

Enhanced Security in Digital Forensics: Secure Storage with Key-Based Encryption

A Final Project Mid Semester Report

submitted by

VEMULA HARAN RITVICK (CS21B1033)

in partial fulfilment of requirements

for the award of the degree of

BACHELOR OF TECHNOLOGY



**Department of Computer Science and Engineering
INDIAN INSTITUTE OF INFORMATION TECHNOLOGY,
DESIGN AND MANUFACTURING, KANCHEEPURAM**

March 2025

DECLARATION OF ORIGINALITY

I, **VEMULA HARAN RITVICK**, with Roll No: **CS21B1033** hereby declare that the material presented in the Project Report titled **Enhanced Security in Digital Forensics: Secure Storage with Key-Based Encryption** represents original work carried out by me in the **Department of Computer Science and Engineering** at the Indian Institute of Information Technology, Design and Manufacturing, Kancheepuram.

With my signature, I certify that:

- I have not manipulated any of the data or results.
- I have not committed any plagiarism of intellectual property. I have clearly indicated and referenced the contributions of others.
- I have explicitly acknowledged all collaborative research and discussions.
- I have understood that any false claim will result in severe disciplinary action.
- I have understood that the work may be screened for any form of academic misconduct.

VEMULA HARAN RITVICK

Place: Chennai

Date: 04.03.2025

CERTIFICATE

This is to certify that the report titled **Enhanced Security in Digital Forensics: Secure Storage with Key-Based Encryption** , submitted by **VEMULA HARAN RITVICK (CS21B1033)**, to the Indian Institute of Information Technology, Design and Manufacturing Kancheepuram, in partial fulfilment of requirements for the award of the degree of **BACHELOR OF TECHNOLOGY** is a bonafide record of the work done by him/her under my supervision. The contents of this report, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Dr. Noor Mahammad SK

Project Internal Guide

Associate Professor

Department of Computer Science and Engineering

IIITDM Kancheepuram, Chennai - 600 127

Place: Chennai

Date: 04.03.2025

ACKNOWLEDGEMENTS

I would like to extend my sincerest gratitude to my internal guide Dr. Noor Mahammad for constantly guiding me throughout the project and always being available to answer my queries and for their valuable guidance. Their integral view, enthusiasm, research and their commitment for providing good quality work, has motivated and inspired me.

ABSTRACT

The field of digital forensics faces significant challenges in ensuring the protection and integrity of digital evidence. Cloud forensics, an evolution of traditional digital forensics, seeks to protect evidence from online threats; however, centralized evidence collection and storage can compromise its reliability. This project presents a novel approach to digital forensic architecture, titled "Enhanced Security in Digital Forensics: Secure Storage with Key-Based Encryption." The architecture incorporates a Secure Block Verification Mechanism (SBVM) for authentication, and secret keys are generated using an Enhanced Equilibrium Optimizer (EEO) model. Data encryption is performed using Elliptic Curve Cryptography (ECC) to ensure robust security. The encrypted data is then securely stored on the cloud server. The simulation results demonstrate that this model outperforms contemporary approaches in multiple performance metrics, offering enhanced security, reliability, and efficiency for digital forensics in cloud environments.

KEYWORDS: Digital forensics; cloud forensics; secure block verification mechanism; optimal key generation; enhanced equilibrium optimizer; Elliptic Curve Cryptography; data encryption; cloud storage; digital evidence security; forensics architecture; performance metrics.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	i
ABSTRACT	ii
LIST OF FIGURES	v
ABBREVIATIONS	vi
1 INTRODUCTION	vii
1.1 Motivation	vii
1.2 Problem Statement	vii
1.3 Objective of the Project	viii
1.4 Scope	viii
1.5 Project Introduction	viii
2 LITERATURE SURVEY	x
2.1 Description of research papers and textbooks on forensic science, cryptography and network security	x
2.1.1 Role of forensic science in criminal justice	x
2.1.2 Design and implementation of FROST	x
2.1.3 Cryptography and network security	xi
3 SYSTEM ANALYSIS	xii
3.1 Existing System	xii
3.2 Disadvantages	xii
3.3 Proposed System	xiii
3.4 Advantages	xiii
3.5 Work Flow of Proposed System	xiv
4 PRODUCT DEVELOPMENT PROGRESS	xv

4.1	Proposed Architecture	xv
4.2	Implementation Progress	xvi
4.2.1	User (Forensic Investigator) Module	xvi
4.2.2	Admin Module	xvi
4.2.3	Court Module	xvi
4.3	Upcoming Implementation Work	xvii
4.3.1	Algorithm Analysis	xvii
4.3.2	User (Forensic Investigator) Module	xvii
4.3.3	Admin Module	xvii
4.3.4	Court Module	xvii

REFERENCES	xviii
-------------------	--------------

LIST OF FIGURES

3.1	Work Flow	xiv
4.1	Product Architecture	xv
4.2	User Registration and Upload Evidence	xvii
4.3	Admin Authorization	xvii

ABBREVIATIONS

SBVM	Secure Block Verification Mechanism
EEO	Enhanced Equilibrium Optimizer
ECC	Elliptic Curve Cryptography
MKHE	Multiparty Key Homomorphic Encryption

CHAPTER 1

INTRODUCTION

1.1 Motivation

The growing complexity of cloud forensics presents a major challenge in protecting and preserving the integrity of digital evidence. As online threats continue to evolve, traditional methods of collecting and storing evidence often fall short, making it difficult to ensure reliability and security. This research aims to bridge that gap by introducing a more secure and efficient forensic framework. By incorporating advanced encryption, strong authentication, and optimized key management, this approach enhances the way digital evidence is handled in cloud environments. Ultimately, the goal is to support digital forensic investigations with a system that is not only more secure but also better suited to the ever-changing landscape of cyber threats.

1.2 Problem Statement

This research aims to develop an advanced digital forensic framework, "Enhanced Security in Digital Forensics: Secure Storage with Key-Based Encryption," to tackle the challenges of securing and preserving digital evidence in cloud environments. The proposed architecture is designed to strengthen security and reliability by integrating a Secure Block Verification Mechanism (SBVM) for robust authentication, an Enhanced Equilibrium Optimizer (EEO) model for efficient key generation, and Elliptic Curve Cryptography (ECC) for strong data encryption. By combining these elements, this approach seeks to surpass existing methods in maintaining the integrity, confidentiality, and accessibility of digital evidence while improving the overall efficiency and reliability of cloud-based forensic investigations.

1.3 Objective of the Project

This research sets out to develop a cutting-edge digital forensic framework, "Enhanced Security in Digital Forensics: Secure Storage with Key-Based Encryption," aimed at overcoming the challenges of securing and preserving digital evidence in cloud environments. To strengthen security and reliability, this architecture integrates a Secure Block Verification Mechanism (SBVM) for robust authentication, leverages an Enhanced Equilibrium Optimizer (EEO) model for efficient key generation, and employs Elliptic Curve Cryptography (ECC) for powerful data encryption. By implementing these advanced techniques, the proposed model aspires to surpass existing solutions, ensuring the integrity, confidentiality, and accessibility of digital evidence while improving the efficiency and dependability of cloud-based forensic investigations.

1.4 Scope

This research focuses on developing a secure and efficient digital forensic architecture tailored for cloud environments that addresses challenges in evidence integrity, authentication, and storage. It incorporates a Secure Block Verification Mechanism (SBVM) for authentication, an Enhanced Equilibrium Optimizer (EEO) for key generation, and Elliptic Curve Cryptography (ECC) for encryption. Designed for scalability and adaptability, the architecture aims to support secure and reliable evidence management for forensic investigations, providing improved performance and practical applicability in cloud-based scenarios.

1.5 Project Introduction

As cloud computing continues to reshape the digital landscape, it brings both exciting possibilities and significant challenges for digital forensics. One of the biggest concerns is ensuring the security and integrity of digital evidence, especially in cloud environments where data is constantly changing, widely distributed, and vulnerable to cyber threats. Traditional forensic methods often fall short, lacking the strong security frame-

works and efficient authentication, storage, and retrieval mechanisms needed to handle these challenges effectively.

To bridge this gap, this project introduces a new forensic architecture, "Enhanced Security in Digital Forensics: Secure Storage with Key-Based Encryption," designed to improve the reliability and security of digital evidence management. The system incorporates a Secure Block Verification Mechanism (SBVM) to authenticate evidence blocks, ensuring data remains intact and tamper-proof. An Enhanced Equilibrium Optimizer (EEO) model is used to generate encryption keys efficiently, optimizing key management for better security. Additionally, Elliptic Curve Cryptography (ECC) is employed to encrypt data, providing robust protection while maintaining high efficiency. Encrypted evidence is securely stored on cloud servers, ensuring confidentiality while allowing authorized forensic investigators to access it when needed.

By overcoming the shortcomings of existing approaches, this project aims to create a scalable, secure, and efficient digital forensic framework tailored for cloud environments. Ultimately, it seeks to support investigators with a reliable and future-ready solution, ensuring that critical evidence remains protected and accessible in an ever-evolving digital world.

CHAPTER 2

LITERATURE SURVEY

This literature survey explores key contributions in digital forensic security, encryption, network security, and evidence preservation, providing a solid foundation for the development of a secure forensic architecture.

2.1 Description of research papers and textbooks on forensic science, cryptography and network security

2.1.1 Role of forensic science in criminal justice

Biedermann et al. (2018) [1] examined the evolving role of forensic science within the criminal justice system, highlighting the growing need for advanced forensic techniques to ensure evidence remains reliable and admissible in court. Their research sheds light on the limitations of traditional forensic methods and emphasizes the importance of interdisciplinary collaboration and technological innovation in improving how evidence is analyzed and interpreted.

2.1.2 Design and implementation of FROST

Dykstra et al. (2013) [2] introduced FROST, a specialized set of digital forensic tools designed to support investigations within OpenStack cloud computing environments. Their study underscores the critical need for secure evidence collection, maintaining the chain of custody, and efficiently analyzing data in virtualized infrastructures. By addressing these challenges, FROST set a strong precedent for developing forensic tools tailored to cloud-based ecosystems.

2.1.3 Cryptography and network security

In his book *Cryptography and Network Security* (2016)[3] William Stallings provides a deep dive into encryption techniques, authentication mechanisms, and principles of secure communication. His work is particularly relevant to digital forensics, as it covers essential concepts such as securing evidence, managing cryptographic keys, and maintaining data integrity throughout forensic investigations. These principles play a crucial role in protecting sensitive forensic data and safeguarding systems from cyber threats.

By examining these key contributions, this survey highlights the growing intersection of forensic science, cybersecurity, and cryptography, reinforcing the need for a secure, reliable, and adaptable forensic architecture in the evolving digital landscape.

CHAPTER 3

SYSTEM ANALYSIS

3.1 Existing System

Many existing digital forensic systems rely on Multi-Key Homomorphic Encryption (MKHE) to secure data in cloud environments. This approach allows computations to be performed on encrypted data without needing decryption, ensuring privacy. However, MKHE comes with several challenges. It struggles with scalability and performance issues, especially when handling large datasets or complex operations. Additionally, managing multiple encryption keys adds significant complexity, often leading to slower processing times and potential risks to data integrity.

3.2 Disadvantages

1. **Performance Overhead:** MKHE requires heavy computational resources, which can significantly slow down performance, particularly when dealing with large datasets or intricate operations.
2. **Scalability Issues:** As the number of users and encryption keys grows, the system becomes harder to manage, making it less efficient for large-scale forensic investigations.
3. **Key Management Complexity:** Handling multiple encryption keys increases security risks and complicates processes like key distribution, storage, and revocation.
4. **Limited Efficiency:** While MKHE enables secure computations on encrypted data, it demands more processing power than traditional encryption methods, leading to inefficiencies.
5. **Potential Vulnerabilities:** Despite its privacy advantages, MKHE-based systems can still be exposed to security risks, particularly if key management is weak or if encryption algorithms have flaws.

3.3 Proposed System

To overcome these limitations, the proposed system introduces a **more secure and efficient forensic framework** designed specifically for cloud environments. This approach integrates:

- A **Secure Block Verification Mechanism (SBVM)** to guarantee evidence integrity and prevent data tampering.
- An **Enhanced Equilibrium Optimizer (EEO) model** for generating encryption keys securely and efficiently.
- **Elliptic Curve Cryptography (ECC)** to encrypt digital evidence, ensuring strong security with lower computational overhead.
- Secure cloud storage for encrypted data, allowing both **scalability and privacy protection**.

Simulation results demonstrate that this approach outperforms existing methods in **security, reliability, and efficiency**, making it an ideal solution for modern cloud-based forensic investigations.

3.4 Advantages

1. **Enhanced Security:** By using Elliptic Curve Cryptography (ECC), the system ensures that digital evidence remains protected from unauthorized access and tampering.
2. **Guaranteed Integrity:** The Secure Block Verification Mechanism (SBVM) prevents any unauthorized modifications, ensuring evidence authenticity.
3. **Efficient Encryption:** ECC provides high security with lower computational requirements, improving overall system efficiency.
4. **Smaller Key Size, Greater Efficiency:** ECC uses smaller keys (a 256-bit ECC key is as secure as a 3072-bit RSA key), making encryption and storage more efficient.
5. **Optimized Key Management:** The EEO model enhances encryption key generation, improving security while simplifying management.
6. **Cloud Scalability:** Secure cloud storage allows investigators to access encrypted evidence remotely, without sacrificing security or integrity.
7. **Superior Performance:** Simulations show that this system outperforms traditional forensic methods in security, reliability, and efficiency, making it a future-ready solution for digital investigations.

3.5 Work Flow of Proposed System

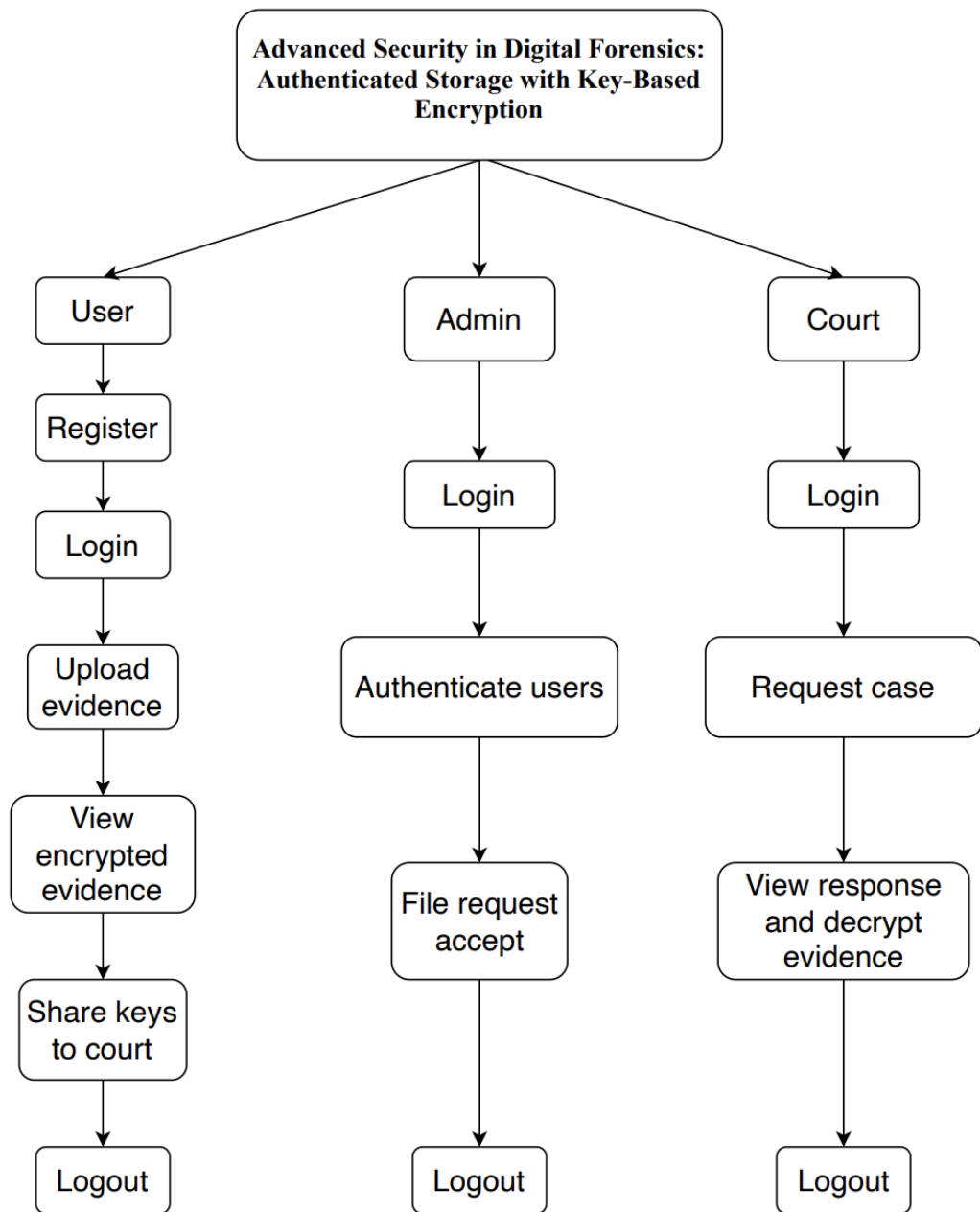


Figure 3.1: Work Flow

CHAPTER 4

PRODUCT DEVELOPMENT PROGRESS

4.1 Proposed Architecture

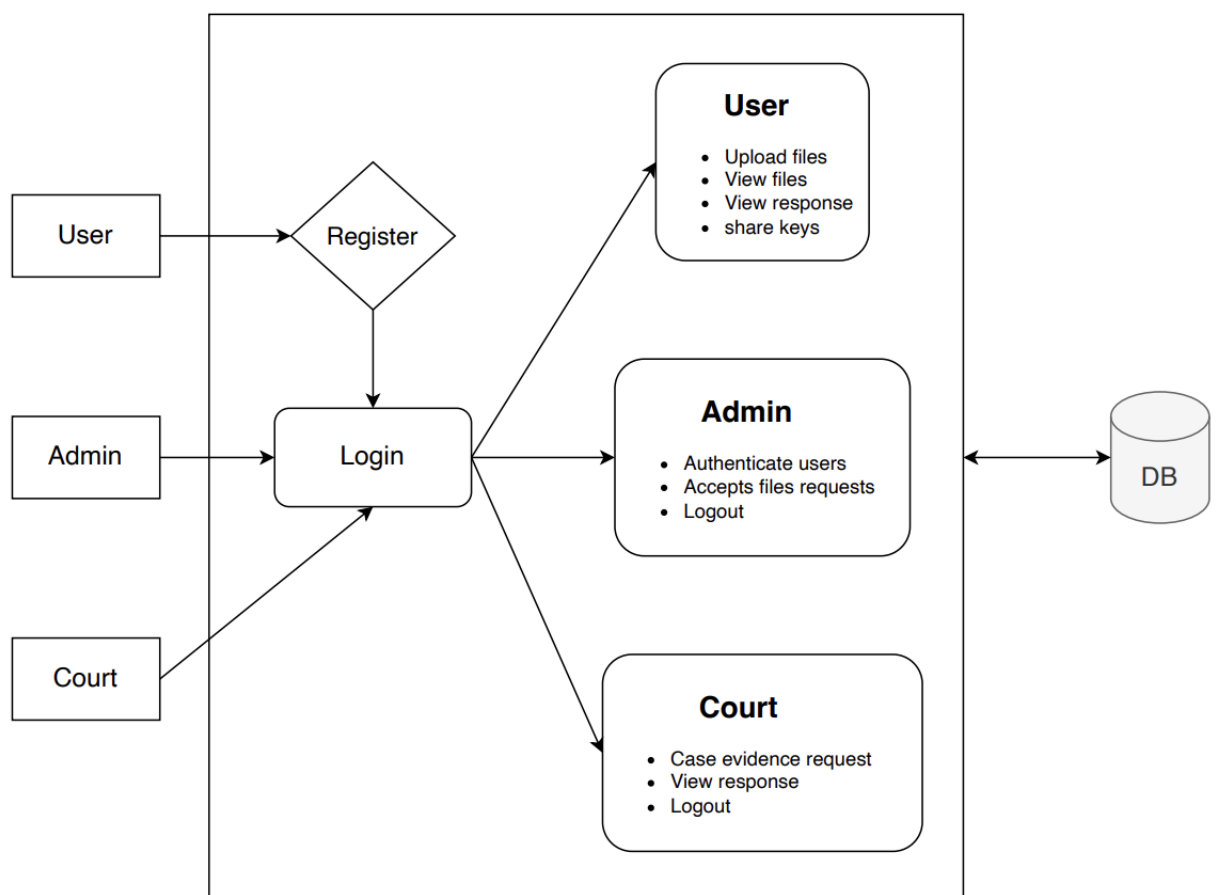


Figure 4.1: Product Architecture

4.2 Implementation Progress

4.2.1 User (Forensic Investigator) Module

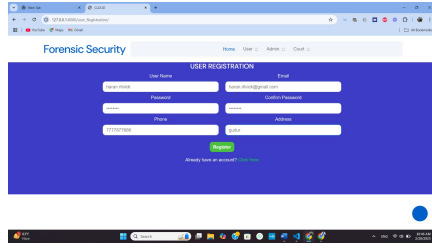
1. **Login:** Investigators log into the system using their credentials.
2. **Register:** Users can register with providing the required information.
3. **Request to admin to share data:** The user of the case should obtain permission from the admin to share evidence information with the court.
4. **Upload Evidence Data:** The case user can able to share the evidence information with the encryption format with the decryption key to the requested court.
5. **Share to court:** Now the user can share the evidence information with the court.
6. **Logout:** The user should be logout.

4.2.2 Admin Module

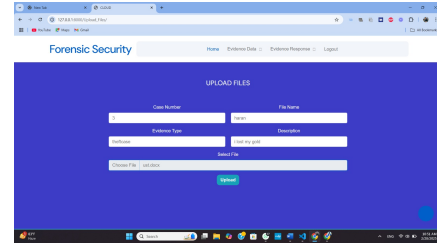
1. **Login:** Admins log into the system using their credentials.
2. **View Users:** Admins view details of all registered users.
3. **Manage Evidence:** Admins oversee the evidence data collection, and storages of that digital evidence.
4. **Logout:** Admin can Logout

4.2.3 Court Module

1. **Login:** Court can login using default credentials.
2. **View the case numbers:** The court can view the case numbers and can request for file access from evidences.
3. **Logout:** the court can logout successfully.

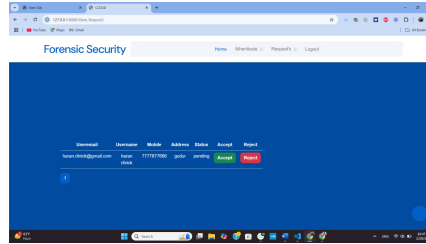


(a) User Registration



(b) Upload Evidence

Figure 4.2: User Registration and Upload Evidence



(a) Admin Authorization

Figure 4.3: Admin Authorization

4.3 Upcoming Implementation Work

4.3.1 Algorithm Analysis

An essential aspect of this project is to explore the possibility of combining Elliptic Curve Cryptography (ECC) with additional cryptographic algorithms. While ECC provides strong encryption with lower computational overhead, integrating it with other encryption mechanisms can potentially improve data confidentiality, integrity, and resistance to cryptographic attacks.

4.3.2 User (Forensic Investigator) Module

1. **View Decryption key response from admin:** The admin should be share the decryption key's to the user for decrypt the data

4.3.3 Admin Module

1. **Monitor Encryption and Key Generation:** Admins supervise encryption and key generation processes to the users.

4.3.4 Court Module

1. **View response:** The court can view the evidence response for decryption key from the case users.


REFERENCES

- [1] A. Biedermann and F. Taroni, “The role of forensic science in the criminal justice system: A reflection on the concept of evidence and the challenges of advancing towards new paradigms,” *Forensic Science International*, vol. 289, pp. e1–e8, 2018.
- [2] J. Dykstra and A. T. Sherman, “Design and implementation of frost: Digital forensic tools for the openstack cloud computing platform,” in *Digital Investigation*, vol. 10, no. S1, 2013, pp. S87–S95.
- [3] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson Education, 2016.

Weekly Review Report

Weekly Review Report

Roll No: CS21B0133
Name: Vemula Haran Ritvick

Week	Start Date - End Date	Work carried out during the week (with Your signature and Date)	Internal guide's comments with signature and Date
1	6/01/2025 - 12/01/2025	Gathered requirements and finalized the project scope.	
2	13/01/2025 - 19/01/2025	Designed the system architecture and work flow	
3	20/01/2025 - 26/01/2025	Developed the User (Forensic Investigator) Module – Login, Registration.	
4	27/01/2025 - 02/02/2025	Implemented Request to Admin for data sharing and studied about the algorithms	
5	03/02/2025 - 09/02/2025	Developed the Admin Module – User management and evidence storage handling.	
6	10/02/2025 - 16/02/2025	Implemented the Court Module – Login, case viewing, and file access request system	
7	17/02/2025 - 23/02/2025	Integrated all modules and tested data flow between User, Admin, and Court.	
8	24/02/2025 - 02/03/2025	Testing, debugging, and finalized the report.	
9	03/03/2025 - 09/03/2025		
	Mid Semester Review Feedback		