Evidence Integrity Management System

Dr. Praveen Kumar P[1], Venkatesh Kannan M S[2], Sri Vignov PandianP S[3], Raj FlintoffS[4]
[1, 2, 3, 4] Dept of Computer Science and Engineering
[1, 2, 3, 4] Kamaraj College of Engineering and Technology, Virudhunagar.

Abstract- *In criminal investigations, evidence of the case serves as major element for final decision in any case. So, these evidences are usually, stored in physical medium method which is called traditional method. Due to long period of duration in the investigation court pending case files which were easily affect by the climate condition or over the time period the paper is not eligible to read. In order to overcome this issue, the existing methodology is maintaining the evidence in the digital form and store it into the server. But it requires more investment on the storage and scalability of the digital data. Alternatively, Cloud computing facilitates to store and access the data remotely over the internet. However, storing the data in the untrusted cloud server leads the privacy and integrity issues in the cloud. Hence, we have proposed a scheme Evidence Integrity Management System that ensures the privacy and integrity. In our scheme, the digital data is stored in the cloud server which is protected by the AES encryption technique. The SHA hash function which is used to maintain the integrity of the evidence. It gives a safe and secure data storage (Evidence history) which can be used for prolong years (future) until the case closed. Security analysis shows our scheme is secure and it maintains the privacy and integrity of the evidence.*

Keywords- Cloud, Encryption, Hash, Privacy, Integrity.

I. INTRODUCTION

Evidence serves as the backbone of the criminal justice system, playing a crucial role in establishing facts, supporting prosecution or defence, ensuring fairness, protecting innocent individuals, guiding investigations, building public trust, and deterring future criminal behaviour. It provides factual information about the crime, aids in proving guilt or innocence, and helps investigators piece together the sequence of events. Moreover, evidence safeguards against miscarriages of justice, guides the direction of investigations, and reinforces societal norms [1]. A transparent and evidence-based approach to criminal investigations builds public trust in law enforcement agencies and serves as a deterrent to potential offenders. Ultimately, evidence is indispensable in ensuring justice, maintaining public safety, and upholding the integrity of the criminal justice system.

Traditional methods of storing physical evidence in criminal investigations have their downsides alongside their benefits. Firstly, there's a risk of contamination or deterioration of evidence over time, especially if not stored properly. Secondly, access to evidence may be limited due to centralized storage facilities, leading to delays or logistical issues. Additionally, space constraints in these facilities can pose challenges as evidence accumulates. There's also a possibility of misplacing or losing evidence due to manual record-keeping systems. Despite security measures, traditional storage methods may still be vulnerable to tampering or theft. Moreover, maintaining these storage facilities requires significant resources, including space, personnel, and infrastructure. Lastly, these methods often lack integration with modern technology, resulting in inefficiencies and missed opportunities for improvement. Overall, while traditional methods have their advantages, addressing these drawbacks may require enhancements in protocols, technology integration, and resource allocation. So that the new technique which is known as cloud computing was introduced in the field of storage [2,3].

The cloud delivers the variety of services such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) to cloud users. SaaS provides the application to the user such as webmail, program interface, and web browser. PaaS provides the programming languages, libraries, services, and tools, etc. IaaS provides the infrastructure, such as storage, networks, and other processing and computing resources. There are various deployment models such as private, public, community, and hybrid cloud. Private cloud is owned by a single organization, whereas the public cloud is shared by multiple consumers. Community cloud means the same kind of community consumers can join and use this service. Hybrid cloud is the combination of any two above said deployment models of the cloud. Based on the user need and requirement, the user may choose specific services and deployment model. In which the evidence of case files can be stored. So that the existing digital storage of data is stored in computing mechanism. Which can accessible from anywhere. The cloud computing offers the ability to store the data in the limitless storage [3,4,5]. It contributes the solution for the main issue of the storage problem. But the major issues are the privacy and integrity of data in evidence. Which can be easily manipulated and the unauthenticated user’s access. To overcome the issue, we are going to use the Evidence Integrity Management System.

The following are the major contribution of our scheme:

- The AES encryption algorithm [6, 7] is used to encrypt the evidence and upload the same into the cloud to maintain the privacy of the evidence.
- To ensure the integrity of evidence, SHA hash value [11] is used. Before accessing the evidence, the hash value is checked with the original hash value. If it same, we conclude the integrity of the evidence.
- Security analysis shows that our scheme is secure and maintains the privacy and integrity of evidence.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

In this section, we present the different related research works. Berta et al. [1] proposed they respond to recent calls for increased use of evidence-based management (EBM) This will be helpful to know the reason for the importance of evidence in the criminal case history and its also includes about the survey of digital evidence should be stored in the limited access storage. Arab et al. [2] proposed a novel image encryption algorithm is proposed based on the combination of the chaos sequence and the modified AES algorithm. Then, the original image is encrypted using the modified AES algorithm and by implementing the round keys produced by the chaos system. Ele et al. [3] proposed Charm an extensible framework for rapidly prototyping cryptographic systems. This paper describes our modular architecture, which includes a built-in benchmarking module to compare the performance of Charm primitives to existing C implementations.

Waters et al. [4] proposed GPU is continuing its trend of vastly outperforming CPU while becoming more general purpose. In order to improve the efficiency of AES algorithm, this paper proposed a CUDA implementation of Electronic Codebook (ECB) mode encoding process and Cipher Feedback (CBC) mode decoding process on GPU. From this we clearly know about the efficiency of the AES. Xing et al. [5] proposed several distributed systems a user should only be able to access data if a user possesses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. From this policy the encryption techniques were developed through this the AES is developed.

Abdullah et al. [6] proposed Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithm used in worldwide. This algorithm has an own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. Till date is not any evidence to crake this algorithm. Pawar et al. [7] proposed Cloud computing is the apt technology for the decade. It allows user to store large amount of data in cloud storage and use as and when required, from any part of the world, via any terminal equipment. Since cloud computing is rest on internet, security issues like privacy, data security, confidentiality, and authentication are encountered.

Ramesh et al. [8] proposed in cloud computing distributed resources are shared via network in open environment. The proposed model uses Short Message Service (SMS) alert mechanism for avoiding unauthorized access to user data. Dwivedi et al. [9] and Shukla et al. [10] proposed exponential growth of cloud computing, an efficient data security system becomes essential for cloud computing-based environment. The proposed algorithm has been compared with various other traditionally used popular encryption algorithms primarily including DES, AES, Blowfish as well as proposed algorithm. Dida et al. [11] and Imam Riad et al. [12] proposed report is on the Secure Hash Algorithm family, better known as the SHA hash functions. The result of UAT shows the result agreed and strongly agree with 86, 00%. From this we can clearly get idea about the SHA hash which can be implemented in our work

III. PROPOSED SOLUTIONS

In this section, we explain the system model and flow of the proposed work Evidence Integrity Management System. In the proposed work, there are four entities available such as Evidence Custodian, Data Users, Data Owners and Cloud Server.

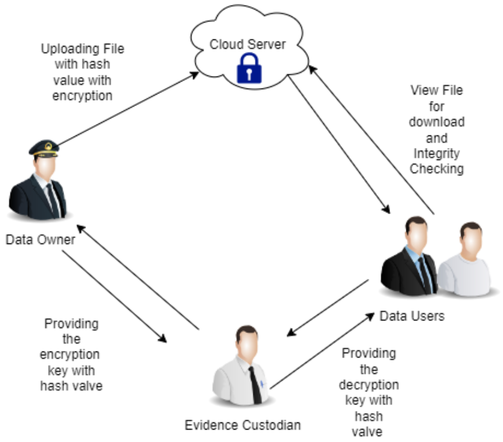

Cloud Server
Uploading File with hash value with encryption
View File for download and Integrity Checking
Data Owner
Data Users
Providing the encryption key with hash valve
Providing the decryption key with hash valve
Evidence Custodian

Figure 1 System Model

Figure 1 describes the proposed system model and work flow. The detailed responsibility of the System Model is explained with role of their entities in below

Evidence Custodian: The Evidence Custodian is the person one who involved in the providing the encryption and decryption key for the Data Owners and Data Users. The evidence custodian creates the new case file with case id and they allow the users does they have the rights to view the file through providing user id. This person generates the key for the encryption of the file to upload with hash value and it's also generating the key for the decryption of the evidence file with hash value. Encryption key is provided to the Data Owner for upload of the evidence file with hash value. Decryption key is provided to the valid Data Users if they have the rights to view the file to download the evidence file with hash value.

Data Owner: The data owners are those who uploads the files of the evidence in the cloud server. The Data Owners (lawyer, police, doctor, etc…. and those who are all involved in the case for the evidence collection). After signing into authorized user login, it shows evidence upload. There the respective user id and case id is to be entered. Then the necessary evidence file uploaded. These users' role is to upload the evidence files in the cloud server with hash valve respectively. These data owners get the encryption key for the evidence files from the Evidence Custodian and Data Owners uploads the encrypted files.

Data Users: The data users are used to get access from the Evidence Custodian. These users are the mostly in the panel of the court. These users get decryption key from the Evidence Custodian. After signing into authorized user login, it shows evidence download. There the respective case id is to be entered. Then the necessary evidence file can be downloaded. These users download the encrypted file with hash valve and decrypt the file to view. They check with hash valve with the decrypted hash valve in the file to ensure the data integrity.

Cloud Server: The case files which are stored in the cloud server with encryption. This part acts as the storage medium. From Cloud Server the users can upload the files and download.

In this section we have proposed that Our work Evidence Integrity Management System have three algorithms Evidence Upload algorithm, Evidence Download Algorithm and Key Generation Algorithm.

Evidence Upload Algorithm

The Evidence file uploaded by the Data Owner to the Cloud Server. After signing into authorized user login, it shows evidence upload. There the respective user id and case id is to be entered. The Data owners get the encryption key from the Evidence Custodian with hash valve for the uploading of the evidence file. The evidence file is encrypted and upload with hash valve from the Data Owner. These steps are explained in the following Algorithm describes the Evidence Upload Algorithm.

Evidence Upload Algorithm

1) Data owner holds the evidence files.
2) Sign in to the User Login.
3) Enter the user id and case id.
4) Creates a random secret key for the encryption of file by the Evidence Custodian.
5) Data owner encrypts the file with hash valve.
6) Upload the encrypted file with hash valve in cloud server

Evidence Download Algorithm

The Evidence file is download by the Data Users from the Cloud server. The Evidence Custodian give only key access for the valid users to view the data. After signing into authorized user login, it shows evidence download. There the respective case id is to be entered. The key is used to download the encrypted file with hash valve. After the decryption of the file the hash valve is compared with the encryption file hash. If the valve matches the data integrity of the file is proved. These steps are explained in the following Algorithm describes the Evidence Download Algorithm.

Evidence Download Algorithm

1) Data user sign in with user id
2) Data user gets the decryption key with hash value for download the file from Evidence Custodian.
3) Decrypts the file with hash value.
4) The hash value with compare the hash value which is the for the encryption of the file.
5) If the hash value is same then it's the proof for the data integrity.

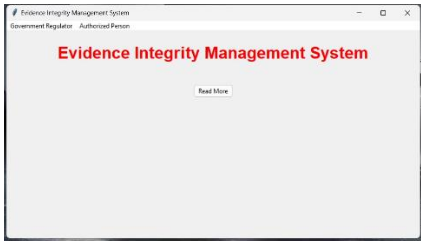
Key Generation Algorithm

The Evidence Custodian is the middle person develops the key for the encryption and decryption with hash value. These steps are explained in the following Algorithm describes the Key Generation Algorithm.

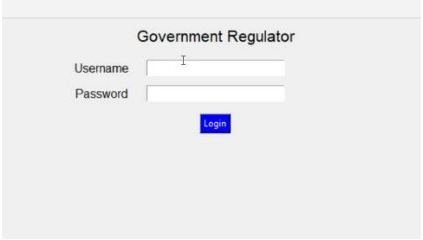
Key generation Algorithm

1)Evidence Custodian creates the new case id for the case file.
2)Evidence Custodian creates user id for the user to view the case file.
3)Evidence Custodian gives the encryption key with hash value for the Data Owner.
4)Data owner uploads the encrypt case file with the user id login.
5)Data Users downloads the encrypt case file with the user id login and decrypts

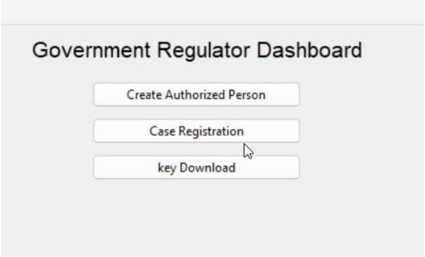
IV. RESULT


Evidence Integrity Management System
Government Regulator
Authorized Person
Evidence Integrity Management System
Read More

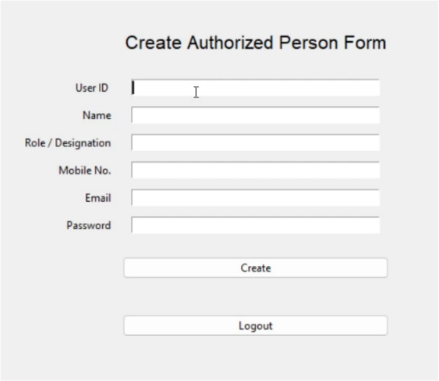
1.Home



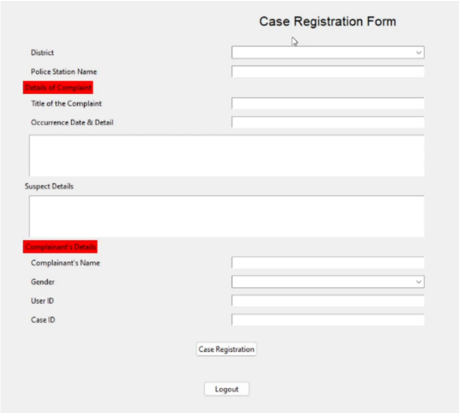
2.Gov Reg page login



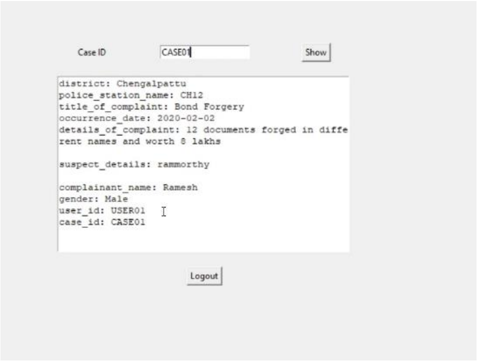
3.Gov Reg Dashboard



4.Create auth person



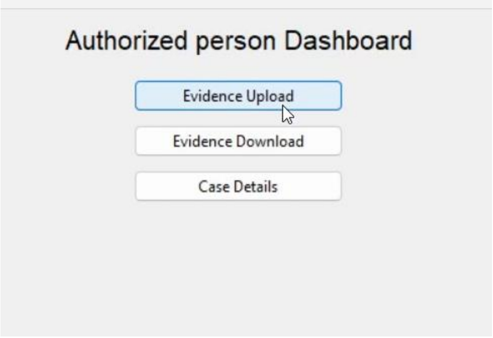
4.Case Reg form



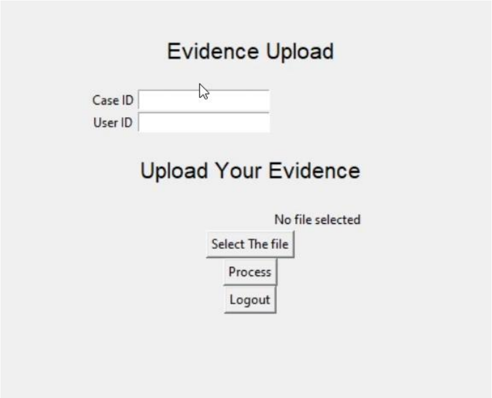
Case ID CASE01

```
district: Chengalpattu
police_station_name: CH12
title_of_complaint: Bond Forgery
occurrence_date: 2020-02-02
details_of_complaint: 12 documents forged in diffe
rent names and worth 8 lakhs

suspect_details: rammorthy

complainant_name: Ramesh
gender: Male
user_id: USER01
case_id: CASE01
```

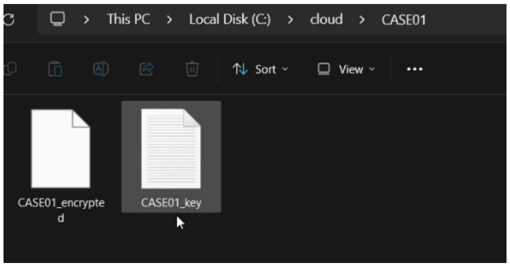
5.case details check



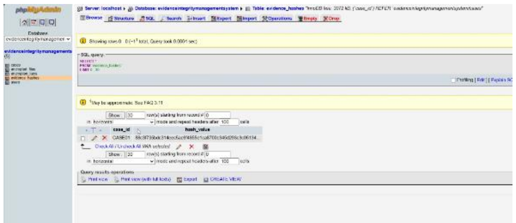
6.authorized person login



7.Authorized person dashboard Evidence upload



8.Evidence Upload Page



Server: localhost ▸ Database: evidenceintegritymanagementsystem ▸ Table: evidence_hashes

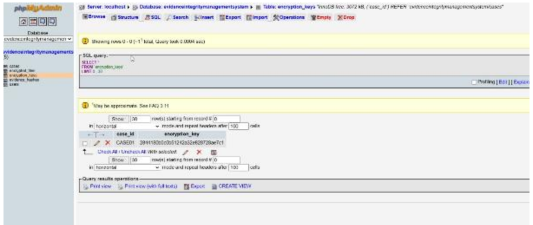
Showing rows 0 - 0 (~1 total, Query took 0.0001 sec)

SQL query:

```
SELECT *
FROM `evidence_hashes`
LIMIT 0 , 30
```

case_id	hash_value
CASE01	88c3f735bdc314ecc5a0f4855c1ca8700c345d2f3c3c06134...

9. Encrypted key and file location



Server: localhost ▸ Database: evidenceintegritymanagementsystem ▸ Table: encryption_keys

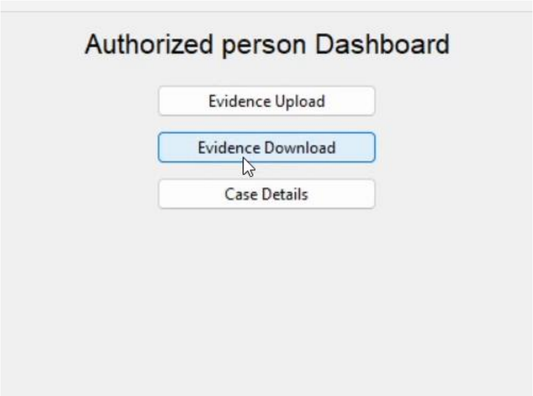
Showing rows 0 - 0 (~1 total, Query took 0.0004 sec)

SQL query:

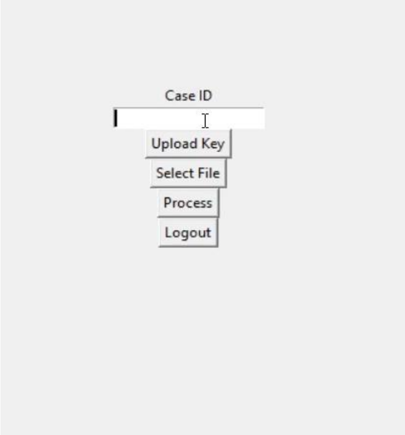
```
SELECT *
FROM `encryption_keys`
LIMIT 0 , 30
```

case_id	encryption_key
CASE01	2844180b0c0b51242a32e828728ae7c1

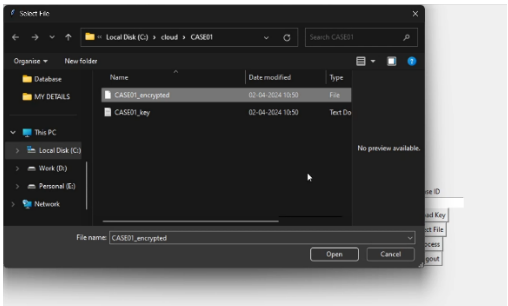
10.Hash stored in database



11. Encryption key stored in database



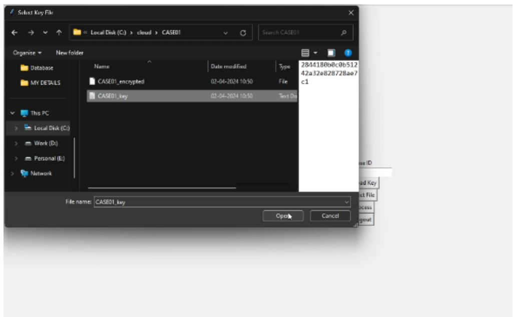
12. Authorized person dashboard evidence downloads



Name	Date modified	Type
CASE01_encrypted	02-04-2024 10:50	File
CASE01_key	02-04-2024 10:50	Text Do

File name: CASE01_encrypted

13. File decryption page

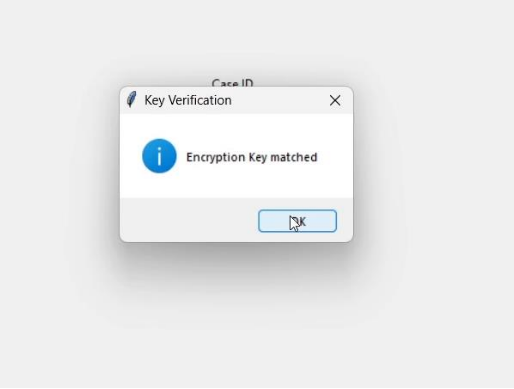


Name	Date modified	Type
CASE01_encrypted	02-04-2024 10:50	File
CASE01_key	02-04-2024 10:50	Text Do

2844180b0c0b512
42a32e828728ae7
c1

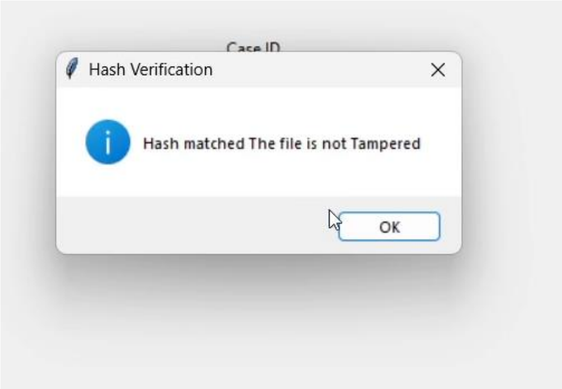
File name: CASE01_key

14. Encrypted file upload



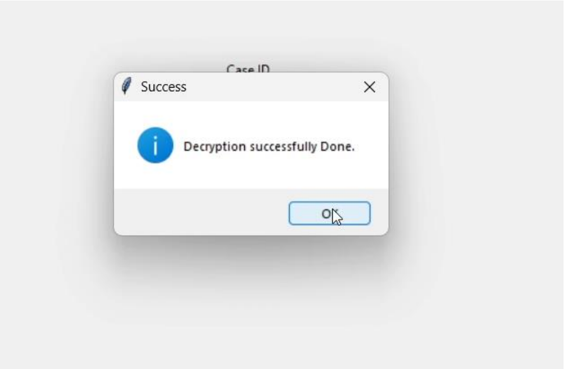
Encryption Key matched

15.key upload



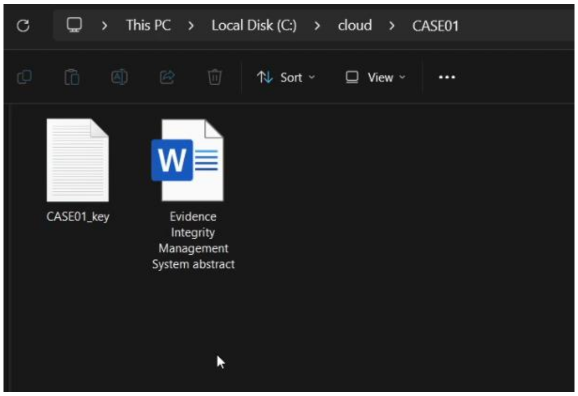
Hash matched The file is not Tampered

16. Hash value match



Decryption successfully Done.

17. Encryption key match


This PC > Local Disk (C:) > cloud > CASE01
Sort
View
CASE01_key
Evidence Integrity Management System abstract

18.Decrypted file.

V. CONCLUSION

The implementation of an evidence management system in cloud computing with AES encryption for security and SHA hash function integration presents a robust solution to address the challenges of access control, privacy and authenticity in digital evidence management. By leveraging cloud infrastructure, organizations can benefit from scalable storage and computational resources while ensuring data accessibility and reliability. The utilization of AES encryption adds an additional layer of protection, securing sensitive information against unauthorized access and ensuring compliance with privacy regulations. AES encryption's strength and reliability make it an ideal choice for safeguarding digital evidence from malicious threats and unauthorized modifications. Furthermore, the incorporation of a SHA hash function enhances the system's capability to detect subtle changes in digital evidence, thereby enabling efficient and accurate identification of duplicate files and tampered data. Overall, the integration of AES encryption and SHA hash functions within a cloud-based evidence management system not only enhances access control and privacy but also streamlines digital forensic processes, empowering organizations to effectively manage and analyse digital evidence while upholding the highest standards of reliability and trustworthiness.

I. REFERENCES

[1] Whitney Berta and Melanie Kazman Kohn “What's the Evidence on Evidence-Based Management?” Academy of Management Perspectives Vol. 23, No. 4, 2017.

[2] Alireza Arab, Mohammad Javad Rostami and Omar Behnam Ghavami, “An encryption method based on thechaos system and AES encryption” The Journal of Supercomputing Vol. 75, No.6663 - 6682, 2016.

[3] Akinyele JA, Garman C, Miers I, Pagano MW, Rushanan M, Green M, “Charm: a framework for rapidly prototyping cryptosystems” The Journal of Cryptographic Engineering Vol.3, No.111 – 128, 2013.

[4] Bethencourt J, Sahai A, Waters B, “: Security and privacy” Ciphertext-policy attribute-based encryption, IEEE Symposium on Security and Privacy (SP '07),2007.

[5] Qinjian Li, Ming Zhang, Xing Xu, “Implementation and Analysis of AES Encryption on GPU” IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems, 2012.

[6] Ako Muhamad Abdullah, “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data” The Journal of Cryptographic and Network Security, 2017.

[7] Prashant Rewagad, YogitaPawar, “Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Use of Digital Signature with Diffie Hellman Computing” International Conference on Communication Systems and Network Technologies ,2013.

[8] Babitha M. P, K. R. Ramesh Babu, “Secure cloud storage using AES encryption” International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 2016.

[9] Dhirendra KR Shukla, Vijay K.R. Dwivedi, “Encryption algorithm in cloud computing” The Journal of Materials Today: Proceedings, 2021.

[10] Saurabh Singh, Young-Sik Jeong, “A survey on cloud computing security: Issues, threats, and solutions” Journal of Network and Computer Applications Volume 75, November 2016, Pages200-222,2016.

[11] WouterPenard, Tim van Werkhoven, “On the Secure Hash Algorithm family” Cryptography in context, 2008•blog.infocruncher.com, 2009.

[12] MeilianaSumagita, Imam Riad, “Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application” International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(4): 373-381 The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001, 2018.