DocuVault: Empowering Paperless Efficiency

Background of the study

DocuVault are critical tools used for organizing and securing digital documents in companies that prioritizes security and includes numerous measures to protect sensitive data from unauthorized access or modification. DocuVault relies heavily on AES encryption, this technique is commonly used to preserve confidentiality and integrity of stored documents. Access control mechanism are critical components of DocuVault security which governs the rights and privileges that users or user groups have in relation to specific documents, incorporating robust security features such as AES-256 encryption, user authentication with bcrypt, access control, and SHA-256 security for file uploads.

Organizations or businesses of all sizes and in a range of industries are the project's target customers or beneficiaries. They may be corporations, governmental bodies, nonprofit groups, educational institutions, or any other organizations that handle a lot of documents and need a more effective and secure document management solution.

The purpose of the study is to assess the efficiency and security of DocuVault, a vital tool for managing and safeguarding digital documents in businesses that place a high priority on security. It focuses on the main security components of the system, such as access control, bcrypt authentication, and SHA-256 security for file uploads. To evaluate the system's robustness and applicability, the research uses real-world simulations, penetration testing, and industry implementation studies.

Problem

In today's data-driven world, there is a growing demand for effective digital document organization and security. The possibility of illegal access, data breaches, and document manipulation is becoming much more concerning as more businesses and organizations switch to digital processes. A significant difficulty that has to be adequately handled is ensuring the confidentiality and integrity of sensitive information.

Objectives:

Create Software to streamline document management, increase accessibility, enhance collaboration, and ensure secure and compliant digital document handling within an organization. Specific Objectives: 1.) Implement the following Security

a) AES 256 Encryption

b) Hashing (SHA256)

c) User Authentication (Bcrypt)

d) Access Control

2.) Deploying the system

3.) Conduct Test Cases

Scope

This project's scope focuses on improving accessibility, collaboration, and safe and compliant digital document handling inside the company while also optimizing document management procedures. It includes putting through particular security safeguards, including user authentication, access restriction, hashing (SHA256), and AES 256 encryption. The project's goal is to organize, store, retrieve, and version control digital documents in order to enhance the organization's document management system. Additionally, it strives to improve accessibility for authorized users by making document retrieval and viewing simple. The initiative places a strong emphasis on security, safeguarding the privacy, authenticity, and accessibility of digital materials. The observance of pertinent legal and compliance requirements will also be covered.

Delimitation

It excludes physical document handling and scanning. MySQL will serve as the system's database, and the system will be constructed using ES6 JavaScript, PHP 8.x, CSS, and Bootstrap 3. Documents will be encrypted using AES 256 and SHA256 hashing, and user authentication will be protected using bcrypt. Role-Based Access Control (RBAC) will be used for access control. The system will be installed on an Apache web server and accessible from computers running web browsers that operate with it. Other file types will not be managed; only PDF and DOC files will.

Technical Background

Web Base : ES6 JavaScript version / PHP 8.x / CSS & Bootstrap 3

IDE: Sublime

DB: MySQL

User Authentication: bcrypt

Encryption: AES 256 Encryption and Hashing SHA256

Access Control: Role-Based Access Control (RBAC)