Project Report

On

ENHANCING DATA SECURITY USING DIGITAL WATERMARKING

Submitted to

Sant Gadge Baba Amravati University, Amravati

In recognition to partial fulfillment of the requirement

For the award of degree in

Bachelor of Engineering

(Computer Science & Engineering)

By

Nayan S. Thorat

Prathamesh A. Yelne

Zibal A. Khan

Om V. Ubhad

Shraddha V. Jaiswal

B.E. (CSE) VIII Semester

Under the Guidance of

Prof. Chetan R. Ingole

Department of Computer Science & Engineering

Prof Ram Meghe College of Engineering and Management, Badnera-Amravati

2022-2023

CERTIFICATE

This is to certify that the Project Report on

ENHANCING DATA SECURITY USING DIGITAL WATERMARKING

is a bonafide work submitted by

Nayan S. Thorat
Prathamesh A. Yelne
Zibal A. Khan
Om V. Ubhad
Shraddha V. Jaiswal

B.E. (CSE) VIII Semester

In recognition to partial fulfillment of the requirement for the award of degree in

Bachelor of Engineering in Computer Science & Engineering

To

Sant Gadge Baba Amravati University, Amravati

during the academic year 2022-2023

Under the guidance of

Prof. Chetan R. Ingole
Project Guide

Dr. Dinesh G. Harkut
Head

(_____)
External Examiner

Date of Examination: ___/___/2023

Department of Computer Science & Engineering

Prof Ram Meghe College of Engineering and Management, Badnera-Amravati

2022-2023

ACKNOWLEDGEMENT

It gives me immense pleasure to express my gratitude to **Prof. Chetan R. Ingole,** my guide who provided me constructive criticism and positive feedback during the preparation of this project. I am indebted to **Dr. Dinesh. G. Harkut,** Head of Department Computer Science and Engineering and other teaching and non-teaching staff who were always there whenever I needed any help. Without them and their co-operation, completion of this project work would have been difficult. Most importantly, I am thankful to my parents, who constantly motivated me during this work.

Nayan S. Thorat (Roll. No. 66)
Prathamesh A. Yelne (Roll. No. 74)
Zibal A. Khan (Roll. No. 30)
Om V. Ubhad (Roll. No. 70)
Shraddha V. Jaiswal (Roll. No. 25)

B. E. (CSE) VIII Semester

CONTENTS

ABSTRACT

Digital watermarking is a relatively new area of study that has attracted the interest of many academic and commercial researchers. Digital watermarking is a relatively new research area that has stimulated the interest of numerous researchers in academia and industry, and it has quickly evolved into one of the most frequently studied topics in the multimedia signal community. Although the term "watermarking" has a few various definitions in the literature, the following seems to be the most common. Watermarking is the practice of altering data invisibly in order to include information about the data. The definition above reveals two key features of watermarking.

First, information embedding should not cause perceptible changes to the host medium (sometimes called cover medium or cover data). Second, consider the message should be linked to the server medium. Watermarking techniques, in this sense, are a subset of hiding data techniques, which also include cases where the hidden information is unrelated to the host medium (e.g., in covert communications).

However, some authors be using the term watermarking to mean the same thing as information hiding in general. A watermarking system should be composed of two distinct modules: one that embeds the information in the host data and another that detects whether a given piece of data contains a watermark and then retrieves the conveyed information. and industry, and has emerged as one of the most hotly debated research topics in the multimedia signal processing community. Although the term "watermarking" has a few different definitions in the literature, the following appears as a popular definition: Watermarking is the practice of altering data invisibly in order to embed data-related information within it. The definition above reveals two key features of watermarking.

For starters, information embedding also shouldn't cause visible changes to the host medium (sometimes called cover medium or cover data). The message should also be related to the host intermediate. Watermarking techniques, in this sense, are a subset of data hiding techniques, which also include cases where the information is unrelated to the host medium (e.g., in covert communications). Although some authors use the term "watermarking" to mean information hiding in general, this is not the case.

LIST OF FIGURES

LIST OF SCREENSHOTS

INTRODUCTION

1. INTRODUCTION

1.1 Basic Definition

Digital watermarking is a technique used for both copyright protection and authentication. This paper presents a nested type of watermarking (a watermark inside another watermark) using digital watermark embedding and extraction techniques. The main benefit of using the nested watermarking method is that it increases the embedding capacity, allowing for the embedding of a large amount of information. In this method, one watermark is embedded within another. The resulting watermark is regarded as the primary watermark. The primary watermark is encrypted before being embedded in the main image. The main reason for encrypting the watermarks before embedding them is to increase security. The A5/1 encryption algorithm is used for encryption and decryption. As a result, our research work Therefore, our research work focuses on two important things i.e., increased watermark embedding capacity and increased safety.

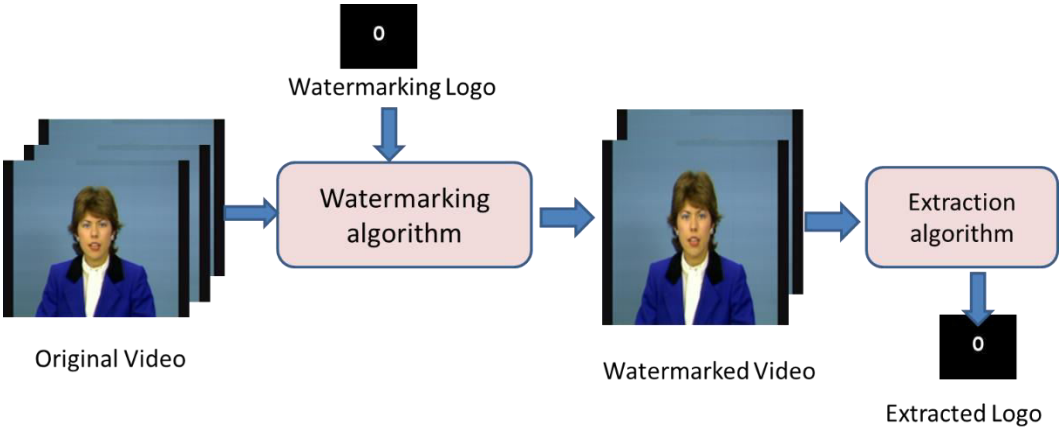


Figure 1.1 Process of Watermarking

Because of increased Internet usage and rapid advancements in the IT industry, digital media files can now be accessed and obtained from the internet in a more convenient manner. As a result, original digital contents face a variety of issues, including copyright infringement, easier modification, and faster content delivery over the Internet. As a result, data piracy and copyright protection have become serious issues in order to protect ownership rights. As a result, in order to resolve these issues, some safeguards must be implemented. Many new techniques for

information concealment and security have been developed. Steganography is a powerful tool that allows any information to be hidden inside any object.

1.2 Basic Concepts

A digital watermark is a "stamp" that has been added to the original document in the form of text (or another photo/image). The additional information can be more or less transparent, making it easier or more difficult to notice the watermark. The added security of a watermark is twofold. Not only does a watermark dissuade individuals from leaking documents, but in the event that a leak occurs, the source of the leak can be easily identified when a watermark with the authorized recipient's name is placed on the file. As more communication and collaboration happens in the digital space, the need for maintaining data and document integrity is growing. In fact, 49 percent of companies will increase their cloud security budget in the next 12 months. As an added layer of security, organizations across all sectors often choose to watermark their documents when shared internally or externally. A digital watermark is data that is inserted into digital data such as audio, video, or images. The data can be inserted into binary images. These data or information can be detected or extracted in the coming days to make a claim about the data, such as who owns it. This information can take the form of text containing information about the owner and copyright information, or it can take the form of an image. If the original owner must be identified, or if any material is duplicated, the contents of digital data inside which the information to be hidden is embedded will be manipulated.

Watermarking discourages recipients from engaging in data exfiltration activity, ensuring that sensitive information such as contracts, budgets, health records, product roadmaps, or manuscripts remains private and compliant throughout its lifecycle, allowing you to collaborate confidently. A watermark provides two layers of security. A watermark not only discourages individuals from leaking documents, but it also allows the source of the leak to be easily identified if a watermark with the authorised recipient's name is placed on the file. Watermarking also disables print and download, providing senders with another mechanism to protect sensitive data.

LITERATURE REVIEW

2. LITERATURE REVIEW

2.1 Previous Research

M. Dobsicek et al. [1] describes the fundamentals of steganography and the various image steganography techniques. Steganography is one powerful method for concealing confidential information within any object. The information can be embedded using a variety of objects. Files of text, image, audio, or video are all examples of objects. How to increase embedding capacity, maintain integrity, and provide security for embedded data are major topics covered in this paper. The most common method for hiding secret information within an object is image steganography. As part of future enhancement, the paper recommends maintaining integrity and increasing embedding capacity.

Changsheng Xu, Yusuk Lim, and Others [2] describes the digital image watermarking web-based image authentication method. The paper also talks about the Internet-based client-server model and different ways to embed watermarks. The paper likewise examines about delicate watermark.

Bede Liu, Fellow of the IEEE, Min Wu, Member of the IEEE, and others [3] talks about how to embed data in binary images. The author also discusses the manipulation of flappable pixels. The paper also discusses a number of issues that arise when data is hidden in binary images.

Harpuneet Kaur, R. S. Salaria et al. [4] The author talks about adding more watermark bits to the main image so that more information can be embedded there without affecting the image's integrity. Additionally, the author suggests a method for encrypting the watermark prior to embedding to enhance the security of the embedded data.

Nameer N. EL-Emam and Associates [5], the author describes how a new algorithm was used to hide a lot of data in a color bitmap image. Image segmentation and filtering are two

examples of various approaches that have been utilized. It is possible to embed a large amount of data, and the quality of the output is also high.

Preeti Gupta and others T+he topic of embedding the data into the gray scale image is addressed in [6]. Additionally, it explains how more watermark bits can be added to the main image without affecting its imperceptibility. Encryption of the watermark has been finished to build the security of the installed data. The author has also talked about the idea of watermarks nesting.

R. K. Tiwari, G. Sahoo, and others [7] talks about steganography methods that are only based on the file hybridization method. What does file hybridization mean? Multiple image files are used to embed the data or information rather than just one. Additionally, the author discusses the various security options available to safeguard embedded data.

RK Arya, S. Singh, R. Saharan, and others [8], the author places a greater emphasis on the watermarking process's past developments and the security provided for embedded data. The paper also discusses steganography methods for protecting confidential information like copyright information, could be incorporated into the cover or main image.

Hatzinakos, Kundur, et al. [9], the author has reviewed and modified LSB-based methods for digital rights protection, including the discrete wavelet transform and singular value decomposition. The cover image is divided into four parts, and a recursive algorithm will be used on each of the four parts.

A. Kumar and others [10], this paper examines a variety of medical watermarking algorithms. They provided various techniques and their components in tabular form toward the end of the paper, along with the survey, customary abstraction of watermarking, major features, area of applications, concepts of implant and retrieval of watermarks.

A. Anand, A.K. Singh, et al. [11] The use of cutting-edge technology for embedding capacity and superior imperceptibility is utilized to provide robust authentication to enhance security.

Mohammad Shorif Uddin, Mahbuba Begum, and others [12], an in-depth investigation of a variety of digital watermarking techniques has been presented. An explanation of a framework for creating a hybrid watermarking method is given. Different hybrid methods' comparative analyses have been discussed.

A. Ray, S. Roy, et al. [13], a number of approaches to watermarking have been suggested in order to safeguard copyright-protected data. Additionally, the most recent advancements in various watermarking methods are discussed in this paper. Additionally, this paper provides a method for investigating methodical watermarking strategies for protecting authentic data.

S.P. Ambadekar, J. Jain, J. Khanapuri, and others [14], the watermarking method has been utilized to safeguard the copyright data. The DWT (Discrete Wavelet Transform) method is used for watermark embedding and extraction. Additionally, encryption is performed to enhance data security. The primary objective of this paper is to enhance authenticity protection.

N. Agarwal, A. K. Singh, and P. K. Singh, et al. [15] In various domains, including the transform domain and the spatial domain, a variety of rigorous and undetectable watermarking techniques have been presented. The paper also discusses a variety of watermarking features, applications, and ideas.

2.2 Methodology

With each organization looking for a benefit in its separate market, exclusive data is strictly confidential. Protecting intellectual property and company assets is made easier with data security. In addition, almost every business processes and stores customer data. A company's reputation is safeguarded and customer loyalty is ensured by safeguarding that data. Companies use data security to stop malicious attackers from stealing customer information from receiving, storing, or transmitting it. However, protecting customer data not only protects a company's

reputation but also saves money because many regulations impose penalties on businesses that fail to implement adequate security measures. In a nutshell, data security aims to safeguard technology, processes, and people. Implementing the most recent tools is only one aspect of data security. While software and tools are essential, good security also involves a process. The impact and scope of a cybersecurity attack are determined by the strategies and procedures implemented by businesses. Security flaws can be found in people as well as in systems.

This comprehensive blog post explains the best data security practices for large businesses. While cyber security methodologies based upon the separation of asset groups and the control of group interconnectivity—such as the methodologies of ISA-62443's "zone and conduit" and the McAfee "3 × 3" cyber security model—are good practice in general, they can be difficult to apply to a system as broad and highly interconnected as a Smart Grid. By carefully mapping a Smart Grid's architecture to these methodologies, an adequate security methodology can be achieved, and a workable reference model can be built. This reference model is a useful tool for security planning and implementation, and has been used extensively in Chapter 6, "Protecting the Smart Grid."

PROBLEM DEFINITION AND REQUIREMENT ANALYSIS

3. PROBLEM DEFINITION AND REQUIREMENT ANALYSIS

3.1 Problem Definition

Due to its scalability and pay-as-you-go features, cloud computing is rapidly gaining popularity. Cloud platforms are being used by many businesses to store important documents. Cloud service providers should improve document security to prevent leakage as tenants demonstrate trust. We proposed a cloud-based social networking system for this project, in which media content will be outsourced to the cloud. If a user transmits another user's content or leaks another user's document, there is a risk of document leakage. As a result, we suggested a watermarking method to prevent document leakage and an XOR-based encryption method to secure document encryption.

3.2 Requirement Analysis

3.2.1 Statement of Scope

Security depends greatly on how a system was designed, so it’s very important to capture security requirements at the requirements engineering phase. Previous research proposes different approaches, but each is looking at the same problem from a different perspective such as the user, the threat, or the goal perspective. This creates huge gaps between them in terms of the used terminology and the steps followed to obtain security requirements. This research aims to define an approach as comprehensive as possible, incorporating the strengths and best practices found in existing approaches, and filling the gaps between them. To achieve that, relevant literature reviews were studied and primary approaches were compared to find their common and divergent traits.

To guarantee comprehensiveness, a documented comparison process was followed. The outline of our approach was derived from this comparison. As a result, it reconciles different perspectives to security requirements engineering by including: the identification of stakeholders, assets and goals, and tracing them later to the elicited requirements, performing risk assessment in conformity with standards and performing requirements validation. It also

includes the use of modeling artifacts to describe threats, risks or requirements, and defines a common terminology.

3.2.2 Aim of the Project

i) To develop an online social networking system with media files leakage detection and prevention techniques.

ii) To implement watermarking techniques for leakage detection.

iii) To implement RC6 encryption algorithm for metadata file encryption.

iv) To implement XOR encryption algorithm for media files encryption and watermarking.

PROPOSED APPROACH AND DESIGN

4. PROPOSED APPROACH AND DESIGN

4.1 Proposed Approach

Cloud computing is rapidly gaining popularity due to its scalability and pay-as-you-go features. Numerous businesses store important documents on cloud platforms. As tenants demonstrate trust, cloud service providers should enhance document security to prevent leaks. For this project, we proposed a social networking system that is cloud-based and will outsource media content to the cloud.

There is a possibility of document leakage if a user transmits another user's content or documents. Consequently, we suggested an XOR-based encryption method to secure document encryption and a watermarking method to prevent document leakage.

4.1.1 Block Schematic

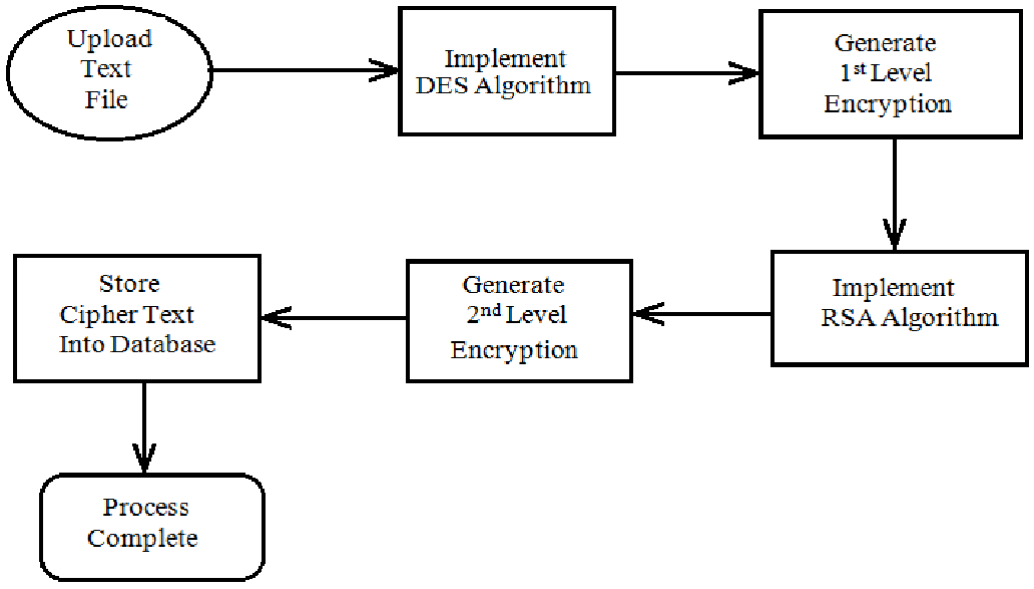


Figure 4.1.1 Block Schematic of Data Security

4.1.2 Algorithm

A) AES (Advanced Encryption Standard)

AES Encryption algorithm (also known as the Rijndael algorithm) is a symmetric block cipher algorithm with a block/chunk size of 128 bits. It converts these individual blocks using keys of 128, 192, and 256 bits. Once it encrypts these blocks, it joins them together to form the ciphertext. It is based on a substitution-permutation network, also known as an SP network. It consists of a series of linked operations, including replacing inputs with specific outputs (substitutions) and others involving bit shuffling (permutations).

How AES encryption works

AES includes three block ciphers:

1. AES-128 (10 - round) uses a 128-bit key length to encrypt and decrypt a block of messages.
2. AES-192 (12 - round) uses a 192-bit key length to encrypt and decrypt a block of messages.
3. AES-256 (14 – round) uses a 256-bit key length to encrypt and decrypt a block of messages.

Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively.
Symmetric, also known as secret key, ciphers use the same key for encrypting and decrypting. The sender and the receiver must both know -- and use -- the same secret key.
The government classifies information in three categories: Confidential, Secret or Top Secret. All key lengths can be used to protect the Confidential and Secret level. Top Secret information requires either 192- or 256-bit key lengths.
There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. A round consists of several processing steps that include substitution, transposition and mixing of the input plaintext to transform it into the final output of ciphertext.

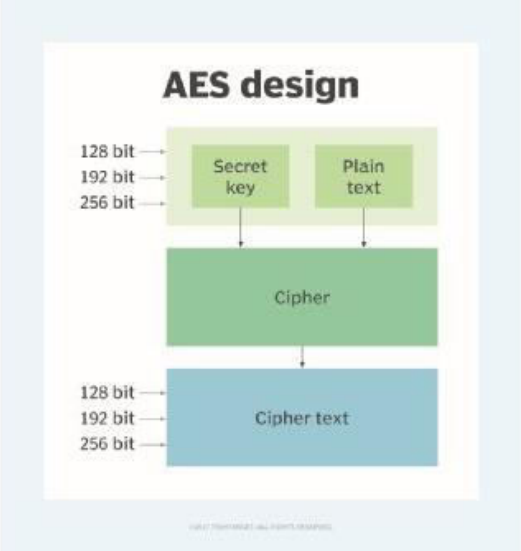


Figure 4.1.2 (a) AES Design

- The AES encryption algorithm defines numerous transformations that are to be performed on data stored in an array.
- The first step of the cipher is to put the data into an array, after which the cipher transformations are repeated over multiple encryption rounds.
- The first transformation in the AES encryption cipher is substitution of data using a substitution table.
- The second transformation shifts data rows.
- The third mixes columns.
- The last transformation is performed on each column using a different part of the encryption key. Longer keys need more rounds to complete.

Is AES secure?

Security experts maintain that AES is secure when implemented properly. However, AES encryption keys need to be protected. Even the most extensive cryptographic systems can be vulnerable if a hacker gains access to the encryption key.

To ensure the security of AES keys:

- Use strong passwords.
- Use password managers.

- Implement and require multifactor authentication (MFA).
- Deploy firewalls and antimalware software.
- Conduct security awareness training to prevent employees from falling victim to social engineering and phishing attacks.

B) DES (Data Encryption Standard

Data Encryption Standard (DES) is a block cipher algorithm that takes plain text in blocks of 64 bits and converts them to ciphertext using keys of 48 bits. It is a symmetric key algorithm, which means that the same key is used for encrypting and decrypting data.

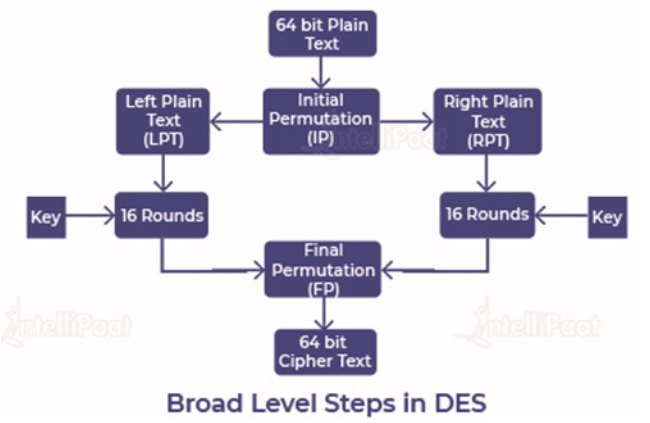


Figure 4.1.2 (b) DES Steps

There are certain machines that can be used to crack the DES algorithm. The DES algorithm uses a key of 56-bit size. Using this key, the DES takes a block of 64-bit plain text as input and generates a block of 64-bit cipher text. The DES process has several steps involved in it, where each step is called a round. Depending upon the size of the key being used, the number of rounds varies.

For example, a 128-bit key requires 10 rounds, a 192-bit key requires 12 rounds, and so on. The DES (Data Encryption Standard) algorithm is a symmetric-key block cipher created in the early 1970s by an IBM team and adopted by the National Institute of Standards and Technology (NIST). The algorithm takes the plain text in 64-bit blocks and converts them into ciphertext using 48-bit keys. Since it's a symmetric-key algorithm, it employs the same key in

both encrypting and decrypting the data. If it were an asymmetrical algorithm, it would use different keys for encryption and decryption.

Initial Permutation (IP)

The plain text is divided into smaller chunks of 64-bit size. The IP is performed before the first round. This phase describes the implementation of the transposition process. For example, the 58th bit replaces the first bit, the 50th bit replaces the second bit, and so on.

The resultant 64-bit text is split into two equal halves of 32-bit each called Left Plain Text (LPT) and Right Plain Text (RPT).

Step 1: Key Transformation

- We already know that the DES process uses a 56-bit key, which is obtained by eliminating all the bits present in every 8th position in a 64-bit key. In this step, a 48-bit key is generated. The 56-bit key is split into two equal halves and depending upon the number of rounds the bits are shifted to the left in a circular fashion.
- Due to this, all the bits in the key are rearranged again. We can observe that some of the bits get eliminated during the shifting process, producing a 48-bit key. This process is known as compression permutation.

Step 2: Expansion Permutation

- Let's consider an RPT of the 32-bit size that is created in the IP stage. In this step, it is expanded from 32-bit to 48-bit. The RPT of 32-bit size is broken down into 8 chunks of 4 bits each and extra two bits are added to every chunk, later on, the bits are permutated among themselves leading to 48-bit data.
- An XOR function is applied in between the 48-bit key obtained from step 1 and the 48-bit expanded RPT.

Triple DES Algorithm

- Triple DES is a symmetric key-block cipher which applies the DES cipher in triplicate.
- It encrypts with the first key (k1), decrypts using the second key (k2), then encrypts with the third key (k3). There is also a two-key variant, where k1 and k3 are the same keys.

Key Takeaways

- The NIST had to replace the DES algorithm because its 56-bit key lengths were too small, considering the increased processing power of newer computers.
- Encryption strength is related to the key size, and DES found itself a victim of the ongoing technological advances in computing.
- It reached a point where 56-bit was no longer good enough to handle the new challenges to encryption.
- Note that just because DES is no longer the NIST federal standard, it doesn't mean that it's no longer in use. Triple DES is still used today, but it's considered a legacy encryption algorithm.
- Note that NIST plans to disallow all forms of Triple-DES from 2024 onward.

DES Algorithm Steps

To put it in simple terms, DES takes 64-bit plain text and turns it into a 64-bit ciphertext. And since we're talking about asymmetric algorithms, the same key is used when it's time to decrypt the text.

The algorithm process breaks down into the following steps:

1. The process begins with the 64-bit plain text block getting handed over to an initial permutation (IP) function.
2. The initial permutation (IP) is then performed on the plain text.
3. Next, the initial permutation (IP) creates two halves of the permuted block, referred to as Left Plain Text (LPT) and Right Plain Text (RPT).
4. Each LPT and RPT goes through 16 rounds of the encryption process.

5. Finally, the LPT and RPT are rejoined, and a Final Permutation (FP) is performed on the newly combined block.
6. The result of this process produces the desired 64-bit ciphertext.

C) XOR (Exclusive OR)

XOR, or "exclusive or" operates on binary data. It returns true if both of its inputs are opposites (one false and one true), otherwise, it returns false. You may see the operator written this way: ⊕.

Input		Output
A	B	A xor B
0	0	0
1	0	1
1	0	1
1	1	0

Figure 4.1.2 (c) XOR Table

For example, in Go, the code would be something like:

```
func exclusiveOr(a bool, b bool) bool {
        return a != b
}
```

XOR Cipher - The Perfect Cipher

It is interesting to note that if:

1. The key is the same size as the message
2. The key is kept secret and generated truly randomly

Then the XOR cipher is certainly **impossible** to crack. This is known as a one-time pad. However, a simple XOR shouldn't be used in production due to the key length needing to be too long to be practical.

Cipher Example

For instance, let's simply encrypt the word "hi"

1. First, convert "hi" to binary, here is a free tool) 01101000 01101001
2. Next, create a random secret key that has the same length: 01010010 01000101
3. Then, create an encrypted message by XOR'ing the message and the key: 01101000 01101001 ("hi")
   XOR 01010010 01000101 (secret key) = 00111010 00101100 (encrypted message)
4. Finally, decrypt the message by XOR'ing the key with the encrypted message again: 00111010 00101100 (encrypted message)
   XOR 01010010 01000101 (secret key) = 01101000 01101001 ("hi")

Why does it work?

XOR works as a cipher because it is its own inverse.

$a = (a \oplus b) \oplus b$

And, as we demonstrated in our example:

$encrypted = message \oplus key$

and

$message = encrypted \oplus key$

Is XOR used in production ciphers?

The simple XOR cipher isn't used in production because it is impractical to use keys that are the same length as the message body. However, the XOR is still extremely useful. In fact, it is used in almost all symmetric encryption algorithms. XOR is the primary operation in the "add round key" step of AES-256. It is also used in the DES cipher

C) SHA-256 Algorithm

SHA 256 is part of the SHA 2 family of algorithms, where SHA stands for Secure Hash Algorithm. It was released in 2001. It was a joint effort between the NSA and NIST to introduce a successor to the SHA 1 family, which was slowly losing strength against brute force attacks.

The meaning of 256 in the name means the final hash digest value, ie. regardless of the size of the plaintext/plaintext, the hash value is always 256 bits. Other algorithms in the SHA family are more or less similar to SHA 256. Now take a look to know a little more about these instructions.

A cryptographic hash function creates a "fingerprint" of the input string. For example, if we hashed the entire text of JRR Tolkien's Lord of the Rings series using the SHA 256 algorithm, we would get a 256-bit output that is unique to the text of that book. If we changed even one letter in the book, the output hash would be very different. It is worth noting that the hash output is "almost unique" due to the limited number of output queues. After all, SHA-256 output is always 256 bits long, which means it has a fixed size. However, the number of possible returns is infinite, which means that some returns will split into the same output. When this happens, it is called a "crash" and is almost impossible. After all, SHA-256 has 2^256 possible outputs.

SHA-2 is known for its security (it hasn't broken down like SHA-1) and its speed. In cases where keys are not generated, such as proof-of-work Bitcoin mining, a fast hash algorithm like SHA-2 often has the upper hand. SHA-256 is formally defined in the National Institute of Standards and Technology's FIPS 180-4. Along with standardization and formalization comes a list of test vectors that allow developers to ensure they've implemented the algorithm properly. As of 2022, SHA-256 is plenty secure to use in your applications.

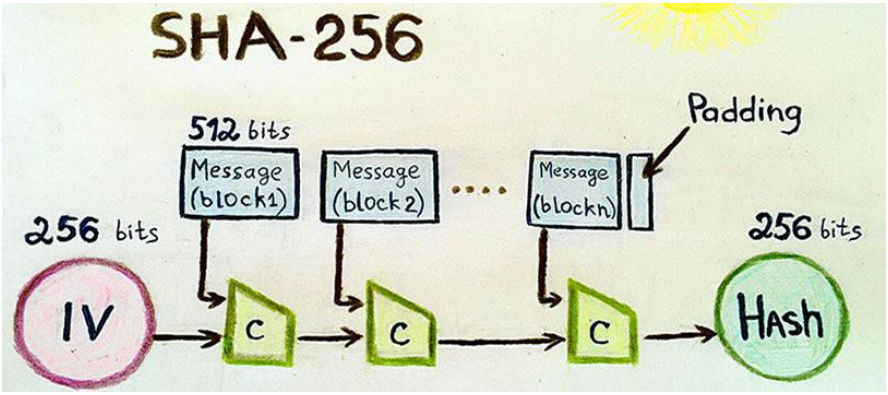


Figure 4.1.2 (d) SHA-256

What is Hashing?

Hashing is the process of scrambling raw information to the extent that it cannot reproduce it back to its original form. It takes a piece of information and passes it through a function that performs mathematical operations on the plaintext. This function is called the hash function, and the output is called the hash value/digest.

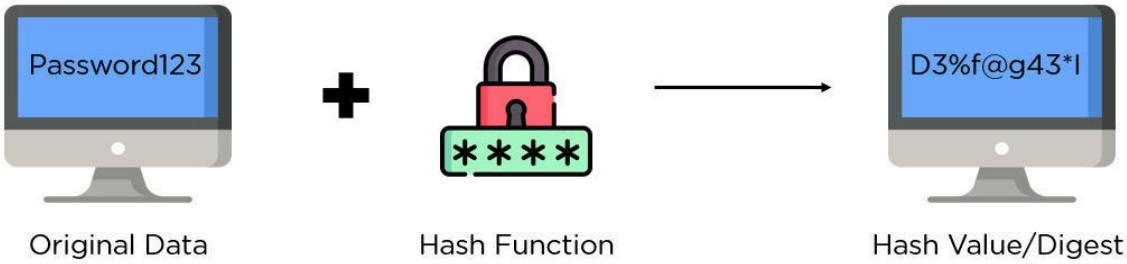


Figure 4.1.2 (e) Hashing Value

As seen from the above image, the hash function is responsible for converting the plaintext to its respective hash digest. They are designed to be irreversible, which means your digest should not provide you with the original plaintext by any means necessary. Hash functions also provide the same output value if the input remains unchanged, irrespective of the number of iterations.

There are two primary applications of hashing:

i. **Password Hashes:** In most website servers, it converts user passwords into a hash value before being stored on the server. It compares the hash value re-calculated during login to the one stored in the database for validation.

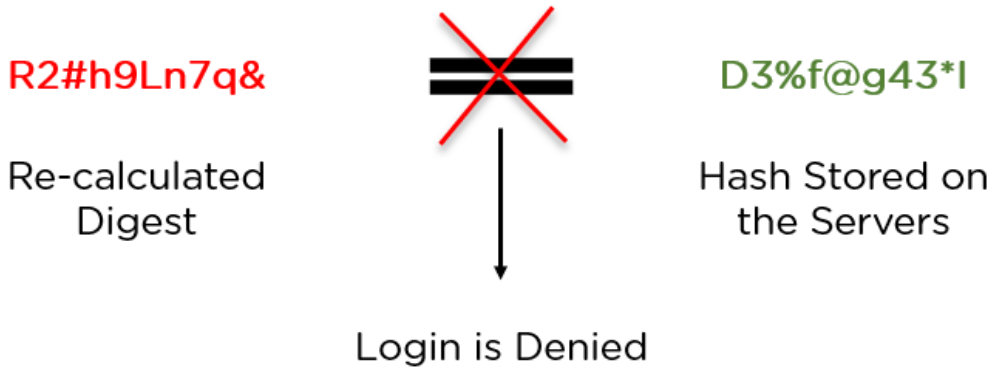


Figure 4.1.2 (f) Password Hashing

ii. **Integrity Verification:** When it uploads a file to a website, it also shared its hash as a bundle. When a user downloads it, it can recalculate the hash and compare it to establish data integrity.

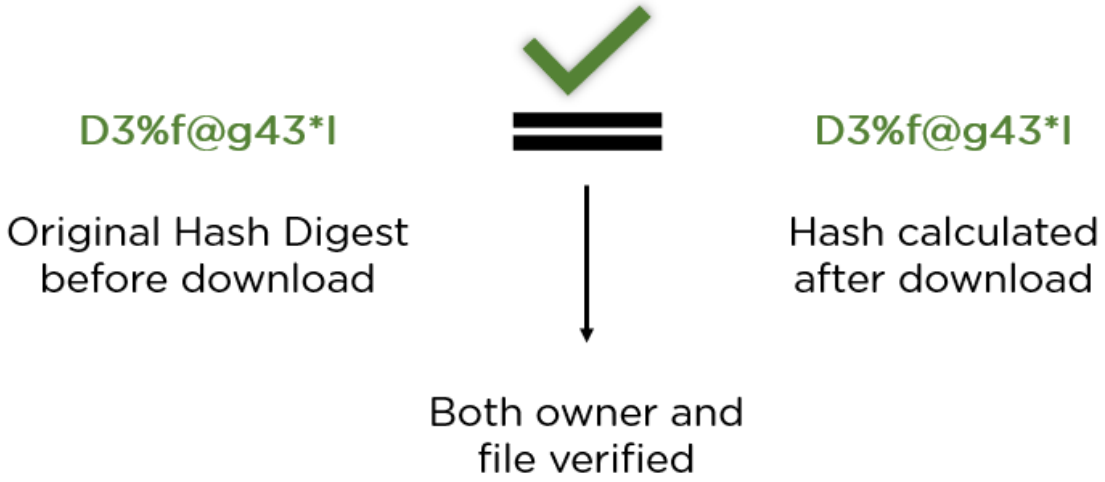


Figure 4.1.2 (g) Integrity Verification

D) RC6 Algorithm

RC6 is a fast block cipher. It is developed based on RC5 and does its job faster than RC5 because it has more registers. RC6 uses integer multiplication in algorithmic calculation. Unlike the meaningless chunks of RC5, the rotation of RC6 also depends on each chunk of the word. RC6 is a derivative of the block cipher created for RC5 and RSA Security. RC6 uses four work block size registers for algorithmic calculations, while RC5 uses only two. So RC6 is faster. RC6 was created as part of the Advanced Encryption Standard (AES) competition, where it was a finalist. This is a proprietary feature algorithm of RSA Security. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits, but, like RC5, it can be parameterised to support a wide variety of word-lengths, key sizes and number of rounds. RC6 is very similar to RC5 in structure, using data-dependent rotations, modular addition and XOR operations; in fact, RC6 could be viewed as interweaving two parallel RC5 encryption processes. However, RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits.

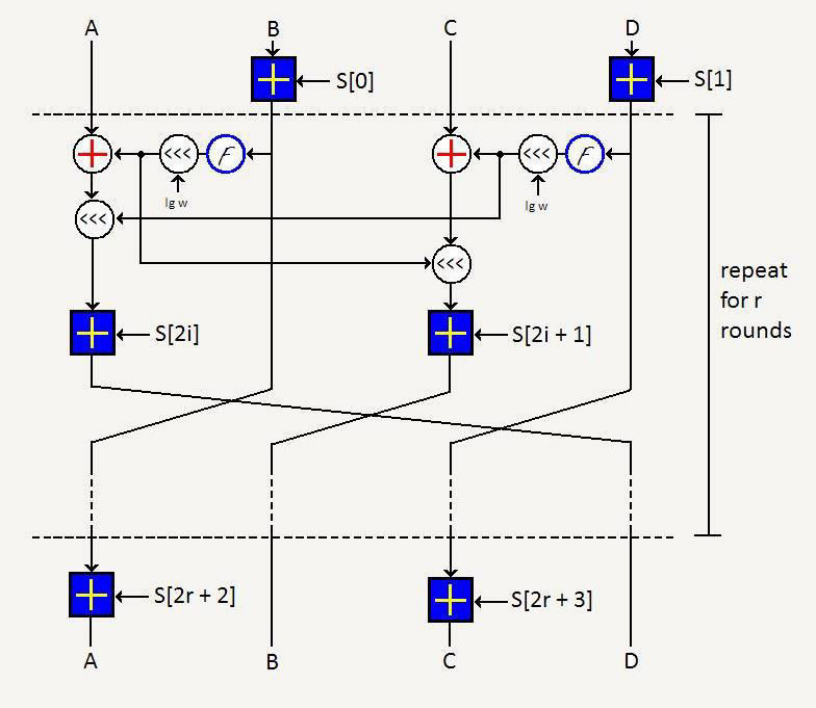


Figure 4.1.2 (h) RC6 Cipher

Rivest Code 6 (RC6) is a modern block cipher cryptography algorithm which is the closest rival algorithm of the Rijndael algorithm, Rijndael is the winning algorithm of the new Advanced Encryption Standard (AES) algorithm search competition held by the National Institute of Standards and Technology (NIST) this is held to look for new algorithms to replace the DES algorithm. RC6 filed by Ronald Linn Rivest et al of RSA Security Inc. In 1998. Famously simple but has a pretty good security. The algorithm is simple because in this algorithm contains six basic primitive operations such as addition, subtraction, XOR, multiplication and shifting bit either right or left (Fishawy & Zaid 2007). This algorithm has three processes, the process of key expansion, encryption and the decryption process. The key expansion process is the process to generating S-box keys with user keys, while encryption is the process of encoding messages with S-box keys that have been generated from the key expansion process, as well as the decryption process.

Encryption and Decryption Procedure

RC6 algorithm in this research will break the block data of 32 bit into 4 pieces of 8 bit block, then this algorithm work with 4 8-bit registers of A, B, C and D. In the process will be obtained (A, B, C, D) = (B, C, D, A) which means that the value located on the right side comes from the register on the left side. The encryption and decryption process of the RC6 algorithm begins and ends with a whitening process that aims to disguise the first and last iteration of the encryption and decryption process, and in the process requires 14 subkeys that have been generated in the key expansion process and named with S [0] to S [13] each of which is 8-bit in length. In each iteration in the encryption process used 2 (two) subkeys. The sub-keys in the first iteration use S [2] and S [3], the next iteration uses sub-advanced subkeys.

4.2 Data Flow Diagram

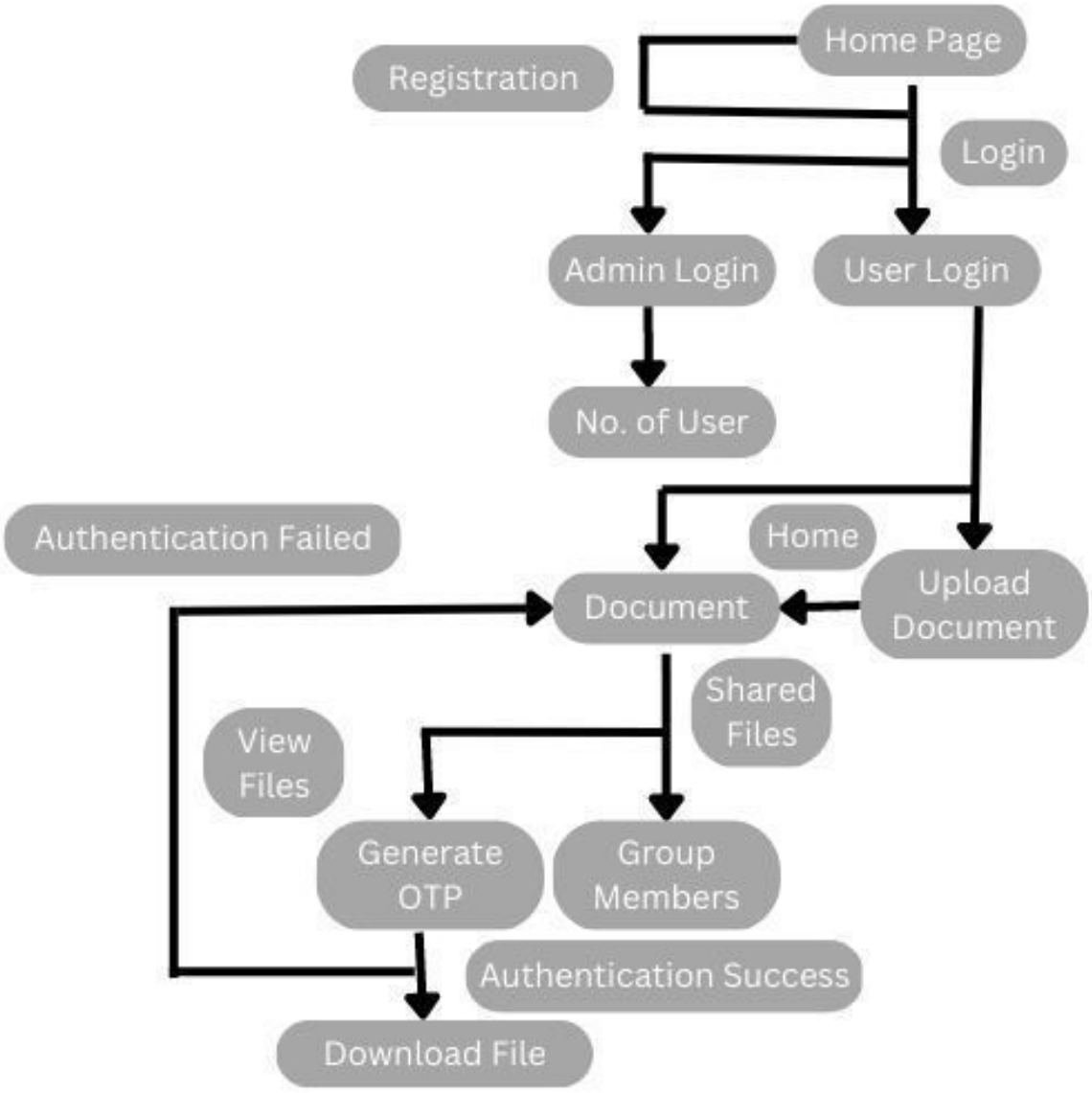


Figure 4.2 Data Flow Diagram

4.3 Control Flow Diagram

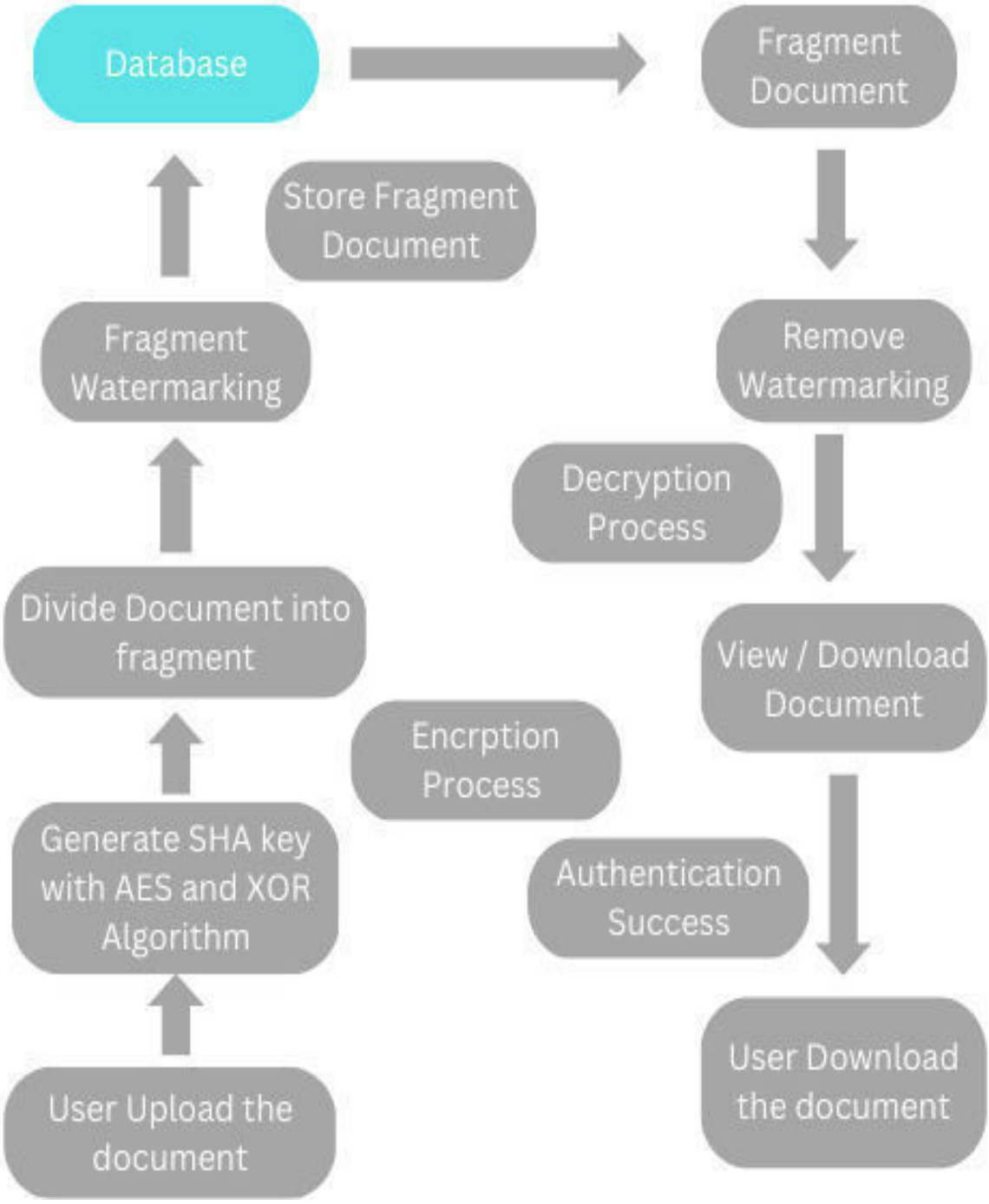


Figure 4.3 Control Flow Diagram

4.4 Architectural Flow Diagram

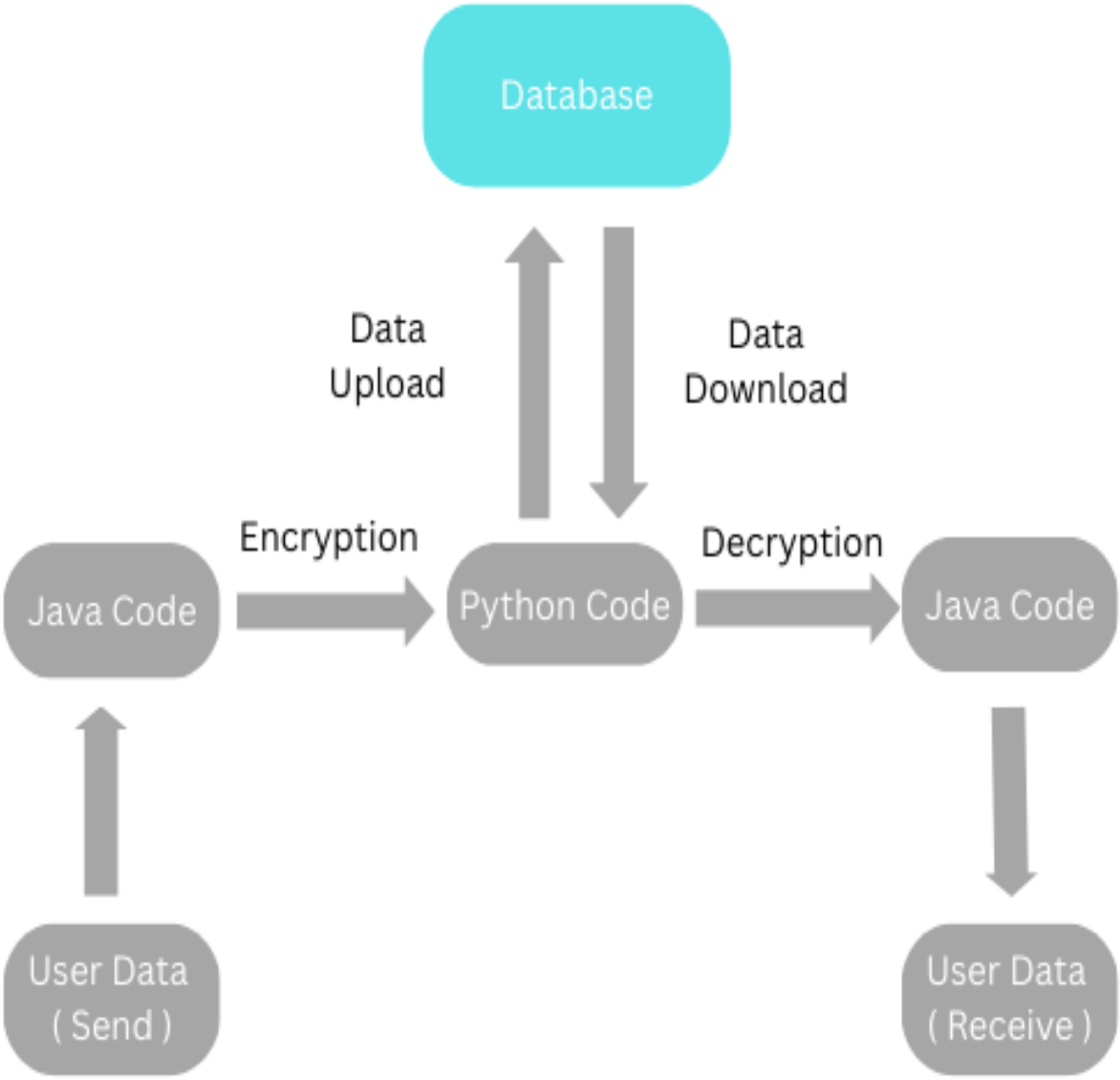


Figure 4.4 Architectural Flow Diagram

EXPERIMENTAL SETUP AND RESULTS

5. EXPERIMENTAL SETUP AND RESULTS

5.1 Experimental Setup

5.1.1 Hardware (System Requirement)

1. **Processor**

    a. **Intel** (Minimum 1.4 GHz; Recommended 2GHz or more)

    OR

    b. **AMD** (Minimum 1.4 GHz; Recommended 2GHz or more)

2. **Internet Connection**

    a. Ethernet Connection

    OR

    a. Wireless Connection

        i. Wi-Fi **2.4 Ghz**

        OR

        i. Wi-Fi **5.0 Ghz**

3. **Storage Drive**

    a. Hard Drive (Minimum 32 GB; Recommended 64 GB or more)

    OR

    b. SSD Drive (Minimum 32 GB; Recommended 64 GB or more)

4. **Memory (RAM):** Minimum 1 GB; Recommended 4 GB or above

5.1.2 Software

There is various application software are used in this project which is listed below:

1) Deployment Platform: - Windows 10 / Windows 11
2) Application Server: - Apache Server and Tomcat
3) Software Environment: - Java 19.0.2 and Python 3.11.2
4) Framework: - Springboot 2.0
5) Database Technologies: - MySQL Workbench, MySQL Server, MySQL Server, Connector Java (Connector J) and Connector Python (Connector P)

6) Web Development: - HTML5, Bootstrap, JSP

7) Development Tools: - Eclipse IDE, Pycharm IDE Community Edition, Sublime Text

5.1.2.1 Deployment Platform

1.1) Windows 10

Windows 10 is a major release of Microsoft's Windows NT operating system. It's the direct successor to Windows8.1, which was released nearly two times before. It was released to manufacturing on July 15, 2015, and latterly to vend on July 29, 2015. Windows 10 was made available for download via MSDN and TechNet, as a free upgrade for retail clones of Windows 8 and Windows 8.1 users via the Windows Store, and to Windows 7 users via Windows Update.

Figure 5.1.2.1 (a) Windows 10

Windows 10 receives new shapes on an ongoing base, which are available at no fresh cost to users, in addition to fresh test shapes of Windows 10, which are available to Windows Interposers. bias in enterprise surroundings can admit these updates at a slower pace, or use long-term support mileposts that only admit critical updates, similar as security patches, over their ten-time lifetime of extended support. In June 2021, Microsoft blazoned that support for Windows 10 editions which aren't in the Long- Term Servicing Channel (LTSC) will end on October 14, 2025.

Windows 10 entered generally positive reviews upon its original release. Critics praised Microsoft's decision to give the desktop- acquainted interface in line with former performances of Windows, differing the tablet- acquainted approach of Windows 8, although Windows10's touch- acquainted stoner interface mode was blamed for containing retrogressions upon the touch- acquainted interface of its precursor.

Critics also praised the advancements to Windows 10's whisked software over Windows 8.1, Xbox Live integration, as well as the functionality and capabilities of the Cortana particular adjunct and the relief of Internet Discoverer with Microsoft Edge. still, media outlets have been critical of the changes to operating system actions, including obligatory update installation, sequestration enterprises over data collection performed by the zilches for Microsoft and its mates, and adware- suchlike tactics used to promote the operating system on its release.

1.2) Windows 11

Windows 11 is the latest major release of Microsoft's Windows NT operating system, released in October 2021. It is a free upgrade to its predecessor, Windows 10 (2015), and is available for any Windows 10 devices that meet the new Windows 11 system requirements. Windows 11 features major changes to the Windows shell influenced by the cancelled Windows 10X, including a redesigned Start menu, the replacement of its "live tiles" with a separate "Widgets" panel on the taskbar, the ability to create tiled sets of windows that can be minimized and restored from the taskbar as a group, and new gaming technologies inherited from Xbox Series X and Series S such as Auto HDR and Direct Storage on compatible hardware. Internet Explorer (IE) has been replaced by the Chromium-based Microsoft Edge as the default web browser, like its predecessor, Windows 10, and Microsoft Teams is integrated into the Windows shell.

Figure 5.1.2.1 (b) Windows 11

Microsoft also announced plans to allow more flexibility in software that can be distributed via the Microsoft Store and to support Android apps on Windows 11 (including a partnership with Amazon to make its app store available for the function).

Citing security considerations, the system requirements for Windows 11 were increased over Windows 10. Microsoft only officially supports the operating system on devices using an eighth-generation Intel Core CPU or newer (with some minor exceptions), a second-generation AMD Ryzen CPU or newer, or a Qualcomm Snapdragon 850 ARM system-on-chip or newer, with UEFI secure boot and Trusted Platform Module (TPM) 2.0 supported and enabled (although Microsoft may provide exceptions to the TPM 2.0 requirement for OEMs). While the OS can be installed on unsupported processors, Microsoft does not guarantee the availability of updates. Windows 11 removed support for 32-bit x86 CPUs and devices that use BIOS firmware.

Windows 11 received a mixed reception at launch. Pre-release coverage of the operating system focused on its stricter hardware requirements, with discussions over whether they were legitimately intended to improve the security of Windows or as a ploy to upsell customers to newer devices and over the e-waste associated with the changes. Upon release, it was praised for its improved visual design, window management, and stronger focus on security, but was criticized for various modifications to aspects of its user interface that were seen as worse than its predecessor, as an attempt to dissuade users from switching to competing applications.

5.1.2.2 Application Server

1) Apache Server

Apache HTTP Server is a free, open-source web server that serves web content over the Internet. Commonly known as Apache, it quickly became the web's most popular HTTP client when it was developed. It is widely believed that Apache got its name from its development history and process of improvement with patches and modules applied, but this was corrected in 2000. Before we dive into Apache, let's first look at what a web application is and what the standard architectures typically found in web applications are. Apache web application architecture

Apache is just one of the components required to serve web content in a web application stack. One of the most popular web application stacks includes LAMP or Linux, Apache, MySQL, and PHP. Linux is an operating system that handles application operations. Apache is a

web server that processes requests and serves web assets and content over HTTP. MySQL is a database that stores all information in an easy-to-query format. PHP is a programming language that works with Apache to create dynamic web content. Your actual stats may vary, but it's safe to say that the vast majority of web applications run on some form of LAMP stack because they're easy to build and free to use. Web applications, in most cases, serve many different functions and purposes, but generally tend to have similar architectures and structures. Most web applications also benefit from firewalls, load balancers, web servers, content delivery networks, and database servers.

Figure 5.1.2.2 (a) Apache Server

Firewalls help protect web applications from both external threats and internal vulnerabilities, depending on where the firewall is configured. A load balancer helps distribute traffic between web servers that handle HTTP(S) requests (this is where Apache comes in) and application servers (servers that handle web application functions and workloads). There is also a database server that handles asset storage and backup. Depending on your infrastructure, you can run both the database and the application on the same server, but it's best to keep them separate.

2) Apache Tomcat

Apache Tomcat is a web-container which allows to run servlet and Java-Server Pages (JSP) based web applications. Most of the modern Java web frameworks are based on servlets, e.g., Java-Server Faces, Struts, Spring. Apache Tomcat also provides by default a HTTP connector on port 8080, i.e., Tomcat can also be used as HTTP server. But the performance of Tomcat is not as good as the performance of a designated web server, like the Apache HTTP server.

It began as the reference implementation for the very first Java-Server Pages and the Java Servlet API. However, it no longer works as the reference implementation for both of these technologies, but it is considered as the first choice among the users even after that. It is still one of the most widely used java-sever due to several capabilities such as good extensibility, proven core engine, and well-test and durable. Here we used the term "servlet" many times, so what is java servlet; it is a kind of software that enables the webserver to handle the dynamic(java-based) content using the HTTP protocols.

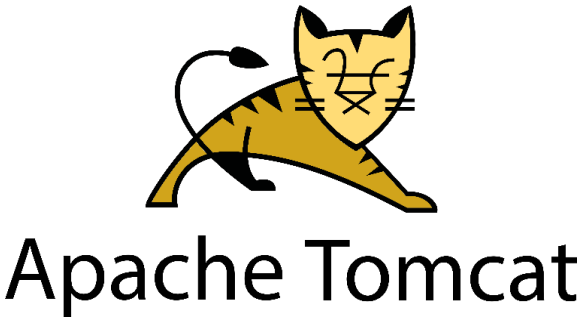


Figure 5.1.2.2 (b) Apache Tomcat

Apache Tomcat is a Java-enabled HTTP server that can run special Java programs called "Java Servlets" and "Java Server Pages (JSP)". Tomcat is an open-source project of the Apache Software Foundation (also providing the most widely used industrial grade open-source Apache HTTP server). Tomcat's mother site is http: You can find Tomcat at http://tomcat.apache.org. //www.apache.org.

5.1.2.3 Software Environment

1) Java (Version. 19.0.2)

Java is a programming language and a platform. Java is a high level, robust, object-oriented and secure programming language. Java was developed by Sun Microsystems (which is now the subsidiary of Oracle) in the year 1995. James Gosling is known as the father of Java. Before Java, its name was Oak. Since Oak was already a registered company, so James Gosling and his team changed the name from Oak to Java. Platform: Any hardware or software environment in which a program runs, is known as a platform. Since Java has a runtime environment (JRE) and API, it is called a platform.

Figure 5.1.2.3 (a) Oracle Java

The Java Platform, Standard Edition 19 Development Kit (JDK 19) is a feature release of the Java SE platform. It contains new features and enhancements in many functional areas. The Release Notes below describe the important changes, enhancements, removed APIs and features, deprecated APIs and features, and other information about JDK 19 and Java SE 19.

2) Python (Version. 3.11.2)

Python is an interpreted, interactive, object-oriented programming language. It incorporates modules, exceptions, dynamic typing, very high-level dynamic data types, and classes. It supports multiple programming paradigms beyond object-oriented programming, such as procedural and functional programming. Python combines remarkable power with very clear syntax. It has interfaces to many system calls and libraries, as well as to various window systems, and is extensible in C or C++. It is also usable as an extension language for applications that need a programmable interface. Finally, Python is portable: it runs on many Unix variants including Linux and macOS, and on Windows.

Figure 5.1.2.3 (b) Python 3.11.2

Python 3.11 is between 10-60% faster than Python 3.10. On average, we measured a 1.25x speedup on the standard benchmark suite. CPython 3.11 is on average 25% faster than CPython 3.10 when measured with the pyperformance benchmark suite, and compiled with GCC on Ubuntu Linux. Depending on your workload, the speedup could be up to 10-60% faster. This project focuses on two major areas in Python: faster startup and faster runtime.

5.1.2.4 Framework

1) Spring – Boot (Version. 2.5.3)

Spring Boot is an open - source Java-based framework used to create a micro service. It is developed by Pivotal Team and is used to build stand-alone and production ready spring applications. Spring Boot is a project that is built on the top of the Spring Framework. It provides an easier and faster way to set up, configure, and run both simple and web-based applications. It is a Spring module that provides the RAD (Rapid Application Development) feature to the

Spring Framework. It is used to create a stand-alone Spring-based application that you can just run because it needs minimal Spring configuration.
Java Spring Framework (Spring Framework) is a popular, open source, enterprise-level framework for creating standalone, production-grade applications that run on the Java Virtual Machine (JVM).

Figure 5.1.2.4 Spring Boot

Spring Framework also offers built-in support for typical tasks that an application needs to perform, such as data binding, type conversion, validation, exception handling, resource and event management, internationalization, and more. It integrates with various Java EE technologies such as RMI (Remote Method Invocation), AMQP (Advanced Message Queuing Protocol), Java Web Services, and others. In sum, Spring Framework provides developers with all the tools and features the need to create loosely coupled, cross-platform Java EE applications that run in any environment.

5.1.2.5 Databases Technologies

1) MySQL Workbench

MySQL Workbench is a unified visual database designing or graphical user interface tool used for working with database architects, developers, and Database Administrators. It is developed and maintained by Oracle. It provides SQL development, data modeling, data migration, and comprehensive administration tools for server configuration, user administration, backup, and many more. We can use this Server Administration for creating new physical data models, E-R diagrams, and for SQL development (run queries, etc.). It is available for all major operating systems like Mac OS, Windows, and Linux. MySQL Workbench fully supports MySQL Server version v5.6 and higher. MySQL Workbench covers five main functionalities, which are given below:

A) SQL Development: This functionality provides the capability that enables you to execute SQL queries, create and manage connections to the database Servers with the help of built-in SQL editor.

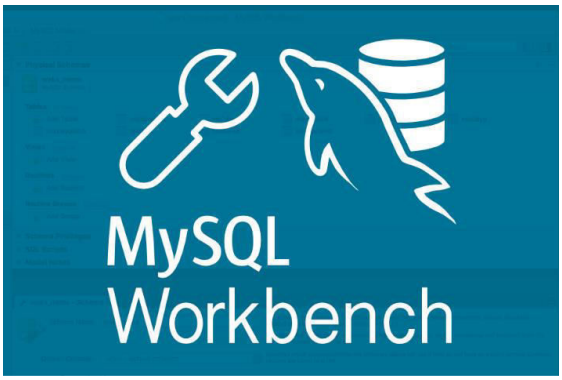


Figure 5.1.2.5 (a) MySQL Workbench

B) Data Modelling (Design): This functionality provides the capability that enables you to create models of the database Schema graphically, performs reverse and forward engineering between a Schema and a live database, and edit all aspects of the database using the comprehensive Table editor. The Table editor gives the facilities for editing tables, columns, indexes, views, triggers, partitioning, etc.

C) Server Administration: This functionality enables you to administer MySQL Server instances by administering users, inspecting audit data, viewing database health, performing backup and recovery, and monitoring the performance of MySQL Server.

2) MySQL Server

MySQL is an Oracle-backed open-source relational database management system (RDBMS) based on Structured Query Language (SQL). MySQL runs on virtually all platforms, including Linux, UNIX and Windows. Although it can be used in a wide range of applications, MySQL is most often associated with web applications and online publishing. MySQL is an important component of an open-source enterprise stack called LAMP. LAMP is a web development platform that uses Linux as the operating system, Apache as the web server, MySQL as the relational database management system and PHP as the object-oriented scripting language. (Sometimes Perl or Python is used instead of PHP.)

Figure 5.1.2.5 (b) MySQL Server

Originally conceived by the Swedish company MySQL AB, MySQL was acquired by Sun Microsystems in 2008 and then by Oracle when it bought Sun in 2010. Developers can use MySQL under the GNU General Public License (GPL), but enterprises must obtain a commercial license from Oracle. Today, MySQL is the RDBMS behind many of the top websites in the world and countless corporate and consumer-facing web-based applications, including Facebook, Twitter and YouTube.

3) MySQL Shell

MySQL Shell is an advanced client and code editor for MySQL. This document describes the core features of MySQL Shell. In addition to the provided SQL functionality, similar to mysql, MySQL Shell provides scripting capabilities for JavaScript and Python and includes APIs for working with MySQL. X DevAPI enables you to work with both relational and document data, see Using MySQL as a Document Store. AdminAPI enables you to work with InnoDB Cluster, InnoDB ClusterSet, and InnoDB ReplicaSet.

Figure 5.1.2.5 (c) MySQL Shell

MySQL Shell processes code written in JavaScript, Python and SQL. Any executed code is processed as one of these languages, based on the language that is currently active. There are also specific MySQL Shell commands, prefixed with which enable you to configure MySQL Shell regardless of the currently selected language.

From version 8.0.18, MySQL Shell uses Python 3, rather than Python 2.7. For platforms that include a system supported installation of Python 3, MySQL Shell uses the most recent version available, with a minimum supported version of Python 3.6. For platforms where Python 3 is not included or is not at the minimum supported version, MySQL Shell bundles Python 3.7.7 up to MySQL Shell 8.0.25, and Python 3.9.5 from MySQL Shell 8.0.26. MySQL Shell maintains code compatibility with Python 2.6 and Python 2.7, so if you require one of these older versions, you can build MySQL Shell from source using the appropriate Python version.

4) Connector Java (Connector J)

MySQL provides connectivity for client applications developed in the Java programming language with MySQL Connector/J. Connector/J implements the Java Database Connectivity (JDBC) API, as well as a number of value-adding extensions of it. It also supports the new X DevAPI.

MySQL Connector/J is a JDBC Type 4 driver, implementing the JDBC 4.2 specification. The Type 4 designation means that the driver is a pure Java implementation of the MySQL protocol and does not rely on the MySQL client libraries.

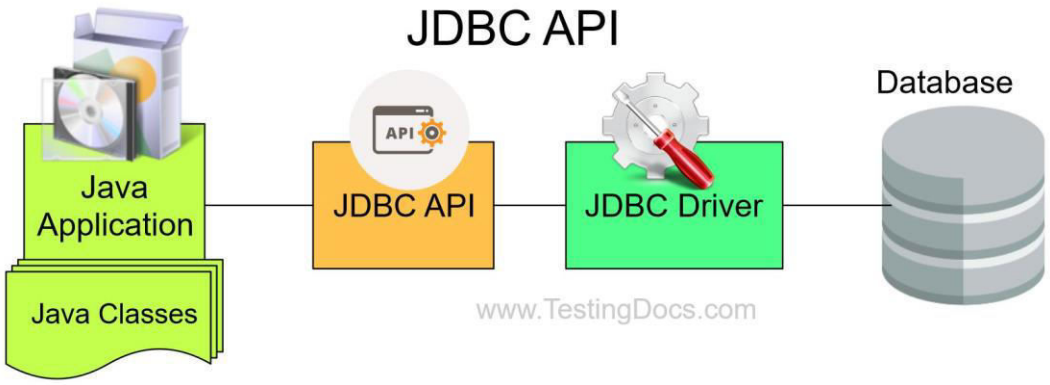


Figure 5.1.2.5 (d) Connector Java

To connect Java application with the MySQL database, we need to follow 5 following steps. In this example we are using MySQL as the database. So, we need to know following information's for the MySQL database:

1. **Driver class:** The driver class for the mysql database is **com.mysql.jdbc.Driver**.
2. **Connection URL:** The connection URL for the mysql database is **jdbc:mysql://localhost:3306/sonoo** where jdbc is the API, mysql is the database, localhost is the server name on which mysql is running, we may also use IP address, 3306 is the port number and sonoo is the database name. We may use any database, in such case, we need to replace the sonoo with our database name.
3. **Username:** The default username for the mysql database is **root**.
4. **Password:** It is the password given by the user at the time of installing the mysql database. In this example, we are going to use root as the password.

5) Connector Python (Connector P)

MySQL Connector/Python enables Python programs to access MySQL databases, using an API that is compliant with the Python Database API Specification v2.0 (PEP 249). It is written in pure Python and does not have any dependencies except for the Python Standard Library.

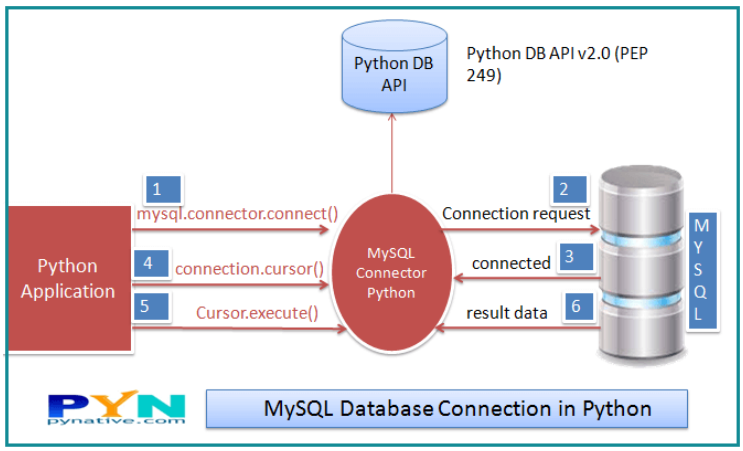


Figure 5.1.2.5 (e) Connector Python

Python MySQL Connector is a Python driver that helps to integrate Python and MySQL. This Python MySQL library allows the conversion between Python and MySQL data types. MySQL Connector API is implemented using pure Python and does not require any third-party library.

5.1.2.6 Web Development

1) HTML5

HTML5 is the newest version of HTML. The term refers to two things. One is the updated HTML language itself, which has new elements and attributes. The second is the larger set of technologies that work with this new version of HTML like a new video format and enable you to build more complex and powerful websites and apps. HTML is an abbreviation of Hypertext and Markup language. Hypertext defines the link between the web pages. The markup language is used to define the text document within the tag which defines the structure of web pages. HTML 5 is the fifth and current version of HTML. It has improved the markup available for documents and has introduced application programming interfaces (API) and Document Object Model (DOM).

Figure 5.1.2.6 (a) HTML5

HTML5 was first released in a public-facing form on 22 January 2008, with a major update and "W3C Recommendation" status in October 2014. Its goals were to improve the language with support for the latest multimedia and other new features; to keep the language both easily readable by humans and consistently understood by computers and devices such as web browsers, parsers, etc., without XHTML's rigidity; and to remain backward-compatible with older software. HTML5 is intended to subsume not only HTML 4 but also XHTML 1 and DOM Level 2 HTML.

HTML5 includes detailed processing models to encourage more interoperable implementations; it extends, improves, and rationalizes the markup available for documents and introduces markup and application programming interfaces (APIs) for complex web applications. For the same reasons, HTML5 is also a candidate for cross-platform mobile applications because it includes features designed with low-powered devices in mind.

2) JavaScript

JavaScript (.js) is a light-weight object-oriented programming language which is used by several websites for scripting the webpages. It is an interpreted, full-fledged programming language that enables dynamic interactivity on websites when applied to an HTML document. It was introduced in the year 1995 for adding programs to the webpages in the Netscape Navigator browser. Since then, it has been adopted by all other graphical web browsers. With JavaScript, users can build modern web applications to interact directly without reloading the page every time. The traditional website uses js to provide several forms of interactivity and simplicity.

Figure 5.1.2.6 (b) JavaScript

Although, JavaScript has no connectivity with Java programming language. The name was suggested and provided in the times when Java was gaining popularity in the market. In addition to web browsers, databases such as CouchDB and MongoDB uses JavaScript as their scripting and query language. JavaScript (JS) is the most popular lightweight, interpreted compiled programming language. It can be used for both Client-side as well as Server-side developments. JavaScript also known as a scripting language for web pages.

3) JSP (Jakarta Server Page)

Java (Jakarta) Server Pages (JSP) is a server-side programming technology that enables the creation of dynamic, platform-independent method for building Web-based applications. JSP have access to the entire family of Java APIs, including the JDBC API to access enterprise databases. Java Server Pages (JSP) is a technology which is used to develop web pages by inserting Java code into the HTML pages by making special JSP tags. The JSP tags which allow java code to be included into it are <% —-java code—-%>. It can consist of either HTML or XML (combination of both is also possible) with JSP actions and commands. It can be used as HTML page, which can be used in forms and registration pages with the dynamic content into it.

Dynamic content includes some fields like dropdown, checkboxes, etc. whose value will be fetched from the database. This can also be used to access JavaBeans objects. JSP can be used for separation of the view layer with the business logic in the web application.

Figure 5.1.2.6 (c) Jakarta Server Pages

Java Server Pages (JSP) is a technology that allows developers to create dynamic web pages using a combination of HTML, XML, and Java code. JSP pages are executed on a web server, and the resulting output is sent to the client's web browser. JSP provides a way to easily access Java code and objects from within a web page, simplifying the creation of dynamic web pages. JSP pages are typically used in conjunction with Java servlets, which handle data processing and client requests. JSP is part of the Java EE platform and is supported by most web servers and servlet containers.

5.1.2.7 Development Tools

1) Eclipse IDE

Eclipse is defined as platform for developing the computer-based applications using various programming language like JAVA, Python, C/C++, Ruby and many more. The Eclipse is IDE (Integrated development kit) and mainly JAVA based programming is done in this platform. There are several plug-ins and other additional plug-ins can be installed in the platform. The advanced client applications can be developed. The JDT is used for doing the programming in Eclipse IDE.

Eclipse started in 2001 when IBM donated three million lines of code from its Java tools to develop an open-source integrated development environment (IDE). Eclipse IDE was initially overseen by a consortium of software vendors seeking to create and foster a new community complementing Apache's open-source community. It has been said, though not confirmed, that the platform's name was derived from a secondary goal, which was to eclipse Microsoft's popular IDE, Visual Studio.

Figure 5.1.2.7 (a) Eclipse IDE

In 2011, Oracle became an Eclipse provider, donating the Hudson continuous integration server it inherited from Sun Microsystems and the Java 2 Platform, Enterprise Edition (Java EE), in 2017. In 2016, Microsoft announced it would join the Eclipse Foundation and support the integration of Visual Studio by giving Eclipse developers full access to Visual Studio Team Services. Eclipse's board of directors includes executive director Mike Milinkovich and strategic members from CA Technologies, IBM, Oracle and SAP.

2) Sublime Text

Sublime Text editor is a sophisticated text editor which is widely used among developers. It includes wide features such as Syntax Highlight, Auto Indentation, File Type Recognition, Sidebar, Macros, Plug-in and Packages that make it easy for working with code base. This tutorial gives you a comprehensive coverage of concepts of Sublime Text and makes you comfortable to use it in your software development projects.

Sublime Text is a versatile, fun, and fast text editor for code and prose that automates repetitive tasks so you can focus on the important stuff. It is supported on macOS, Windows and Linux. Its versatility comes from a wide range of community-developed third-party packages that provide syntax highlighting, snippets, or other automation backed by Python plugins. The default distribution of Sublime Text aims to provide a basic but very functional set of features, but it can easily be turned into a full-fledged IDE, if so desired.

Figure 5.1.2.7 (b) Sublime Text

Sublime Text editor is used as an Integrated Development Editor (IDE) like Visual Studio code and NetBeans. The current version of Sublime Text editor is 3.0 and is compatible with various operating systems like Windows, Linux and MacOS.

3) Pycharm IDE (Community Edition)

PyCharm is an integrated development environment (IDE) used for programming in Python. It provides code analysis, a graphical debugger, an integrated unit tester, integration with version control systems, and supports web development with Django. PyCharm is developed by the Czech company JetBrains. It is cross-platform, working on Microsoft Windows, macOS and Linux. PyCharm has a Professional Edition, released under a proprietary license and a Community Edition released under the Apache License. PyCharm Community Edition is less extensive than the Professional Edition.

Figure 5.1.2.7 (c) Pycharm IDE

PyCharm is a hybrid platform developed by JetBrains as an IDE for Python. It is commonly used for Python application development. PyCharm is one of the most popular Python IDEs. There is a multitude of reasons for this, including the fact that it is developed by JetBrains, the developer behind the popular IntelliJ IDEA IDE that is one of the big 3 of Java IDEs and the "smartest JavaScript IDE" WebStorm. Having the support for web development by leveraging Django is yet another credible reason. There are a galore of factors that make PyCharm one of

the most complete and comprehensive integrated development environments for working with the Python programming language.

5.2 Results

5.2.1 Application of Digital Watermarking

Digital watermarking can be used for the following purposes:

- Copyright Protection: This is by far the most famous application of watermarks. With tons of images being exchanged over lacking confidence networks every day, patent protection becomes a very important issue. Watermarking an image will prevent redistribution of pretended images.

- Authentication: Sometimes the ownership of the contents has to be verified. This can be done by embedding a watermark and providing the owner with a private key which gives him an admission to the message. ID cards, ATM cards, credit cards are all examples of documents which require confirmation.

- Broadcast Monitoring: As the name suggests broad cast monitoring is used to verify the programs broadcasted on TV or radio. It especially helps the advertising companies to see if their advertisements appeared for the right duration or not.

- Content Labeling: Watermarks can be used to give more information about the cover object. This process is named as content labeling.

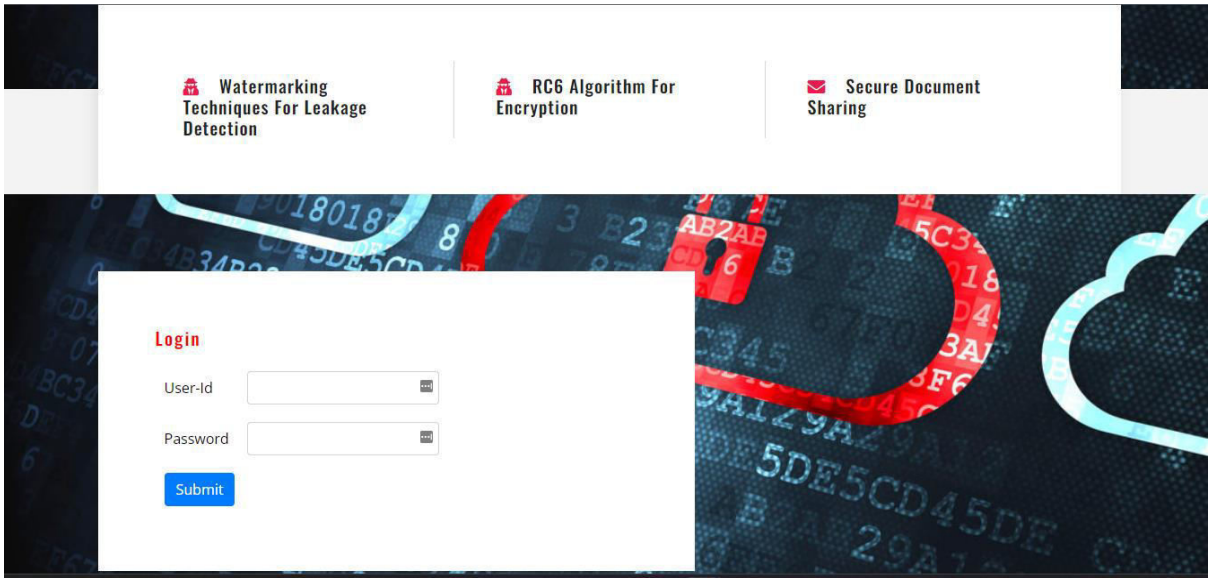
- Tamper Detection: Fragile watermarks can be used to detect tampering in an image. If the fragile watermark is degraded in any way, then they can say that the image or document in question has been tampered.

- Content Protection: In this process the content printed with a visible watermark that is very hard to remove so that it can be openly and freely distributed

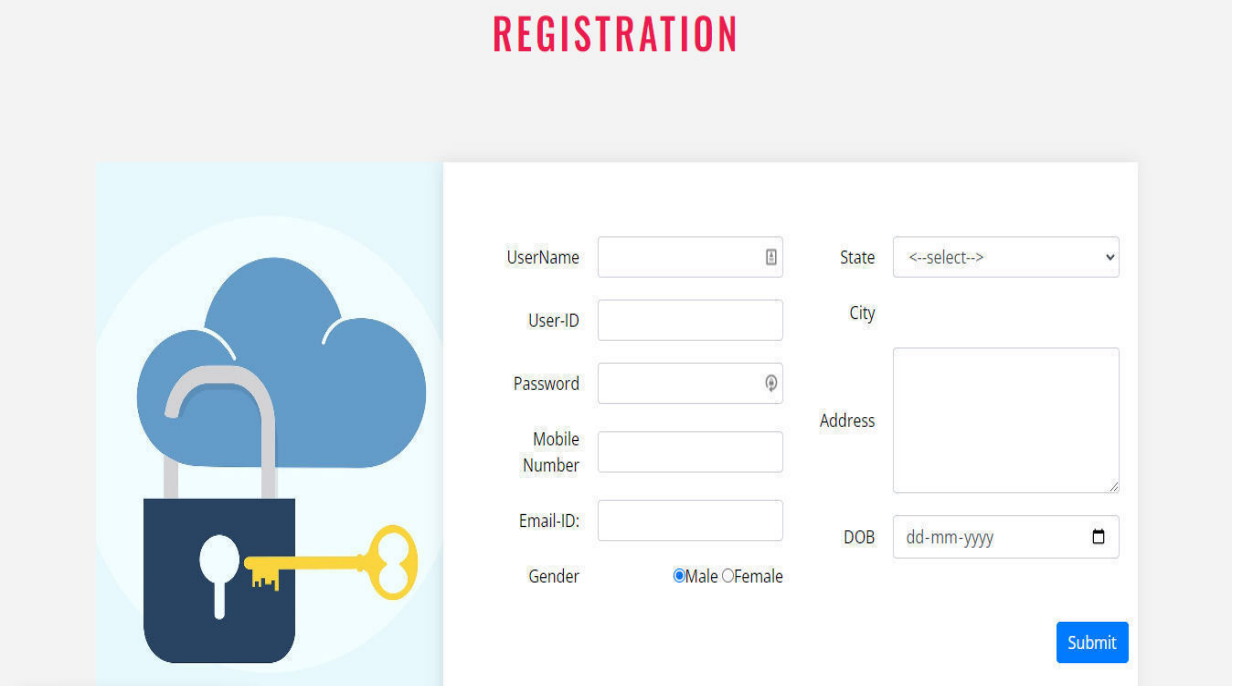
5.2.2 Screenshots

Screenshot 1: Home Page

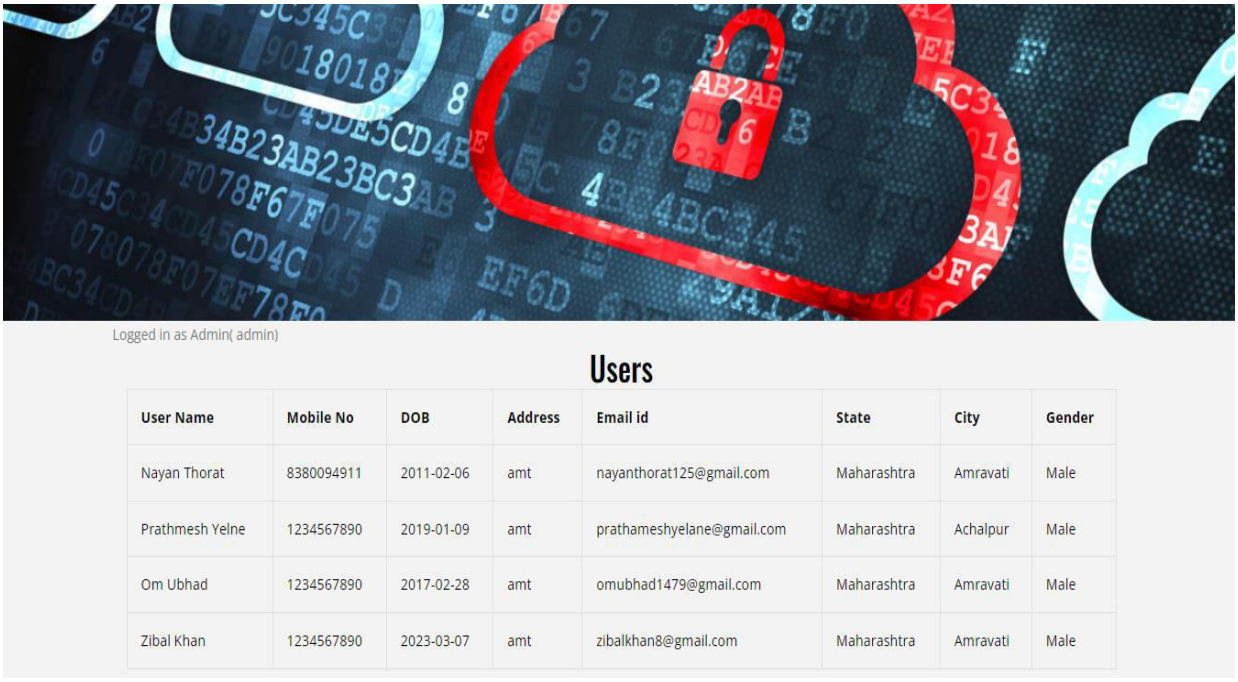
Screenshot 2: Login Page



Screenshot 3: Registration Page



Screenshot 4: Admin Page (No. of Registered Users)

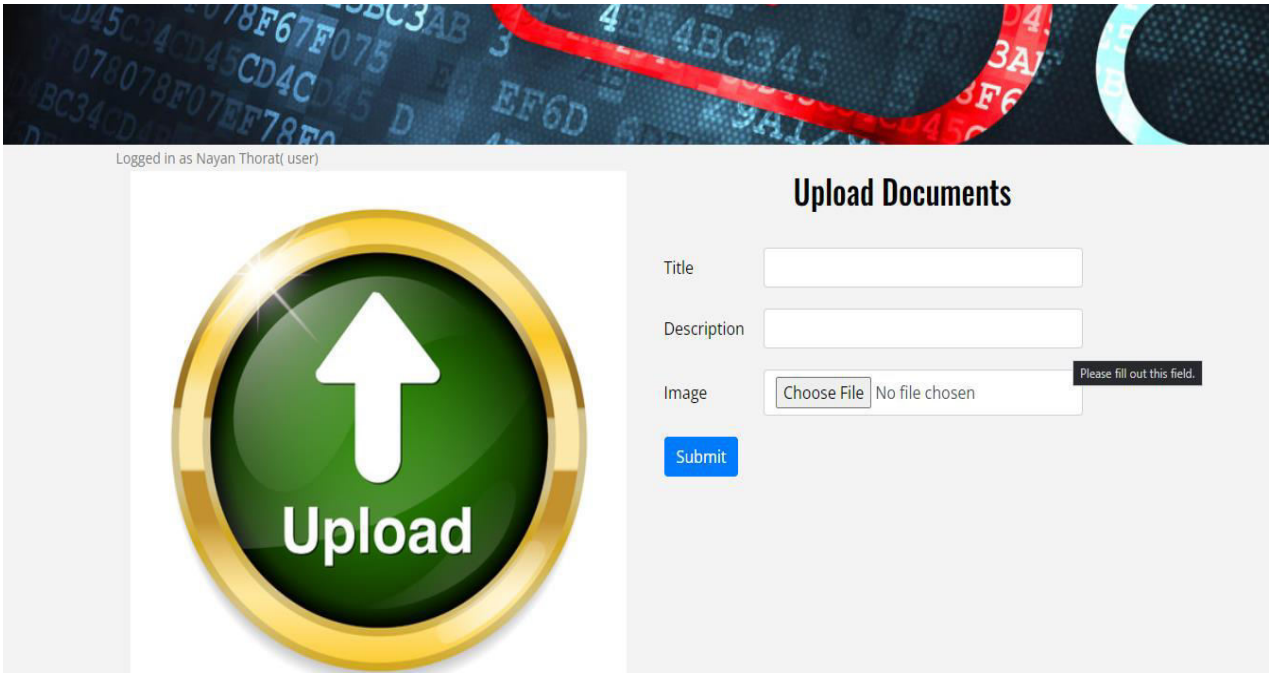


Logged in as Admin(admin)

Users

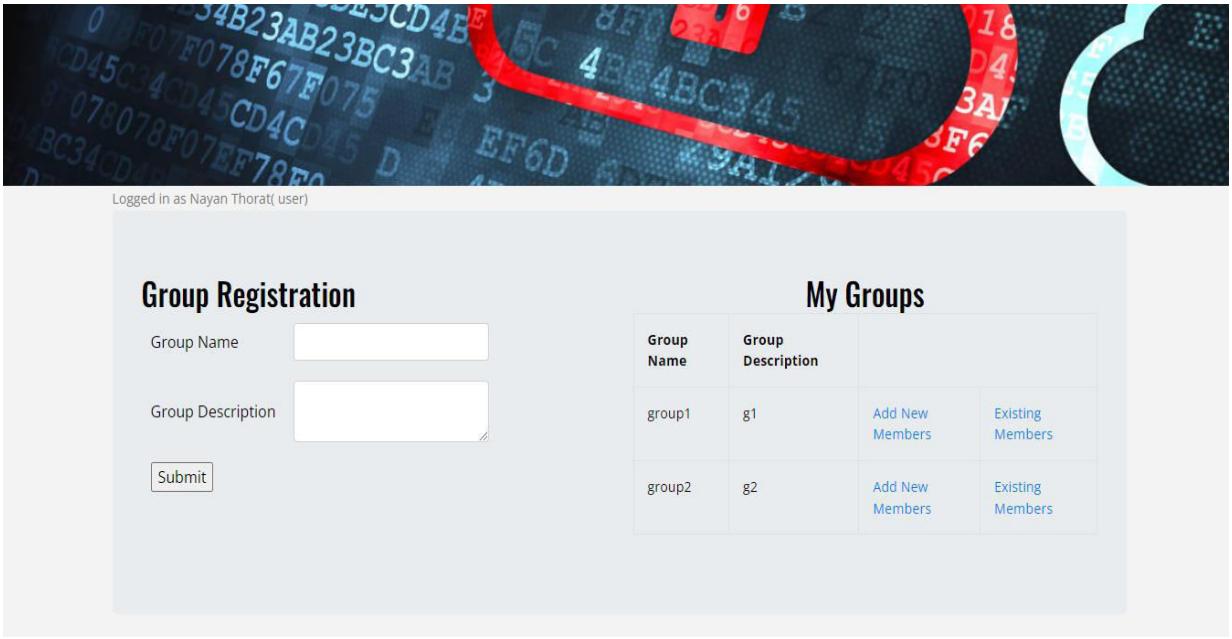
User Name	Mobile No	DOB	Address	Email id	State	City	Gender
Nayan Thorat	8380094911	2011-02-06	amt	nayanthorat125@gmail.com	Maharashtra	Amravati	Male
Prathmesh Yelne	1234567890	2019-01-09	amt	prathameshyelane@gmail.com	Maharashtra	Achalpur	Male
Om Ubhad	1234567890	2017-02-28	amt	omubhad1479@gmail.com	Maharashtra	Amravati	Male
Zibal Khan	1234567890	2023-03-07	amt	zibalkhan8@gmail.com	Maharashtra	Amravati	Male

Screenshot 5: Upload Documents



Screenshot 6: Documents Page

Screenshot 7: Group Registration and Group Name



Screenshot 8: User Home Page

Screenshot 9: Existing Group Members

Logged in as Nayan Thorat(user)

Existing Group Members

User Name	Mobile No	DOB	Address	Email id	
Nayan Thorat	8380094911	2011-02-06	amt	nayanthorat125@gmail.com	Remove
Prathmesh Yelne	1234567890	2019-01-09	amt	prathameshyelane@gmail.com	Remove

Screenshot 10: Shared Documents

Logged in as Prathmesh Yelne(user)

Shared Documents

Title	Description	Date	Time	Sender		
doc1	doc1	1/3/2023	14:39	Nayan Thorat	Send OTP	Share With Groups

Screenshot 11: Cloud Usage Report

Logged in as Admin(admin)

Mar 2023 Get Report

Cloud Usage Report for 3/2023

Client Name	Encryption	Decryption	Email	Login	Total
Nayan Thorat	1	0	0	0	1
Om Ubhad	0	0	0	0	0
Prathmesh Yelne	0	0	0	0	0
Zibal Khan	0	0	0	0	0

Screenshot 12: User Payment History

Logged in as Admin(admin)

Nayan Thorat 2023 Get Report

Payment History Customer Name : Nayan Thorat for 2023

Months	encryption	decryption	email	login	Total Rent	Status	Payment Date
March	2.0	0.0	0.0	0.0	2.0	pending	NA

Screenshot 13: Cloud Payment Report

Logged in as Admin(admin)

March 2023 Get Report

Cloud Payment Report for 3/2023

Name	encryption	decryption	email	login	Total Rent	Status	Payment Date	Action
Nayan Thorat	2.0	0.0	0.0	0.0	2.0	pending	NA	Current Month

CONCLUSION AND FUTURE SCOPE

6. CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

In this topic we conclude that methods of encryption are still prevalent in the digital world. Because every piece of data that travels through a computer network is now unprotected. The goal of the cryptography method is to make secure and unbreakable communication possible while also protecting records from being attacked. In the end, it is clear that this paper has examined cryptography's semantics, evolution, and syntax to some extent. Some crucial axioms, various flavors, and the significance of cryptography were established.

The general watermarking technique is discussed in this project. Because this method employs two-way encryption on a watermarked file, it is evident that the watermark's data or image is protected and offers superior security to other methods.
In order to achieve better results in the areas of robustness and security, this method should be used with a lot of new techniques.

Due to the interactive and digital communication of multimedia data at this time, information can be easily duplicated. Digital watermarking is a significant area of study because of this problem. An important tool for authentication, integrity verification, tamper detection, copyright protection, and digital security of any data has been digital watermarking using various techniques. We looked at the most prevalent watermarking methods in this project. In order to create an effective watermarking system, it is necessary to have capacity, imperceptibility, and robustness. However, meeting all of these requirements simultaneously is almost impossible. As a result, these three requirements must be balanced in a satisfactory manner.

Digital watermarking technologies still face significant security issues, and researchers face difficulties integrating IoT and blockchain-based authentication methods. Therefore, in order to satisfy the aforementioned three essential requirements, future work can be extended by combining various techniques from various fields.

6.2 Future Scope

There has been a lot of discussion about cloud computing and cloud storage, such as Microsoft Azure, Google Cloud, and Amazon Web Services, in a society that is increasingly dependent on technology. Considering that almost everything in the digital world is connected to the cloud in some way, unless it is specifically stored locally for security reasons; The organization, processing, and presentation of data are continually improved by tech geniuses. Cloud computing will become an increasingly important part of our lives as a result of extraordinary technological innovation.

An additional factor is the rate of innovation in infrastructure and services. Businesses primarily dislike being locked in. Cost wars will result from cloud wars. There may be significant annual savings for a business if infrastructure costs are significantly reduced. The IT teams are forced to think about the best ways to use orchestration and data mobility to their full potential as a result of this.

When it comes to testing, this is of the utmost significance. Having said that, organizations now have a customized multi-cloud strategy that improves performance in ways that were previously unimaginable prior to the cloud revolution because they can experiment with additional applications on various platforms in a quick, simple, and cost-effective manner. Companies will begin selecting a managed solution as cloud users realize the difficulties of managing it. The aforementioned forecasts demonstrate the enormous growth potential of cloud computing. The use of this technology must be prioritized by more and more organizations. In fact, they need to reorganize and make investments in coding standards that will enable seamless cloud migration.

Additionally, there is a strong connection between cloud computing and concepts like the internet of things. The Internet of Things can more easily guarantee performance, security, and functionality when data is stored in the cloud. The network's speed, which controls the rate at which data is gathered and processed, would be the only restriction. Everything else about using cloud computing will work just fine if the network is fast.

REFERENCES

REFERENCES

[1] Y. M. Chu, N. F. Huang, and S. H. Lin (2014) "*Quality of service provision in cloud based storage system for multimedia delivery.*" IEEE Systems Journal, 8 (1): 292-303.

[2] A. Anees, I. Hussain, A. Algarni, and M. Aslam (2018) "*A robust watermarking scheme for online multimedia copyright protection using new chaotic map*." Hindawi, Security and Communication Networks, Article ID 1840207 2018: 1- 20.

[3] W. Luo, F. Huang, and J. Huang (2010) "*Edge adaptive image steganography based on LSB matching revisited*." IEEE Trans. On Information Forensics and Security, 5 (2): 201-214.

[4] K. S. Kim, M. J. Lee, H. Y. Lee, and H. K. Lee (2009) "*Reversible data hiding exploiting spatial correlation between sub-sampled images.*" Pattern Recognition, 42 (11): 3083-3096.

[5] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon (1997) "*Secure spread spectrum watermarking for multimedia.*." IEEE Transactions on Image Processing, 6 (12): 1673- 1687.

[6] G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni (2004) "*Reversible data hiding based on wavelet spread spectrum.*" IEEE 6th workshop on Multimedia Signal Processing: 211-214.

[7] C. C. Chang, P. Y. Lin (2008) "*Adaptive watermarking mechanism for rightful ownership protection.*" J. Syst. Software, 81 (7): 1118-1129.

[8] G. J. Lee, E. J. Yoon, K. Y. Yoo (2008) "*A new LSB based digital watermarking scheme with random mapping function*." International Symposium on Ubiquitous Multimedia Computing: 130-134.

[9] W. Luo, F. Huang, and J. Huang (2010) "*Edge adaptive image steganography based on LSB matching revisited.*" IEEE Trans. On Information Forensics and Security, 5 (2): 201- 214.

[10] X. Y. Wang (2003) "*Chaos in the Complex Nonlinear systems*." Electronics Industry Press.

[11] S. E. Asad (2012) "*Chaos Based Information Hiding and Security*." 7thInternational conference for internet Technology and secured Transactions: 67-2.

[12] B. D. Figueiredo, J. C. Diambra, L. Glass, L. Malta (2002) "*Chaos in two looped negative feedback systems*." Physical Review E., 65: 05190-1-05190-8.

[13] R. Babara, (2007) "Dynamics of hyperchaotic Lorenz system." *Int. J. Bifurcation and Chaos"*, 17 (12): 4285-4294.

[14] Juergen Seitz, University of Cooperative Education Heidenheim, Germany, "*Digital Watermarking for Digital Media*", 1st edition May 2005

[15] Potdar V.M., Han, S., Chang, E.; "*A survey of digital image watermarking techniques*", Industrial Informatics, 2005.INDIN '05.

[16] Brassil, J.T.; Low, S.; Maxemchuk, N.F.; O'Gorman, L.; "*Electronic marking and identification techniques to discourage"*

[17] Mohan Durvey (2014), "*A Review Paper on Digital Watermarking* "International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 4,Pp 99- 105

[18] Jaishri guru (2014), "*A Review of Watermarking Algorithms for Digital Image* ",International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 9, Pp 5701- 5708

[19] Hai Tao (2014), "*Robust Image Watermarking Theories and Techniques: A Review* "Journal of Applied Research and Technology, Volume 12, Issue 1, Pages 122–138

[20] Inita Gupta M (2014), "*A Review on Image Watermarking and Its Techniques*" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 1,Pp 92- 97

[21] Manjit Thapa (2011)" *Digital Image Watermarking Technique Based on Different Attacks*", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4,Pp 14 -19

[22] Radhika v (2013), "*Comparative Analysis of Watermarking in Digital Images Using DCT & DWT*" International Journal of Scientific and Research Publications, Volume 3, Issue 2,Pp 1-4

[23] Zhu Yuefeng (2015), "*Digital image watermarking algorithms based on dual transform domain and self-recovery*" international journal on smart sensing and intelligent systems vol. 8, no. 1,pp 199- 219

[24] Puneet Kr Sharma (2012), "*Analysis of image watermarking using least significant bit algorithm*" International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4,Pp 95 -101

[25] Md. Selim Reza (2012), "*An Approach of Digital Image Copyright Protection by Using Watermarking Technology*" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2,Pp 280 -286

[26] Shrusti Porwal (2013), "*Data Compression Methodologies for Lossless Data and Comparison between Algorithms*" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2,Pp 142- 147

[27] Shankar Thawkar (2012," *Digital Image Watermarking for Copyright Protection*" International Journal of Computer Science and Information Technologies, Vol. 3 (2) , pp 3757- 3760

[28] Das Subhajit, Maity Reshmi, Maity N. P, "*VLSI-Based Pipeline Architecture for Reversible Image Watermarking by Difference Expansion with High-Level Synthesis Approach*", Springer Science+ Business Media(2017).

[29] Qu Gang, Publicly Detectable "*Watermarking for Intellectual Property Authentication in VLSI Design*", IEEE transactions on computer aided design Of Integrated circuits and systems (2002) 1363- 1368, Vol. 21, No.11.

[30] Zhang Jiliang and Liu Lele, "*Publicly Verifiable Watermarking for Intellectual Property Protection in FP*" (2010)