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

VEMULA HARAN RITVICK
CS21B1033

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY, DESIGN AND MANUFACTURING, KANCHEEPURAM

Dr. Noor Mahammad SK
Dept. of CSE, IIITDM Kancheepuram

Table of Contents

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		

4/5

Introduction

- **Challenges in Cloud Forensics**
  - Traditional forensic methods struggle with security, integrity, and retrieval of digital evidence in cloud environments due to data distribution and online threats.
- **Proposed Forensic Architecture**
  - Introducing "Enhanced Security in Digital Forensics: Secure Storage with Key-Based Encryption," integrating Secure Block Verification Mechanism (SBVM) and optimized key management.
- **Enhanced Security & Efficiency**
  - Utilizing **Elliptic Curve Cryptography (ECC)** for encryption and an **Enhanced Equilibrium Optimizer (EEO)** for key generation, ensuring strong security, tamper resistance, and scalable cloud-based evidence storage.

Problem Definition

- **Security & Integrity Challenges in Cloud Forensics** – Traditional forensic methods fail to securely collect, authenticate, and store digital evidence in cloud environments, making it vulnerable to tampering, unauthorized access, and cyber threats.
- **Lack of Robust Encryption & Authentication** – Existing approaches lack efficient encryption, authentication, and key management, leading to compromised evidence integrity and reliability, making forensic investigations inefficient and unreliable.
- **Legal & Investigative Importance** – With the increasing volume of cybercrimes, ensuring **tamper-proof, confidential, and accessible** digital evidence is crucial for legal cases, law enforcement, and justice, demanding a scalable and secure forensic solution

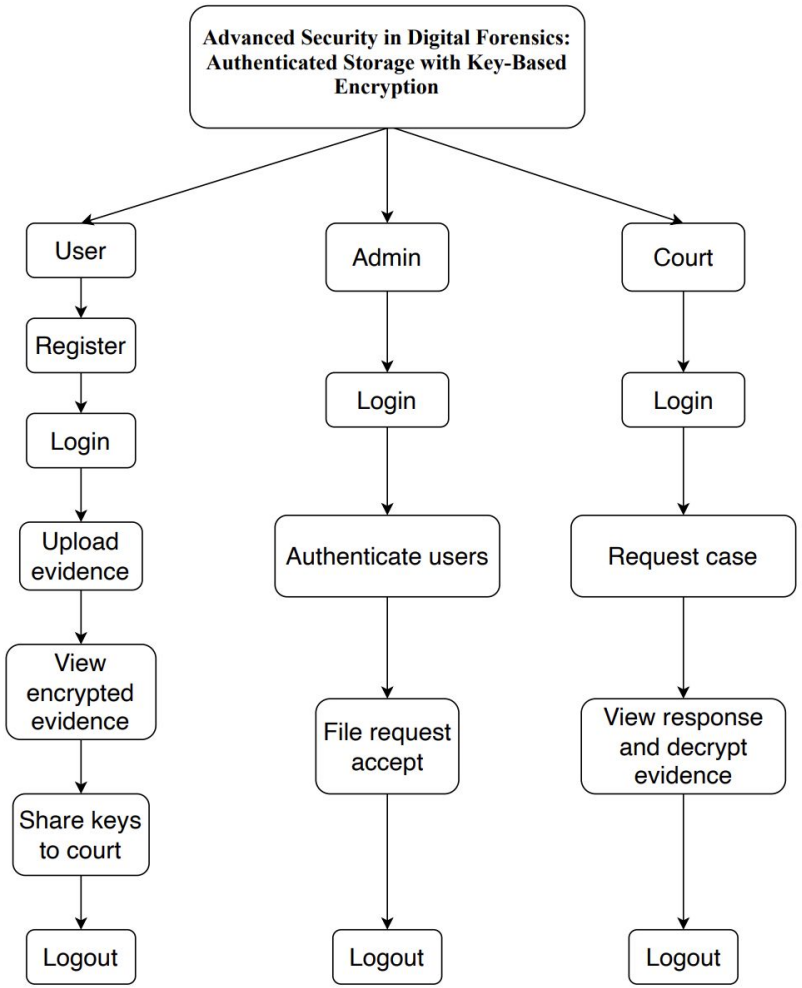
Literature Survey

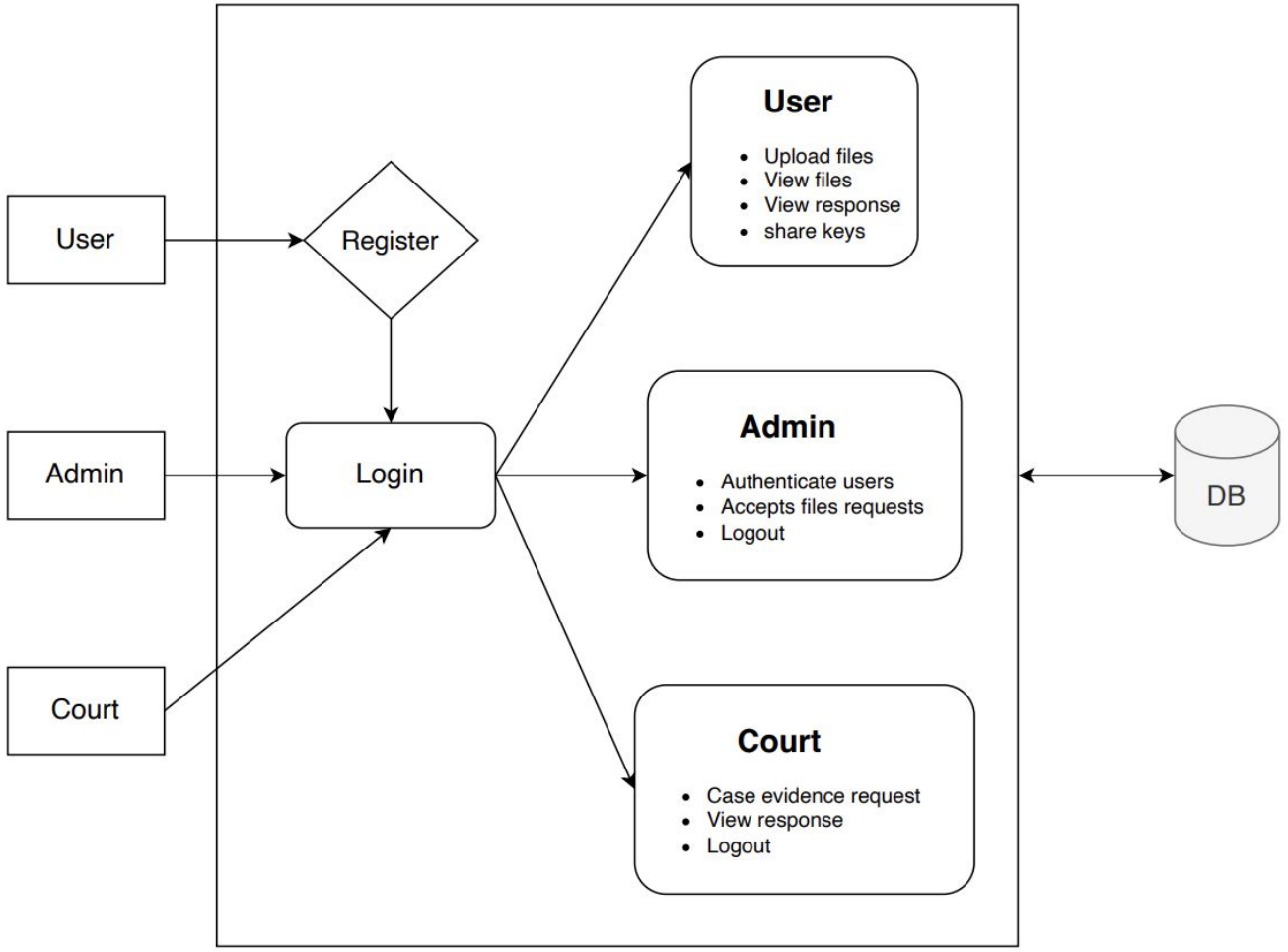
- **Biedermann et al. (2018) " Role of Forensic Science in Criminal Justice"**
  - Highlights challenges in traditional forensic paradigms and emphasizes interdisciplinary collaboration & technological innovations for reliable evidence analysis.
- **Dykstra et al. (2013) "Design and Implementation of FROST"**
  - Establishes a foundation for forensic tools in cloud computing, ensuring efficient data analysis & secure evidence handling in virtualized infrastructures.
- **Mujawib et al. "Improving Digital Forensic Security"**
  - Highlights the key idea to encrypt the data with MKHE encryption algorithm and established the structure/flow to encrypt an evidence.

Work Done

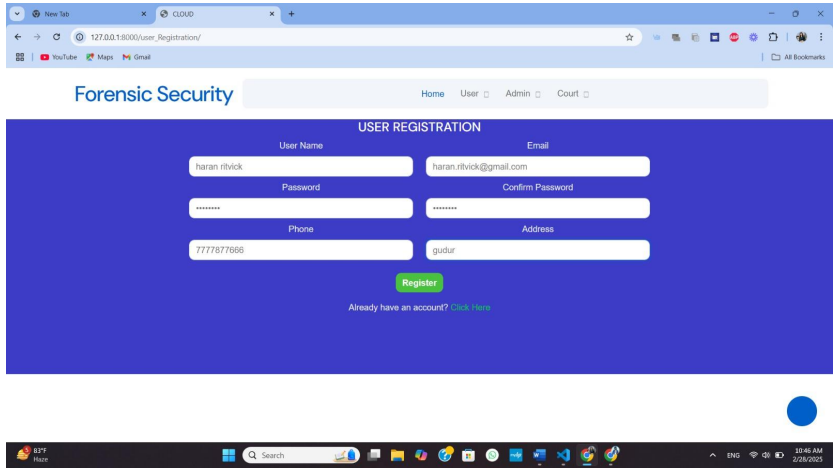
- Designed the workflow and architecture of the project with key structure.
- Implemented the following modules w.r.t features of each module:
- **User (forensic investigator) module:**
  - Login, register, request admin to share data, Upload evidence, share to court, logout.
- **Admin Module:**
  - Login, view users, manage evidence, logout.
- **Court Module:**
  - Login, View case numbers, logout.
- Studied about the MKHE algorithm, SBVM for authentication and EEO for key-generation.

Analysis/ Results

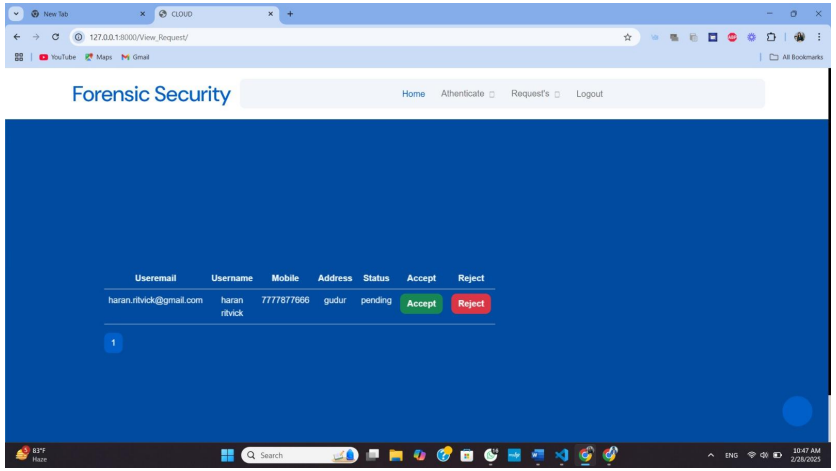




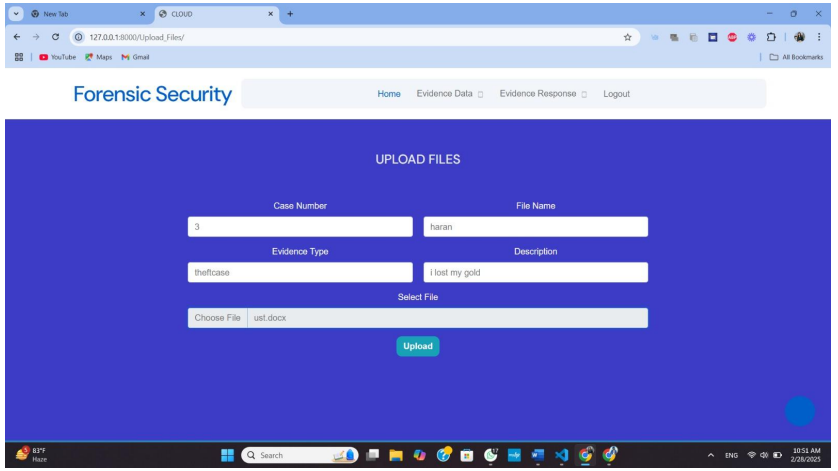
Prototype / Products



User registration



Admin Authorization



User Upload evidence

Conclusion

- **Key Insights from Literature** – Forensic science enhances evidence reliability, FROST ensures secure cloud-based evidence collection, and cryptographic techniques strengthen data integrity and authentication.
- **Integration of Advanced Security Mechanisms** – The proposed forensic architecture leverages SBVM for authentication, EEO for optimized key management, and ECC for strong encryption, addressing security gaps in cloud forensics.
- **Impact** – This research lays the groundwork for a scalable, secure, and efficient forensic framework, ensuring confidentiality, integrity, and accessibility of digital evidence in cloud environments.

Future Work

- Plan for the next two months:
  - Study about different algorithms and its computational complexities.
  - Try out the security by combining different encryption algorithms for better security of the evidence.
  - **User Module:** View decryption key response from admin
  - **Admin Module:** Monitor Encryption and key generation
  - **Court Module:** View the decrypted file.

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.
4. Abdullah Mujawib et. al, “Improving Digital Forensic Security”, IEEE, 2024

Thank You

Any Questions?