# ATTRIBUTE – BASED EXPRESSIVE AND RANKED KEYWORDS SEARCH OVER ENCRYPTED DOCUMENTS IN CLOUD COMPUTING

Ms.Yogapriya Vadivel

UG Scholar

AUTHOR: Sundari S, Ananthi M

AUTHOR: Sundari S, Ananthi M
AUTHOR: Sundari S, Ananthi M

## Abstract

To ensure information security, the information proprietor necessities to check the respectability of information put away somewhat in the server with the public examining method. Notwithstanding, the evaluation result will be invalid assuming the information has been adjusted progressively in the course of information anonymization while sharing information with other people with delicate data. In existing arrangements, an information sensitive is expected to anonymize the information and change the mark. Notwithstanding, such information sensitive data present new security chances, and the static unknown procedure isn't adaptable to various application situations. Subsequently, we propose another plan in light of the redactable signature. In our proposed plot, the server can change the mark straightforwardly without the extra sanitizer while sharing delicate information. The marked change doesn't impact the trustworthiness checking of the put-away information. The mark not exclusively can be utilized to validate the wellspring of sharing information, yet can likewise be used to take a look at the trustworthiness of the put-away information in the cloud. Both the security confirmation and exploratory examination show that our proposed plot is secure and more effective than the current plans.

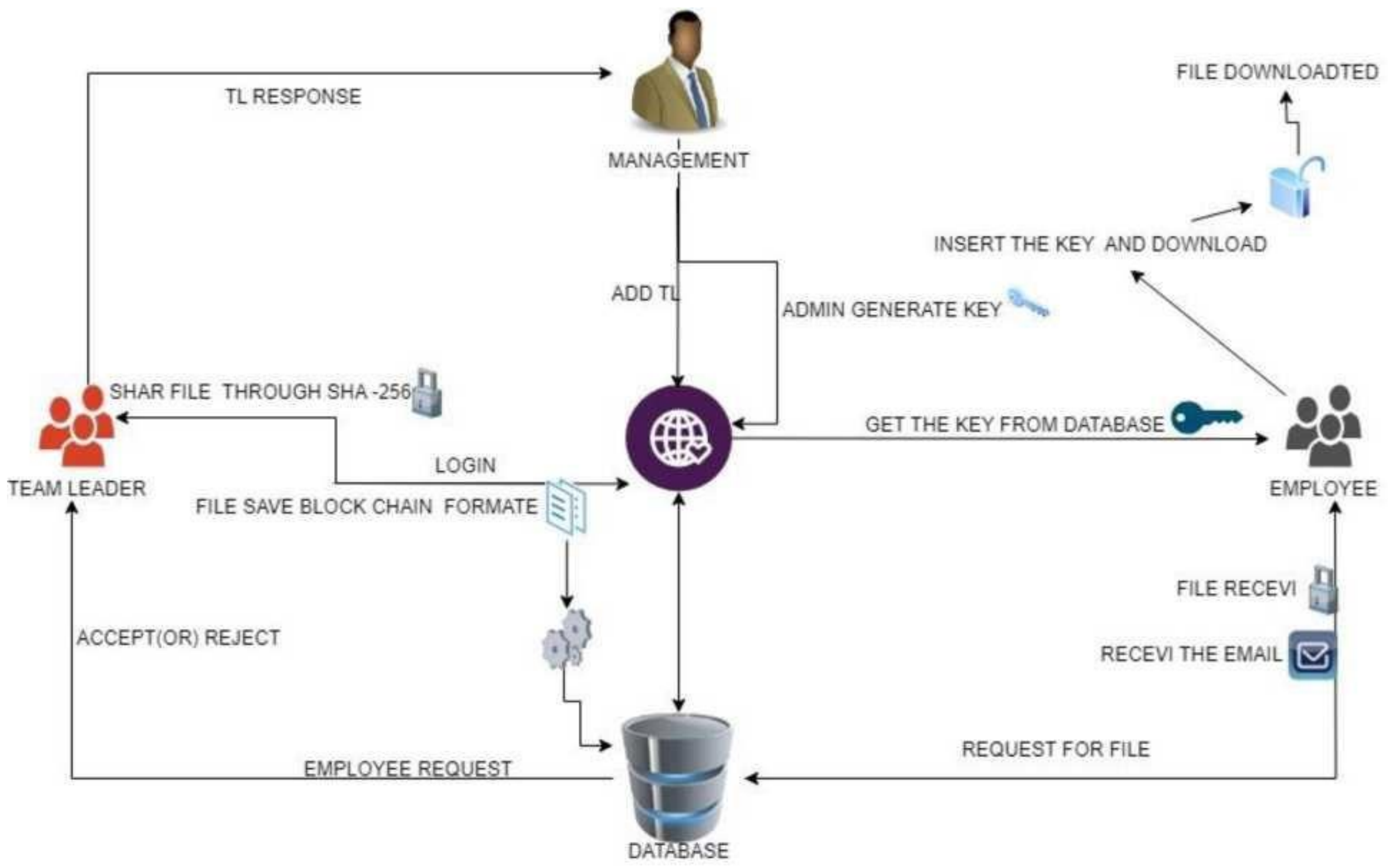
## Introduction

Sensitive data transaction is confidential information that must be kept safe and out of reach from all outsiders unless they have permission to access it. Access to sensitive data should be limited through sufficient data security and information security practices designed to prevent data leaks and data breaches. Sensitive data can be any sort of information that needs to be protected from unauthorized access to safeguard the privacy or security of an individual or organization

## Related Works

Scholars have explored various cryptographic techniques, such as searchable encryption and attribute-based encryption (ABE), to enable secure and efficient information retrieval while preserving data confidentiality. The integration of ranked keyword search adds an additional layer of complexity, requiring innovative solutions for efficient query processing and result ranking in encrypted environments. Works in this domain often address the challenges of designing expressive search queries, ensuring access control through ABE, and optimizing search algorithms to operate on encrypted data. Researchers have also examined the use of homomorphic encryption and proxy re-encryption to enhance privacy-preserving information retrieval. As cloud computing continues to evolve, these related works contribute valuable insights into the development of secure and privacy-aware search mechanisms over encrypted documents in the cloud.

## System Architecture



The systems architect establishes the basic structure of the system, we propose a Hash code Solomon algorithm and we can put a small part of data in local machine. and fog server in order to protect the privacy. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively. Through the theoretical safety analysis and experimental evaluation, the feasibility of our scheme has been validated, which is really a powerful supplement to existing cloud storage scheme

## Blockchain Technology

The emerging blockchain technologies also use SHA-256 to secure the integrity and immutability of data stored in blocks. Because each block in blockchain contains a unique value, nobody can change the contents of the block without changing their hashes. In other words, by linking blocks using their hash values, the blockchain creates a transparent and tamper-proof ledger that anyone can verify.

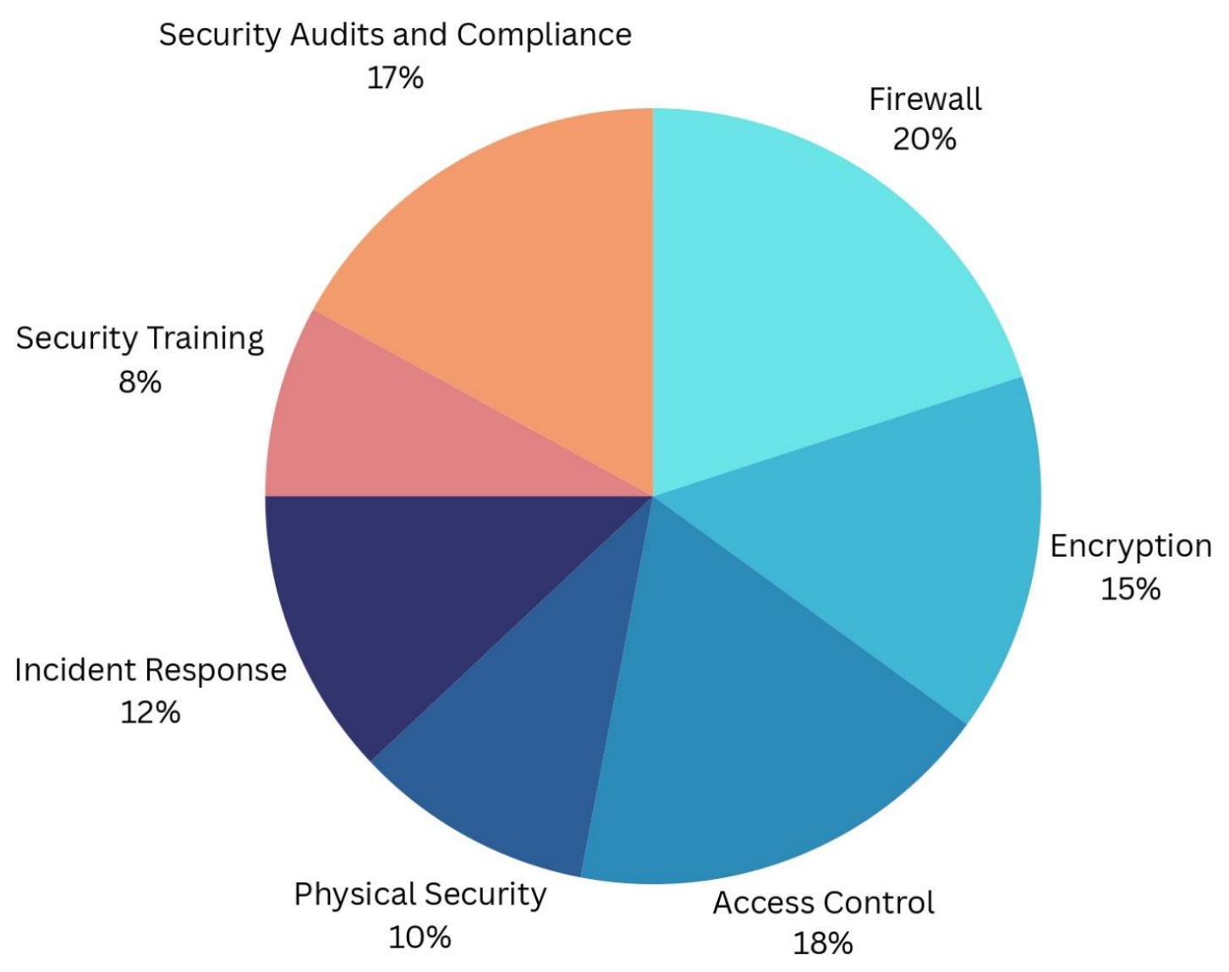
## Modules

- □ STAFF REGISTER
- □ STAFF LOGIN
- □ STAFF FILE VIEW
- □ STAFF FILE REQUEST
- □ STAFF FILE DOWNLOAD
- □ TEAM LEADER LOGIN
- □ TEAM LEADER FILE UPLOAD
- □ TEAM LEADER FILE VIEW
- □ MANAGEMENT LOGIN
- □ MANAGEMENT TEAM LEADER REGISTRATION
- □ MANAGEMENT GENERATE KEY
- □ MANAGEMENT RESPONSE

## Algorithm

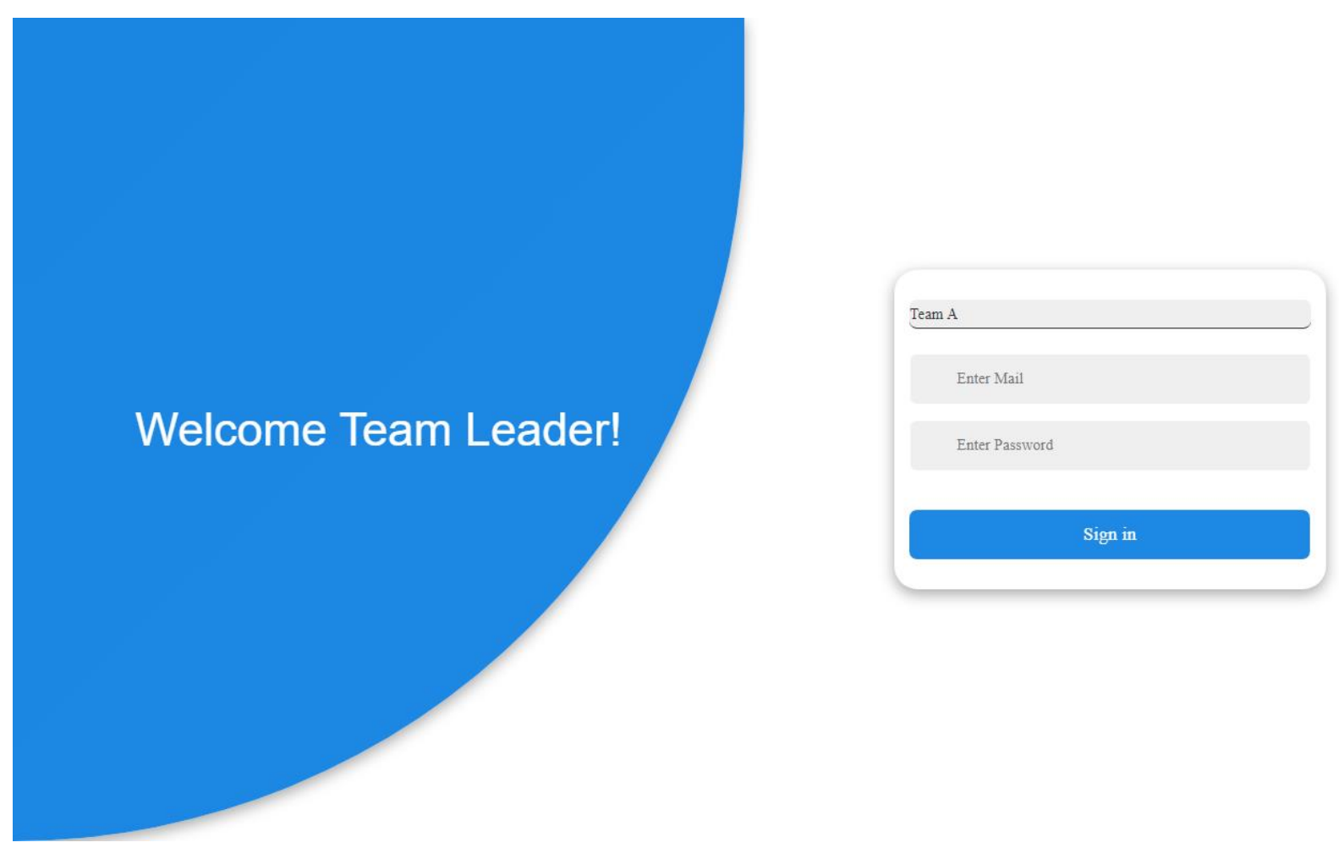
The RSA algorithm is an asymmetric cryptography algorithm; this means that it uses a public key and a private key (i.e two different, mathematically linked keys). As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.

The RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman.



## Output

Team Leader

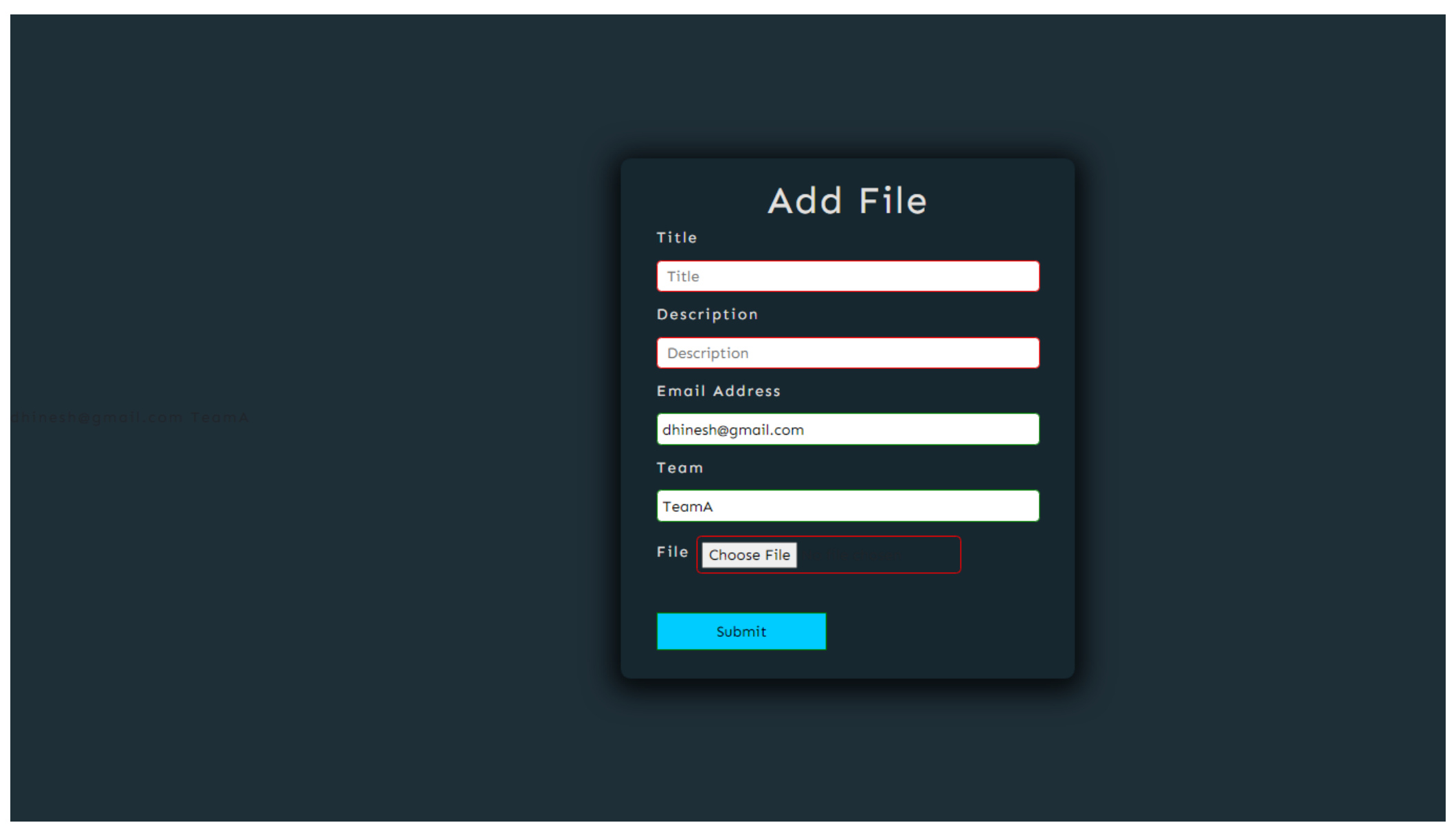

Welcome Team Leader!

Team A

Enter Mail

Enter Password

File With Encryption


Add File

Title: Title

Description: Description

Email Address: dhinesh@gmail.com

Team: TeamA

File: Choose File

## References

❑ TITLE: Secure Secret Sharing Using Homomorphic Encryption
AUTHOR: Nileshkumar Kakade; Utpalkumar Patel
YEAR: 2020

❑ TITLE: Secure multi-party computation in differential private data with Data Integrity Protection
AUTHOR: Sundari S, Ananthi M
YEAR: 2015