the secure infrastructure of ScamSafe, introducing more sophisticated security features and usability enhancements based on user feedback and technological advancements. Each version will aim to integrate the latest cybersecurity technologies and compliance measures to stay ahead of potential threats.

For detailed information on each version's planned features and functionalities and the rationale behind the phased development approach, developers are encouraged to refer to Section 6 of the System Proposal. This section provides a comprehensive roadmap for ScamSafe's evolution, aligning development efforts with strategic objectives and user needs.

## **Document Outline**

The System Specification document for ScamSafe provides a comprehensive guide for the development team, detailing the software's technical requirements, system architecture, and evolution plan. This document serves as a blueprint for the development process, ensuring all team members are aligned with the project goals and understand the functionalities and technicalities involved. Here’s an outline of the document structure:

**1. Cover Page**

* Title of the document.
* Project title: ScamSafe.
* Date of preparation.
* Names and details of the project team.

**2. Table of Contents**

* Automatically generated to include all sections and sub-sections with page numbers for easy navigation.

**3. Executive Summary**

* A brief overview of the project, highlighting the purpose, scope, and significance of the ScamSafe system.

**4. Introduction**

* A brief introduction to ScamSafe, focusing on the need for the system and its intended users.
* Summary of the document's purpose, particularly for new developers or as a refresher for existing team members.

**5. System Overview**

* Provide a high-level description of ScamSafe, including its main components and functionalities.
* Summary of the system’s goals and how it addresses specific user needs.

**6. Functional Requirements**

* Detailed listing of all functional requirements identified during the system analysis phase.
* Each requirement is briefly described with its corresponding use case ID for reference.

**7. Non-functional Requirements and Design Constraints**

* Discussion of the non-functional requirements, including performance, security, usability, and scalability.
* Overview of design constraints that impact the system architecture and development.

**8. System Architecture**

* Description of the overall architecture of ScamSafe.
* Diagrams and explanations of the structural layout, including data flows, process networks, and interface designs.

**9. Security Specifications**

* Detailed security protocols and measures implemented within ScamSafe.
* Describe compliance with relevant standards and legal requirements.

**10. System Evolution**

* Outline the planned enhancements and functionalities to be added in subsequent versions.
* Description of the roadmap for the phased development of ScamSafe.

**11. Appendices**

* Additional supporting information such as glossaries, reference documents, and detailed diagrams.
* Any supplementary materials that provide deeper insight into the development process or technical details.

**12. References**

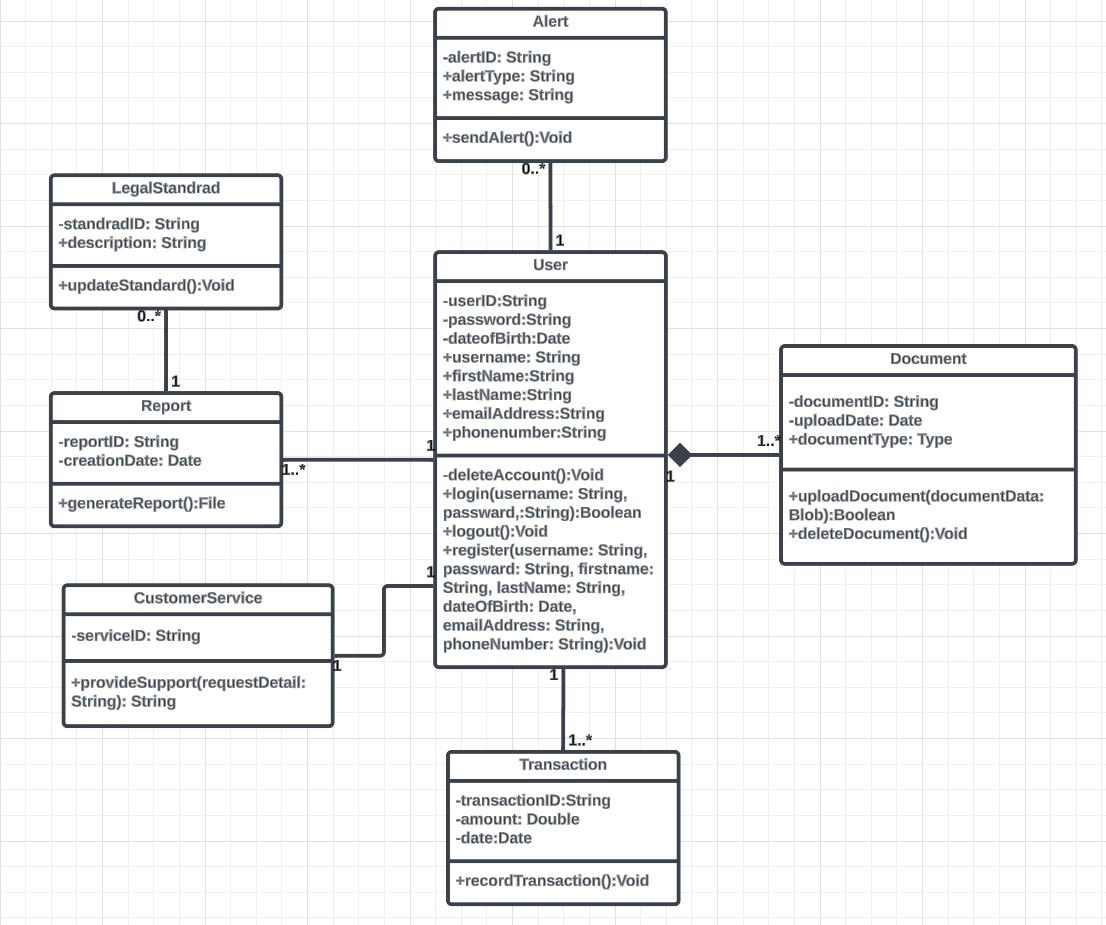
* Provide a comprehensive listing of all sources and materials referenced throughout the document.

# **Structural Model**

## **Model Introduction**

This section features a detailed Unified Modeling Language (UML) Class Model of the ScamSafe system, designed to offer developers a clear overview of the architecture. It includes crucial classes, attributes, operations, and their interrelationships, all detailed for optimal clarity of the system’s structure and function.

## **Class Diagrams**



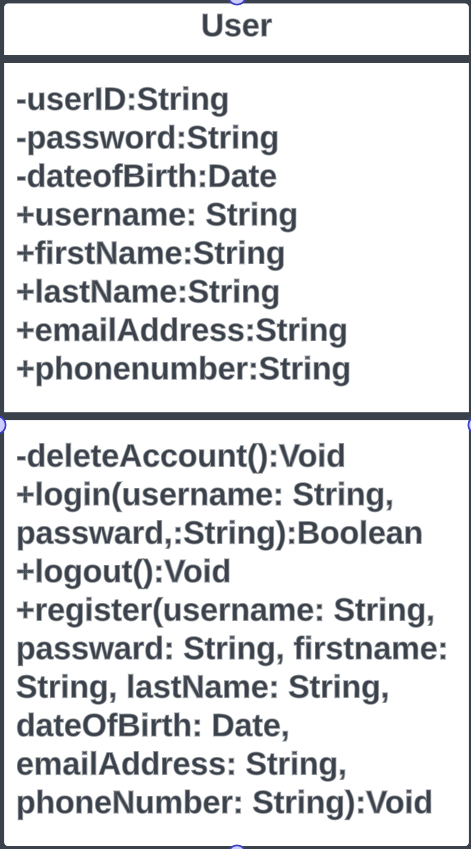
[**Class Diagram**](https://lucid.app/lucidchart/a71803f2-bb7d-41b7-bd0a-2fdee8841bf3/edit?viewport_loc=-2930%2C-1810%2C2827%2C1512%2C0_0&invitationId=inv_1f959831-3250-40ec-a5e2-330b459e5204)

## **Metadata**

This section provides a detailed exploration of each class's data elements and operations within the ScamSafe system. Each class’s description and visibility are briefly covered to offer a clear understanding of its role and accessibility. The classes are listed in alphabetical order with corresponding page numbers for easy reference:

1. **User** - Page 12
2. **Transaction** - Page 13
3. **Report** - Page 14
4. **LegalStandard** - Page 15
5. **Document** - Page 16
6. **CustomerService** - Page 17
7. **Alert** - Page 18

**3.3.1 User**



* **Description**: Represents a registered user of the ScamSafe system, capable of interacting with documents, transactions, alerts, and customer services.
* **Visibility**: Public
* **Is Abstract**: No

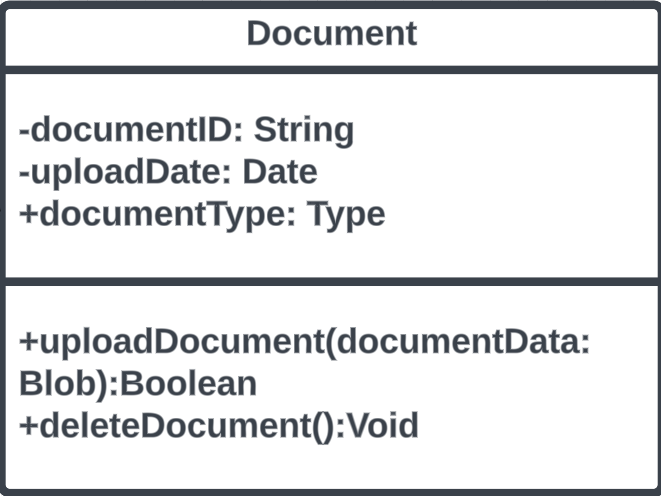
**Attributes**

| **Name** | **Description** | **Read Only?** | **Multiplicity** |
| --- | --- | --- | --- |
| userID | Unique identifier for each user | Yes | 1 |
| password | Encrypted password for user login | No | 1 |
| dateOfBirth | Date of birth of the user | No | 1 |
| username | Username used for user login | No | 1 |
| firstName | First name of the user | No | 1 |
| lastName | Last name of the user | No | 1 |
| emailAddress | Email address of the user | No | 1 |
| phoneNumber | Phone number of the user | No | 1 |

**Operations**

| **Name** | **Description** | **Is Query?** | **Is Polymorphic?** |
| --- | --- | --- | --- |
| deleteAccount | Removes a user account from the system | No | No |
| login | Authenticates a user based on username and password | No | No |
| logout | Logs out a user from the system | No | No |
| register | Registers a new user with personal details and login credentials | No | No |

* + 1. **Document**

****

* **Description:** Represents a document uploaded by a user, including various files.
* **Visibility**: Public
* **Is Abstract**: No

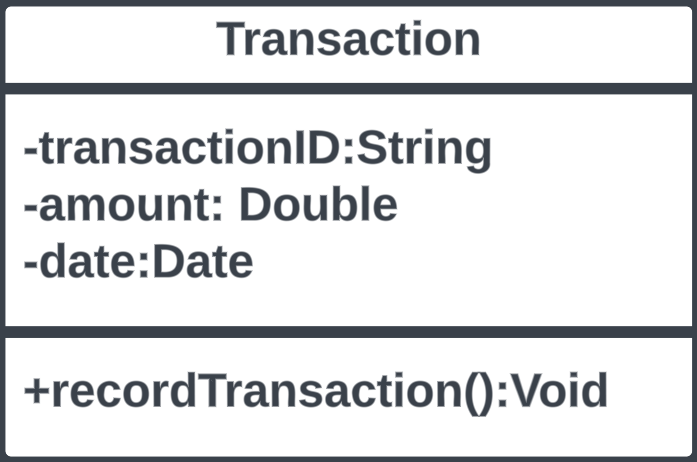
**Attributes**

| **Name** | **Description** | **Read Only?** | **Multiplicity** |
| --- | --- | --- | --- |
| documentID | Unique identifier of each document | Yes | 1 |
| uploadDate | Date when the document was uploaded | No | 1 |
| documentType | Type of the document | No | 1 |

**Operations**

| **Name** | **Description** | **Is Query?** | **Is Polymorphic?** |
| --- | --- | --- | --- |
| uploadDocument | Uploads a new document to the system | No | No |
| deleteDocument | Deletes a specific document from the system | No | No |

* + 1. **Transaction**



* **Description**: Represents financial transactions conducted by a user within the system.
* **Visibility**: Public
* **Is Abstract**: No

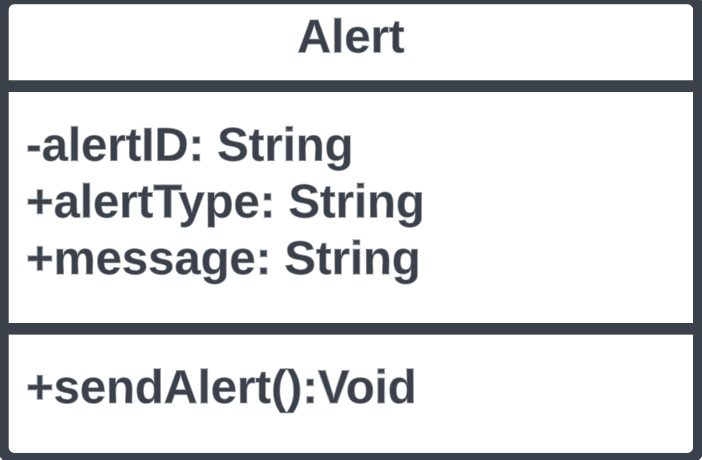
**Attributes**

| **Name** | **Description** | **Read Only?** | **Multiplicity** |
| --- | --- | --- | --- |
| transactionID | Unique identifier for each transaction | Yes | 1 |
| amount | Amount involved in the transaction | No | 1 |
| date | Date when the transaction was executed | No | 1 |

**Operations**

| **Name** | **Description** | **Is Query?** | **Is Polymorphic?** |
| --- | --- | --- | --- |
| recordTransaction | Records a new transaction in the system | No | No |

* + 1. **Alert**



* **Description**: Represents alerts generated for users, typically based on specific triggers or conditions within the system.
* **Visibility**: Public
* **Is Abstract**: No

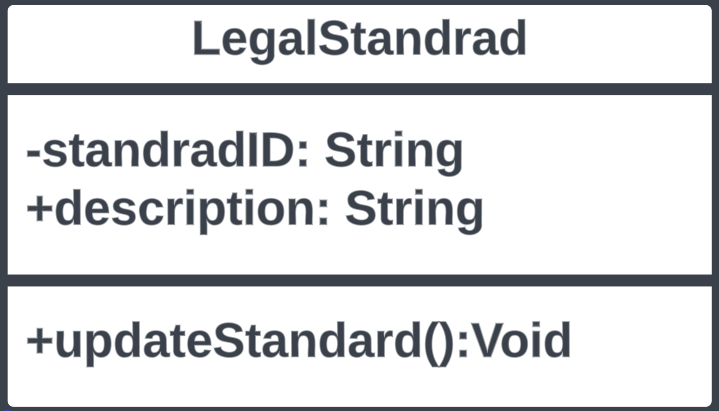
**Attributes**

| **Name** | **Description** | **Read Only?** | **Multiplicity** |
| --- | --- | --- | --- |
| alertID | Unique identifier of each alert | Yes | 1 |
| alertType | Type of alert (e.g., security, reminder) | No | 1 |
| message | Message content of the alert | No | 1 |

**Operations**

| **Name** | **Description** | **Is Query?** | **Is Polymorphic?** |
| --- | --- | --- | --- |
| sendAlert | Sends an alert to the user's interface | No | No |

* + 1. **LegalStandard**



* **Description**: Encapsulates legal standards or regulations that reports or documents must comply with.
* **Visibility**: Public
* **Is Abstract**: No

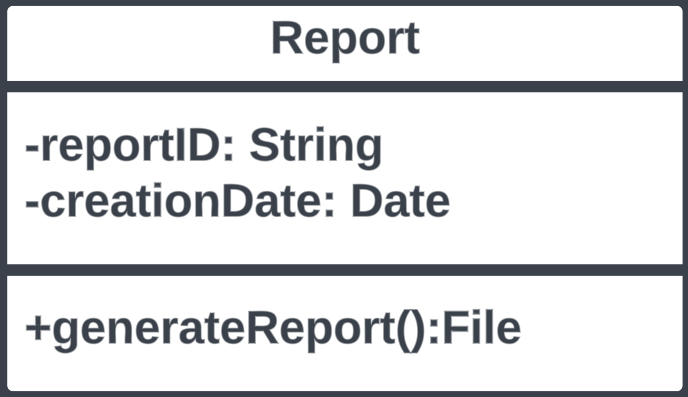
**Attributes**

| **Name** | **Description** | **Read Only?** | **Multiplicity** |
| --- | --- | --- | --- |
| standardID | Unique identifier for each legal standard | Yes | 1 |
| description | Detailed description of the standard | No | 1 |

**Operations**

| **Name** | **Description** | **Is Query?** | **Is Polymorphic?** |
| --- | --- | --- | --- |
| updateStandard | Updates the details of the existing standard | No | No |

* + 1. **Report**



* **Description**: Manages the generation of reports based on user data, transactions, or compliance with legal standards.
* **Visibility**: Public
* **Is Abstract**: No

**Attributes**

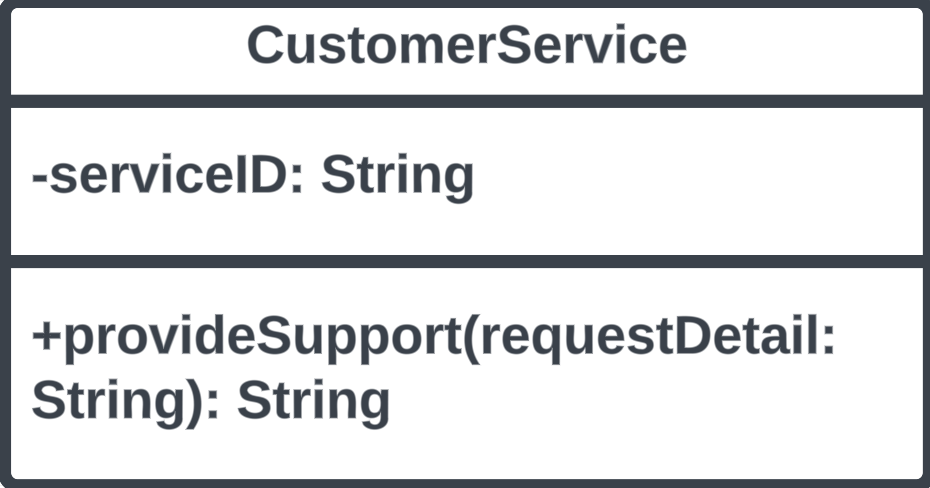
| **Name** | **Description** | **Read Only?** | **Multiplicity** |
| --- | --- | --- | --- |
| reportID | Unique identifier of each report | Yes | 1 |
| creationDate | Date when the report was generated | No | 1 |

### 

**Operations**

| **Name** | **Description** | **Is Query?** | **Is Polymorphic?** |
| --- | --- | --- | --- |
| generateReport | Generates a detailed report and returns a file | No | No |

* + 1. **CustomerService**



* **Description**: Provides support services to users, handling inquiries and issues regarding system use.
* **Visibility**: Public
* **Is Abstract**: No

**Attributes**

| **Name** | **Description** | **Read Only?** | **Multiplicity** |
| --- | --- | --- | --- |
| serviceID | Unique identifier for the customer service | Yes | 1 |

**Operations**

| **Name** | **Description** | **Is Query?** | **Is Polymorphic?** |
| --- | --- | --- | --- |
| provideSupport | Responds to user requests for assistance | No | No |

# **Architecture Design**

## **Architecture Overview**

This section provides a high-level overview of the ScamSafe application's architecture, focusing on its structured design to enhance understanding and implementation. The architectural layout is designed as a 3-tier client-server system, which efficiently segregates the presentation layer, application logic, and database management to ensure scalability, maintainability, and security. Readers will learn how each system component interacts with others, the technologies involved, and the protocols ensuring secure data exchange. Recommendations include upgrading to robust, scalable server solutions to accommodate anticipated increases in user traffic and data volume, implying the potential acquisition of additional high-performance servers.

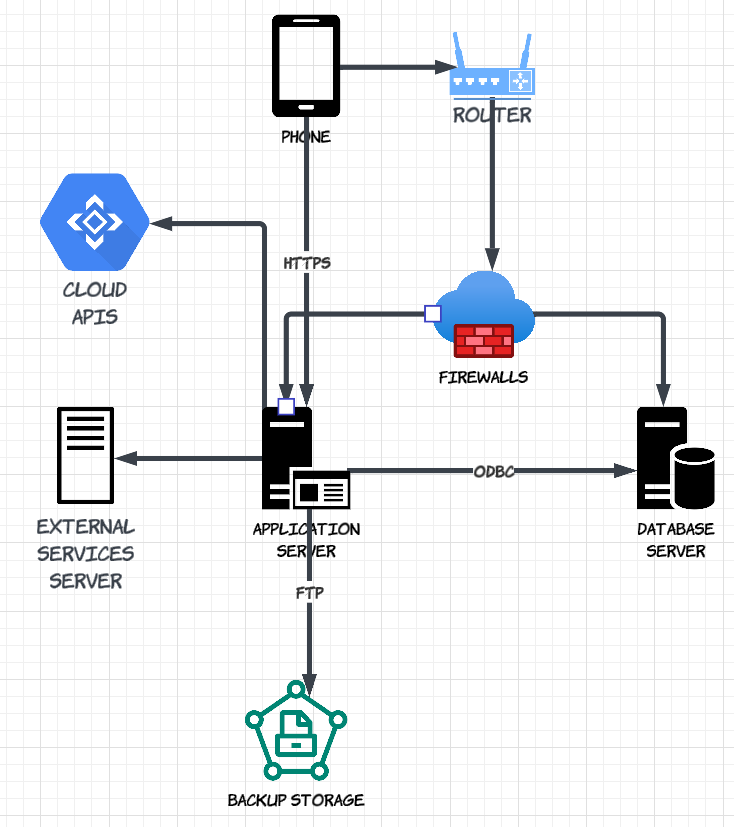
## **Infrastructure Model**

Accompanied by two deployment diagrams, this section visualizes the physical and logical components of the ScamSafe architecture. These diagrams serve as practical guides for understanding the deployment of application components across various environments, from local servers to cloud-based infrastructure. Each diagram is carefully aligned to ensure consistency and clarity:

* **Deployment Diagram 1 – Architecture Overview**: This diagram provides a bird's-eye view of the system architecture, illustrating how client devices interact with the application server through a secure network facilitated by routers and firewalls. It details the use of HTTPS for secure communication, ODBC for database interactions, and FTP for backup operations.
* **Deployment Diagram 2 – Nodes and Artifacts**: Expanding on the first, this diagram delves deeper into the specific software and services (artifacts) deployed on each node. It shows the precise allocation of responsibilities among the servers, such as application processing, data management, and external services, ensuring comprehensive coverage of system functionalities.

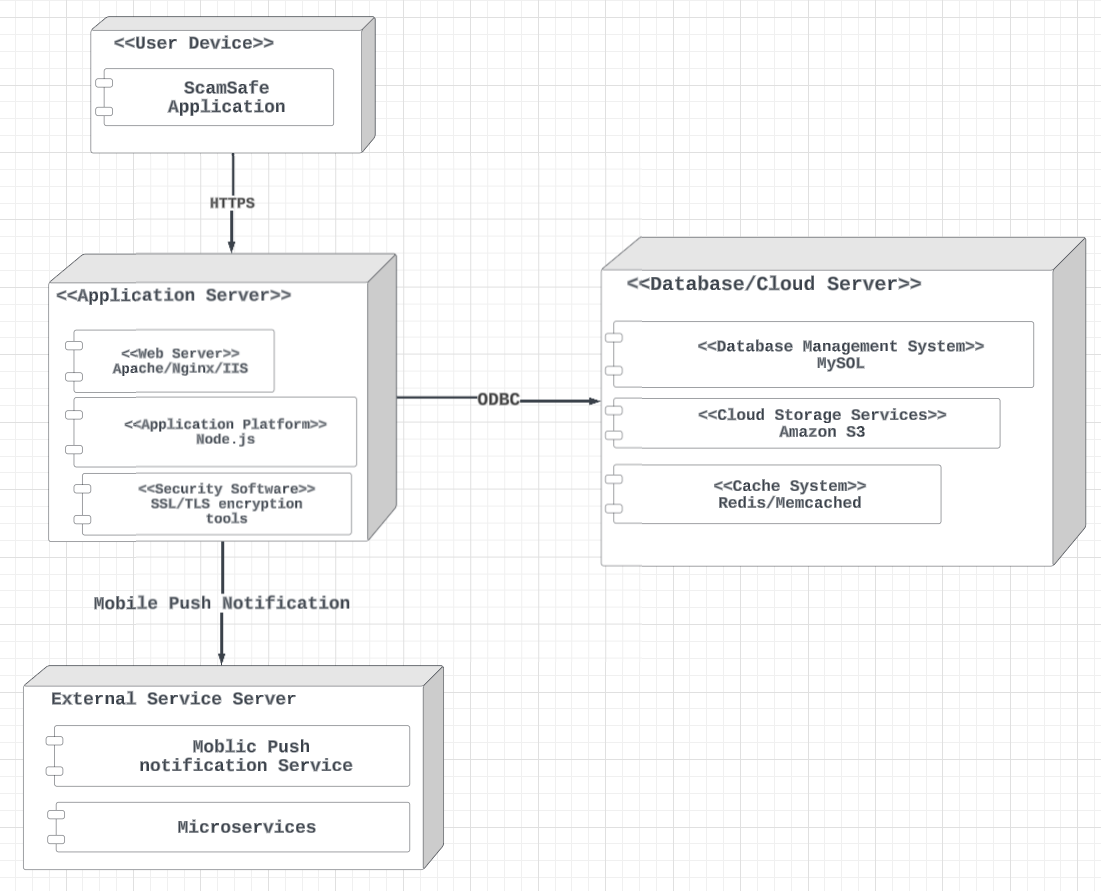
Both diagrams are designed to maintain identical node and connection configurations to emphasize the system's structured and uniform approach. This alignment aids in clear communication of the deployment strategy to stakeholders, facilitating better understanding and collaboration in developmental and operational processes. By exploring these sections, stakeholders and technical teams gain a thorough insight into the physical setup and logical partitioning of the ScamSafe system, ensuring all participants are aligned with the architectural strategies and prepared for implementation phases.

* + 1. **Deployment Diagram 1 – Architecture Overview**

****

[**Deployment Diagram 1 - Architecture Overview**](https://lucid.app/lucidchart/f3ce2b3f-5589-4ee8-82e5-e35b8c317ec1/edit?viewport_loc=-3953%2C-609%2C5785%2C2562%2C0_0&invitationId=inv_b1523851-0496-4d4b-9c56-0c2e982aae1e)

* + 1. **Deployment Diagram 2 – Nodes and Artifacts**

****

[**Deployment Diagram 2 - Node and Artifacts**](https://lucid.app/lucidchart/f3ce2b3f-5589-4ee8-82e5-e35b8c317ec1/edit?viewport_loc=-3953%2C-609%2C5785%2C2562%2C0_0&invitationId=inv_b1523851-0496-4d4b-9c56-0c2e982aae1e)

## **Hardware and Software Requirements**

This section delineates the hardware (HW) and software (SW) requirements to support and run the ScamSafe application adequately. It outlines both the infrastructure requirements for the servers and the end-user requirements for accessing the application.

* + 1. **Hardware Components**

**Server-Side Hardware:**

* 1. **Application Servers**
* High-performance servers capable of handling significant computational loads are required. Suggested specifications include multi-core processors (Intel Xeon, AMD EPYC), a minimum of 32 GB RAM, and fast SSD storage for optimal performance. Depending on the load, multiple servers may be necessary to handle user requests efficiently.
  1. **Database Servers**
* Servers equipped with high I/O capacity and ample storage to manage large datasets and ensure quick data retrieval. Recommended are RAID configurations for redundancy and at least 1 TB of SSD storage.
  1. **Backup and Recovery Systems:**
* Dedicated backup servers or storage solutions (such as NAS or SAN) with high capacity and reliability to ensure data integrity and availability.

**Client-Side Hardware:**

* **User Devices:** Users will need internet-capable devices such as smartphones, tablets, or computers. No specific hardware requirements are necessary beyond the ability to run a web browser or a mobile application compatible with iOS or Android.

**Existing vs. New Hardware:**

* A combination of new purchases and existing infrastructure can be considered. New, powerful servers may be required to handle increased loads, while some existing servers could be repurposed for less critical roles such as development and testing environments.

**Alternative Configurations:**

* **Cloud-Based Alternatives:** Instead of investing heavily in physical hardware, cloud services like AWS EC2 for application servers or Amazon RDS for database services can be considered, which offer scalability and potentially reduce upfront costs.
  + 1. **Required Software Components**

**System Software:**

* **Operating Systems:** Server machines should run on stable and secure operating systems such as Ubuntu Server 20.04 LTS, Red Hat Enterprise Linux 8, or Microsoft Windows Server 2019, depending on the application requirements and team expertise.
* **Web Servers:** Apache 2.4 or Nginx 1.18 are recommended for handling HTTP requests effectively.
* **Database Management Systems:** MySQL 8.0, PostgreSQL 12, or higher to ensure robust data management and security features.
* **Development Frameworks:** Node.js 14 or .NET Core 3.1 for the backend application logic.

**Client-Side Software:**

* **Web Browsers:** Latest versions of Google Chrome, Mozilla Firefox, Microsoft Edge, or Safari.
* **Mobile OS:** iOS 13.0 or higher and Android 10 or higher for mobile app compatibility.

These software components are essential to building a scalable, secure, responsive ScamSafe application that meets modern standards and user expectations. By specifying these requirements, the deployment team can ensure that all system components are compatible and perform optimally.

## **Security Plan**

* + 1. **Security Overview**

The ScamSafe system is designed to ensure robust security across all levels of its operation, from data entry to data storage and communications. Given the nature of the application, which deals with sensitive user data, the most significant areas of concern are data breaches, unauthorized access, and data integrity. Ensuring the confidentiality, integrity, and availability of user data is paramount.

**Recommended Security Software:**

* **Firewalls:** To monitor and control incoming and outgoing network traffic based on predetermined security rules.
* **Encryption Software:** For encrypting data at rest (e.g., database encryption using AES 256-bit) and in transit (e.g., TLS 1.3 for all communications).
* **Antivirus and Anti-malware:** To protect the system from malicious software and attacks.
* **Intrusion Detection and Prevention Systems (IDPS):** To swiftly identify and respond to potential threats.
* **Data Loss Prevention (DLP) Software:** To prevent data breaches and ensure that sensitive information is not lost or misused.
  + 1. **Security Plan**

The security table below organizes the critical components of the ScamSafe system, potential threats, and the controls implemented to mitigate these risks. This arrangement helps quickly identify the security measures for each component and threat type.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Components/Threats | Fire | Flood | Power Loss | Circuit Failure | Virus | Unauthorized Access (External/Internal Intruders) |
| Servers | 1,12 | 2,12 | 3,12 | 4 | 5 | 6,8,12 |
| Client Devices | 12 | 12 | 3 |  | 5 | 6,12 |
| Network Devices | 1,12 | 2,12 | 3,12 | 4 | 5 | 6,8,12 |
| Application Software | 10 |  |  |  | 5 | 6,10 |
| Data Storage | 1,12 | 2,12 | 3,12 | 4 | 5 | 6,7,12 |

**Controls**

1. Fire suppression systems, fire-resistant materials
2. Waterproof barriers, elevated hardware
3. Uninterruptible Power Supplies (UPS), backup generators
4. Redundant power circuits
5. Antivirus and anti-malware software
6. Strong authentication, encryption, and access controls
7. Regular data backups
8. Network firewalls and intrusion detection systems (IDS)
9. Security awareness training for employees
10. Use of secure coding practices
11. Monitoring and logging mechanisms
12. Physical security controls (e.g., locks, security personnel, surveillance)

# **User-Interface**

## **User-Interface Requirements and Constraints**

In this section, we detail the essential user-interface requirements and constraints that shape the design and functionality of the ScamSafe application. The focus here is on creating an interface that is intuitive, user-friendly, and accessible, ensuring that users of all technical skill levels can navigate and utilize the app effectively.

Guiding Principles:

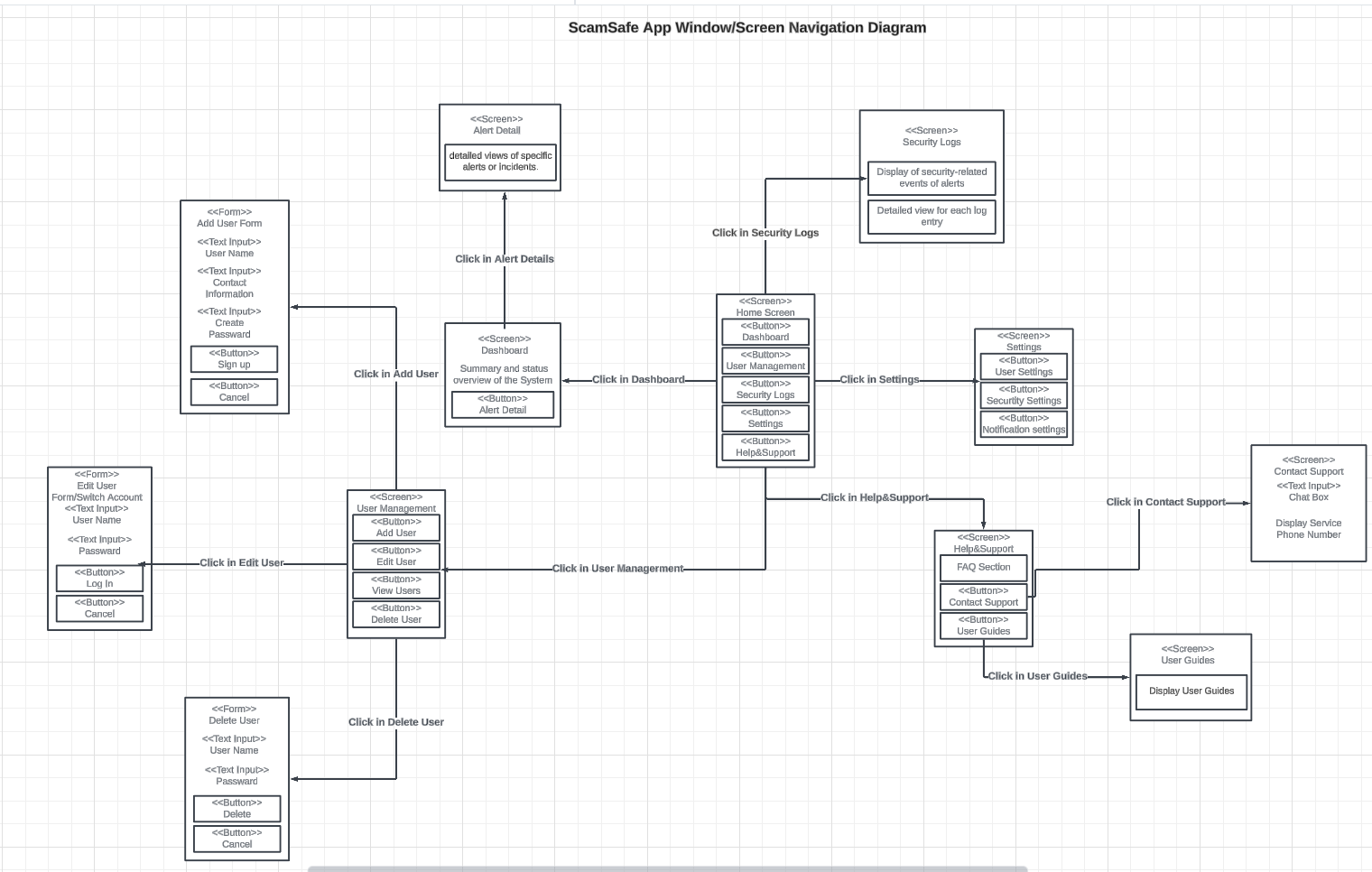
1. **Consistency:** The interface maintains a uniform layout and interaction patterns across all screens to minimize user confusion and learning time.
2. **Simplicity:** Designs are kept straightforward, avoiding unnecessary complexity that might overwhelm the user.
3. **Accessibility:** The app adheres to accessibility standards to ensure that it is usable by people with various disabilities, including visual, auditory, and motor impairments.
4. **Responsiveness:** The interface is responsive to different device screens—optimizing user experience on phones, tablets, and desktop computers.
5. **Feedback:** Immediate and clear feedback is provided for user actions to inform them about successful operations or errors that need attention.

Constraints:

* The interface must operate within the performance limits set by the underlying system architecture, ensuring quick load times and smooth transitions.
* Design elements must comply with the latest web and mobile app security and data protection standards.
* Adherence to brand guidelines is mandatory to maintain visual identity and user trust.

## **Window/Screen Navigation Diagram**

The diagram below outlines the navigational structure and layout of the ScamSafe application. It shows the connections and flow between various user interface components and screens, providing a clear overview of the app's user interaction pathways. Further details and annotations about the diagram are provided in the subsequent sections to enhance understanding.



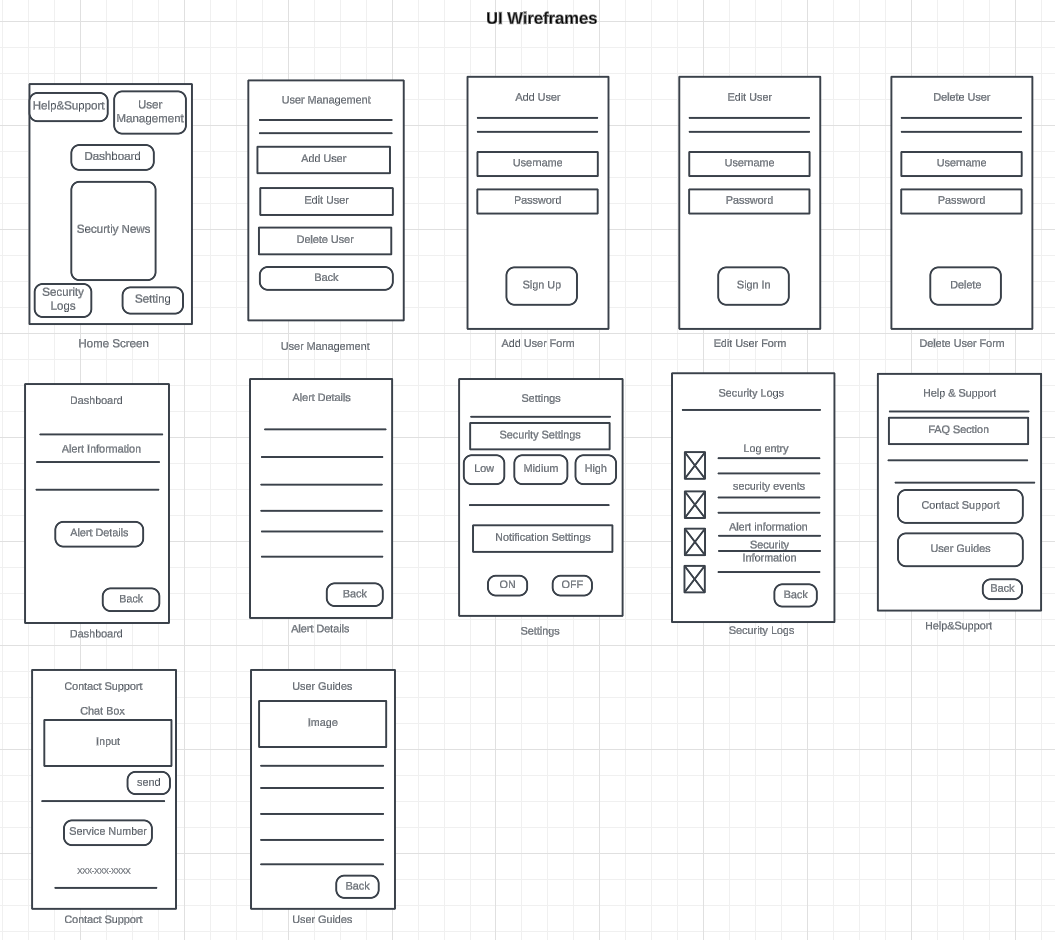
[ScamSafe App Window/Screen Navigation Diagram](https://lucid.app/lucidchart/6f9ad554-aeb0-4709-9a22-bf36e8f356db/edit?viewport_loc=-5161%2C-363%2C6852%2C3034%2C0_0&invitationId=inv_f139c1c1-65a6-467e-86b8-c25271c603f0)

Addition Details:

* User Management: Allows for adding, editing, and deleting user profiles, ensuring user access is appropriately managed.
* Alert Details: Provides in-depth information on security alerts, enabling users to understand and react to potential threats promptly.
* System Settings: Contains sub-menus for personalizing user settings, security configurations, and notification preferences, tailoring the app to individual user needs.
* Help & Support: Offers direct links to FAQ sections, user guides, and contact support, ensuring users can access necessary assistance and information.

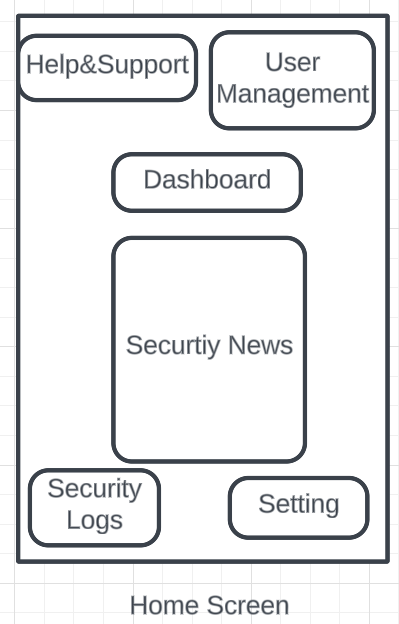
## **UI Wireframes**

The provided UI wireframes illustrate the primary interfaces of the ScamSafe application, designed to ensure a cohesive and intuitive user experience. Each panel represents a different aspect of the application's functionality, enabling users to interact effectively with the system.

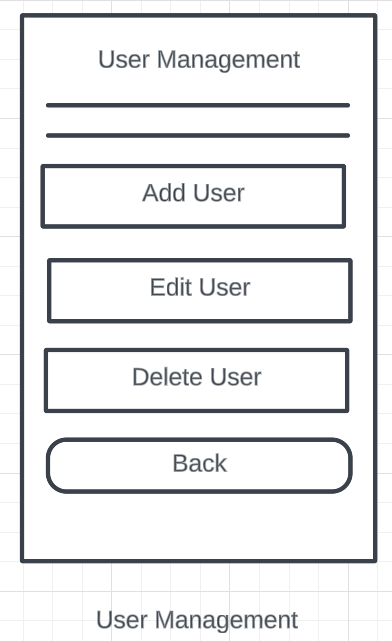


[UI Wireframes](https://lucid.app/lucidchart/6f9ad554-aeb0-4709-9a22-bf36e8f356db/edit?viewport_loc=-213%2C-383%2C5442%2C2911%2C0_0&invitationId=inv_f139c1c1-65a6-467e-86b8-c25271c603f0)

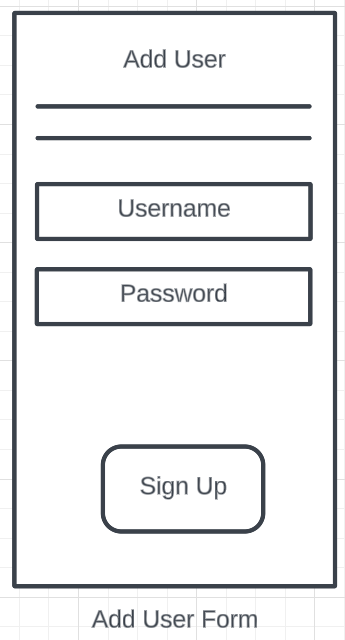
* + 1. **Home Screen**



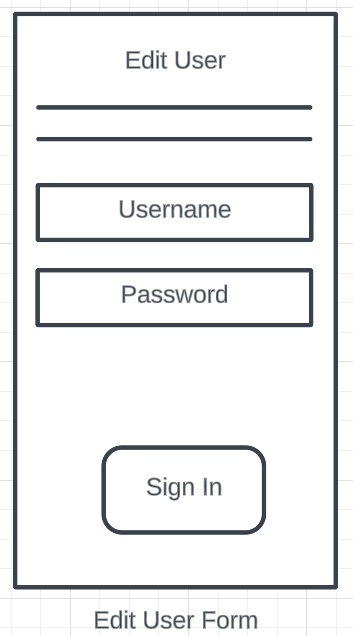
* + Serves as the central navigation point to various app sections, including User Management, Dashboard, Security Logs, and Help & Support.
    1. **User Management**



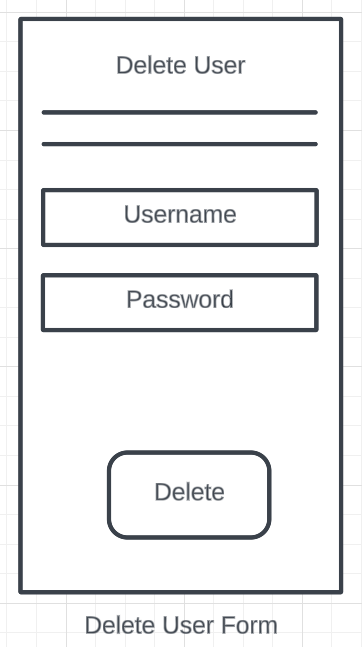
* Allows for user account operations, including adding, editing, and deleting user accounts and viewing detailed lists of users.
  + 1. **Add User Form**



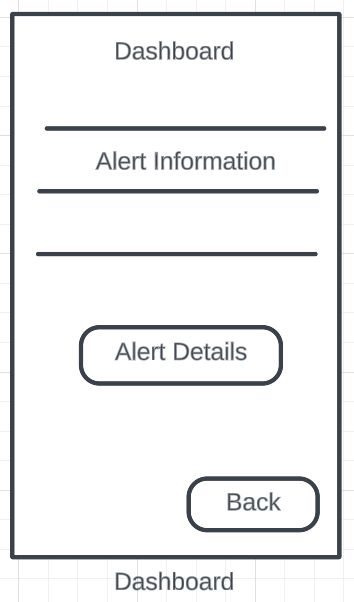
* + **Add User**: Allows administrators to create new user accounts by entering usernames, contact information, and passwords.
    1. **Edit User Form**



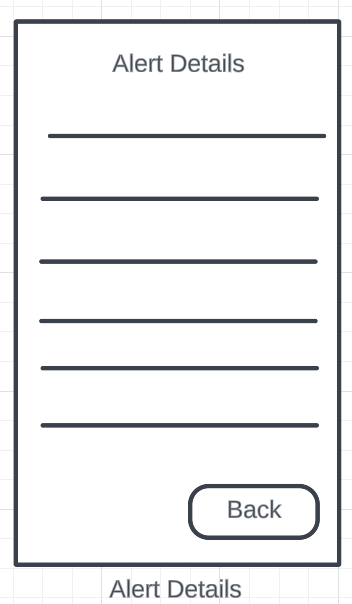
* + **Edit User**: Provides the ability to update existing user account details or switch between accounts.
    1. **Delete User Form**



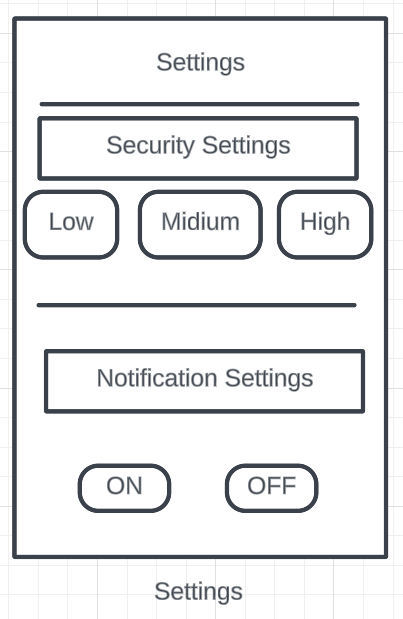
* + **Delete User**: Facilitates the removal of user accounts from the system.
    1. **Dashboard**



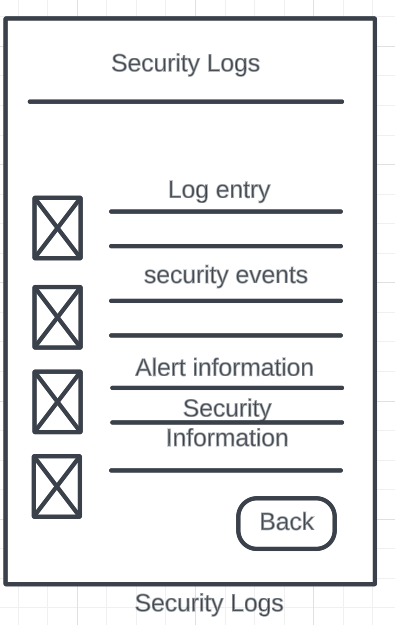
* **Alert Information**: Shows summaries and status overviews of the system’s alerts.
  + 1. **Alert Details**



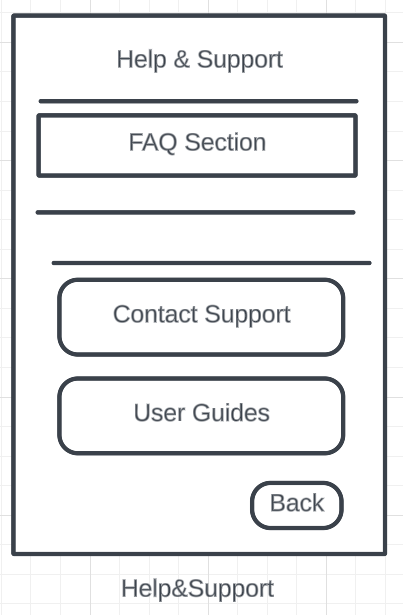
* **Alert Details**: Offers detailed views of specific alerts or incidents, accessible from the summary panels.
  + 1. **Settings**



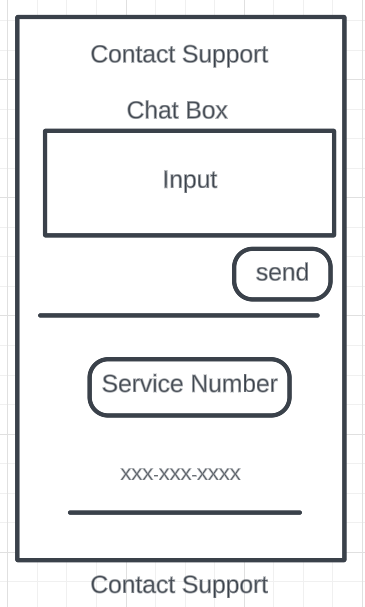
* + **Security Settings**: Allows users to set the application's security level (Low, Medium, High).
  + **Notification Settings**: Users can toggle on or off notifications for various events and alerts.
    1. **Security Logs**



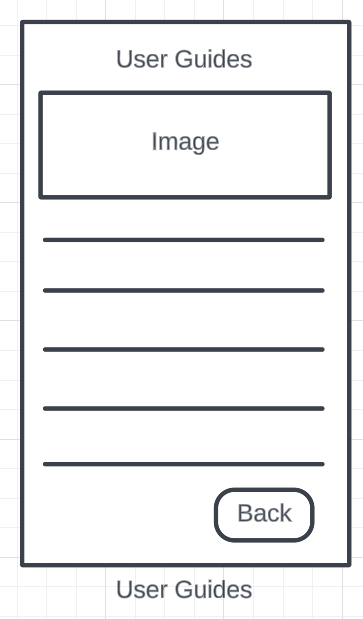
* + Captures and displays logs related to security events, providing a log entry list and detailed views of each event.
    1. **Help & Support**



* **FAQ Section**: Provides answers to frequently asked questions to help users resolve common issues.
  + 1. **Contact Support**



* **Contact Support**: Includes contact details and a chat box for real-time support.
  + 1. **User Guides**



* **User Guides**: Offers detailed user guides and documentation to help users understand and utilize the application more effectively.

## **Reports: "Formal Output" Design**

The ScamSafe application is designed to provide real-time security and user management solutions without generating formal outputs such as printed reports, receipts, or invoices. The system focuses on digital interactions and displays, ensuring all necessary information is accessible within the application interface.

Users will not find traditional printable outputs within ScamSafe. Instead, all pertinent security logs, user management, and system settings data are managed and reviewed directly through the application's screens. This approach aligns with ScamSafe's goal to maintain a streamlined, environmentally friendly, and cost-effective digital environment, minimizing the need for physical document management and enhancing the ease of use.

This section ensures stakeholders know that the application does not incorporate separate output functionalities but maintains robust digital record-keeping and display capabilities critical for user operations and security oversight.

# **Appendices**

## **Glossary**

**API (Application Programming Interface)**

A set of routines, protocols, and tools for building software applications. APIs specify how software components should interact and are used when programming graphical user interface (GUI) components.

**Compliance Certifications**

Documents or credentials that verify the software meets all legal and regulatory requirements applicable to its function and use, ensuring adherence to standards such as GDPR or HIPAA.

**Data Encryption**

Converting information or data into a code to prevent unauthorized access. This security measure protects sensitive data by making it unreadable without the proper decryption key.

**GDPR (General Data Protection Regulation)**

A regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.

**Non-functional Requirements**

Requirements that describe how a system operates rather than the specific behaviors of that system. This includes aspects such as system performance, security, and user accessibility.

**Prototype**

An early sample, model, or release of a product built to test a concept or process. In software development, a prototype is used to evaluate a new design to enhance precision by system analysts and users.

**Scalability**

The capability of a system, network, or process to handle a growing amount of work or its potential to be enlarged to accommodate that growth. For software systems, this refers to the ability to handle increased loads on the system by making hardware or software adjustments.

**Stakeholders**

Individuals, groups, or organizations interested in a project's success or failure. Stakeholders for ScamSafe include users, developers, investors, and regulatory bodies.

**HTTPS (Hypertext Transfer Protocol Secure)**

An extension of HTTP is used for secure communication over a computer network and is widely used on the Internet. HTTPS encrypts the session with a digital certificate, typically SSL or TLS.

**ODBC (Open Database Connectivity)**

A standard API is used to access database management systems (DBMS). It allows the use of SQL to access the data independent of the system managing it.

**FTP (File Transfer Protocol)**

A standard network protocol transfers computer files between a client and server on a computer network. It is built on a client-server model architecture and uses separate control and data connections between the client and the server.

## **References / Bibliography**

Cameron, Andrew. Class Lecture, System Design, Seattle Pacific University, Seattle, Washington, May 2024

Federal Trade Commission. (2024). Consumer Information. Retrieved from <https://consumer.ftc.gov/>

National Institute of Standards and Technology. (2024). *Framework for Improving Critical Infrastructure Cybersecurity*. Available at: <https://www.nist.gov/cyberframework>