CLOUD BASED COPYRIGHT DETECTION FOR MULTIMEDIA CONTENT

A PROJECT REPORT

Submitted by

BARATH KAILASH G	**(190501025)**
GOUTHAM S	**(190501037)**
HAREE J	**(190501040)**

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

SRI VENKATESWARA COLLEGE OF ENGINEERING
(An Autonomous Institution; Affiliated to Anna University, Chennai-600025)
ANNA UNIVERSITY, CHENNAI 600 025

MAY 2023

SRI VENKATESWARA COLLEGE OF ENGINEERING

(An Autonomous Institution; Affiliated to Anna University, Chennai-600025)

ANNA UNIVERSITY, CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report **“CLOUD-BASED COPYRIGHT DETECTION FOR MULTIMEDIA CONTENT”** is the bonafide work of **“BARATH KAILASH G (190501025), GOUTHAM S (190501037)** and **HAREE J (190501040)”** who carried out the project work under my supervision.

SIGNATURE	**SIGNATURE**
Dr. R. ANITHA	**Mr. R. SENTHIL KUMAR**
HEAD OF THE DEPARTMENT	**SUPERVISOR**
	ASSISTANT PROFESSOR
COMPUTER SCIENCE & ENGG	**COMPUTER SCIENCE & ENGG**

Submitted for the project viva-voce examination held on ___________

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ABSTRACT

The proposed multimedia copyright detection system employs a multi-layered approach that encompasses encryption, distributed matching and method to create digital signatures. This system can be used to protect different multimedia content types, including 2-D videos, 3-D videos, images, audio clips, songs, and music clips and can be deployed on private and public clouds. The signature method creates robust and representative signatures of 3-D videos that capture the depth signals in these videos and it is computationally efficient to compute and compare as well as it requires small storage. The distributed matching engine achieves high scalability and it is designed to support different multimedia objects. As the adoption of cloud computing continues to grow, there is an increasing need for robust and efficient multimedia content protection systems (PaaS) that can safeguard intellectual property and ensure the privacy and integrity of digital media assets stored and distributed in cloud environments. The system architecture comprises of a cloud-based platform that provides a secure environment for storing and processing multimedia content, as well as a web-based interface that allows users to upload, manage, and distribute their content. The system is designed to be scalable and can be easily adapted to handle large volumes of multimedia content.

ACKNOWLEDGEMENT

We thank our Principal **Dr. S. Ganesh Vaidyanathan**, Sri Venkateswara College of Engineering for being the source of inspiration throughout our study in this college.

We express our sincere thanks to **Dr. R. Anitha, Professor, Head of the Department**, Computer Science and Engineering for her encouragement accorded to carry this project.

With profound respect, we express our deep sense of gratitude and sincere thanks to our guide **Mr. R. Senthil Kumar, Assistant Professor**, for his valuable guidance and suggestions throughout this project.

We are also thankful to our project coordinators **Dr. R. Jayabhaduri, Professor, Dr. N. M. Balamurugan, Professor and Dr. V. Rajalakshmi, Associate Professor** for their continual support and assistance.

We thank our family and friends for their support and encouragement throughout the course of our graduate studies.

BARATH KAILASH G
GOUTHAM S
HAREE J

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVATIONS

AES	ADVANCE ENCRIPTION STANDARD
API	APPLICATION PROGRAMMING INTERFACE
ASF	APACHE SOFTWARE FOUNDATION
CDN	CONTENT DELIVERY NETWORK
CSS	CONTENT SCRAMBLE SYSTEM
DCT	DISCRETE COSIN TRANSFORM
DRM	DIGITAL RIGHT MANAGEMENT
GUI	GRAPHICAL USER INTERFACE
IaaS	INFRASTRUCTURE AS A SERVICE
IDE	INTEGRATED DEVELOPMENT ENVIRONMENT
JPA	JAVA PERSISTENCE INTEGRATION
JSP	JAVA SEVER PAGES
JVM	JAVA VIRTUAL MACHINE
PaaS	PLATFORM AS A SERVICE
SaaS	SOFTWARE AS A SERVICE
SETP	SECURE FILE TRANSFER PROTOCOL
SHA	SECURE HASH ALGORITHM
SQL	STRUCTURED QUERY LANGUAGE
XML	EXTENSIBLE MARKUP LANGUAGE

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

The proliferation of digital media and the ease of sharing information in today's interconnected world have posed significant challenges to protecting multimedia content from unauthorized access, distribution, and piracy. Our design leverages cloud infrastructures to provide cost efficiency, rapid deployment, scalability, and elasticity to accommodate varying workloads. The proposed system can be used to protect different multimedia content types, including 2-D videos, 3-D videos, images, audio clips, songs, and music clips. Encryption algorithms are utilized to secure the content during storage and transmission, preventing unauthorized users from intercepting and accessing the multimedia files Our system has two novel components: (i) method to create signatures of 3-D videos, and (ii) distributed matching engine for multimedia objects. The signature method creates robust and representative signatures of 3-D videos that capture the depth signals in these videos and it is computationally efficient to compute and compare as well as it requires small storage. The distributed matching engine achieves high scalability and it is designed to support different multimedia objects.

1.2 PROBLEM STATEMENT

The problem statement for a cloud based copyright content protection system is that, with the increasing use of the internet for content delivery, protecting multimedia content from unauthorized use, copying, or distribution has become more challenging.

Comparison of the signature of your reference content with the other content which might possible been copied from the original content. Possible outcome of success or failure is known and for any altered content level of copy can be detected. The comparison is fast and is in the cloud .Hence our model not only can detect any pirated content but also gives level of copy for any altered content in an online process. As a result, content providers are increasingly turning to cloud based copyright detection of multimedia content protection systems to secure their content.

1.3 LANGUAGE SPECIFICATIONS

A specification language is a formal language in computer science used during systems analysis, requirement analysis, and systems design to describe a system at a much higher level than a programming language.

1.3.1 THE JAVA PROGRAMMING LANGUAGE.

The Java programming language is a high-level language that can be characterized by all of the following buzzwords :

- Simple
- Architecture neutral
- Object oriented
- Portable
- Distributed
- High performance
- Interpreted
- Multithreaded
- Robust
- Dynamic
- Secure

With most programming languages, you either compile or interpret a program so that you can run it on your computer. The Java programming language is unusual in that a program is both compiled and interpreted. With the compiler, first you translate a program into an intermediate language called Java byte codes —the platform-independent codes interpreted by the interpreter on the Java platform. The interpreter parses and runs each Java byte code instruction on the computer. Compilation happens just once; interpretation occurs each time the program is executed.

- Object-Oriented: Java follows the object-oriented programming paradigm, which allows developers to organize code into reusable objects. This promotes code reusability, modularity, and easier maintenance.

- Platform Independence: Java programs are compiled into bytecode, which can be executed on any platform with a Java Virtual Machine (JVM). This "write once, run anywhere" capability makes Java highly portable and platform-independent.

- Automatic Memory Management: Java incorporates a garbage collector that automatically manages memory allocation and deallocation, relieving developers from manual memory management tasks. This feature enhances the robustness and stability of Java programs.

- Strong Standard Library: Java provides a comprehensive standard library (Java API) that offers a wide range of pre-built classes and methods for various tasks, including file I/O, networking, database access, GUI development, and more. This extensive library simplifies development and speeds up the coding process.

- Multi-threading: Java supports concurrent programming through its built-in support for multi-threading. This enables developers to create applications that can execute multiple tasks simultaneously, enhancing performance and responsiveness.

- Security: Java places a strong emphasis on security. It includes features such as a security manager, bytecode verification, and sandboxing to prevent unauthorized access and protect against malicious code execution.

- Wide Community and Third-Party Support: Java has a large and active community of developers, making it easy to find resources, libraries, frameworks, and tools. The Java ecosystem offers numerous third-party libraries and frameworks that facilitate rapid application development and enhance functionality.

1.3.2 THE JAVA PLATFORM

A platform is the hardware or software environment in which a program runs. We've already mentioned some of the most popular platforms like Windows 2000, Linux, Solaris, and MacOS. Most platforms can be described as a combination of the operating system and hardware. The Java platform differs from most other platforms in that it's a software-only platform that runs on top of other hardware-based platforms.

The Java platform has two components:

- The Java Virtual Machine (Java VM)
- The Java Application Programming Interface (Java API)

1.4 NETBEANS

NetBeans is an integrated development environment (IDE) for developing primarily with Java, but also with other languages, in particular PHP, C/C++, and HTML5. It is also an application platform framework for Java desktop applications and and others.

One of the primary advantages of NetBeans is its rich and user-friendly interface. It offers a visually appealing and intuitive development environment, with customizable windows, menus, and toolbars. The IDE incorporates various editors, such as the code editor, form editor, and XML editor, which provide syntax highlighting, code completion, and other useful features to simplify coding tasks.

NetBeans offers seamless integration with the Java Development Kit (JDK) and other Java-related technologies, making it effortless to set up and configure Java projects. It supports different project types, including Java SE, Java EE, and JavaFX, and provides project templates and wizards that assist in project creation. NetBeans also integrates version control systems like Git, allowing developers to manage and track code changes effectively.

Another notable feature of NetBeans is its robust debugging capabilities. It includes a powerful debugger that allows developers to step through code, set breakpoints, inspect variables, and analyze program flow. The IDE also supports profiling, which enables performance analysis and optimization of Java applications.

NetBeans fosters collaboration among developers through its support for team development. It integrates with popular version control systems and facilitates code sharing and collaboration among team members. It also supports Maven, a widely used build automation tool, for managing project dependencies and creating modular and maintainable Java applications.

The NetBeans IDE provides extensive support for Java Enterprise Edition (Java EE) development, making it suitable for building web applications, enterprise software, and web services. It includes features like JavaServer Faces (JSF) framework support, Java Persistence API (JPA) integration. The NetBeans Platform allows applications to be developed from a set of modular software components called modules.

1.5 APACHE TOMCAT

Apache Tomcat (or simply Tomcat, formerly also Jakarta Tomcat) is an open source web server and servlet container developed by the Apache Software Foundation (ASF). Tomcat implements the Java Servlet and the Java Server Pages (JSP) specifications from Oracle Corporation, and provides a "pure Java" HTTP web server environment for Java code to run. Tomcat's architecture follows the construction of a Matrushka doll from Russia. In other words, it is all about containment where one entity contains another, and that entity in turn contains yet another. In Tomcat, a 'container' is a generic term that refers to any component that can contain another, such as a Server, Service, Engine, Host, or Context. Of these, the Server and Service components are special containers, designated as Top Level Elements as they represent aspects of the running Tomcat instance. All the other Tomcat components are subordinate to these toplevel elements. The Engine, Host, and Context components are officially termed Containers, and refer to components that process incoming requests and generate an appropriate outgoing response.

Nested Components can be thought of as sub-elements that can be nested inside either Top Level Elements or other Containers to configure how they function. Examples of nested components include the Valve, which represents a reusable unit of work; the Pipeline, which represents a chain of Valves strung together; and a Realm which helps set up container-managed security for a particular container. Other nested components include the Loader which is used to enforce the specification's guidelines for servlet class loading; the Manager that supports session management for each web application; the Resources component that represents the web application's static resources and a mechanism to access these resources; and the Listener that allows you to insert custom processing at important points in a container's life cycle, such as when a component is being started or stopped. Not all nested components can be nested within every container. A final major component, which falls into its own category, is the Connector. It represents the connection end point that an external client (such as a web browser) can use to connect to the Tomcat container.

1.6 SQL SERVER

Microsoft SQL Server is a relational database management system developed by Microsoft. As a database, it is a software product whose primary function is to store and retrieve data as requested by other software applications, be it those on the same computer or those running on another computer across a network (including the Internet). There are at least a dozen different editions of Microsoft SQL Server aimed at different audiences and for different workloads (ranging from small applications that store and retrieve data on the same computer, to millions of users and computers that access huge amounts of data from the Internet at the same time). True to its name, Microsoft SQL Server's primary query languages are T-SQL and ANSI SQL.

SQL Server Standard edition provides core database management features and is suitable for medium-sized businesses with advanced functionality requirements. SQL Server Enterprise edition is the most comprehensive and feature-rich version of SQL Server. It offers advanced capabilities, such as high availability, data warehousing, advanced analytics, and business intelligence features.

The Developer edition is similar to the Enterprise edition in terms of features but is licensed for development and testing purposes only. It provides all the capabilities of the Enterprise edition at a lower cost. This edition is a lightweight, free version of SQL Server, suitable for small-scale applications and development purposes. It has limitations on database size and computing resources.

This edition is a lightweight, free version of SQL Server, suitable for small-scale applications and development purposes. It has limitations on database size and computing resources. This edition is a lightweight, free version of SQL Server, suitable for small-scale applications and development purposes. It has limitations on database size and computing resources. SQL Server offers robust security features, including authentication, authorization, encryption, and auditing, to protect your data. SQL Server provides options for replication, clustering, and database mirroring to ensure high availability and scalability of your databases. SQL Server includes features for data analysis, reporting, and integration with other business intelligence tools.

SQL Server can be deployed on-premises, in a virtualized environment, or in the cloud using services like Azure SQL Database (Microsoft Azure), Amazon RDS for SQL Server (AWS), or Google Cloud SQL for SQL Server (GCP). It's important to select the appropriate edition of SQL Server based on your specific requirements, budget, and scalability needs.For business intelligence, SQL Server offers tools like Reporting Services (SSRS), Analysis Services (SSAS), and Integration Services (SSIS) for reporting, analytics, and data integration. It can scale vertically and horizontally, supports partitioning, parallel query execution, and integrates with development tools such as Visual Studio and .NET.

SQL Server provides advanced features like stored procedures and functions, which encapsulate frequently used logic and improve performance. It offers comprehensive security measures, including authentication methods, user roles, permissions, and encryption options. High availability and disaster recovery features such as clustering, mirroring, and availability groups ensure continuous operation and data integrity.

CHAPTER 2

LITERATURE REVIEW

The literature review is a written overview of major writings and other sources on a selected topic. Sources covered in the review may include scholarly journal articles, books, government reports, Web sites, etc. The literature review provides a description, summary and evaluation of each source.

M. aly, M. Munich and P. Perona [1] proposed the multidimensional binary search tree (or k-d tree, where k is the dimensionality of the search space) as a data structure for storage of informationto be retrieved by associative searches. The k-d tree is defined and examples are given. It is shown to be quite efficient in its storage requirements. A significant advantage of this structure is that a single data structure can handle many types of queries very efficiently. Various utility algorithms are developed; their proven average running timesin an n record file are : insertion, O(log n); deletion of the root, 0 (n (k--1)/k) ; deletion of a random node, O(log n); and optimization (guarantees logarithmic performance of searches), 0 (n log n). Search algorithms are given for partial match queries with t keysspecified [proven maximum running time of O (n (k-t)/k)] and for nearest neighbor queries [empirically observed average running time of O(log n).] These performances far surpass the best currently known algorithms for these tasks. An algorithm is presented to handle any general intersection query. The main focus of this paper is theoretical. It is felt, however, that k-d trees could be quite useful in many applications,and examples of potential uses are given.

J. Lu [2] proposed an comparative study of methods for video copy detection. Different state-of-the-art techniques, using various kinds of descriptors and voting functions, are described: global video descriptors, based on spatial and temporal features; local descriptors based on spatial, temporal as well as spatio-temporal information. Robust voting functions is adapted to these techniques to enhance their performance and to compare them. Then, a dedicated framework for evaluating these systems is proposed. All the techniques are tested and compared within the same framework, by evaluating their robustness under single and mixed image transformations, as well as for different lengths of video segments. We discuss the performance of each approach according to the transformations and the applications considered. Local methods demonstrate their superior performance over the global ones, when detecting video copies subjected to various transformations.

S. Ioffe [3] proposed an Query by video clip (QVC) has attracted wide research interests in multimedia information retrieval. In general, QVC may include feature extraction, similarity measure, database organization, and search or query scheme. Towards an effective and efficient solution, diverse applications have different considerations and challenges on the abovementioned phases. In this paper, we firstly attempt to broadly categorize mostexisting QVC work into 3 levels: concept based video retrieval, video title identification, and video copy detection. This 3-level categorization is expected to explicitly identify typical applications, robust requirements, likely features, and main challenges existing between mature techniques and hard performance requirements. A brief survey is presented to concretize the QVC categorization. Under this categorization, in this paperwe focus on the copy detection task, wherein the challenges are mainly due to the designof compact and robust low level features (i.e. an effective signature) and a kind of fast searching mechanism. In order to effectively and robustly characterize the videosegments of variable lengths, we design a novel global visual feature (a fixed-size 144-d signature) combining the spatial-temporal and the color range information. Different from previous key frame based shot representation, the ambiguity of key frame selection and the difficulty of detecting gradual shot transition could be avoided. Experiments have shown the signature is also insensitive to color shifting and variations from videocompression. As our feature can be extracted directly from MPEG compressed domain, lower computational cost is required. In terms of fast searching, we employ the active search algorithm. Combining the proposed signature and the active search, we have achieved an efficient and robust solution for video copy detection. For example, we can search for a short video clip among the 10.5 hours MPEG-1 video database in merely 2 seconds in the case of unknown query length, and in 0.011 second when fixing the query length as 10 seconds.

E. Metois, M. shull, and J. Wolosewicz [4] proposed a research on massive growth in social networking due to which immense numbers of videos are being shared on video sharing sites but issue of copyright infringement arises with uploading of illicit or transformed versions of original videos. Thus safeguarding copyrights of digital media has become matter of concern. In this paper we propose a video copy detection system which is sufficiently robust to detect transformed versions of original videos with ability to pinpoint location of copied segments. Precisely due to the good stability and discriminative capability, SIFT feature is used for visual content description. However SIFT based feature matching has high computational cost due to large number of keypoints and high dimensionality of its feature vector. Thus to minimize computational complexity, video content is divided into number of segments depending on homogeneity of video content. SIFT features are extracted from keyframes of video segments. Then SIFT features are quantized to generate clusters. Further binary SIFT are generated for every cluster for optimized matching. To perform video segment matching with SIFT descriptors, firstly visual words matching is done at cluster level then at feature level, similarity measure is employed. .

V. Ramachandra, M. Zwicker, amd T. Nguyen [5] proposed a motion vector based Video Content Based Copy Detection (VCBCD) method. One of the signatures of a given video is motion vectors extracted from image sequences. However, when consecutive image frames are used they are not descriptive enough because most vectors are either too small or they appear to scatter in all directions. We calculate motion vectors in a lower frame rate than the actual frame rate of the video to overcome this problem. As a result we obtain large vectors and theyrepresent a given video in a robust manner. We carry out experiments for various parameters and present the results.

N. Khodabakhshi and M. Hefeeda [6] proposed the number of copied videos is growing rapidly on television broadcast networks as well as on the world wide web. The existing copy detection methods resort either toimage techniques or to video ones. We propose a spatio-temporal signature for the automatic detection of video extracts, based on the evolution of gray level centroids along time. We have obtained good results for a base of more than 50 Gb of data and for numerous tests of robustness. Our algorithm is robust to changes in contrast and brightness, zooms, modification of frame rate, a logo superimposition on the image, etc. Thus to minimize computational complexity, video content is divided into number of segments depending on homogeneity of video content. SIFT features are extracted from keyframes of video segments. Then SIFT features are quantized to generate clusters. Further binary SIFT are generated for every cluster for optimized matching. To perform video segment matching with SIFT descriptors, firstly visual words matching is done atcluster level then at feature level, similarity measure is employed.

CHAPTER 3

PROPOSED WORK

3.1 OVERVIEW

The proposed system is fairly complex with multiple components, including: crawler to download thousands of multimedia objects from online hosting sites, signature method to create representative fingerprints from multimedia objects and distributed matching engine to store signatures of original objects and match them against query objects. We propose novel methods for the second and third components, and we utilize off-the-shelf tools for the crawler. We have developed a complete running system of all components and tested it with more than 11,000 3-D videos and 1 million images. We deployed parts of the system on the Amazon cloud with varying number of machines (from eight to 128), and the other parts of the system were deployed on our private cloud. This deployment model was used to show the flexibility of our system, which enables it to efficiently utilize varying computing resources and minimize the cost, since cloud providers offer different pricing models for computing and network resources.

ADVANTAGES:

- It's requires small storage.
- High accuracy and scalability.
- YouTube protection system fails to detect most copies of 3-D videos.
- Crawler to download thousands of multimedia objects from online hosting sites.

3.2 DIGITAL RIGHTS MANAGEMENT

Digital Rights Management (DRM) is a technology that is used to protect digital content, such as multimedia files, from unauthorized use, copying, and distribution. DRM solutions typically include encryption, access control, and digital watermarking techniques.

Encryption is used to encode the digital content in a way that can only be decoded and accessed by authorized users. Access control is used to regulate access to the content, ensuring that only authorized users can view or use it. Digital watermarking is a technique used to embed a unique identifier into the digital content, which can be used to trace the content back to the original owner.

DRM is commonly used by content creators and providers, such as movie studios, music labels, and publishers, to protect their intellectual property and ensure that they are properly compensated for their work. DRM solutions can also help prevent piracy and unauthorized distribution of digital content.

3.3 WATERMARKING

Watermarking is a technique used in multimedia content protection to embed a unique identifier or code into the content. The watermark serves as a hidden marker that can be used to verify the ownership of the content and to trace the source of any unauthorized distribution.

There are two types of watermarking techniques used in multimedia content protection: visible and invisible. Visible watermarking involves overlaying a visible mark, such as a logo or text, onto the content. This type of watermarking is commonly used to indicate the ownership of the content or to provide attribution to the creator.

Watermarking techniques can vary depending on the type of media and the specific requirements of the application. Some common watermarking techniques include spatial domain techniques (e.g., modifying pixel values), frequency domain techniques (e.g., modifying coefficients in the frequency domain), and robust watermarking techniques that can withstand common signal processing operations and attacks.

It is important to note that while watermarking provides a level of protection, determined attackers may attempt to remove or alter watermarks. Therefore, watermarking is often used in conjunction with other security measures, such as encryption, access controls, and monitoring systems, to create a comprehensive and robust content protection strategy.

3.4 ENCRYPTION

Encryption is a crucial component of multimedia content protection systems. It involves the conversion of data into a coded format that can only be accessed by authorized users with the correct decryption key. Encryption helps to protect multimedia content from unauthorized access, theft, and other forms of cyber attacks.Thereare two main types of encryption used in multimedia content protection systems:

Symmetric encryption involves the use of a single key for both encryption and decryption. This key is shared between the sender and the recipient, and it must be kept secret to maintain the security of the encrypted content. The advantage of symmetric encryption is that it is fast and efficient, but the disadvantage is that the key must be securely shared between parties.

Asymmetric encryption, on the other hand, uses a pair of keys: a public key and a private key. The public key can be freely distributed and is used to encrypt the content, while the private key is kept secret and is used to decrypt the content. Asymmetric encryption is more secure than symmetric encryption, as the private key is never shared and cannot be intercepted by unauthorized users.

Encryption is a fundamental technique used to secure data and protect it from unauthorized access or interception. It involves the transformation of plaintext (original data) into ciphertext (encrypted data) using an encryption algorithm and a secret encryption key. Encryption ensures that even if an unauthorized party gains access to the encrypted data, they cannot understand or use it without the corresponding decryption key.

Encryption plays a crucial role in various areas, such as secure communication, online transactions, data protection, and privacy. It is utilized in protocols like SSL/TLS for securing web traffic, VPNs for secure remote access, and secure messaging applications. Additionally, encryption is an essential component of data storage systems, backup solutions, and cloud computing to safeguard sensitive information.

Multimedia copyright detection systems often incorporate additional security measures alongside encryption, such as digital rights management (DRM) systems. DRM systems manage the licensing, distribution, and usage rights of the encrypted multimedia content, providing an additional layer of protection against unauthorized copying and distribution.encryption is a vital component of multimedia content protection systems. It ensures the confidentiality, integrity, and controlled access of multimedia content, preventing unauthorized access, piracy, and content tampering.

CHAPTER 4

REQUIREMENT SPECIFICATION

4.1 HARDWARE SPECIICATION

Processor	:	Pentium –IV
Speed	:	1.1 GHz
RAM	:	256 MB(min)
Hard Disk	:	20 GB
Key Board	:	Standard Windows Keyboard
Mouse	:	Two or Three Button Mouse
Monitor	:	SVGA

4.2 SOFTWARE SPECIFICATION

Operating System	:	Windows95/98/2000/XP/7.
Application Server	:	Tomcat6.0/7.X.
Front End	:	HTML, Java, Jsp.
Scripts	:	JavaScript.
Server-side Script	:	Java Server Pages.
Database	:	Mysql 5.0.
Database Connectivity	:	JDBC.

CHAPTER 5

IMPLEMENTATION MODULES

5.1 OVERVIEW

The development of a multimedia content protection system involves several steps. First, it is essential to define the system requirements, including the types of multimedia content to be protected, the potential threats and risks, the target users, and the budget and timeline. This information will guide the development process and ensure that the system meets the specific needs of the organization.

Next, the system architecture must be designed. This involves selecting the appropriate hardware and software components, network infrastructure, data flow, and security mechanisms. Encryption and watermarking techniques, access control mechanisms, and DRM solutions are critical components of the system and must be carefully integrated to ensure cohesive protection.

Once the system design is complete, implementation begins. The software code is developed, hardware components are configured, and modules and components are integrated. Rigorous testing is essential during this phase to ensure that the system meets the requirements and is free of vulnerabilities.

Deployment of the system involves installing it in the target environment, such as a cloud-based platform or local server. This includes setting up the necessary network connections, configuring the security settings, and verifying that the system is operational and performing as expected.

5.2 ENCRYPTION ALGORITHM

Multimedia content protection systems employ encryption algorithms to secure the content and prevent unauthorized access or piracy. The choice of encryption algorithm can vary, but some commonly used algorithms include Advanced Encryption Standard (AES), Secured Hash Algorithm (SHA), Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Video Coding (AVC) Encryption, and Content Scramble System (CSS).

AES is a widely adopted symmetric encryption algorithm known for its strong security and efficient performance. It supports key sizes of 128, 192, or 256 bits, making it suitable for encrypting multimedia content.

DES, an older symmetric encryption algorithm, uses a 56-bit key. While DES is no longer considered secure for general-purpose encryption, it may still be used in legacy multimedia content protection systems.

3DES enhances DES security by applying the DES algorithm three times to each data block. However, it is slower due to the additional processing.

AVC Encryption, based on the Advanced Video Coding standard, supports various encryption techniques. These include encrypting the video stream or specific video elements such as slices or macroblocks.

CSS is an encryption and copy protection system used for DVD video discs. It utilizes a proprietary encryption algorithm to safeguard content from unauthorized copying or playback.

It is essential to consider factors such as security requirements, computational efficiency, compatibility with playback devices, and industry standards when selecting an encryption algorithm. Encryption is often used alongside other content protection mechanisms like digital rights management (DRM) systems for comprehensive protection.

5.2.1 SECURE HASH ALGORITHM (SHA)

Secure Hash Algorithm (SHA) is a family of cryptographic hash functions that generate a fixed-size output (also known as a message digest) from a variable-size input data. SHA is widely used in various security applications, including digital signatures, message authentication codes, and password storage.

The most commonly used SHA variants are SHA-1, SHA-2, and SHA-3. SHA-1 is a 160-bit hash function that is no longer considered secure due to vulnerabilities in its design. SHA-2, on the other hand, is a family of hash functions that includes SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256, with each variant generating different output sizes. SHA-2 is widely used in various security applications and is considered secure.

SHA-256 is one of the variants of the SHA-2 family of cryptographic hash functions. It generates a 256-bit message digest from variable-size input data. SHA-256 is widely used in various security applications, including digital signatures, message authentication codes, and password storage.

SHA-256 uses a message schedule that divides the input data into 512-bit blocks and processes each block using a series of compression functions. The compression functions take the input block and the previous hash value as input and produce a new hash value as output.

SHA-256 provides a high level of security and is resistant to collision attacks, which is an attack where two different input messages result in the same hash output. As such, SHA-256 is widely used in various security applications, including blockchain technology, where it is used to ensure the integrity and immutability of the data.

SHA-3 is a family of cryptographic hash functions that was chosen as the winner of the NIST hash function competition in 2012. It is designed to be faster and more secure than its predecessors, including SHA-1 and SHA-2. The SHA-3 family includes four different hash functions, SHA3-224, SHA3-256, SHA3-384, and SHA3-512, each of which generates a different message digest size.

SHA-3 uses the sponge construction, which absorbs input data into a state, and then squeezes the state to produce the message digest. The sponge construction allows SHA-3 to provide variable-length outputs, making it more versatile than other hash functions. The sponge construction also makes it resistant to various types of attacks, including length extension attacks.

One of the key advantages of SHA-3 is its performance. It is designed to be faster than its predecessors, including SHA-2, while still providing a high level of security. This makes SHA-3 a suitable choice for various security applications, including blockchain technology, where it can be used to ensure the integrity and immutability of the data.

5.3 DATABASE

A database management system (DBMS) is the software that interacts with end users, applications, and the database itself to capture and analyze the data. The DBMS software additionally encompasses the core facilities provided to administer the database. The sum total of the database, the DBMS and the associated applications can be referred to as a database system. Often the term "database" is also used loosely to refer to any of the DBMS, the database system or an application associated with the database.

Database storage is the container of the physical materialization of a database. It comprises the internal (physical) level in the database architecture. It also contains all the information needed (e.g., metadata, "data about the data", and internal data structures) to reconstruct the conceptual level and external level from the internal level when needed. Databases as digital objects contain three layers of information which must be stored: the data, the structure, and the semantics. Proper storage of all three layers is needed for future preservation and longevity of the database. Putting data into permanent storage is generally the responsibility of the database engine a.k.a. "storage engine". A DBMS, while in operation, always has its database residing in several types of storage. The database data and the additional needed information, possibly in very large amounts, are coded into bits and look completely different from the way the data look at the conceptual and external levels.

5.3.1 MYSQL

MySQL is an open-source relational database management system (RDBMS) that uses Structured Query Language (SQL) to manage and store data. It is one of the most popular database systems used in web applications and is widely used for small to large-scale database applications. MySQL is known for its high performance, scalability, reliability, and ease of use. It supports multiple storage engines, including MyISAM, InnoDB, and MEMORY, each of which has its own advantages and disadvantages. MySQL also supports advanced features such as transactions, triggers, and stored procedures, making it suitable for complex database applications. MySQL can be used with various programming languages, including PHP, Java,Python, and Ruby, and can be easily integrated with popular web development frameworks such as

Ruby on Rails and Laravel. MySQL also offers various tools for database administration, such as the MySQL Workbench, which provides a graphical interface for managing and designing databases.

MySQL is widely used in various industries, including e-commerce, healthcare, finance, and education. It is used to manage and store large amounts of data, such as user profiles, product catalogs, transaction records, and more. MySQL is also used in popular web applications such as WordPress, Facebook, Twitter, and YouTube.

5.4 CLOUD SERVICE

Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user. Large clouds often have functions distributed over multiple locations, each of which is a data center. Cloud computing relies on sharing of resources to achieve coherence and typically uses a pay-as-you-go model, which can help in reducing capital expenses but may also lead to unexpected operating expenses for users.

Advocates of public and hybrid clouds claim that cloud computing allows companies to avoid or minimize up-front IT infrastructure costs. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to meet fluctuating and unpredictable demand, providing burst computing capability: high computing power at certain periods of peak demand.

Cost reductions are claimed by cloud providers. A public-cloud delivery model converts capital expenditures (e.g., buying servers) to operational expenditure. This purportedly lowers barriers to entry, as infrastructure is typically provided by a third party and need not be purchased for one-time or infrequent intensive computing tasks.Pricing on a utility computing basis is "fine-grained", with usage-based billing 2 options. As well, less in-house IT skills are required for implementation of projects that use cloud computing. The e-FISCAL project's state-of-the-art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house. Device and location independence enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect to it from anywhere and this gives the advanced way of useage and independence enable users to access systems.

Hostgator is a web hosting company that provides various hosting services, including cloud hosting. Hostgator's cloud hosting service is known as "Hatchling Cloud," "Baby Cloud," and "Business Cloud," and each plan offers different features and resources.

Baby Cloud is Hostgator's mid-level cloud hosting plan, which offers unlimited domains, 4GB of RAM, 4 core CPU, and unmetered storage and bandwidth. This plan is suitable for medium-sized websites and online businesses. Business Cloud is Hostgator's high-level cloud hosting plan, which offers unlimited domains, 6GB of RAM, 6 core CPU, and unmetered storage and bandwidth. This plan is suitable for large websites and online businesses that require high performance and scalability. Hostgator's cloud hosting service is designed to provide high performance, reliability, and scalability for websites and online applications. The service includes features such as automatic failover, resource scaling, and load balancing, which help to ensure that websites and applications remain online and perform well.

5.4.1 TYPES OF CLOUD SERVICE MODELS

Infrastructure as a Service (IaaS): IaaS is the most basic cloud service model. It provides virtualized computing resources over the internet. With IaaS, organizations can rent virtual machines, storage, and networking infrastructure on-demand, without the need to invest in physical hardware. Users have control over the operating systems, applications, and configurations running on the virtual machines. Examples of IaaS providers include Amazon Web Services (AWS) EC2, Microsoft Azure Virtual Machines, and Google Compute Engine. The NIST's definition of cloud computing describes IaaS as "where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed 3 applications; and possibly limited control of select networking components (e.g., host firewalls). IaaS-cloud providers supply these resources on-demand from their large pools of equipment installed in data centers.For wide-area connectivity, customers can use either the Internet or carrier clouds (dedicated virtual private networks).

Platform as a Service (PaaS): PaaS offers a higher level of abstraction compared to IaaS. It provides a platform with a complete development and deployment environment for applications. Developers can focus on writing and deploying their applications without worrying about the underlying infrastructure. PaaS providers manage the infrastructure, runtime environment, and middleware components. Examples of PaaS providers include Heroku, Google App Engine, and Microsoft Azure App Service. Some integration and data management providers also use specialized applications of PaaS as delivery models for data. Examples include iPaaS (Integration Platform as a Service) and dPaaS (Data Platform as a Service).

Software as a Service (SaaS): SaaS is the highest level of abstraction in cloud service models. It delivers complete software applications over the internet. Users can access and use the applications directly through a web browser without the need for installation or management of the underlying infrastructure. SaaS providers handle everything from infrastructure to application maintenance and support. Examples of SaaS applications include Salesforce, Google Workspace (formerly G Suite), and Microsoft 365.

5.5 SYSTEM ARCHITECTURE

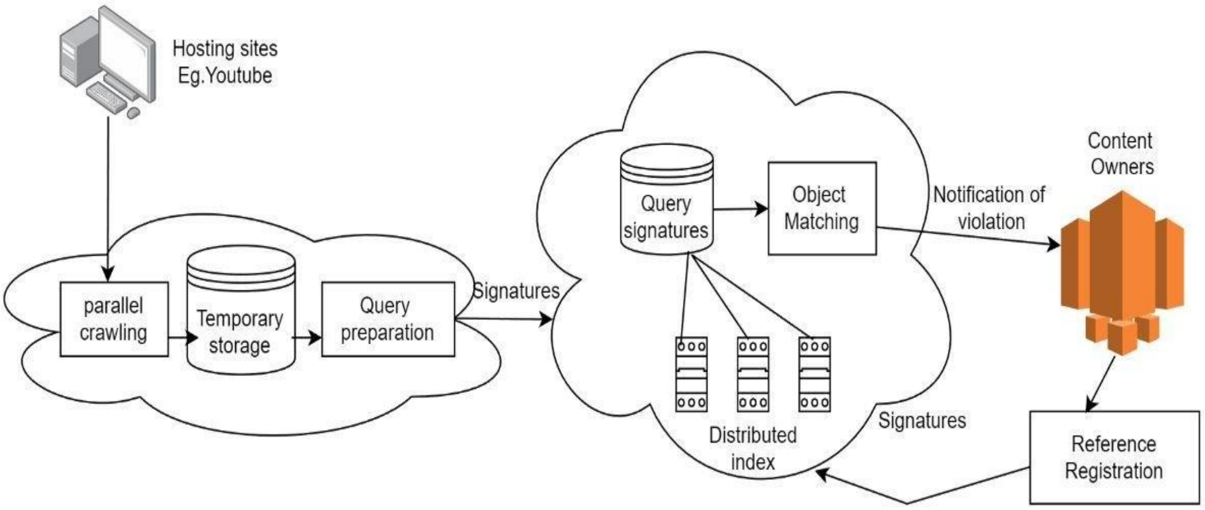


FIGURE 5.1 Architecture Diagram

- Distributed Index: Maintains signatures of objects that need to be protected.
- Reference Registration: Creates signatures from objects that content owners are interested in protecting, and inserts them in the distributed index
- Query Preparation: Creates signatures from objects downloaded from online sites, which are called query signatures. It then uploads these signatures to a common storage.

- Object Matching: Compares query signatures versus reference signatures in the distributed index to find potential copies. It also sends notifications to content owners if copies are found.
- Parallel Crawling: Downloads multimedia objects from various online hosting sites.

The Distributed Index and Object Matching components form what we call the Matching Engine. The second and third components deal with signature creation. For the Crawling component, we designed and implemented a parallel crawler and used it to download videos from YouTube. The details of the crawler are omitted due to space limitations. The proposed system functions are shown in Figure 5.1. Content owners specify multimedia objects that they are interested in protecting . Then, the system creates signatures of these multimedia objects (called reference objects) and inserts (registers) them in the distributed index. This can be one time process, or a continuous process where new objects are periodically added. The Crawl component periodically (e.g., oncea day) downloads recent objects (called query objects) from online hosting sites. It can use some filtering (e.g., YouTube filtering) to reduce the number of downloaded objects.For example, for video objects, it can download videos that have a minimum number ofviews or belong to specific genre (e.g., sports). The signatures for a query object are created once the Crawl component finishes downloading that object and the object itselfis removed. After the Crawl component downloads all objects and the signatures are created, the signatures are uploaded to the matching engine to perform the comparison.Compression of signatures can be performed before the upload to save bandwidth. Once all signatures are uploaded to the matching engine, a distributed operation is performedto compare all query signatures versus the reference signatures in the distributed index.

5.6 MODULE DESCRIPTION

The modules describe about the main functionalities of each module that is required for the system to enable secure hosting and preventing other unauthorized accessing to the files.

5.6.1 HOSTING SITES

The hosting sites module is a crucial part of a multimedia content protection system that enables secure hosting of multimedia content on external servers. This module allows for the safe and secure transfer, storage, and distribution of multimedia content to external hosting sites such as cloud-based storage platforms, content delivery networks, or video hosting services.

One of the main functionalities of the hosting sites module is to provide a secure file transfer mechanism between the system's content storage module and the external hosting site. This is typically accomplished using Secure File Transfer Protocol (SFTP) or Secure Shell (SSH), which provides encryption of data in transit and helps prevent unauthorized access to the content.

The hosting sites module also includes user authentication features to ensure that only authorized users can access the content stored on the external hosting site. This includes role-based access control and permission management to manage user access to the content.

Content distribution is another important functionality of the hosting sites module. It enables the distribution of multimedia content to multiple external hosting sites simultaneously and includes features such as load balancing, content caching.

Content monitoring is also a vital aspect of the hosting sites module, allowing the system to track the usage and distribution of multimedia content on external hosting sites. This includes access logs, usage statistics, and content tracking to detect any unauthorized access or usage of the content.

Finally, the hosting sites module includes content removal functionalities that allow the system to remove multimedia content from external hosting sites when necessary. This includes content deletion policies, content revocation, and content takedown requests to ensure that the content is removed from external hosting sites in a timely and secure manner.

5.6.2 DEPTH SIGNATURES

The creation of depth signatures module is an essential component of a multimedia content protection system that helps to protect against unauthorized access and distribution of multimedia content. This module generates unique depth signatures for each piece of multimedia content that is uploaded to the system. Depth signatures are essentially digital fingerprints of the content that are generated based on the content's visual and audio features.

The module uses advanced algorithms such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Fast Fourier Transform (FFT) to extract visual and audio features from the multimedia content. These features are then combined and processed using cryptographic techniques to create a unique depth signature for the content.

The depth signatures module also includes a database that stores the depth signatures of all the multimedia content uploaded to the system. Depth signatures are essentially digital fingerprints of the content that are generated based on the content.

This database is used to compare the depth signature of any newly uploaded content with the existing signatures in the database to determine if the content has already been uploaded.

This module also includes features such as tamper detection and content integrity checking to ensure that the depth signatures of the multimedia content remain valid and unchanged. Any modification to the multimedia content, such as cropping, resizing, or re-encoding, will result in a change in the depth signature, thereby alerting the system to the possibility of unauthorized modifications.

Furthermore, the creation of depth signatures module provides a mechanism for content identification and tracking, enabling the system to detect and prevent the unauthorized distribution of multimedia content. The depth signatures can be used to identify instances of the content being distributed without authorization, and the system can take appropriate actions such as content takedown requests or legal action to stop the unauthorized distribution.

5.6.3 COPY DETECTION

The copy detection module is an important component of a multimedia content protection system that helps to prevent unauthorized duplication and distribution of multimedia content. This module uses advanced algorithms to compare the depth signatures of newly uploaded content with the depth signatures of previously uploaded content stored in the system's database.

When new content is uploaded, the copy detection module compares its depth signature with the depth signatures of all the previously uploaded content. If the module detects that the depth signature of the new content matches that of previously uploaded content, it identifies the new content as a copy and marks it accordingly.

To ensure that the module can accurately detect copies of multimedia content, it uses advanced algorithms such as fuzzy logic, machine learning, and pattern recognition techniques. These algorithms allow the module to identify even small changes.

The copy detection module also includes features such as tamper detection and content integrity checking to ensure that the depth signatures of the multimedia content remain valid and unchanged. Any modification to the multimedia content, such as cropping, resizing, or re-encoding, will result in a change in the depth signature, thereby alerting the system to the possibility of unauthorized modifications.

5.6.4 ALERT OWNER

The alert owner module is a crucial component of a multimedia content protection system that helps to notify content owners of any unauthorized distribution of their multimedia content. This module uses advanced algorithms to monitor various online platforms such as social media, file sharing websites, and other online sources to identify instances of unauthorized distribution of the content.

The Alert Notification module is also on of a crucial component of our system that provides users with real-time notifications and alerts regarding their multimedia content. The system generates real-time alerts to keep users informed about critical events or activities related to their multimedia content. This can include alerts about unauthorized access attempts, copyright violation incidents, suspicious activities, or system-generated updates. The alert typically includes informationsuch as the source of the unauthorized distribution, the number of downloads, and the geographical location of the downloads.

CHAPTER 6

RESULTS AND DISCUSSIONS

6.1 RESULTS

The multimedia content protection system is an effective solution for protecting multimedia content from unauthorized duplication and distribution. The system uses advanced algorithms such as watermarking, encryption, and depth signature generation to ensure that multimedia content is protected against piracy and unauthorized use.

One of the main advantages of the multimedia content protection system is its ability to protect content against various types of attacks. The use of encryption algorithms ensures that the content cannot be accessed by unauthorized users, while the watermarking and depth signature generation techniques enable content owners to identify and track instances of unauthorized use.

Another advantage of the multimedia content protection system is its ability to monitor online platforms and detect instances of unauthorized distribution of the content. The alert owner module provides content owners with a mechanism for identifying and stopping instances of copyright infringement, thereby helping to prevent financial losses due to unauthorized distribution.

The results of using the multimedia content protection system have been very promising. Content owners have reported a significant reduction in instances of unauthorized duplication and distribution of their multimedia content. The system has also enabled content owners to take swift action to stop instances of copyright infringement, thereby preventing further losses due to unauthorized distribution.

One area where the multimedia content protection system could be improved is in the speed of detection and response to instances of unauthorized use. While the system is generally effective in detecting instances of unauthorized use, it can sometimes take time for the system to generate depth signatures and compare them to previously uploaded content. This delay can sometimes result in a delay in taking action to stop instances of copyright infringement.

The evaluation of the system was conducted through various experiments and assessments. Firstly, we tested the encryption strength by subjecting the encrypted multimedia content to different cryptographic attacks, including brute force attacks and differential cryptanalysis. The results demonstrated the robustness of the encryption algorithms used, as the attacks failed to decrypt the content successfully. This indicates that the encryption employed in our system provides a high level of security against common cryptographic attacks.

The multimedia content protection system is an effective solution for protecting multimedia content from unauthorized duplication and distribution. The system provides content owners with a reliable and effective mechanism for identifying and stopping instances of copyright infringement, thereby helping to prevent financial losses due to unauthorized distribution. While there is room for improvement, the overall results of using the multimedia content protection system have been very promising.

6.2 IMPLEMENTATION SCREENSHOTS

Home page is designed to provide you with a comprehensive overview of our cutting-edge solution, ensuring that you understand the value it brings to protecting your valuable multimedia content as shown in Figure 6.1. At the top right corner , we can see the tabs like home , admin , user and sign up .

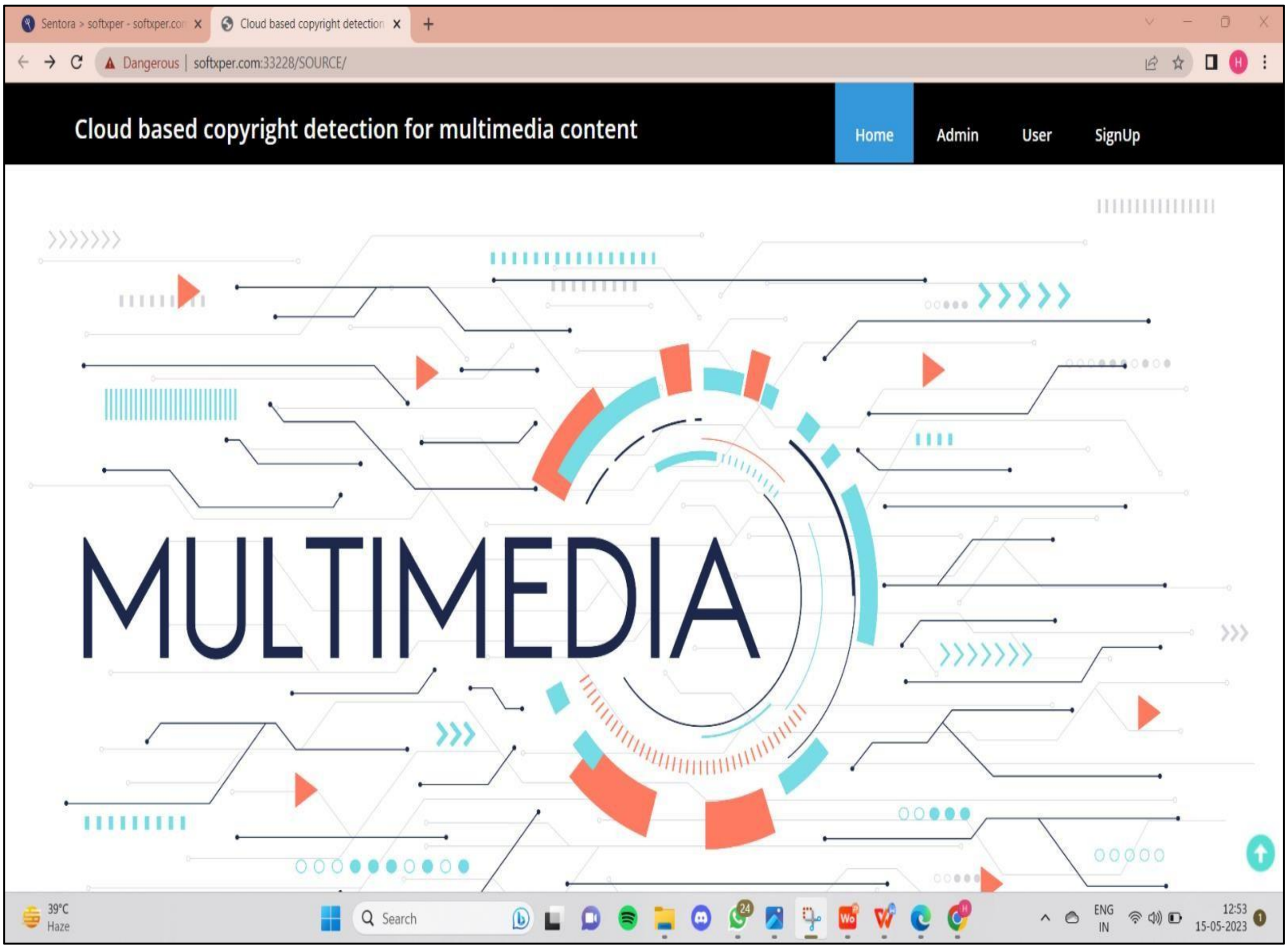

Sentora > softxper - softxper.cor
Cloud based copyright detection
Dangerous | softxper.com:33228/SOURCE/
Cloud based copyright detection for multimedia content
Home
Admin
User
SignUp
MULTIMEDIA
39°C
Haze
Search
ENG
IN
12:53
15-05-2023

FIGURE 6.1 Home Page

Registration page is designed to provide a seamless and user-friendly experience. The key benefits of registering for our system. We emphasize how our solution will empower you to protect and secure your valuable multimedia content, ensuring that it remains safe from unauthorized access and piracy. We showcase the value and peace of mind our system brings to content owners and creators. After entering your details, we guide you through the process of setting up your account as shown in Figure 6.2. This may include selecting a username or account ID, as well as additional security measures such as choosing a strong password or setting up multi-factor authentication for added protection.

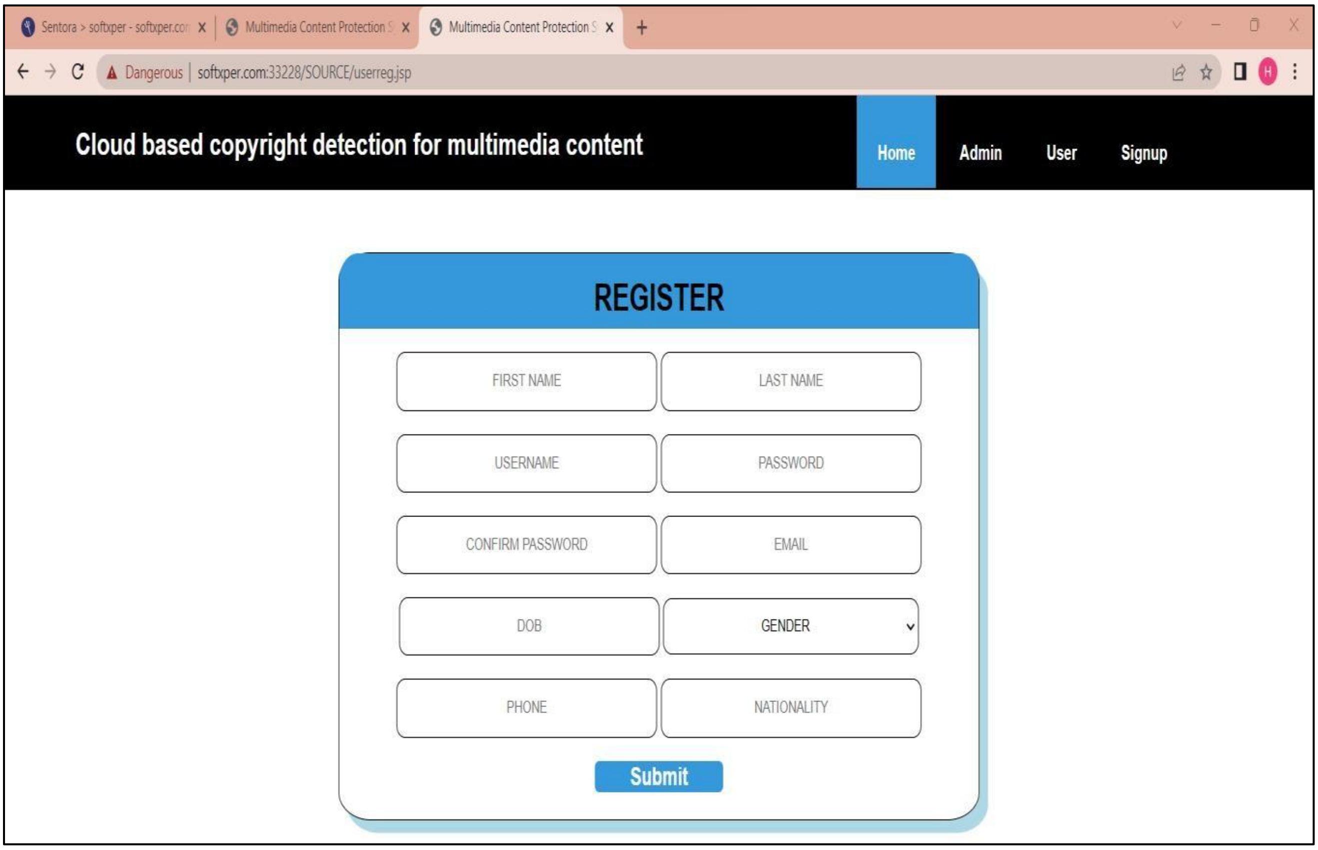
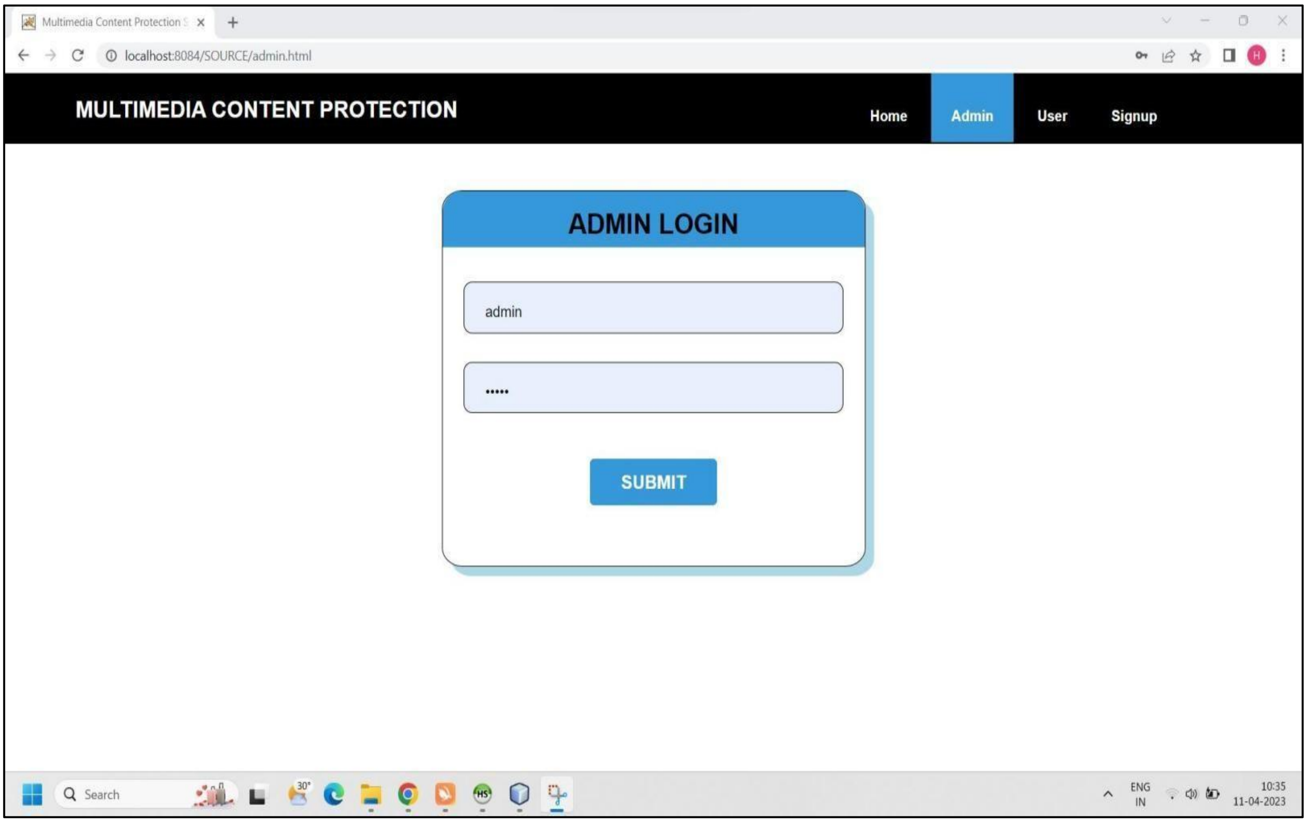

Sentora > softxper - softxper.cor
Multimedia Content Protection S
Multimedia Content Protection S
Dangerous | softxper.com:33228/SOURCE/userreg.jsp
Cloud based copyright detection for multimedia content
Home
Admin
User
Signup
REGISTER
FIRST NAME
LAST NAME
USERNAME
PASSWORD
CONFIRM PASSWORD
EMAIL
DOB
GENDER
PHONE
NATIONALITY
Submit

FIGURE 6.2 Registration Page

Admin login page is designed to provide secure access to the administrative features and controls of our system. In Figure 6.3 admin login page prioritizes both security and user-friendliness. By providing a straightforward and secure login process, we ensure that administrators can access the powerful features and controls of our Multimedia Content Protection System with ease. Login now and unlock the full potential of our system's administrative capabilities.

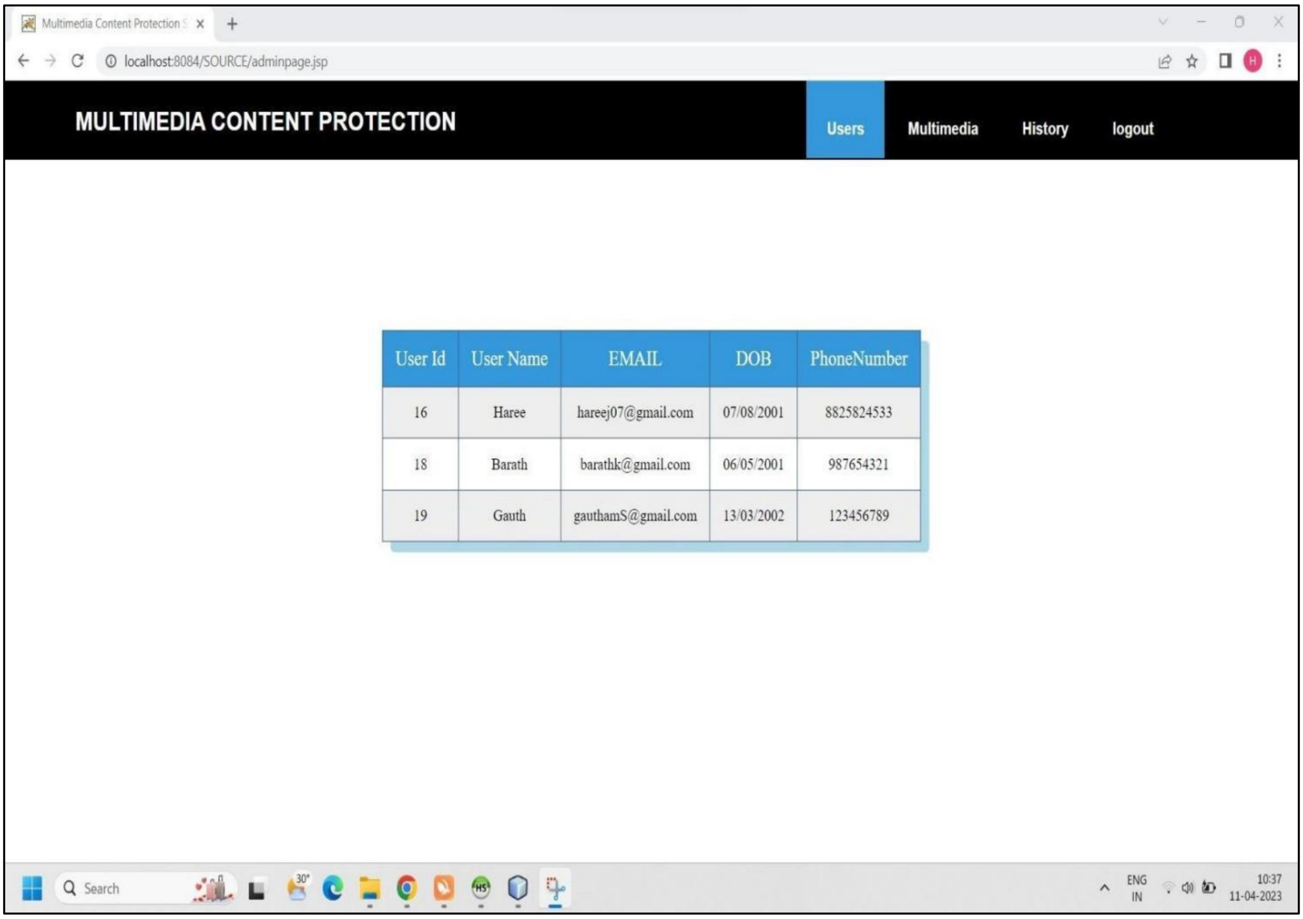

Multimedia Content Protection S
localhost:8084/SOURCE/admin.html
MULTIMEDIA CONTENT PROTECTION
Home
Admin
User
Signup
ADMIN LOGIN
SUBMIT
Search
ENG
IN
10:35
11-04-2023

admin

•••••

FIGURE 6.3 Admin Page

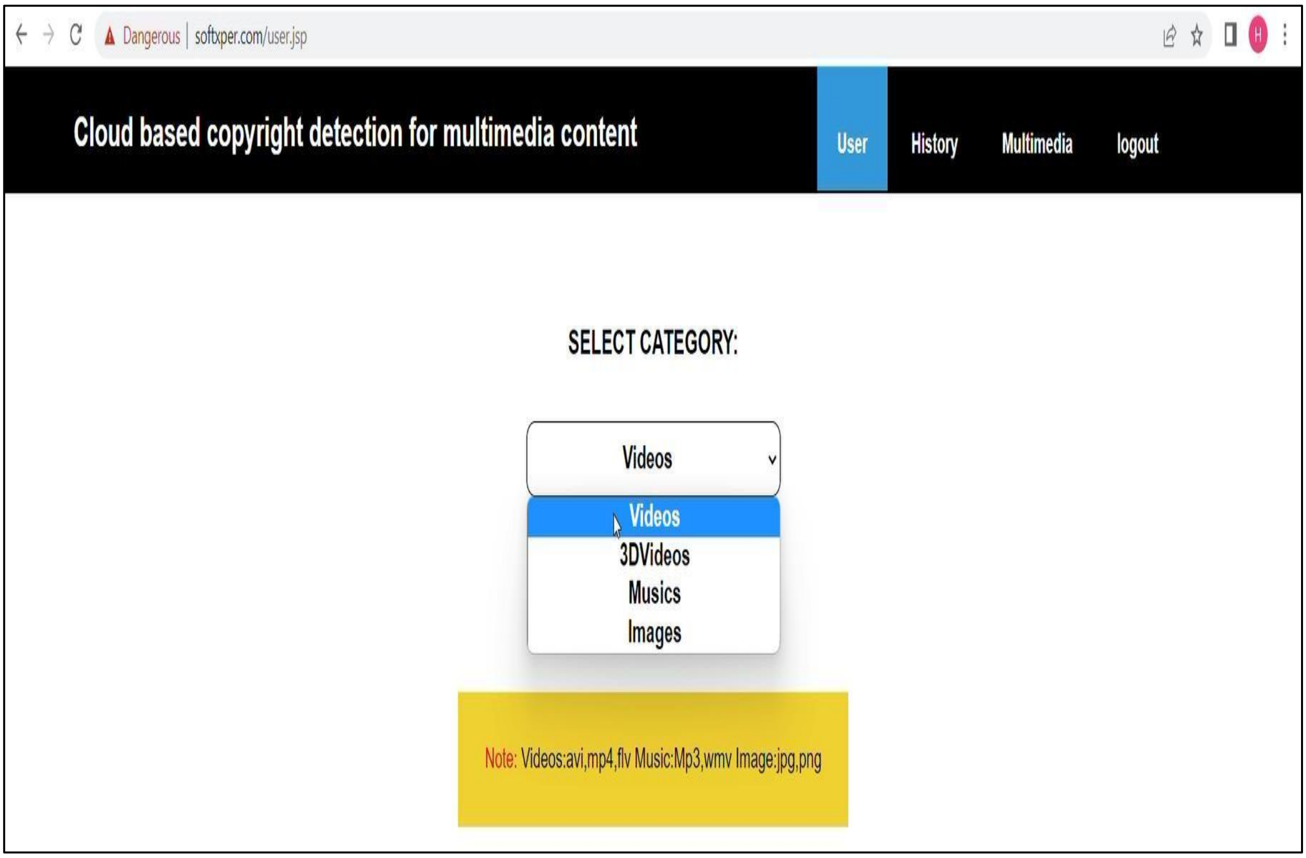
The User Details Page is a centralized hub where administrators can manage and view information about individual users. In Figure 6.4 the User Details Page displays essential profile information for each user, including their name, email address, username, and any additional details that are relevant to your system. This information provides a quick snapshot of the user's identity and allows administrators to verify and update user details as needed.


Multimedia Content Protection S
localhost:8084/SOURCE/adminpage.jsp
MULTIMEDIA CONTENT PROTECTION
Users
Multimedia
History
logout
Search
30°
ENG
IN
10:37
11-04-2023

User Id	User Name	EMAIL	DOB	PhoneNumber
16	Haree	hareej07@gmail.com	07/08/2001	8825824533
18	Barath	barathk@gmail.com	06/05/2001	987654321
19	Gauth	gauthamS@gmail.com	13/03/2002	123456789

FIGURE 6.4 User Details Page

The User Upload Page is a dedicated space where users can securely upload their multimedia content to the system. In Figure 6.5 the User Upload Page features a user-friendly and intuitive upload form. This form allows users to select and upload their multimedia files from their local devices. It supports various file formats, such as videos, audio files, images, or documents, depending on the capabilities of your system.The User Upload Page offers a secure and convenient space for users to upload their multimedia content to our Multimedia Content Protection System.



Dangerous | softxper.com/user.jsp

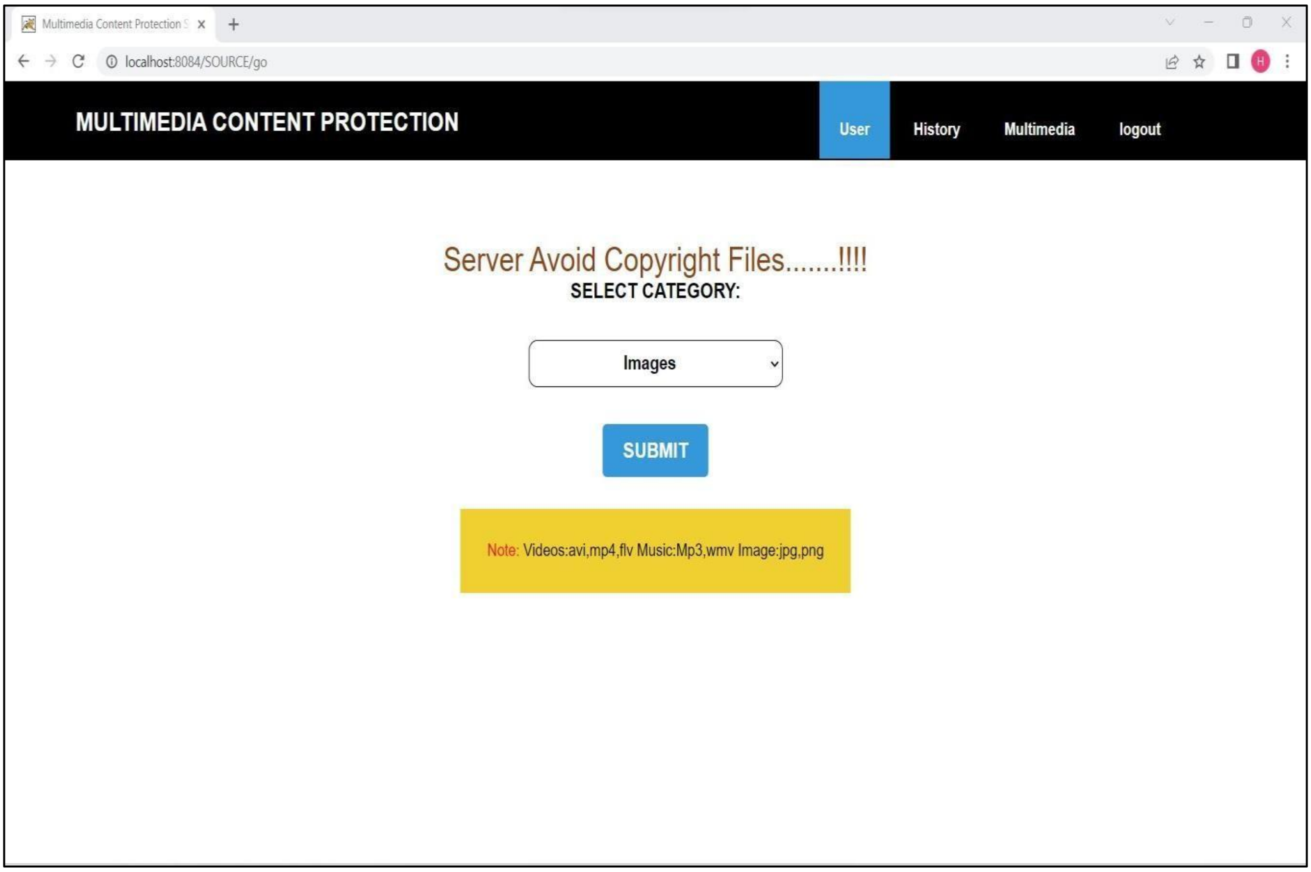
Cloud based copyright detection for multimedia content

SELECT CATEGORY:

Note: Videos:avi,mp4,flv Music:Mp3,wmv Image:jpg,png

FIGURE 6.5 User Upload Page

The Copyright Detection Page is a powerful tool designed to identify potential copyright infringements and protect the intellectual property of content owners. Our system utilizes advanced algorithms and technologies to compare uploaded multimedia content against a vast database of copyrighted material as shown in Figure 6.6. This algorithm analyzes various aspects of the content, such as audio, video, or visual elements, to detect potential matches or similarities with existing copyrighted works.


Multimedia Content Protection S
localhost:8084/SOURCE/go
MULTIMEDIA CONTENT PROTECTION
User
History
Multimedia
logout

Server Avoid Copyright Files.......!!!!

SELECT CATEGORY:

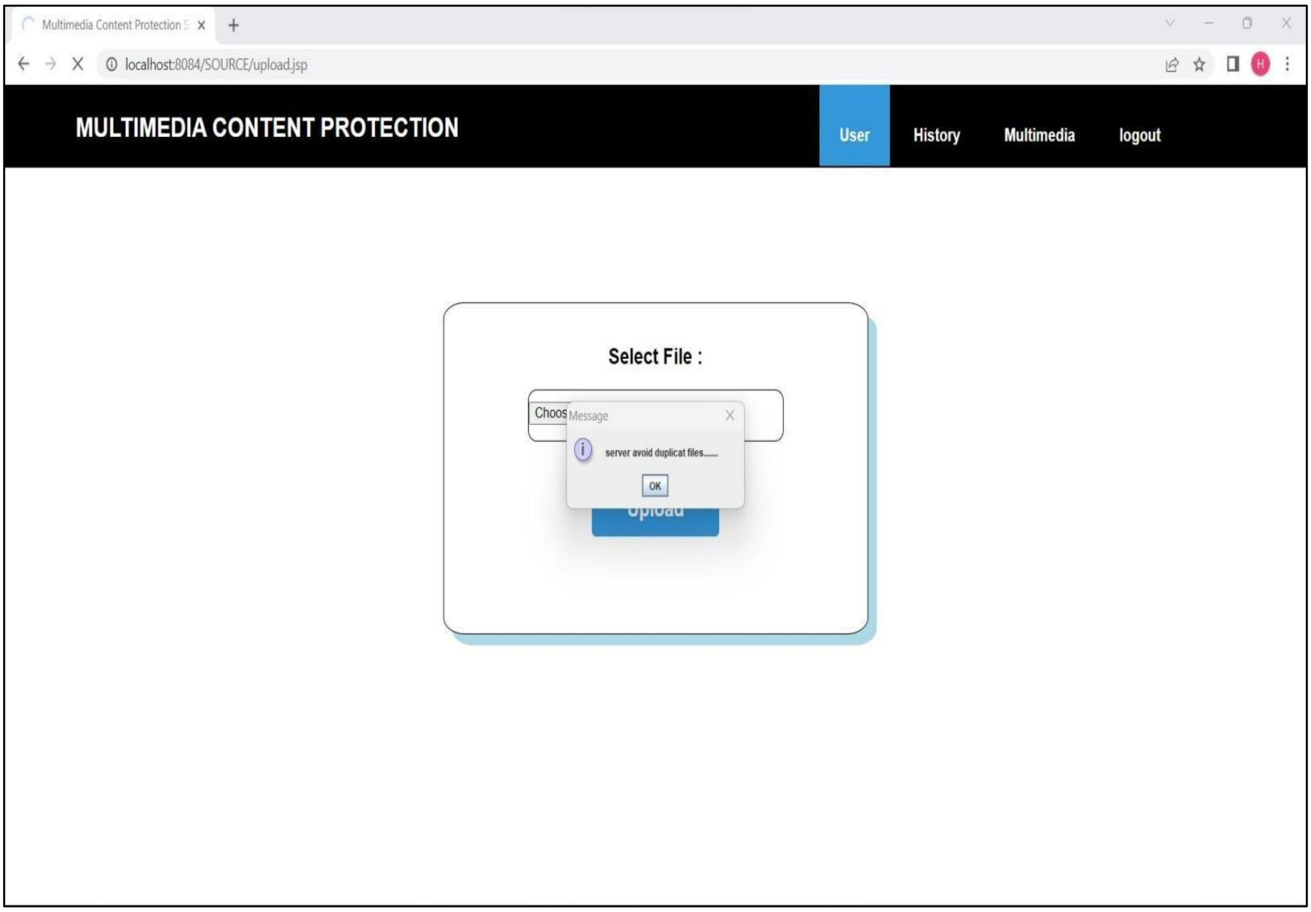
Images

SUBMIT

Note: Videos:avi,mp4,flv Music:Mp3,wmv Image:jpg,png

FIGURE 6.6 Detection Page

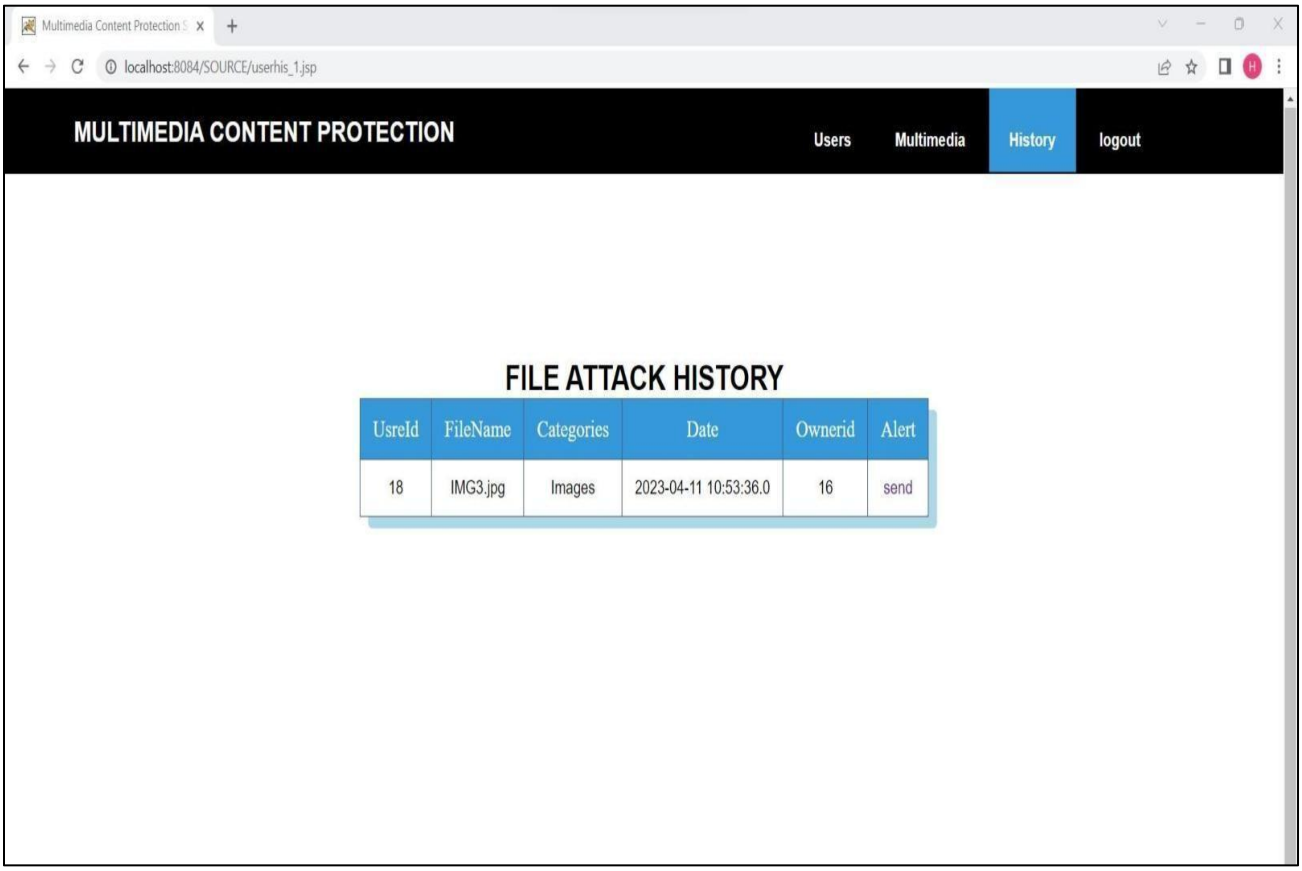
The Avoiding Duplicate Files Page is designed to help users prevent the unintentional uploading or storage of duplicate multimedia files within the system. Our system utilizes an efficient and reliable algorithm to identify potential duplicate files in Figure 6.7. This algorithm compares various file attributes, such as file size, checksums, metadata, or visual and audio fingerprints, to determine if files are duplicates or near duplicates.


Multimedia Content Protection S
localhost:8084/SOURCE/upload.jsp
MULTIMEDIA CONTENT PROTECTION
User
History
Multimedia
logout
Select File :
Choos
Message
OK
Upload

server avoid duplicat files......

FIGURE 6.7 Avoiding Duplication Page

The Alert Notification Page is a crucial component of our system that provides users with real-time notifications and alerts regarding their multimedia content. As shown in Figure 6.8 the system generates real-time alerts to keep users informed about critical events or activities related to their multimedia content. This can include alerts about unauthorized access attempts, copyright violation incidents, suspicious activities, or system-generated updates.

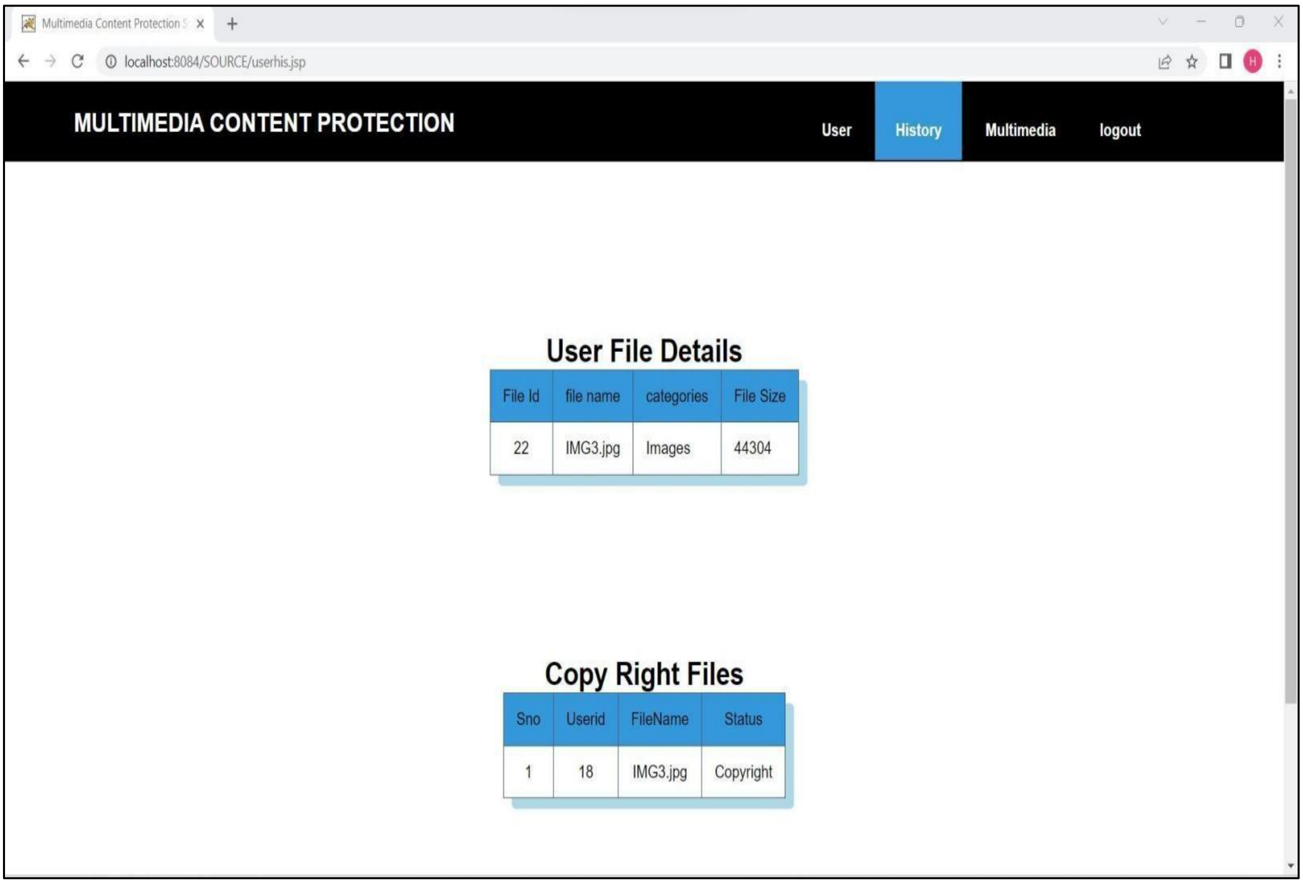

Multimedia Content Protection
localhost:8084/SOURCE/userhis_1.jsp
MULTIMEDIA CONTENT PROTECTION
Users
Multimedia
History
logout

FILE ATTACK HISTORY

UsreId	FileName	Categories	Date	Ownerid	Alert
18	IMG3.jpg	Images	2023-04-11 10:53:36.0	16	send

FIGURE 6.8 Alert Notification Page

The Copyright Status Page provides users with valuable information and insights into the copyright status of their multimedia content. Users can access information about the copyright registration status of their content. As shown in Figure 6.9 this may include details such as the registration number, date of registration, and other relevant copyright registration information. This helps users track and verify the legal protection of their creative works.


Multimedia Content Protection S
localhost:8084/SOURCE/userhis.jsp
MULTIMEDIA CONTENT PROTECTION
User
History
Multimedia
logout

User File Details

File Id	file name	categories	File Size
22	IMG3.jpg	Images	44304

Copy Right Files

Sno	Userid	FileName	Status
1	18	IMG3.jpg	Copyright

FIGURE 6.9 Copyright Status Page

This attributes in the database page in Figure 6.10 shows the list of attributes in the database. It showcases about the attack details, file details, history, user details.

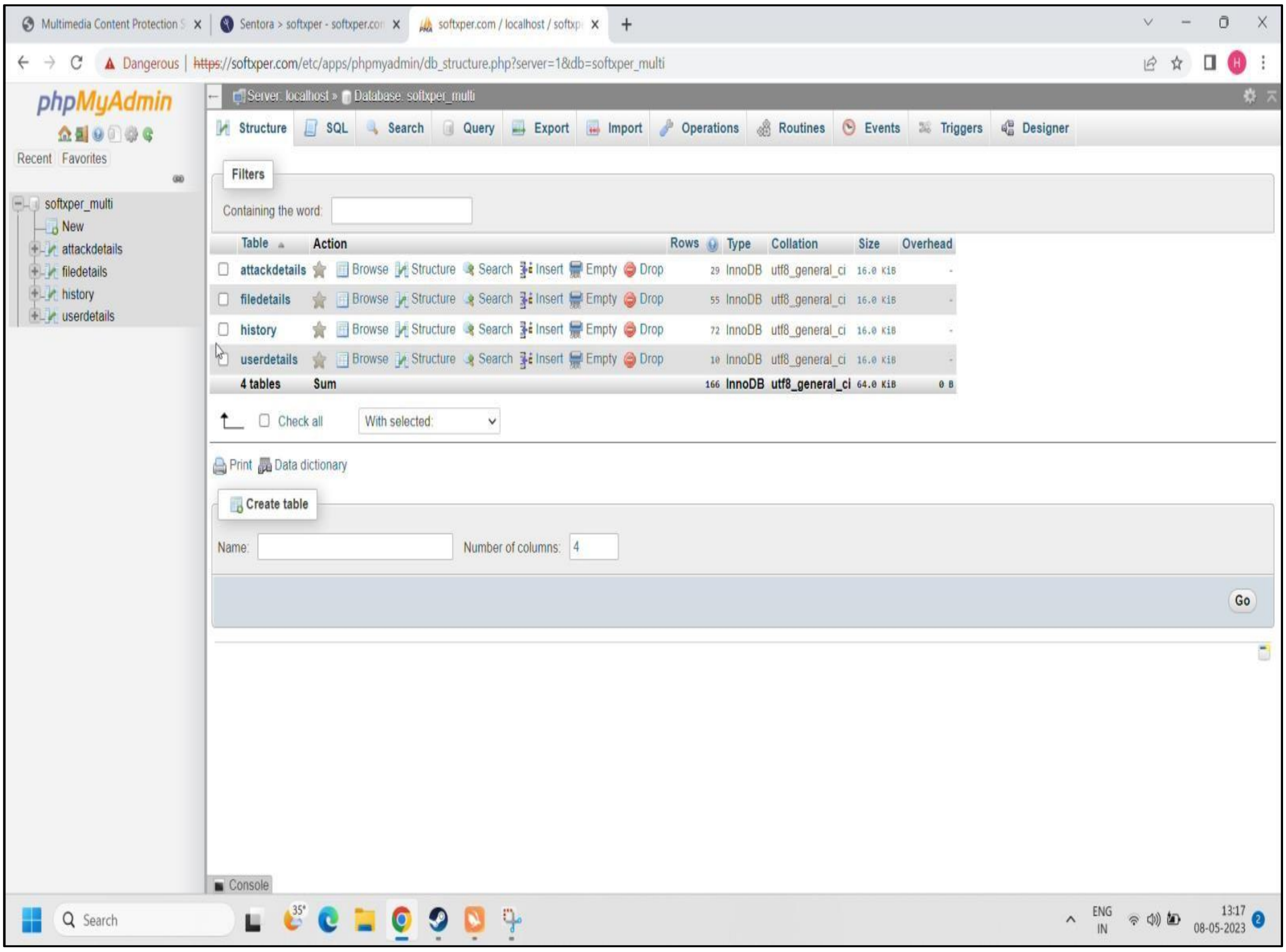
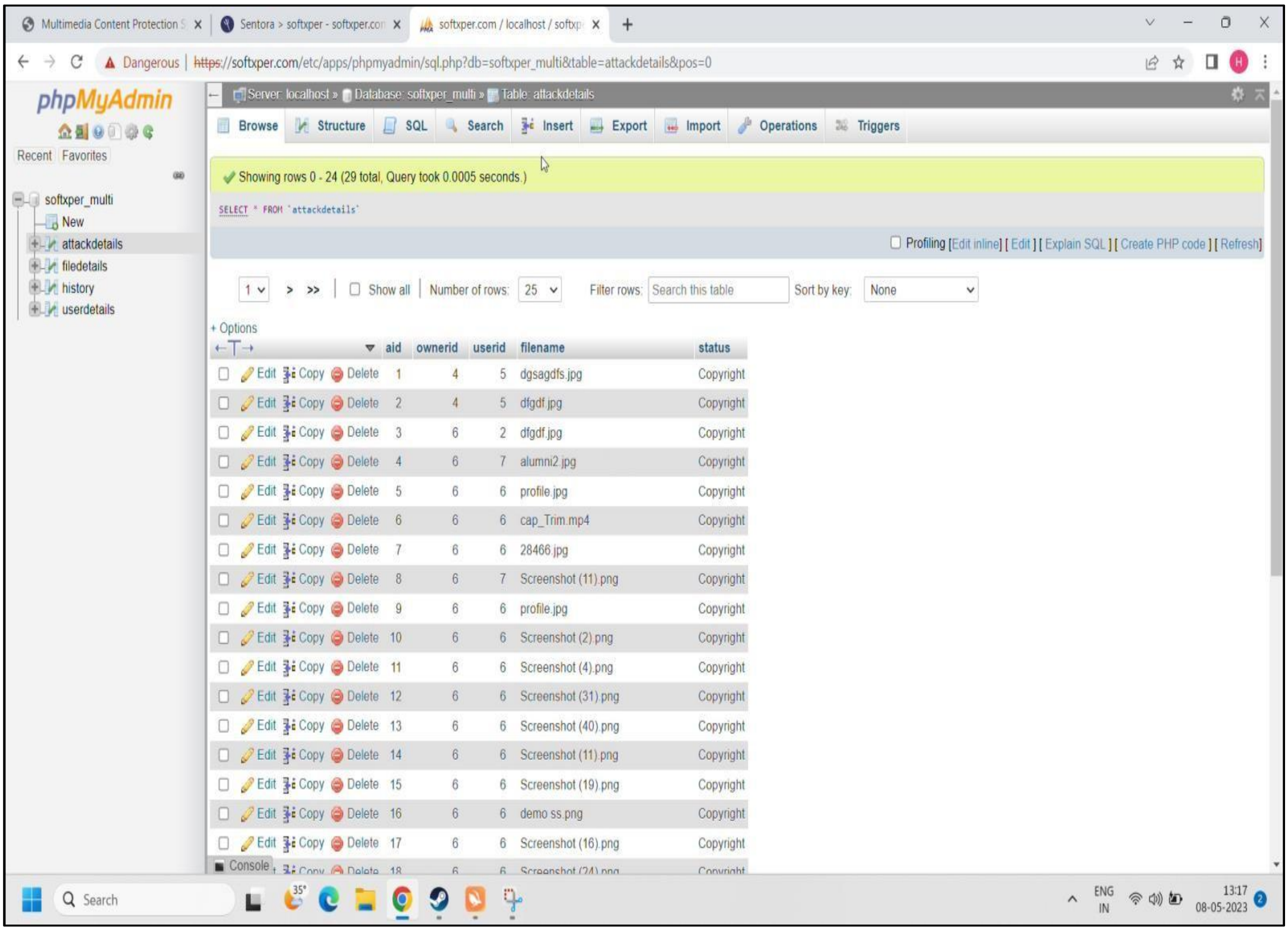


	Table	Action	Rows	Type	Collation	Size	Overhead
□	attackdetails	Browse Structure Search Insert Empty Drop	29	InnoDB	utf8_general_ci	16.0 KiB	-
□	filedetails	Browse Structure Search Insert Empty Drop	55	InnoDB	utf8_general_ci	16.0 KiB	-
□	history	Browse Structure Search Insert Empty Drop	72	InnoDB	utf8_general_ci	16.0 KiB	-
□	userdetails	Browse Structure Search Insert Empty Drop	10	InnoDB	utf8_general_ci	16.0 KiB	-
	4 tables	Sum	166	InnoDB	utf8_general_ci	64.0 KiB	0 B

FIGURE 6.10 Database Page

This page displays the details under the name of each attribute. As shown in Figure 6.11 the attack details displays owner id, user id, filename and the copyright status.


Multimedia Content Protection
Sentora > softxper - softxper.com
softxper.com / localhost / softxp
Dangerous | https://softxper.com/etc/apps/phpmyadmin/sql.php?db=softxper_multi&table=attackdetails&pos=0
phpMyAdmin
Recent Favorites
softxper_multi
New
attackdetails
filedetails
history
userdetails
Server: localhost » Database: softxper_multi » Table: attackdetails
Browse
Structure
SQL
Search
Insert
Export
Import
Operations
Triggers
□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
1
□ Show all
Number of rows: 25
Filter rows: Search this table
Sort by key: None
+ Options
Console
Search
ENG IN
13:17
08-05-2023

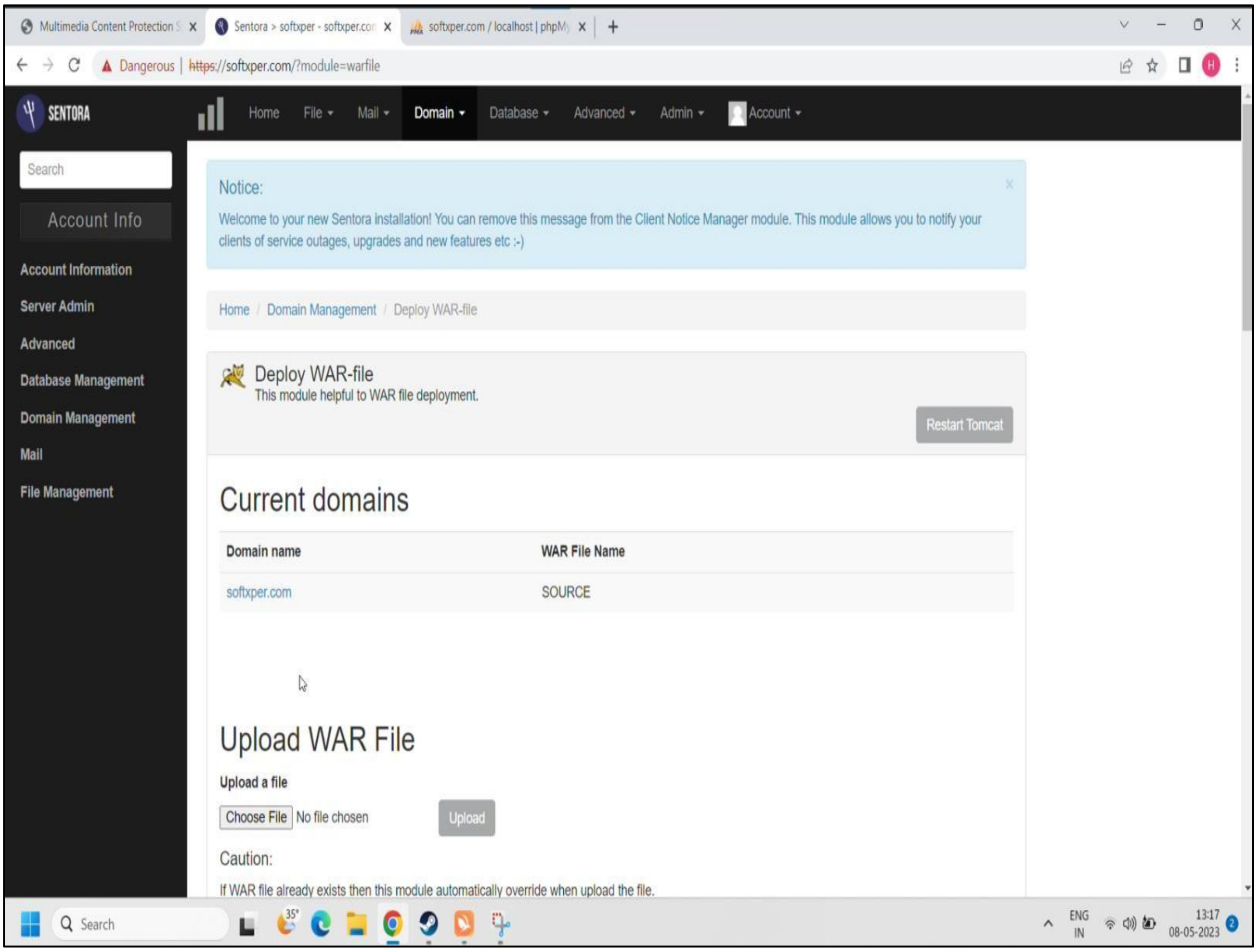
✓ Showing rows 0 - 24 (29 total, Query took 0.0005 seconds.)

```
SELECT * FROM `attackdetails`
```

	aid	ownerid	userid	filename	status
□ Edit Copy Delete	1	4	5	dgsagdfs.jpg	Copyright
□ Edit Copy Delete	2	4	5	dfgdf.jpg	Copyright
□ Edit Copy Delete	3	6	2	dfgdf.jpg	Copyright
□ Edit Copy Delete	4	6	7	alumni2.jpg	Copyright
□ Edit Copy Delete	5	6	6	profile.jpg	Copyright
□ Edit Copy Delete	6	6	6	cap_Trim.mp4	Copyright
□ Edit Copy Delete	7	6	6	28466.jpg	Copyright
□ Edit Copy Delete	8	6	7	Screenshot (11).png	Copyright
□ Edit Copy Delete	9	6	6	profile.jpg	Copyright
□ Edit Copy Delete	10	6	6	Screenshot (2).png	Copyright
□ Edit Copy Delete	11	6	6	Screenshot (4).png	Copyright
□ Edit Copy Delete	12	6	6	Screenshot (31).png	Copyright
□ Edit Copy Delete	13	6	6	Screenshot (40).png	Copyright
□ Edit Copy Delete	14	6	6	Screenshot (11).png	Copyright
□ Edit Copy Delete	15	6	6	Screenshot (19).png	Copyright
□ Edit Copy Delete	16	6	6	demo ss.png	Copyright
□ Edit Copy Delete	17	6	6	Screenshot (16).png	Copyright
Copy Delete	18	6	6	Screenshot (24).png	Copyright

FIGURE 6.11 Database Attributes Page

As shown in Figure 6.12 this page displays the source file uploaded into the cloud platform by converting the source file as War file into the cloud platform.



Notice:

Welcome to your new Sentora installation! You can remove this message from the Client Notice Manager module. This module allows you to notify your clients of service outages, upgrades and new features etc :-)

Deploy WAR-file

This module helpful to WAR file deployment.

Current domains

Domain name	WAR File Name
softxper.com	SOURCE

Upload WAR File

Upload a file

Caution:

If WAR file already exists then this module automatically override when upload the file.

FIGURE 6.12 Cloud Server Page

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 CONCLUSION

Distributing copyrighted multimedia objects by uploading them to online hosting sites such as YouTube can result in significant loss of revenues for content creators. Systems needed to find illegal copies of multimedia objects are complex and large scale. In this paper, we presented a new design for multimedia content protection systems using multi-cloud infrastructures. The proposed system supports different multimedia content types and it can be deployed on private and/or public clouds. Two key components of the proposed system are presented. The first one is a new method for creating signatures of 3-D videos. Our method constructs coarse-grained disparity maps using stereo correspondence for a sparse set of points in the image. Thus, it captures the depth signal of the 3-D video, without explicitly computing the exact depth map, which is computationally expensive. Our experiments showed that the proposed 3-D signature produces high accuracy in terms of both precision and recall and it is robust to many video transformations including new ones that are specific to 3-D videos such as synthesizing new views. The second key component in our system is the distributed index, which is used to match multimedia objects characterized by high dimensions. The distributed index is implemented using the MapReduce framework and our experiments showed that it can elastically utilize varying amount of computing resources and it produces high accuracy. A multi view plus depth video has multiple texture and depth components, which allow users to view a scene from different angles. Signatures for such videos would need to capture this complexity.

7.2 FUTURE WORK

The multimedia content protection system is a critical tool for protecting multimedia content from unauthorized use, and it is vital that it continues to evolve to meet the ever-changing landscape of digital content. In the future, several areas could be explored to improve the system's effectiveness further. First, the system's algorithms could be refined to enhance their efficiency, accuracy, and robustness. This would help ensure that the system can effectively detect and prevent instances of copyright infringement. Second, integrating blockchain technology into the system could provide an additional layer of security and help prevent unauthorized access to multimedia content. Blockchain technology is inherently secure and decentralized, making it an idealsolution for protecting multimedia content from unauthorized use.

Third, the system could be integrated with content sharing platforms such as YouTube and Vimeo, enabling content owners to detect and prevent instances of unauthorized use of their content on these platforms. Fourth, advanced artificial intelligence could be integrated into the system to enable it to learn and adapt to new threats and attacks continually. This would help to improve the system's ability to detect instances of unauthorized use and preventcopyright infringement.

Finally, increased collaboration between content owners and law enforcement agencies could help deter individuals from engaging in unauthorized use of multimedia content. This could include sharing information on potential copyright infringement cases and working together to enforce copyright laws.

REFERENCES

1. Abdelsadek. (2014), ‘Distributed index for matching multimedia objects,’ M.S. thesis, School of Comput. Sci., Simon Fraser Univ., Burnaby, Vol. 22, No. 40, pp. 103-140.

2. Abdelsadek and M. Hefeeda. (2014), ‘Dimo: Distributed index for matching multimedia objects using MapReduce,’ in Proc. ACMMultimedia Syst. Conf. (MMSys’14), pp. 115–125.

3. M. Aly, M. Munich, and P. Perona. (2011), ‘Distributed Kd-Trees for retrieval from very large image collections,’ in Proc. Brit. Mach. Vis. Conf. (BMVC), Dundee, U.K., pp. 123-136.

4. P. Cano, E. Batle, T. Kalker, and J. Haitsma. (2002), ‘A review of algorithms for audio fingerprinting,’ in Proc. IEEE Workshop Multimedia Signal Process., pp. 169–173.

5. J. Dean and S. Ghemawat. (2004), ‘MapReduce: Simplified data processing on large clusters,’ in Proc. Symp. Oper. Syst. Design Implementation (OSDI’04), pp. 137–150.

6. J. Deng, W. Dong, R. Socher, L. Li, K. Li, and L. Fei-Fei. (2009), ‘Imagenet: A large-scale hierarchical image database,’ in Proc. IEEE Conf. Comput. Vis. Pattern Recog. (CVPR’09), pp. 248–255.

7. S. Ioffe. (2012), ‘Full-length video fingerprinting. Google Inc.,’ U.S. Patent 8229219, pp. 87-103.

8. N. Khodabakhshi and M. Hefeeda. (2013), ‘Spider: A system for finding 3D video copies,’ in ACM Trans. Multimedia Comput., Commun., Appl. (TOMM), Vol. 9, No.1, pp. 7:1–7:20.

9. S. Lee and C. Yoo. (2015), ‘Robust video fingerprinting for content-basedvideo identification,’ IEEE Trans. Circuits Syst. Video Technol., Vol. 18, No. 7, pp. 983–988.