Project Report on

BetterCrypt

(Data Encryption System - AES with Complement)

BACHELOR OF TECHNOLOGY IN

COMPUTER SCIENCE

SUBMITTED BY

Sayan Sahu - 19070122150

Sharath B Pai - 19070122155

Shubhankar Haldia - 19070122166

Under the Guidance of

PROF. POOJA BAGANE

SYMBIOSIS INSTITUTE OF TECHNOLOGY

(A CONSTITUENT OF SYMBIOSIS INTERNATIONAL UNIVERSITY)

Pune - 412115

2021-22

Software Requirement Specification

Table of Contents **..**

1. Introduction 4

1.1 Purpose 4

1.2 Document Conventions …... 4

1.3 Intended Audience and Reading Suggestions 4

1.4 Product Scope 4

1.5 References 5

2. Overall Description 5

2.1 Product Perspective 5

2.2 Product Functions 5

2.3 User Classes and Characteristics 6

2.4 Operating Environment 6

2.5 Design and Implementation Constraints 6

2.6 Process Model 6

2.7 Assumptions and Dependencies 7

3. Functional Requirements 8

3.1 Encrypt / Decrypt selection 8

3.2 Data selection 8

3.3 Encryption Bit Size Selection 8

3.4 Secret Key Selection 8

3.5 Confirm the Encrypt/Decrypt Operation 9

3.6 Exit 9

4. Other Nonfunctional Requirements 9

4.1 Performance Requirements 9

4.2 Safety Requirements 9

4.3 Security Requirements 9

4.4 Software Quality Attributes 9

5. Analysis Models 10

5.1 Use-Case Diagram 10

5.2 Class Diagram 11

5.3 ER Diagram 12

Conclusion and Future Scope.. 13

1. Introduction

1.1 Purpose

This document provides all of the requirements for the BetterCrypt. Sections 1 and 2 are intended primarily for customers of the application, but will also be of interest to software engineers building or maintaining the software. Section 3 is intended primarily for software engineers, but will also be of interest to customers.

1.2 Document Conventions

- References are mentioned throughout the document in square bracket (e.g. [1])
- 'Heading 1' is used for top level heading of main sections.
- 'Heading 2' is used for subsection heading.
- URLs are metalinked from the document. Ctrl-Click them to open hyperlink.

1.3 Intended Audience and Reading Suggestions

This is a cryptographic application that is usable by all classes of users (who need to secure their data).

This document is mainly intended to be used by the development team, project managers, marketing staff, testers, documentation writers. The SRS has been organised approximately in the order of increasing specificity.

1.4 Product Scope

1. This document covers the requirements for release 0.1 of BetterCrypt. Mention will be made throughout this document of selected probable features of future releases. The purpose of this is to guide developers in selecting a design that will be able to accommodate the full-scale application.

2. Using this Software you can easily encode your data in encrypted form. This

software is necessary for your sensitive files and document.

3. In this software you can choose a text/image file, secret key and then the file will be encrypted.

4. Through the software the other person can decrypt the file with the help of the secret key .

1.5 References

1. **https://howtodoinjava.com/java/java-security/java-aes-encryption-example/**
2. **https://www.baeldung.com/java-aes-encryption-decryption**
3. **https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm**
4. **https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard**

2. Overall Description

2.1 Product Perspective

This project will have two interfaces for encrypting and decrypting a file respectively. It is implemented in java. It's a web based software, technical and non-technical people can also use this software very easily. This software is made in Java latest version 8.0.

2.2 Product Functions

The function will provide following functionality:-

1. Open the web application in a preferred web browser.

2. It provides an interface on which the end user enters their text or image file along with the secret key. Then the given data is changed in encrypted form.

3. It also provides an interface on which the end user enters the encrypted file along with the secret key. Then the given encrypted data is decrypted.

2.3 User Classes and Characteristics .

This is a generic cryptographic application that is usable by all classes of users (who need to secure their data) with any level of technical expertise, education and experience. This suite is usable both for novice or non-technical users as well as expert technical users.

2.4 Operating Environment

BetterCrypt, being a web application, is intended to be operating system independent. Therefore no specific operating system is excluded. It is also platform independent. Therefore no specific hardware is excluded.

2.5 Design and Implementation Constraints .

Constraints:

1. There is no provision for the sender (who encrypts the file and generates the secret key) to send the secret key to the receiver. The receiver has to manually enter the secret key to decrypt the file.

2.6 Process Model

Incremental Process Model is used to develop our project. The model combines the elements of the waterfall model with the iterative philosophy of prototyping. New features and maintenance of the waterfall model will be developed timely. We are using this process model as with every linear increment addition of new features to the software will help in development of the software. Hence we are using this model as it is more flexible. Also it is easy to test and debug the software through this model.

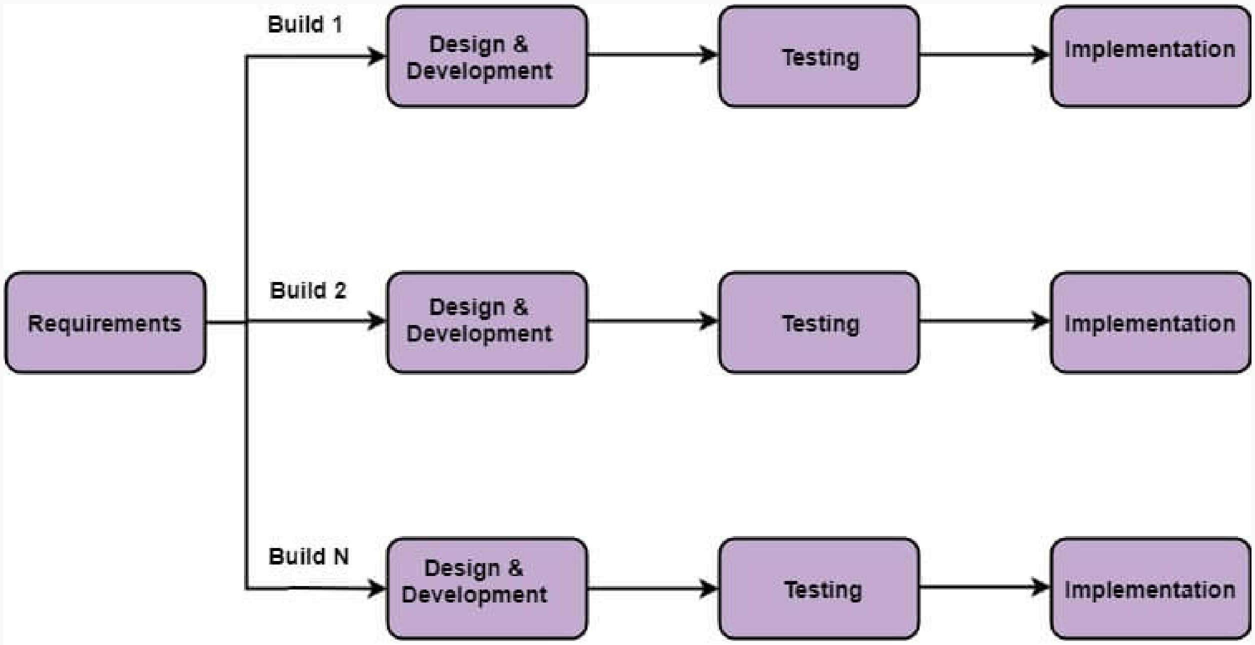


Fig: Incremental Model

2.7 Assumptions and Dependencies

Dependencies:

1. The user must have an active internet connection.
2. The web browser has javascript enabled.

Assumptions:

1. It is assumed that only the sender and receiver has access to the secret key to encrypt and decrypt the file.

3. Functional Requirements

This subsection represents the functional requirements of the software. The general functional requirements pertaining to the software are given below.

3.1 Encrypt / Decrypt selection

3.1.1 Refinement of Requirement 1:

Input: Selection from the 2 options:

1. Encrypt
2. Decrypt

Output: Display selected web page

3.2 Data selection

3.2.1 Refinement of Requirement 2:

Input: Selection from 2 options:

1. Text
2. Image

Output: Get required input from the user

3.3 Encryption Bit Size Selection

3.3.1 Refinement of Requirement 3:

Input: Selection from the 3 options:

1. 128 bit
2. 192 bit
3. 256 bit

Output: Encryption Bit Size is selected

3.4 Secret Key Selection

3.4.1 Refinement of Requirement 4:

Input: Selection from 2 options

1. User defined secret key
2. Random secret key generated by the website

Output: Secret key is selected

3.5 Confirm the Encrypt/Decrypt Operation

3.5.1 Refinement of Requirement 5:

Input: Press the encrypt/decrypt button

Output: The encrypted/decrypted output is displayed

3.6 Exit

3.6.1 Refinement of Requirement 6:

Input: Press exit button

Output: The user’s data is removed from the website.

4. Other Nonfunctional Requirements

4.1 Security Requirements

Any uploaded file or any secret key being used is not stored anywhere to protect the privacy of the user.

4.2 Software Quality Attributes

4.2.1 Portability

As our program runs on a website, it can be easily accessed through any OS.

4.2.2 Availability

The website will be up 24/7 for complete availability to any user at any time.

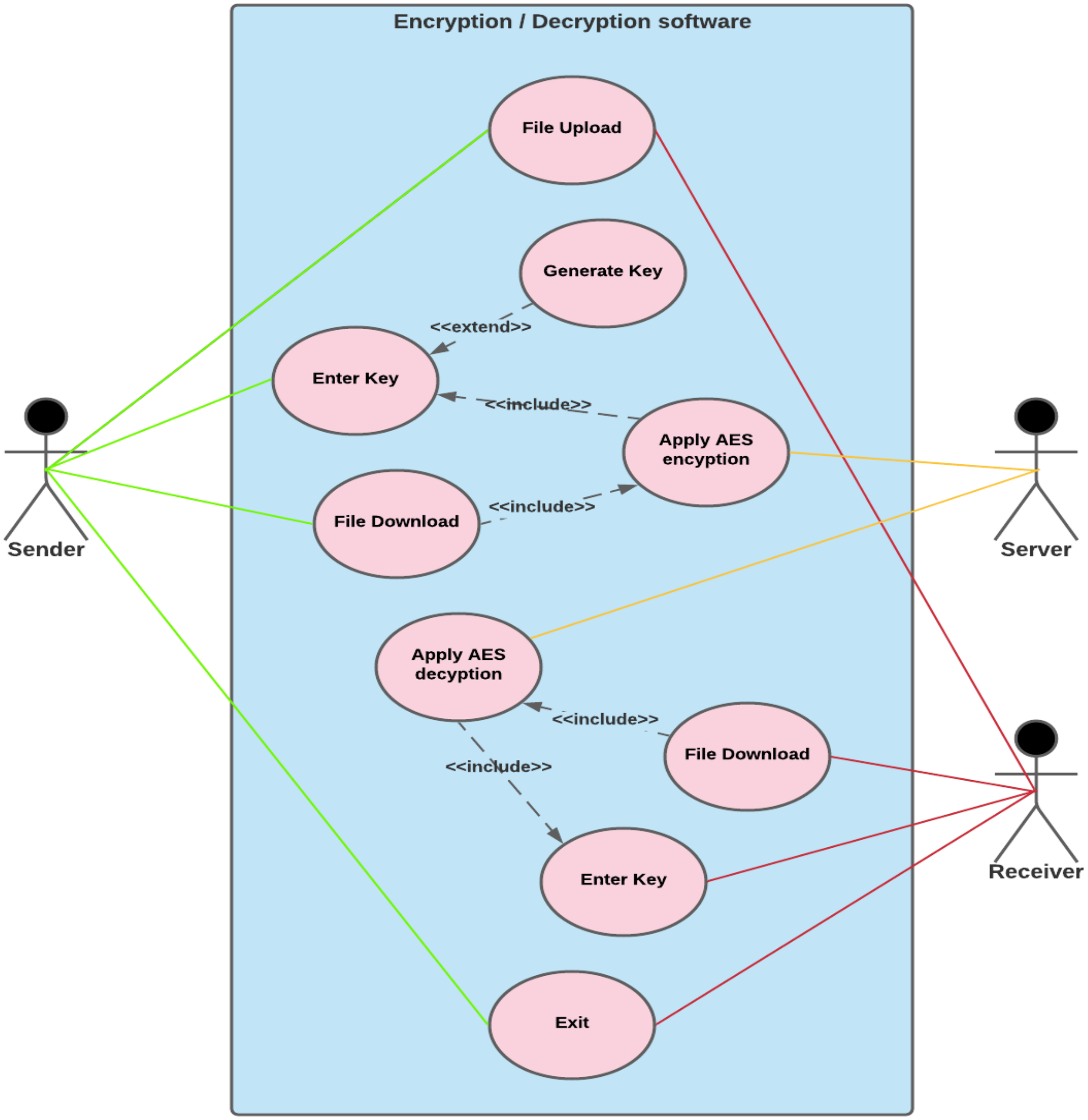
4.2.3 Usability

Anyone can easily understand and use our website.

5. Analysis Models

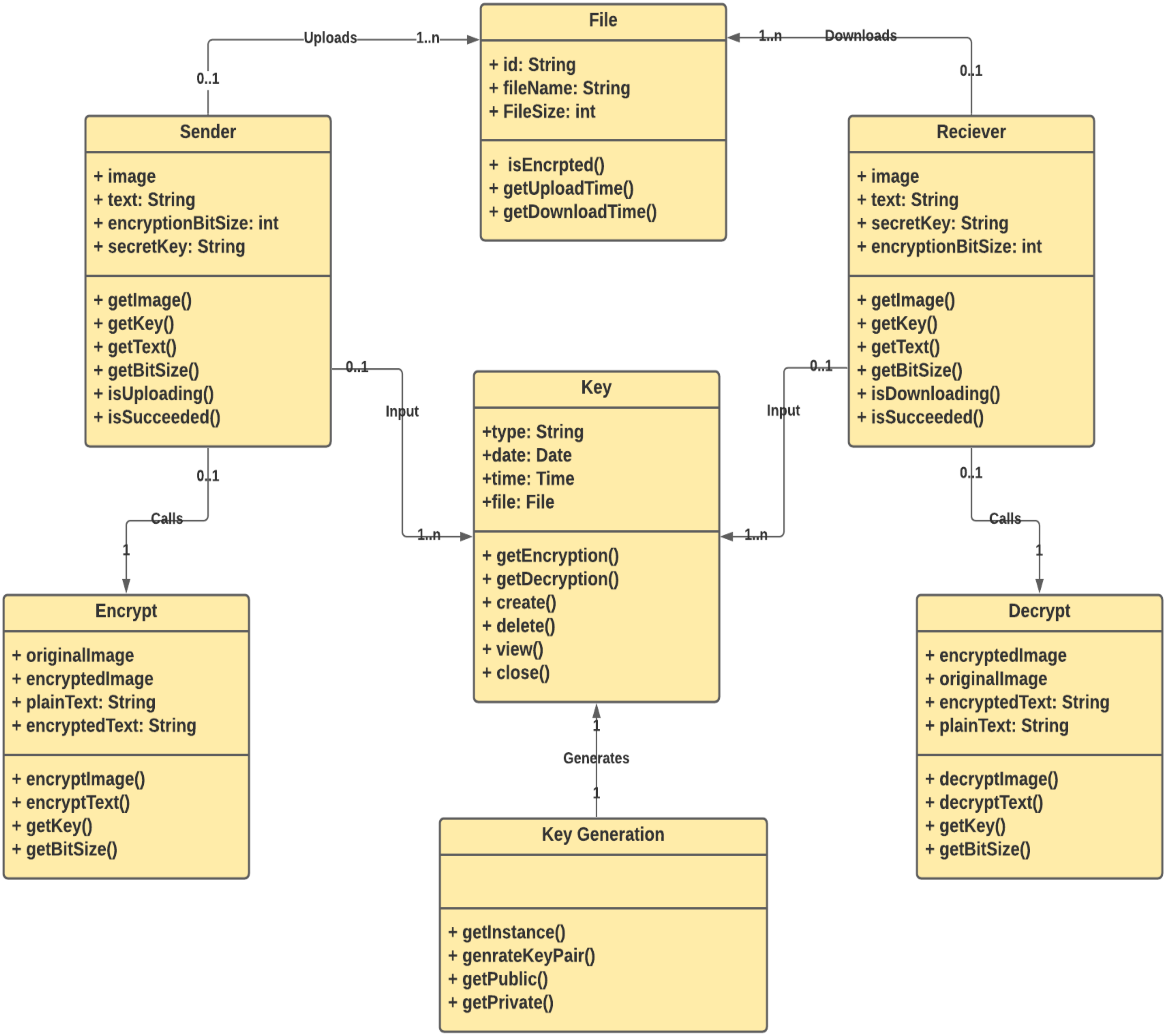
5.1 Use-Case Diagram

Use case diagrams are usually referred to as behavioral diagrams used to describe a set of actions (use cases) that some system or systems (subject) should or can perform in collaboration with one or more external users of the system (actors). Each use case should provide some observable and valuable result to the actors or other stakeholders of the system.



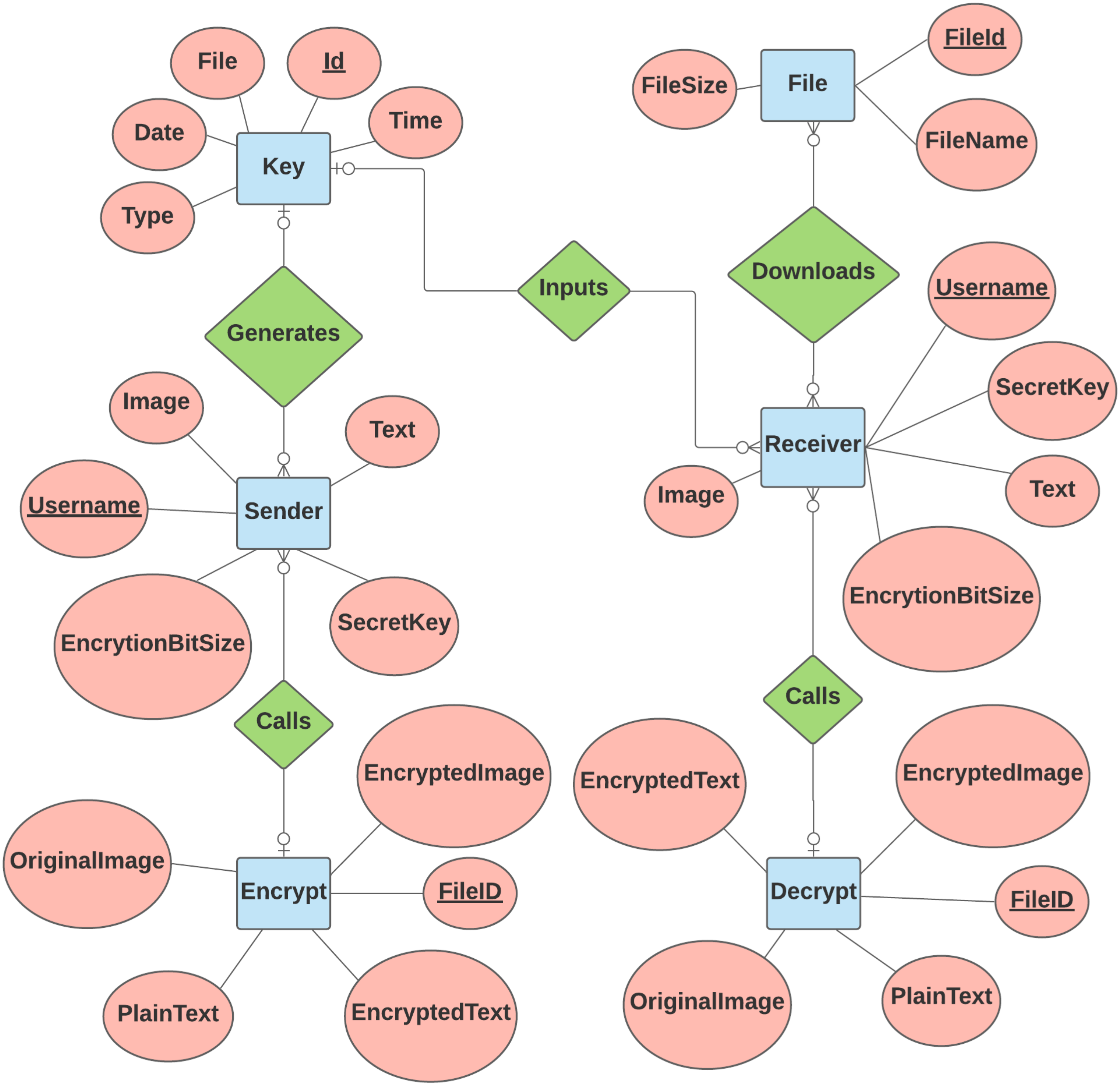
5.2 Class Diagram

A class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects.



5.3 ER Diagram

An entity–relationship model (or ER model) describes interrelated things of interest in a specific domain of knowledge. A basic ER model is composed of entity types (which classify the things of interest) and specifies relationships that can exist between entities (instances of those entity types). Here the underlined attributes are the primary keys.



Conclusion and Future Scope

We know of security of information to be a hot topic since, well, forever. We entrust our personal and sensitive information to lots of major entities and still have problems with data breaches, data leaks, etc. Some of this happens because of security protocols in networking, or bad practices of authentication management — but, really, there are many ways that data breaches can occur. However, the actual process of decrypting a ciphertext without a key is far more difficult. For that, we can use the encryption algorithms like AES and the secure keys to secure our data.

The software uses AES with compliment encryption algorithm to encrypt the data. It helps in encrypting sensitive data, which can later be sent securely across any network and decrypted by the receiver.

In future the website can be made to transfer encrypted files from the sender to the receiver.

Also, along with the existing encryption algorithms the website can implement other encryption algorithms.