IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.115110

WATERMARKING AND RE-ENCRYPTION APPROACH TO AVOID DATA LEAKAGE

Shalini A[1], Biju Balakrishnan[2]

II MCA Student, MCA, Hindusthan College of Engineering and Technology, Coimbatore, India[1]

Assistant Professor, MCA, Hindusthan College of Engineering and Technology, Coimbatore, India[2]

Abstract: Sharing multimedia data is becoming a more and more necessary component of daily life for users to access various systems, services, and applications. with the actual world, data exposure happens often with cloud storage services. In safe data transfer medium, authentication and copyright protection of multimedia materials have long been issues. utilization of modern technology and the Internet, the problem has gotten worse. Making copyright protection is more challenging and complex, though. The copyright protection issue has a solution: digital watermarking. Both watermarking and the Proxy Re-encryption (PRE) methodology are employed in the suggested method for effective sharing of multimedia material. In digital material like photographs, watermarking is used to conceal information like secret information. Data security is achieved using encryption methods. In order to prevent unauthorised access, information is encoded using encryption, making it impossible for anyone who are not authorised to view it. In the proposed approach, a key may be used to encrypt a secret key using an encryption method. The user's private key may then be integrated into the picture using LSB (Least Significant Bit), along with encrypted key information. Images may be encrypted using the ECC Encryption technique once secret information has been included. With the aid of the inbuilt data verification procedure, the decryption key may finally be extracted by an authorised user. When user Data does not correspond embedded information, illegal or unauthorised access can be recognised.

I. INTRODUCTION

Determining whether to grant a person access to a particular system or resource is known as authentication, and it is a crucial field of study in security research. Integrity and secrecy are crucial components of authentication. Additionally, proper authentication is the first line of defense for safeguarding any resource. Here As a service, we use authentication to protect the resources. It is important to keep in mind that not all situations necessitate using the same kind of authentication.Users may have many passwords for websites, networks, and banks, which presents a challenge. Having a lot of passwords causes confusion and creates interference, which might result in password forgetting. Any authentication scheme's acceptability is largely determined by how resilient it is to assaults and how much resources it requires on the client and server ends.

1.1 RELATED WORKS:

The process of adding information, or watermarks, to digital assets, including pictures, movies, or documents, is known as watermarking. Although these watermarks are typically invisible to the human eye, they can be found utilizing of sophisticated algorithms. Sensitive Information can be uniquely marked with watermarking in the context of preventing data leaks. The watermark can be used to identify the original owner of the material in the event that it is leaked or shared without permission. Re-encryption is the process of first encrypting data using one key, then using a different key to re-encrypt it. It is possible to restrict access to sensitive data using this procedure. For instance, When multiple parties need access to encrypted data, each party could have its own encryption key. When the data has been encrypted using a shared key, it can be re-encrypted using each party's unique key.

1.2 WATERMARKING TECHNIQUE:

This technique involves embedding a unique identifier or watermark into the data itself. This identifier is typically imperceptible to humans but can be detected by specialized software or algorithms. If the watermarked data is leaked or shared without authorization, the watermark ca n be utilized to determine the original owner's location where the leak originated. Digital assets, including pictures, movies, and audio files, frequently use watermarking to prevent unlawful sharing or dissemination.Re- Encryption is the method by which of encrypting data with a fresh encryption key before

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.115110

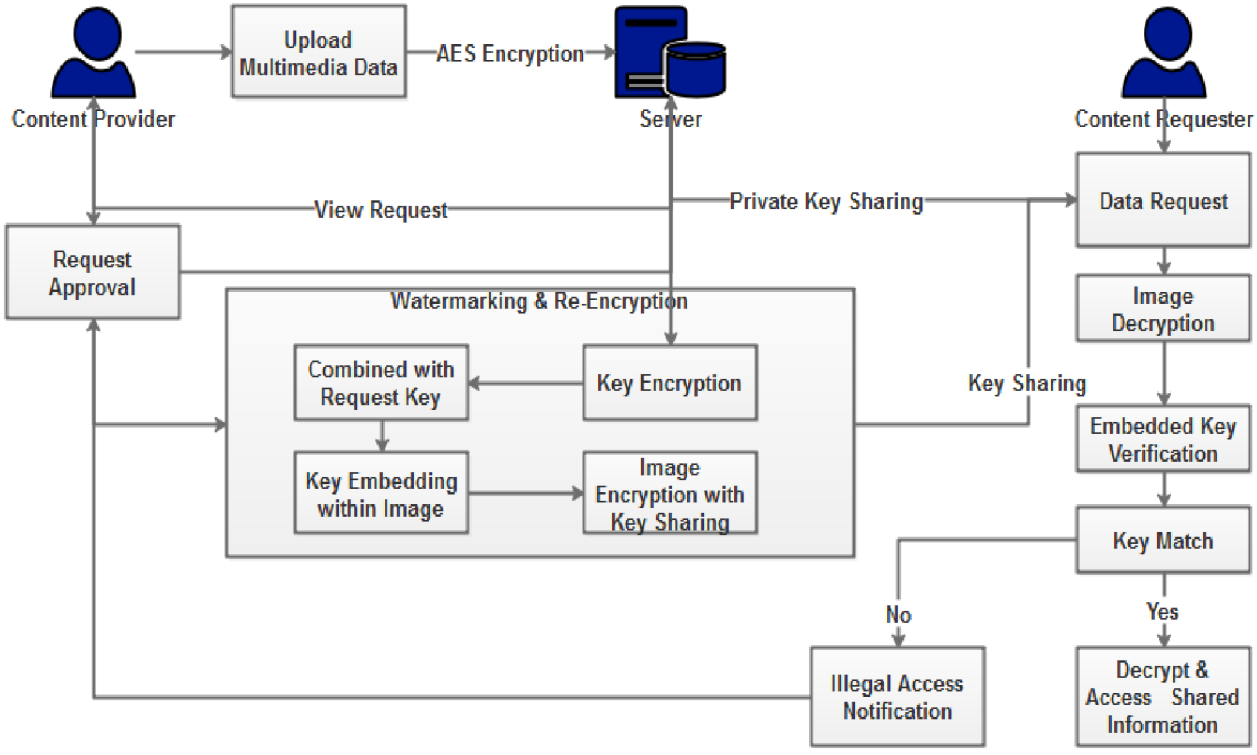
sending it to another system or receiver. This procedure makes sure that the data stays encrypted and unreadable without the right decryption key, even in the case that it is accessed or intercepted by unauthorized individuals. Re-encryption can be used in concert with other security measures, such as authentication and access controls, to better protect sensitive data.

1.3 SYSTEM IMPLEMENTATION:

Start by identifying the sensitive data that needs protection. This could include customer information, financial data, intellectual property, or any different confidential information.Choose a suitable watermarking method according to the kind of data and your security requirements. Common methods include visible watermarks (easily visible to users) and invisible watermarks (embedded within the data and not visible to users Integrate the watermarking process into your data handling workflows. For example, when uploading images or documents to your system, automatically embed watermarks to uniquely identify each piece of dataGenerate Encryption Keys: Develop a strategy for generating and managing encryption keys. Consider using strong encryption algorithms such as AES (Advanced Encryption Standard) for re-encryption.Integrate re-encryption logic into your data access and sharing mechanisms. When Data has to be shared with authorized parties, re-encrypt it using a new key before transmission.Access Controls and Authentication.Enhance security by mandating MFA for users accessing sensitive data or performing actions that involve watermarking or re-encryption.Enable logging and monitoring of watermarking and re-encryption activities. Maintain audit trails to track who accessed data, applied watermarks, and performed re-encryption.Set up alerts and notifications for suspicious activities connected to data handling, such as unauthorized attempts to access or modify data.Conduct regular security assessments and penetration testing to identify vulnerabilities in your watermarking and re-encryption implementations. Address any weaknesses or gaps in security promptly.Ensure that your watermarking and re-encryption practices adhere to applicable data protection regulations and as well as industry norms(e.g., GDPR, HIPAA, ISO/IEC 27001).

1.4 ARCHITECTURE DIAGRAM:

The theoretical framework that describes a system's behavior, structure, and other aspects referred to as asystems architecture, or simply systems architecture. A system's formal description and representation, structured to facilitate inference about the system's behaviors and structures, is called an architecture description. System components, their outwardly evident characteristics, and the interactions (such as behaviors) between them can all be included within a framework architecture. It can offer a strategy from which systems and products can be created that will cooperate to execute the system as a whole.Architecture description languages (ADLs) are a group of formalized languages that have been created to describe system architecture.



IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.115110

1.5 SYSTEM TESTING:

Test the visibility and detectability of watermarks to ensure they can be recognized without affecting the data's usefulness.Test the re-encryption procedure if multiple users exchange or access the same piece of data or systems.Ensure that re- encryption is seamless and does not compromise data integrity or accessibility for authorized users.Conduct tests to verify access controls are enforcedproperly. Attempt to access sensitive data without the necessary permissions to check if access is denied.Test different user roles and permissions to ensure that each role has the appropriate level of access to data.Validate that logging and monitoring mechanisms are capturing relevant events related to watermarking, re-encryption, and data access.

Review audit logs to confirm that they contain sufficient information to trace data leakage incidents back to their source.Test the integration of watermarking and re-encryption functionalities with other system components and applications. Ensure smooth data flow and operation across the system.Verify that APIs or plugins used for automation of watermarking and re-encryption processes function correctly.Conduct security vulnerability assessments and penetration testing to identify potential weaknesses in the watermarking and re-encryption implementations.Address any security vulnerabilities or gaps discovered during testing to strengthen the overall data leakage prevention measures.

II. SYSTEM STUDY AND FEASIBILITY

The CP wants to use the cloud for hosting and distributing media since it has a lot of media content. The collection of media items will be encrypted by the CP in order to stop data leakage and illegal access. The CP will transmit the cloud a re- encryption key to delegate the decryption right in order to share the media content with a permitted user. In addition, fair watermarking for traitor tracing requires watermarks to be securely inserted into shared media assets. and the decryption rights for the specific Permission has been granted to the user content, they may access the media content.

Nevertheless, authorised individuals may re-distribute the decrypted media material to the general public owing to financial incentives or commercial objectives. All of the CP's encrypted media content is kept on a cloud server. Upon receiving the request from the CP, it serves as an intermediary to assign the decryption privilege to a licence user and covertly include both the CP's and the user's watermarks into the target media item. The server will verify the shared data's authorization when accessing it. The server will give the requester the data access key if the user complies with the conditions. Otherwise, user access to data is prohibited. Notify the content provider of any more illicit content access

2.1 HARDWARE REQUIREMENTS:

- Processor : Intel core processor 2.6.0 GHZ
- RAM : 4GB
- Hard disk : 320 GB
- Compact Disk : 650 Mb
- Keyboard : Standard keyboard
- Monitor : 15 inch color monitor

2.2 SOFTWARE REQUIRMENTS:

- Systems of operation : Windows OS
- Front End : ASP.NET (C#)
- Back End : SQL SERVER
- IDE : VISUAL STUDIO

III. RESULT ANALYSIS

Every modification that SQL Server makes to the database during a conversation is recorded. This is necessary in the case that there is a lapse in the exchange's execution. In this case, every explanation that has already been given throughout the conversation needs to be withdrawn. Every every one of these records—more especially, the values that came before and after the fact—are stored by SQL Server in a document or documents referred to as the exchange log. Each database within the SQL Server framework has a unique exchange log. For instance, concurrency in multi-client frameworks like SQL Server has a selected influence of execution. When information is made available in a way that allows a single, standout project to use it, preparation dramatically decreases.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.115110

SQL Program Every announcement made within a trading platform creates a nuclear unit. This suggests that either every announcement is carried out or, in the event of a letdown, every announcement is eliminated.

It is necessary to securely insert watermarks into the shared media products in order to use fair watermarking for traitor tracking. Upon receiving a request from the CP, the server functions as a proxy, granting authorized users the ability to decrypt data and discreetly inserting the watermarks of both the CP and the user into the intended media item. One could first encrypt the decryption key for a media asset. These two watermarks, which include an encrypted key and a user watermark, are then safely inserted into the target media item.

3.1 ADVANTAGES:

- The user's watermark is well protected against hackers, preventing the unauthorized sharing of shared data in storage.
- All private data is adequately protected against the cloud, achieving the purpose of data confidentiality.
- The Content Provider should be
- able to track down unauthorized redistribution of content.

3.2 DISADVANTAGES:

- Data sharing by email is not secure.
- Only analysed the activity of mail access
- Easily hack the uploaded data

IV. CONCLUSION

Provide a method for the safe transfer of data via an email server that combines watermarking and cryptography. AES is utilized for encryption, and discrete wavelet method is employed for watermarking. The suggested method is intended to offer media In addition to copyright protection, the Geofense framework is the basis for data integrity and authentication services. It features a machine learning system that chooses group data sharing based on the geographical location of the group.

Consequently, its goal is to identify any illicit activity on the watermarked material rather than to be resilient against alteration attacks. This technique's ability to determine whether the transferred information's integrity and authentication have been compromised at the recipient end has been identified. The suggested method identified this alteration at the recipient end and informed the content supplier about the unauthorized distribution. Additionally, offer a postal delivery system so that recipients can track the status of their letters.

In the future, the suggested method can be put into practice in medical information systems to offer confidentiality, system authentication, and medical image integrity. It is possible to suggest other reversible watermarking techniques to raise the volume of data embedded, as well as additional lossless compression techniques to improve the suggested technique's capacity to embed more data.

4.1 FUTURE ENHANCEMENT:

In the future, the suggested method can be put into practice in medical information systems to offer confidentiality, system authentication, and medical image integrity. It is feasible to suggest other reversible watermarking techniques to raise the volume of data embedded, as well as additional lossless compression techniques to improve the suggested technique's capacity to embed more data. The lock manager acts as a mediator between users and shared objects, granting or denying access to resources.

In addition, SQL Server has an optimistic concurrency control approach that is comparable to other databases' multiversion concurrency control. The most important database frameworks used in today's product industry are social database frameworks. Exceptional amidst the Microsoft SQL Server among the most notable frameworks. Microsoft developed and exhibited the SQL Server database administration framework.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

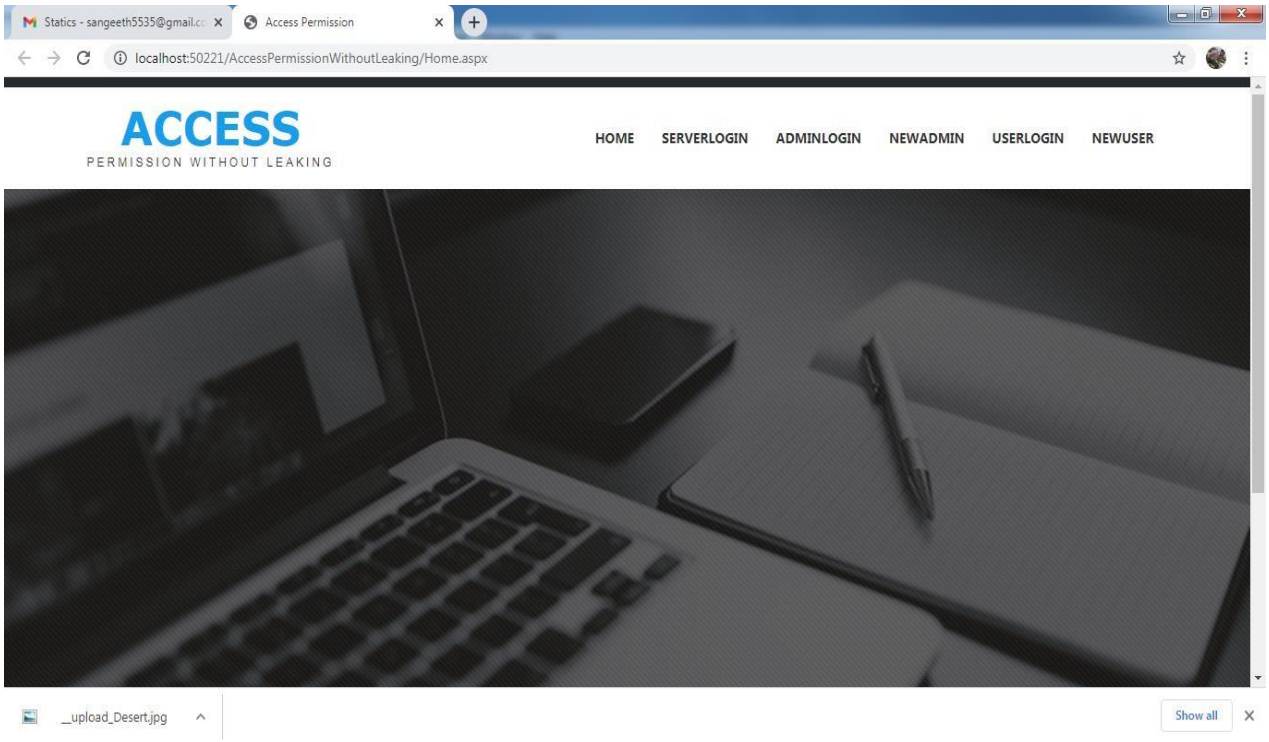
International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

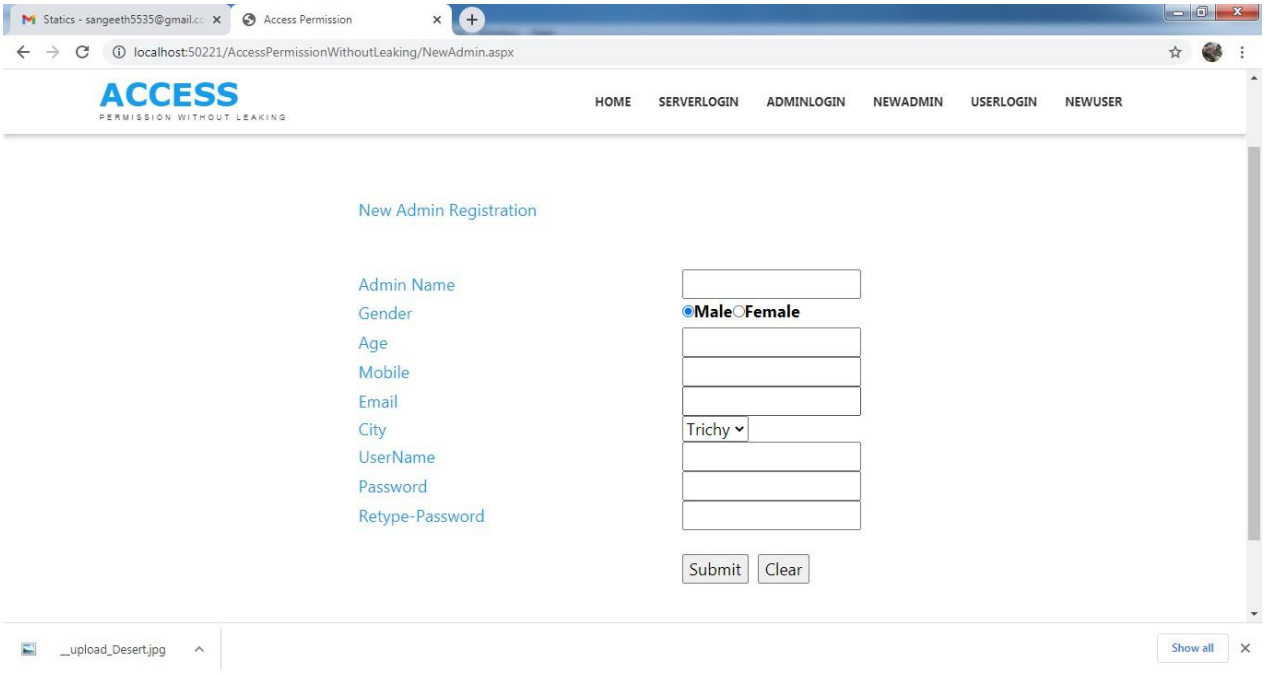
DOI: 10.17148/IARJSET.2024.115110

V. SCREENSHOT

5.1 HOME PAGE:



5.2 ADMIN LOGIN:



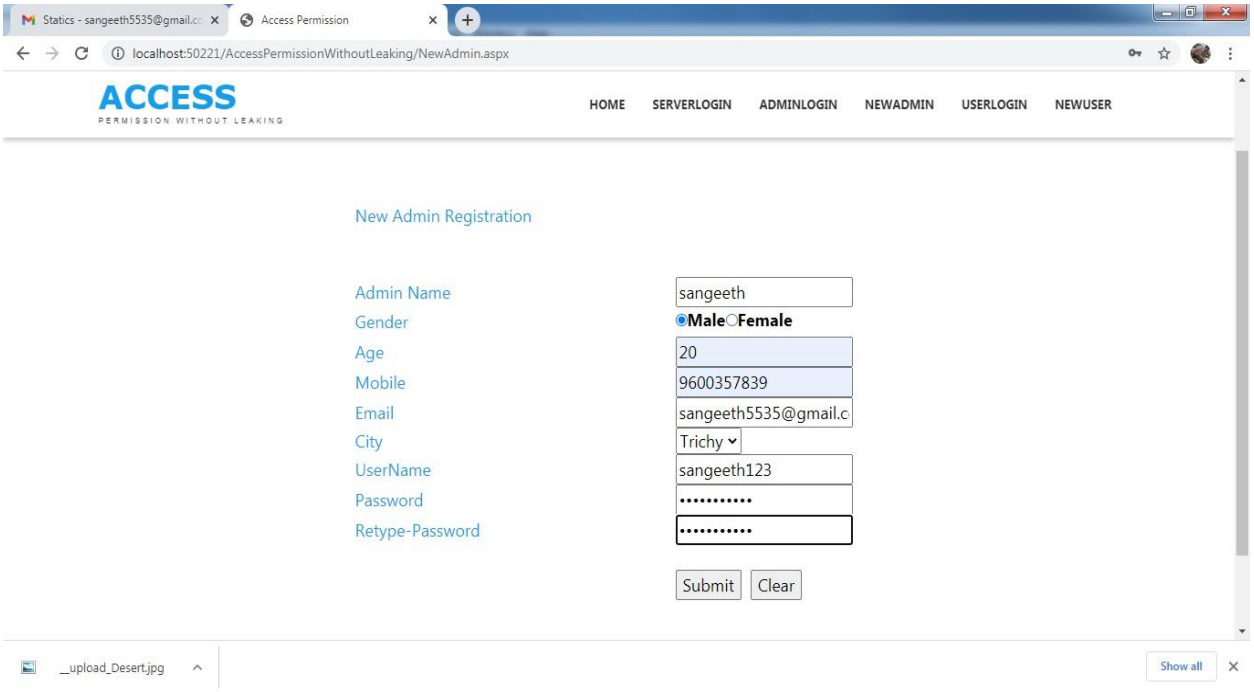
IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

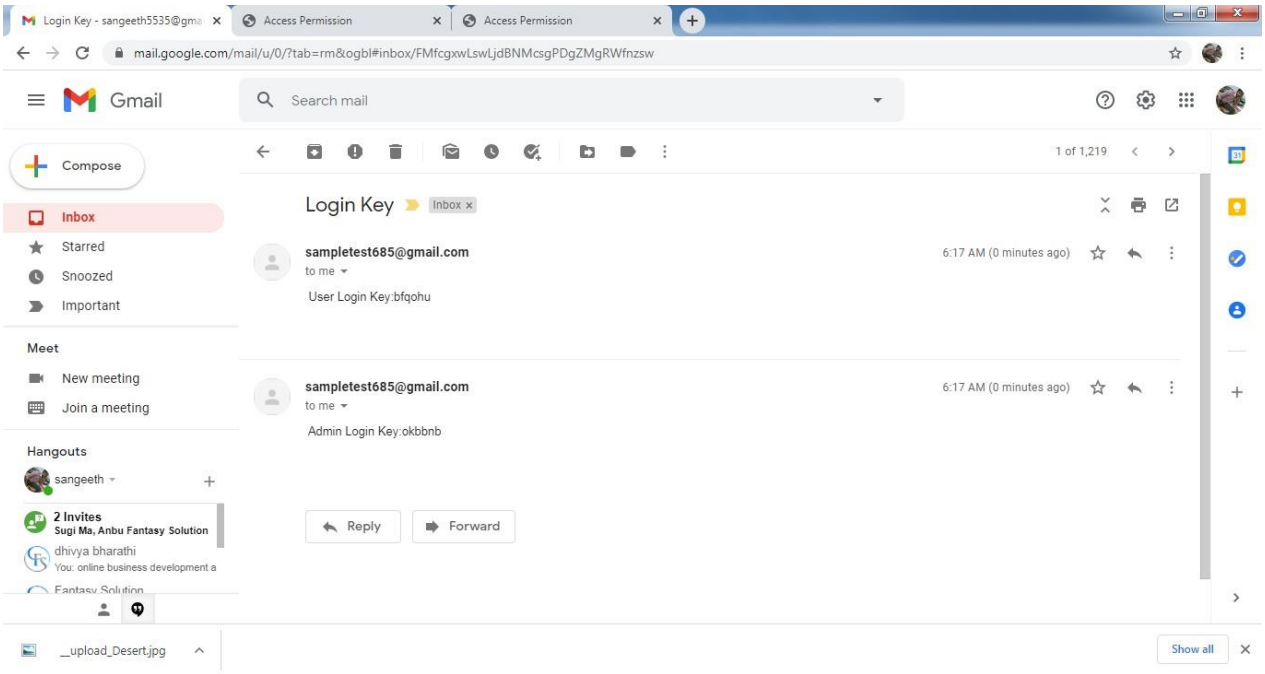
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.115110

5.3 SERVER DETAILS:



5.4: KEYS DETAILS:



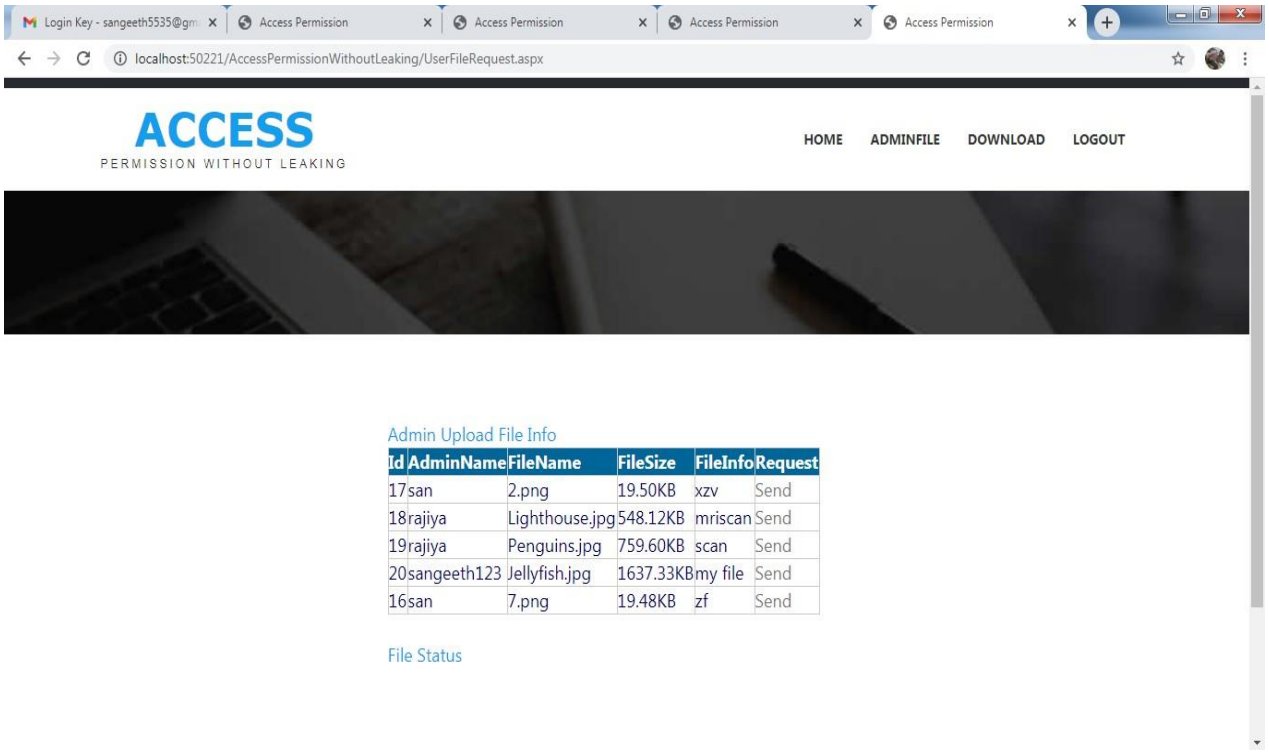
IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

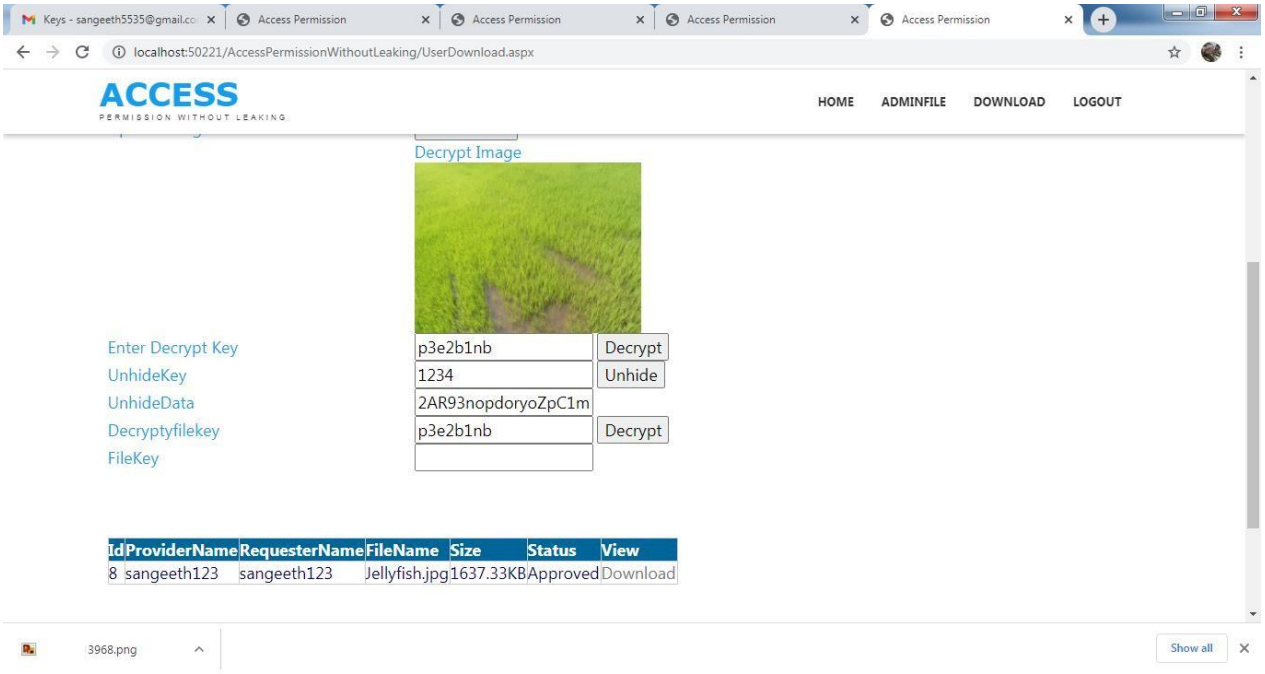
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.115110

5.5: FIL SEND APPROVED:



5.6: ENCRYPTION AND DECRYPTION KEYS PROCESS:



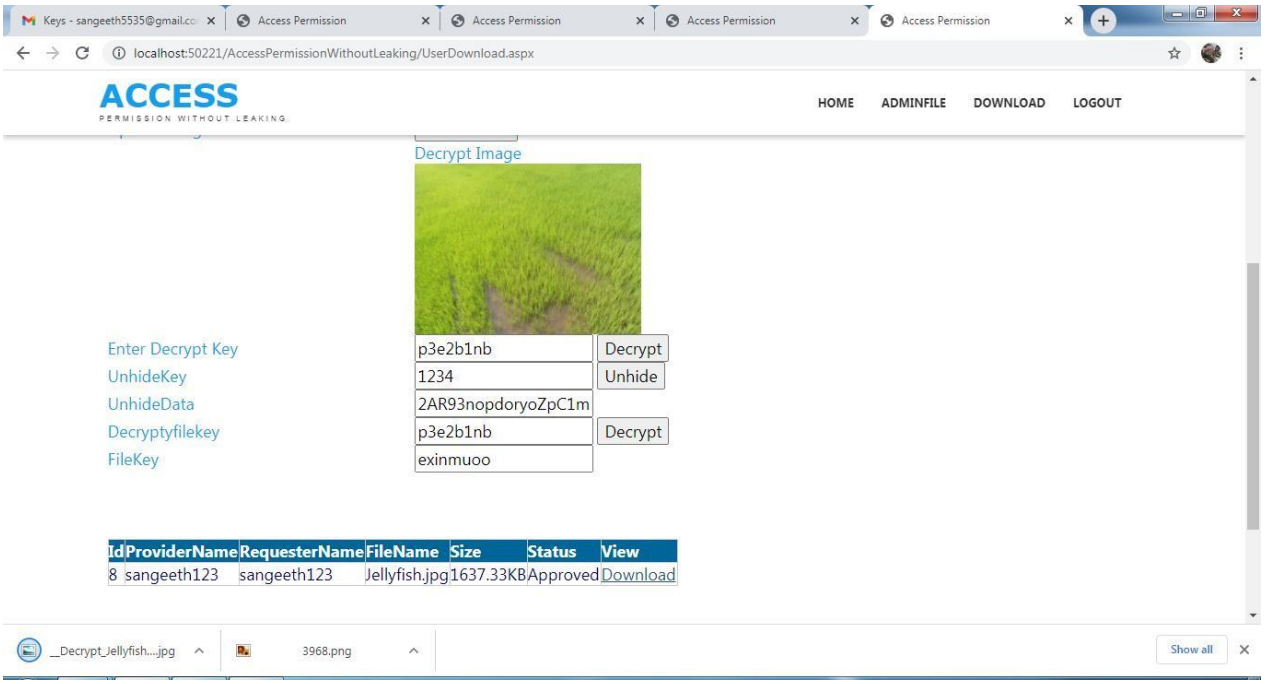
IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.115110

5.7: ORIGINAL DATAS:



REFERENCES

[1]. N.J. Belkin and W.B. Croft, “Information Filtering and Information Retrieval: Two Sides of the Same Coin?”Comm.
[2]. Advanced .NET Remoting in VB.NET (Ingo Rammer, Apress, July 2002)
[3]. ASP to ASP.NET Migration Handbook (Christian Nagel et al, Wrox, January 2003)
[4]. Beginning Visual C# (Christian Nagel et al, Wrox, September 2001)
[5]. Data-Centric .NET Programming (Christian Nagel et al, Wrox, December 2001)
[6]. Professional .NET Network Programming 2nd Edition (Christian Nagel et al, Wrox, September 2004)
[7]. P.W. Foltz and S.T. Dumais, “Personalized Information Delivery: An Analysis of Information Filtering Methods,” Comm.
[8]. S. Pollock, “A Rule-Based Message Filtering System,” ACM Trans. Office Information Systems.