duction

According to Levien (1989), any information that is recorded and structured into a unit for the purpose of human

consumption is referred to as a document. Organizing and extracting documents/records from large volumes of physical

documents are very difficult. It is possible for documents to be misplaced or even get lost, and they are also prone to

human error (Akashah et al., 2011). Many years ago, organization documents were stored and managed on paper, usually

regarded as a manual approach, and this approach is characterized by lots of inefficiencies and work-related issues such as

high time consumption, errors, and redundancy during information collection, storage, and retrieval (Mehandjiev et al.

2013, Balogun, et al. 2019). Heckman (2008) was of the view that without the use of an efficient and effective document

management system, it is almost certain that the management of documents will always be prone to human error.

An **Electronic Document Management System (EDMS)** is software designed to manage, store, and track electronic documents securely. When it is **secure and cloud-based**, it means the system operates on the cloud with advanced security measures to protect sensitive information.

 When a document is uploaded to the EDMS, **AES encrypts it before storing it** in the cloud or database.

 This ensures that **even if someone gains access to the storage location, they cannot read the file** without the encryption key.

AES (**Advanced Encryption Standard**) is a widely used encryption algorithm that secures digital data by converting it into an unreadable format. Only authorized users with the correct **decryption key** can access the original information.

**AES Algorithm Steps**

**1. Key Expansion (Key Schedule)**

* The encryption key is **expanded into multiple round keys** using a key schedule.
* The number of rounds depends on the key size:
  + **AES-128:** 10 rounds
  + **AES-192:** 12 rounds
  + **AES-256:** 14 rounds

**2. Initial Round**

* **AddRoundKey:** The first round key is XORed with the plaintext block.

**3. Main Rounds (Repeated for Each Round)**

Each round consists of four transformation steps:

**Step 1: SubBytes (Substitution)**

* Each byte in the data block is replaced using a **S-Box (Substitution Box)**, which introduces non-linearity.

**Step 2: ShiftRows**

* Rows in the 4x4 byte matrix are **shifted left** in a cyclic manner.
  + **Row 0:** No shift
  + **Row 1:** 1-byte shift
  + **Row 2:** 2-byte shift
  + **Row 3:** 3-byte shift

**Step 3: MixColumns (Not in the Last Round)**

* Each column is transformed using **matrix multiplication** in Galois Field (**GF(2^8)**), ensuring diffusion (spreading of plaintext information across ciphertext).

**Step 4: AddRoundKey**

* The **round key** is XORed with the current state.

**4. Final Round (No MixColumns)**

* The last round is slightly different:
  + **SubBytes**
  + **ShiftRows**
  + **AddRoundKey**

3.1.1. Security

This is an absolute necessity for any electronic document management system. A strict security system allows

authorized persons to perform the necessary duties. Before the file can be transferred, it must be encrypted for security

purposes. Likewise, document access is restricted to the authorized department (even within the organization) and for the

authorized employee/staff only.

3.1.2. Level of Abstraction

This feature ensures that document access is restricted to the authorized department (even within the

organization) and for the authorized employee only.

A staff working on a client machine will store and retrieve documents within their own directory stored inside the

department. The system allows a staff to access only their files and not of any other staff. Also, files from one particular

department will not be authorized for staff of the other department. Documents that are common to all departments will

be put in a common directory to which every staff has access

"Sub Bytes" in AES (Advanced Encryption Standard) refers to a step in the encryption process where each individual byte of data is replaced with another byte based on a predefined lookup table called an "S-box",

What is meant by digital signature?

A digital signature—a type of electronic signature—is a mathematical algorithm routinely used to validate the authenticity and integrity of a messag

Base64 encoding is a way to represent binary data as a string of printable characters. It's used to transport binary data over mediums that can't handle binary data formats.

3.1.6. File Versioning

This feature of the system keeps track of the versions of a particular document over time. Staff working on a

particular document over a period of days may want to revert to a previous version of the same file. For this, the server

will keep multiple copies of the same file on it.

3.1.3. Workflow Services

This feature of the system allows users to route files from worker to worker in an organized way which includes

the ability to prioritize the sending of files based on the sender-designated hierarchy order.

3.1.7. Data Recovery

This feature makes it possible to restore data that has been lost, accidentally deleted, corrupted, or made

inaccessible. Common causes of data loss include power outages, natural disasters, equipment failures or malfunctions,

accidental deletion of data, software crashes, and logical errors. However, this system takes care of these incidents and the

information about that file is stored in different places.

A **Secured Cloud-Based Electronic Document Management System (SECEDAMAS)** is designed to store, manage, and retrieve documents securely over the internet.

**How It Works:**

1. **Uploading Documents**
   * Users create a document (internal or external).
   * They upload it through a web-based interface.
   * While uploading, they enter details like file name, folder, and description.
   * Users also set access permissions (who can view or edit).
2. **Storage & Security**
   * The system encrypts the document using **AES-256 and AES-128** encryption for security.
   * Encrypted documents are stored on a **file server** (a central storage system).
   * System data is stored in a **database server** for security and organization.
3. **Retrieving & Sharing**
   * Users can search for documents using a **search engine**.
   * Security settings control who can view or share documents.
   * Documents can be opened or shared based on permissions.

**Why It's Secure?**

* Uses **encryption (AES-256, AES-128)** to protect documents.
* Authentication ensures only authorized users can access files.
* Database and file servers provide **safe storage and controlled access**.

This system makes document management **easy, secure, and accessible from anywhere** via the cloud.

The document can either be internal or external. After the document has been created, the user goes online and uploads the document through the web-based interface. During document uploading, the user needs to fill in some data fields that provide the metadata or indexing tags (e.g., file name, folder name, document description)

. This system leveraged AES-256 and AES-128 encryptions provided by Laravel (a PHP framework), which provides us with a powerful encryption service. It uses Open SSL for encryption and Base64 for encoding the files on the server

. The encrypted and encoded document/file is then stored in the file server.

The database server is used to store system data and operate the entire system. The reason behind using this server is to increase system security and archiving