# Software Requirements Specification

**for**

# Advanced Onion Encryption Standard

**Version 3.0 approved**

**Prepared by – Vatsal Sutariya (202001027)**

**Vidhi Ahir (202001195)**

**DAIICT**

**30 April,2023**

# Table of Contents


Error! Bookmark not defined.

# Revision History

| Name | Date | Reason For Changes | Version |
|---|---|---|---|
| Initial | 17-04-23 | Adding the purpose, Basic Information and Description | 1.0 |
| Update | 23-04-23 | Adding External Interface and Features | 2.0 |
| Final | 30-04-23 | Adding Non-Functional Requirements and final Proof Reading | 3.0 |

# 1. Introduction

AOES is an algorithm based on the concept of hiding the key through layers of different encryption methods, hence it's mainly a new conceptual algorithm developed by us, this software is made only for showing the very basic implementation of our algorithm.

## 1.1 Purpose

Hackers are mainly intended to hack the financial data for the money. AOES is mainly designed for generating the encrypted data file of the real financial data, so that user can send that encrypted data through this system without any threat of hacking on the channel on which it is being passed.

## 1.2 Document Conventions

For maintaining the consistency and clarity throughout the SRS document, there are some conventions used as follows:

**Acronyms:**

- AOES: Advanced Onion Encryption Standard
- DES: Data Encryption Standard
- AES: Advanced Encryption Standard

## 1.3 Intended Audience and Reading Suggestions

The intended audience for this SRS is the organizations dealing with financial data.

## 1.4 Product Scope

The features and functionalities of this AOES helps the bank servers to send the risky information safely. Moreover, It also increases the reliability of data sender and receiver.

# 2. Overall Description

## 2.1 Product Perspective

The AOES is an algorithm developed by us which is implemented in this software. The needs of this AOES system can vary depending upon its use, but we have mainly designed it for securing financial data.

## 2.2 Product Functions

- **Encryption**: This system will encrypt the given entered text using AOES and will show the encrypted text.

- **Decryption**: This system also decrypt the text which was encrypted using AOES and will show the decrypted text.

## 2.3 User Classes and Characteristics

- **Sender:**
  Any person who wants to send the data privately without any security risk, can encrypt the data from this website and then he/she can send it over channel.

- **Receiver:**
  If sender sends the encrypted data to the receiver then he/she can decrypt the same data from this site.

## 2.4 Operating Environment

The AOES is designed to run on any web-based platform that can be accessed via a standard web browser with internet connectivity. The system can be run on any operating system that supports a web-based platform like windows, MacOS or Linux.

## 2.5 Technologies Used

**Front-end Development**: HTML, CSS, JavaScript
**Back-end Development**: Node JS, Express JS

## 2.6 User Documentation

Website Link: https://aoes-cryptosystem-app.onrender.com
Demo Video: https://www.youtube.com/channel/UCWMQNThN17UGx2pM5jK62zQ

## 2.7 Assumptions and Dependencies

The software assumes that the user is using private and secure internet connection and operating system. It also assumes that the user has efficient network connection and also a compatible web browser to access the system. It also assumes that the user has a basic knowledge about the technical aspect.

The software depends on the third-party technologies, which has to be available and accessible for the system hence it can function properly. The system may also depend on the availability and responsiveness of technical support to assist users with any kind of questions that may arise while using it.

# 3. External Interface Requirements

## 3.1 User Interfaces

**General Encryption-Decryption Interface**:

This Interface allows the user to encrypt or decrypt the data using AOES methodology. It will show the result of the same i.e. Encrypted or Decrypted resultant text.

**Banking Application**:
For banking information, the system will encrypt the banking details i.e. Name, Card number, Expiry date, CVV code etc. using AOES.
These Information can be decrypt at the destination using AOES.

## 3.2 Hardware Interfaces

The system can be run on any operating system supporting a web-based platform like Windows, MacOS, Linux or Android with internet connectivity.

## 3.3 Software Interfaces

**Operating System:**
AOES can be run on an operating system that is compatible with the software used to develop this system. The operating system should meet the performance and security specified by the AOES.

**Web Browsers:**
The AOES can be accessed through web browsers, Hence the system should be compatible with popular web browser like Google Chrome, Mozilla Firefox, and Microsoft Edge.

## 3.4 Communications Interfaces

**Web Browser:** The system will require a web browser to access the AOES. With the user friendly interface, it will support all major web browsers like Google Chrome, Mozilla Firefox, and Microsoft Edge.

# 4. System Features

## 4.1 General Encryption:

### 4.1.1 Description and Priority

This feature allows the user to encrypt any kind of data. The priority of this feature is high.

### 4.1.2 Stimulus and Response

Stimulus: The user clicks on the Encrypt button on the Home page.
Response: The system asks the user to enter the data which is needed to be encrypted by AOES.

Stimulus: The user enters the data in the text box and click on submit.
Response: The system shows the confirmation message which says “successfully encrypted” and also shows the encrypted text in the same dialogue box.

### 4.1.3 Functional Requirements

REQ-1: The system should provide the home page to the user.
REQ-2: The system should redirect the user to home page after successful Encryption.

## 4.2 General Decryption:

### 4.2.1 Description and Priority

This feature allows the user to decrypt any kind of data which was before encrypted using AOES. The priority of this feature is high.

### 4.2.2 Stimulus and Response

Stimulus: The user clicks on the Decrypt button on the Home page.
Response: The system asks the user to enter the data which is needed to be decrypted and this data must be encrypted beforehand using AOES.

Stimulus: The user enters the data in the text box and click on submit.
Response: The system shows the confirmation message which says “successfully decrypted” and also shows the decrypted text in the same dialogue box.

### 4.2.3 Functional Requirements

REQ-1: The system should provide the home page to the user.
REQ-2: The system will show an error message of invalid input if the entered data is not encrypted using AOES.
REQ-3: The system should redirect the user to Home page after successful Decryption.

## 4.3 Banking details Encryption:

### 4.3.1 Description and Priority

This feature allows the user to encrypt the bank details. The priority of this feature is high.

### 4.3.2 Stimulus and Response

Stimulus: The user clicks on the bank details from the menu-bar on the home page.
Response: The system redirects the user to the banking details page

Stimulus: The user enters the bank details and click on submit
Response: The system shows the confirmation message which says “successfully encrypted” and also shows the encrypted text in the same dialogue box.

Note: the user can copy this encrypted data and paste it into the general decryption to get back the details which he/she entered.

### 4.3.3 Functional Requirements

REQ-1: The system should provide the bank details page to the user.
REQ-2: The system should show an encrypted text when user clicks on submit button.

# 5. Other Nonfunctional Requirements

## 5.1 Performance Requirements

The system should be able to manage the traffic of the users simultaneously. The system should respond quickly to user requests and should have less processing time.

## 5.2 Safety Requirements

**5.2.1 Data Privacy:** The data entered in the system should be confidential and should only be known by the owner of the system.

## 5.3 Security Requirements

The system should be secured with different level of security as per the user's need.

## 5.4 Software Quality Attributes

**5.4.1 Maintainability:** The software should be easy to maintain and update, with clear and well documented codebase, and the ability to quickly identify and fix issues.

**5.4.2 Portability:** The software should be able to run on different platforms and operating system without significant modifications**.**

**5.4.3 Usability:** The system should be user-friendly and easy to use, with clear instructions and quick feedback.

**5.4.4 Reliability:** The system must be available all the time, with the minimum amount of disruption or downtime.

## 5.5 Business Rules

**5.5.1 Data Access:** Only reliable and authorized person should have access to the encrypted or decrypted text.

**5.5.2 System Access**: Only the reliable organization should have access and knowledge of this system and it should not be known by other organizations.