CyberSentinel

Sprint 1 By Team Tech Titans

Agenda

01 Team & Planning

- Team Roles & Responsibilities
- Improvements Based on Professor Feedback
- Project Description
- Team Working Agreement

02 User & Product Definition

- Personas
- Minimum Viable Product (MVP)

03 Technology & Implementation

- Technologies
- Algorithms

04 Project Documentation & Management

- Diagrams
- Product Backlog
- Sprint 1 Backlog

05 Tracking & Evaluation

- Metrics & Progress Tracking
- Sprint 1 Retrospective
- Sprint 2 Planning

06 Demonstrations & Resources

- Project Demo - Sprint 1
- GitHub Repository Link
- Live Application Demo

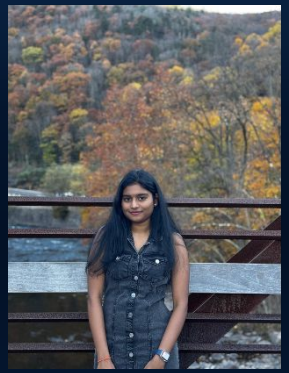
Team Members

Vaishnavi Dasari

Machine learning Engineer

Snehitha Bodiga

Full Stack Developer



Aasritha Bhimisetty

Frontend Developer

Team Members

Abisainath

Backend Developer

Shoib Khan Patan

Backend Developer

Dhanush Kolapalli

Machine Learning Engineer

Team Members

Neelkamal Rana

Full Stack Developer

Improvements

- Addition of Team page
- Fixing the wikipage.
- Fixing up the team agreement.

Project Description

Project Name:	CyberSentinel
Team:	Tech Titans
Project Description:	For individuals and enterprises who need protection against cyber threats, the CyberSentinel platform is a real-time AI-driven cybersecurity solution that detects and prevents phishing attacks, fraudulent transactions, and identity theft using advanced machine learning, behavioral analytics, and cloud-based threat intelligence. Unlike traditional security measures that struggle to detect sophisticated attack vectors, our application employs AI-powered risk assessment, real-time email scrutiny, transactional anomaly detection, and intelligent web link verification—continuously adapting to emerging threats to provide proactive and highly sophisticated cybersecurity defenses.
Benefit Outcomes:	• Real-time detection and prevention of cyber threats, including phishing and fraudulent transactions. • Adaptive learning capabilities to counter evolving attack techniques. • Seamless integration of automation and analytics for efficient and proactive cybersecurity. • User-friendly and intuitive design, making cybersecurity accessible for individuals and businesses.
Github Link:	https://github.com/htmw/2025S-Tech-Titans/wiki

Team Agreement

TEAM AGREEMENT

Communication:

- The team will use **Zoom and WhatsApp** as primary communication channels.
- **Google Docs** will serve as a platform for collaborative document editing, resource sharing, and note-taking during discussions.
- **Weekly Zoom meetings** will be scheduled to review progress, discuss roadblocks, and align on next steps. Additional meetings may be scheduled as needed.
- Team members should inform the group in advance if they are unable to attend a scheduled Zoom meeting.
- Regular updates on task progress are expected, and any challenges or delays should be promptly communicated to the team.
- Active participation is encouraged, with members providing constructive feedback and support when necessary.
- Discussions should be **focused**, with members listening attentively, speaking clearly, and staying on topic to prevent misunderstandings.
- All assigned work must be completed before the deadline. If any difficulties arise, members should reach out for assistance as early as possible to prevent disruptions to the project timeline.

Professionalism:

- Team interactions will be conducted with **mutual respect**, valuing diverse perspectives and contributions.
- Feedback should remain **constructive**, focusing on the project rather than personal attributes.
- If a team member disagrees with a decision, they may request a discussion in the next meeting for reconsideration.
- The team strives to maintain an **inclusive and supportive environment** where all members feel comfortable expressing their ideas.
- Any conflicts should be addressed **respectfully and transparently** within the team. If an agreement cannot be reached internally, the matter will be escalated to the professor for guidance.

Meeting Cadence:

- **Primary Meeting:** Weekly Zoom meeting to discuss progress, challenges, and next steps.
- **Check-ins:** Mid-week asynchronous updates via WhatsApp to ensure task alignment.
- **Ad-hoc Meetings:** Additional meetings scheduled as needed for urgent discussions or blockers.

Team Members:

- **Dasari Vaishnavi**
- **Snehitha Bodiga**
- **Arepalli Abisainath Reddy**
- **Shoaib Khan Patan**
- **Aasritha Bhimisetty**
- **Kolapalli Dhanush**
- **Rana Neelkamal**

Persona

Name: Alex Johnson
Age: 32
Occupation: Software Developer

Alex works at a mid-sized tech company and is well-versed in various technologies. Spends considerable time online, both professionally and personally. Aware of cybersecurity threats but seeks advanced tools to enhance personal security.

Goals:

- Protect personal and professional data from phishing and other cyber threats.
- Stay informed about the latest cybersecurity practices.
- Utilize AI-driven solutions for proactive threat detection.

Challenges:

- Balancing convenience with robust security measures.
- Identifying trustworthy cybersecurity tools amidst numerous options.

Persona

Name: Maria Thompson
Age: 40
Occupation: Project Manager

Manages a team remotely for a marketing firm. Juggles professional responsibilities with parenting two teenagers. Uses multiple devices for work and personal tasks.

Goals:

- Ensure the security of sensitive work-related information.

- Protect family members, especially children, from online threats.

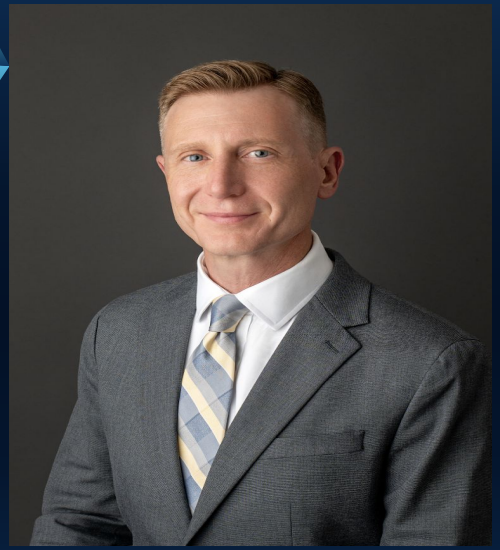
- Maintain a secure digital environment across all devices.

Challenges:

- Limited time to manage and monitor cybersecurity measures.

- Keeping up with evolving cyber threats and ensuring family compliance with best practices.

Persona



Name: David Kim
Age: 45
Occupation: Owner of a local retail store

Runs an online storefront in addition to the physical store. Handles customer data, including payment information. Has basic knowledge of cybersecurity but lacks specialized expertise.

Goals:

- Protect customer data to maintain trust and comply with regulations.

- Prevent financial losses due to cyber attacks.

- Implement cost-effective security solutions without extensive technical knowledge.

Challenges:

- Limited budget for cybersecurity investments.

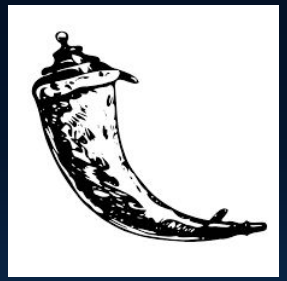
- Difficulty in assessing which security measures are necessary and effective.

Minimum Viable Product (MVP)

- Phishing Email Detection – Classifies emails as safe or phishing using NLP models trained on datasets.
- Fraudulent Transaction Detection – Identifies suspicious transactions using anomaly detection techniques.
- URL Classification – Determines if a website link is malicious or safe based on its lexical features.
- User Dashboard – Displays alerts and risk analysis based on detect threats.

Technologies - Development Stack

- **Frontend:** React.js (for simple and interactive UI)
- **Backend:** Flask (lightweight Python-based API)
- **Database:** PostgreSQL (to store detected threat data)
- **Hosting:** AWS (for cloud deployment and scalability)



Technologies – AI & Cybersecurity Tools

- **Machine Learning:** Scikit-learn, PyTorch (for phishing and fraud detection)
- **Security:** OAuth 2.0 (for authentication), OpenCV (for URL analysis)
- **Threat Detection Models:** NLP-based phishing email classification, anomaly detection for fraudulent transactions, and URL classification algorithms

Algorithms

Phishing Email Detection:

Algorithm: BERT (Bidirectional Encoder Representations from Transformers)

- Utilizes a **pre-trained deep learning model** for **text classification**.
- **Captures contextual meaning** of words, improving phishing email detection.
- **Fine-tuned** on phishing email datasets for high accuracy.

Fraudulent Transaction Detection:

Algorithm: Autoencoder with Isolation Forest

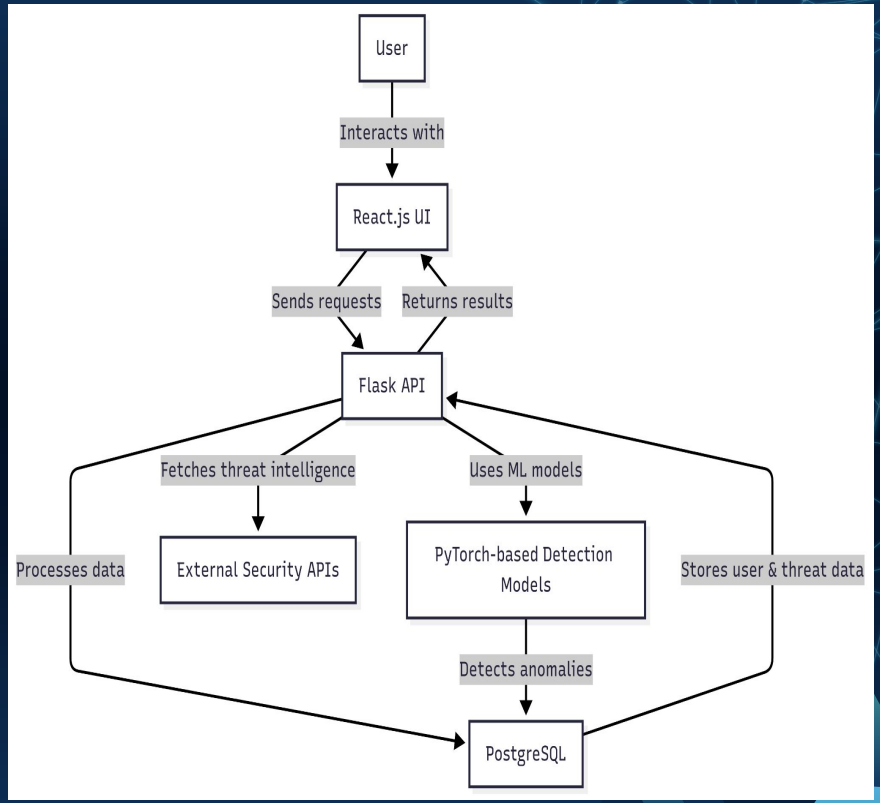
- **Autoencoder** reduces dimensionality and extracts essential transaction features.
- **Isolation Forest** detects anomalies based on learned representations.
- Efficient for **unsupervised learning**, detecting fraud without requiring labeled data.

URL Classification:

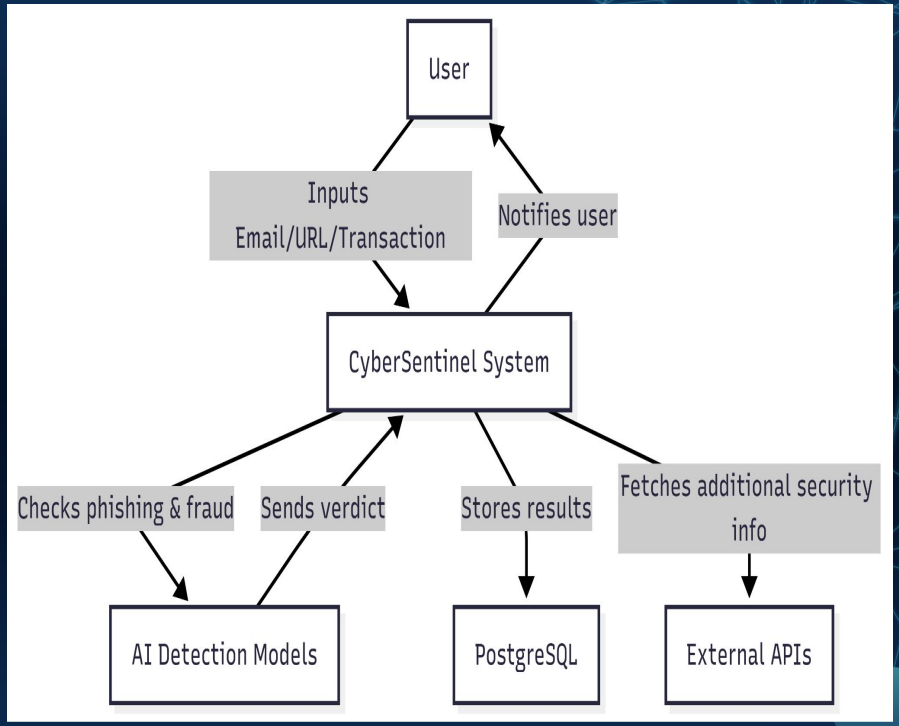
Algorithm: CNN + LSTM (Convolutional Neural Network + Long Short-Term Memory)

- **CNN extracts spatial features** from URL structure.
- **LSTM captures sequential patterns**, improving detection of phishing URLs.
- **Hybrid deep learning model** for better performance over traditional classifiers.

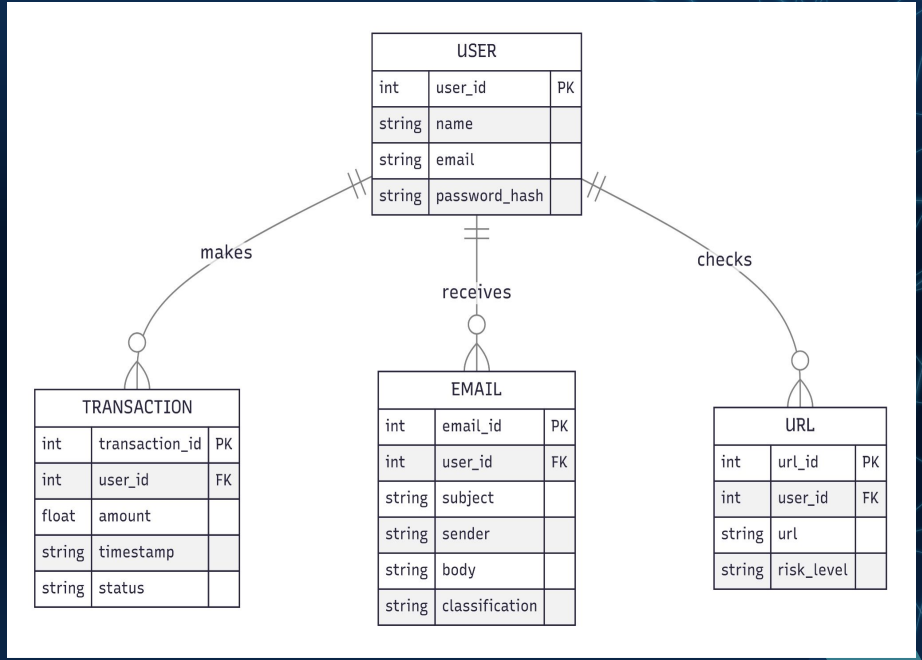
Architecture Diagram



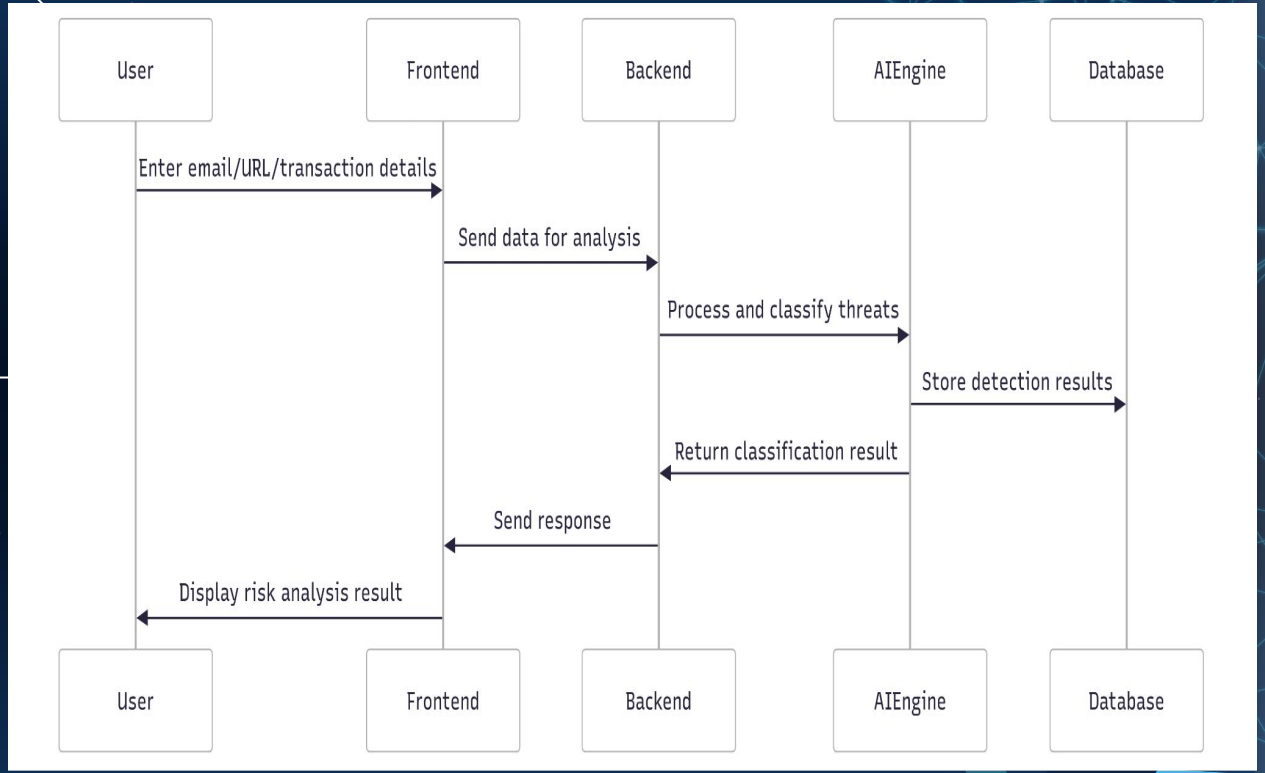
Context Diagram



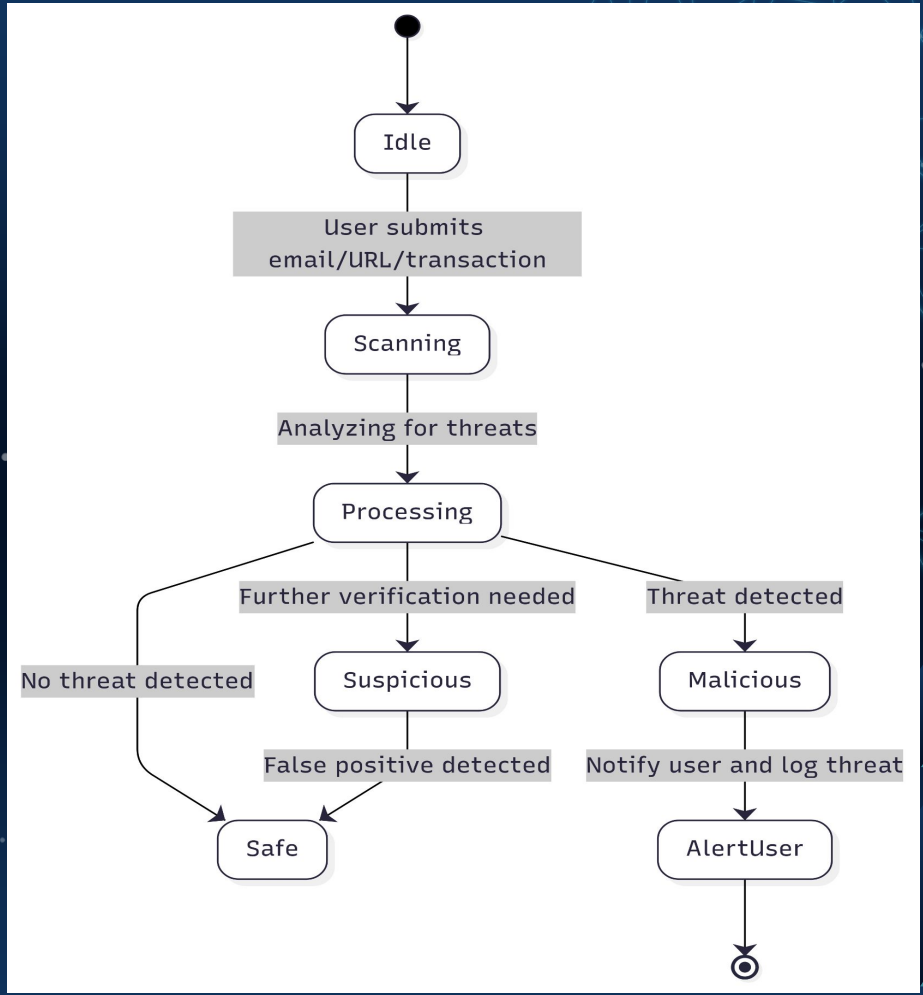
ER Diagram


USER
int user_id PK
string name
string email
string password_hash
makes
receives
checks
TRANSACTION
int transaction_id PK
int user_id FK
float amount
string timestamp
string status
EMAIL
int email_id PK
int user_id FK
string subject
string sender
string body
string classification
URL
int url_id PK
int user_id FK
string url
string risk_level

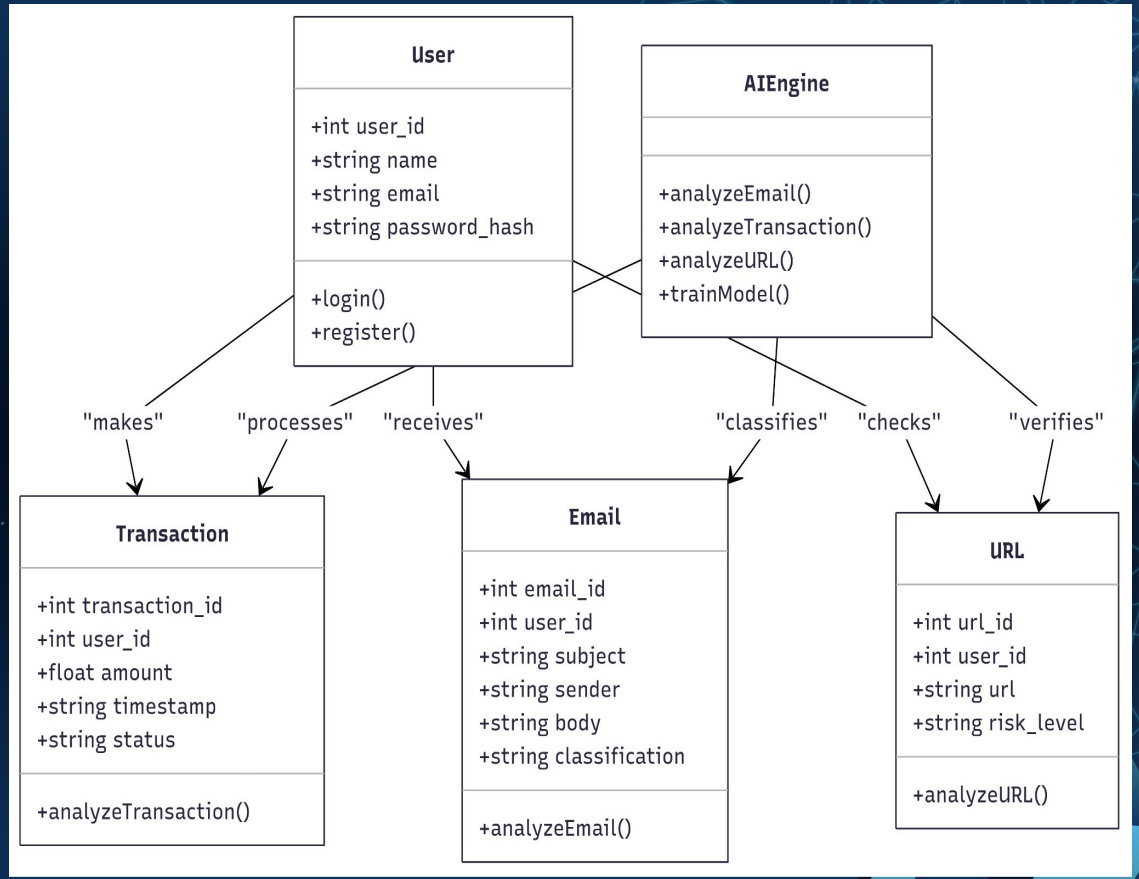
Sequence Diagram



State Diagram



Class Diagram



Product Backlog – User Stories

ID	User Story	Acceptance Criteria	Feature	Sprint	Story Points
US_01	As a user, I want a dashboard to view phishing email history so that I can track past threats.	Dashboard displays list of phishing emails with filtering options.	Dashboard & Reporting	Sprint 1	5
US_02	As a user, I want to filter emails based on risk level so that I can quickly identify dangerous emails.	System allows filtering by safe, suspicious, and phishing categories.	Phishing Email Filtering	Sprint 1	3
US_03	As an admin, I want to view statistics on detected threats so that I can analyze system performance.	Dashboard provides statistics on phishing, fraud, and malicious URLs.	Threat Statistics	Sprint 1	8
US_04	As an admin, I want to manage user roles and permissions so that I can control access levels.	System supports different access levels for users and admins.	User Management	Sprint 1	8
US_05	As a user, I want to upload an email for phishing detection so that I can know if it's safe.	System classifies email as safe, suspicious, or phishing with an alert.	Phishing Email Detection	Sprint 2	8

Product Backlog – User Stories

ID	User Story	Acceptance Criteria	Feature	Sprint	Story Points
US_06	As a user, I want to upload transaction data so that I can detect fraudulent activities.	System flags transaction as normal or suspicious with a confidence score.	Fraudulent Transaction Detection	Sprint 2	13
US_07	As a user, I want to check if a URL is malicious so that I can avoid phishing sites.	System checks URL structure and domain reputation, classifying it as safe, suspicious, or malicious.	URL Classification	Sprint 2	5
US_08	As a user, I want to verify if a sender email is trustworthy so that I can decide whether to engage with the sender.	System checks sender reputation and displays a trust score.	Sender Reputation Check	Sprint 2	8
US_09	As a user, I want to receive real-time alerts for detected threats so that I can take immediate action.	User receives notifications via email or app for detected threats.	Real-time Alerts	Sprint 3	8
US_10	As a user, I want an option to report a false positive classification so that I can help improve detection accuracy.	Users can flag an incorrect detection for review.	User Feedback System	Sprint 3	3

Product Backlog – Technical Stories

ID	Technical Story	Acceptance Criteria	Feature	Sprint	Story Points
TS_01	Create a dashboard for threat statistics so that admins can monitor system performance.	Dashboard displays data on detected threats.	Threat Statistics	Sprint 1	8
TS_02	Design a user role management system so that access levels can be controlled efficiently.	Admins can assign permissions to different user roles.	User Management	Sprint 1	8
TS_03	Implement OAuth authentication for secure user access so that users can log in securely.	User authentication is secure, and access tokens work correctly.	Security & Authentication	Sprint 1	5
TS_04	Set up AWS for cloud deployment so that the system can be scalable and accessible.	Backend deployed and accessible via API.	Cloud Deployment	Sprint 1	5
TS_05	Integrate BERT model for phishing email detection so that emails can be classified accurately.	Model achieves at least 90% accuracy on test data.	AI Model Training	Sprint 2	8

Product Backlog – Technical Stories

ID	Technical Story	Acceptance Criteria	Feature	Sprint	Story Points
TS_06	Implement Autoencoder + Isolation Forest for fraud detection so that anomalies in transactions can be detected.	Model correctly classifies anomalies in dataset.	AI Model Training	Sprint 2	13
TS_07	Deploy CNN + LSTM model for URL detection so that phishing websites can be identified.	Model classifies URLs with at least 85% accuracy.	AI Model Training	Sprint 2	8
TS_08	Implement email sender verification model so that sender reputation can be assessed.	System provides a sender trust score based on reputation.	Sender Reputation Check	Sprint 2	5
TS_09	Develop a notification system for real-time alerts so that users are informed of potential threats.	Users receive accurate notifications for detected threats.	Notification System	Sprint 3	8
TS_10	Develop a feedback mechanism for false positive reports so that the system can improve over time.	Users can flag and submit incorrect classifications for review.	User Feedback System	Sprint 3	3

Sprint 1 Backlog

ID	User Story	Acceptance Criteria	Feature	Story Points
US_01	As a user, I want a dashboard to view phishing email history so that I can track past threats.	Dashboard displays list of phishing emails with filtering options.	Dashboard & Reporting	5
US_02	As a user, I want to filter emails based on risk level so that I can quickly identify dangerous emails.	System allows filtering by safe, suspicious, and phishing categories.	Phishing Email Filtering	3
US_03	As an admin, I want to view statistics on detected threats so that I can analyze system performance.	Dashboard provides statistics on phishing, fraud, and malicious URLs.	Threat Statistics	8
US_04	As an admin, I want to manage user roles and permissions so that I can control access levels.	System supports different access levels for users and admins.	User Management	8
TS_01	Create a dashboard for threat statistics so that admins can monitor system performance.	Dashboard displays data on detected threats.	Threat Statistics	8

Sprint 1 Backlog

ID	User Story	Acceptance Criteria	Feature	Story Points
TS_02	Design a user role management system so that access levels can be controlled efficiently.	Admins can assign permissions to different user roles.	User Management	8
TS_03	Implement OAuth authentication for secure user access so that users can log in securely.	User authentication is secure, and access tokens work correctly.	Security & Authentication	5
TS_04	Set up AWS for cloud deployment so that the system can be scalable and accessible.	Backend deployed and accessible via API.	Cloud Deployment	5

Test Cases Sprint 1

Story ID	Test Case	Expected Outcome	Actual Outcome	Pass/Fail
US_01	Verify that the dashboard displays a list of phishing emails.	Emails are displayed with filtering options.	Emails displayed, filtering working correctly.	Pass
US_02	Test email filtering by risk level (safe, suspicious, phishing).	Emails are categorized correctly based on risk.	Emails categorized correctly.	Pass
US_03	Verify that statistics on phishing, fraud, and malicious URLs are displayed correctly.	Statistics are accurate and match the database records.	Statistics displayed correctly.	Pass
US_04	Test user role management to ensure different permissions apply correctly.	Users with different roles have the correct access.	Role-based access not working as expected.	Fail

Test Cases Sprint 1

Story ID	Test Case	Expected Outcome	Actual Outcome	Pass/Fail
TS_01	Validate that the dashboard correctly retrieves and displays threat statistics.	Data loads correctly without errors.	Dashboard loads data correctly.	Pass
TS_02	Verify that admins can create, modify, and delete user roles.	Role-based access control works as expected.	Role modifications failing due to permission errors.	Pass
TS_03	Test OAuth login to confirm secure authentication and token generation.	Users can log in securely and receive valid tokens.	Authentication failing, token issue detected.	Fail
TS_04	Verify AWS deployment accessibility.	The system is deployed and can be accessed via API.	Deployment unsuccessful, API inaccessible.	Pass

Sprint 1 Stories Completed

ID	User Story / Task	Story Points
US_01	As a user, I want a dashboard to view phishing email history so that I can track past threats.	5
US_02	As a user, I want to filter emails based on risk level so that I can quickly identify dangerous emails.	3
US_03	As an admin, I want to view statistics on detected threats so that I can analyze system performance.	8
TS_01	Create a dashboard for threat statistics so that admins can monitor system performance.	8
TS_02	Design a user role management system so that access levels can be controlled efficiently.	8
TS_04	Set up AWS for cloud deployment so that the system can be scalable and accessible.	5

Total Completed Story Points: 37

Sprint 1 Stories Not Completed

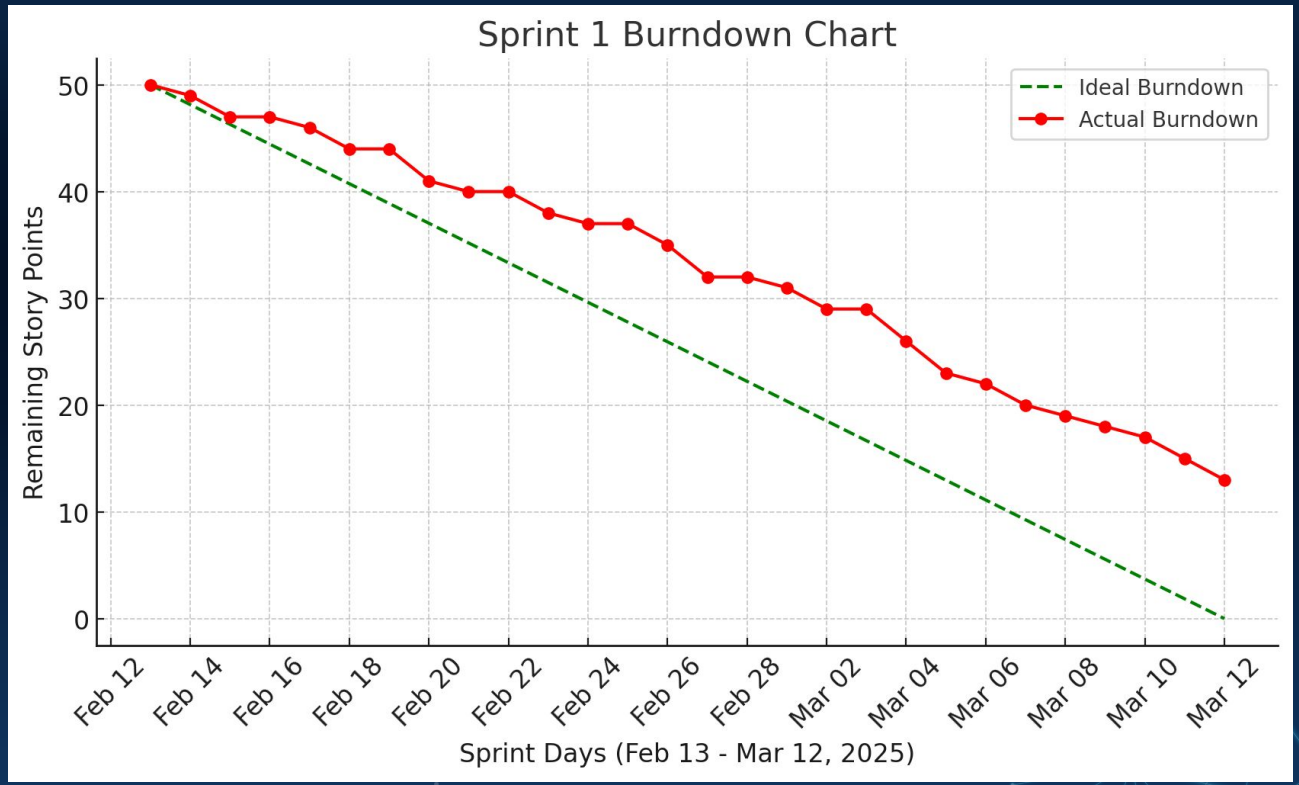
ID	User Story / Task	Story Points
US_04	As an admin, I want to manage user roles and permissions so that I can control access levels.	8
TS_03	Implement OAuth authentication for secure user access so that users can log in securely.	5

Total Not Completed Story Points: 13

Team Velocity

Total Story Points Completed: 37

Burn Down Chart



Completed/Committed Ratio

Committed Story Points

Completed Story Points

Completed/Committed Ratio

Retrospective

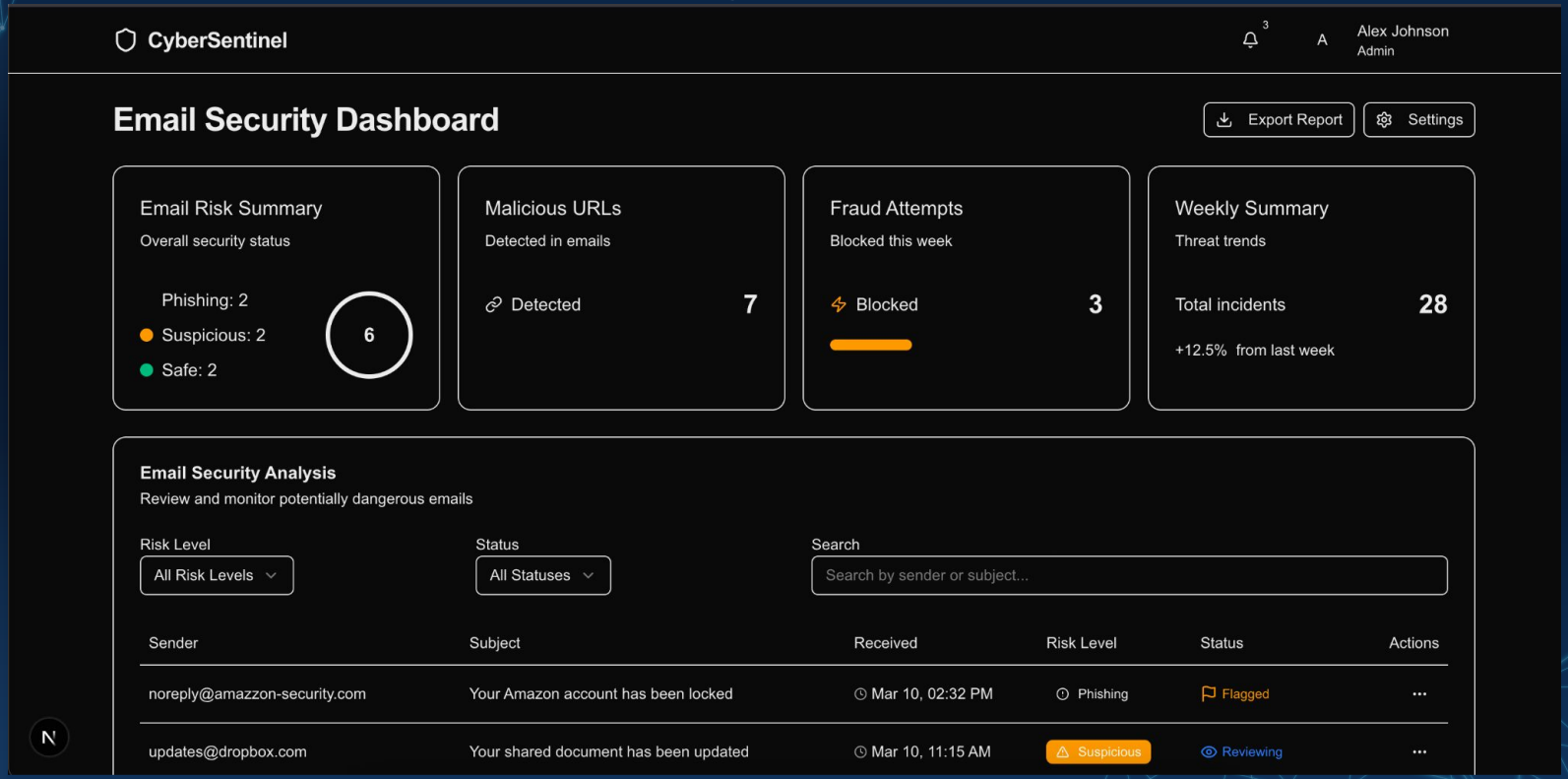
Sprint 2 Planning

ID	User Story / Task	Acceptance Criteria	Feature	Story Points
US_04	As an admin, I want to manage user roles and permissions so that I can control access levels.	System supports different access levels for users and admins.	User Management	8
TS_03	Implement OAuth authentication for secure user access so that users can log in securely.	User authentication is secure, and access tokens work correctly.	Security & Authentication	5
US_05	As a user, I want to upload an email for phishing detection so that I can know if it's safe.	System classifies email as safe, suspicious, or phishing with an alert.	Phishing Email Detection	8
US_06	As a user, I want to upload transaction data so that I can detect fraudulent activities.	System flags transaction as normal or suspicious with a confidence score.	Fraudulent Transaction Detection	13
US_07	As a user, I want to check if a URL is malicious so that I can avoid phishing sites.	System checks URL structure and domain reputation, classifying it as safe, suspicious, or malicious.	URL Classification	5

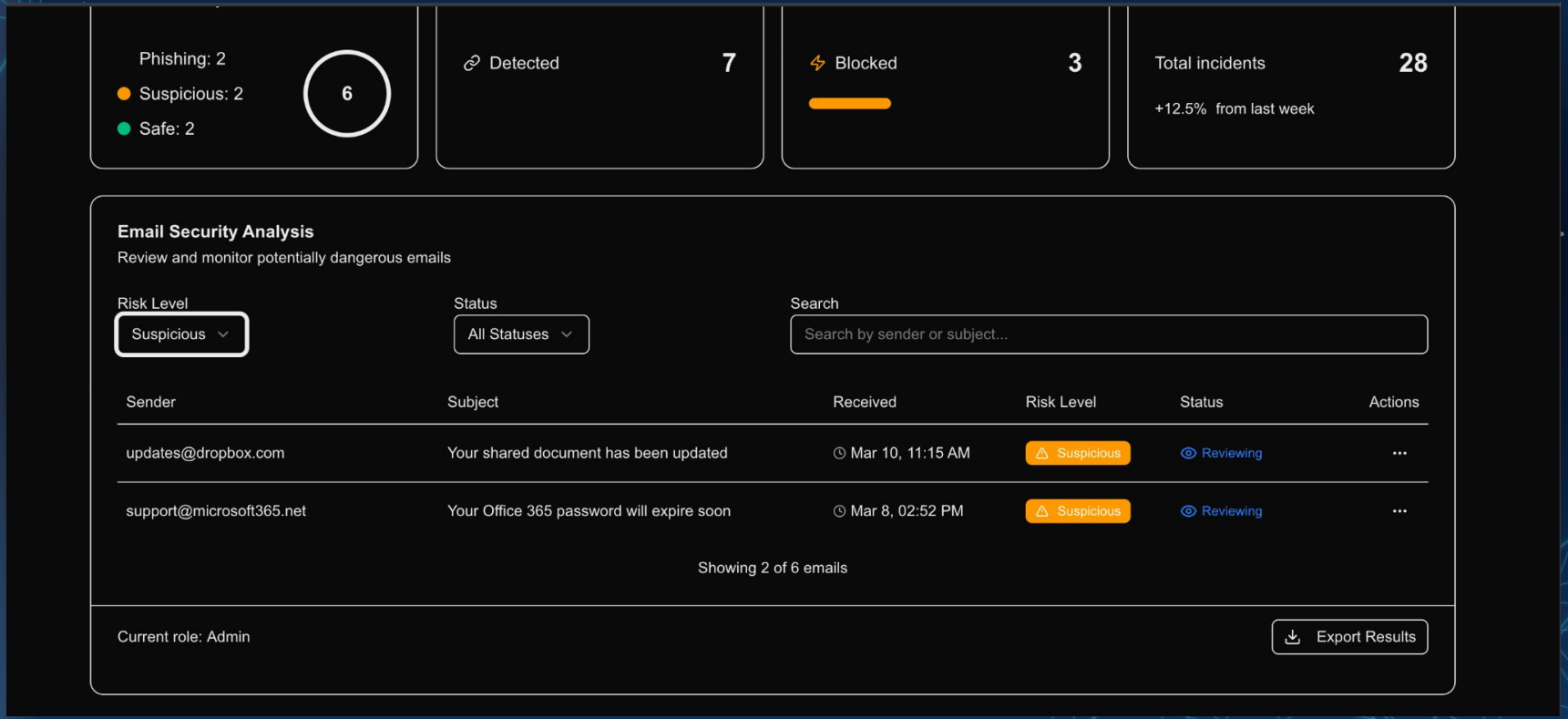
Sprint 2 Planning

ID	User Story / Task	Acceptance Criteria	Feature	Story Points
US_08	As a user, I want to verify if a sender email is trustworthy so that I can decide whether to engage with the sender.	System checks sender reputation and displays a trust score.	Sender Reputation Check	8
TS_05	Integrate BERT model for phishing email detection so that emails can be classified accurately.	Model achieves at least 90% accuracy on test data.	AI Model Training	8
TS_06	Implement Autoencoder + Isolation Forest for fraud detection so that anomalies in transactions can be detected.	Model correctly classifies anomalies in dataset.	AI Model Training	13
TS_07	Deploy CNN + LSTM model for URL detection so that phishing websites can be identified.	Model classifies URLs with at least 85% accuracy.	AI Model Training	8

Application Screenshots



Application Screenshots



Github Wikipage Link

https://github.com/htmw/2025S-Tech-Titans/wiki

Application Demo

Thank You