System Design Document

For

Analysis Tool for Commercially Available Cybersecurity AI Tools

Nicolas Rodriguez, Jeremiah Webb, Olivia Meholic, Sarah Gleixner, Joseph Alesandrini, Troy Neubauer

Version/Author	*Date*
V1.0/Nicolas Rodriguez, Jeremiah Webb, Olivia Meholic, Sarah Gleixner, Joseph Alesandrini	*29SEP2023*
V2.0/Nicolas Rodriguez, Jeremiah Webb, Olivia Meholic, Sarah Gleixner, Joseph Alesandrini	*31OCT2023*
V3.0/Nicolas Rodriguez, Jeremiah Webb, Olivia Meholic, Sarah Gleixner, Joseph Alesandrini	*21NOV2023*
V4.0/Nicolas Rodriguez, Jeremiah Webb, Olivia Meholic, Sarah Gleixner, Joseph Alesandrini, Troy Neubauer	*05FEB2024*
V5.0/Nicolas Rodriguez, Jeremiah Webb, Olivia Meholic, Sarah Gleixner, Joseph Alesandrini, Troy Neubauer	*03MAR2024*
V6.0/Nicolas Rodriguez, Jeremiah Webb, Olivia Meholic, Sarah Gleixner, Joseph Alesandrini, Troy Neubauer	*14APR2024*

TABLE OF CONTENTS

SYSTEM DESIGN DOCUMENT

1 INTRODUCTION

1.1 Purpose And Scope

This document is designed to provide clear and concise technical guidance to the development team, ensuring consistency and alignment with the envisioned solution. Furthermore, it aids in facilitating communication among our product owner, enabling reviews, feedback, and ensuring that the software built aligns with the initial design objectives.

1.2 Project Executive Summary

This section provides an overview of Cybertool, a public website that will enable users to filter through a variety of cybersecurity tools depending on the needs of the user (commercial, personal, etc.). This website will be hosted on an Amazon Web Services (AWS) server including all necessary architecture for the product. Among this architecture, there will be a database containing the cybersecurity products and the key values that were determined during research of said products. Recommendations will be generated from the database based on user preferences/requirements. Upon user request, a comparative report will be generated containing prospective tools and/or tools they already have.

1.3 System Overview

Figure 1 describes a use case overview of the web application, named 'CyberTool WebApp', that interacts with various services in the AWS Cloud. The Figure illustrates how different types of users (Guests and Authenticated Users) interact with the system and the actions they can perform. Guests can retrieve web resources like HTML, CSS, JS, and images, and have the option to sign up. Once authenticated, users can manage a saved list of security tools, query for tools, complete a questionnaire, and request reports. The AWS Cloud side shows services such as CloudFront for content delivery, Cognito for user authentication, API Gateway for creating RESTful services, DynamoDB for database storage, and Simple Storage Service (S3) for file storage. The processes include retrieving the latest web files, running queries to return results, storing report URLs, authorizing pre-signed URLs, and creating reports.

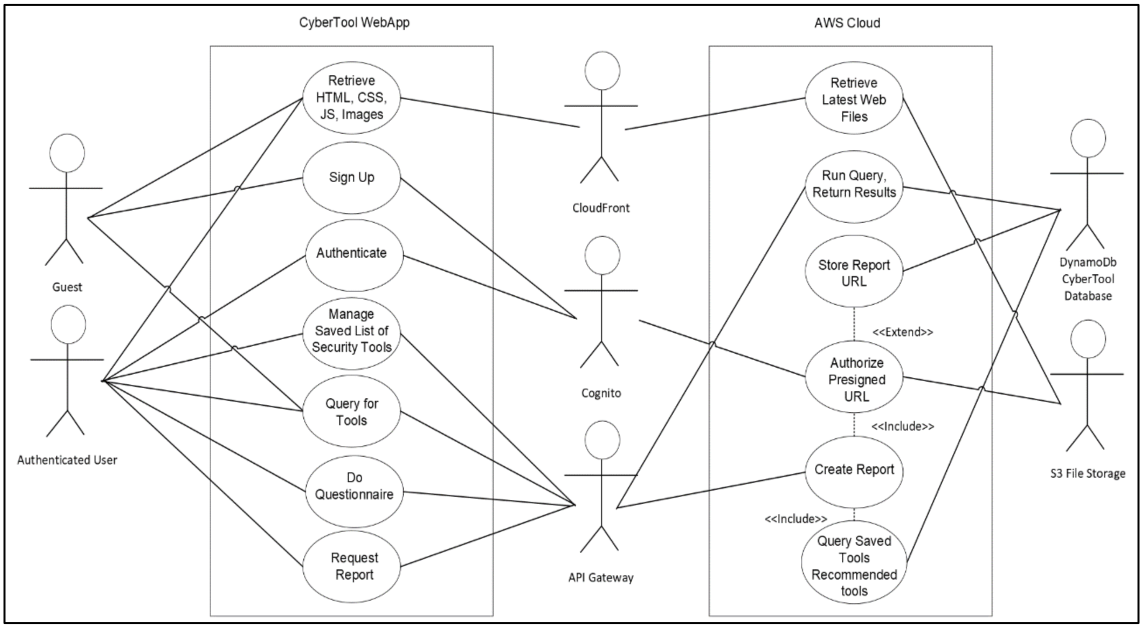


Figure 1: CyberTool Use Case Diagram

1.4 Design Constraints

Design constraints of CyberTool include hosting, currently the cybertoolsusa domain is on rent for 1 year. Time constraint of the CS 491 course forces CyberTool to be developed over 2 semesters. CyberTool is dependent on the AWS service eco system to function and relies on AWS servers. Some design constraints for security include exposing HTTP endpoints. Furthermore, due to the small development team, the number of tools available in DynamoDb will be limited.

1.5 Future Contingencies

This system architecture is based upon the AWS hosting platform with its many integrated services. The success of the project depends on the successful flow of data between these integrated services; however, problems could arise due to differences in data types and individual system configurations. These issues can be resolved through a series of overall system inspections and refinements.

1.6 Document Organization

The Systems Design Document is intended to provide an overview of the system design. This documents reviews both the hardware and software for the System Architecture, its Human Machine Interface, both hardware and software Detailed Design, any External Interfaces being used, and System Integrity Controls implemented throughout.

1.7 Project References

Amazon Web Services Documentation, from https://docs.aws.amazon.com/

1.8 Glossary

AI – Artificial Intelligence
A field of computer science focused on developing intelligent machines that perform tasks requiring human intelligence, using techniques like machine learning and natural language processing.

AWS – Amazon Web Services
Cloud computing platform by Amazon, providing a wide array of infrastructure services like computing power, storage options, and networking capabilities, available on a pay-as-you-go basis.

CIAM – Amazon Cognito Customer Identity and Access Management
Amazon Cognito aligns with CIAM objectives by providing authentication, authorization, and user management for web and mobile applications, supporting sign-in through both user pools and third parties.

IAM – Identity and Access Management
An AWS service that secures control over access to AWS resources, enabling management of users, groups, and permissions to ensure that only authenticated and authorized entities can access specified resources.

JWT – JSON Web Token
A compact, URL-safe means of representing claims to be transferred between two parties. The claims in a JWT are encoded as a JSON object that is used as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web Encryption (JWE) structure, enabling the claims to be digitally signed or integrity-protected with a Message Authentication Code (MAC) and/or encrypted.

LLM – Large Language Model
A type of artificial intelligence model designed to understand, generate, and interpret human language by analyzing vast amounts of text data, capable of supporting tasks like translation, question answering, and content creation.

OU - Organization Unit
An AWS service that secures control over access to AWS resources, enabling management of users, groups, and permissions to ensure that only authenticated and authorized entities can access specified resources.

RBAC – Role-based Access Control
Implemented through IAM roles in AWS, RBAC allows assignment of permissions based on the roles within an organization, enabling entities to perform actions according to their roles without assigning permissions to individual users directly.

SCP - Service Control Policy
Policies within AWS Organizations that offer centralized control over permissions for all accounts, allowing administrators to enforce compliance and management policies across the organization.

SSE – Server-Side Encryption
An encryption service in AWS that protects data at rest by encrypting it on the server before storage, with options for managing encryption keys via AWS managed keys, customer master keys in AWS Key Management Service, or customer-provided keys.

UUIDv4 – Universally Unique Identifier
A Version 4 UUID is a universally unique identifier that is generated using random numbers.

Vector Embedding
A method of transforming objects, such as words, images, or items, into numerical vectors in a high-dimensional space, enabling mathematical operations and comparisons that capture semantic or contextual similarities.

WAF – Web Application Firewall
A security service in AWS that protects web applications from common web exploits and vulnerabilities by filtering and monitoring HTTP traffic between the application and the Internet.

2 SYSTEM ARCHITECTURE

This section describes an overview of the hardware and software architecture for the CyberTool system and subsystems.

2.1 System Software Architecture

- The CyberTool system takes advantage of multiple programming languages for specific use cases.
- The CyberTool web client will be written in JavaScript using the React Framework.
- Functions in AWS Lambda will be written in Python to prototype functions.
- Functions in AWS Lambda for final production will be written in Rust.
- All Lambda functions depend on the AWS Software Development Kits for their respective programming languages to work with AWS services.

2.2 Internal Communications Architecture

All services and storage, databases, functions, will be stored on AWS Cloud Infrastructure. To detail how all the services interact within this system, a diagram is provided below. Figure 2 illustrates how the CyberTool website will operate on the AWS server. A user can navigate to the CyberTool website where it will establish a connection to our delivery network CloudFront. Amplify will contain all HTML, CSS, and JavaScript files that will be delivered to the user's computer browser for viewing.

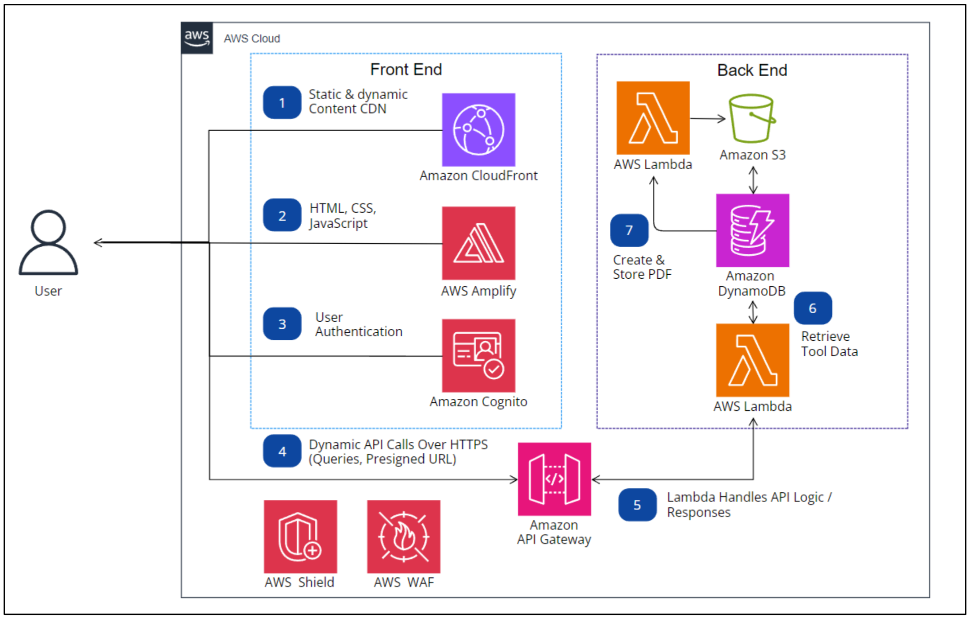


Figure 2: Internal Communications Architecture Overview

Figure 3 illustrates the authentication process using AWS Cognito. Upon a user's attempt to access the website, Cognito will first validate their credentials. Once verified, the user's request is approved, granting them entry to the site's content.

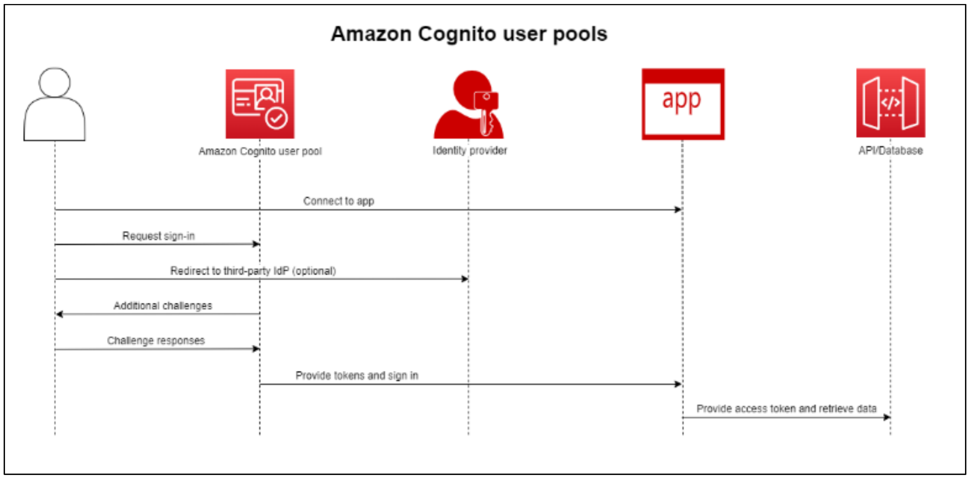

Amazon Cognito user pools
Amazon Cognito user pool
Identity provider
app
API/Database
Connect to app
Request sign-in
Redirect to third-party IdP (optional)
Additional challenges
Challenge responses
Provide tokens and sign in
Provide access token and retrieve data

Figure 3: Amazon Cognito User Pool Authentication Data Flow

3 HUMAN-MACHINE INTERFACE

This section details the inputs and outputs to our system as they relate to the user interacting with the application.

3.1 Inputs

CyberTool is designed to be easily navigated by all users. As a general user, he/she will be able to view all the listed tools within the website and filter through based on user preferences. As an authorized user, he/she will be prompted for a username and password to be authenticated by Amazon Cognito. Authorized users will then be able to input their login information, as well as their preferences for the type of cybersecurity tool they are searching for once authenticated.

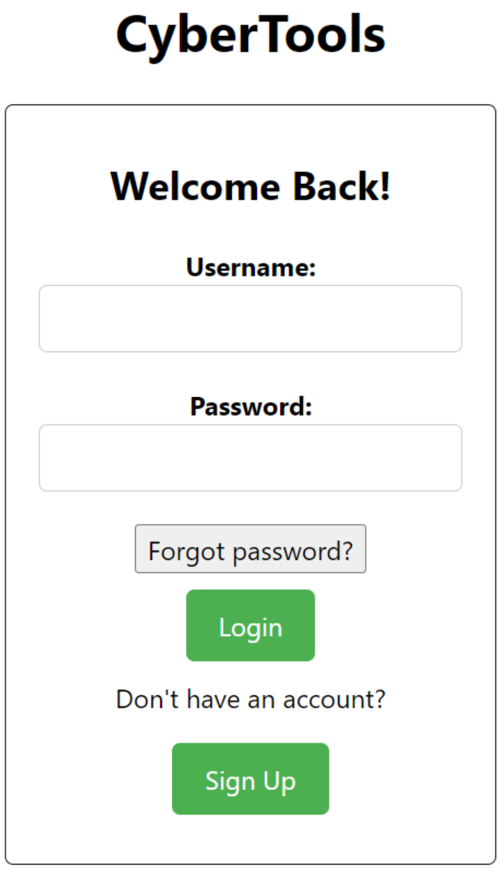


Figure 4: Sign In Page

Upon initialization of the system, the user will be prompted for a username and password to be entered in their respective text boxes as shown in Figure 4. The “Login” button is used to submit the inputs for username and password to Amazon Cognito, which is used to authenticate the users’ credentials if they are already a registered user. Upon successful authentication, a user is brought to the CyberTool Dashboard as shown in Figure 14. If a user has forgotten their password to their username, they may use the “Forgot Password” button to navigate to the Forgot Password page shown in Figure 5 to enter their registered email. If a user does not have an account, they can use the “Sign Up” button to navigate to the Sign Up page shown in Figure 7.

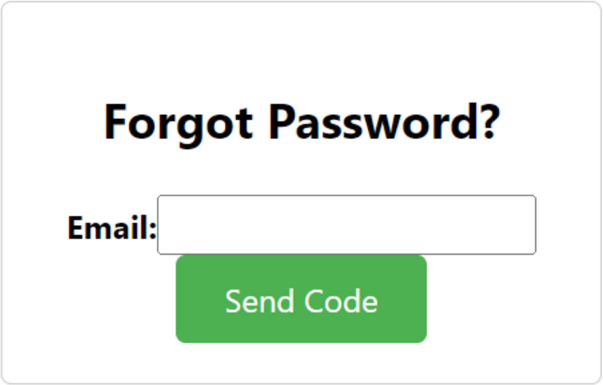


Figure 5: Forgot Password Page

Upon pressing the “Forgot Password” button shown in Figure 4, users are taken to the Forgot Password page shown in Figure 5 to reset their password. Users will input their registered email address to receive a one-time validation code. Using Amazon Cognito, the user will only receive a validation code if they are authenticated. The “Send Code” button will navigate the user to the Reset Password page shown in Figure 6 only if the email is validated by Amazon Cognito.

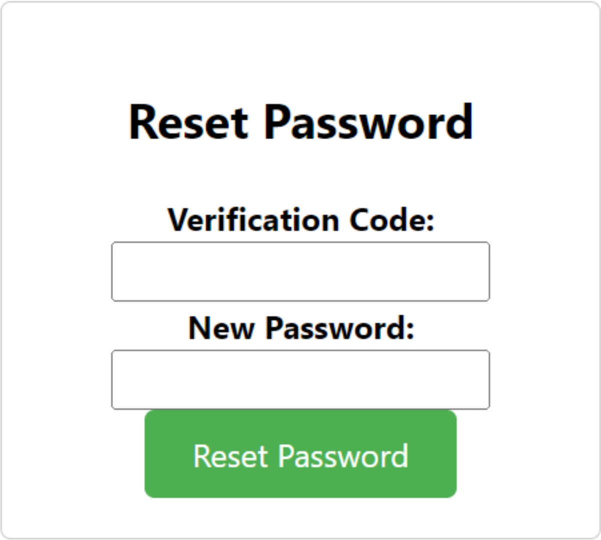


Figure 6: Reset Password Page

In order to reset their password, users must input the verification code that was sent to their registered email address. Finally, users can input their new password in the “New Password” field shown above in Figure 6. Upon pressing the “Reset Password” button, the verification code will be authenticated by Amazon Cognito, and then a user’s password will only be updated in the Amazon Cognito user pool upon successful verification. After this authentication, the user will be automatically directed back to the Sign In Page shown in Figure 4.

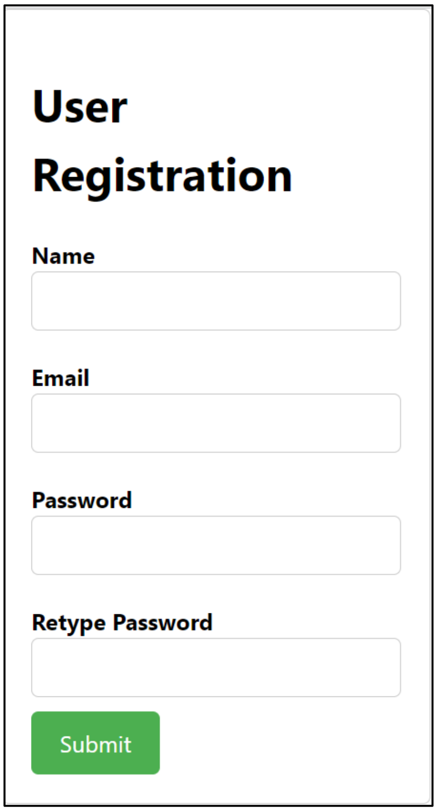
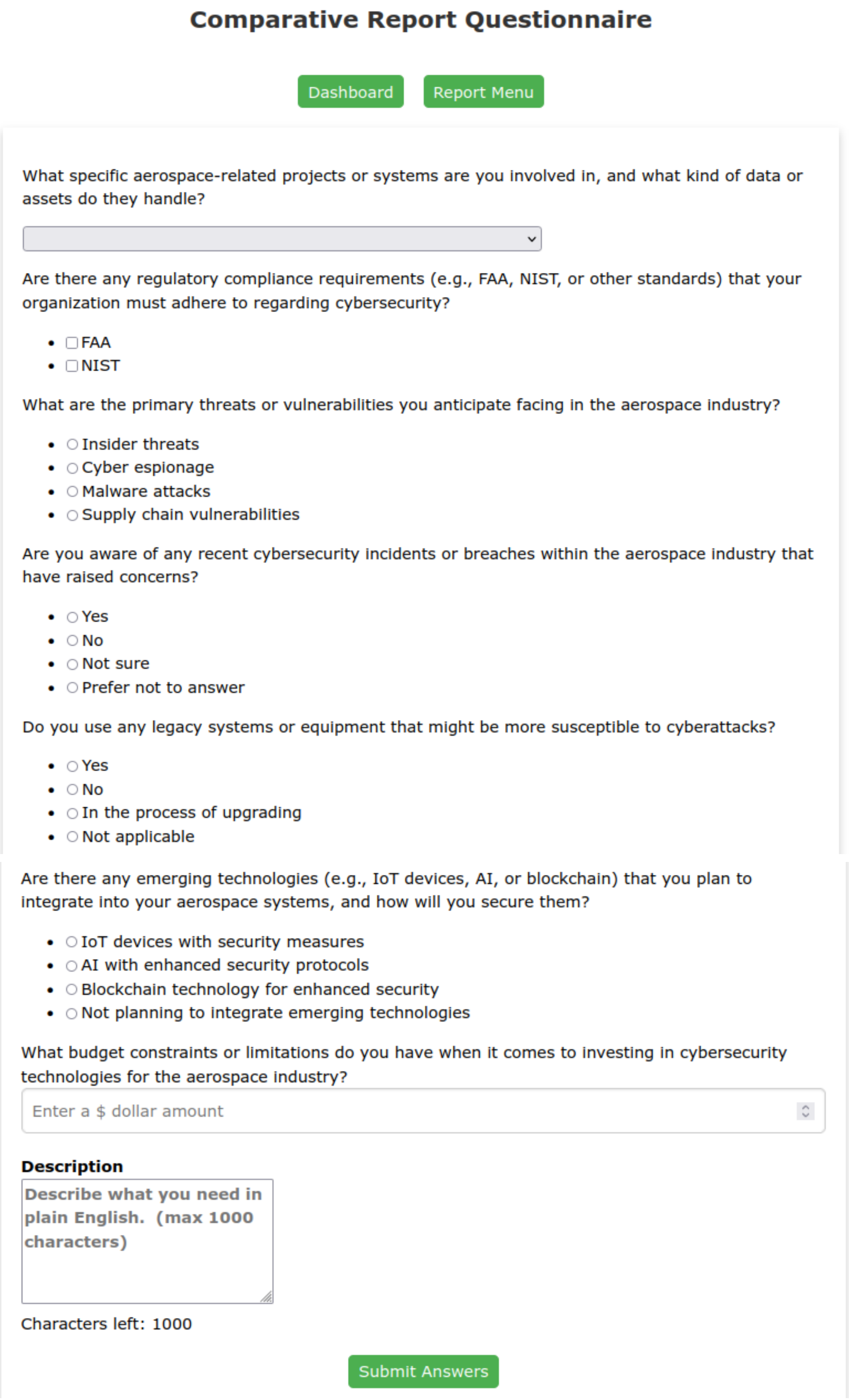


Figure 7: Sign Up Page

If a user does not have an account, the sign-in window provides the option to sign up for an account. Upon choosing the "Sign Up" option, users are prompted to provide their full name, email, password, and a retype password in their respective text boxes. These data entries are intended to uniquely identify each user in the user database. Each text box has a character limit of 30 characters. If the user provides data that is not already found in our database, they are successfully registered upon pressing the "Submit" button. This button directs users to the CyberTool Dashboard shown in Figure 14.



Comparative Report Questionnaire

What specific aerospace-related projects or systems are you involved in, and what kind of data or assets do they handle?

Are there any regulatory compliance requirements (e.g., FAA, NIST, or other standards) that your organization must adhere to regarding cybersecurity?

- □ FAA
- □ NIST

What are the primary threats or vulnerabilities you anticipate facing in the aerospace industry?

- ○ Insider threats
- ○ Cyber espionage
- ○ Malware attacks
- ○ Supply chain vulnerabilities

Are you aware of any recent cybersecurity incidents or breaches within the aerospace industry that have raised concerns?

- ○ Yes
- ○ No
- ○ Not sure
- ○ Prefer not to answer

Do you use any legacy systems or equipment that might be more susceptible to cyberattacks?

- ○ Yes
- ○ No
- ○ In the process of upgrading
- ○ Not applicable

Are there any emerging technologies (e.g., IoT devices, AI, or blockchain) that you plan to integrate into your aerospace systems, and how will you secure them?

- ○ IoT devices with security measures
- ○ AI with enhanced security protocols
- ○ Blockchain technology for enhanced security
- ○ Not planning to integrate emerging technologies

What budget constraints or limitations do you have when it comes to investing in cybersecurity technologies for the aerospace industry?

Enter a $ dollar amount

Description

Describe what you need in plain English. (max 1000 characters)

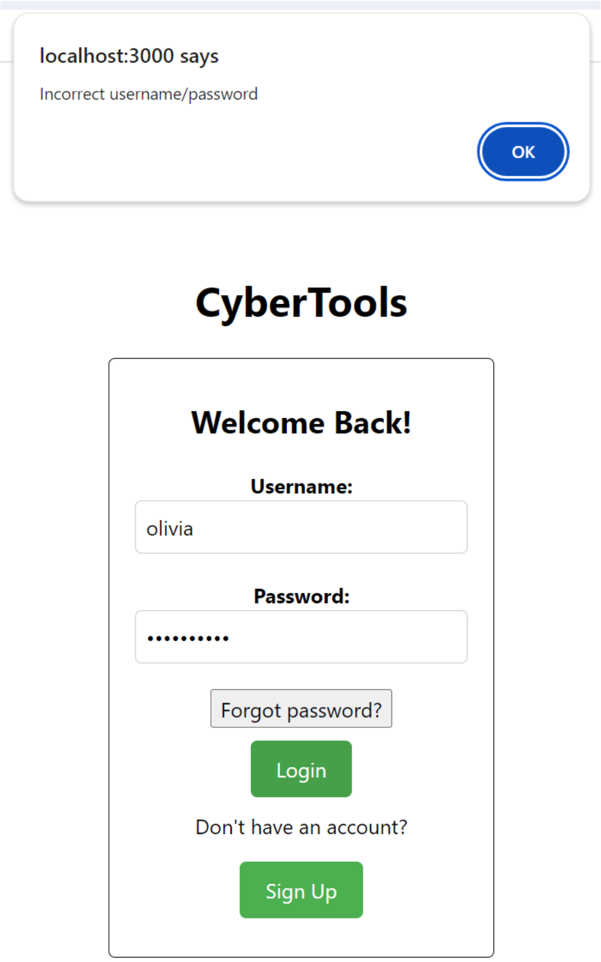
Characters left: 1000

Figure 8: Questionnaire Page

Upon choosing "Questionnaire" from Figure 14, authorized users are presented with the Questionnaire Page shown in Figure 8 to input preferences to serve as the query on the main database of stored cyber tools. The survey includes explicit questions with answers that will define which attributes the user desires in their cyber tool. Only one answer will be accepted per question. Additionally, in Figure 8, users will be asked to enter a plain English description of their desired tool.

3.2 Outputs

With a user’s login information and desired tool requirements, the CyberTool system will output a list of tools that match their preferences along with other recommended products. Authorized users will also have the option to generate a comparative report containing prospective tools and/or tools they already have.



localhost:3000 says

Incorrect username/password

CyberTools

Welcome Back!

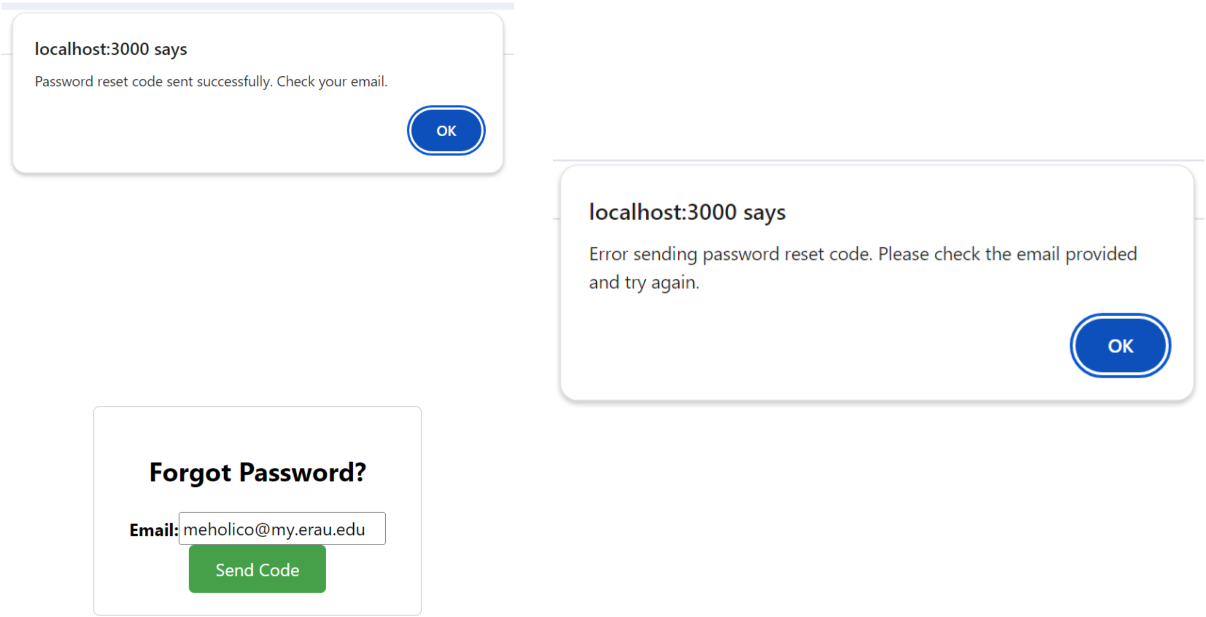
Username: olivia

Password: ••••••••••

Don't have an account?

Figure 9: Sign In Page Error Message

Outputs associated with the Sign In page from Figure 4 include an error message as is shown in Figure 9 if user credentials are not accepted by Amazon Cognito. Clicking the “OK” button on the error message will close the error message.



localhost:3000 says

Password reset code sent successfully. Check your email.

localhost:3000 says

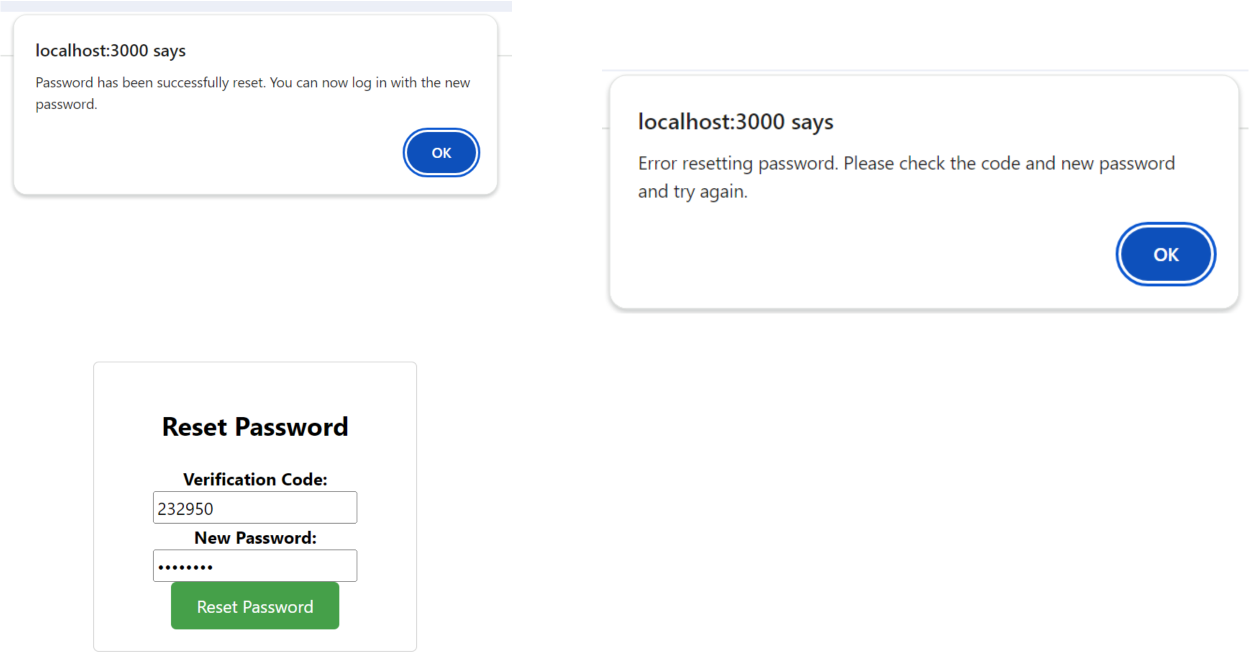
Error sending password reset code. Please check the email provided and try again.

Forgot Password?

Email: meholico@my.erau.edu

Figure 10: Forgot Password Success and Error Messages

Outputs associated with the Forgot Password page from Figure 5 include a success message shown above in Figure 10 that alerts the users of successful email verification from Amazon Cognito. Clicking the “OK” button will close the success message and automatically direct the user to the Reset Password page shown in Figure 6. It also includes an error message shown in Figure 10 if the entered email address is not found in the Amazon Cognito user pool. Clicking the “OK” button on the error message will close the error message.



localhost:3000 says

Password has been successfully reset. You can now log in with the new password.

localhost:3000 says

Error resetting password. Please check the code and new password and try again.

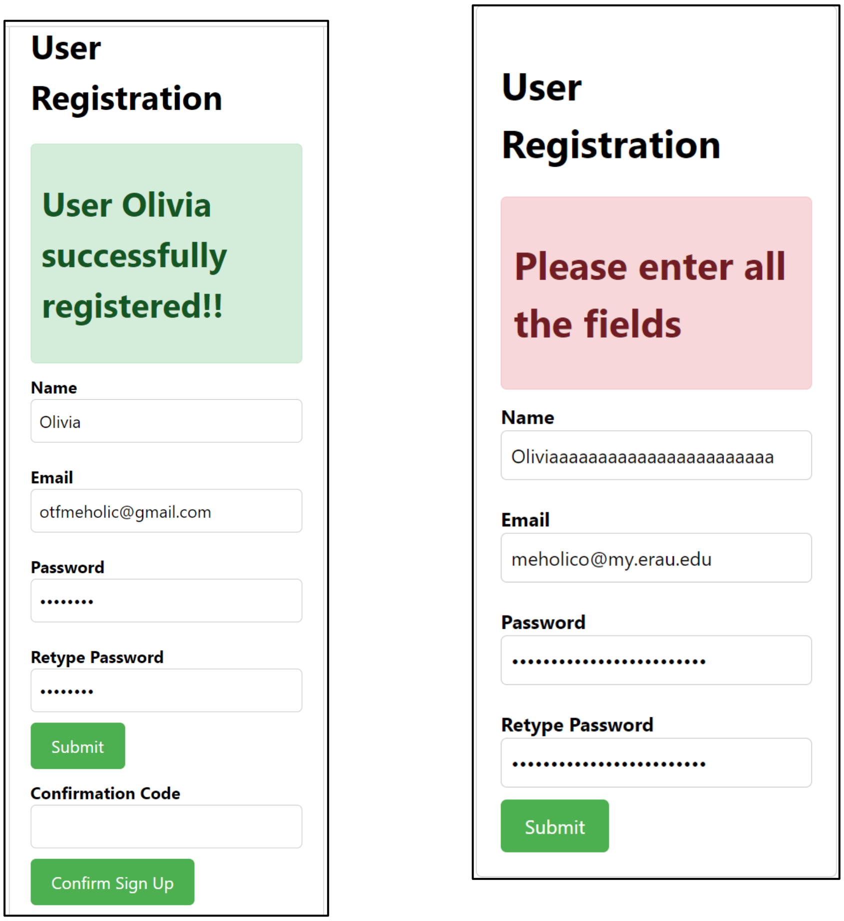
Reset Password

Verification Code: 232950

New Password: ••••••••

Figure 11: Reset Password Page Success and Error Messages

Outputs associated with the Reset Password page from Figure 6 include a success message shown above in Figure 11 that alerts the users of successful code verification from Amazon Cognito. Clicking the “OK” button will close the success message and automatically direct the user to the Sign In page shown in Figure 4. It also includes an error message shown in Figure 11 if the entered verification code is not authenticated by Amazon Cognito. Clicking the “OK” button on the error message will close the error message.



User Registration

User Olivia successfully registered!!

Name: Olivia

Email: otfmeholic@gmail.com

Password: ••••••••

Retype Password: ••••••••

Confirmation Code:

User Registration

Please enter all the fields

Name: Oliviaaaaaaaaaaaaaaaaaaaaaaaa

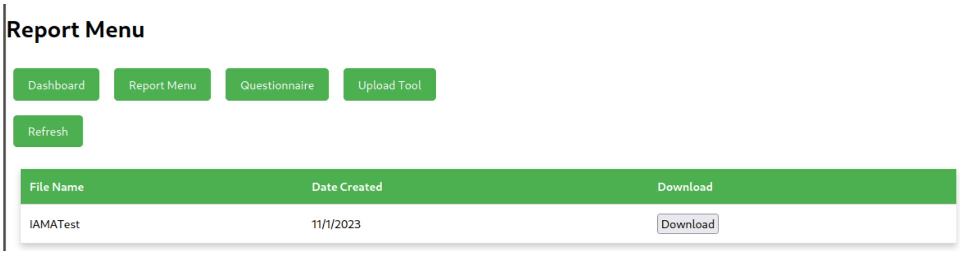
Email: meholico@my.erau.edu

Password: ••••••••••••••••••••••••

Retype Password: ••••••••••••••••••••••••

Figure 12: Sign Up Page Success and Error Message

Outputs for the above Sign-Up display include an error message shown in Figure 12 if the user attempts to include more than 25 characters in any text entry. Outputs also include a success message as shown in Figure 12 if all fields are accepted by Amazon Cognito and the user is successfully entered into the user pool.

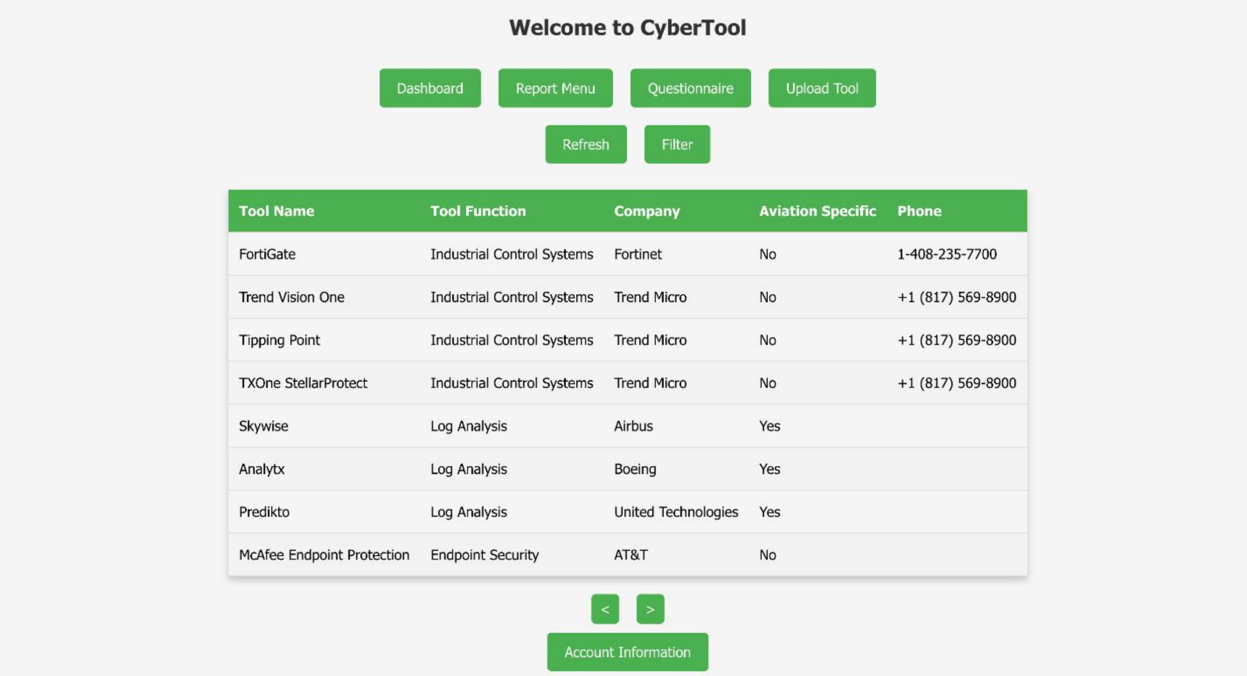


Report Menu

File Name	Date Created	Download
IAMATest	11/1/2023	Download

Figure 13: Report Dashboard

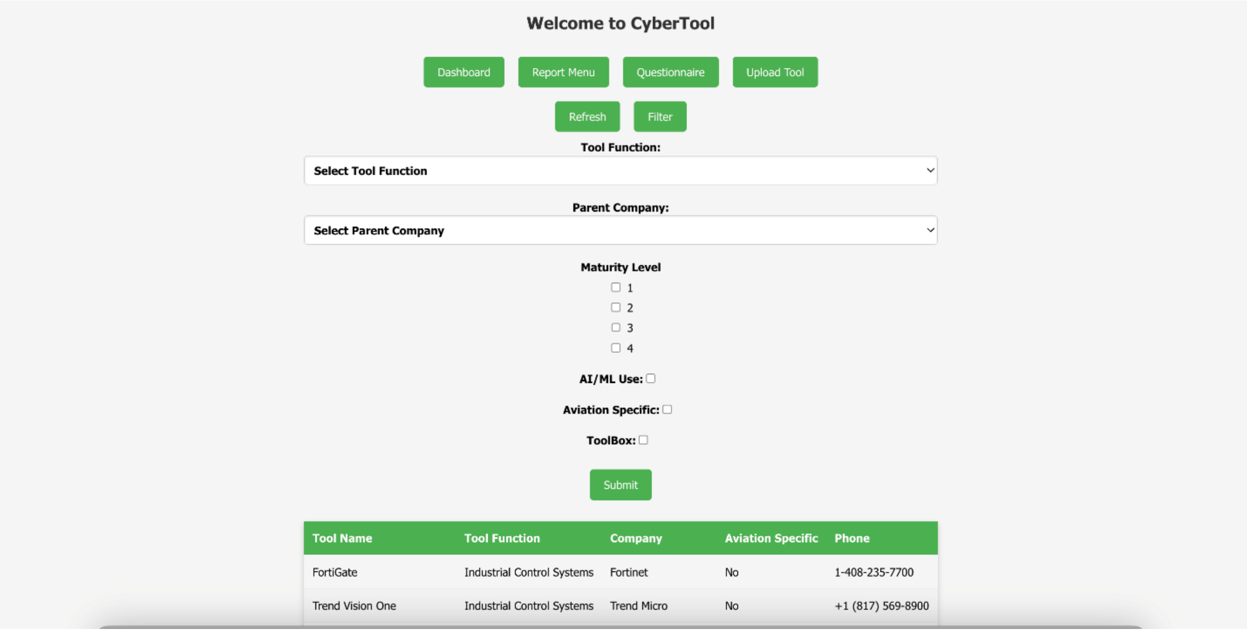
As a result of choosing “Report Menu” from the Dashboard (Figure, 14), the Report Dashboard in Figure 13 is shown to the user. This display shows all past comparative reports generated by that unique user. Upon choosing “Download” in the above display, users can download the generated reports.



Tool Name	Tool Function	Company	Aviation Specific	Phone
FortiGate	Industrial Control Systems	Fortinet	No	1-408-235-7700
Trend Vision One	Industrial Control Systems	Trend Micro	No	+1 (817) 569-8900
Tipping Point	Industrial Control Systems	Trend Micro	No	+1 (817) 569-8900
TXOne StellarProtect	Industrial Control Systems	Trend Micro	No	+1 (817) 569-8900
Skywise	Log Analysis	Airbus	Yes	
Analytx	Log Analysis	Boeing	Yes	
Predikto	Log Analysis	United Technologies	Yes	
McAfee Endpoint Protection	Endpoint Security	AT&T	No	

Figure 14: CyberTool Dashboard

In addition, Figure 14 above shows the initial layout currently implemented for listing the various tools accessible to users. Each tool entry is defined by its name, its function, company, whether the tool is aviation specific, and the company’s phone number. Additionally, the buttons above the table direct the user to either the Report Menu, Questionnaire, Account Information Page, or refresh the page.



Tool Function: Select Tool Function

Parent Company: Select Parent Company

Maturity Level

□ 1

□ 2

□ 3

□ 4

AI/ML Use: □

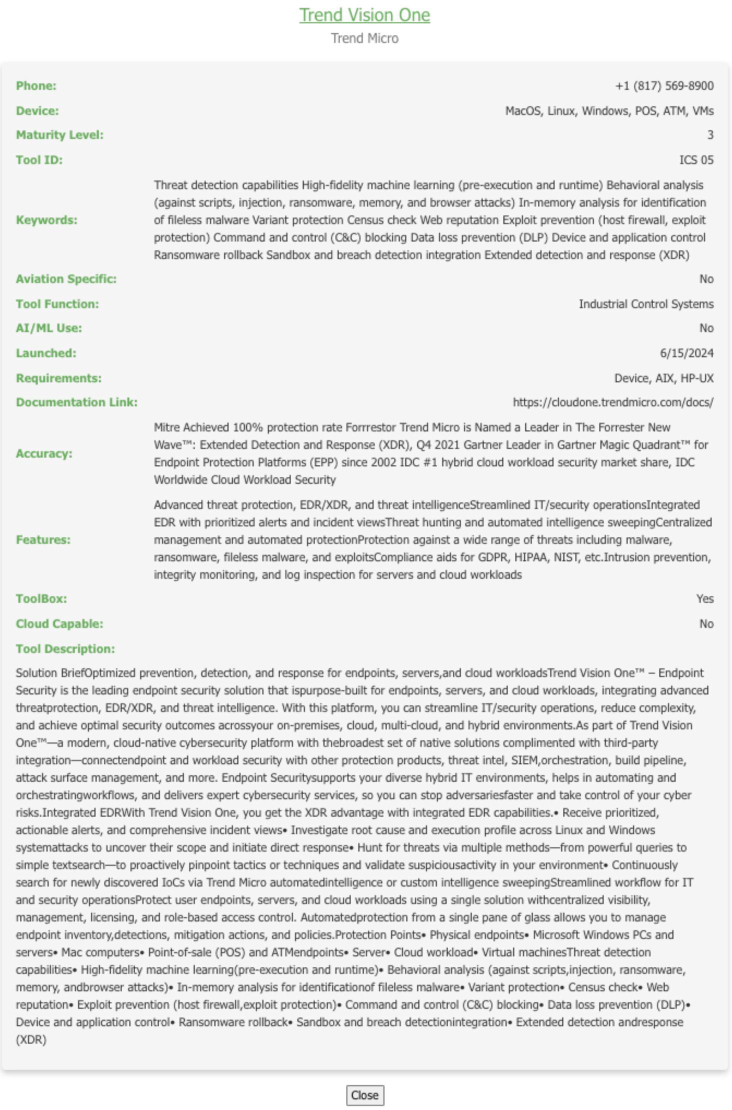
Aviation Specific: □

ToolBox: □

Tool Name	Tool Function	Company	Aviation Specific	Phone
FortiGate	Industrial Control Systems	Fortinet	No	1-408-235-7700
Trend Vision One	Industrial Control Systems	Trend Micro	No	+1 (817) 569-8900

Figure 15: Filtering Tool

Figure 15 shows the filtering system displayed when the user presses the “Filter” button on the dashboard page. The filtering system uses checkboxes and dropdowns. Its JSON object is updated with each user input. Its checkbox options include whether the tool is aviation specific, a toolbox, or for AI/ML use. In addition, the maturity levels of the tools are represented with checkboxes. These tools are checkboxes so that the user can input more than one option at a time. However, with Tool Function and Company, the filtering is a dropdown menu. With this system, the user can input more than one filter. Once the user has finished choosing their filtering options, they can press the “Submit” button to successfully filter the dashboard on the bottom.



Trend Vision One

Trend Micro

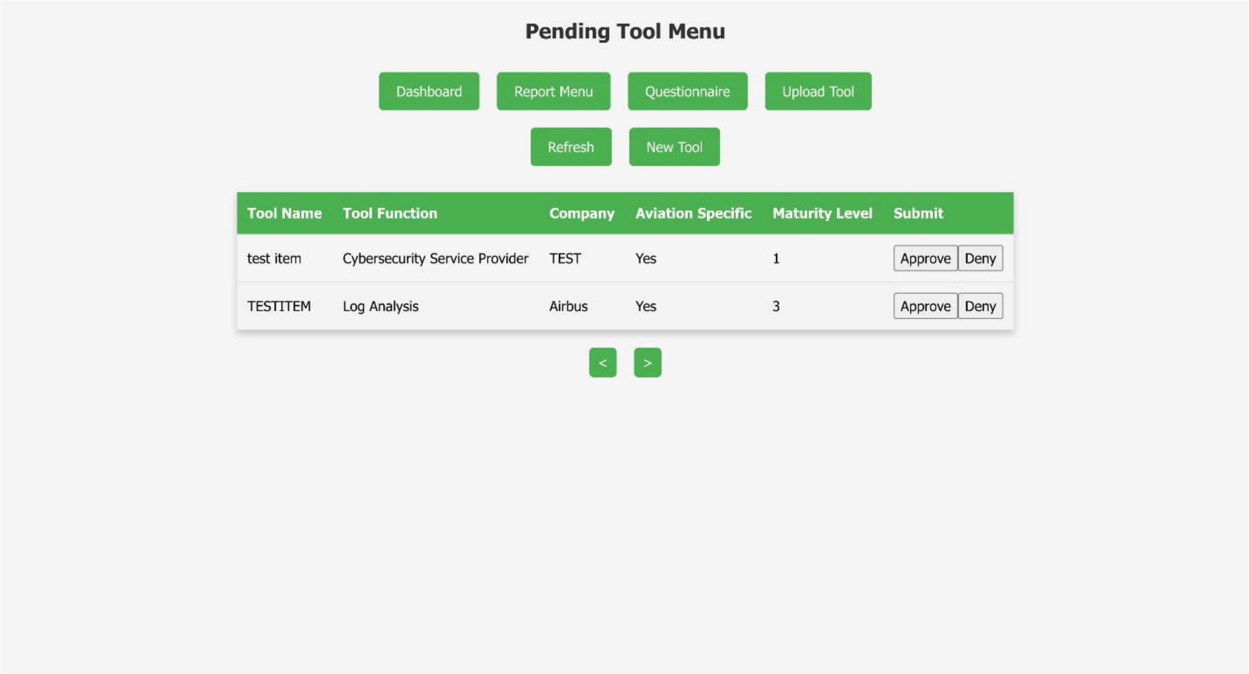
Phone:	+1 (817) 569-8900
Device:	MacOS, Linux, Windows, POS, ATM, VMs
Maturity Level:	3
Tool ID:	ICS 05
Keywords:	Threat detection capabilities High-fidelity machine learning (pre-execution and runtime) Behavioral analysis (against scripts, injection, ransomware, memory, and browser attacks) In-memory analysis for identification of fileless malware Variant protection Census check Web reputation Exploit prevention (host firewall, exploit protection) Command and control (C&C) blocking Data loss prevention (DLP) Device and application control Ransomware rollback Sandbox and breach detection integration Extended detection and response (XDR)
Aviation Specific:	No
Tool Function:	Industrial Control Systems
AI/ML Use:	No
Launched:	6/15/2024
Requirements:	Device, AIX, HP-UX
Documentation Link:	https://cloudone.trendmicro.com/docs/
Accuracy:	Mitre Achieved 100% protection rate Forrrestor Trend Micro is Named a Leader in The Forrester New Wave™: Extended Detection and Response (XDR), Q4 2021 Gartner Leader in Gartner Magic Quadrant™ for Endpoint Protection Platforms (EPP) since 2002 IDC #1 hybrid cloud workload security market share, IDC Worldwide Cloud Workload Security
Features:	Advanced threat protection, EDR/XDR, and threat intelligenceStreamlined IT/security operationsIntegrated EDR with prioritized alerts and incident viewsThreat hunting and automated intelligence sweepingCentralized management and automated protectionProtection against a wide range of threats including malware, ransomware, fileless malware, and exploitsCompliance aids for GDPR, HIPAA, NIST, etc.Intrusion prevention, integrity monitoring, and log inspection for servers and cloud workloads
ToolBox:	Yes
Cloud Capable:	No

Tool Description:

Solution BriefOptimized prevention, detection, and response for endpoints, servers,and cloud workloadsTrend Vision One™ – Endpoint Security is the leading endpoint security solution that ispurpose-built for endpoints, servers, and cloud workloads, integrating advanced threatprotection, EDR/XDR, and threat intelligence. With this platform, you can streamline IT/security operations, reduce complexity, and achieve optimal security outcomes acrossyour on-premises, cloud, multi-cloud, and hybrid environments.As part of Trend Vision One™—a modern, cloud-native cybersecurity platform with thebroadest set of native solutions complimented with third-party integration—connectendpoint and workload security with other protection products, threat intel, SIEM,orchestration, build pipeline, attack surface management, and more. Endpoint Securitysupports your diverse hybrid IT environments, helps in automating and orchestratingworkflows, and delivers expert cybersecurity services, so you can stop adversariesfaster and take control of your cyber risks.Integrated EDRWith Trend Vision One, you get the XDR advantage with integrated EDR capabilities.• Receive prioritized, actionable alerts, and comprehensive incident views• Investigate root cause and execution profile across Linux and Windows systemattacks to uncover their scope and initiate direct response• Hunt for threats via multiple methods—from powerful queries to simple textsearch—to proactively pinpoint tactics or techniques and validate suspiciousactivity in your environment• Continuously search for newly discovered IoCs via Trend Micro automatedintelligence or custom intelligence sweepingStreamlined workflow for IT and security operationsProtect user endpoints, servers, and cloud workloads using a single solution withcentralized visibility, management, licensing, and role-based access control. Automatedprotection from a single pane of glass allows you to manage endpoint inventory,detections, mitigation actions, and policies.Protection Points• Physical endpoints• Microsoft Windows PCs and servers• Mac computers• Point-of-sale (POS) and ATMendpoints• Server• Cloud workload• Virtual machinesThreat detection capabilities• High-fidelity machine learning(pre-execution and runtime)• Behavioral analysis (against scripts,injection, ransomware, memory, andbrowser attacks)• In-memory analysis for identificationof fileless malware• Variant protection• Census check• Web reputation• Exploit prevention (host firewall,exploit protection)• Command and control (C&C) blocking• Data loss prevention (DLP)• Device and application control• Ransomware rollback• Sandbox and breach detectionintegration• Extended detection andresponse (XDR)

Figure 16: Tool Information

Figure 16 shows the tool information displayed after the user clicks on a dashboard tool. The information displayed includes: the company’s phone number, the device the tool uses, the maturity level, tool ID, keywords, aviation specific, too function, AI/ML function, launched, requirements, documentation link, accuracy, features, toolbox, cloud capable, and tool description. The user presses the “close” button to go back to the dashboard.

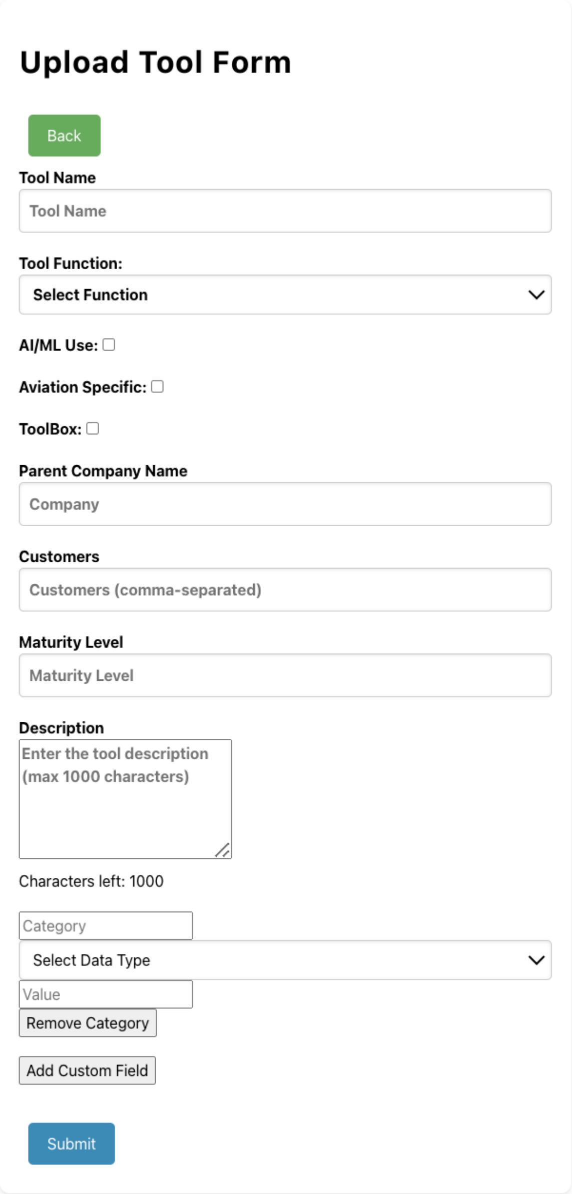


Pending Tool Menu

Tool Name	Tool Function	Company	Aviation Specific	Maturity Level	Submit
test item	Cybersecurity Service Provider	TEST	Yes	1	Approve Deny
TESTITEM	Log Analysis	Airbus	Yes	3	Approve Deny

Figure 17: Tool Menu

Figure 17 shows the pending tool Menu, used to approve or deny new tools from the upload tool form. The formatting is the same as the dashboard, but instead has “approve” and “deny” buttons.



Upload Tool Form

Back

Tool Name

Tool Name

Tool Function:

Select Function

AI/ML Use: □

Aviation Specific: □

ToolBox: □

Parent Company Name

Company

Customers

Customers (comma-separated)

Maturity Level

Maturity Level

Description

Enter the tool description (max 1000 characters)

Characters left: 1000

Category

Select Data Type

Value

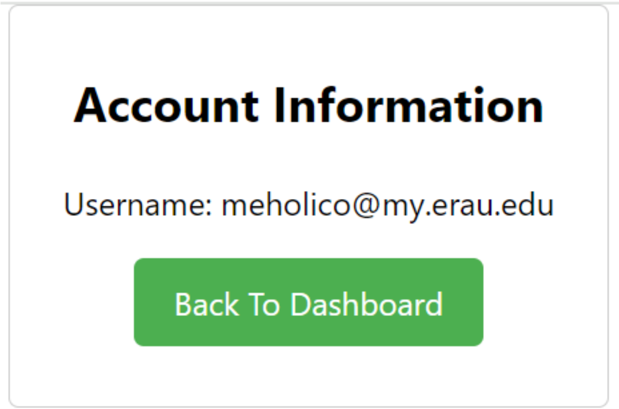
Remove Category

Add Custom Field

Submit

Figure 18: Upload Tool Form

Figure 18 shows the upload tool form displayed after the user presses the “New Tool” button. The tool form will have a mix of text boxes, dropdowns, check boxes, and buttons to add or remove categories. The form will ask for: the name of the tool, the tool function, whether it’s for AI/ML use, aviation specific, or a toolbox, the parent company name, the customers, the maturity level, a description, a category, the data type, the value, and buttons to remove and add custom fields. Once the user has finished the form, they press “Submit” where the tool will be displayed on the pending tool menu where the user can choose to approve or deny the tool.



Account Information

Username: meholico@my.erau.edu

Figure 19: Account Information Page

Upon pressing the "Account Information" button shown in Figure 14, users are directed to the Account Information page shown in Figure 15. This page displays the email of the current user that is logged into the CyberTool website. The "Back To Dashboard" button directs users to the CyberTool Dashboard displayed in Figure 14.

4 DETAILED DESIGN

Front-End Design: The front-end prioritizes user accessibility, incorporating a search bar and tailored filter options. Its visual design adapts seamlessly across devices. Users can create accounts for personalized experiences, saving preferences, and generating reports.

Back-End Design: The entirety of the back end is supported by AWS. DynamoDB is a scalable, NoSQL database that was used to store cyber tools for querying. The sorting system is based on a primary key of the tool function and a secondary sorting key of a unique identifier string. These two keys, including a list of defined attributes, allow for the system to navigate and locate tools in the table. DynamoDB allows the developers to add, update, delete, and compare items in the table. API Gateway is used to connect DynamoDB to CloudWatch and allows the front-end to communicate with the back end. API Gateway uses endpoints that interpret the user preferences (attained from questionnaire) and translate this to a query of various sorting keys and attributes in DynamoDB. Amazon S3 is integrated with DynamoDB to create and store PDF results for the user based on the query results.

4.1 Hardware Detailed Design

CyberTool is strictly hosted on AWS infrastructure and servers. For more insight into what technologies are used, please look at the AWS website. No hardware is handled directly by the team.

4.2 Software Detailed Design

4.2.1 Frontend Navigation and State Flow

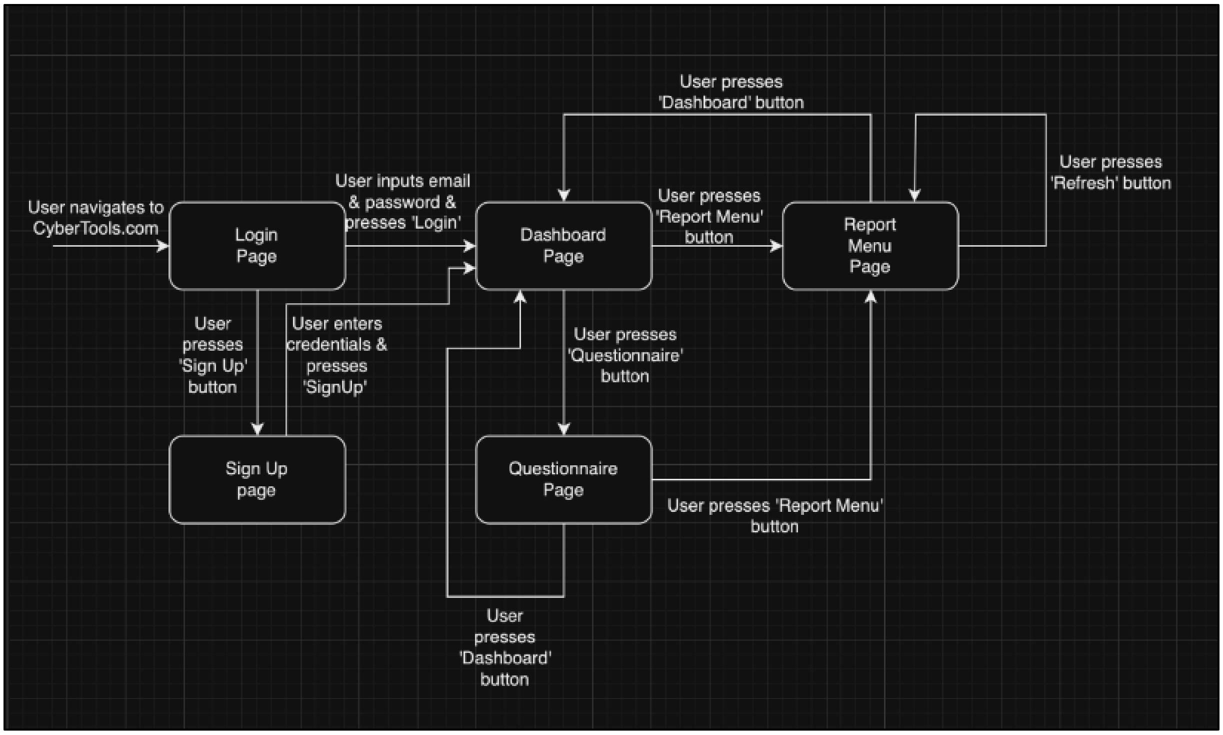

User navigates to CyberTools.com
Login Page
User inputs email & password & presses 'Login'
Dashboard Page
User presses 'Dashboard' button
User presses 'Report Menu' button
Report Menu Page
User presses 'Refresh' button
User presses 'Sign Up' button
User enters credentials & presses 'SignUp'
User presses 'Questionnaire' button
Sign Up page
Questionnaire Page
User presses 'Report Menu' button
User presses 'Dashboard' button

Figure 16: Front-End Navigation Diagram

Figure 16 illustrates the front-end process using AWS Amplify & AWS React. When the user navigates to CyberTools.com, the login page will be presented to the user. Once verified, the user will be directed to the dashboard page. If the user does not have an account, they can enter their credentials to sign up. Once finished, the user is directed to the dashboard page. Once on the dashboard page, they can press the ‘Questionnaire” button or the ‘Report Menu’ button. If the questionnaire is clicked, the user can choose to go back to the dashboard to the report menu page. If the report menu page is clicked, the user can go back to the dashboard page or click the refresh button, which essentially reloads the page.

4.2.2 AI Enabled tool search

The integration of AI search into our cyber tool recommendation website addresses a large limitation of traditional survey-based filtering methods: the nuanced understanding of user needs and context. While multiple-choice questions effectively categorize users based on predefined criteria such as industry, price range, and cloud reliance, they fall short in capturing the complex and specific requirements users might have. AI search, leveraging large language models (LLMs), allows users to express their needs in their own words, providing a more personalized and accurate tool recommendation. This approach not only enhances user satisfaction by better aligning recommendations with their actual needs but also differentiates our service in a competitive market by offering a more intuitive and user-centric experience.

Large Language Models transform text into high-dimensional vector spaces, a process known as vector embedding. This technique involves encoding the semantic and syntactic features of text into a vector of real numbers. Each dimension of the vector represents a latent feature captured from the text, allowing the model to understand and compare the meanings of different texts mathematically. This is achieved through deep learning architectures that have been trained on vast amounts of text data, enabling the model to generate embeddings that reflect the nuanced relationships between words and phrases. By converting natural language into a mathematical form, LLMs facilitate a wide range of language tasks, including similarity comparison, which is essential for AI search functionalities.

To implement the AI search functionality, we first preprocess user prompts and tool descriptions to normalize the text, including lowercasing and removing special characters. Each preprocessed text is then fed into a pre-trained LLM (currently LLAMA 2, with 7-billion parameters) to generate vector embeddings. We use cosine similarity to compare the embedding vector of the user's prompt with the embedding vector of each tool's description. Cosine similarity measures the cosine of the angle between two vectors, providing a value between -1 and 1 indicating how similar the texts are in their semantic content. Tools are then ranked based on their similarity scores, with higher scores indicating a closer match to the user's expressed needs. This process allows for dynamic and precise matching between user requirements and tool capabilities, leveraging the power of LLMs to interpret and act upon natural language input effectively.

4.3 Internal Communications Detailed Design

The state transition diagram presented in Figure 17 illustrates the various user interactions and system state changes within the CyberTool website. It serves as a visual guide to understand the flow of operations a user can perform, starting from the initial access to the webpage. This diagram delineates conditional paths based on user authentication, tool usage, questionnaire engagement, and report generation. It effectively captures the dynamic behavior of the CyberTool website, providing insights into the user experience and the system's response to different user actions.

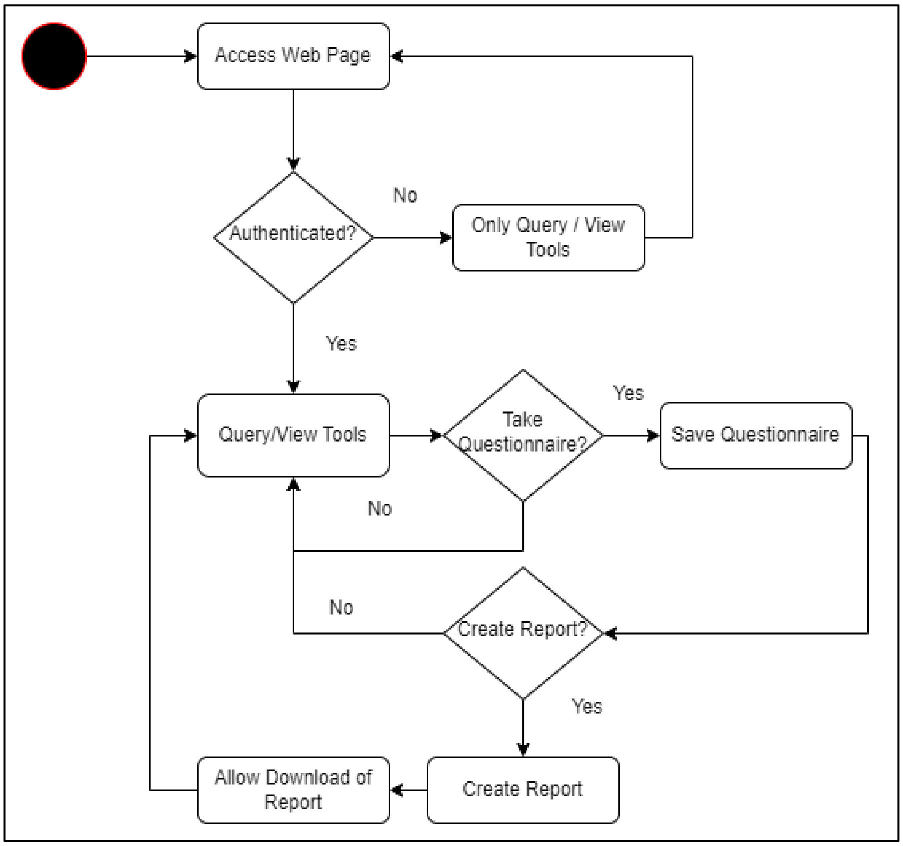


Figure 17: State Transition Diagram for CyberTool Website Users

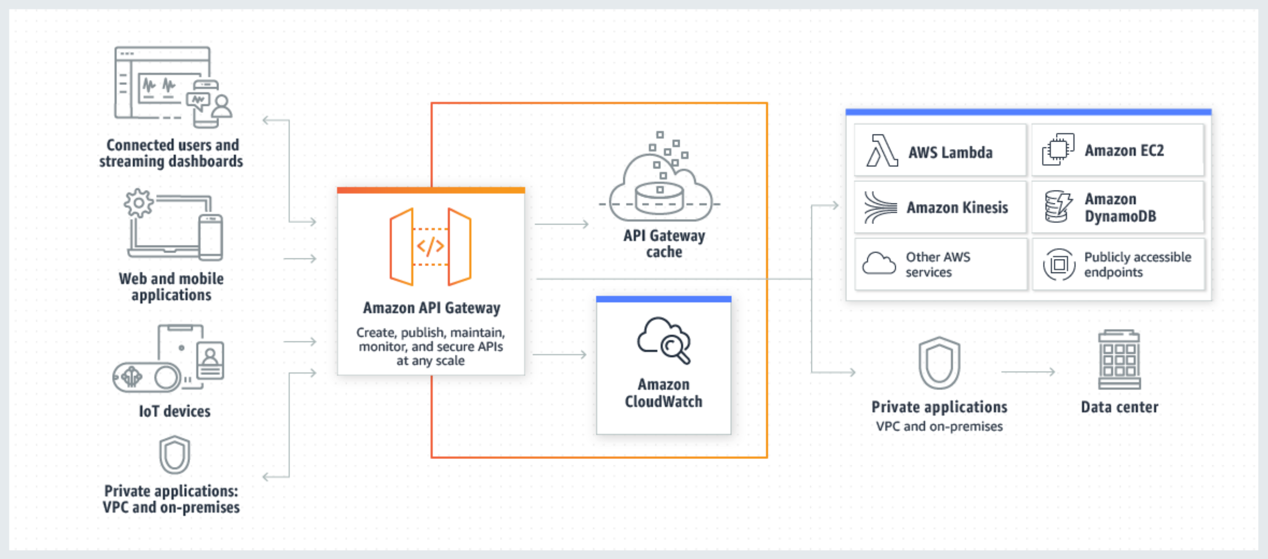

Connected users and streaming dashboards
Web and mobile applications
IoT devices
Private applications: VPC and on-premises
Amazon API Gateway
Create, publish, maintain, monitor, and secure APIs at any scale
API Gateway cache
Amazon CloudWatch
AWS Lambda
Amazon EC2
Amazon Kinesis
Amazon DynamoDB
Other AWS services
Publicly accessible endpoints
Private applications
VPC and on-premises
Data center

Figure 18: Amazon API Gateway, connections

Amazon API Gateway is used to facilitate communication between different AWS services by allowing for the development of a RESTful API, as shown in Figure 18.

API Gateway makes use of AWS Lambda, another AWS-provided service which allows for code to be run on the serverless web application. Together with Lambda, API Gateway will act as a proxy between the front-end web application managed through Amplify and the back-end resources and data stored in DynamoDB. For both developers and users, API Gateway uses URL endpoints to invoke different HTTP methods to access or modify resources. See Section 5.1.1 for methods.

5 SYSTEM INTERFACES

This section describes the interfaces that CyberTool will use to interact with AWS and the user's web client.

5.1 Interface Architecture

The primary internal communication for the CyberTool system will be via a web browser as specified.

5.2 API Architecture

This API architecture utilizes AWS API Gateway and Cognito for authentication, aimed at facilitating seamless interaction between users and cloud resources. It outlines the support for various HTTP methods (GET, POST) to perform a wide range of operations, from tool retrieval to report generation. Overall, the API has set instructions and endpoints for user interaction with the React Frontend.

5.3 HTTP Methods

In order for the CyberTool React website client to communicate with appropriate resources in the AWS backend, a list of API endpoints will be created in API gateway.

1. POST beginCreateReportForUser - Create a new Report for user

2. POST fetchDashboard - Get a list of tools for user for dashboard presentation

3. POST getReportListForUser - Get a list of reports for user that can be downloaded

4. POST getSingularToolData - Get a tool's data for a webpage

5. POST getPresignedURL - Get a url to download a reports URL

5.4 Request Body, Request Headers

- Request headers contain metadata and instructions for the API regarding the request. Necessary headers will include:
- Content-Type: specifies the format of the data in the request body (this will be JSON unless otherwise noted).
- Authorization*:* contains credentials for authenticating the client making the request.
- Accept: specifies the preferred media type for the response.

Request bodies contain the actual data regarding the request if any further data is needed. For example, a POST request with a JSON content type will contain the key-value attributes for a new item formatted in JSON in the request body.

5.5 Query parameters

Endpoints can include query parameters to provide additional information for the request. Query parameters are appended to the endpoint URL.
This is important for filtering queries. For example, the request

```
GET /tools?category=log_analysis&year=2004
```

should only retrieve tools categorized as Log Analysis tools that launched in 2004.
Query parameters shall accept strings, integers, or Boolean values (true/false) as data types depending on the attribute being requested.

5.6 Report Generation

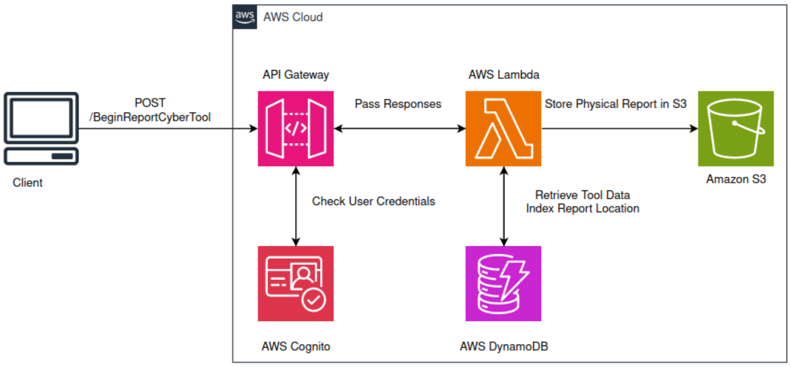


Figure 19: BeginReportCyberTool Architecture

As shown by Figure 19, once a user has completed the questionnaire, the /BeginReportCyberTool endpoint will receive and serialize the questions and answers, and generate a report based on the answers and other entered data, such as already used cyber tools. Within the Lambda function, the report will be physically created as a pdf, and stored within S3. At any time if the report generation fails, a server failure 500 error tells the user what error and when it happened. At success of generation, the file's location in s3 is saved in DynamoDB and can be queryable by the user in the ListReport endpoint.

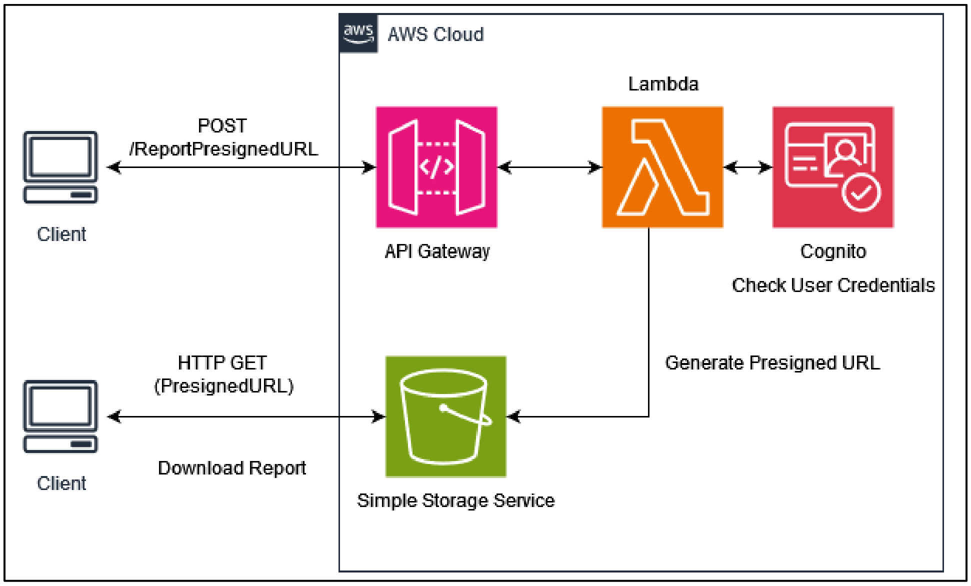


Figure 20: GetPresignedURL Interface for Getting an Object from S3.

As seen by Figure 20, using API Gateway as an interface and proxy for resources on AWS, the user will send the API user credentials & a specific UUID for the report. Using Lambda & Cognito to authenticate the user's credentials and ensure they have personal access to these files on the cloud, the API will send back a URL, containing a JWT that contains security credentials for a limited time, in this case 1 week, to access the specified report file. This report file will be accessed via the browser in a PDF file type.

6 INTERFACE DETAILED DESIGN

6.1 Data Format Requirements

All data passed from front-end React Website to API Gateway must be done via JSON Document I/O.

6.2 Security Interaction Front/Back-End

All website connections are done with HTTPS protocol, SSL/TLS.

6.3 Error Handling

- Client-Server errors will be reported to users via JavaScript Alerts.
- Report Creation failures & errors will be reported to users via emails.

7 SYSTEM INTEGRITY CONTROLS

7.1 AWS Log Creation

7.1.1 Amazon CloudWatch

Function: Central log management service for collecting, storing, and monitoring log data from a wide range of AWS resources and applications.
Organization: Log data is organized into log groups and log streams, facilitating efficient log management.

7.1.2 AWS CloudTrail

Function: Provides a detailed history of API calls made on an AWS account, offering insights into who made the calls and the actions performed.
Importance: Crucial for security and compliance monitoring, as it records all API activities.

7.2 AWS Log Storage

7.2.1 Amazon S3 (Simple Storage Service)

Function: Amazon S3 simple object storage. Necessary for long-term log retention, storing both CloudWatch and CloudTrail Logs.
Retention: Amazon S3 allows for the configuration of retention policies, providing flexibility in meeting storage duration requirements.

7.3 API Security

Using AWS Firewall Manager, employ AWS WAF to safeguard against common web exploits and attacks, complemented by request and response validation for input sanitization. Set up rate limiting and throttling to protect against abuse and Distributed Denial of Service (DDoS) attacks using AWS Shield. For API authentication, Amazon Cognito User Pools will act as access control to API.

7.4 Object Storage Security

7.4.1 Bucket Policies and Access Control Lists (ACLs)

Bucket policies and ACLs control access to S3 buckets and objects, allowing you to grant or deny permissions to specific AWS accounts or users.

7.4.2 Bucket and Object-Level Encryption

Implement (SSE) to encrypt data at rest within S3. AWS provides three SSE options: SSE-S3, SSE-KMS, and SSE-C, each with distinct advantages.

7.4.3 Access Logging

Enable access logging on S3 buckets to maintain records of all requests made to objects, which is invaluable for auditing and monitoring access.

7.4.4 Versioning

Enable versioning to preserve all versions of an object, protecting against accidental overwrites or deletions and aiding in data recovery.

7.4.5 Pre-Signed URLs and Cookies

Use pre-signed URLs or cookies to grant temporary access to S3 objects, for time-limited access to private content.

7.4.6 Monitoring and Alerts

Amazon CloudWatch alarms and AWS CloudTrail to monitor and log S3 bucket activity, setting up alerts for suspicious or unauthorized actions.

7.5 Database Security

7.5.1 Data Encryption, Encryption at Rest

Implement server-side encryption (SSE) to protect data at rest. SSE ensures that data stored in DynamoDB remains encrypted and secure.

7.5.2 Access Control

Leverage IAM policies and fine-grained access control to limit access to DynamoDB tables and items to authorized entities only.

7.5.3 Auditing and Monitoring

Implement Amazon CloudWatch to monitor and audit DynamoDB queries & transactions.

7.6 User Control in AWS

7.6.1 AWS Organizations – Centralized Account Management

Centralized Platform for management and organization of AWS accounts, this enables users of the main AWS account to be grouped in OUs. The advantage of using OUs is to add fine-grained access control policies through SCPs. This ensures the consistency of security and compliance policies across the organization. Furthermore, through the use of AWS Organizations, RBACs can be leveraged to define granular permissions on the user level. RBACs can explicitly grant and deny specific resources or actions within each user account.

7.7 User Control in CyberTool

User control, including authorization and authentication, will be done via Amazon Cognito. Amazon Cognito User Pools operates as a CIAM that offers secure identity storage and authenticator that can support login with social identity providers and SAML or OIDC-based identity providers. Users can register within CyberTool to access specific pages to the webapp.

7.8 Application Logging

(See 6.1) AWS X-Ray can provide insights into the health and operation of services and resources in live use. Integrating X-ray with CloudWatch Logs can enable CloudWatch alarms to resolve issues based on trace X-ray traced data.

7.9 Application Log Storage

(See 6.2)

7.10 Application Security

All client-webapp communication will be encrypted via HTTPS. Cognito endpoints for authorization will be encrypted via HTTPS.

7.11 HTTPS Encryption

Using Amazon CloudFront as a low latency content delivery network, the base requirement for client to server communication is SSL/TLS security certificate with TLS 1.3. The security certificate must be in X.509 format. The security certificate will be from the AWS Certificate Manager.