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
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
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
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