2018

Architecture Design

PART II

MENGSHAN CHEN, KAREN MARCJAN, CHIDOZIE ONONIWU

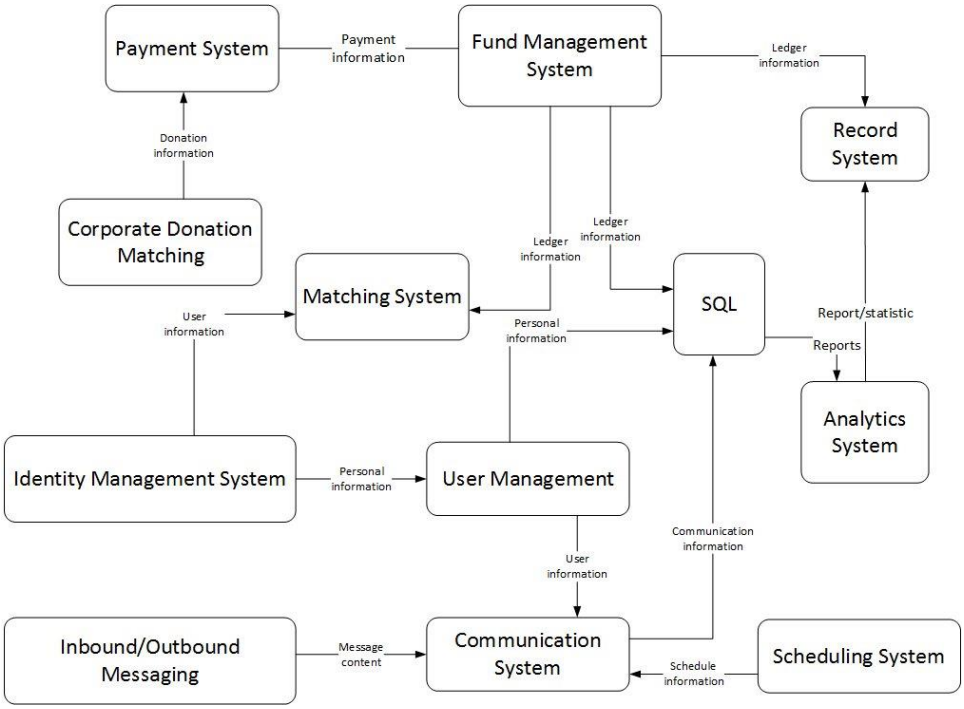
Table of Contents

1. Overview

This document shows the software, security, and deployment architectural views of student aid. It also shows the technology choices that have been made in the design of the system.

2. Software Architecture

As shown in deliverable two, the architecture for Student Aid has been broadly divided into two sets of components. The first set are components which will be developed from scratch by developers chosen for this project. We have called them internal components because these components will be developed, deployed and run from within the selected public cloud service. These components contain key business differentiators to F2E. The second set of components, called external components, are SaaS solutions that will be tightly integrated with the student Aid solution.



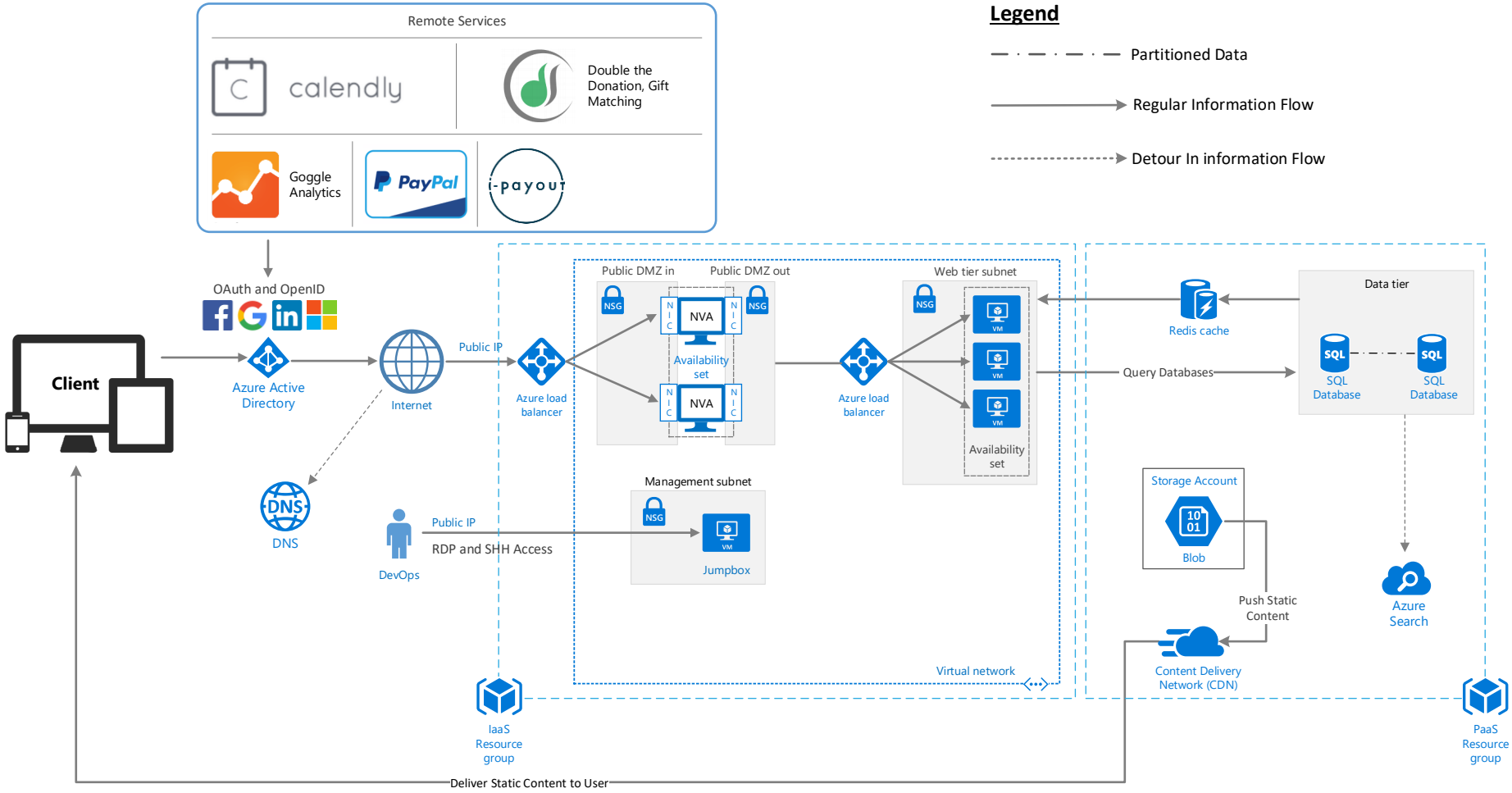
Module View Showing the Subsystem block that make up the solution

Component	Description	Functional or Non-Functional Requirement Satisfied
To be Bought		
Payment System	All electronic money transfers will be handled in and out of the system. It should comply with PCI-DSS to protect card information and maintain an average response time of 2s for one transaction.	Epic 4: User Story 1, User Story 2, Performance, Security
Identity Management System	The management of identities will be handled in different systems. The identity management system shall be available 24/7, all days of the year. It	Availability Security

Component	Description	Functional or Non-Functional Requirement Satisfied
	will cooperate with advance security measures such as multi-factor authentication, to secure personal sensitive data and limit the potential data loss to 0.5%.	
Corporate Donation Matching	Donations that qualify for corporate gift matching will be identified. This system should be available 24/7, all days of the year for the donors to make a payment.	Epic 2: User Story 3, Availability
Inbound/ Outbound Messaging	This provides the solution with a flexible avenue for communication with all external actors interacting with Student Aid. It should support different languages, provide a consistent experience and same workflows and be protected.	Epic 6: User Story 1, User Story 2, User Story 3, User Story 4, Usability, User Experience, Security
Scheduling System	This provides a solution for users to manage their appointments. It should provide a consistent experience and same workflows for all users, and the data should be protected.	Epic 3: User Story 3, Epic 5: User Story 1, Epic 7: User Story 2, Epic 7: User Story 3 User Experience Security
Record System	This generates reports and statistics about the F2E program. It should clearly maintain a single source of truth for information stored, make an appropriate number of copies of the data, and the data should be protected.	Epic 1: User Story 1, Single Source of Truth, Security, Data Resiliency

Component	Description	Functional or Non-Functional Requirement Satisfied
Analytics System	This is the internal user portal to view various reports. Typically, this information is retrieved real time from SQL. It should clearly maintain a single source of truth for information stored, and the data collected or generated should be protected.	Epic 1: User Story 1, User Story 2, Single Source of Truth, Security
To be built		
User Management	This is make up of a catalogue of users, including external users and F2E employees. It should be available on different devices 24x7, all days of the year. Also, the private information should be protected.	Epic 2: User Story 4, Availability, Security
Communication System	This allows communication between users within the scope of the solution through the option of messages and notifications. It should provide a consistent experience and same workflows for all users, and the data should be protected.	Epic 6: User Story 3, User Experience, Security
Fund Management System	This keeps track of all financial transactions flowing in or out of the solution. It should be available 24x7, all days of the year, and the financial information should be protected.	Epic 2: User Stories 1-5, Availability, Security
Matching System	This employs advanced search and filter functionality to match coordinators/mentors to students.	Epic 6: User Story 2, User Experience, Flexibility, Security

Component	Description	Functional or Non-Functional Requirement Satisfied
	Also, it enables the allocation of funds to students, so the information will be protected. It should be modified easily and provide a consistent experience and same workflows for the users.	
SQL	This can store various data. The data inside should be protected, and be available 24 x 7, all days of the year. Also, the number of copies of the data will be made.	Availability Data Resiliency Security



Software Architecture Showing components connectors and runtime behavior

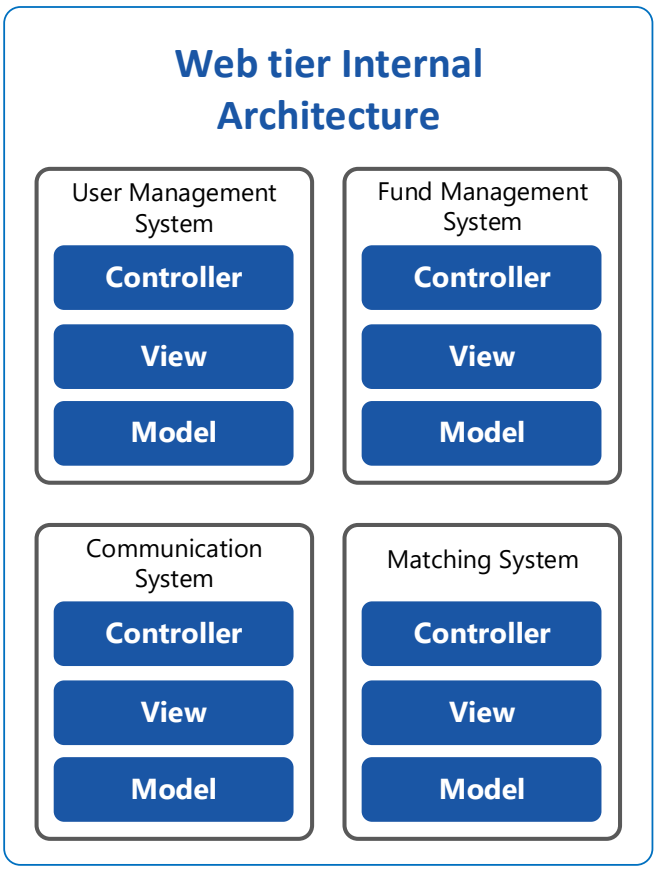
Architectural Styles

- N-tier

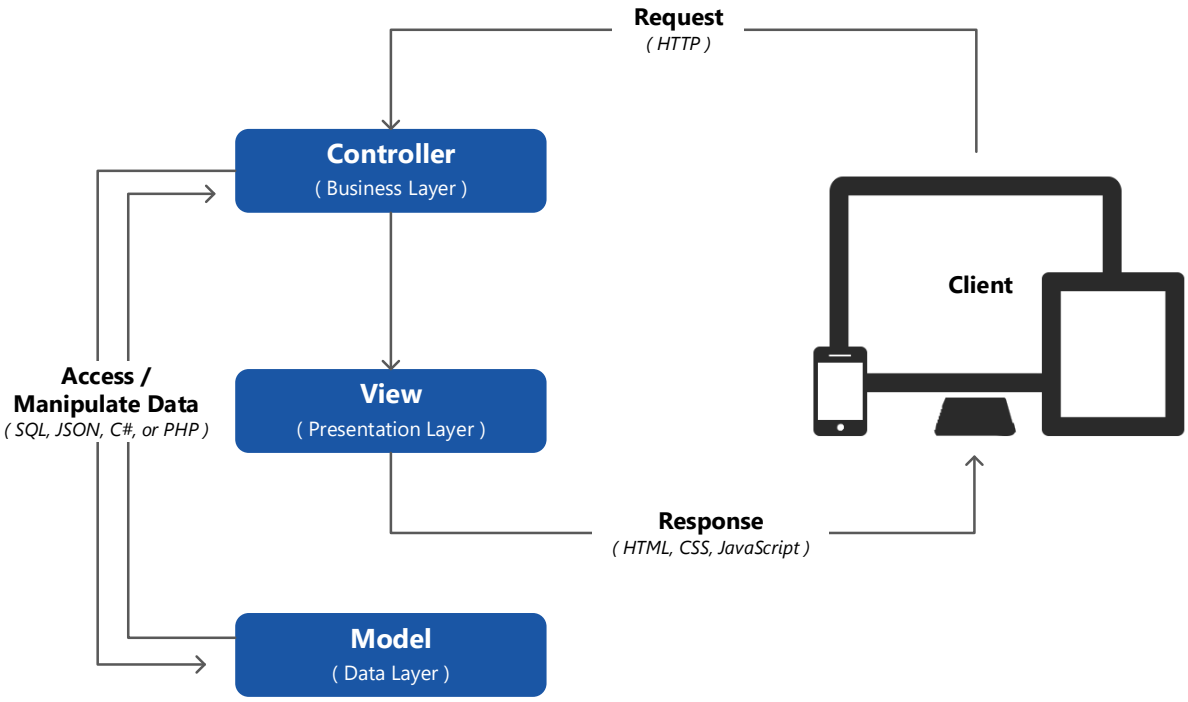
  We use **N-tier** architecture as the primary architectural style for the solution. This style lets us divide up our application into **logical layers** and **physical tiers** which allow us separate responsibilities and manage dependencies. To keep our solution simple, we make use of only two physically separate tiers, a **Web tier** and a **Data tier.** Separation of tiers physically helps us improve scalability and resiliency, using only two tiers instead of the traditional three allows us minimize network latency. Within the Web tier we further divided the application into various logical layers a **Business Layer**, a **Presentation Layer** and **Data Layer.**

- Model-View-Controller

  Within the web tier we make use of **Model-View-Controller** layered architecture to separate the internal responsibilities of information from the way it is presented to the user. Each internal component: User Management System, Fund Management System, Communication System, and Matching System will be decoupled into three major components (Model, View and Controller) which will allow efficient code reuse and parallel development. Secure HTTP requests are received by the controller from the user's device (Website, or Mobile App). The controller contains the main program flow and processes the information it receives and passes it on to the Model. The Model is responsible for querying the databases. It manipulates data in the databases based on information it received from the controller. The results of those queries are passed back to the controller which in turn passes it on to the view for presentation. This architectural style offers us the advantages of high cohesion and loose coupling.



This diagram shows the high level architectural style to be used for each internal component of Student Aid deployed within a VM. ***Model – View – Controller*** *is a popular layered architecture style that has proven effective in the design of web applications.*



Model – View – Controller *Architecture diagram showing how internal responsibilities of manipulating and presenting information is separated.*

Component	Description
Client Layer	All users access the Student Aid solution through a web browser or a mobile App. The will be optimized for Mozilla Firefox, Google Chrome an Microsoft edge on the Windows operating system and Safari Browser on Mac OS. Users will be provided a mobile version of the site optimized for devices of different screens, Native Mobile Apps will be available for Apple iOS and Google Android.
Presentation Layer	The **View** is the presentation layer. HTML, CSS, and JavaScript will be used to present rich media contents to clients.
Business Layer	The **Controller** is responsible for managing the flow of business rules that determine how data is manipulated. The controller provides a separation between the presentation layer and model layer. The Client is not given any means or directly accessing or modifying F2E data.
Data Layer	The **Model** is the data layer. It is responsible for querying the databases. It is an abstraction of the logic used to query our data stores.

- Our architecture leverages the advantages of different cloud delivery models, all external components will be integrated as remote services using SaaS, the web tier will be implemented as IaaS while the data tier will be implemented as PaaS.
- Implementing the web tier as IaaS gives us full control of the development environment allowing us greater flexibility for developing the internal components. Although deployment as IaaS implies that more work will have to be put into the maintenance of the infrastructure, we choose to go with it so that we can carry out the development using any technology and frameworks that the developers are already comfortable with. It will be also relatively cheaper than using managed services. We make use of three virtual machines placed in an availability set, this is done to avoid single point of failure and provided resiliency

in case one machine fails. An external load balancer is used to distribute request across the VMs in the web tier.

- The Data tier is implemented as PaaS which requires less management than IaaS. We employ various managed services for caching, storage, messaging, database and search. The web tier connects to the data tier using synchronous communication.

Component	**Description**	**Quality Attribute Satisfied**
External Components (Remote Services)		
Google Analytics	This freemium web analytics service will be used to track and report website traffic. It will provide useful insights about the performance and usage of F2Es website and Mobile Apps.	Testability, Agility
PayPal	This payment system allows payments to be received.	Epic 4: User Story 1, User Story 2, Performance, Security
i-Payout	This payment system allows payments to be sent.	Epic 4: User Story 1, User Story 2, Performance, Security
Double the Donations	This corporate matching system allows donations to be matched.	

Service used to design Internal Components		
Azure Storage Account	This is managed storage as a service. It offers highly available, secure and scalable data storage services. Microsoft Azure handles the maintenance and patching of the underlying infrastructure on which it runs. Azure Blob storage is the service that will be within the storage account.	Availability, Modularity
Resource Group	These are Logical containers that we use to group related Azure resources. Resource groups will enable us automate setup and provisioning. It will also enable geo-replication and load testing. We have made use of two resource group to separate resources that are IaaS from those that are PaaS. This will enable us to monitor and track billing for related resources together.	Modularity, Availability, Testability
Virtual Machine	These are compute resources that give virtually full control over how our application is hosted. Aside from management of the actual hardware we will have control of the operating system, server configuration and application configuration, this also means that we will be responsible for patching and keeping the system antivirus running. The website and mobile application code will be hosted these virtual machines.	Availability, Scalability

Virtual Network	This is a service that enable azure resources to communicate privately with each other and publicly with the internet. It is essentially a specific IP space configured to provide a logical isolation of azure resources. Our virtual network is further broken down into subnets which contain either individual virtual machines or VMs within an availability set. Virtual machines have completed communication across the virtual network even if they are in different subnets. Our architecture has a subnet for the web tier, DMZ, and management subnets.	Modularity,
Network Security Group	Network Security Groups are assigned to each subnet. NSG enable us to assign security rule to each subnet which then applies down to each VMs with the subnet. With network security groups we ensure that only the Public DMZ in and management subnet is given open access to the internet. The web tier subnet does not have open accessed to the internet, it can only be accesses through the public DMZ out subnet.	Security
	This is a hosting service for DNS domains. We provide DNS resolution using Azure infrastructure.	Security
Availability Set	The availability set ensures that our virtual machines are distributed across multiple isolated hardware nodes in a cluster. It helps ensure that if hardware or software failure occurs within azure only a subset of our VMs will be impacted. Using at least two virtual machines within each availability set enables us to take advantage of Azures 99.95% SLA.	Availability, Scalability,

Azure Storage Blob	Blob Storage is a Managed Storage service which we will use to store static content such as Images, CSS, ad Scripts, which will then be pushed to the content delivery network from where it is served directly to the client. CDN will deliver these contents directly to the client from a location closest to the user. Blob storage works together with the CDN to optimize the performance of the website and Mobile Apps. This also indirectly improves the usability.	Performance
Azure SQL Database	This is a relational managed database service which we will use to store transactional data entities used in the solution. Need to have ability for replication.	Data Resilience, Performance, Security
Azure Redis Cache	This is a distributed open source cache that is managed by Azure. This component will prove significant as student Aids solution is scaled up. It provides quick access to data from all the services and all instances running in our application. It will enable us to reduce the load on the database by caching frequently used queries. We will also implement a disaster recovery plan that guarantees maximum uptime.	Performance, Scalability, Availability
Azure Search	This provides indexing and querying capabilities for data stored in the data tier.	Performance

Azure Content Delivery Network	This is a CDN service that enables the storing and accessing of data on different content servers and locations. It helps provide better bandwidth and quick delivery of data by placing content on servers in different geographical location across the world so that content can be served from a location closest to the client.	Performance
Load Balancer	This is a service that allows a group of virtual machines to appear as a single machine to user's requests. When the load balancer receives a request, it decides which Virtual Machine to send that request and then forwards the request to the machine. The load balancer determines which VMs is available and has the least amount of load on it. It ensures that requests are not sent to VMs that are offline. We make use of both external and internal load balancers in our architecture.	Availability
Jump Box	This is a special virtual machine within its own subnet that uses special network security group rules to allow connection to other VMs using Remote Desktop (RDP) or Secure Shell (SSH). All other VMs in the system do not allow RDP or SSH connection except for the Jump box. We set these rules using the NSG.	Security

3. Security architecture

Our threat modeling reveals that, there are five main types of threats involving our systems, including spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. To mitigate these potential security issues, we will provide various layers of security for our architecture to ensure sufficient defense in-depth without crippling functionality of the system. Security has been a main consideration in the design of our architecture. We now go into the details of how security has been achieved at various levels.

Network Protection is front-end access protection declared at various layers to ensure a secure network environment.

Network Protection	
Components	Description
DDoS protection	A layer of the Azure physical network that protects the Azure platform from large-scale internet-based attack and monitors out-bound traffic and cross-Azure region traffic. This service is automatically provided by Microsoft Azure
Demilitarized Zone	The first layer of network security within our system is achieved by creating a demilitarized zone (DMZ) that faces the public and handles traffic from the internet. External users access the system through a public IP. An external load balancer is used to direct the traffic to one of two

	Network virtual appliance (NVA) within an availability set in the public DMZ. Approved requests are then passed on to the web tier through an internal load balancer. The DMX is our perimeter security for the system. The internet facing load balancer is configured to accept requests only on the ports necessary for internet traffic. Inbound HTTP requests are restricted to port 80 and inbound HTTPS requests to port 443. The NVA are specially monitored to make sure that at least one NVA is available. Monitoring and management of the NVAs in the public DMZ is performed by the jump box in the management subnet. A single network route to the jump box is used to restrict access. NSG rules for the inbound and outbound public DMZ subnets prevent the NVAs from being compromised, all requests outside the NSG rules are blocked. Network address routing configurations for the NVAs directs incoming requests on port 80 and port 443 to the web tier load balancer but ignores requests on all other ports. We will log all incoming requests on all ports. Any request that falls outside of expected parameters indicate intrusion attempts.
Azure Virtual Network Isolation	Azure virtual network isolation ensures complete isolation from all other networks and that traffic only flows through user configured paths and methods.
NSG	Network security groups contain a list of security rules that allow or deny network traffic to resources connected to Azure virtual networks. It creates security boundaries to protect the application deployments in the protected network. We configure network security group rules such that only the public DMZ subnet allows traffic to flow in from the internet. All other subnets can only communicate within the Virtual Network.
Role Based Access Control	Using Azure Active directory and Azure Resource Manager we add another layer of security to the system through implementation of Role Based Access Control. Different administrators are assigned different levels of privileges to different resource groups. We will restrict access to

	IP addresses within our virtual network.

Advanced Threat Detection security services provides the ability to detect, diagnose and analyze the risks associated with the malicious activities targeted against servers.

Advanced Threat Detection	
Components	**Description**
Active Directory Identity Protection	Active Directory identity protection can detect risk events and risky accounts and generate reports and alerts that enable F2E to investigate risk events and take appropriate mitigation action.
Azure Security Center	Using Azure Security Center, we monitor traffic, collects logs, and automatically collect security information to identify threat. It also uses big data and machine learning technologies to detect threats that would be impossible to identify using manual approaches and predicting the evolution of attacks.
Azure antimalware	It has following features, including real-time protection, scheduled scanning, malware remediation, signature updates, antimalware engine updates, antimalware platform update, active protection, samples reporting, exclusion, and antimalware event collection. It will run in the background without human intervention.

Auditing and logging of security-related events and alerts are important in data protection. The following components will provide F2E with an electronic record of suspicious activities and help F2E to detect patterns that may indicate attempted or successful external penetration of the network, as well as internal attacks.

Auditing and logging	
Components	**Description**
Azure Active Directory Audit Report	Azure Active directory provides security, activity and audit reports for F2E directory. It helps F2E to identify privileged actions that occurred in the Azure Active Directory. The reports provide the audit record for the event name, the actor who performed the action, the target resource affected by the change, and the date and time (in UTC).

Azure Security Center Alerts	Azure Security Center automatically collects, analyzes and integrates log data from Azure resources, the network, and connected partner solutions, like firewall and endpoint protection solutions, to detect real threats and reduce false positives. Security Center will show a list of prioritized security alerts along with recommendations for how to remediate an attack.
Azure monitor	It is basic monitoring by allowing the collection of metrics, activity logs, and diagnostic logs.

Identity and access is to manage user access for security purpose.

Identity & Access	
Components	Description
Azure Active Directory	Azure Active Directory will create and manage a single identity for each user across hybrid enterprise, keeping users, groups, and devices in sync, provide single sign-on access to the applications including thousands of pre-integrated SaaS apps, and enable application access security by enforcing rules-based Multi-Factor Authentication for cloud applications.
Multi-factor Authentication	A method of authentication that requires the use of more than one verification method and adds a critical second layer of security to user sign-ins and transactions. MFA helps safeguard access to data and applications while meeting user demand for a simple sign-in process.
Analytics & Reporting	F2E can use Azure Active Directory's access and usage reports to gain visibility into the integrity and security of your organization's directory. These reports include anomaly reports, integrated application reports, error reports, user-specific reports, and activity logs.

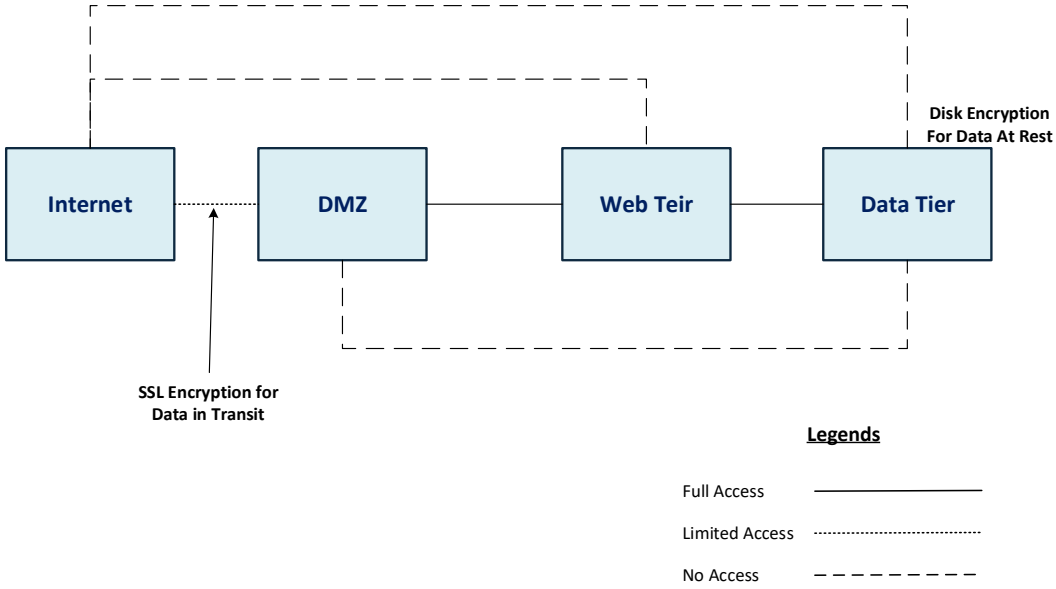
Network security control is for F2E to manage the security of its cloud-based assets in Azure virtual network, a public cloud service platform.

Network Security Control	
Components	**Description**

Network Access Controls	Network access control provides isolation and protection. F2E can control access by permitting or denying communication between the workloads within a virtual network. NSG will be the main tool.
Load balancer	Load balancer can deliver high availability and network performance to applications because it can distribute incoming traffic among backend virtual machine instances and support network address translation to route traffic between public and private IP address.
Traffic manager	Traffic manager control the distribution of user traffic for service endpoints in different datacenters. It uses the domain name system (DNS) to direct client request to the most appropriate endpoint and the health of the endpoints.
Resource manager	Resource manager helps F2E to deploy, manage and monitor all the resources for its solution. Also, F2E can apply access control to all services in its resource group because role-based access control is integrated into the management platform.

Data security is for F2E to protect data in the cloud.

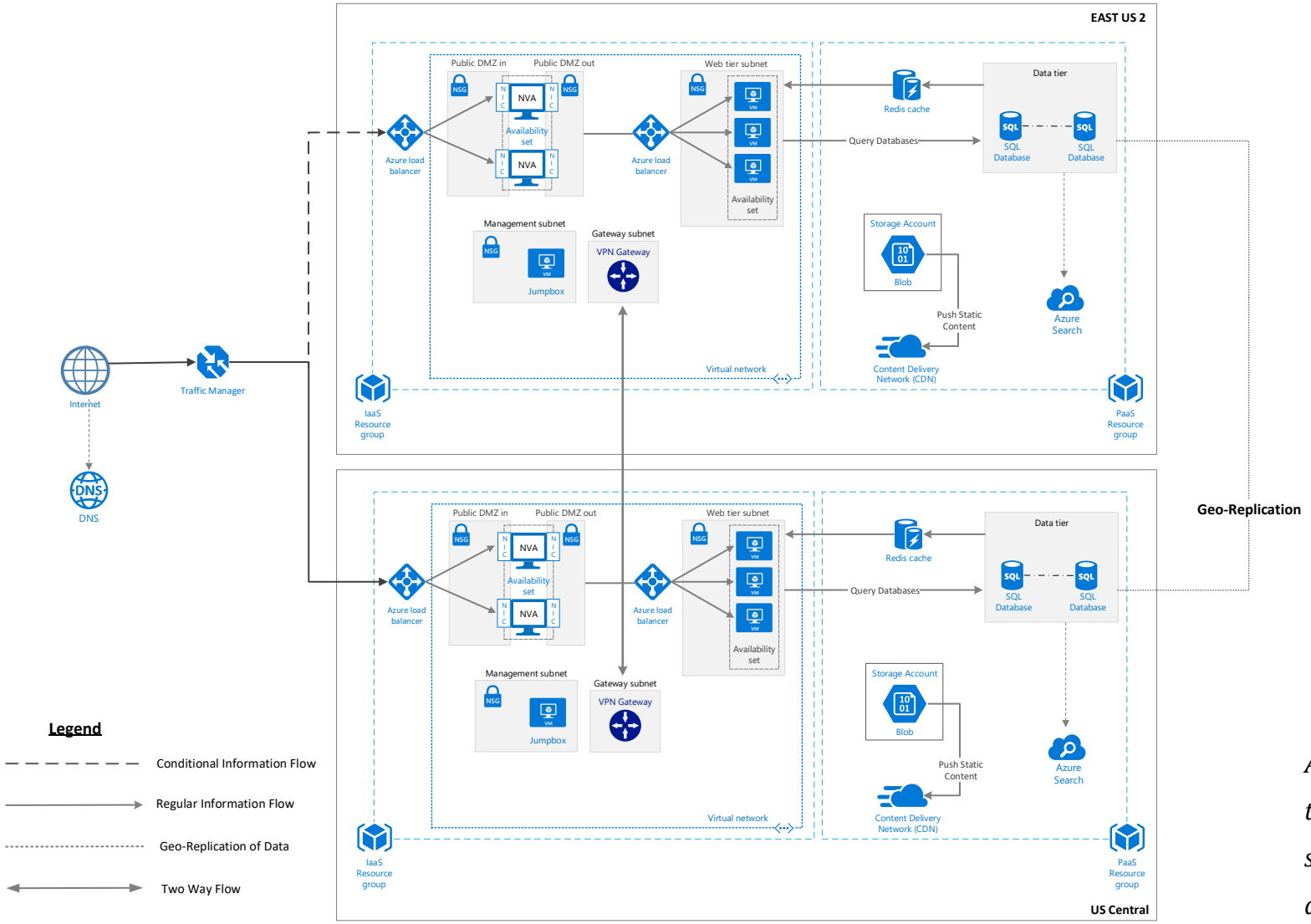
Data Security	
Components	Description
TLS/SSL	Transport layer security protocol is to protect data when it is traveling between the cloud services and customers. It provides strong authentication, message privacy, integrity, interoperability, algorithm flexibility ease of deployment and use.
PFS	Perfect forward secrecy is to protect connections between customers' client systems and cloud services by unique keys.
Azure Disk Encryption	This provides us with data encryption at rest without having to bear the cost of implementation and management. Azure provides this service.
Azure key vault	Azure key value safeguard encryption keys and application secrets like passwords using keys stored in hardware security modules. It can improve performance and reduce the latency of cloud applications by storing cryptographic keys in the cloud.



Security View Showing How Architectural Decision affect the Security of the System

3. Infrastructure/Deployment architecture

To manage the various incoming requests, the Traffic Manager routes each to one of the regions available: primary or secondary. Two regions are used to achieve higher availability, so if one is down, the other will take over. The DNS hosting service provides name resolution using Microsoft Azure infrastructure. The DNS records can be managed using the same credentials, APIs, tools, and billing as with the other Azure services. Microsoft azure ensure that the deployments in the two regions are connected vis a virtual private network.



Allocation View Showing the deployment of the solution in various regions and the geo-replication of data

4. Technology stack

- **List of criteria used:**

The list of criteria used for choosing the specific products are popularity, price, usage, agility and security.

1. Record system:

Product Name	Pros	Cons	Decision
SharePoint	Usage: can create forms or surveys that can collect information in an effective way including end-user information Security: Restrict access to specific content, folders or files. Agility: It can quickly allow you to organize, filter, and search content	Price: $5-10 per user per month More complex	No
OpenText	Usage: Create metadata to help with searching and control versioning to see multiple versions of a document Security: One source of the truth		Yes

2. Payment System:

Product Name	Pros	Cons	Decision
PayPal	Popularity: well-known and trusted by millions of people Security: it provides 60 days for claiming refunds against unauthorized charges Agility: transaction can be completed within minutes Usage: support more than 220 countries and available for all devices Price: free for pay; 2.4%-3.4% + $0.30 USD per domestic transaction if receiving more than $3000; charity organizations such as F2E pay less	Security: PayPal company will store personal information. Users must have a PayPal account.	Yes
Apple Pay	Security: Users can pay by using touch ID or double-clicking Apple Watch to securely provide their payment information and Apple will not see or store any of private information.	Usage: can be used only on iOS device or safari Agility: Transfers to a bank account take one to three days	No
Google wallet	Usage: Users can send money through app, Gmail, web or text message. Price: No fees to send or receive money if users pay via bank account linked to google wallet ID Security: Google offers a 180-day for claiming refunds against unauthorized charges	Price: 2.9% per transaction for any payments done via a debit or credit card Usage: only available to US-based Gmail users	No

3. Analytics System:

Product Name	Pros	Cons	Decision
Google Analytics	Popularity: It has been used in more than 60 million websites and more than 224 countries Price: Free if the website gets less than 10 million hits per month Usage: can be applied to website, mobile and other digital environment; allow customized data collection and report creation	Usage: Custom reports may have limits and it requires training Price: expensive if upgraded to premium when the traffic is high	Yes
Power BI	Usage: Easily analyze key data, share critical insights across the enterprise, and create innovative visualizations and reports; it can also connect to google analytics Price: Standard (free to any single user and comes with 1 GB of storage; Data can be streamed from this cloud offering at 10k rows/hour.); Pro ($9.99 per user per month with 10 GB of storage; Data can be streamed at 1 million rows/hour)	Usage: cannot publish reports; only available on a SaaS model.	No
Tableau	Price: Tableau Online is fully hosted and starts at $42 Usage: Easily accessible in the cloud for users to share reports quickly from anywhere	Usage: Businesses must rely on Tableau to maintain servers and provide support for any issues. Price: high cost for small business	No
Quantcast	Popularity: It has been used in more than 12 million websites Price: Free Usage: Good at analyzing volume of traffic, showing geographic distribution of traffic and demographic information of website visitors	Usage: Only support Android app	No

4. Identity management system

Product Name	Pros	Cons	Decision
Facebook	Popularity: 750 million users		Yes
Google	Popularity: 1 billion users		Yes
LinkedIn	Popularity: 500 million users		Yes
Microsoft	Popularity: 400 million users		Yes
Twitter	Popularity: 330 million users	Less suitable for our users	No

5. Scheduling system

Product Name	Pros	Cons	Decision
Calendly	Usage: Easy to navigate; it can connect with multiple services making it simple and easy for various users. Basic plan has multiple features, including Calendar integrations with Google Calendar, Office 365, Outlook and iCloud, Schedule unlimited events and Automated event notifications. Premium plan provides several choices for integrations. Price: Free for basic, $8 for premium per user per month, $15 for pro per user per month.		Yes
Acuity	Price: Free for basic, at least $15 per month for pro. Usage: Embed scheduler into your website; Syncing with Google Calendar and so on.	Price: More expensive than Calendly if needed more features. Usage: Basic plan is free but it only has self-scheduling and appointment services.	No

6. Payout System

Product Name	Pros	Cons	Decision
i-Payout	Usage: Make payments easily without requiring recipients to have an account.		Yes

7. Inbound/outbound messaging system

Product Name	Pros	Cons	Decision
SendGrid	Usage: Provides scalability, real-time analytics, and flexible APIs.		Yes
GoDaddy	Usage: Provides domain email. Popular and provides expert 24/7 support. Works with Outlook, Apple Mail, and others.	Usage: Cannot be managed within Azure.	No
MailChimp	Usage: Send bulk emails easily.		No

8. Corporate Donation Matching system

Product Name	Pros	Cons	Decision
Double the donation	Popularity: Mainly for small and medium sized nonprofits Price: $299/year of basic plan for smaller individual nonprofits with fewer than 1000 donors, $499/year of premium plan which provides flexibility, customization and	Usage: only premium plan has embedded plugin	Yes

	integration to the website and donation process. Usage: Can be embed double the donation's matching gift plugin in F2E website.		
360MatchPro	Popularity: Mainly for large nonprofits with more than $25000 in annual matching gift revenue Price: $3000/year Usage: Automate matching gift identification across your fundraising, drive matches to completion and provide actionable insights and reporting portal. It also can be embedded in website.	Price: more expensive than double the donation	No

Technology stack table

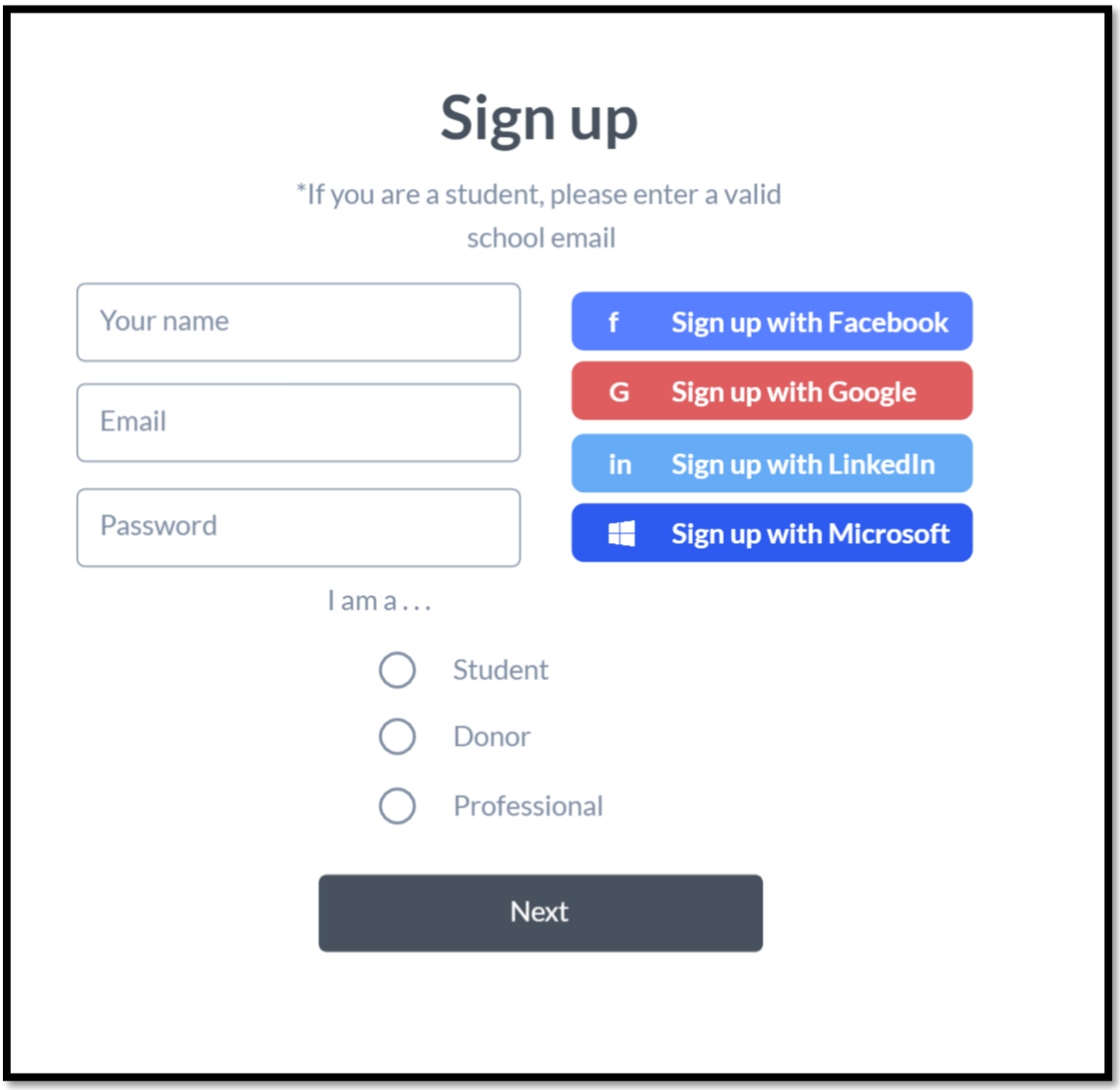
Architecture component	Technology Choice	Justification
Front-End	HTML	To build website
Front-End	CSS	To customize website
Front-End	JavaScript	
Back-End	Python	
Back-End	SQL	To store data
Back-End	Apache	HTTP Server
SaaS Payment System	PayPal	More popular, cheaper and can be used in more countries
SaaS Analytics System	Google Analytics	Free for basic plan which has many features and it can publish reports
Database	SQL Database	
Virtual Machines	Windows Server	
SaaS Scheduling System	Calendly	cheaper
SaaS Identity Management System	Active Directory, Facebook, Google, LinkedIn, or Microsoft	More popular
SaaS Record System	OpenText	Simple
SaaS Payout System	i-payout	
SaaS Inbound/Outbound Messaging System	SendGrid	Can be used in Azure
SaaS Corporate Donation Matching System	Double the Donations	cheaper

5. User Interface

The Student Aid UI will offer similar formats across platforms including website browser and mobile application. Each device will be presented with a welcome screen, login / signup, account information, the ability to make payments online, and view messaging inbox for logged in users. Users may select a language of their preference and may have the page read aloud. There is also an option to sign up with Facebook, Google, or LinkedIn to make registration easier. Students will be prompted to enter a valid school email to sign up. There is a consistent format across all devices.

UI: Website / Browser

1. Login and Sign Up



Students are required to provide a valid school email during sign up.

Login

Email

Password

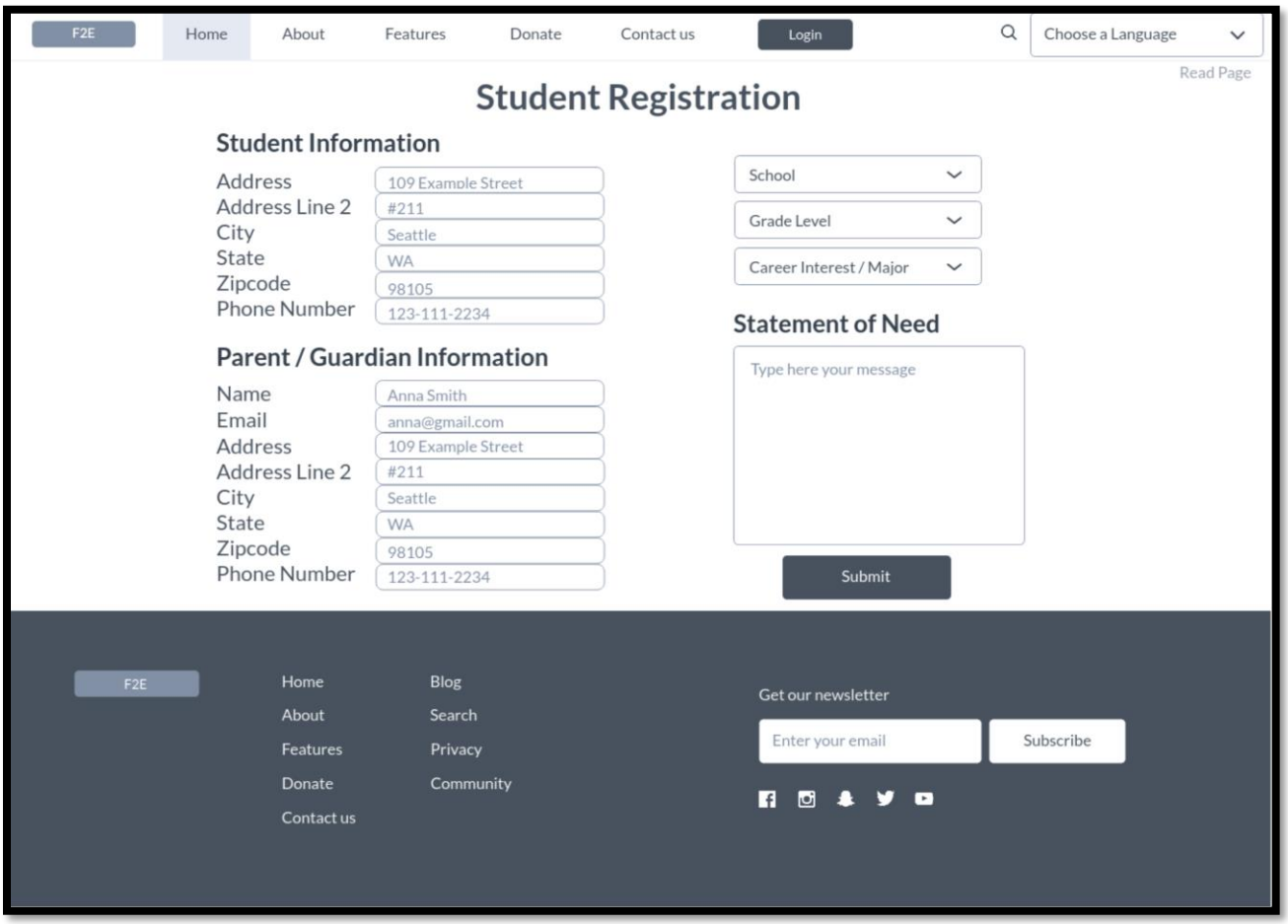
Sign Up

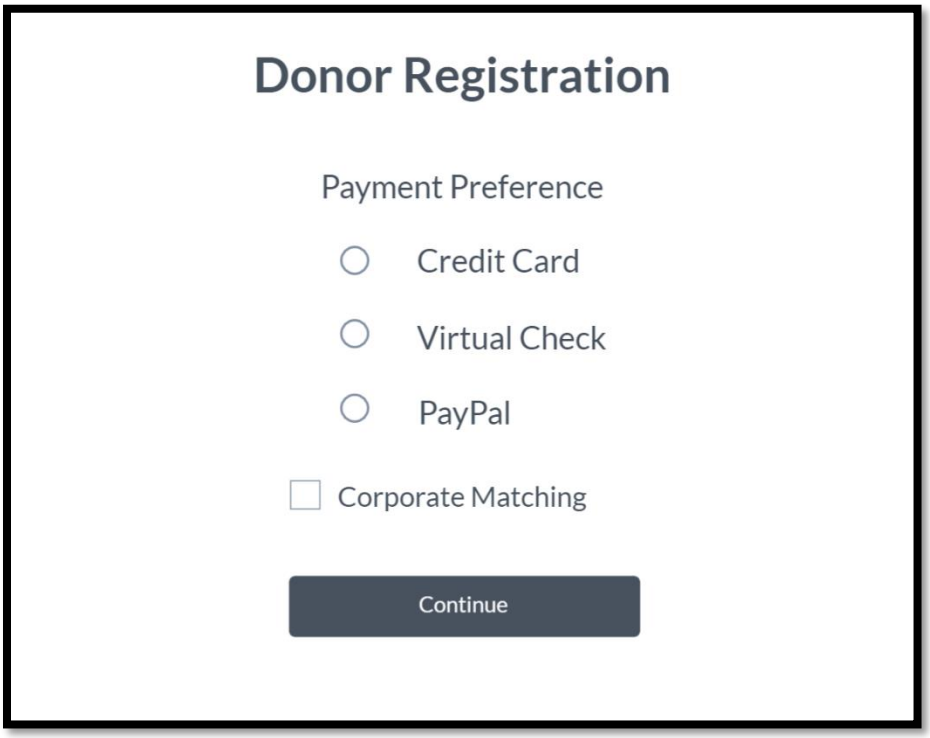
Login

Forgot your password?

2. Registration and Payment

All users must provide basic information in the registration page.





If donors choose PayPal, then a PayPal sign in / sign up page will pop up.

Virtual Check Payment

Billing Address

*Address

Address Line 2 (optional)

*City | *State | *Zip Code

*Phone Number

Virtual Check

Account Name

Account Number

Routing Number

Confirm

Credit Card Payment

Billing Address

*Address

Address Line 2 (optional)

*City | *State | *Zip Code

*Phone Number

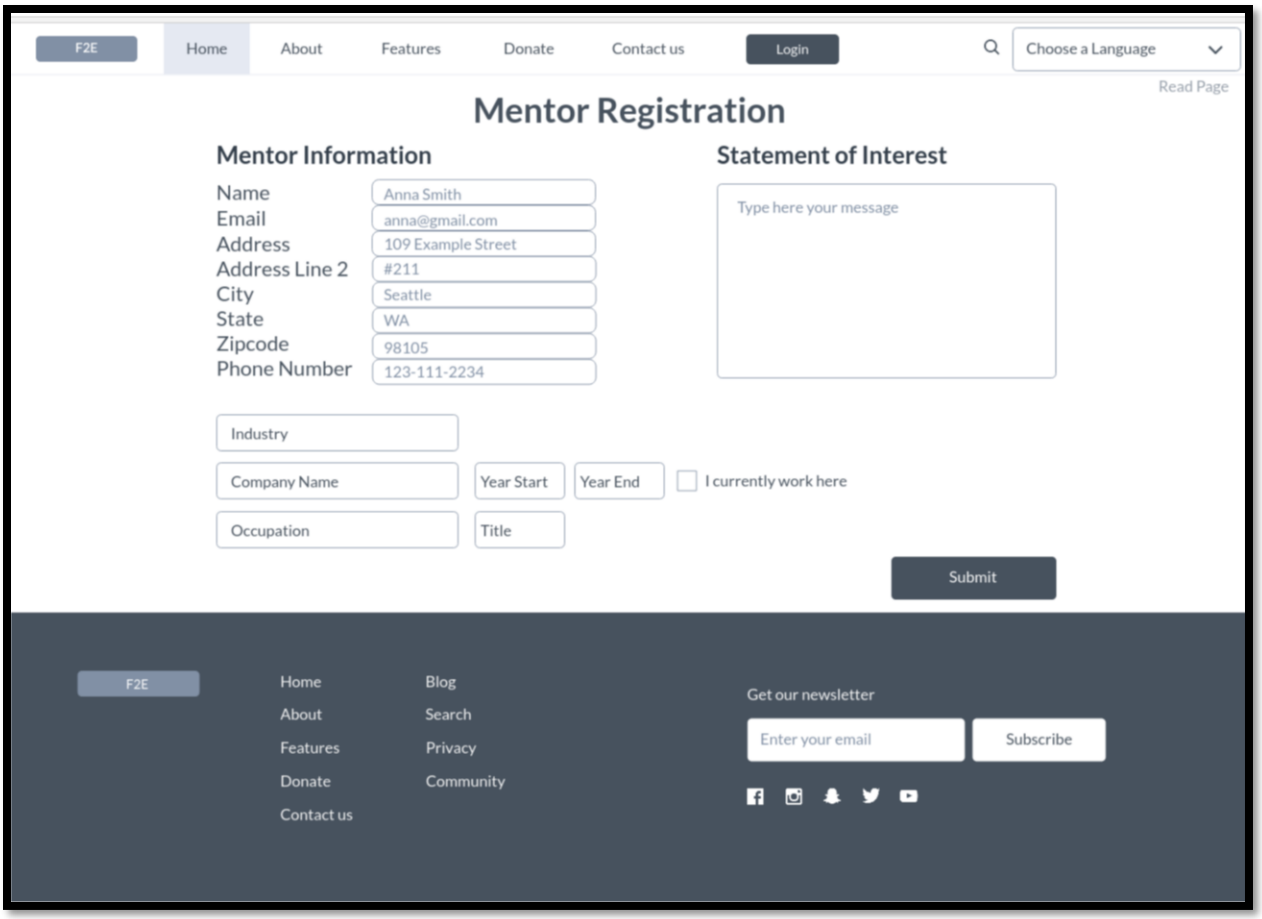
Credit Card

Account Name

Card Number

Exp Date | CVV

Confirm



3. Account Pages

Student Account

- Account Information
- Payment Tracking
- Find Mentor
- Send Reports
- Inbox

Donor Account

- Account Information
- Make a Payment
- Payment History
- Inbox

Mentor Account

- Account Information
- Requests
- Calendar
- Inbox

Admin Account

- Account Information
- Requests
- Review Files
- Templates
- Inbox

F2E | Home | About | Features | Donate | Contact us | Logout | Choose a Language

Read Page

John Goodman
Student

- Account Information
- Payment Tracking
- Find Mentor
- Send Reports
- Inbox

Rate us

Student Account Information

Student Information

Address	109 Example Street
Address Line 2	#211
City	Seattle
State	WA
Zipcode	98105
Phone Number	123-111-2234

School	Seattle University
Grade Level	Freshman
Career Interest	Computer Science

Expected Graduation Date 06/10/2021

Parent / Guardian Information

Name	Anna Smith
Email	anna@gmail.com
Address	109 Example Street
Address Line 2	#211
City	Seattle
State	WA
Zipcode	98105
Phone Number	123-111-2234

Back | Request Change

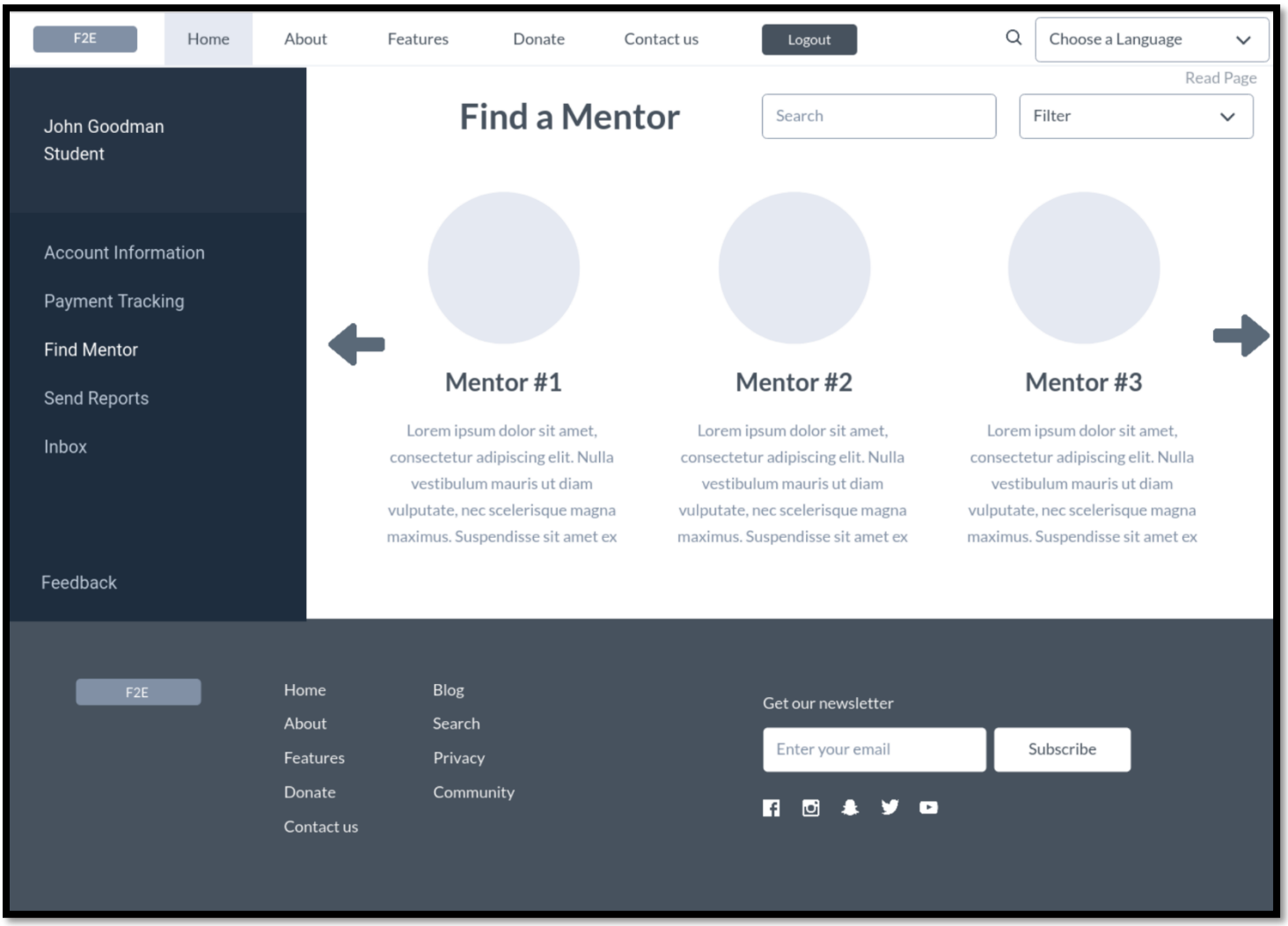
F2E

Home
About
Features
Donate
Contact us

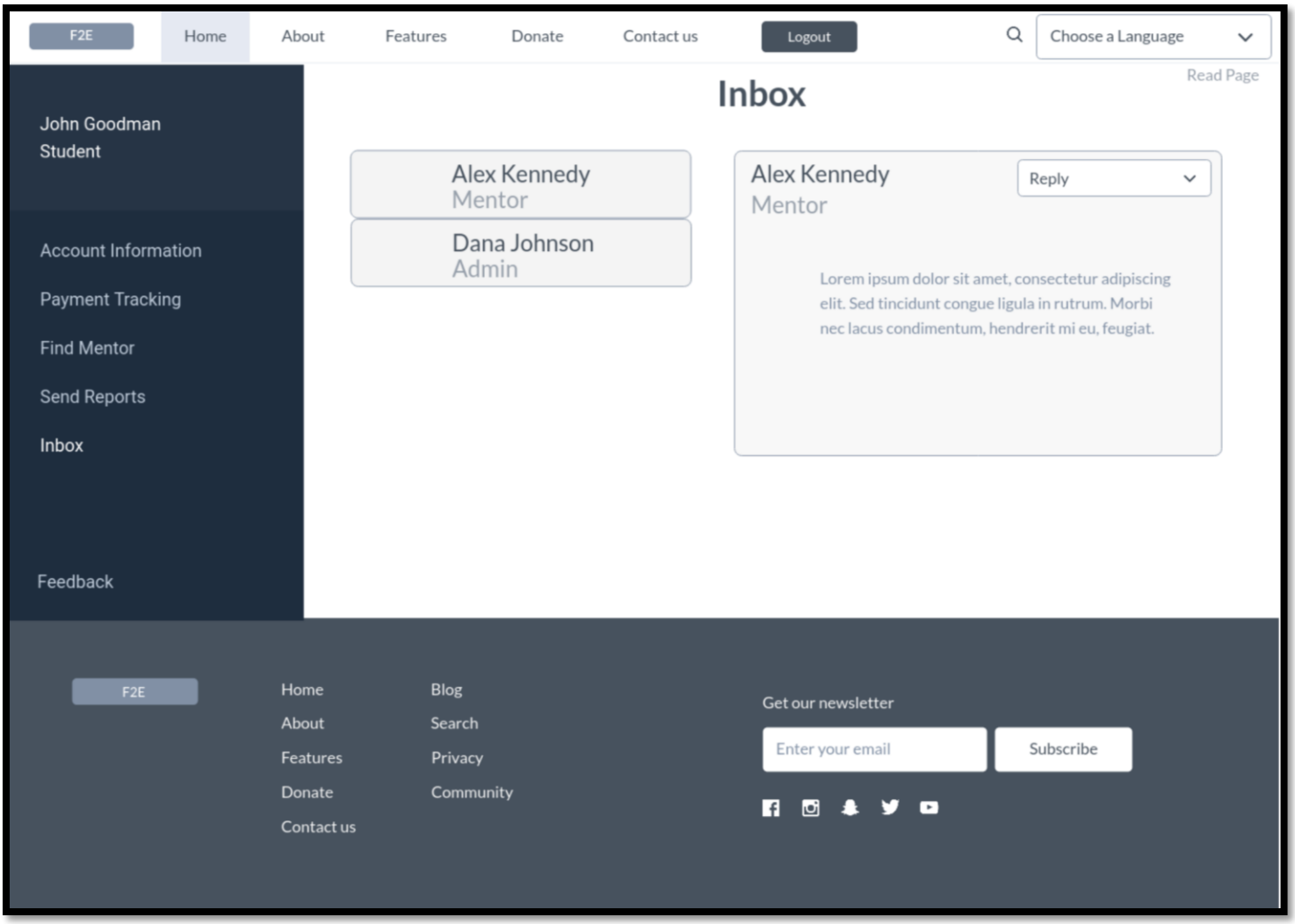
Blog
Search
Privacy
Community

Get our newsletter

Enter your email | Subscribe

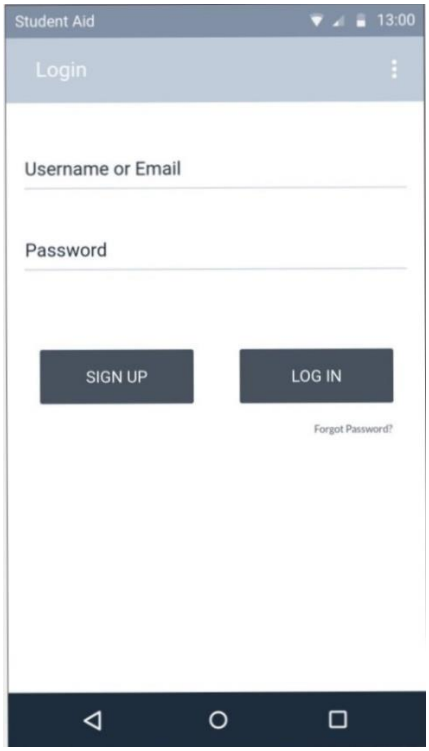


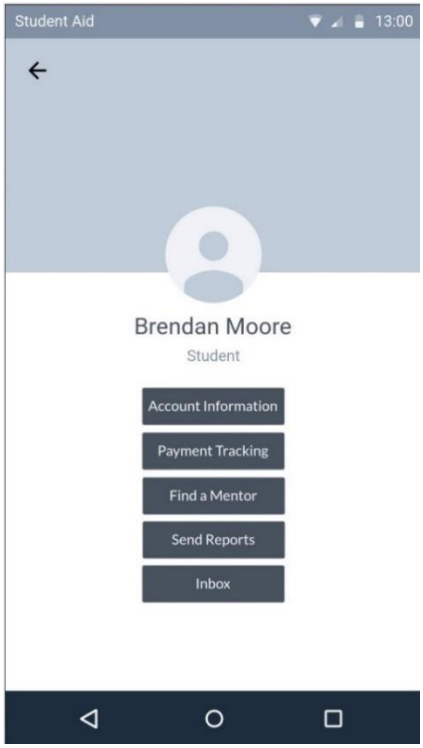
Students can use search and filter options to find a particular mentor of their choice.

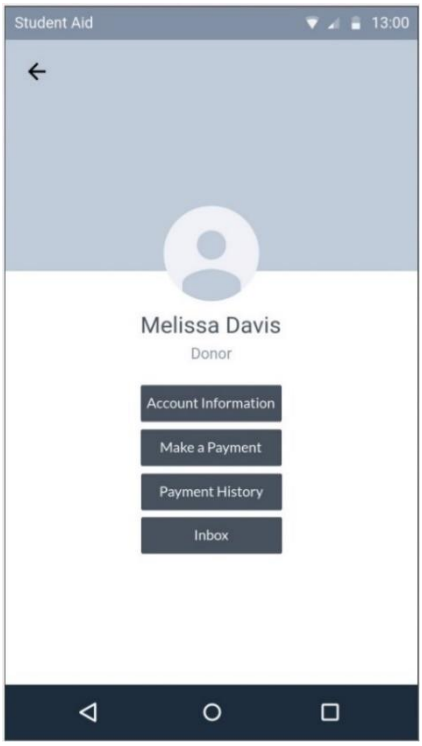


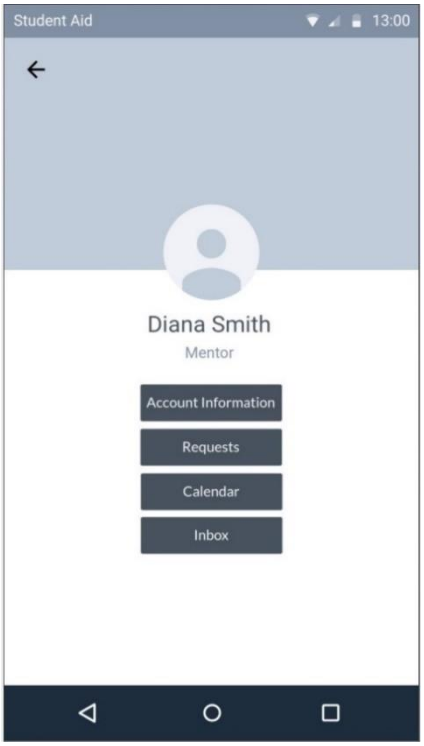
Users may communicate with their mentor or F2E admins using their inbox.

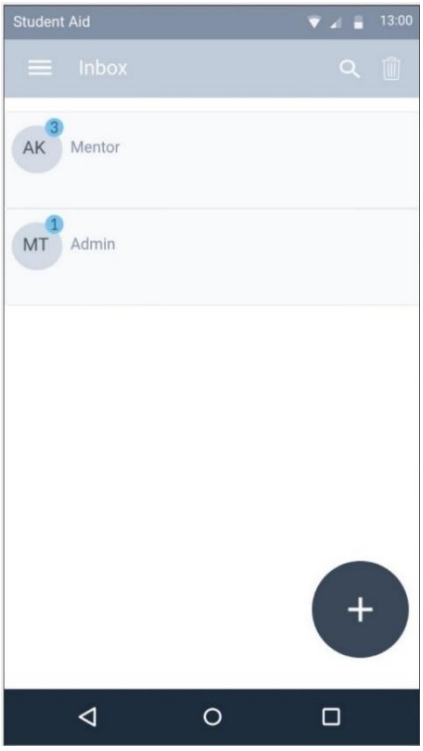
Mobile Application Screens:

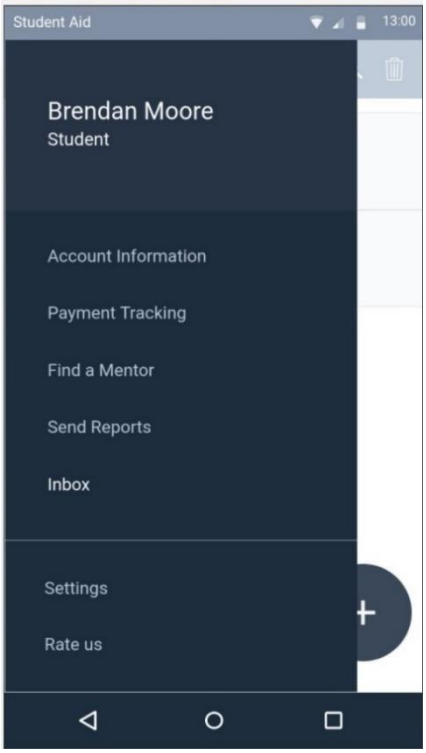


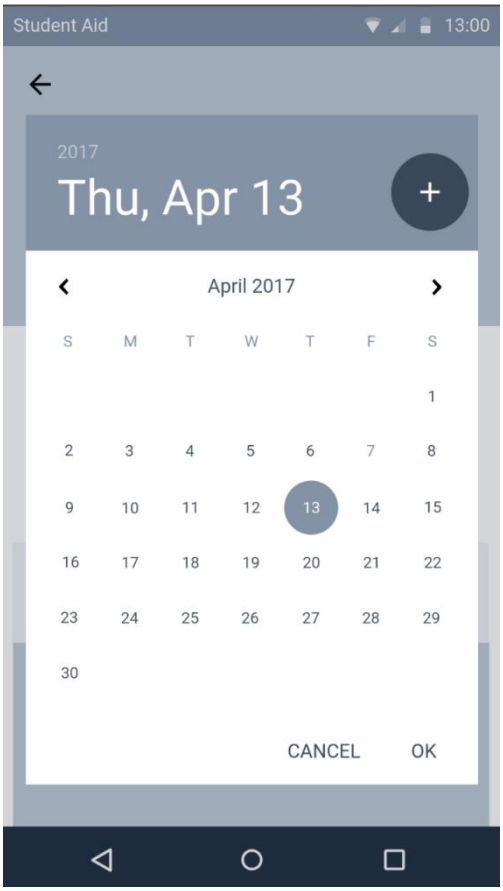






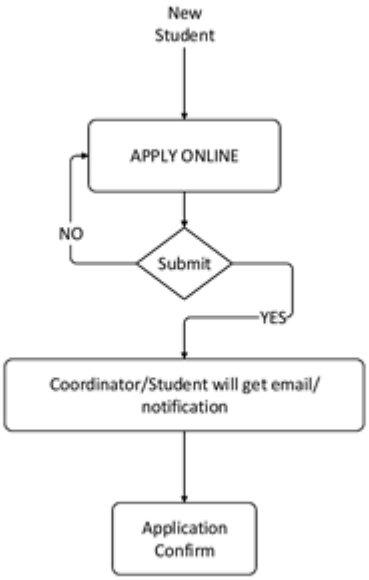




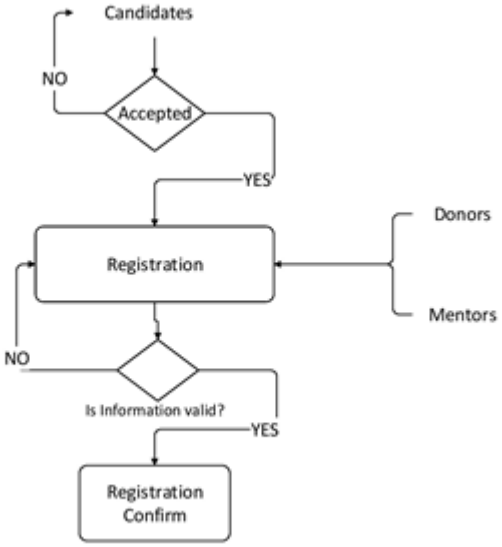


Process diagram

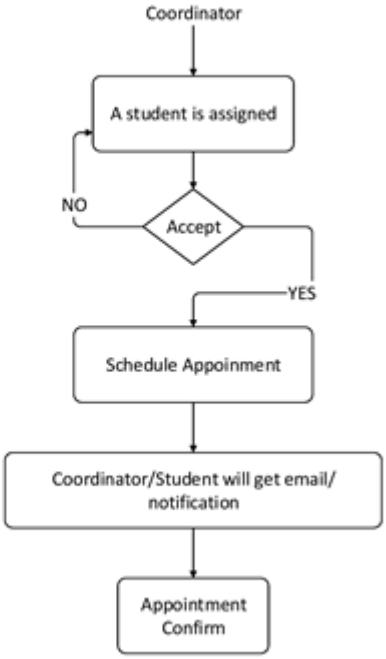
1. Application:



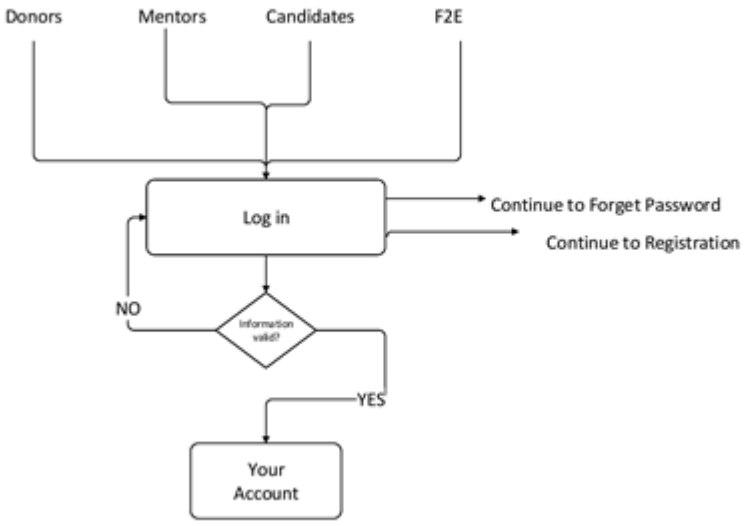
2. Registration



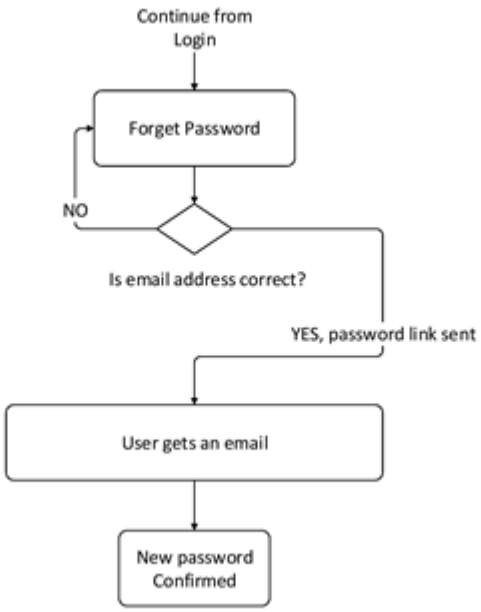
1. Assessment



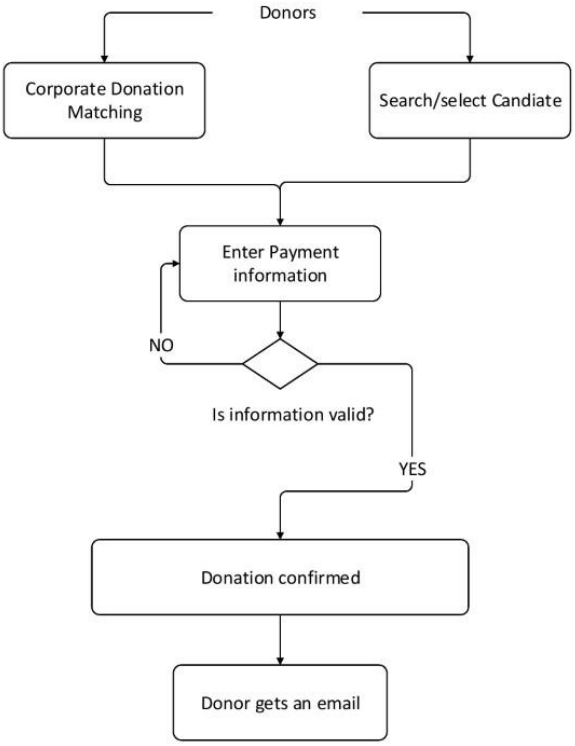
2. Login



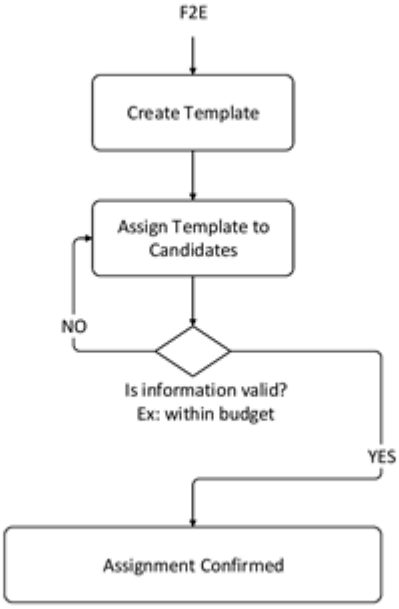
3. Forgot password



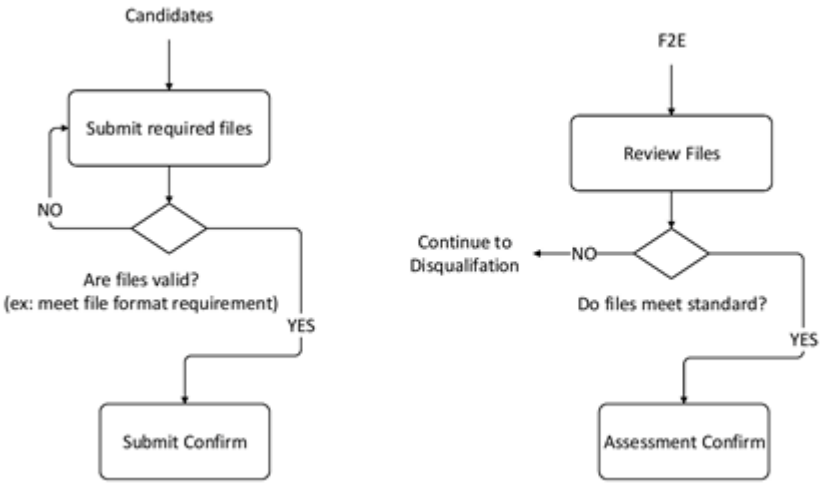
4. Donation



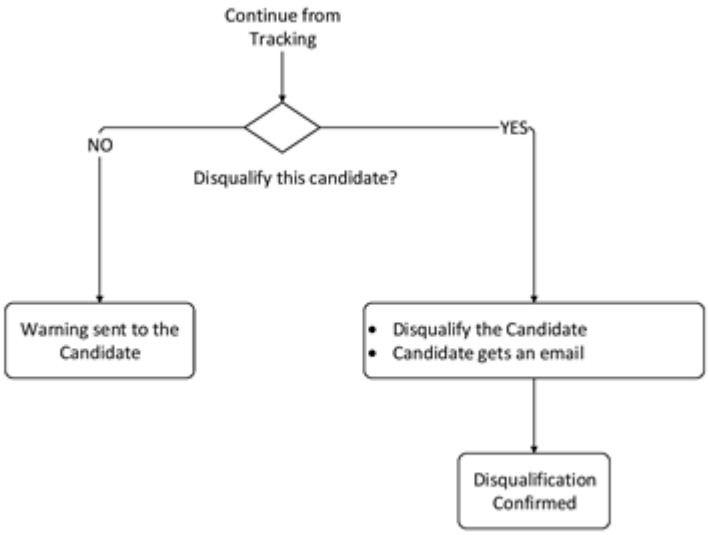
5. Funding



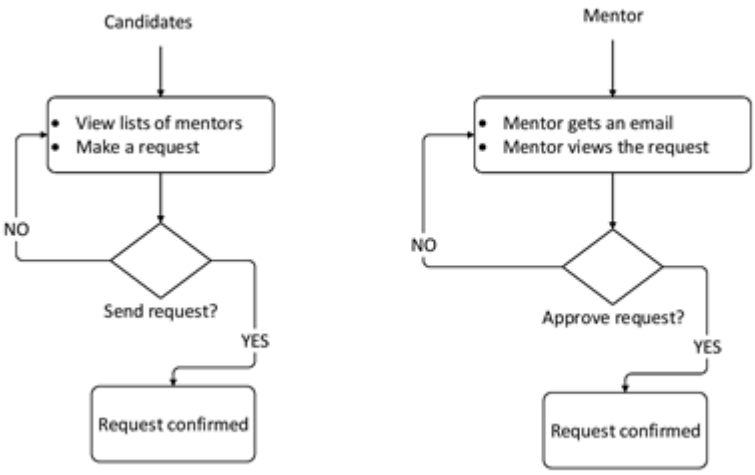
6. Tracking



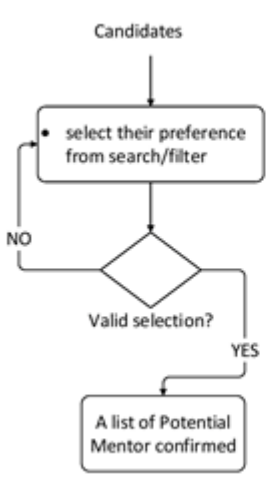
7. Disqualification

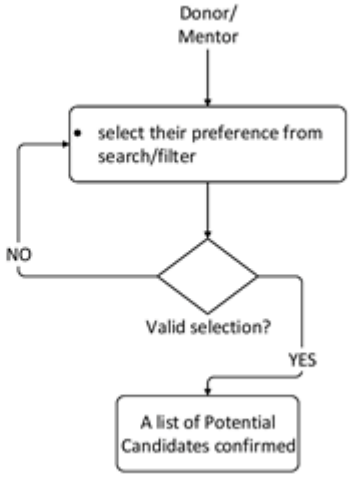


8. Mentorship



9. Matching


Candidates
select their preference from search/filter
NO
Valid selection?
YES
A list of Potential Mentor confirmed

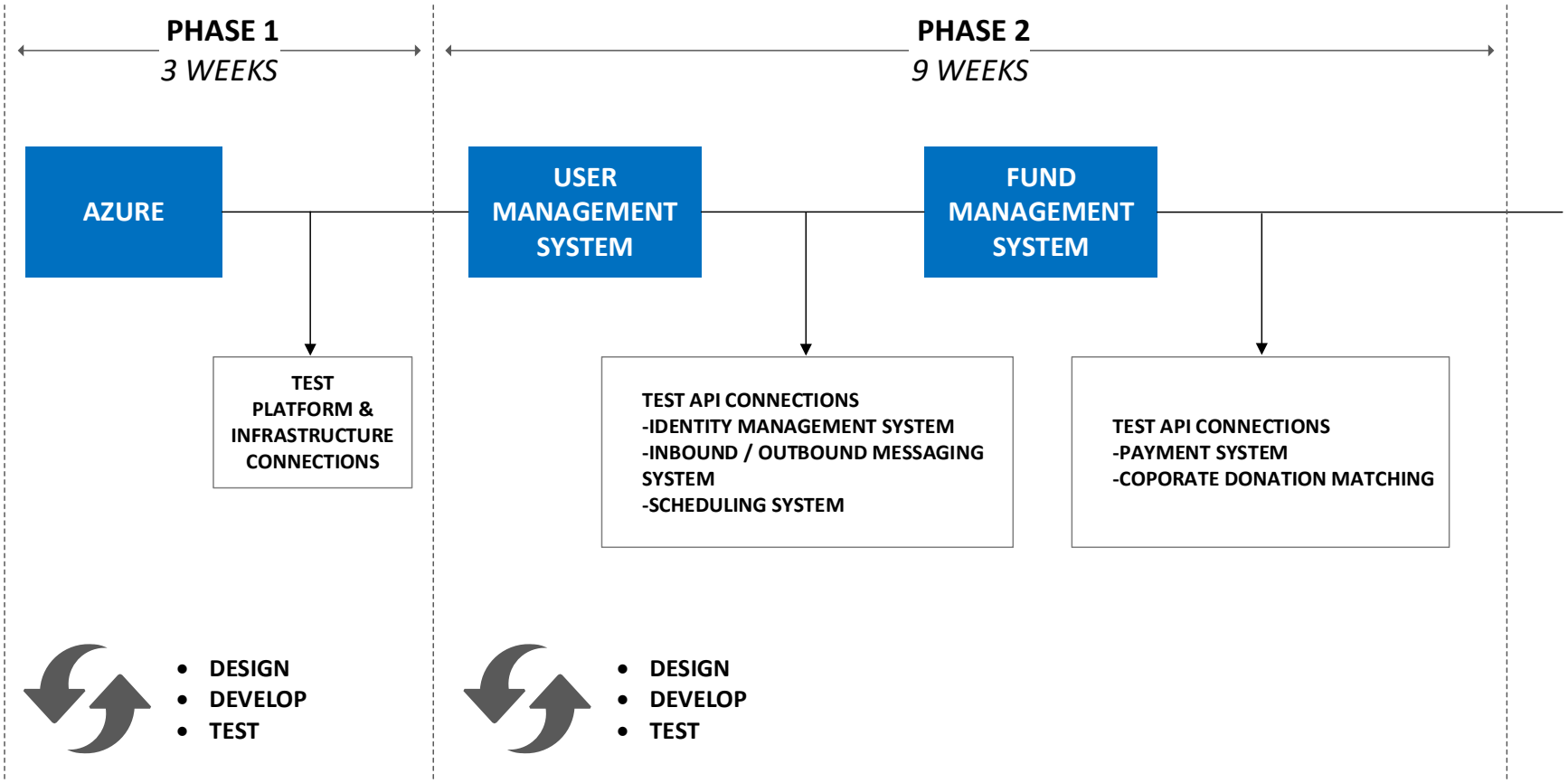

Donor/ Mentor
select their preference from search/filter
NO
Valid selection?
YES
A list of Potential Candidates confirmed

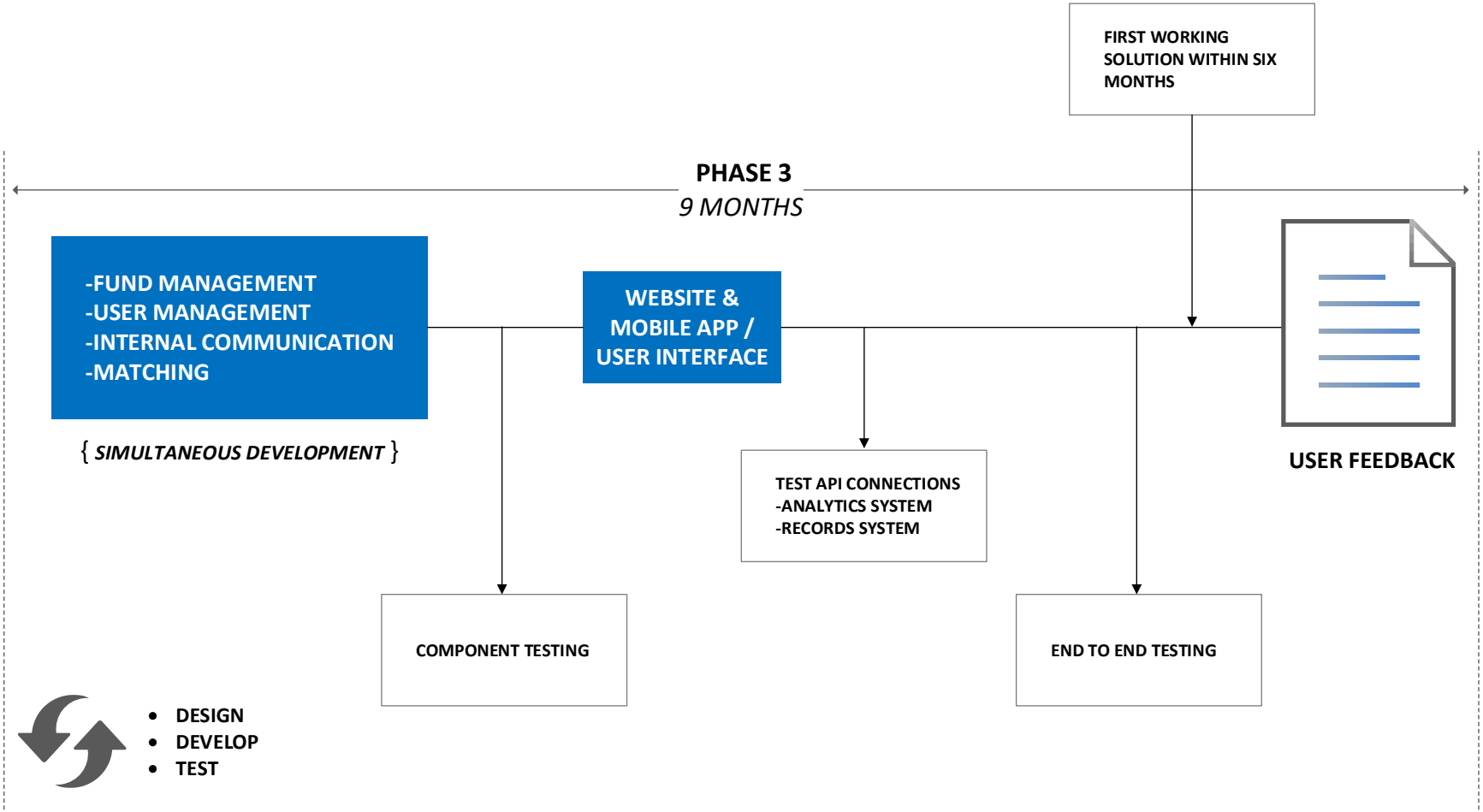
6. Architecture Execution Plan

6.1 Timeline

Our execution of this solution will start out with setting up the Azure components, testing the connections and making sure each cloud component properly communicates with the other, this stage will be completed within 3 weeks. We will then build out the foundations of the main components to be built i.e. the User management and Fund management system, we will also connect a few of the external software's at this stage. We will test the connection to external API's to ensure that the basics of the communication is established. This stage will be completed within 9 weeks.

The final stage of the execution will take 9 Months. Emphasis will be placed on iteration and simultaneous development. It will involve the fleshing out of the core functionalities of the system as well as testing the components. At this stage of the execution we will might engage the services of more developers and testers. The website and mobile app user interface will also be built in this stage. The first working solution will be made available within the first six months of the execution. End to end testing will be carried out and the solution will be rolled out to a few users so as to get user feedback. Phase 3 will be iterated until the solution is deemed satisfactory for release.


PHASE 1
3 WEEKS
PHASE 2
9 WEEKS
AZURE
USER MANAGEMENT SYSTEM
FUND MANAGEMENT SYSTEM
TEST PLATFORM & INFRASTRUCTURE CONNECTIONS
TEST API CONNECTIONS
-IDENTITY MANAGEMENT SYSTEM
-INBOUND / OUTBOUND MESSAGING SYSTEM
-SCHEDULING SYSTEM
TEST API CONNECTIONS
-PAYMENT SYSTEM
-COPORATE DONATION MATCHING
DESIGN
DEVELOP
TEST
DESIGN
DEVELOP
TEST


FIRST WORKING SOLUTION WITHIN SIX MONTHS
PHASE 3
9 MONTHS
-FUND MANAGEMENT
-USER MANAGEMENT
-INTERNAL COMMUNICATION
-MATCHING
{ SIMULTANEOUS DEVELOPMENT }
WEBSITE & MOBILE APP / USER INTERFACE
USER FEEDBACK
TEST API CONNECTIONS
-ANALYTICS SYSTEM
-RECORDS SYSTEM
COMPONENT TESTING
END TO END TESTING
DESIGN
DEVELOP
TEST

7. Glossary

Term	Description
VM	Virtual Machine, which is an emulation of a computer system

References:

1. https://medium.com/get-ally/how-to-architect-online-payment-processing-system-for-an-online-store-6dc84350a39
2. https://www.webpagefx.com/blog/web-design/online-payment-systems/
3. https://www.pcmag.com/article2/0,2817,2491437,00.asp
4. https://www.owasp.org/index.php/Top_10_2010-Main
5. https://www.encorebusiness.com/blog/power-bi-vs-tableau/
6. https://www.betterbuys.com/bi/microsoft-power-bi-pricing/
7. http://fortune.com/2017/04/24/linkedin-users/
8. https://news.microsoft.com/bythenumbers/outlook-users
9. https://acuityscheduling.com/signup.php#advanced
10. https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool
11. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview
12. https://azuremarketplace.microsoft.com/en-us/marketplace/apps/Microsoft.KeyVault
13. https://calendly.com/pages/integrations
14. https://www.encorebusiness.com/blog/power-bi-vs-tableau/