1

##### **NIT6150**

##### **Advanced Project**

##### Project Proposal

**Beyond Traditional Security: Innovative Application Layer Encryption Algorithms**

**Team Leader:** Riski Nurfajriani (Kiki) (s4675655)

**Team Members:** Raniel Pascua (s4682362)

Le Bao Duy Nguyen (s8067123)

Brendon Ashton (s4674934)

**Client:** Wenjie Ye  
VU Melbourne

**Supervisor:** Wenjie Ye

VU Melbourne

**Coordinator:** **Wenjie Ye**

College of Engineering and Science

Victoria University, Melbourne

Table of Contents

[1. Introduction 3](#_Toc1320284286)

[2. Background and Client Profile 3](#_Toc1692378564)

[3. Purpose and Objectives 4](#_Toc2071878196)

[4. Technology Stack 5](#_Toc1115263724)

[5. Scope and Exclusion 5](#_Toc1361082013)

[6. Assumptions and Constraints 6](#_Toc1428978728)

[7. Deliverables 6](#_Toc1653651208)

[8. Schedule 7](#_Toc1534424078)

[9. Budget 9](#_Toc280245646)

[10. Resources Roles and Responsibility 10](#_Toc440936447)

[11. Functional Requirements 11](#_Toc534167320)

[12. Use Case Diagram 12](#_Toc1619338312)

[13. Non-Functional Requirements 13](#_Toc1699798034)

[Feel, Look and Portability 16](#_Toc315517571)

[14. Maintainability and support requirements. 19](#_Toc448436772)

[15. UML Diagram and Data Types 22](#_Toc1940517467)

[16. System Navigation and User Interface Design 23](#_Toc1561568269)

[17. Project Management 28](#_Toc899862376)

[18. References 32](#_Toc2112713805)

GitHub Repository: <https://github.com/ranpascua/adv_proj_cyberguardians>

# Introduction

In an increasingly interconnected world where data privacy and security have become paramount, DataSafe Inc. stands as a well-recognised guardian of sensitive information. Renowned for their exceptional technology services catering to individual consumers, businesses, and governmental entities, Data-Safe Inc. has built a strong reputation based on their unwavering commitment to data encryption and cybersecurity. With new challenges from cyber-attacks such as man-in-the-middle (MITM) attacks, DataSafe Inc. ‘s new focus is on developing a new method to address the issue and protect their infrastructures. As we delve into this proposal document, it becomes evident that The Data-Safe Inc. is not just a technology service provider, but a pioneer in encryption, with new secure and efficient approaches to tackle this challenge.

# Background and Client Profile

**Client Profile**

Name: DataSafe Inc.

Industry: Technology Services

Segment: Individual consumers, businesses, governmental entities

Focus: Data encryption, cybersecurity, prevention of man-in-the-middle attacks

DataSafe Inc., (herein referred to as “the client”), is an industry leader that distinguishes itself through its unparalleled expertise in data encryption and cybersecurity. Their suite of technological solutions assists individual consumers, businesses, and governmental entities to manage, process, and transmit their sensitive data. What helps them stand out from their competitors is not only their product and infrastructures, but also their unwavering commitment to data security and privacy, which involves handling and dealing with personal details, financial transactions, governmental records, etc.

**Background**

Despite their steadfast commitment to data security, the client recently faced a series of advanced man-in-the-middle (MITM) attacks. These attacks strategically exploited existing security vulnerabilities, enabling unauthorized interception and potential manipulation of sensitive data transmitted between the client's applications and servers. This breach not only exposed weaknesses in their security infrastructure but also emphasized the evolving nature of cyber threats and its threat to the cyber space.

The client recognizes the imperative to enhance their data encryption protocols and strengthen their defences against MITM attacks. The client acknowledges the need to refine their systems with robust encryption mechanisms which ensure end-to-end protection of data, thereby preventing unauthorized access and manipulation.

# Purpose and Objectives

We propose to provide an implementation strategy for application layer encryption to enhance data integrity, confidentiality, and availability, thereby protecting against threats like data breaches and man-in-the-middle attacks.

Application Layer Encryption/Decryption

* Implementing encryption between application's client-server communication.
* Ensuring that even if the data is intercepted, it cannot be read without proper decryption keys.
* Selecting an appropriate encryption algorithm and key management system.

Additional Security Measures

* Employing authentication mechanisms like OAuth2 or JWT.
* Using secure coding practices to minimize vulnerabilities.

# Technology Stack

The following latest technology and security feature are being used to develop our application:

* + **.NET Framework (Back-end)** - is a software development framework for building and running applications on Windows.
  + **ReactJS (Front-end)** - React is a free and open-source front-end JavaScript library for building user interfaces based on components.
  + **AWS RDMS MySQL** - collection of managed services that makes it simple to set up, operate, and scale databases in the cloud.
  + **AWS App Runner** - Fully managed container application service that lets you build, deploy, and run containerized web applications and API services without prior infrastructure or container experience.

# Scope and Exclusion

The scope of this project is concentrated on the architecture, design, implementation, and validation of advanced security mechanisms for an application:

* Designing and integrating encryption and decryption at the application layer for both backend and frontend. This will facilitate secure data transmission and reception.
* Ensuring all implemented measures are aligned with industry standards and setting up regular updates and maintenance for constant vigilance against evolving threats.

While the scope provides a comprehensive plan for enhancing the application's security, certain aspects are intentionally excluded:

* The focus is on digital security, so physical security controls are outside the project's focus.
* Security measures for third-party services or APIs are beyond the control of this project.
* The project aims to deal with current and future systems, so support for outdated systems is not included.

# Assumptions and Constraints

**Assumptions**

**External factors:**

* + Attackers are fast to catch up with the current technology, therefore, the solution that we propose could already be expected by them.
  + There might be little to no regulations covering the proposed idea

**Technical Assumptions:**

* + Tools and knowledge require for this project could be beyond our experience, and it could be complex.

**Resource Assumptions:**

* Each personnel in this team have broad range of experience outside of IT that could help with streamlining the process.

**Constraints**

**Time Constraints:**

* + As cybersecurity can be a complex topic, the time to complete the project might not be ideal, as it requires a deep understanding and analysis of the current cyber issue that could still be undetectable.

**Technical Constraint:**

* Some personnel might still familiarise themselves with the required tools.

**Regulatory and compliance constraints:**

* Amending or adding new law to the existing regulation might be time consuming and hard to break.

# Deliverables

The project deliverables are as follows:

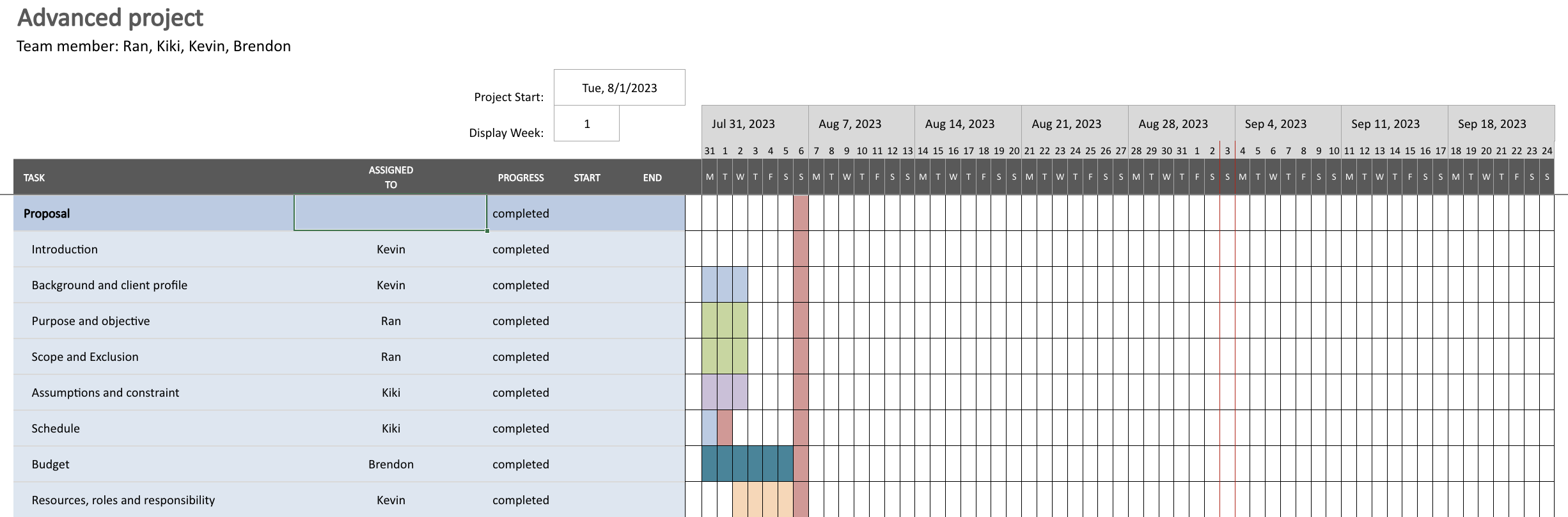
* Project Allocation Form
* Project Proposal
* System Analysis and Design Documentation
* Detailed documentation describing the encryption/decryption process.
* Project Evaluation Report including Software Testing
* Implementation of secure authentication mechanisms (e.g., OAuth2, JWT) within the application.
* Training materials, tutorials, and guides for developers, administrators, and stakeholders.
* E-Poster
* Source Code

# Schedule

The utilisation of a Gantt chart will prove to be pivotal strategy for managing our advanced research-oriented project. Employing a Gantt chart will involve visually mapping out task sequences and timelines, establishing a framework for well-structures and organised project execution.

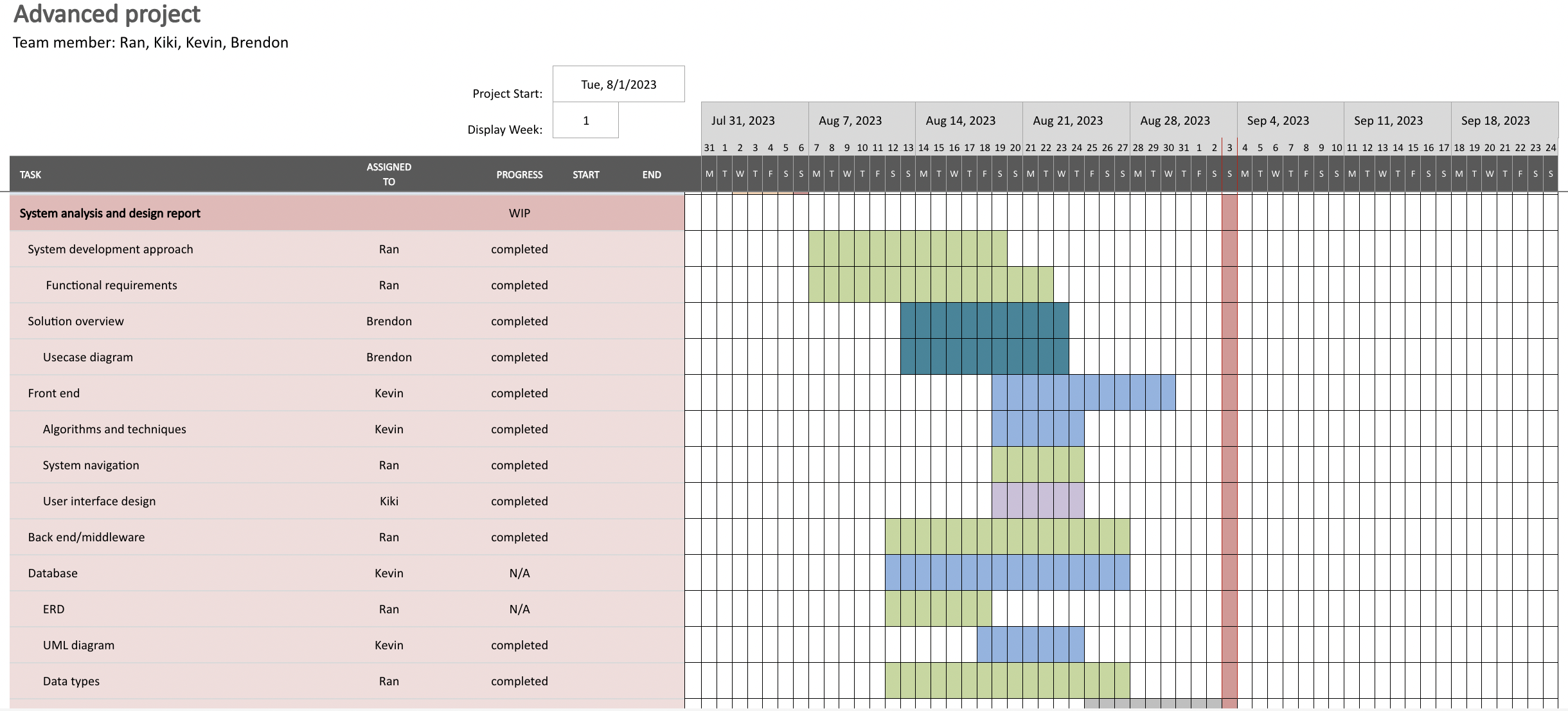
In this research project, we will structure around the research process three pivotal stages are illuminated as shown below:

**Phase 1:**



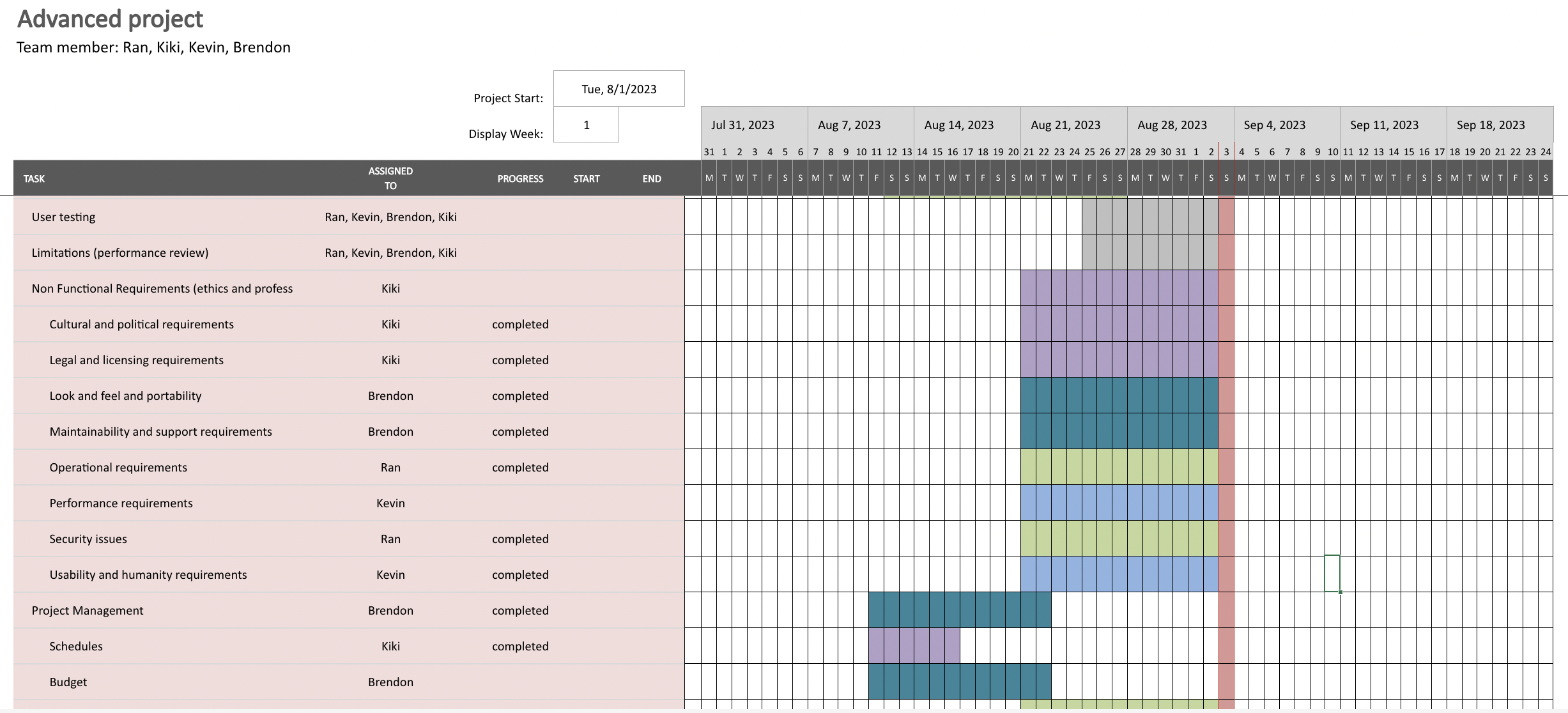
* Process one **(Proposal submission)**: This phase will establish the project’s foundation, encompassing introduction, background, client profile, objectives, budget, and resources requirements. Creating a Gantt chart here outlines the timeline for proposal development, aligning all essential components including setting up the required development environment for timely submission.

**Phase 2:**



* Proces two **(Technical implementation)**: Following supervisor approval, the project’s technical dimension will take precedence. Crafting a Gantt chart for this phase disaggregates technical tasks, optimises resources allocation, and averts potential bottlenecks.

**Phase 3:**



* Process three **(Final Delivery and Enhancement)**: The final phase’s Gantt chart will encapsulate delivery, improvements, ethical considerations, human factors, privacy safeguards, and the creation of a user manual. This comprehensive visualisation streamlines project finalisation, ensuring comprehensive task fulfilment before delivery.

Incorporating a Gantt chart into our advanced project will fosters seamless orchestration, elevating coordination, transparency, and successful project realisation throughout the project journey.

# Budget

Our professional fees for the web application development services referred to above is **$68,168.50**. The project duration is from the 7 August 2023 to 1 October 2023.

|  |  |  |
| --- | --- | --- |
| **Budget Category** | **Details** | **Cost** |
| **Software Licensing** | Data Encryption Software License | $0.00 |
|  | Additional Modules/Features | $0.00 |
| **Implementation and Integration** | Initial Setup and Configuration | $5000.00 |
|  | Integration with Existing Systems | $3000.00 |
| **Personnel Costs** | Project Manager x 1 | $16,667.00 |
|  | Developer x 1 | $13,334.00 |
|  | Data Analyst x 1 | $11,667.00 |
|  | Tester x 1 | $11,667.00 |
| **Training** | Training for IT Staff | $500.00 |
|  | End-User Training | $334.00 |
| **Hardware Costs** | for Compatibility | $200 Upgrades |
| **Support and Maintenance** | Annual Support Subscription | $1500.00 |
|  | Maintenance and Updates | $1500.00 |
| **Testing and QA** | Security Testing | $2500.00 |
| **Contingency** | Buffer for Unexpected Costs | 10% of Budget |
| **Total Estimated Budget** |  | **$68,168.50** |

# Resources Roles and Responsibility

|  |  |  |
| --- | --- | --- |
| **Resource** | **Role** | **Skill Set** |
| Ran | Developer/Data Analyst | .NET, MySQL, Tableau, Crystal Report |
| Le | Developer | .NET, C#, MySQL, JavaScript, ReactJS, IIS, HTML |
| Kiki | Product Manager/ Tester | Project Mangement, .NET, C#, MySQL, Github, AdobeXD |
| Brendon | Developer | .NET, C#, MySQL |

# Functional Requirements

The proposed project is a strategic initiative to bolster data security by implementing application layer encryption for both the front end and back end of a system. Utilizing a combination of Symmetric and Asymmetric keys, the project aims to create a secure environment where the Symmetric key is used to encrypt the payload, and Asymmetric keys are used to encrypt the Symmetric keys needed to decrypt the payload. This dual-layer approach ensures enhanced data integrity and confidentiality.

As a part of the project's demonstration, a corporate website has been developed to showcase the encryption process in action. The website includes key features such as a login page, an inquiry page, and a list of enquiries page. Each of these functionalities adheres to the project's encryption protocols, offering a seamless and secure user experience.

The following functional requirements detail the specific features and components that align with the project's objectives:

**Encryption System Functionalities:**

**Symmetric Key Encryption**

* The application shall use a Symmetric key algorithm to encrypt the payload data during transmission between the client and server.
* The application shall securely manage Symmetric keys, ensuring their appropriate usage and disposal.

**Asymmetric Key Encryption**

* The application shall utilize Asymmetric keys to encrypt the Symmetric keys used for payload decryption, enhancing the overall security.
* Asymmetric key pairs must be generated, stored, and managed securely, without exposing the private key.

**Corporate Website Functionalities:**

**Login Page**

* The application shall allow users to log in using an email and password, with credentials encrypted during transmission.
* The application shall provide appropriate error messages for incorrect login details and include measures to prevent unauthorized access.

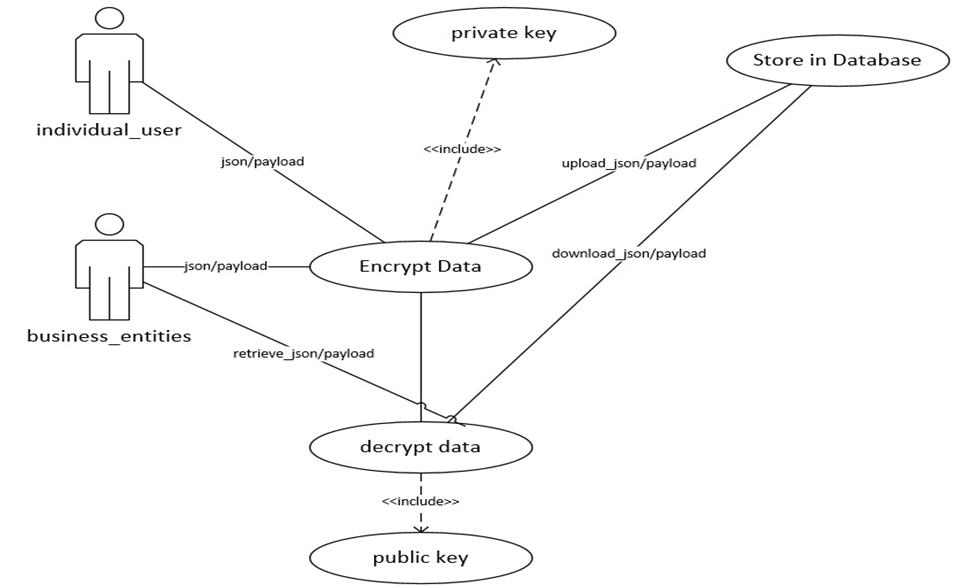
**Inquiry Page**

* Users shall be able to submit inquiries by providing their full name, email, mobile number, and inquiry details, with all sensitive data encrypted.
* The application shall provide a confirmation message upon successful submission of an inquiry.

**List of Inquiry Page**

* Authorized users shall be able to view a list of inquiries, with all displayed data decrypted securely for authorized viewing.
* Authorized users shall have the ability to search inquiries and view detailed information about each inquiry.

# Use Case Diagram



# Non-Functional Requirements

**Cultural and Political Requirements**

Cultural and political requirements for encryption involve balancing privacy, security, and lawful access. Respecting cultural norms, individual privacy, and freedom of expression is crucial. Likewise, fostering a culture of security awareness and responsible data use enhances national security. Encryption’s role in data protection and building consumer trust necessitates strong encryption practices and transparency.

Global cooperation is needed to establish common encryption standards, while research and innovation should prioritise security without compromising accessibility. Ethical discussions must address encryption’s impact on vulnerable populations. Prohibiting encryption backdoors and vulnerabilities maintains security integrity. Education campaigns should promote encryption awareness and digital literacy.

Cultural and political requirements for encryption and decryption encompass a range of factors that need to be considered to establish a comprehensive and effective framework:

1. Individual Privacy and Freedom of Expression:
   1. Cultural requirement: recognise and respect diverse cultural norms regarding privacy and personal autonomy. Different societies might have varying expectations about what constitutes private information.
   2. Political requirement: enact laws and regulations that protect individuals' rights to privacy and freedom of expression. Encryption should be available as a tool for individuals to secure their digital communications.
2. National security and law enforcement:
   1. Cultural requirement: foster a culture of security awareness and responsibility within society to mitigate risks associated with malicious use of encryption
   2. Political requirement: Establish mechanisms for lawful access to encrypted data in cases of legitimate national security concerns and criminal investigations. While safeguarding against abuse of power.
3. Data protection and consumer trust:
   1. Cultural requirements: encourage a cultural of data stewardship and responsible data use among businesses and individuals.
   2. Political requirement: implement and enforce data protection laws that mandate strong encryption practices to safeguard sensitive personal and corporate information, thereby enhancing consumer trust.
4. International cooperation and diplomacy:
   1. Cultural requirements: Promote cross-cultural understanding of the global importance of encryption for securing digital interactions.
   2. Political requirement: engage in international cooperation to establish common standards for encryption that balance security needs with individual rights, preventing fragmentation that could hinder global communication.
5. Transparency and accountability:
   1. Cultural requirement: foster a culture of transparency and accountability, encouraging individuals and organisations to be responsible for their actions.
   2. Political requirement: implement regulations that require companies to be transparent about their encryption practices, ensuring that users are informed about how their data is protected.

**Legal and Licensing Requirements**

Legal and licensing requirements covers a broad range of scope. The coverage of these requirements heavily depends on the nature of the business, or the type of industry, locations, and the type of activities that the business is engaged in. The legal and licensing requirements of Cyber Guardians, as a cyber security provider include but not limited to; Business structure and registration, industry-specific licenses and permits, professional licensing, intellectual property (IP) environmental regulations, data privacy and protection. The following explains each of those permits and licensing in details:

1. **Business structure and registration**

Under The Corporations Act 2001, Business in Australia must register prior to opening, registration involves a variety of things from drafting the right documents to registering Intellectual Property to comply with rules around taxes. A register business with an Australian Business Number (ABN) in the IT industry must also have:

1. ASIC company registration – Taking into consideration that Cyber Guardian is a proprietary limited company, Cyber Guardian will need to register with the Australian Securities and Investments Commission (ASIC).
2. Occupational Licenses – Employees who works at Cyber Guardians needs to obtain relevant certifications.
3. Industry-Specific Certification:

* Certified Information Systems Security Professional (CISSP)
* Certified Information Security Manager (CISM)
* Certified Ethical Hacker (CEH)

1. Compliance with the Privacy Act – If the company processes personal information, it is required to adhere to the provisions of the Privacy Act 1988. This may entail registering as an organisation conducting Privacy Impact Assessment (PIA) and adhering to the Australian Privacy Principles (APPs).
2. Australian Signals Directorate (ASD) certification – this would help Cyber Guardians to improve the cybersecurity practices.
3. Export and Import Controls – could help export and import of certain encryption technologies or cybersecurity software.
4. Intellectual Property Protection
5. Data Breach Notification Compliance

**Operational Requirements**

Below, you will find the detailed list of the minimum software requirements that are essential for the successful implementation and operation of the proposed project. These specifications have been carefully analyzed and selected to ensure compatibility, functionality, and performance. Meeting these requirements is crucial for the seamless execution of the project, and they have been chosen to align with the overall goals and objectives:

* + .NET Framework 4.5 (>= 4.8.1)
  + Internet Information Services (IIS) (>=8.0)
  + MySQL (=>8.0)

Our application was launched on Amazon Web Services (AWS), utilizing the following specific instances:

* + SSL (HTTPS) Protocol
  + Frontend – AWS App Runner (1 vCPU & 2 GB with auto scale)
  + Backend – AWS App Runner (1 vCPU & 2 GB with auto scale)
  + AWS RDS (db.t3.micro, 2vCPU, 1GB RAM, 20GB Storage)

# **Feel, Look and Portability**

The look and feel should incorporate the following attributes in the context of DataSafe Inc.'s new project to combat man-in-the-middle (MITM) attacks and improve data security.

**Professionalism -** DataSafe Inc.'s position as a pioneer in data encryption and cybersecurity should be reflected in the design's sense of professionalism and expertise. This can be accomplished by using refined typography, crisp lines, and a harmonious colour scheme.

**Modern and Innovative** - The design should follow current design trends to convey DataSafe Inc.'s dedication to cutting-edge technology. This might include visually appealing graphics that exude an air of innovation, minimalist layouts, and sleek user interface components.

**Trustworthiness** - Given the nature of the company, the design ought to inspire confidence and dependability. This trust can be built by utilising components like shield icons, secure padlocks, and other security-related visual cues.

**Consistency** - A unified and coherent experience for users is ensured by maintaining a consistent design across the entire project, including the website and any software interfaces. Consistency in UI elements, typography, and colour schemes promotes familiarity and usability.

**User-Centric** - The user experience should come first in the design. Users can interact with the technology clearly thanks to intuitive navigation, understandable labels, and readily available features.

**Portability** - It is essential to ensuring that their novel approach to combating MITM attacks can be easily integrated into a variety of scenarios and systems. Here is a solution for portability.

**Cross-Platform Compatibility** - It should be possible to use the solution on a variety of computers (desktops, laptops, and mobile devices) and operating systems (Windows, macOS, and Linux). The use of platform-independent technologies or the provision of native applications for each platform could be examples of this.

**APIs and Integration** - The solution should, where possible, provide APIs (Application Programming Interfaces) that make it simple to integrate it with other platforms, applications, or software systems. As a result, DataSafe Inc.'s technology can operate in perfect harmony with current tools.

**Cloud Readiness** - The solution can be easily deployed in cloud environments if it was created with cloud compatibility in mind. Users can access the technology anywhere thanks to its flexibility, which scales effectively to handle a range of workloads.

**Modularity** - The solution can be easily modified to fit various use cases by being divided into modular components. The flexibility of these modules ensures that the technology can handle a variety of problems.

**Scalability** - Scalability of the solution is necessary to support usage ranging from small businesses to large consumers. This could entail structuring the solution so that extra resources can be allocated as required.

**Usability and humanity requirements**

**Usability Requirements**

**Intuitive UI/UX** - The user interface must be easy to understand and use, even for users who are not tech-savvy. It should offer visual cues for encryption and decryption processes.

**Quick Encryption/Decryption** - The service should be capable of encrypting and decrypting data quickly, so as not to make the user wait too long.

**Accessibility** - Users should be able to easily encrypt and decrypt their data from multiple devices.

**Multi-Language Support** - Consider language localization for global reach.

**Minimal Interference** - The process of encrypting and decrypting should be seamless and minimally invasive in the user’s primary task.

**Help & Documentation** - Detailed guides and FAQs should be available to assist users.

**Error Handling** - Clear and helpful error messages should be displayed, guiding users on what went wrong and how to fix it.

**Humanity Requirements**

**User Consent** - Always get clear, informed consent from the user before any data is encrypted or decrypted.

**Transparency** - Users should be informed about what kind of data is being encrypted, where it's stored, and who has access to it.

**Compliance** - The service should comply with GDPR, HIPAA, or any other relevant data protection laws.

**Anonymity** - Make sure that user data is anonymous and can’t be traced back to the individual, unless absolutely necessary for the service.

**Recovery Options** - Users should have a means to recover encrypted data in case they forget their keys or passcodes.

**Audit Trails** - Keep a secure, immutable log of all encryption and decryption activities for auditing purposes.

**Non-Discrimination** - Ensure that the service is available to everyone, regardless of age, race, gender, etc.

**Environmental Impact** - Consider the energy consumption of the service, especially if it involves complex cryptographic algorithms, and aim for energy-efficient options.

# Maintainability and support requirements.

|  |  |
| --- | --- |
| **Aspect** | **Description** |
| Maintainability | **Modular Architecture:** Document the codebase in detail, including comments, descriptions of the algorithms, and usage guidelines. This makes the code easier for future developers to comprehend and modify. |
|  | **Version Control:** Utilise version control software such as Git. To track changes, communicate with team members, and quickly revert to earlier versions, if necessary, keep a repository for the project. |
|  | **Coding Standards:** Utilise version control software such as Git. To track changes, communicate with team members, and quickly revert to earlier versions, if necessary, keep a repository for the project. |
|  | **Testing infrastructure:** To ensure consistency across the codebase, enforce coding standards and best practises. This makes maintenance easier and lessens the chance of making mistakes. |
|  | **Bug Tracking**: Create a thorough testing framework for the proposed solution. To identify problems early in the development process, this includes unit tests, integration tests, and automated testing. |

|  |  |
| --- | --- |
| **Support Requirements** | **Description** |
| **User Support** | **Documentation:** To help users use the technology effectively, provide clear and thorough user documentation. Online resources, FAQs, and user manuals are some examples of this. |
|  | **Customer support:** Create channels so users can contact you with queries, grievances, or technical problems. To ensure a positive user experience, offer prompt and effective customer service. |
|  | **Feedback Collection:** To find areas for improvement, collect user feedback. This can assist in improving the technology based on the needs and difficulties of actual users. |
|  | **Regular Updates:** Release fixes, additions, and security upgrades to the solution on a regular basis. Notify users of updates and highlight changes in release notes. |
|  | **Compatibility Updates:** To make sure the solution continues to be compatible and useful, constantly check for and adjust to changes in underlying technologies (operating systems, browsers, etc.). |

|  |  |
| --- | --- |
| Maintenance and Support Tools | Description |
| **Issue Tracking System** | Use a bug tracking system (like JIRA or Bugzilla) to record, assign, prioritise, and monitor the progress of feature requests, bug fixes, and other tasks related to upkeep and improvement. |
| **Collaboration Tools** | Use collaboration tools (like Slack or Microsoft Teams) to help the development, support, and documentation teams communicate with one another. This guarantees effective information updates and sharing. |
| **Monitoring and Analytics** | Use monitoring tools to keep tabs on the system's usage patterns, performance, and potential problems. Analyse the information gathered to proactively address new issues and improve the solution. |
| **Automated Deployment** | Use automated deployment tool to make updates and patches more quickly available. This minimises human error and guarantees uniform deployments across environments. |

**Security Issues**  
Security issues are paramount in software systems. For the implementation of this project, we have taken comprehensive measures to address various security aspects, aligning our approach with industry best practices to ensure a robust and secure environment.

.NET Framework

* + Implemented Content Security Policy (CSP) to mitigate XSS attacks.
  + Regularly updated the .NET Framework for security enhancements.
  + Established strict input validation and sanitization to block malicious inputs.
  + Conducted regular security code reviews to identify and rectify potential vulnerabilities.
  + Integrated automated security scanning tools within the development pipeline.

MySQL

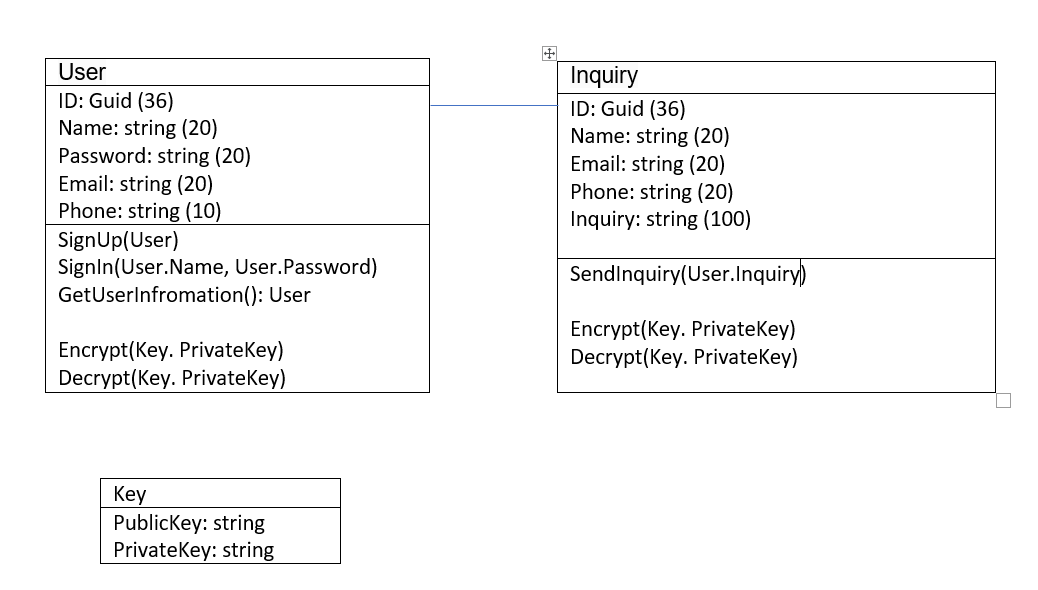
* + Utilized prepared statements to protect against SQL Injection.
  + Enforced strong password policies and two-factor authentication.
  + Implemented role-based access controls for granular security.
  + Encrypted sensitive data within the database.
  + Monitored and logged database activities for audit and anomaly detection.

AWS Deployment (including App Runner and RDS)

* + Crafted IAM roles with least privilege access to minimize risks.
  + Enabled encryption using AWS KMS and SSL/TLS for secure data handling.
  + Strategically configured security groups to limit exposure.
  + Regularly reviewed and rotated AWS access keys and credentials.
  + Implemented AWS CloudTrail for logging and monitoring AWS activities.

# UML Diagram and Data Types

This section outlines the UML diagram and data types within the database. Although the primary emphasis of the project is on encryption implementation, modules for login, inquiry, and inquiry listing have been developed to demonstrate the application of encryption security.



Inquiries

|  |  |
| --- | --- |
| **Field Name** | **Data Type** |
| Id | Char(36) - GUID |
| Email | Varchar(20) |
| Name | Varchar(20) |
| Phone | Varchar(10) |
| Email | Varchar(20) |
| Inquiry | Varchar(100) |

Users

|  |  |
| --- | --- |
| **Field Name** | **Data Type** |
| Id | Char(36) - GUID |
| Email | Varchar(50) |
| FirstName | Varchar(50) |
| LastName | Varchar(50) |
| Password | Varchar(150) |
| PasswordSalt | longblob |

# System Navigation and User Interface Design

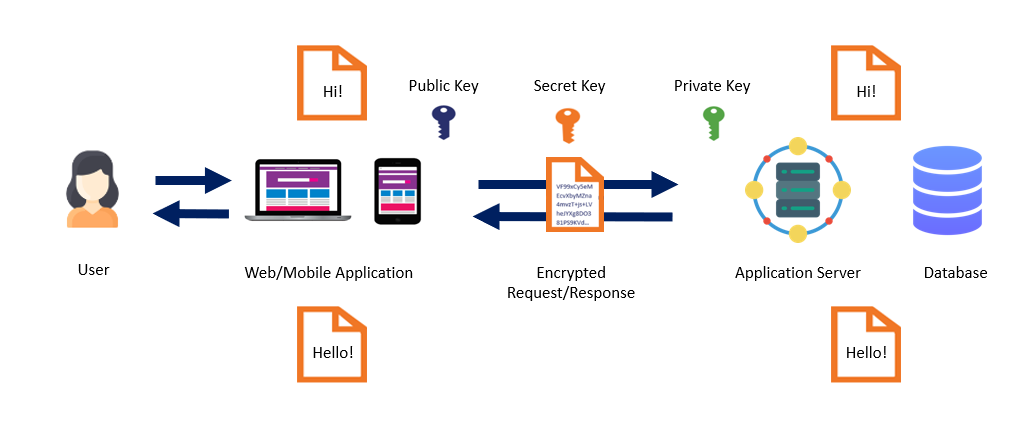


Figure 1 - shows the complete encryption process of system’s payload.

**Encrypting the Payload (API Request)**

* + Step 1 - Client-Side Symmetric Encryption. The client encrypts the payload (e.g., login credentials, inquiry details) using the static Symmetric key.
  + Step 2 - Client-Side Asymmetric Encryption. The Symmetric key itself is encrypted using the server's public key (Asymmetric encryption).
  + Step 3 - Transmission to Server. Both the encrypted payload and the encrypted Symmetric key are transmitted to the server.

**Decrypting the Payload (API Request)**

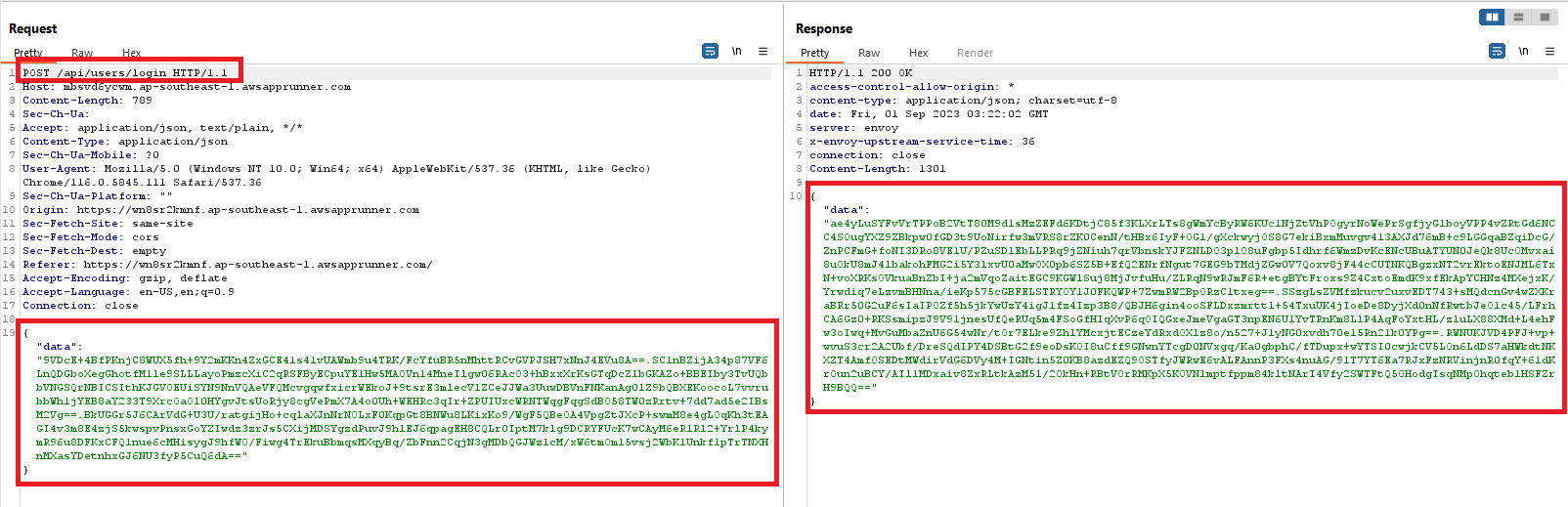
* + Step 1 - Server-Side Asymmetric Decryption. The server uses its private key to decrypt the encrypted Symmetric key.
  + Step 2 - Server-Side Symmetric Decryption. Using the decrypted static Symmetric key, the server decrypts the encrypted payload to process the request.

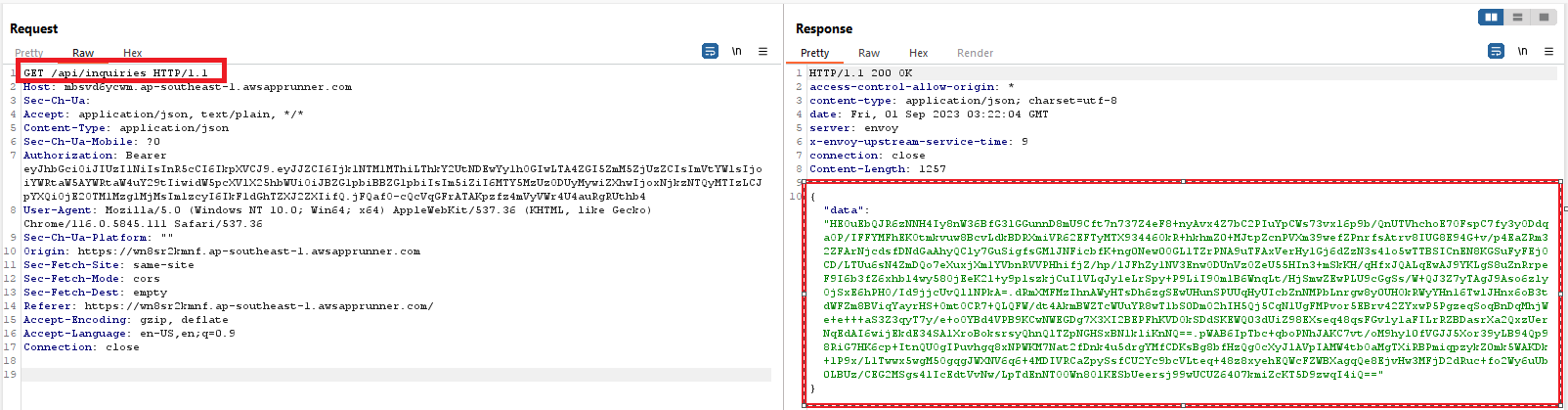
**Encrypting the Response (API Response)**

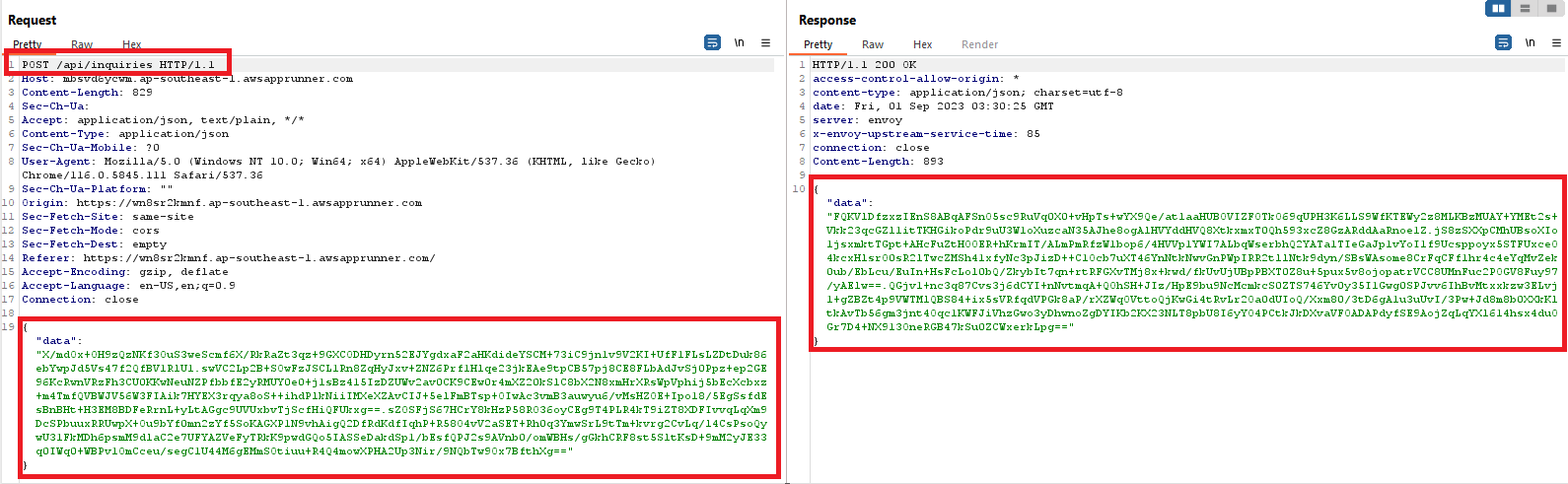
* + Step 1 - Server-Side Symmetric Encryption. The server encrypts the response data (e.g., inquiry results, confirmation messages) using the static Symmetric key.
  + Step 2 - Transmission to Client. The encrypted response is transmitted to the client.

**Decrypting the Response (API Response)**

* + Step 1 - Client-Side Symmetric Decryption. The client uses the static Symmetric key to decrypt the server's encrypted response.

Figure – 2 Preview of encrypted frontend request and backend response of login API.

Figure – 3 Preview of encrypted frontend request and backend response of list inquiries API.

Figure – 4 Preview of encrypted frontend request and backend response of submit inquiry API.

System Link: <https://wn8sr2kmnf.ap-southeast-1.awsapprunner.com>

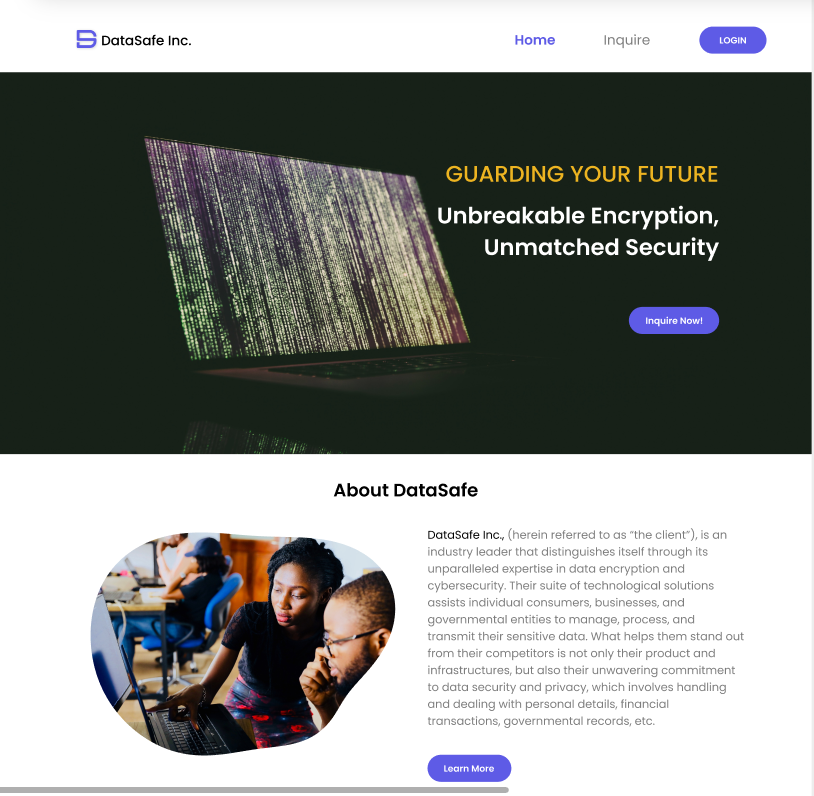
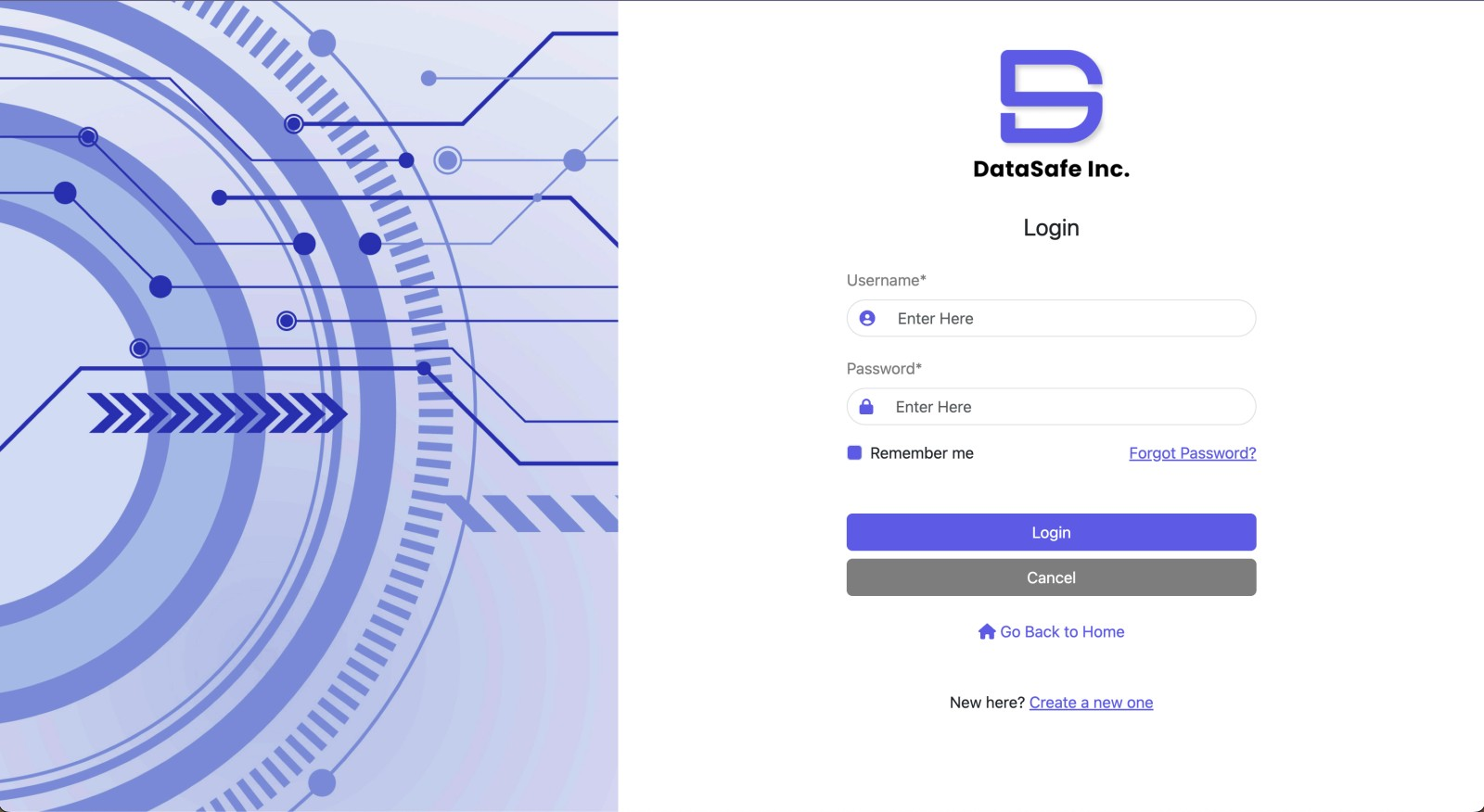


Figure – 5 Home Page

Figure – 6 Login

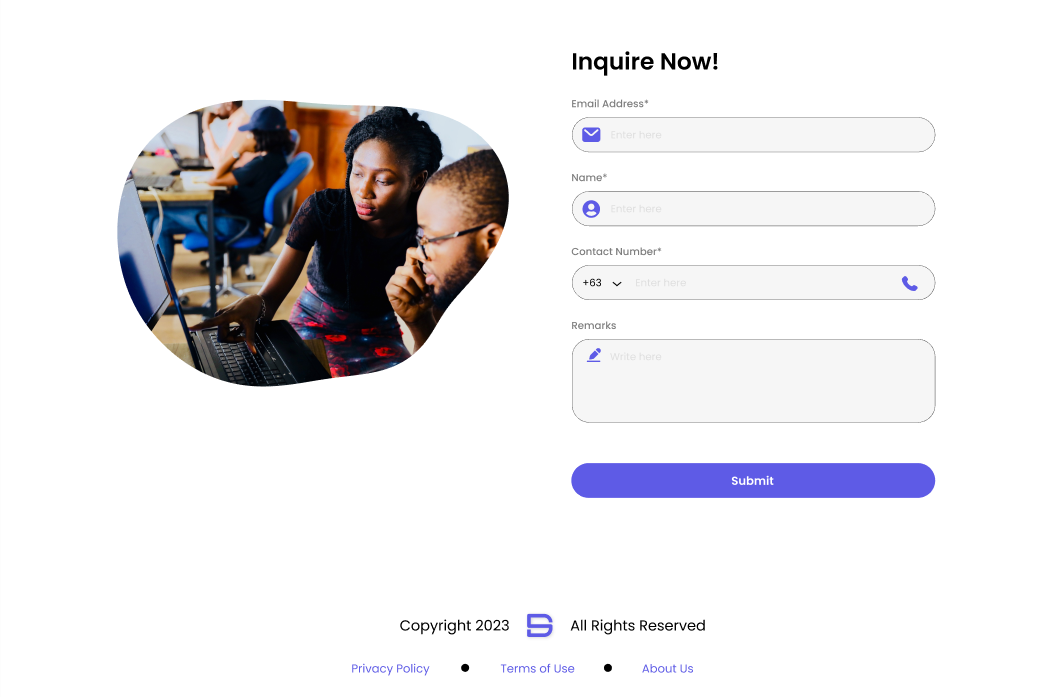
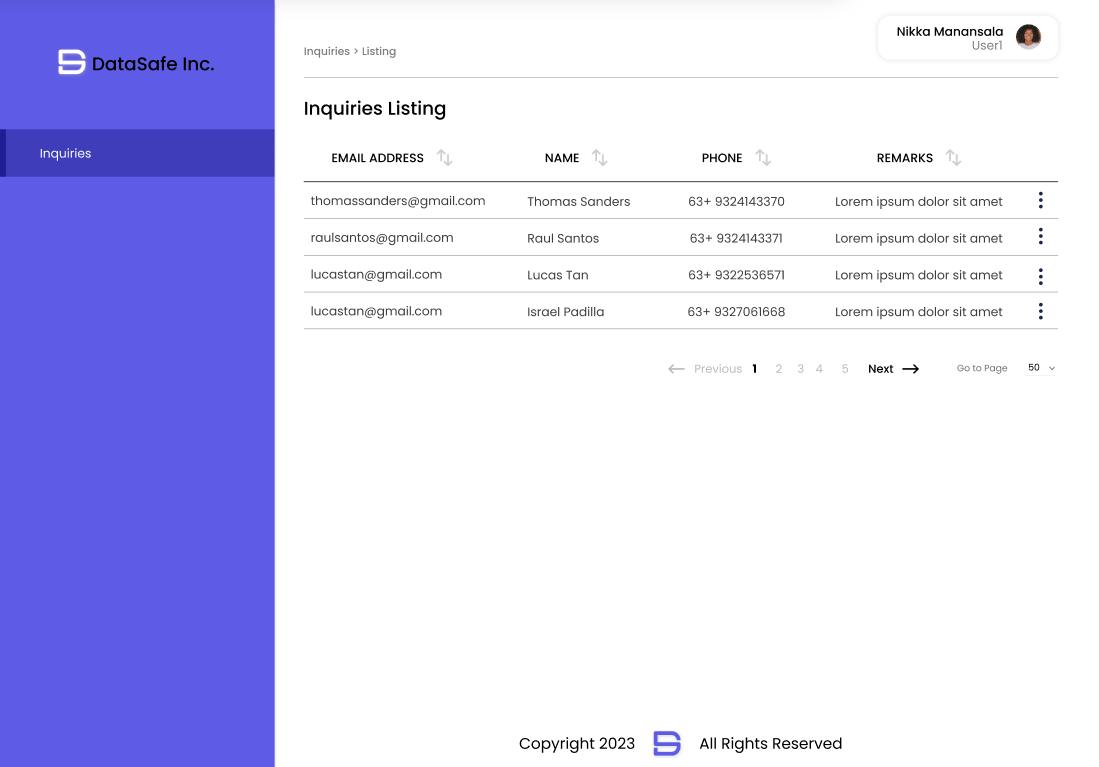


Figure 7 – Send Inquiry

Figure 8 – List of Inquiries

# Project Management

A thorough and strategic project management approach is necessary for DataSafe Inc.'s project to create a new technique to counter man-in-the-middle (MITM) attacks. With a focus on ensuring efficient project planning, execution, and monitoring in line with the business's reputation for top-notch technological services and dedication to data security.

**Project Initiation** - The scope, objectives, and anticipated results are all defined during the project's initiation phase. Experts in encryption, cybersecurity, software development, and system architecture make up the project team assembled by DataSafe Inc. The project manager is chosen to supervise the work and guarantee its success. To gather requirements and gain a clear understanding of the project's significance and objectives.

**Planning and Strategy** - The development of a thorough project plan that specifies the project's timeline, checkpoints, deliverables, and resource allocation. To find potential issues and risks connected to the creation of the new method, risk assessment is done. To deal with these risks, we define mitigation strategies. Together, the project manager and team develop a thorough plan that incorporates technical, operational, and communication elements.

Considering the nature of software development project which involves back and forth testing prio

**Requirement Analysis** - The project team worked to specify the precise specifications for the new approach. This includes determining the flaws and gaps in the current approaches that the new approach needs to fill. The team draws on the depth of cybersecurity and encryption expertise at DataSafe Inc. to make sure the new approach is in line with the company's reputation for excellence.

**Design and Development** - The project team starts designing the new method using the results of the requirements analysis. To ensure the method's efficacy and efficiency, close coordination is kept between cybersecurity experts, software developers, and encryption experts. Agile development methodologies can be used to accommodate changes and improvements as they happen. To make sure the project is proceeding according to plan, frequent progress reviews are carried out.

**Testing and Quality Assurance** - The project's critical phase involves rigors testing. To verify its functionality and security precautions, the developed method is put through a variety of testing scenarios, including simulated MITM attacks. To ensure that the procedure complies with the strictest requirements for cybersecurity and encryption, quality assurance procedures are put in place. Any problems are dealt with right away to guarantee a solid resolution.

**Deployment and Rollout** - The new approach is ready for deployment once it has successfully completed all testing phases. To ensure a seamless integration into the current infrastructure of DataSafe Inc., the project team coordinates with the appropriate teams. To make it easier for internal teams and clients to adopt the new method, thorough documentation and training materials are prepared.

**Monitoring and Evaluation** - Deployment does not mark the end of the project. The effectiveness, efficiency, and user satisfaction of the method are continuously monitored and evaluated. To update and improve the solution, real-world feedback and potential incidents are examined.

Strong lines of communication are kept open between team members, stakeholders, and management during every stage of the project. To guarantee openness and well-informed decision-making, regular status updates, progress reports, and risk assessments are shared.

**Risks**

Risk management serves as a pivotal tool in heightening our awareness and enabling the identification of potential risks within the project. It encompasses the assessment of the likelihood of adverse incidents occurring and the potential ramifications of such events. These consequences might manifest as financial losses, project delays, or diminished performance. A crucial aspect of this process is the risk rating, which quantifies the severity of a risk by combining its probability and potential impact, allowing for a structured approach to prioritizing and addressing each identified risk.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Name** | **Description/Cause** | **Owner** | **Impact** | **Probability** |
| New Technology Adoption | Current staff may resist adopting new technology due to long-standing habits. | Staff | High | High |
| Data Breach | Unauthorized access to encrypted data due to vulnerabilities in the encryption process. | DataSafe Inc. | High | Medium |
| MITM Attacks | Cyber attackers intercepting data during transmission despite encryption. | DataSafe Inc. | High | Medium |
| Key Mismanagement | Loss or unauthorized access to encryption keys, compromising the integrity of encrypted data. | IT Admin | High | Medium |
| Regulatory Non-compliance | The encryption methods or data handling might not meet certain regulatory or compliance standards. | Legal Team | High | Low |
| Inadequate Staff Training | Staff unfamiliar with the new encryption system, leading to operational inefficiencies and potential security breaches. | Staff | Medium | High |
| System Downtime | Unexpected system outages due to technical issues, affecting user accessibility and experience. | IT Admin | Medium | Medium |
| Software Incompatibility | Current systems may not be fully compatible with the new encryption methods, leading to integration issues. | Development Team | Medium | Medium |
| Third-party Service Vulnerabilities | Relying on third-party services or APIs that might have their own set of vulnerabilities. | Third-party Vendor | Medium | Medium |
| Budget Overrun | Project costs exceeding the allocated budget due to unforeseen complexities or additional requirements. | Project Manager | Medium | Low |

# References

* 知乎专栏. (n.d.). *如何将Kali Linux秒变成一个能够拦截网络流量的代理路由器*. [online] Available at: <https://www.zhihu.com/column/p/29260111> [Accessed 3 Sep. 2023].
* Microsoft. (n.d.). *What is .NET Framework? A software development framework.* [online] Available at: <https://dotnet.microsoft.com/en-us/learn/dotnet/what-is-dotnet-framework>.
* Wikipedia. (2023). *React (software)*. [online] Available at: <https://en.wikipedia.org/wiki/React_(software>).
* B., R. (2018). *What is MySQL: MySQL Explained for Beginners*. [online] Hostinger Tutorials. Available at: <https://www.hostinger.com/tutorials/what-is-mysql>.
* www.solarwinds.com. (n.d.). *What Is IIS (Internet Information Services) and How Does It Work? - IT Glossary | SolarWinds*. [online] Available at: https://www.solarwinds.com/resources/it-glossary/iis-server.
* Application Level Encryption for Software Architects. (2021). *InfoQ*. [online] 23 Jan. Available at: <https://www.infoq.com/articles/ale-software-architects/>.
* Agrawal, M. and Mishra, P. (n.d.). *A Comparative Survey on Symmetric Key Encryption Techniques*. [online] Available at: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=20f3dd8943a17138c3eefa4258aa1b6837ffcb59>.
* Cryptography Stack Exchange. (n.d.). *public key - Why is hybrid encryption more effective than other encryption scheme?* [online] Available at: <https://crypto.stackexchange.com/questions/31234/why-is-hybrid-encryption-more-effective-than-other-encryption-scheme>.
* ‌ Verma, K. (2019). *Symmetric, Asymmetric and Hybrid Encryption*. [online] Medium. Available at: <https://54m4ri74n.medium.com/symmetric-asymmetric-and-hybrid-encryption-25d57c1c327b>.
* ‌ DEV Community. (n.d.). *What is application-level encryption and why it’s not TLS*. [online] Available at: <https://dev.to/cossacklabs/what-is-application-level-encryption-and-why-its-not-tls-49hb>.