Chapter 1

**Introduction**

The effective management of documents has become a pressing challenge for both organizations and individuals in the current digital era. The problem of document overload has grown to staggering proportions as a result of the spread of digital content and the persistence of paper-based records. This overabundance of paperwork causes inefficiencies, disarray, and a higher risk of data breaches and compliance problems. It can be time-consuming to search through this sea of information for particular documents, which hinders productivity and decision-making. Additionally, since traditional methods are frequently prone to mistakes and misunderstandings, document collaboration and version control continue to be formidable obstacles. These difficulties are made even more difficult by the urgent need for improved data security and compliance.

Document Management Systems (DMS) provide a comprehensive solution to these problems by utilizing technology to organize, streamline retrieval, and secure documents. DMS are critical tools in the modern era of information management because they address document disarray, facilitate efficient access, and ensure data integrity and security. This study seeks to delve into the complexities of DMS, investigating their functionalities, benefits, and real-world applications, with the goal of shedding light on how organizations and individuals can use this technology to revolutionize their document management practices.

**Project Context**

Document and Information inorganizations grapple with the growing influx of documents, ranging from contracts and invoices to reports and emails. The effective management of these documents is vital for maintaining productivity, ensuring compliance, and safeguarding data security. A Document Management System (DMS) is a technological solution designed to address these challenges by providing centralized storage, version control, and workflow automation. This project aims to implement and customize a DMS tailored to the unique needs of our organization, with the goal of improving operational efficiency, enabling seamless collaboration, and enhancing information security.

Document management challenges are well-documented in the literature, including issues such as document retrieval delays, version control errors, and the potential for data breaches. Inefficient document management practices can result in significant productivity losses and pose compliance risks.

Document Management Systems have emerged as effective tools to address these challenges, offering features like efficient search capabilities, automated workflows, and robust security controls. Research indicates that organizations implementing DMS solutions experience improvements in document handling efficiency and reduced operational costs. Additionally, DMS solutions enhance collaboration among team members by providing a centralized platform for document access.

The primary objective of this project is to implement a DMS system that aligns with our organization's specific requirements, offering benefits such as streamlined workflow automation, enhanced data security, effective version control, and compliance with industry-specific regulations. As organizations continue to grapple with the increasing volume of digital documents, the implementation of a well-designed Document Management System becomes imperative. This project aims to address the specific document management challenges faced by our organization, aligning with best practices and industry standards to enhance efficiency, collaboration, and information security.

**Purpose and Description**

"A Document Management System (DMS) is a digital hub that allows organizations to efficiently manage their documents and files. Its primary purpose is to streamline document-related processes by providing a centralized repository for storing, organizing, and retrieving digital documents. DMS ensures version control.

A Document Management System (DMS) is a digital solution that aims to transform how businesses manage their documents and data. It provides a structured framework for document storage, retrieval ensuring that important data is organized, secure, and easily accessible. It eliminates the chaos of outdated documents and protects sensitive data with version control and access permissions. DMS automates workflows, speeds up decision-making with quick search capabilities, and ensures compliance with industry regulations. In essence, a DMS improves efficiency, lowers costs associated with paper-based processes, and enables businesses to maximize the value of their digital assets."Here’s the potential beneficiaries for a project proposal of an IT system:

Administrators and Users: Users of the system will benefit from improved document management capabilities, and efficient user management. Administrators will have tools to oversee user accounts effectively.

IT Department: The IT team will benefit from implementing robust security features, including encryption and data integrity checks, to protect sensitive documents and user data.

End Users: Any employee or individual who needs to access documents for their work will benefit from the improved search capabilities, making it easier to find the information they need.

**Objectives:**

To design and develop a comprehensive and secure Document Management System that ensures data integrity and confidentiality through AES 256 encryption and SHA 256.

**Specific Objectives:**

1. To design and create a user registration module that will register the user as a user.
2. To design and create a user management module that manage the user’s profile.
3. To design and create a version control module that track documents revision and changes.
4. To design and create a search bar module, including full-text search and metadata-based search quickly locate documents.
5. To integrate following security features:
6. AES 256 encryption will be used after uploading a file, user authentication, and database storage.
7. Password hashing using bcrypt will be used in passwords in database.
8. To perform test cases on authentication, input validation, and Application Logic.
9. To evaluate the functionality, security and reliability of the system using ISO/IEC 25010.

**Scope and Delimitation**

This project's scope focuses on improving accessibility, and safe 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. Hashing(SHA256) for the password in the database. The project's goal is to organize, store, and version control digital documents in order to enhance the organization's document management system. The work of user can upload files, edit. In the other hand the administrator responsible in managing user accounts, roles and permission. They can modify, deactivate user accounts as needed. To integrate a search bar module into our Document Management System (DMS) to improve document retrieval efficiency and user experience. The module will include full-text search capabilities, enabling users to search for documents using keywords or phrases, and metadata-based search options that allow filtering and searching based on document attributes like titles, authors, dates, categories, tags, and custom metadata fields. The scope encompasses the design of an intuitive user interface, advanced search features like Boolean operators and date ranges, relevance ranking for search results, and performance optimization measures to ensure rapid response times. Security and permissions features will be integrated to protect sensitive documents, limiting access to authorized users. Javascript, PHP8.x, CSS, and Bootsrap 3. Documents will be encrypted using AES 256 and SHA 256 hashing, and user authentication. RBAC (Role Based Access Control) will be used for access control. To be install on an Apache Web Server and accessible from computers running web browser that operate with it. Authentication and input validation are critical components of ensuring a software application's security and dependability. In the context of authentication, the scope should include positive testing to ensure that valid usernames and passwords grant. Negative testing includes attempting to login with invalid credentials, testing account lockout mechanisms, evaluating the system's response to brute force attacks, and looking for session management issues such as session fixation. To assess user behavior in response to potential threats such as phishing attacks, social engineering testing should be considered.

The scope of input validation should include testing different types of inputs that the system accepts. This includes checking for the presence of required fields, the length and format of inputs, and how the system handles special characters and potentially malicious inputs. Boundary testing should be performed to evaluate how the system handles inputs at the system's defined limits. To ensure data integrity and security, input validation should include both client-side and server-side validation, as well as any backend database validation. Overall, the scope of authentication and input validation testing should be broad in order to detect flaws and protect the application from potential security threats.

The delimitation of Document Management System lies in its primary focus on digital documents. It excludes physical document handling and scanning. Other file types will not be managed; only PPT, TXT, ZIP, PDF and DOC files will. And also the limit of the file size to be upload is only 25 MB, files larger than this range will not be supported, also aim to optimize user, experience, system performance, and resource management. The exclusions include multimedia files, advanced security features like DRM, or complex version control scenarios. Testing aims to cover common scenarios, and specialized aspects may be omitted. The system will use AES 256 and SHA 256 encryption for security, other encryption algorithm will not be supported. The system has no dedicated mobile application. Users will access the system via web interface.

**Chapter II**

**Review of Related Literatures and Technologies**

**Technical Background**

**Web Base: ES6 JavaScript version**

The JavaScript programming language will be used by the system. The most recent iteration of JavaScript was released in 2015 and is called JavaScript ES6 (also known as ECMAScript 2015 or ECMAScript 6). A number of additional additions and improvements to JavaScript are made by ES6, including spread operators, template literals, and arrow functions. The coding of the document management system is more legible and maintained because to these features' cleaner and shorter code. JavaScript (JS) is a dynamic, weakly-typed and object-based programming language that expanded its reach, in recent years, from the desktop web browser to a wide range of runtime platforms in embedded, mobile and server hosts by Diamantidis

**Web Based: PHP 8.0**

To communicate with the database, the system will use PHP 8.0. Popular server-side programming language for web development is PHP 8.0. It is crucial for creating interactive and responsive websites since it enables us to design dynamic web pages and online apps, process data, and connect with databases. PHP & MySQL Novice to Ninja by Kevin Yank2. This book teaches you how to use PHP and MySQL to create powerful web applications from scratch. You will learn the basics of PHP, object-oriented programming, database design, security, and testing.

**Web Base: CSS**

CSS will be used by the system to style and layout web pages, including font, color, size, content spacing, animations, and other adornments. The design and layout of HTML documents are managed using the style sheet language known as CSS (Cascading Style Sheets). It enables us to specify the colors, fonts, spacing, and positioning of various web page elements. Ricardo Queirós stated that Cascading Style Sheets (CSS) are frequently used to style web documents and have gained widespread popularity in the digital world. This W3C specification was written for web designers with limited programming experience, despite their widespread use. Consequently, it is deficient in a number of programming elements, including variables, conditional and repeating blocks, and functions.

**Web Base: Bootstrap 3**

For designing and arranging web pages, including font, color, size, content spacing, animations, and other adornments, the system will employ Bootstrap 3. For creating a DMS application that can adapt to different screens and devices, Bootstrap provides pre-built templates and responsive CSS frameworks. The bootstrap, extensively studied during the last decade, has become a powerful tool in different areas of Statistical Inference. In this work, we present the main ideas of bootstrap methodology in several contexts, citing the most relevant contributions and illustrating with examples and simulation studies some interesting aspects by Juan Romo.

**IDE: Visual Studio**

The system will use Visual Studio as integrated development environment (IDE) for software development. It provides a wide range of tools, frameworks, and languages for creating custom applications. In lieu of an IDE, we use sublime text, a strong text editor that is well worth the cost. If you want text editors that are straightforward, Visual Studio Text should be at the top of your list when talking about IDE. It is a very quick text editor without many bulky add-ons or toolbars. Less than a second is required for it to load. Its auto-completion capability makes it the best in its field and enables us to create quick and straightforward automation scripts by Rafael Hernandez.

**DB: MySQL**

The system will use MySQL to store and manage documents efficiently, it is a widely used open-source relational database management system that plays a crucial role in the local server infrastructure. It is employed to store and manage data associated with Docu-vault. By utilizing MySQL, the project ensures a dependable and efficient approach to storing and retrieving data in a structured manner, thus enabling effective data management for the system. rom the fundamentals of populating a database and creating queries to utilizing MySQL with PHP or Perl to create dynamic web pages, author Paul DuBois covers it all. He also covers designing your own programs that access MySQL databases and managing MySQL servers. A thorough reference section that provides in-depth information on MySQL's structure, language, syntax, and APIs is also included in the book.

**User Authentication: bcrypt**

The system will use bcrypt for hash and store passwords. A strong cryptographic algorithm used to hash passwords is called bcrypt. It creates a distinct and irreversible hash for each password, ensuring that they are securely saved in the database. Data security is improved and the risk of password theft is decreased. On the surface bcrypt, an 11-year-old security algorithm designed for hashing passwords by Niels Provos and David Mazieres, which is based on the initialization function used in the NIST approved blowfish algorithm seems almost too good to be true. It is not vulnerable to rainbow tables (since creating them is too expensive) and not even vulnerable to brute force attacks.

**Encryption: AES (Advanced Encryption Standard) 256**

The system will encrypt using the AES (Advanced Encryption Standard) 256 encryption method. AES is substantially more secure when used in web-based applications since it makes sure that data is encrypted before being stored in the database. In many applications, the Advanced Encryption Standard (AES) algorithm has taken the place of other encryption algorithms as the default option. In this paper, Hamalainen presents a hardware core for AES encryption that is suitable for low-cost, low-power systems.

**Access Control: Role-Based Access Control (RBAC)**

Based on their roles and responsibilities, the system will control access using role-based access control (RBAC). Administrators can design roles with various levels of access and permissions using RBAC. As a result, only those who are permitted can access, view, alter, or delete documents. RBAC works to prevent unauthorized access and data breaches by giving users specified roles. Role-Based Access Control (RBAC), in accordance with Barsha Mitra, is the most extensively used paradigm for advanced access control applied in many organizations of all sizes. Roles are a crucial component of RBAC because they act as a functional bridge between users and permissions. A suitable set of responsibilities must therefore be identified for RBAC to be effective. Roles can be deduced from the user-permission assignments that are already set in many organizations' systems in some way.

**Operating System:** **Windows 11**

Windows 11 is the latest version of the Windows operating system released by Microsoft. It features a new, centered taskbar, a redesigned Start menu, enhanced window management, improved gaming performance with DirectX 12 Ultimate support, and deeper integration with Microsoft Teams, among other new features and visual changes.

**Review Related Literature**

**File Management System**

An essential part of managing and organizing data files inside of a computer system is a file management system. It is essential for keeping files of all kinds, including records and office documents, organized and accessible. As the three writers outline their findings, it becomes clear how important file management systems are and how they affect the effectiveness of both electronic and physical document management.

In the study conducted by Jesse David Dinneen and Charles-Antoine Julien (2019), Computer users spend time every day interacting with digital files and folders, including downloading, moving, naming, navigating to, searching for, sharing, and deleting them. Such file management has been the focus of many studies across various fields, but has not been explicitly acknowledged nor made the focus of dedicated review.

Furthermore, Jienan Chen, Chuang Zhang, Yu Yan and Yuan Liu. (2021) Online file management systems enable cooperatively editing and sharing. However, due to the cost of communication and storage infrastructures, traditional online file management services, e.g., Google Drive and OneDrive, usually provide limited storage space and relatively low download speed for free users. To achieve better performance, ordinary users have to purchase their expensive services. Moreover, these file management systems are based on centralized architecture and bear the privacy leakage risk, because users’ personal files are stored and controlled by their servers.

FileWeaver: Flexible File Management with Automatic Dependency Tracking, Jienan Chen, Chuang Zhang, Yu Yan and Yuan Liu. (2020). Knowledge management and sharing involves a variety of specialized but isolated software tools, tied together by the files that these tools use and produce. We interviewed 23 scientists and found that they all had difficulties using the file system to keep track of, re-find and maintain consistency among related but distributed information.

**Security Management System**

Modern systems require security management, which includes safety and security considerations to guarantee the integrity and dependability of numerous applications. The conversation amongst the many writer’s sheds light on cutting-edge methods that address the connections between safety and security, cause-and-effect analysis, and coordinated mitigation measures.

In the study conducted by Kwo-Jean Farn, Shu-Kuo Lin, Andrew Ren-Wei Fung,

The security of information system is like a chain. Its strength is affected by the weakest knot. Since we can achieve 100% Information Security Management System (ISMS) security, we must cautiously fulfill the certification and accreditation of information security. In this paper, we analyzed, studied the evaluation knowledge and skills required for auditing the certification procedures for the three aspects of ISMS—asset, threat, and vulnerability.

While Heru Susanto12, Mohammad Nabil Almunawar1 and Yong Chee Tuan. It cannot be denied that nowadays information is a very important asset for any modern organization. Therefore, protecting its security is very important and becoming a top priority for many organizations. Unfortunately, there is no single formula that can guarantee 100% of information security. Therefore, there is a need for a set of benchmarks or standards to ensure the best security practices are adopted and an adequate level of security is attained. In this paper, authors introduce various information security standards briefly and then provide a comparative study for major information security standards, namely ISO27001, BS 7799, PCIDSS, ITIL and COBIT. The study will provide a picture of the position and specialization of each standard, adoption by countries and their usability levels.

In their research, Kriaa et al. (2016). Give a notable case study where they use the BDMP formalism to simulate the interdependencies between safety and security within an industrial control system. This ground-breaking methodology offers a thorough assessment of the dynamic interaction between safety and security, taking into account elements like antagonistic, conditional reliance, and mutual reinforcement. Notably, BDMP not only supports risk assessment but also makes it easier to select the best defenses against prospective assaults. This study acts as a single, integrated task that tackles security and safety issues, with the option to incorporate information from other safety and security tasks.

**User Authentication**

With the need to build trust and manage access to sensitive data in the cloud, user authentication is essential to cloud computing security. Insights from many sources, such as the correlation matrix of latent factors in assessing security risk in public cloud computing, will be discussed in depth by the authors. It will also look at the popularity of password-based authentication techniques and how multi-factor authentication has changed in reaction to password vulnerabilities.

In a study by Campbell and Bryant (2015), it was found that 80% of typical passwords could be deciphered within a week by a computer. When users mixed several symbols into a passphrase, this process got even more difficult. Password cracker software changed its methods as hardware capabilities advanced throughout time in order to speed up the cracking process. As noted by Dasgupta et al. (2016), multi-factor authentication became more popular as a result of the vulnerabilities of password-based authentication and its ability to improve security across a variety of applications and websites.

In paper titled "The science of guessing: analyzing an anonymized corpus of 70 million passwords," published in 2012, Bonneau described his ground-breaking research. In this study, he delves into the analysis of a vast dataset of anonymized passwords, aiming to gain insights into how users typically choose their passwords. This study reveals the weaknesses connected to widespread password usage.

The National Institute of Standards and Technology (NIST) also published Special Publication 800-63-3, "Digital Identity Guidelines," in 2017, which offers thorough rules for maintaining digital identities, including user authentication. Its main goal is to improve security procedures in authentication procedures, which reflects NIST's dedication to raising the bar for cybersecurity standards and protocols.

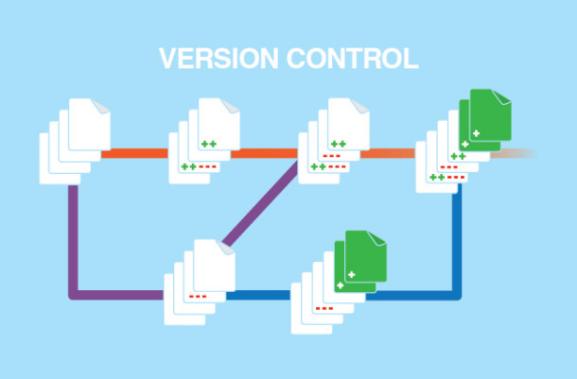
**Synthesis**

Campbell and Bryant's 2015 study revealed that 80% of passwords can be deciphered within a week, with multi-factor authentication becoming popular due to vulnerabilities in password-based authentication and its ability to improve security across various applications and websites while in 2012, Bonneau conducted a groundbreaking study analyzing 70 million anonymized passwords to understand user preference and identify weaknesses in widespread password usage then NIST's 2017 publication, "Digital Identity Guidelines," aims to enhance security procedures for digital identities, including user authentication, demonstrating their commitment to cybersecurity standards and protocols. Jesse David Dinneen and Charles-Antoine Julien's 2019 study highlights the daily interaction of computer users with digital files and folders, including downloading, moving, naming, navigating, searching, sharing, and deleting them while Jienan Chen, Chuang Zhang, Yu Yan, and Yuan Liu (2021) discuss the limitations of traditional online file management systems like Google Drive and OneDrive, which offer limited storage space and low download speed for free users, and are centralized, posing privacy leakage risks due to server-controlled storage and control then the study by Chen, Zhang, Yan, and Liu (2020) explores the challenges faced by 23 scientists in managing and sharing knowledge using specialized software tools tied together by files. They found difficulties in tracking, re-finding, and maintaining consistency among distributed information. The study by Farn, Lin, and Fung highlights the importance of achieving 100% Information Security Management System (ISMS) security by carefully fulfilling certification and accreditation procedures. It analyzes the evaluation knowledge and skills required for auditing certification procedures for asset, threat, and vulnerability aspects while This paper discusses the importance of information security in modern organizations. It introduces various standards, including ISO27001, BS 7799, PCIDSS, ITIL, and COBIT, and compares their adoption, position, specialization, adoption by countries, and usability levels. No single formula can guarantee 100% information security then Kriaa et al. (2016) use the BDMP formalism to simulate safety and security interdependencies in an industrial control system. This methodology assesses dynamic interactions, aids risk assessment, and aids in selecting defenses against potential attacks, integrating information from other safety and security tasks.

**Review of Related Technologies**

**Version control**

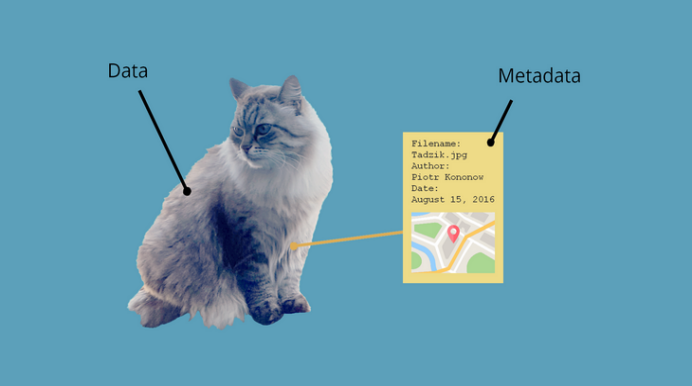
In Docu-vault, version control is utilized to maintain track of changes made to documents over time. It enables users to monitor, control, and maintain a history of all document versions. This feature makes it feasible for several users to work on documents without losing track of changes by keeping track of revisions to avoid version conflicts. The same document may be edited by multiple users at once, and the system logs each change made by each user.

****

*Figure 1. Version Control*

**Metadata tagging**

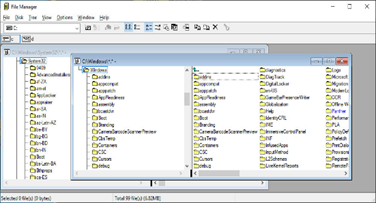
Documents in Docu-vault are organized and classified using metadata tags, making it simpler to find them using sophisticated search options based on certain traits or keywords. As a result, it is possible to retrieve papers quickly and save time by avoiding the need to manually search through a big collection of documents.



*Figure 1. Metadata Tagging*

**File Manager**

A file manager is a piece of software that users can use to manage the files and folders on their computer or other storage devices. Users are given access to a graphical user interface (GUI) that enables them to carry out a number of tasks, including creating, deleting, renaming, moving, copying, and searching files and folders. With numerous choices for organizing and browsing them, file managers typically show a hierarchical directory tree of files and folders. Additionally, they frequently have tools for sorting and filtering data, as well as the ability to open and update data using related software programs.



*Figure 1. File Manager*

**Advanced search and retrieval**

Docu-vault integrate a search bar module into our Document Management System (DMS) to improve document retrieval efficiency and user experience. The module will include full-text search capabilities, enabling users to search for documents using keywords or phrases, and metadata-based search options that allow filtering and searching based on document attributes like titles, authors, dates, categories, tags, and custom metadata fields. Using keywords, metadata, or other search criteria, document management systems use advanced search algorithms to retrieve specific documents rapidly.

*Figure 1. Advance Search and Retrieval*

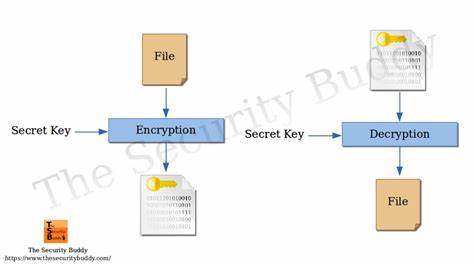
**Security and access control**

Based on their roles and responsibilities, the system will control access using role-based access control (RBAC). Administrators can design roles with various levels of access and permissions using RBAC. As a result, only those who are permitted can access, view, alter, or delete documents. RBAC works to prevent unauthorized access and data breaches by giving users specified roles. Access control, user authentication, and encryption are elements that document management systems utilize to protect data and stop illegal access.



*Figure 1: Security and Access Control*

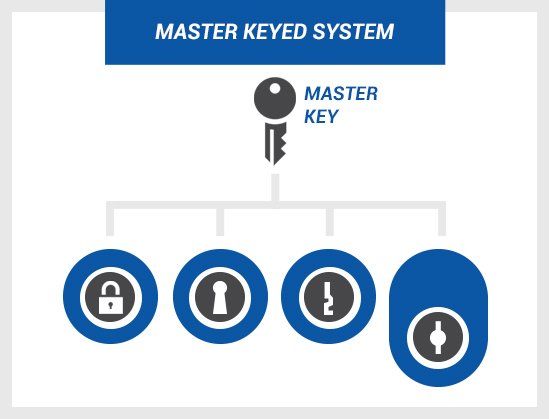
**File Encryption Algorithms**

The system will encrypt using the AES (Advanced Encryption Standard) 256 encryption method. AES is substantially more secure when used in web-based applications since it makes sure that data is encrypted before being stored in the database. The document management system uses these methods to encrypt documents, protecting sensitive information and preventing access or modification without the right decryption keys.

*Figure 1.* File Encryption Algorithm

**Key management systems**

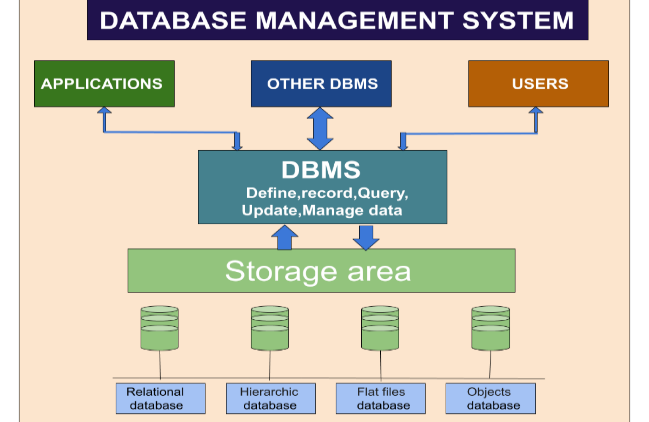
In order to encrypt and decode documents in the document management system, these systems are used to securely generate, store, and manage encryption keys.



*Figure 1.* Key Management System

**Database Management systems**

The system will use MySQL to store and manage documents efficiently, it is a widely used open-source relational database management system that plays a crucial role in the local server infrastructure. It is employed to store and manage data associated with Docu-vault. By utilizing MySQL, the project ensures a dependable and efficient approach to storing and retrieving data in a structured manner, thus enabling effective data management for the system. Implementing robust database system like MySQL help store and manage transaction data, resident information, and service histories efficiently.



*Figure 1.* Database Management System

**Cloud Storage**

 With the adaptability and scalability of cloud storage, Docu-vault can safely store and access documents from any location. The system will leverage Cloud Platform for storage. It is a cloud-based storage and file sharing service. Cloud storage is a popular and versatile cloud-based storage and file sharing service that offers users a convenient way to store and access files from anywhere with an internet connection.

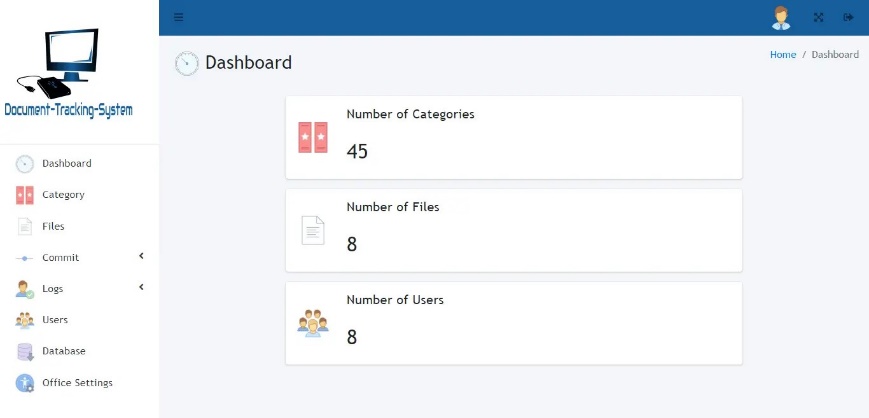
*Figure 1. Cloud Storage*

**Review of Related Technologies**

**Document Management and Tracking System**

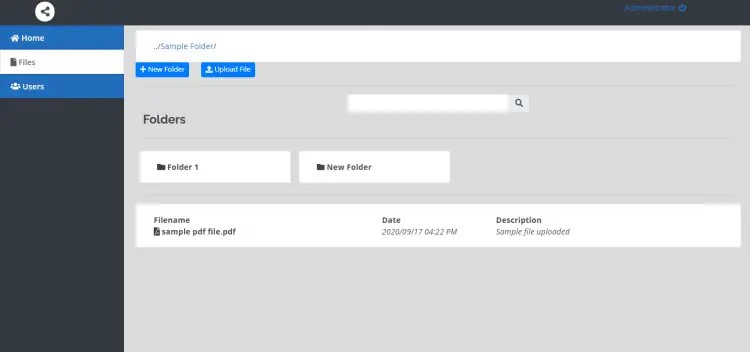
The “Document Management and Tracking System” capstone project is designed to serve as a centralized platform for document uploading. Organizations will be able to conveniently track and monitor papers for company operations thanks to the project. The solution will increase the organization’s efficiency in organizing key papers for the authorized corporate staff to access.

With today’s rapid technological advancements, businesses and organizations must adapt to change and use technology to expedite their transactions and processes. Every corporate activity relies heavily on documents. Documents are sent back and forth between departments. Traditionally, documents are sent in the form of physical copies, which takes time and effort to distribute to each employee. The firm may produce an inadequate service and the client experience will be greatly impacted without an effective system to trace the travels of the papers. Businesses need a system that will automate the process of all document-related transactions. (“Document Management and Tracking System”).



*Figure 1.* Document Management and Tracking System

**File Management System**

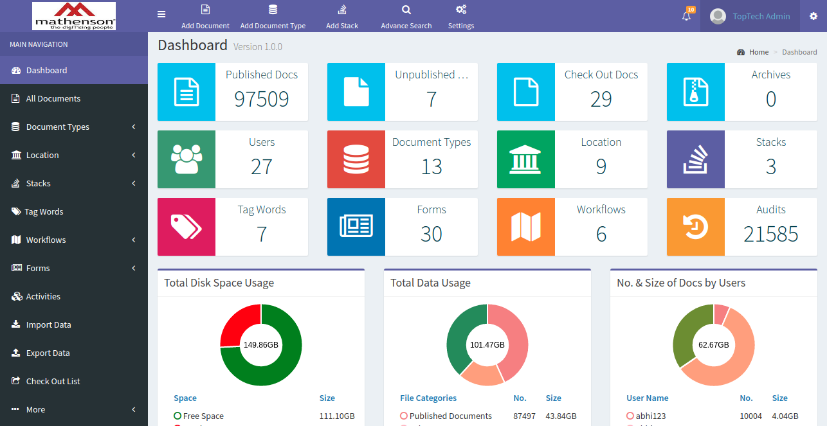
File management system is a file system that is used to organize and keep track of files. Users need not browse through network folder but instead are given instant result, and are provided a system where files can be accessed anytime and anywhere over the Internet. The Web-based File Management System for College will minimize or eliminate loss of files or loss of work of faculty and students. Faculty and students can actually manage, edit, share and approve content or files from their computers.

*Figure 1.* File Management System

**Document Track System**

Today’s rapid development in technology prompts business organizations to invest in computerized systems for fast and efficient business operations. Technology has made different business operations fast, easy and convenient to perform and accomplish.

The project, “Document Track System” is purposely designed for companies and organizations that allow them to electronically store and track documents. The system will track the in/out of the documents across different departments. The typical way of tracking documents is done using the manual approach. The staff will call or personally ask for updates about the documents which are time-consuming and inefficient.

As a response to the need for an effective tool to track documents, the researchers make use of an IT-based solution. The researchers aim to digitized the processing of documents for easy monitoring, retrieval, revisions, and updates. The researchers aim to develop an automated Document Tracking System that will ease up tracking and monitoring of different documents. The system will make exchanging of documents across different departments fast and smooth. The system will eliminate loads paper works that are dealt with by the employees as well as save their time and effort.

*Figure 1.* Document Track System

**CHAPTER III**

**Methodology**

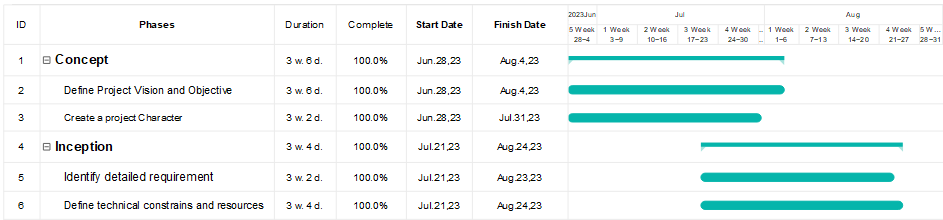
The researchers are led by a pragmatic perspective as they investigate the development of a secure Document Management System using AES 256 encryption and SHA 256 for the protection of data integrity and confidentiality. Their main emphasis within this research paradigm is on applicability and resolving real-world issues, with a strong dedication to discovering efficient solutions.

Their study, which adheres to the pragmatist paradigm, is driven by the need to solve a real problem, namely the pressing need for a secure Document Management System that can effectively protect both data integrity and confidentiality. They have the adaptability provided by this pragmatic approach, enabling them to choose and use the best software development processes and security procedures to complete their study.

Their study ultimately aims to create a safe and effective Document Management System that directly satisfies the stipulated standards for data security and confidentiality. Furthermore, the pragmatic paradigm they follow is open to improvement and change, allowing them to flexibly modify tactics and methodologies as the research advances, accommodating changing requirements and emerging security risks throughout the software development process.

**Concept**

The team will be using the Agile methodology; therefore, each phase will be organized into iterations. The iterative process is the practice of building, refining, and improving a project, product, or initiative. Teams that use the iterative development process create, test, and revise until they’re satisfied with the end result.

****

*Fig. 1 Project Initiation and Planning phase*

The first stage of development process is known as phase 1, also known as the Project Initiation phase. The two sub-tasks of Define Project Vision and Objectives and Create a project charter, which will be employed for the proposed project, make up the majority of this phase.

The concept phase marks the beginning of the capstone project for research group. This phase focuses on the fundamental tasks of creating a thorough project vision and identifying the project's primary goals. During the defining the project's vision and objectives, the team will define the boundaries of the project, including: determining the stakeholders: listing every stakeholder whose requirements will be affected by the project; defining the problem statement: specifying the issue the project is trying to resolve; creating a vision statement: outlining the project's intended results; and creating SMART goals that are in line with the vision statement. The research team outlines the critical requirement for a reliable and secure Document Management System (DMS) in the context of our capstone project, with a high priority on preserving data integrity and confidentiality through the use of AES 256 encryption and SHA 256.

The Concept Phase also requires the creation of a project charter or vision statement, which will act as the capstone project's compass. This document summarizes the goals, scope, and expected results of our study, ensuring that all research group members have a clear grasp of the overall direction, purpose, and goals of the project.

In addition, the research team carefully identifies and records the project's main goals, drawing on the supplied precise goals. These goals include developing user administration and registration modules, a version control system, search capabilities, and the seamless incorporation of strong security elements.

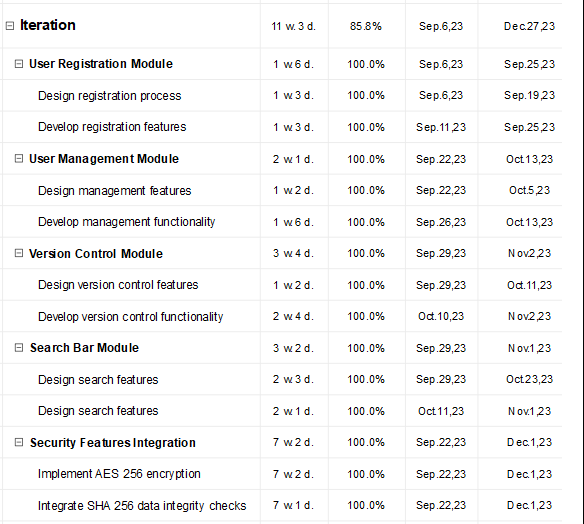
**Inception Phase**

The team behind the capstone project meticulously documented detailed requirements for their Document Management System (DMS) during the inception phase. They utilized PHP, JavaScript, HTML, CSS, and MySQL for the database. The team collaborated with stakeholders, end-users, and subject matter experts to capture their specific needs and expectations. For each of the defined objectives, such as the user registration module, user management, version control, and search functionality, the team created granular user stories or feature specifications using these technologies. These detailed requirements served as the foundation for the project’s development work in subsequent iterations, ensuring that the team had a clear understanding of what needed to be built and how it aligned with the project’s goals.

The team also defined technical constraints and resources within the PHP, JavaScript, HTML, CSS, and MySQL environment in parallel with the requirements gathering. This involved evaluating the project’s technical feasibility and identifying any constraints related to the technology stack, infrastructure, and architectural decisions. For instance, the team defined how AES 256 encryption and SHA 256 would be integrated into the system, considering technical challenges and resource requirements using the PHP, JavaScript, HTML, CSS, and MySQL technologies. The team assessed whether they had the necessary skills and resources to implement these security features effectively. By establishing these technical constraints and resource requirements upfront within their chosen technology stack, the project could proceed with a clear understanding of the potential challenges and resource needs.

**Iteration**

In the Iteration phase, our team uses EdrawMax for seamless project management, automating progress tracking and task timelines. Tasks are clearly defined with start dates and durations, and EdrawMax helps compute sprint durations for realistic planning. As we concentrate on advancing the goals of the Document Management System (DMS) during Sprint2, EdrawMax's collaborative features aid in efficiently addressing dependencies.



*Fig. 2 Frontend Development*

The User Registration Module is started by the development team by designing and creating an easy user registration process. This entails developing a user-friendly account registration interface, gathering crucial user data, and putting in place a step-by-step registration workflow. The objective is to make it simple for users to open accounts in the DMS.

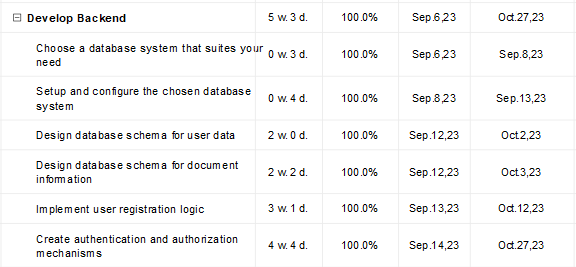
The team moves on to the User Management Module once the User Registration Module is well under way. In this case, the team creates and develops user management features that let administrators effectively manage users. In accordance with the "User Management Module," the user management interface should include elements such user profiles, roles, permissions, and account management.

The Version Control Module is created in tandem with these initiatives. The team concentrates on developing version control tools that allow for the tracking of document changes and revisions. In accordance with the 'Version Control Module,' this entails creating an interface for version history, comparison tools, and access control to manage document versions effectively.

Integrating security measures, such as AES 256 encryption and SHA 256 data integrity checks, is a priority. These features are used to protect the confidentiality and integrity of data inside the DMS during file uploads, user authentication, and database storage.

To guarantee the DMS's security and functionality are strong and trustworthy, the team is also designing rigorous test cases for authentication and input validation. These test cases, which fall under the 'Test Cases and Quality Assurance' assignment, are crucial for verifying the system's integrity and security.

Sprint 2 makes significant advancements toward delivering a thorough and user-friendly Document Management System that satisfies the project's goals.

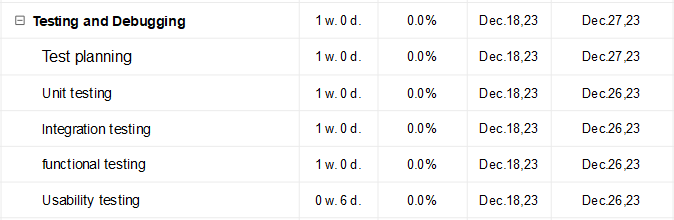
The team performs particular duties to make sure the project is moving forward smoothly and that the backend and frontend are integrated with ease during the Iteration phase of DocuVault's development. The goal of this phase—Sprint 3 is to establish a robust and user-friendly system, therefore coordination of backend development efforts with database setup is a key priority. A MySQL database and PHP are used in the creation of DocuVault to link the frontend and backend technologies.

*Fig. 3 Continuation of sprint 2*

The development team gets started by comprehending the data structures required for user data, document management data, and data pertaining to document version control. Following that, they begin the process of creating the database schema. This entails creating the relevant tables, outlining their interrelationships, and identifying the data types for each field. The ability to create intricate and effective database structures is provided by MySQL, which is essential for a document management system.

Security characteristics must be taken into account by the development team in addition to the fundamental database structure. Although MySQL lacks built-in row-level security features, the team can still develop its own security measures to guarantee that access to rows within database tables is correctly regulated based on predetermined criteria. To control access and protect important document data, they may set roles and access permissions.

The team starts by creating the database before moving on to creating the registration logic. In order to do this, PHP will be used to link the user registration interface on the frontend with the backend. User registration data is validated and safely stored in the MySQL database by the backend logic. By doing this, the development of a user registration module is ensured.

**The testing and debugging phase 4 comes next. The developers will concentrate on thoroughly testing the application and fixing any problems or defects that may appear during this phase.

*Fig. 4 testing and debugging phase*

To ensure that users can easily register and access the system, they first test the user registration procedure. They examine each stage of the registration process to make sure everything goes as planned and that user information is kept safe and secure.

The security measures that guard against unauthorized access to sensitive data, such as robust encryption and data integrity checks, are then put to the test.

Additionally, the team tests the user management module, which enables administrators to add, edit, and remove user accounts.

To ensure that it accurately captures document history, the version control module, which keeps track of changes to documents, is examined carefully.

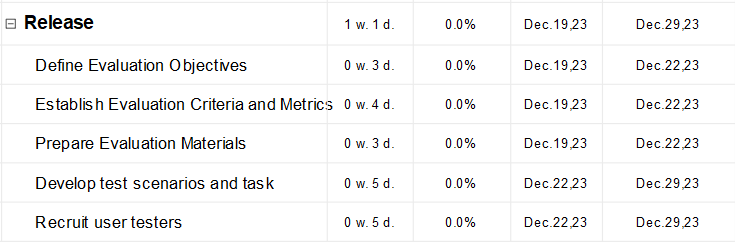
The search tool, which is essential for speedy document retrieval, is put to the test to make sure it can quickly find documents based on keywords or other details.

In addition, the system's fundamental business principles are carefully scrutinized to make sure it correctly performs operations like document retrieval and access rights.

The team makes that the DMS is not only functional but also secure, dependable, and in line with the project's goals by carrying out these tests during the Iteration phase. Any problems are quickly fixed, ensuring that the system is reliable and ready for usage.

**Release**

The Release phase, which follows the successful completion of the testing and debugging phase, is crucial because it allows the development team to assess if the Document Management System (DMS) adheres to the accepted standard, ISO/IEC 25010. This standard provides in-depth instructions for assessing the reliability, security, and usefulness of software. The structured framework provided by ISO/IEC 25010 can be used to evaluate how well the DMS satisfies the needs of both the organization and its intended users.



*Fig. 5 Release/evaluation Phase*

The development team clearly outlines the ISO/IEC 25010 evaluation objectives at the beginning of the Release phase. These goals include assessing the DMS's functionality, security, and reliability. In the context of functioning, they will take factors like efficacy, efficiency, and satisfaction into account. For security, they will analyze the application of AES 256 encryption and SHA 256 data integrity procedures. They will look into the system's stability and resilience in terms of reliability.

Drawing from these principles, the team establishes specific criteria and metrics aligned with ISO/IEC 25010, such as task completion, error rates, data integrity, system security, and overall user satisfaction. While ISO/IEC 25010 is a standard, the developers undertake a thorough examination of its principles and concepts, gaining an in-depth understanding of the standard. This may involve studying the standard itself and pertinent literature on software quality.

The following stage is to decide which evaluation techniques are best for evaluating functionality, security, and dependability in accordance with ISO/IEC 25010 standards. This could entail thorough testing of features and user scenarios for functionality. Penetration testing for data integrity and encryption purposes may be part of a security assessment. To assure the system's stability under diverse scenarios, the team may undertake stress testing as part of the reliability component.

A combination of professional opinions and end-user feedback is necessary for a thorough evaluation. This is similar to the strategy used in ISO 9241-11, which involves actual end users and usability specialists in the evaluation process. The developers select an appropriate sampling strategy for the assessment participants, ensuring a complete picture of the functionality, security, and dependability of the DMS.

Developers also employ paper-based assessment questionnaires to document usability problems, vulnerabilities, and observations during the review process. These records are essential for pinpointing areas that need to be strengthened in terms of functionality, security, and dependability.

When the evaluation is successful, developers update the DMS to comply with the ISO/IEC 25010 requirements by implementing the suggested adjustments and enhancements. They record the whole assessment process, including with the results, conclusions, suggestions, and actions done.

Sprint 5, the Release phase is crucial in ensuring that the DMS satisfies the functionality, security, and reliability requirements of ISO/IEC 25010, thereby raising its overall quality and user satisfaction.

**REQUIREMENT ANALYSIS**

Knowing the existing features and procedures related to your document management system (DMS) is the first step in this analysis. Examining the current management of these processes, evaluating the benefits and drawbacks of the systems in place, and pinpointing opportunities for development are all part of this.

Next, by carefully analyzing and managing stakeholder relationships, you can ensure a successful document management system (DMS) implementation that meets the needs of all involved parties and delivers long-term value to the organization. This is important to ensure efficient collaboration and accountability within the system.

Additionally, creating data flow diagrams is a fundamental aspect of requirements analysis. This diagram provides a visual representation of how data moves within a document management system (DMS), from the entry of information to its processing and storage. We also emphasize the various security protocols that are in place to safeguard user data, such as SHA 256 security and AES encryption.

Furthermore, enhancing security, facilitating collaboration, streamlining document management, and offering insightful data for increased organizational effectiveness are all goals of the current document management system (DMS) process.

STAKEHOLDER STRUCTURE

1. End Users:

Those who will interact with the system, providing input and utilizing the DMS for requirements documentation.

2. IT Support/Operations:

Responsible for the ongoing maintenance and support of the DMS, ensuring its availability for requirement-related activities.

3. System Administrators:

Responsible for the technical setup, configuration and maintenance of the DMS, may also be responsible for user provisioning, access control, and security.

4. IT Security and Infrastructure Teams:

Responsible for ensuring the security and integrity of the DMS, involved in implementing and maintaining security measures, such as encryption and access controls.

**Requirements Documentation**

(DMS) like DOCUVAULT must fulfill essential functional requirements. It captures and organizes documents from various sources, implements version control, and ensures secure storage with access control. Efficient search, workflow automation, and collaboration tools enhance usability. The system maintains an audit trail, integrates with other applications, and supports the entire document lifecycle. Reporting, mobile access, and backup mechanisms contribute to comprehensive functionality. Compliance with regulations is crucial, and user training and support are integral for successful implementation. In summary, DOCUVAULT provides a robust solution for organized, secure, and efficient document management within an organization.

**Web interface**: from any web browser, users can view and manage requirement documentation. Team members can work together to create and review requirement documents, making this a convenient option for companies with geographically dispersed teams or for users who need to access it from outside the office. Users can access the most recent versions of the requirement documents by logging into the web interface from any location in the world. They can also add notes and recommendations to the documents, which other team members can review and comment on.

**Desktop interface:** gives users access to a more robust feature set for managing requirement documentation, including the capacity to produce reports, conduct sophisticated searches, and create and edit complex documents. Desktop interfaces are commonly utilized by individuals who have to handle substantial amounts of requirement documentation or who must carry out intricate tasks like impact analysis and requirements traceability. They can also be used to create and modify intricate requirement documents like functional specifications and requirements traceability matrices. The desktop interface allows users to cross-reference other documents, format documents, and add images and tables. Additionally, they can create reports on the requirement documentation, like coverage reports and requirements status reports, using the desktop interface.

**In-Scope**

1. User Registration Module

This module involves designing a form for user input, validating the data, and integrating it with the DMS system. Consider using a secure authentication method and database storage for user information, includes essential features such as user profile creation, role-based access controls, secure authentication, data validation, customizable fields, email verification, an audit trail, seamless system integration, and a user-friendly management dashboard. These features collectively aim to enhance security, streamline user onboarding, and facilitate efficient document access and management within the organizational framework. DOCUVAULT/DMS involves designing a secure database schema, creating backend logic with API endpoints for registration, and ensuring frontend-backend integration. Key components include user interface design, secure password handling, authentication with tokens, role-based access control, error handling, and rigorous testing. Security measures, documentation, deployment on a secure server, and ongoing monitoring and maintenance are crucial for a robust and reliable system. It also includes functions such as capturing user details, role assignment, access control, authentication, and authorization. The module ensures security through password policies and features like multi-factor authentication. User profiles are dynamic, and the system maintains an audit trail for comprehensive auditing. Notifications, password recovery, and user deactivation functionalities contribute to a seamless user experience. Integration with external directories streamlines management, and user reports provide insights. Customization, training resources, and consent management features enhance flexibility and compliance with data protection standards.

2. User Management Module

Tis module for DocuVault/DMS is a robust system that enhances user interactions and security. It includes features such as defined user roles, access control, and a secure registration process. The interface offers a user-friendly experience with a dashboard, user list, and profile management tools. The module supports role-based permissions, user suspension, and bulk user management. Security measures include encryption, secure session management, and regular audits. Integration capabilities encompass LDAP/Active Directory integration, APIs, and Single Sign-On (SSO). Overall, it optimizes collaboration while prioritizing the security of DocuVault/DMS.

3. Version Control Module

This module for DocuVault/DMS is a robust addition, offering features like detailed version history, branching for collaborative work, access control, and conflict resolution. The interface is user-friendly with a centralized dashboard, side-by-side comparison, and search options. Functions include creating and merging versions, locking documents, and customizable workflows. Notifications keep users informed, and API support allows for integration and automation, making it a comprehensive solution for efficient document management.

4. Integrate Following Security Features

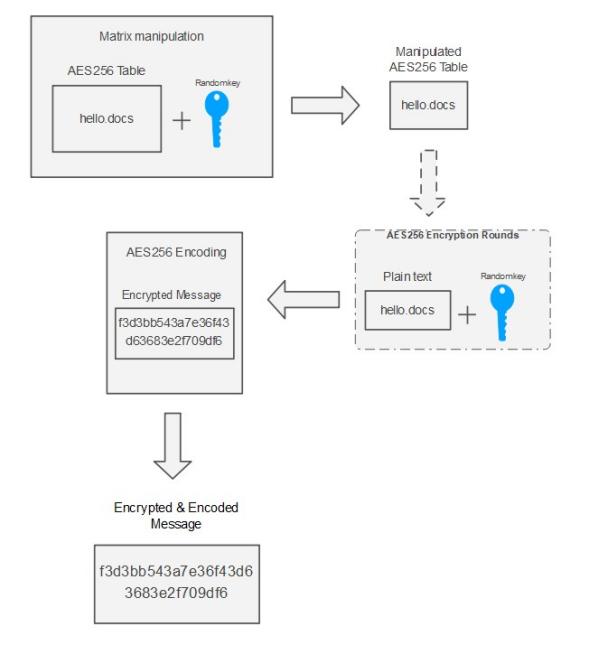
In this module enhance security in DocuVault/DMS, integrate AES 256 encryption for robust data protection and SHA 256 for data integrity verification. Implement secure key management practices to safeguard encryption keys, ensuring they are stored and transmitted securely. Regularly update encryption algorithms and security protocols to stay resilient against evolving threats. Conduct periodic security audits and vulnerability assessments to identify and address potential risks. Additionally, enforce access controls, authentication mechanisms, and secure communication channels to bolster overall system security.

5. Functionality, Security and Reliability of the system using ISO/IEC 25010.

The assessment of the DMS/DOCUVAULT based on ISO/IEC 25010 involves a comprehensive analysis of its functionality, security, and reliability. Functionality evaluation focuses on features like document storage and collaboration tools to ensure alignment with user requirements. Security assessment includes scrutinizing authentication, authorization, encryption, and data protection measures, ensuring compliance with standards and regulations. Reliability is gauged through examining availability, fault tolerance, data integrity, and system stability. A thorough evaluation of these aspects ensures the DMS/DOCUVAULT meets high standards in terms of functionality, security, and reliability.

6. Authentication Module

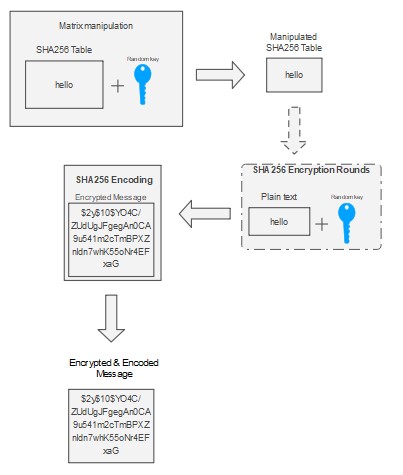
The Authentication Module of DMS/DocuVault is designed to verify and grant access to users based on their credentials. It typically involves authentication methods such as username/password, multi-factor authentication, or integration with external authentication systems like LDAP or Active Directory. The module ensures secure access to the document management system, protecting sensitive information from unauthorized users.

******

*Fig. Block diagram of AES256 Encryption*

AES-256, the 256-bit key generated serves as the foundation for encryption and decryption. When encrypting “hello.docs,” the data is divided into fixed-size blocks, undergoing intricate operations like substitution and permutation. This process, done for multiple rounds, transforms the data into the secure ciphertext “f3d3bb543a7e36f43d63683e2f709df6.” During decryption, the same random key is used in reverse, reconstructing the original “hello.docs.”

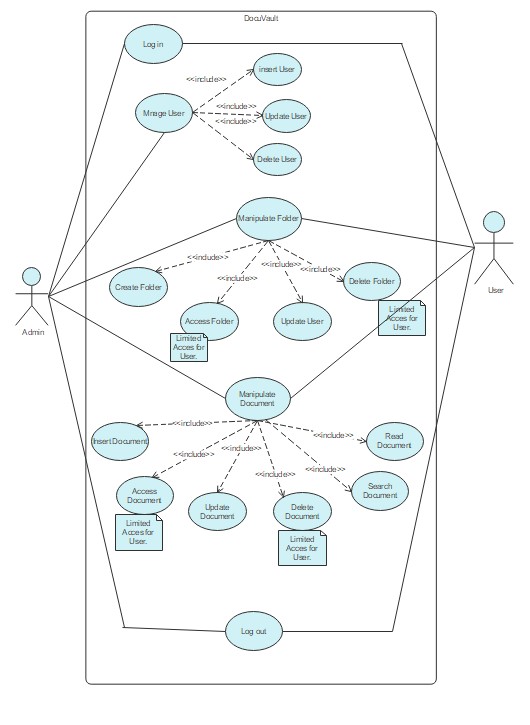
Audit logging: This function keeps track of every system activities so that businesses can look into any suspicious activity.

*****Fig. SHA256 Encryption*

SHA-256 introduces randomness through an initial value for hashing. When hashing "hello" for a password, the algorithm converts it to binary and employs logical and bitwise operations on fixed-size blocks. This results in a 256-bit hash, like "$2y$10$YO4C/ZUdUgJFgegAn0CA9u541m2cTmBPXZnIdn7whK55oNr4EFxaG," ensuring data integrity and irreversibility.

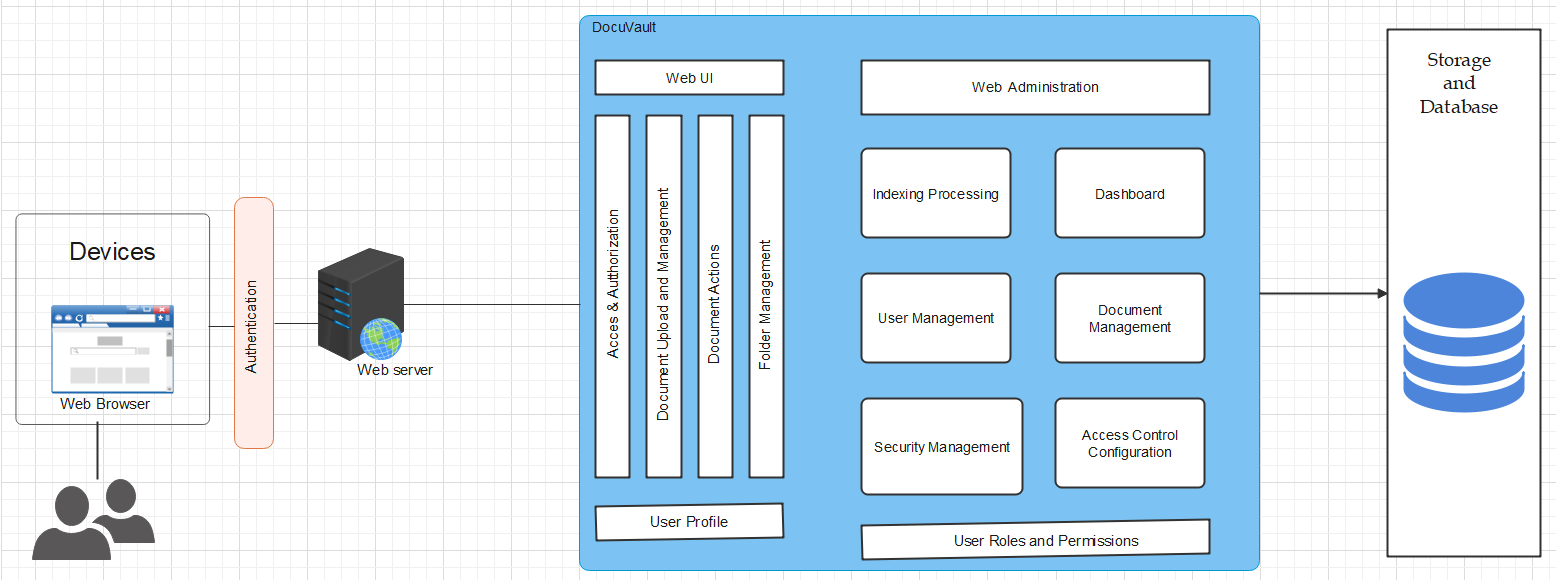
**Design of Software, Systems, Products and/or Process**

Use Case Diagram



*Fig. 6 Use case Diagram*

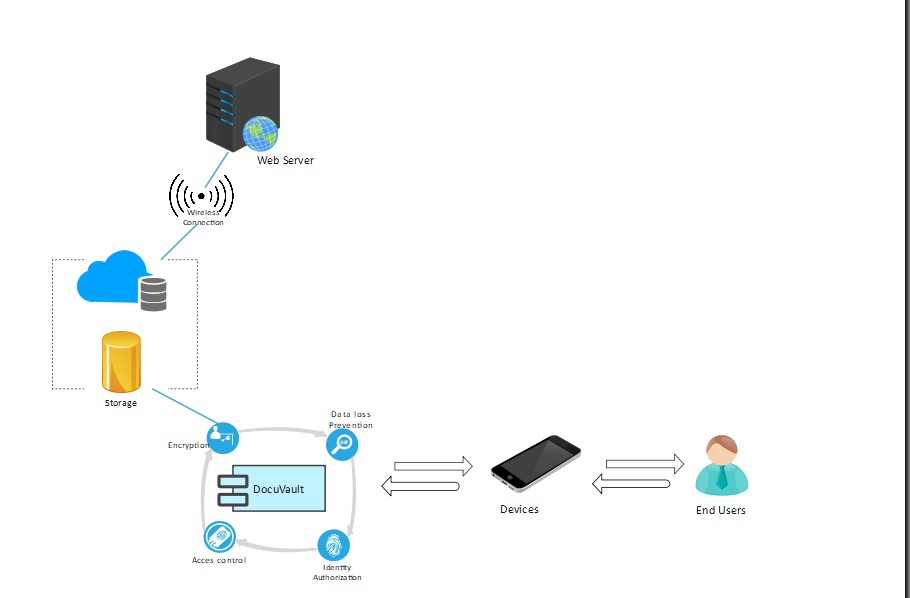
**System Architecture**

**** The system architecture refers to the overall design and structure of a system, including its components, user and admin interactions with the system, and relationships. It provides a representation of how different elements of a system work together to achieve a specific goal.

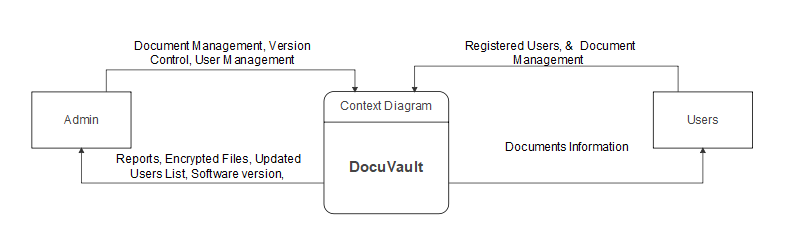
*Figure 7. System Architecture Diagram*

**Context Data Flow Diagram**

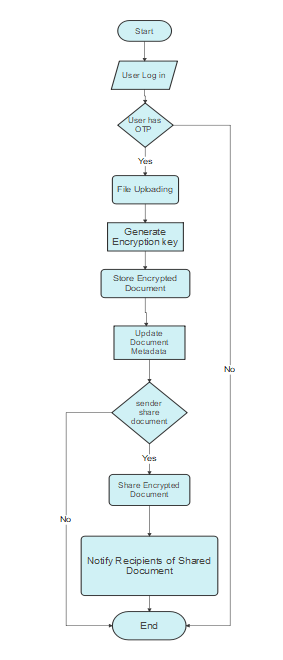
The context data flow in the system under description entails a smooth communication between different parts. End users interact with wirelessly networked devices to access a centralized web server. This server, which houses the website, responds to user inquiries and communicates with the storage system, which safely stores and retrieves data. Integration with the specific Docuvault system may happen in document management instances. The seamless exchange of requests and answers is ensured by the wireless connection, which makes it easier for devices to communicate with the web server. Devices, the web server, storage, and specialized systems work together to meet user demands as a coherent and effective system. The entire process is designed to give end users the desired data or services.

****

*Fig. 9 Workflow Diagram*



*Fig. 10 Data flow Diagram*



*Fig.N Flowchart of the file encryption process in User Interface*

1. Start:

The process begins here.

1. User Log In:

The user needs to provide their login credentials.

Successful, the process continues.

If the login fails, the process ends, indicating that the user could not be authenticated.

1. OTP Check:

If a user logs in successfully, an additional security check may involve an OTP authentication (One-Time Password).

If the OTP is valid, the process continues.

If the OTP is invalid, the process ends, indicating that the user failed the OTP check.

1. File Uploading:

The user uploads the file they want to encrypt.

1. Generate Encryption Key:

The system generates a unique encryption key. This key is essential for encrypting and decrypting the file.

1. Store Encrypted File:

The uploaded file is encrypted using the generated encryption key.

The encrypted file is stored securely, ensuring that only authorized users can access it.

1. Update Document Metadata:

Metadata associated with the document is updated. This might include information about the encryption status, the random key used, and other relevant details.

1. Share Encrypted Document:

Check if the sender wants to share the encrypted document with others.

If yes, the process continues.

If no, the process ends, indicating that the user does not want to share the document.

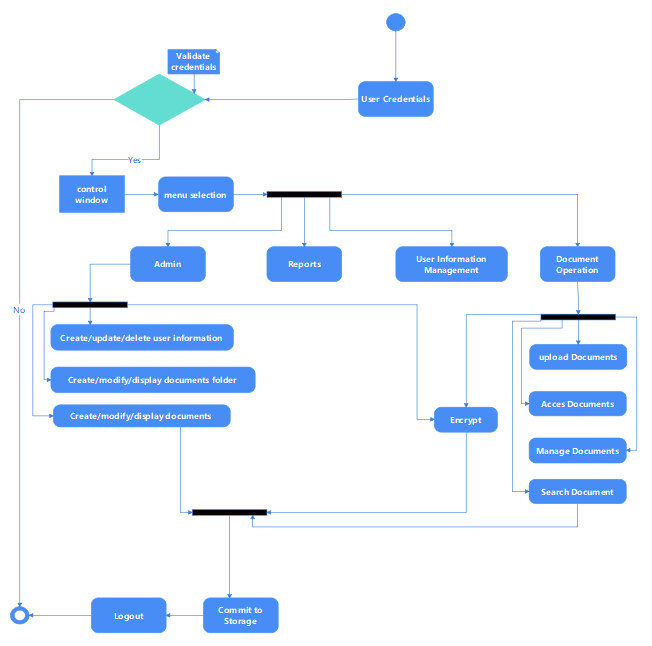
1. Notify Recipients:

If the sender wants to share the document, the system notifies the specified recipients about the shared encrypted document.

1. End:

The process concludes here.

This flowchart represents a series of steps involved in securing a document through encryption. It incorporates user authentication, an OTP check for added security, file uploading, key generation, secure storage, metadata updates, and an optional step for sharing the encrypted document with recipients. It's a structured representation of the file encryption process, helping to ensure security and proper handling of the encrypted files.



*Fig.n Activity Diagram*

**Development & Testing**

To bring about the effectiveness of the project, the survey questionnaire was utilized by the researcher. The basic objective of this evaluation is to determine the actual worth of the project as much as possible. The researcher used ISO/IEC 25010 to guarantee the efficacy, efficiency, and quality of systems and products in a variety of sectors. The International Organization for Standardization (ISO) sets requirements and guidelines. (ISO 25010, n.d.) In order to fully evaluate the ISO functioning of a system or product, it is necessary to use rigorous assessment tools that explore a variety of features and sub-features. These tools are essential for analyzing usability and functional appropriateness because they offer a comprehensive view of the system or product being studied. (ISO/IEC 25010:2011, n.d.)

Functional Suitability Characteristics:

1. Functional completeness

The degree to which the set of functions covers all the specified tasks and user objectives.

1. Functional correctness

The degree to which a product or system provides the correct results with the needed degree of precision.

1. Functional appropriateness

The degree to which the functions facilitate the accomplishment of specified tasks and objective.

Usability Characteristics:

1. Appropriateness recognizability

The degree to which users can recognize whether a product or system is appropriate for their needs.

1. Learnability

The degree to which a product or system can be used by specified users to achieve specified goals of learning to use the product or system with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use.

1. Operability

The degree to which a product or system has attributes that make it easy to operate and control.

1. User error protection

The degree to which a system protects users against making errors.

1. User interface aesthetics

The degree to which a user interface enables pleasing and satisfying interaction for the user.

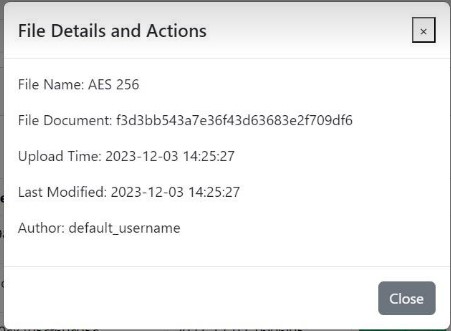
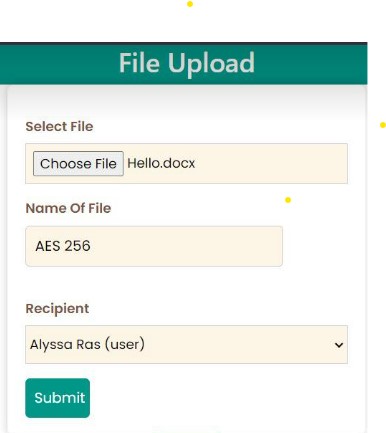
1. Accessibility

The degree to which a product or system can be used by people with the widest range of characteristics and capabilities to achieve a specified goal in a specified context of use.

**Encryption Output**

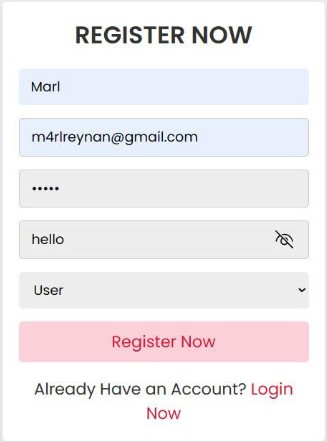
Encryption is a process of converting information or data into a secure form to prevent unauthorized access. AES256 encryption is used to secure the content of files, making them unreadable without the appropriate key. SHA256 hashing is employed to securely store and verify passwords by transforming them into irreversible hash values, adding an extra layer of protection against unauthorized access.

AES256



*Fig. AES256 encryption output*

SHA256



*Fig. SHA256 encryption Output*

A statistical method called Slovin's Formula may be used to calculate the ideal sample size for a given population size and allowable margin of error (Zach, 2023)

In the field of statistical research, choosing the right sample size is essential to guaranteeing the validity and applicability of study results to the whole population. It can be difficult for researchers to strike a balance between the limitations of their resources and the requirement for accuracy in their work.

The goal is to assess the Docuvault System for a total of 100 users who are spread throughout 10 workplaces. In order to preserve a 5% margin of error, or 0.05 in decimal notation, we want to make sure that the sample size is enough for making significant inferences about the total population.

The formula is calculated as follows:

S = N / (1 + Ne^2)

S = N / (1 + Ne^2)

S = 100 / (1 + 100(0.05)^2)

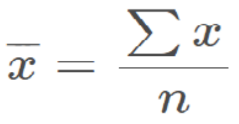
S ≈ 57

Thus, with a 5% margin of error, a sample size of 57 would be suitable for assessing the Docuvault System across the entire population of 100 people scattered over different offices around University of Antique. This sample size enables a thorough assessment of the system's efficacy in various office environments by allowing researchers to derive significant insights from the selected subset.

The descriptive statistics using the mean were employed to present the demographic characteristics of the respondents and the level of system effectiveness.

***Mean***

This is the average of the scores – the mathematical center of a distribution. It used symmetrical, unimodal distributions of interval or ration scores. The formula for mean is:

Where:

∑x = sum of all scores

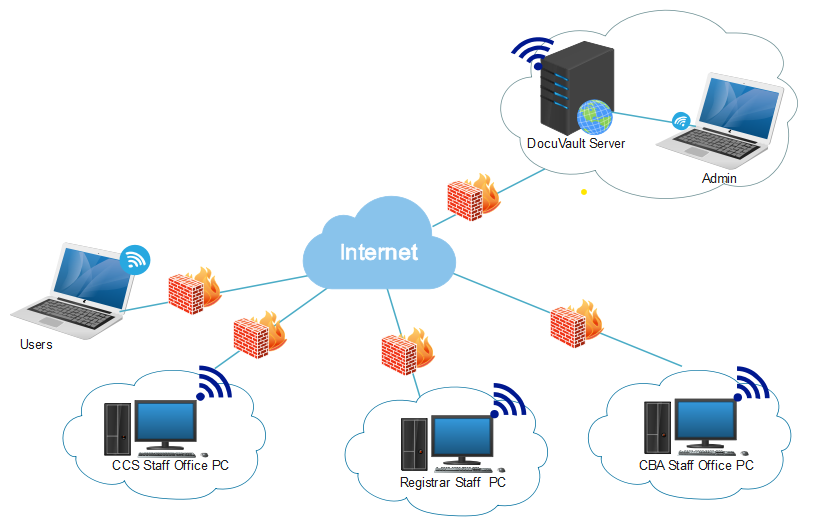
n = number of scores

***System Usability Scale***

The SUS survey has 10 statements and it uses a [Likert Scale](https://www.simplypsychology.org/likert-scale.html" \t "_blank). The user can evaluate at which level the statement is agreeable. So the user answers each question with a value between 1 and 5. Who is interpreting the data then has to apply a simple formula to the number.

* For each of the odd numbered questions, subtract 1 from the score.
* For each of the even numbered questions, subtract their value from 5.
* Take these new values which you have found, and add up the total score. Then multiply this by 2.5.

**Implementation Plan**

Deploying DocuVault on a strong server infrastructure is part of the implementation strategy, which guarantees safe document storage and centralized control. In order to facilitate flexibility and distant accessibility, users will access the system over wireless Internet. The documents will be protected during wireless communications by the use of strict security features including authentication methods and encryption. This strategy provides an effective and safe document management solution that is in line with current trends in remote work.

*Fig. Network Implementation*