

# **Decentralized Intellectual Property (IP) Protection Platform with AI-Powered Similarity Detection**

R25-016

Project Proposal Report

Lindamulage Jehan Shenil Silva

B.Sc. (Hons) Degree in Information Technology  
Specialized in Software Engineering

Department of Computer Science and Software  
Engineering

Sri Lanka Institute of Information Technology Sri Lanka

January 2025

# **Decentralized Intellectual Property (IP) Protection Platform with AI-Powered Similarity Detection**

R25-016

Project Proposal Report

Lindamulage Jehan Shenil Silva – IT21804342

Supervisor: Dharshana Kasthurirathna

B.Sc. (Hons) Degree in Information Technology  
Specialized in Software Engineering


Department of Computer Science and Software  
Engineering

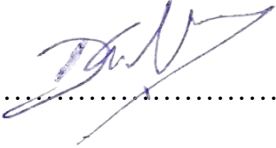
Sri Lanka Institute of Information Technology Sri Lanka

January 2025

# DECLARATION

I declare that this is my own work, and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Name	Student ID	Signature
Silva L. J. S	IT21804342	

  
.....  
Signature of the Supervisor  
(Dharshana Kasthurirathna)

03/02/2025  
.....  
Date

# ABSTRACT

In response to the escalating digitalization and the growing risk of intellectual property (IP) infringement, this research focuses on advancing **similarity checking and continuous model learning for video content**. It forms a core component of a decentralized IP protection platform, leveraging the convergence of blockchain technology and artificial intelligence (AI). The study aims to develop adaptive AI/ML models capable of detecting video similarity in real time, catering to diverse video formats. This is achieved by integrating APIs that deliver immediate similarity analysis and employing continuous learning pipelines to ensure model improvement with evolving datasets and user feedback.

The novelty lies in the real-time adaptive capabilities of the proposed system, enabling dynamic detection of video-based infringements while preserving scalability and accuracy. This approach integrates federated learning and context-aware detection techniques to refine its precision further. The decentralized nature of the platform ensures secure, tamper-proof IP registration and robust infringement detection, while the integration of blockchain reinforces trust, transparency, and data integrity.

By addressing the limitations of traditional IP protection mechanisms, such as reliance on centralized databases, this research paves the way for a scalable and globally applicable solution tailored specifically for video content. It highlights the significant potential for advancing IP protection standards while fostering innovation and collaboration across industries.

**Keywords: Intellectual Property Protection, Video Content Similarity, Continuous Model Learning, Adaptive AI/ML Models, Blockchain Integration, Real-Time Similarity Detection, Federated Learning, Video Analysis, Decentralized IP Platform, Context-Aware Detection**

# TABLE OF CONTENTS

Declaration .....	iii
ABSTRACT.....	iv
List of Figures .....	vii
List of tables.....	viii
LIST OF ABBREVIATIONS .....	ix
1. INTRODUCTION .....	1
2. Background & Literature Survey .....	2
3. Research Gap .....	4
3.1 Addressing the Gap.....	7
4. Research Problem .....	8
5. OBJECTIVES .....	10
5.1 Main Objective.....	10
5.2 Specific Objectives .....	10
6. METHODOLOGY .....	12
6.1 System Architecture diagram.....	12
6.2 Component diagram.....	12
6.3 The flow of the project.....	14
6.3.1. Requirement Gathering and Analysis .....	14
6.3.2. Feasibility Study .....	14
6.3.3. Implementation .....	15
6.3.4. Testing.....	16
6.4 Flow Chart .....	18
7. Project Requirements .....	19

7.1	Functional and Non-Functional Requirements .....	19
7.2	Software Requirements .....	20
7.3	Software Solution.....	21
7.4	Requirement Gathering and Analysis .....	21
7.5	Expected test cases.....	23
7.5.1.	Functional test cases .....	23
7.5.2.	Non-Functional Test Cases .....	23
7.5.3.	Security Test Cases .....	24
7.5.4.	Integration Test Cases .....	25
7.5.5.	Edge Case Test Cases.....	25
8.	GANTT CHART.....	26
9.	COMERCIALIZATION .....	27
9.1	The Problem We Solve .....	27
9.2	Our Solution.....	27
9.3	Key Features and Benefits .....	27
9.4	Target Market and Revenue Model.....	28
9.5	Why Choose Us?.....	29
10.	REFERENCES .....	30
11.	APPENDICES .....	32
11.1	Plagiarism Report.....	32

# LIST OF FIGURES

Figure 1: System architecture diagram .....	12
Figure 2: Component diagram .....	13
Figure 3: Flow Chart.....	18
Figure 4: Agile Methodology.....	21
Figure 5: Grant Chart.....	26
Figure 6: Plagiarism report .....	32

# LIST OF TABLES

Table 1: Comparison with existing applications .....	6
Table 2: Functional and Non-Functional Requirements .....	19
Table 3: Functional test cases .....	23
Table 4: Non-Functional Test Cases .....	23
Table 5: Security Test Cases .....	24
Table 6: Integration Test Cases .....	25
Table 7: Edge Case Test Cases.....	25



# LIST OF ABBREVIATIONS

IP	Intellectual Property
AI	Artificial Intelligence
ML	Machine Learning
API	Application Programming Interface
I3D	Inflated 3D ConvNet
C3D	3D Convolutional Neural Network
CNN	Convolutional Neural Network
UI	User Interface
UAT	User Acceptance Testing
ROI	Return on Investment
SDLC	Software Development Life Cycle
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
AWS	Amazon Web Services
IPFS	InterPlanetary File System
NoSQL	Not Only SQL (Non-relational Database)
TRIPS	Trade-Related Aspects of Intellectual Property Rights
GAN	Generative Adversarial Network
FLV	Flash Video (File Format)
NFT	Non-Fungible Token
JSON	JavaScript Object Notation
PDF	Portable Document Format
SIFT	Scale-Invariant Feature Transform
HOG	Histogram of Oriented Gradients
CVPR	Conference on Computer Vision and Pattern Recognition
ICML	International Conference on Machine Learning
AISTATS	Artificial Intelligence and Statistics Conference
WIPO	World Intellectual Property Organization

WTO	World Trade Organization
U.S.	United States
EU	European Union
GPU	Graphics Processing Unit
NFTs	Non-Fungible Tokens
DAO	Decentralized Autonomous Organization

# 1. INTRODUCTION

With the rapid growth of digital media, video content has become a dominant form of communication across platforms like social media, streaming services, and educational environments. This surge in video creation and distribution has increased the risk of intellectual property (IP) infringement, making it challenging to protect the authenticity, ownership, and originality of digital content. Traditional IP protection methods—such as watermarking, centralized databases, and manual review processes—are often inefficient, prone to manipulation, and lack the capability to handle large-scale, real-time content verification.

To address these challenges, this research focuses on developing a system for Similarity Checking for Video-Based Content with Continuous Model Learning. The primary objective is to create a real-time, adaptive, and secure solution for detecting similarities in video content, thereby enhancing IP protection. The system leverages advanced artificial intelligence (AI) and machine learning (ML) models, including Inflated 3D ConvNets (I3D), 3D ConvNets (C3D), and transformer-based models like TimeSformer, to accurately detect similarities by analyzing both spatial and temporal patterns in videos.

A key feature of the system is its continuous model learning capability, which allows AI models to adapt over time by learning from new data and user feedback. This ensures the system remains effective against evolving infringement techniques. Additionally, the integration of blockchain technology enables decentralized IP registration and ownership verification, providing tamper-proof, transparent records that enhance trust and security.

In conclusion, this component offers a comprehensive solution for protecting video-based IP through a combination of real-time similarity detection, adaptive learning, and decentralized security. It aims to provide a scalable, efficient, and future-ready framework for addressing IP challenges in the digital landscape.

## 2. BACKGROUND & LITERATURE SURVEY

The increasing reliance on digital media has resulted in the exponential growth of multimedia content, with videos emerging as one of the most dominant forms of communication and expression. Videos are extensively used across industries such as entertainment, education, marketing, journalism, and research, making them highly valuable intellectual property (IP) assets. Consequently, protecting the originality and ownership of video content has become crucial in combating unauthorized usage, piracy, and copyright infringement.

Traditional methods for protecting video content primarily rely on watermarking, centralized databases, and manual review processes. While watermarking helps in asserting ownership, it can often be removed or tampered with, making it an unreliable standalone solution. Centralized databases, on the other hand, face challenges related to data security, limited scalability, and susceptibility to tampering, thereby reducing their effectiveness in large-scale environments. Manual review processes are time-consuming, resource-intensive, and prone to human error, making them impractical for real-time IP protection.

Research in video similarity detection has made significant progress with the advent of machine learning (ML) and artificial intelligence (AI). Early approaches utilized feature extraction techniques such as Scale-Invariant Feature Transform (SIFT), Histogram of Oriented Gradients (HOG), and Optical Flow to detect visual similarities across video frames. While these traditional methods were effective for basic similarity checks, they often struggled with complex video manipulations, such as temporal distortions, frame alterations, and compression artifacts.

Recent advancements have shifted towards deep learning architectures, particularly Convolutional Neural Networks (CNNs) and 3D Convolutional Networks (C3D), which have significantly improved the accuracy of similarity detection by capturing both spatial and temporal features in videos. Additionally, models like Inflated 3D ConvNet (I3D) and TimeSformer have demonstrated strong performance in understanding spatiotemporal patterns, making them suitable for video similarity tasks. Transformer-based models, initially designed for natural language processing, have also been adapted to video analysis, offering promising results in learning complex temporal relationships.

However, despite these advancements, the application of video similarity detection in real-time scenarios and decentralized ecosystems remains limited. Existing solutions often struggle with scalability, latency issues, and the inability to continuously learn from new data. Moreover, the lack of robust integration with decentralized technologies like blockchain further limits their effectiveness in providing tamper-proof IP protection.

This research aims to bridge these gaps by developing an AI-powered video similarity detection system with continuous model learning capabilities, integrated into a decentralized IP protection platform. By leveraging advanced AI models and blockchain technology, the system aims to deliver real-time, scalable, and secure video IP protection, addressing the limitations of traditional approaches.

### 3. RESEARCH GAP

Despite significant advancements in video similarity detection, existing systems face notable challenges when it comes to addressing intellectual property (IP) infringement in decentralized and scalable environments. The evolution of deep learning and AI has improved the accuracy of similarity detection; however, there are still critical limitations that hinder the effectiveness of current solutions, especially in protecting video-based content. The key gaps identified are as follows:

1. **Centralized Infrastructure:**

Most traditional IP protection systems rely on centralized databases to store and manage video content and ownership information. This approach creates a single point of failure, making the system vulnerable to data breaches, tampering, and unauthorized access. Additionally, centralized architecture often struggles to handle the demands of large-scale operations, leading to scalability issues when dealing with vast amounts of video data.

2. **Limited Real-Time Capabilities:**

Existing video similarity detection systems primarily operate in batch-processing modes, where content is analyzed in large sets rather than in real time. This results in delays in detecting infringements, making it challenging to respond promptly to unauthorized usage, especially in fast-paced environments like social media and live streaming platforms. Real-time detection is essential to prevent IP violations before they cause significant damage.

3. **Lack of Adaptability:**

Many current AI models used for similarity detection are static, meaning they are trained once and rarely updated. This leads to decreased effectiveness over time as new types of video manipulations and infringement techniques emerge. Without the ability to continuously learn from new data and adapt to evolving threats, these models become outdated, reducing their accuracy in identifying sophisticated forms of video alterations.

4. **Data Privacy Concerns:**

Centralized systems raise serious privacy issues, particularly when dealing with sensitive or proprietary video content. Users often need to upload their data to third-party servers, increasing the risk of data leaks, unauthorized access, and misuse. This lack of privacy

can discourage individuals and organizations from adopting such systems, especially in industries where confidentiality is a top priority.

**5. Inefficient Handling of Complex Video Structures:**

While some systems can detect basic similarities, they struggle with complex video formats, such as videos with dynamic scenes, varying frame rates, and advanced editing effects. The inability to accurately analyze spatiotemporal features limits the effectiveness of these systems in detecting subtle manipulations commonly used in copyright infringement cases.

**6. Weak Integration with Decentralized Technologies:**

Current solutions rarely incorporate decentralized technologies like blockchain, which could provide tamper-proof ownership records and enhance the security of IP management. Without such integration, IP protection systems remain vulnerable to fraudulent claims, data manipulation, and lack of transparency in content ownership.

Table 1: Comparison with existing applications

	<b>Amazon Rekognition Video</b>	<b>Video Duplicate Finder (VDF)</b>	<b>Video Comparer</b>	<b>Proposed Solution</b>
AI-powered similarity detection	✓	✗	✓	✓
Real-time API integration	✓	✗	✗	✓
Continuous learning pipelines	✗	✗	✗	✓
Multimedia content coverage	✓	✗	✗	✓
Decentralized IP protection	✗	✗	✗	✓

The comparison reveals that while existing platforms like **Amazon Rekognition Video**, **Video Duplicate Finder (VDF)**, and **Video Comparer** provide basic video analysis or duplicate detection features, they fall short in several critical areas. None of these solutions offer a comprehensive framework that combines real-time detection, adaptive learning, and decentralized IP management.

In contrast, the proposed solution offers a holistic approach to video similarity checking and IP protection. By integrating AI-powered detection, real-time APIs, continuous model learning, and blockchain technology, it addresses the limitations of existing systems, providing a scalable, secure, and future-proof platform for protecting video-based intellectual property in the digital era.



### **3.1 Addressing the Gap**

This research aims to bridge these gaps by developing a decentralized video similarity detection system powered by adaptive AI/ML models and blockchain technology. The system will support real-time detection, enable continuous learning for model adaptability, ensure data privacy through decentralized storage, and provide secure IP management via blockchain. This approach promises to deliver a scalable, secure, and future-proof solution for protecting video-based intellectual property in the digital age.

## 4. RESEARCH PROBLEM

The identified gaps highlight the urgent need for an innovative solution that addresses the limitations of current video similarity detection methods, particularly in the context of intellectual property (IP) protection. Existing systems struggle with centralization issues, limited real-time capabilities, lack of adaptability, and data privacy concerns, making them inadequate for today's fast-evolving digital landscape.

Specifically, the research problem can be defined as:

- **"How can a decentralized and adaptive system be developed to detect similarity in video content in real-time, while ensuring scalability, security, and data privacy?"**

This research aims to address the problem by designing a **decentralized platform** that integrates **blockchain technology** for secure IP registration and management with advanced **AI/ML models** for video similarity detection. The proposed solution will focus on the following key aspects:

1. **Real-Time Video Similarity Detection:**

Developing AI models capable of analyzing video content in real time, detecting similarities even in cases of advanced manipulations, such as temporal edits, frame distortions, and visual alterations.

2. **Decentralized Architecture for Enhanced Security:**

Utilizing blockchain to create a tamper-proof environment for IP registration, ensuring transparent and secure management of video ownership records without relying on centralized databases.

3. **Adaptive Continuous Learning Pipelines:**

Implementing continuous model learning techniques that allow the system to adapt to new types of video manipulations and evolving infringement tactics. This ensures the models remain effective over time.

4. **Federated Learning for Data Privacy:**

Incorporating federated learning to enable model training on distributed datasets without

compromising user privacy. This approach minimizes the risk of data exposure while enhancing the model's learning capabilities.

#### **5. Scalability and Global Applicability:**

Ensuring that the solution is scalable to handle large volumes of video data and globally applicable across different industries, including entertainment, education, media, and content creation.

By bridging the gaps in existing systems, this research seeks to provide a robust, innovative approach to protecting video-based intellectual property in the digital age. The combination of real-time AI-driven detection, blockchain-based security, and continuous learning mechanisms promises to revolutionize the way IP protection is managed for video content, fostering a safer and more transparent digital ecosystem.

## 5. OBJECTIVES

### 5.1 Main Objective

To develop a decentralized and adaptive system for real-time similarity detection of video content using advanced AI/ML techniques and blockchain technology, ensuring scalability, security, and data privacy.

This objective focuses on creating an innovative solution that not only detects video similarities with high accuracy but also provides robust intellectual property (IP) protection through decentralized technologies. The system will be designed to adapt to evolving video manipulation techniques while maintaining performance, privacy, and reliability in diverse environments.

### 5.2 Specific Objectives

1. Design and Develop AI/ML Models for Video Similarity Detection
  - Implement robust AI/ML models specifically designed for detecting similarities in video content.
  - Utilize advanced deep learning architectures, such as Convolutional Neural Networks (CNNs), 3D ConvNets (C3D), and Transformer-based models for precise and efficient video content analysis, focusing on both spatial and temporal features.
2. Enable Real-Time Video Similarity Detection
  - Integrate APIs to facilitate real-time similarity checking and provide immediate infringement alerts to users.
  - Optimize the system for low-latency processing and high-throughput performance, ensuring seamless detection even in dynamic environments like live streaming platforms.
3. Implement Continuous Model Learning
  - Establish a continuous learning pipeline that allows the AI models to adapt and improve over time based on new datasets, evolving infringement patterns, and user feedback.

- Leverage federated learning techniques to enhance model performance while maintaining data privacy, allowing the system to learn from distributed data without compromising sensitive information.
4. Integrate Blockchain for Decentralized IP Management
    - Utilize blockchain technology to securely register video intellectual property and maintain tamper-proof ownership records, ensuring authenticity and trust.
    - Implement smart contracts for automating IP transactions, licensing agreements, and ownership transfers, reducing the need for manual intervention and increasing efficiency.
  5. Enhance System Scalability and Security
    - Design a flexible architecture capable of handling large-scale video datasets with global accessibility, supporting a wide range of industries and applications.
    - Employ advanced security measures, including encryption, secure APIs, and privacy-preserving techniques, to protect both IP data and user information from potential threats.
  6. Ensure Practical Application and Usability
    - Develop user-friendly interfaces and tools for seamless IP registration, video similarity checking, and infringement reporting, making the system accessible to both technical and non-technical users.
    - Provide integration capabilities with industry-specific workflows, including entertainment, education, digital marketing, and legal domains, to support diverse use cases.
  7. Promote Cross-Industry Adoption
    - Design the platform to be compatible with existing IP protection standards and legal frameworks to facilitate smooth adoption across different industries.
    - Ensure interoperability with other decentralized systems and traditional IP mechanisms, promoting collaboration and ease of use in global IP ecosystems.

These objectives collectively aim to address the gaps in existing IP protection systems by providing an innovative, scalable, and secure platform for detecting and managing video-based content similarity.

## 6. METHODOLOGY

### 6.1 System Architecture diagram

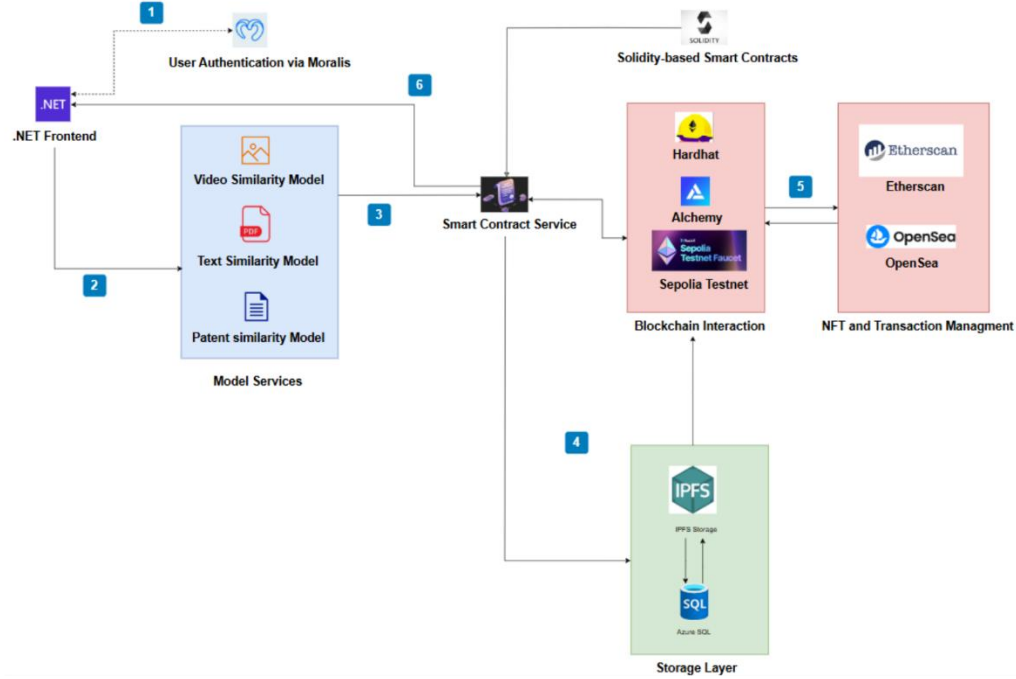


Figure 1: System architecture diagram

### 6.2 Component diagram

The system architecture for the Video Similarity Checking and Continuous Model Learning component, as illustrated in **Figure 2**, is designed to provide real-time video similarity detection with secure, decentralized IP protection. Users upload videos through the UI/Dashboard, which communicates with the API Module to handle requests and ensure secure access via the Authentication & Security Module. The uploaded video is processed by the Multimedia Input Handler and then sent to the Preprocessing Module for keyframe extraction and data normalization.

Next, the Feature Extraction Module uses AI models like I3D, C3D, and TimeSformer to analyze spatiotemporal patterns, while the Similarity Computation Module compares these features against stored data to generate similarity scores. The AI/ML Model powers this analysis and

continuously improves through the Adaptive Learning Pipeline, which updates the model based on new data and user feedback.

Similarity results and metadata are stored securely in the Content Storage system. The Blockchain Module ensures tamper-proof IP registration and ownership verification, with additional support from IPFS/Decentralized Storage for secure data handling. Finally, users receive real-time similarity results and infringement alerts via the API module. This architecture, depicted in **Figure 2**, ensures the system is scalable, adaptive, and secure, effectively supporting the goal of robust, real-time IP protection for video content.

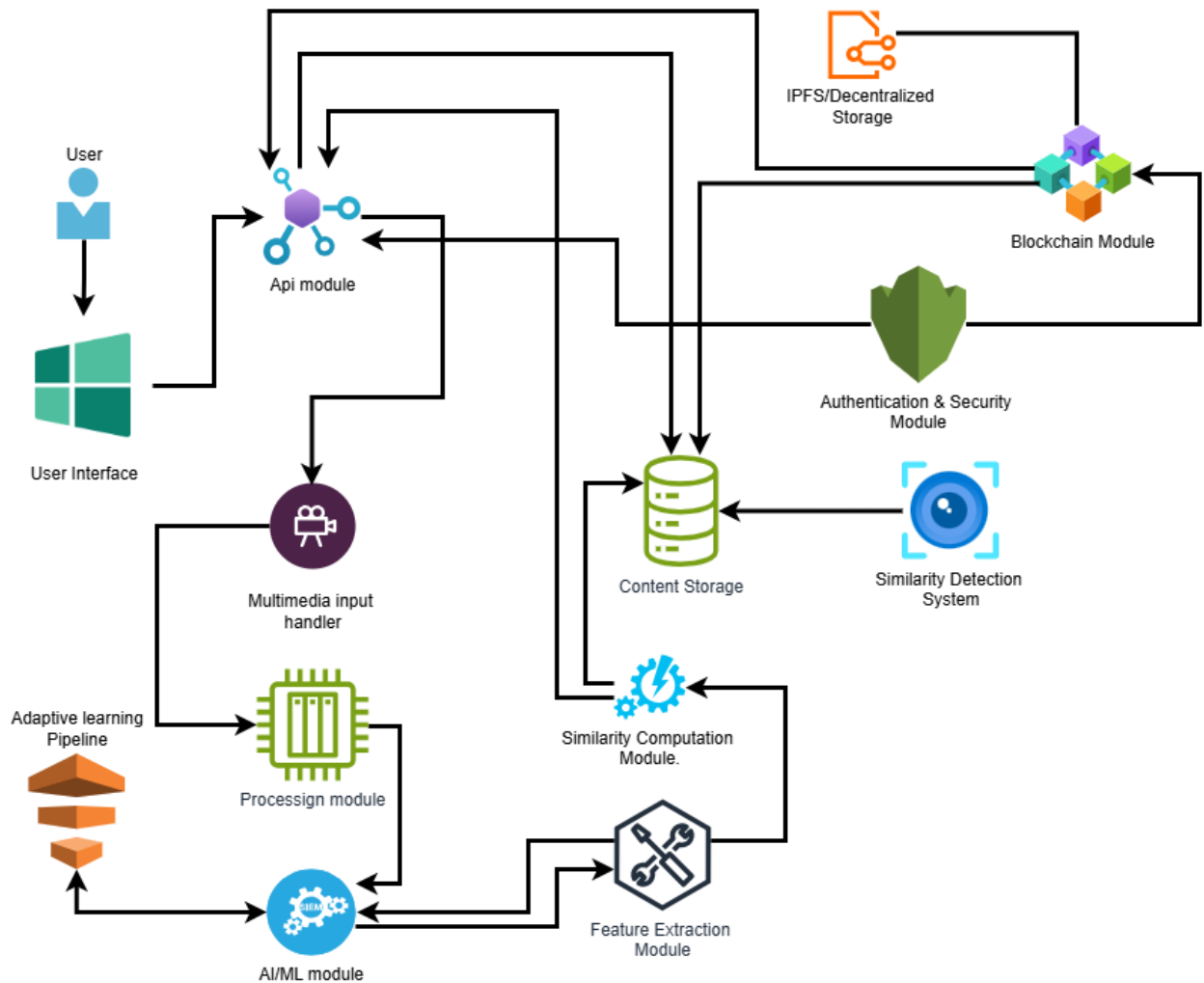


Figure 2: Component diagram

## 6.3 The flow of the project

The project follows a structured approach to ensure the successful development and deployment of a system for Similarity Checking for video based and Continuous Model Learning. The flow is divided into four primary phases, detailed below:

### 6.3.1. Requirement Gathering and Analysis

The first phase involves understanding the system's purpose, identifying key stakeholders, and documenting functional and non-functional requirements. The main activities include:

- **Stakeholder Identification:** Engaging content creators, legal entities, and platform users to understand their expectations and challenges in IP protection.
- **Data Collection:** Utilizing surveys, interviews, and workshops to gather insights into user needs. For example, content creators require a secure and efficient similarity detection mechanism, while legal entities prioritize tamper-proof ownership records.
- **Functional Analysis:** Defining the core functionalities, such as real-time similarity detection, blockchain-based IP registration, and continuous learning pipelines.
- **Non-Functional Requirements:** Establishing critical performance metrics, such as system scalability, data security, and latency thresholds.
- **Requirement Prioritization:** Categorizing requirements into high, medium, and low priorities to ensure phased delivery while addressing critical user needs first.

This phase culminates in a requirements specification document that serves as the blueprint for subsequent stages.

### 6.3.2. Feasibility Study

The feasibility study evaluates the technical, operational, and economic viability of the proposed system. The key aspects include:

- **Technical Feasibility:**



- Analyzing the compatibility of technologies such as AI/ML models, blockchain platforms, and authentication frameworks (e.g., Moralis).
- Evaluating the ability to handle large-scale multimedia datasets and real-time similarity detection using existing hardware and software.
- **Operational Feasibility:**
  - Assessing whether the system aligns with the workflows of target users, such as content creators and IP regulators.
  - Ensuring usability through user-friendly interfaces and clear navigation paths for critical operations like registering IP and viewing similarity results.
- **Economic Feasibility:**
  - Estimating the development cost, including licensing for tools (e.g., Hardhat, Alchemy) and training AI models.
  - Projecting return on investment (ROI) based on adoption by industries requiring IP protection, such as media and technology.

### 6.3.3. Implementation

The implementation phase focuses on building the system, integrating its components, and ensuring smooth operation. The activities include:

- **System Design and Architecture:**
  - Finalizing a modular architecture where components like the AI/ML engine, blockchain layer, and frontend interface interact seamlessly.
  - Establishing APIs for communication between the backend and other services.
- **Component Development:**
  - Developing the AI/ML models for similarity detection using frameworks like TensorFlow or PyTorch.

- Implementing blockchain-based smart contracts to register IP and manage licensing.
- Creating a responsive and interactive frontend using technologies like React and Moralis for authentication.
- **Integration and Deployment:**
  - Integrating the developed components, such as linking the AI/ML engine to the backend for similarity processing.
  - Deploying the system on a cloud infrastructure to ensure scalability and accessibility.

Iterative development techniques are employed, allowing for incremental feature delivery and continuous improvement.

#### 6.3.4. Testing

Testing ensures the system functions as intended and meets the defined requirements. This phase involves multiple levels of validation:

- **Unit Testing:**
  - Testing individual components, such as AI model inference, blockchain interactions, and frontend modules, to ensure correctness.
- **Integration Testing:**
  - Verifying that components interact seamlessly, such as ensuring similarity results from the AI/ML engine are accurately displayed in the frontend.
- **System Testing:**
  - Evaluating the entire system for functional and non-functional requirements, such as real-time performance, scalability, and data security.
- **User Acceptance Testing (UAT):**

- Engaging end-users, such as content creators and legal advisors, to test the system in real-world scenarios.
- Gathering feedback to refine features and improve usability.
- **Regression Testing:**
  - Ensuring new updates, such as model improvements or additional blockchain functionalities, do not introduce errors into existing features.

Testing concludes with the preparation of detailed reports highlighting the system's readiness for deployment and any unresolved issues.

## 6.4 Flow Chart

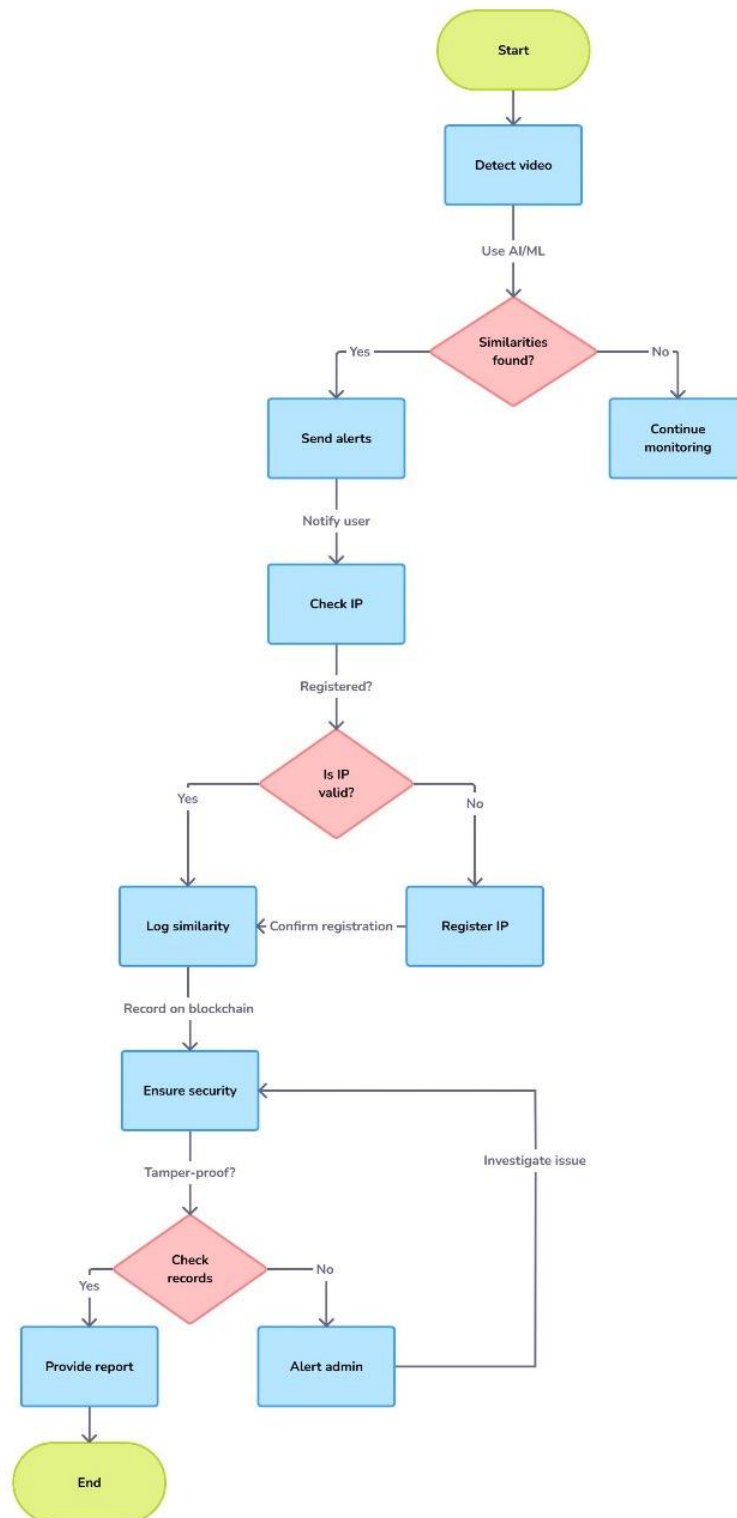


Figure 3: Flow Chart

## 7. PROJECT REQUIREMENTS

The success of the Similarity Checking for **video-based** Contents and Continuous Model Learning system relies on well-defined project requirements. These are categorized into functional, non-functional, and software requirements to ensure comprehensive coverage of the system's needs.

### 7.1 Functional and Non-Functional Requirements

Table 2: Functional and Non-Functional Requirements

Category	Requirement	Description
Functional Requirements	Real-Time Similarity Detection	Allow users to upload video content and receive similarity detection results instantly.
	Continuous Model Learning	Implement a pipeline for AI/ML models to improve accuracy using new data, user interactions, and feedback.
	Blockchain-Based IP Registration	Provide secure, tamper-proof IP registration with smart contract capabilities for ownership verification and licensing.
	User Authentication	Ensure secure login and verification through blockchain wallet connections (e.g., using Moralis).
	Reporting and Alerts	Generate detailed reports for detected similarities and send real-time alerts for potential infringements.
	Data Management	Efficiently maintain multimedia metadata, user feedback, and similarity scores in a structured database.
Non-Functional Requirements	Scalability	Handle increasing numbers of users and large multimedia datasets without performance degradation.

	Performance	Ensure low-latency responses for real-time similarity detection and backend processing.
	Security	Protect data integrity and privacy using encryption, blockchain for tamper-proof records, and federated learning for model privacy.
	Reliability	Maintain high availability and minimal downtime for uninterrupted user access.
	Usability	Design intuitive, user-friendly interfaces to ensure seamless navigation and ease of use.
	Interoperability	Ensure compatibility with existing IP protection frameworks and decentralized platforms for broad adoption.

## 7.2 Software Requirements

The software requirements identify the tools, frameworks, and platforms necessary for development and deployment:

- **Frontend:**  
React for building user interfaces and Moralis for authentication services.
- **Backend:**  
Node.js or Python-based backend for API development and integration with other components.
- **AI/ML Frameworks:**  
TensorFlow or PyTorch for implementing and training similarity detection models.
- **Blockchain Tools:**  
Solidity for smart contract development, Hardhat for blockchain testing, and Alchemy for API interactions with the Ethereum network.

- **Database:**

A NoSQL database like MongoDB for storing metadata and results, along with multimedia datasets.

- **Other Tools:**

Git for version control, Docker for containerization, and cloud services (e.g., AWS or Azure) for deployment and scalability.

## 7.3 Software Solution

For implementing the Video Similarity Checking and Continuous Model Learning component, the most suitable SDLC model would be the Agile Software Development Lifecycle. Given the system's complexity, need for continuous learning, integration with blockchain, and real-time processing requirements, Agile offers the flexibility, adaptability, and iterative approach necessary for such an evolving project.

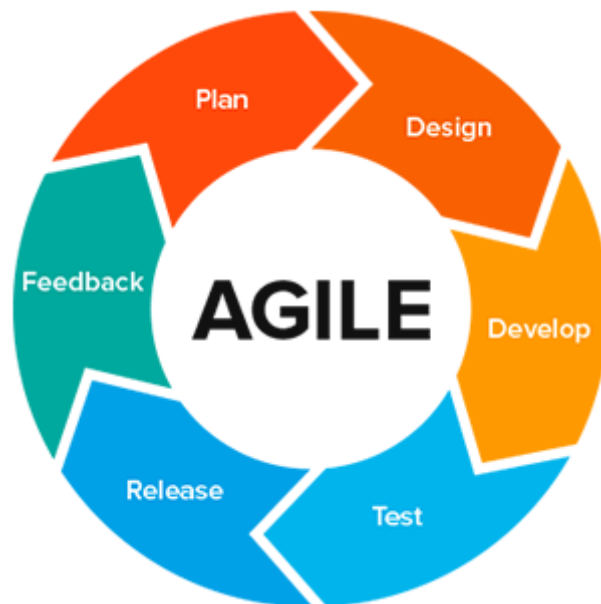


Figure 4: Agile Methodology

## 7.4 Requirement Gathering and Analysis

**Stakeholder Interviews:**

- Conduct interviews with key stakeholders, including product owners, legal advisors, developers, and potential end-users.
- Focus on understanding pain points with current IP protection mechanisms and expectations from the new system.

#### **Workshops and Brainstorming Sessions:**

- Organize collaborative sessions to gather diverse perspectives on system functionalities and potential challenges.
- Use brainstorming to generate innovative ideas, particularly for AI model adaptability and blockchain integration.

#### **Surveys and Questionnaires:**

- Distribute structured questionnaires to potential users to understand their needs regarding video content similarity detection and IP registration.

#### **Document Analysis:**

- Review existing documentation from related IP protection systems, AI-based similarity tools, and blockchain solutions to identify gaps and opportunities.

#### **Use Case and User Story Development:**

- Create use cases and user stories to describe specific scenarios, such as:
  - "As a content creator, I want to upload my video and receive similarity results in real-time to detect potential infringements."



## 7.5 Expected test cases

### 7.5.1. Functional test cases

Table 3: Functional test cases

Test Case ID	Test Case Description	Input	Expected Output	Status
TC_F001	Upload Video for Similarity Detection	Upload a valid MP4 video	Video is processed, and similarity score is displayed	Pass/Fail
TC_F002	Detect Similar Video	Upload a video similar to an existing one	System detects similarity and returns matching percentage	Pass/Fail
TC_F003	Detect Non-Similar Video	Upload a completely different video	System returns a low or 0% similarity score	Pass/Fail
TC_F004	Real-Time API Response Test	Send API request with video data	API responds within defined time threshold (e.g., <2s)	Pass/Fail
TC_F005	Continuous Model Learning Update	Add new training data and retrain model	Model updates without affecting system uptime	Pass/Fail

### 7.5.2. Non-Functional Test Cases

Table 4: Non-Functional Test Cases

Test Case ID	Test Case Description	Input	Expected Output	Status
TC_NF001	Performance Test under Load	Upload 100 videos simultaneously	System processes without significant delays	Pass/Fail

TC_NF002	Scalability Test	Increase number of users accessing system	System handles requests without crashing	Pass/Fail
TC_NF003	Response Time Test	Upload large video file (1GB)	Response time within defined limits (e.g., <5s)	Pass/Fail
TC_NF004	Usability Test	Navigate user dashboard	Intuitive, responsive, and user-friendly interface	Pass/Fail
TC_NF005	Data Consistency Test	Upload same video twice	System returns consistent similarity results	Pass/Fail

### 7.5.3. Security Test Cases

Table 5: Security Test Cases

Test Case ID	Test Case Description	Input	Expected Output	Status
TC_S001	Unauthorized Access Attempt	Attempt login with invalid credentials	Access denied with error message	Pass/Fail
TC_S001	Data Encryption Test	Upload video and metadata	Data is encrypted during transmission and storage	Pass/Fail
TC_S001	Smart Contract Tampering Test	Try altering blockchain record	Tampering detected; changes are rejected	Pass/Fail

#### 7.5.4. Integration Test Cases

Table 6: Integration Test Cases

Test Case ID	Test Case Description	Input	Expected Output	Status
TC_I001	Integration with Blockchain	Register video ownership via API	Transaction recorded on blockchain successfully	Pass/Fail
TC_I002	Integration with External IP Databases	Search for registered IPs	Retrieves correct IP data from external databases	Pass/Fail

#### 7.5.5. Edge Case Test Cases

Table 7: Edge Case Test Cases

Test Case ID	Test Case Description	Input	Expected Output	Status
TC_E001	Upload Corrupted Video File	Upload a corrupted or incomplete video file	System returns error message and rejects file	Pass/Fail
TC_E002	Upload Unsupported Video Format	Upload video in unsupported format (e.g., FLV)	System returns format error	Pass/Fail

## 8. GANTT CHART

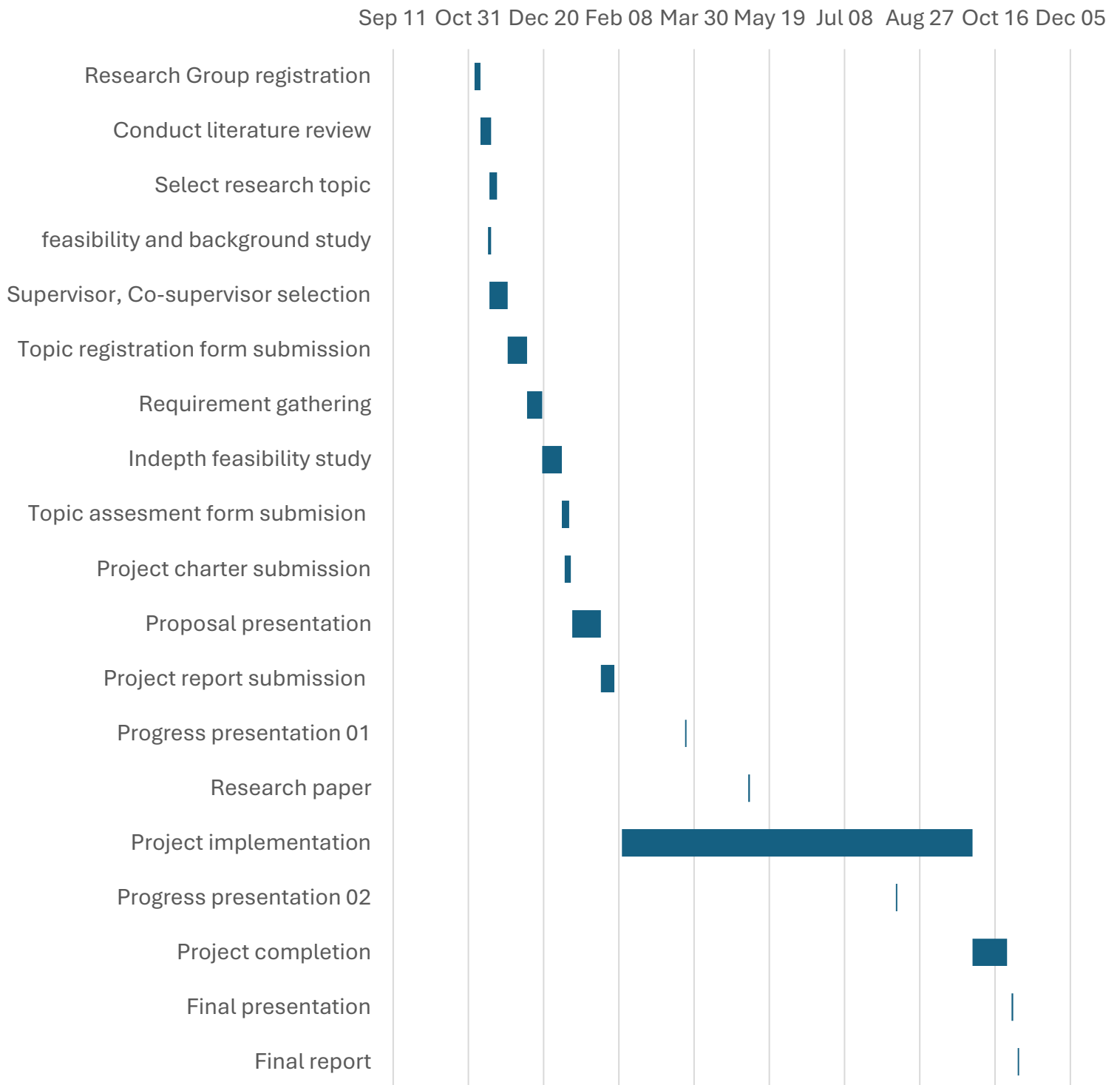


Figure 5: Grant Chart

## 9. COMERCIALIZATION

In the modern digital era, the exponential growth of video based content has created a critical need for robust intellectual property (IP) protection solutions. Our innovative Similarity Checking for video based and Continuous Model Learning application offers a groundbreaking approach to safeguarding digital assets while being affordable and accessible for individuals, small businesses, and enterprises alike.

### 9.1 The Problem We Solve

Content creators, brands, and businesses face constant threats of IP infringement, piracy, and unauthorized usage of video based content. Existing solutions are expensive, rely on centralized systems prone to tampering, and lack real-time capabilities. As a result, creators often encounter significant delays and obstacles in protecting their valuable intellectual property.

### 9.2 Our Solution

We provide an affordable, efficient, and scalable platform that combines cutting-edge artificial intelligence (AI) and blockchain technology to address these challenges. Our system enables real-time similarity detection for video based contents, supported by continuous model learning to ensure accuracy and adaptability. By integrating blockchain, we provide a decentralized and tamper-proof mechanism for registering, managing, and verifying intellectual property ownership.

### 9.3 Key Features and Benefits

#### 9.3.1. Real-Time Similarity Detection:

- Users can instantly upload content and receive similarity results, helping them quickly identify potential IP infringements.

#### 9.3.2. Continuous Model Learning:

- Our system evolves with new data, user feedback, and real-world examples, ensuring it stays accurate and relevant.

#### 9.3.3. Blockchain-Powered Security:

- IP registration and ownership tracking are securely managed using smart contracts, offering unparalleled trust and transparency.

#### 9.3.4. **Affordable Accessibility:**

- The platform is designed to cater to a wide audience, from freelancers and small businesses to large organizations, with flexible pricing tiers and no hidden costs.

#### 9.3.5. **User-Friendly Design:**

- A simple and intuitive interface allows users to interact with the platform seamlessly, regardless of their technical expertise.

#### 9.3.6. **Scalability:**

- Our cloud-based infrastructure ensures the platform can scale effortlessly to meet the needs of a growing user base and large multimedia datasets.

## 9.4 **Target Market and Revenue Model**

Our primary target markets include:

- **Content Creators:** Freelancers, photographers, videographers, and digital artists who need to protect their creative works.
- **Businesses and Brands:** Companies seeking to safeguard their promotional and branding materials.
- **Legal and Regulatory Agencies:** Organizations requiring advanced tools for detecting and resolving IP disputes.

We employ a **subscription-based revenue model** with tiered pricing plans:

- **Basic Plan:** Affordable access for individuals with limited usage and core features.
- **Pro Plan:** Advanced features, including continuous model updates, real-time alerts, and priority support.
- **Enterprise Plan:** Customized solutions for large businesses with extended functionalities and API integrations.

## **9.5 Why Choose Us?**

Our application stands out in the market for its affordability, ease of use, and innovative technology. Unlike competitors that rely on expensive centralized systems, we utilize a decentralized architecture, making it both cost-effective and highly secure. Furthermore, our focus on continuous model learning ensures that our system improves over time, keeping pace with evolving IP protection needs.

## 10. REFERENCES

- [1] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, 2016, pp. 779–788.
- [2] A. Dosovitskiy et al., "An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale," *arXiv preprint arXiv:2010.11929*, 2020.
- [3] Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015.
- [4] J. M. Koo et al., "Plagiarism Detection in Multimedia Using Deep Learning," in *Proc. Int. Conf. Multimedia Retrieval (ICMR)*, 2021, pp. 149–157.
- [5] T. Mikolov et al., "Distributed Representations of Words and Phrases and Their Compositionality," in *Advances Neural Inf. Process. Syst.*, vol. 26, pp. 3111–3119, 2013.
- [6] WIPO, *Understanding Copyright and Related Rights*. Geneva, Switzerland: World Intellectual Property Organization, 2016. [Online]. Available: [https://www.wipo.int/edocs/pubdocs/en/copyright/909/wipo\\_pub\\_909.pdf](https://www.wipo.int/edocs/pubdocs/en/copyright/909/wipo_pub_909.pdf).
- [7] WIPO, *Guide on Intellectual Property (IP) and Artificial Intelligence (AI)*, Geneva, Switzerland: World Intellectual Property Organization, 2021. [Online]. Available: <https://www.wipo.int/publications/en/details.jsp?id=4514>.
- [8] WIPO, *Blockchain and IP Ecosystems*, Geneva, Switzerland: World Intellectual Property Organization, 2022. [Online]. Available: <https://www.wipo.int/blockchain/en/>.
- [9] WIPO, *Berne Convention for the Protection of Literary and Artistic Works*, Geneva, Switzerland: World Intellectual Property Organization, 1886 (rev. 1979). [Online]. Available: <https://www.wipo.int/treaties/en/ip/berne/>.
- [10] WTO, *Trade-Related Aspects of Intellectual Property Rights (TRIPS)*, World Trade Organization, 1995. [Online]. Available: [https://www.wto.org/english/tratop\\_e/trips\\_e/trips\\_e.htm](https://www.wto.org/english/tratop_e/trips_e/trips_e.htm).
- [11] *Copyright Act of 1976*, U.S. Copyright Office, United States, 1976. [Online]. Available: <https://www.copyright.gov/title17/>.
- [12] European Parliament and Council, *Directive 2019/790 on Copyright in the Digital Single Market*, European Union, 2019. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2019/790/oj>.



- [13] Sri Lanka Intellectual Property Act No. 36 of 2003, World Intellectual Property Organization. [Online]. Available: <https://www.wipo.int/edocs/lexdocs/laws/en/lk/lk036en.pdf>.
- [14] Solidity, "Introduction to Smart Contracts," [Online]. Available: <https://docs.soliditylang.org/en/latest/introduction-to-smart-contracts.html>.
- [15] OpenZeppelin, "Smart Contract Libraries for Secure Development," [Online]. Available: <https://www.openzeppelin.com/>.
- [16] Alchemy, "Blockchain Development Platform," [Online]. Available: <https://www.alchemy.com/>.
- [17] Hardhat, "Ethereum Development Environment," [Online]. Available: <https://hardhat.org/>.
- [18] T. Dreier and B. Hugenholtz, *Concise European Copyright Law*, 2nd ed. Alphen aan den Rijn, Netherlands: Kluwer Law International, 2016.
- [19] S. Ricketson and J. Ginsburg, *International Copyright and Neighbouring Rights: The Berne Convention and Beyond*, 2nd ed. Oxford, U.K.: Oxford University Press, 2006.
- [20] E. Rosati, *Copyright and the Court of Justice of the European Union*. Oxford, U.K.: Oxford University Press, 2019.
- [21] H. B. McMahan et al., "Communication-Efficient Learning of Deep Networks from Decentralized Data," in *Proc. Int. Conf. Artificial Intelligence and Statistics (AISTATS)*, 2017, pp. 1273–1282.
- [22] I. Goodfellow, J. Pouget-Abadie, M. Mirza et al., "Generative Adversarial Networks," in *Advances Neural Inf. Process. Syst.*, vol. 27, pp. 2672–2680, 2014.
- [23] T. Chen, S. Kornblith, M. Norouzi, and G. Hinton, "A Simple Framework for Contrastive Learning of Visual Representations," in *Proc. Int. Conf. Mach. Learn. (ICML)*, 2020, pp. 1597–1607.
- [24] N. Z. Gong, "Privacy-Preserving Data Analysis for Federated Learning," *ACM Comput. Surv.*, vol. 55, no. 3, pp. 1–33, May 2022.
- [25] ISO/IEC 27001, *Information Security Management Standards*. Geneva, Switzerland: International Organization for Standardization, 2013.

# 11. APPENDICES

## 11.1 Plagiarism Report

> 4th year Assignmet ?				
Paper Title	Uploaded	Grade	Similarity	
<a href="#">IT21804342.pdf</a>	03 Feb 2025 19:25	--	<div><div></div>9%</div>	  

Figure 6: Plagiarism report