IJDI-ERET

INTERNATIONAL JOURNAL OF DARSHAN INSTITUTE ON ENGINEERING RESEARCH AND EMERGING TECHNOLOGIES
Vol. 11, No. 2, 2022
www.ijdieret.in

(Review Article)

# Proxy Re-Encryption based Approach for Digital Evidence Management in Cybercrime Investigation - A Review

**Rachana Y. Patil[1*], Yogesh H. Patil[2]**

[1*]*Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, Maharashtra, INDIA*
[2]*Department of Instrument Engineering, D. Y. Patil Institute of Technology, Pune, Maharashtra, INDIA*

***Abstract***

*Cybercrime is on the rise as the digital world continues to expand. Gathering legitimate evidence is what digital forensics is all about. In a legal context, such proof is essential since it demonstrates the victim's crime beyond a reasonable doubt. It is crucial to keep evidence using a good evidence management system to ensure its admissibility in court during trials. We suggest a proxy re-encryption system that only works in one way for delegating power. The suggested approach will provide the safe delegation of access to electronic evidence. Proxy re-encryption as a means of incorporating access control into a secure evidence management solution is validated by the re-encryption scheme's enhanced sense of security. Within this study, we compare and contrast the many different systems that have been presented over the years. Future proposals for improved evidence handling could benefit from this investigation.*

*Keywords: Chain of Custody, Cybercrime, Digital forensics, Digital Evidence, Proxy Re-encryption*

## 1. Introduction

In any nation's judicial system, the law is a crucial component. Peace and harmony are easier to preserve as a result. When an individual commits an act that is deemed illegal by a government or other authoritative body, they have committed a crime. There is constantly an increase in both the variety and incidence of crime due to the proliferation of new technologies and other factors [1-2]. This adds to the already heavy burden placed upon law enforcement at all levels. Proving the facts or convicting the guilty party relies heavily on evidence. As the volume of work rises, it becomes more challenging to monitor and manage the evidence because of the increased likelihood of mistakes being made and of the evidence being tampered with. Mistaken convictions and repercussions would result. As a result, protecting the honesty and veracity of the evidence is essential. As per NCRB India, the number of cybercrime cases recorded is substantially higher than the number of arrests made. Due to insufficient evidence management, this discrepancy exists. Figure 1 shows the increasing trend of the number cases reported over the past years.

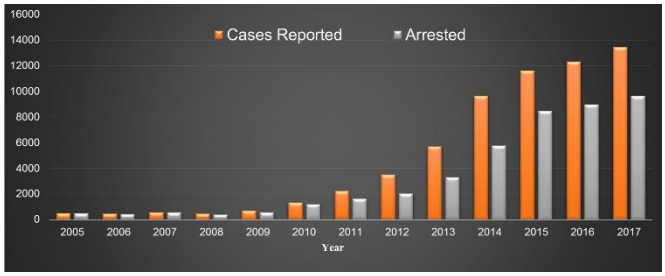


**Figure 1.** Statistics of cybercrime cases in India

Due to increment in cases, we can observe some evidence mishandling, evidence tempering cases which leads to incorrect result in court of law.

The motivation behind this work is to develop a solution which will manage a complete evidence life cycle from evidence collection to court trials. Our project will provide transparency, auditability, speed and accuracy in evidence management.

Given the complexities of dealing with digital evidence, it is important to keep track of it at all times. The term "chain of custody" (CoC) refers to the chronological record of the handling of evidence from its initial acquisition through its eventual presentation in court. It is a useful tool for keeping tabs on who now possesses the evidence and for verifying their claims to it. CoC relies heavily on evidence documentation in order to keep track of changes and ownerships, hence preventing evidence contamination. Information such as the

[*]*Corresponding Author: e-mail: rachana.patil@pccoepune.org, Tel-+91-9421307607*
ISSN 2320-7590 (Print) 2583-3863 (Online)

issuing jurisdiction, the date and duration of the evidence's issuance, the medium upon which the evidence is kept and transferred, and the medium and time stamp of the transfer itself are all recorded. The actor, a detective in this case, issues evidence, records it, and then turns it over to secure storage. For the sake of a thorough investigation, it is essential that all records of these dealings be kept in pristine condition. Forensic investigators should know the full history of the digital evidence they're working with, including where it was found, how it was collected, who handled it, when it was handled, and so on, and this is why chain of custody and evidence integrity play such a crucial role in the digital forensics process.

The objective of this work is twofold, one to maintain the integrity and authenticity of evidences from collection till verification. Second, to develop the system for maintaining chain of custody according to the guidelines given in Indian Evidence Act Section 65(B).

## 2. Related Work

In [4], the authors propose a blockchain-based system for establishing a traceable chain of custody and protecting the authenticity of evidence as it is passed from one user to another. In this case, the evidence is encrypted with a hash produced by the Base64 algorithm before being sent to the recipient, who then decodes it to obtain the unencrypted evidence. The Base64 approach is ideally suited since it can encrypt media assets (including audio, pictures, and video) into String format, making them suitable for uncompressed transfer over the network. Through the usage of chain code, the system validates a transaction by communicating with an application and the blockchain ledger.

In [5], the authors propose a model built on blockchain Technology that safeguards evidence from malicious third parties. Each block in the chain includes the cryptographic hash of preceding block to ensure the integrity of the entire chain. This model implements the Chain of Custody method, which protects the data, guarantees the evidence's authenticity and security, and prevents any tampering with the data or the evidence. Components that communicate with one another make up the system's implementation. The fundamental modules are responsible for enacting the primary alterations to the blockchain ledger. Participants are bound by an agreed-upon consensus and linked by a decentralized ledger called a blockchain. For authorized users, the implementation of the chain of custody in blockchain ensures safety, integrity, and authenticity.

In order to provide complete transparency throughout the inquiry process, the authors of [6] offer a reliable time stamping technique for digitally signing evidence. The time stamp, which is received from a trusted third party, serves as further proof of who accessed the evidence and when. From the input, the hashing function outputs a one-of-a-kind number, or hash value. Each piece of evidence receives its own unique hash value, which is then transmitted to a time stamp authority and signed using a private key before being returned to the client. To ensure the accuracy of the time stamp, it is checked against a public key and then saved locally. This system relies on an external source to generate a timestamp due to the high degree of difficulty involved in doing so internally.

Many countries have unique procedures for the Chain of custody and the writers of [7] help to explain such procedures. Implementing this involves incorporating multiple layers in the technical realm, which in turn brings transparency, legitimacy, and legality. There are two components to this system's execution. First, there are the protections built into procedures that guarantee openness and confidentiality. Second, the accountability mechanisms that are built into the system are a direct result of the data protection precautions. The data is encrypted from the beginning of the process until it reaches the court of law, where the encryption key is revealed.

The following is a suggestion made by the authors of [8]. These days, it's possible to get more out of your gadget thanks to developments in battery life and portability. So it's a bit of a challenge to keep digital evidence safe. In order to gather, preserve, and analyze digital evidence without compromising its veracity or security, this research makes use of block chain technology. A proof-of-concept implementation of hyper ledger composer has been developed and is being used. If digital evidence is authentic, complete, reliable, and credible, it will be admitted into court as valid evidence. Technical aspects for admissibility as digital evidence, such as transparency and explain ability, must also be met. The goal is to create a private block chain using hyper ledger to record the handling history of digital evidence from the perspective of the Creator, the forensic investigator, the prosecutor, the defense, and the court.

This hypothesis is proposed by the authors of [9]. This research will oversee the complete evidence flow, from the initial collecting of evidence by police investigators to the final verdicts rendered by juries, because the current system enforces a weak security paradigm. Jurors can cast their votes privately depending on the evidence presented, and the results will be recorded and used in reaching a verdict. The primary goal of this research is to create a system for the safe and efficient processing of evidence from the first police inquiry through any subsequent court proceedings.

In [10], the authors suggest a study that would create a proof-of-concept blockchain-based system to guarantee legal agreements. Digital evidence will be received, stored, and managed by this program. Users should refrain from doing anything that might change the results of the study. In the event of a change, he would have to brief the relevant authorities on the ramifications of the shift.

The following is a suggestion made by the authors of [11]. Current evidence management systems tend to be centralized and easily manipulated. In light of this propensity for pre-trial manipulation, such evidence is highly suspect. Therefore, the authors have developed a workaround based on blockchain technology, constructed on a private Ethereum, and ensuring the integrity of a Chain-of-Custody (CoC) (viz. a log file used to store the chronological sequence of the evidence collection). The author's primary concerns are keeping the evidence secure, making sure it can be used in court, and limiting access to it to the appropriate parties. They got there by using the Raft Consensus Algorithm. In contrast to other algorithms, the Raft algorithm is relatively sluggish (IBFT).

The authors of [12] are leveraging blockchain technology and the Chain-of-Custody in an effort to keep digital evidence trustworthy and untampered with. The method basically works by storing evidence in blocks, with each block including the cryptographic hash value of the prior block. The writers made an effort to pay special attention to the reliability of the evidence. The evidence management process is made more trustworthy and transparent by the writers of [13]. The suggested system must provide the features they require, such as. Digital Evidence Inventory is a data repository built on the blockchain protocol, and it is used to gather evidence digitally. This cannot be changed, and anyone with internet connection can use DEI. In forensics, the reliability of the evidence is evaluated using a confidence rating. Digital world timeline that shows evidence in chronological sequence. Consequently, their approach improves the credibility of evidence presented in court or by investigators.

In [14], the authors implement a Chain-of-Custody system utilizing blockchain technology. Their infrastructure is based on Ethereum and has a blockchain Digital Evidence Bag (B-DEC). The following notion is proposed by the authors of [15]. In most cases, gathering evidence is the first step of an investigation. Officials analyze the facts to determine what likely occurred and why. By recording the evidence in a distributed ledger, it becomes impossible to alter it. Additional admissible evidence in legal proceedings is necessary [16-17]. With the approach outlined in this article, each authorized party can see the relevant information with minimal effort. For the purposes of Chain-Of-Custody, it is useful. To ensure the database is safe, clear, and tamper-proof, it issues a unique identity to each user who logs in.

In order to improve the opaque nature of CoC, the authors of this research [18] propose using a blockchain-based solution. A timestamp and cryptographic hash of the previous block are recorded in each block. One of the three main forms of blockchain was considered for use here by the author. The public blockchain, which is fully dispersed since each node verifies each transaction, is a type of blockchain. Private or permissioned blockchain, which can process transactions at a lower cost and in a shorter amount of time than public blockchain. Not only are only approved users able to access them, but all transaction information is kept confidential. The idea of proxy re-encryption was proposed in [19], and it was implemented using a safe file system. Using a centralized access control system, it manages who can read encrypted data stored on dispersed replicas. With the goal of facilitating centralized access control without giving the access control server full decryption capabilities. The main server in a distributed system can now act as a proxy, which is a huge improvement.

In this study [20], the authors evaluate the naturally occurring secure access delegation rights and propose implementing Proxy Encryption as a cryptographic solution to make the system efficient and practical.

Delegating the ability to decrypt data to an application is facilitated by this tool. Proxy re-encryption, Identity-based re-encryption, Type-based re-encryption, Attribute-based re-encryption, Key-private re-encryption, and Threshold-based re-encryption are just some of the data encryption methods that the authors of [21] have investigated. Data security was a primary concern, thus a number of cryptographic methods were employed to ensure confidentiality, authenticity, and integrity, and authorization was handled in the cloud. It is important to encrypt data before sending it over a network. In [22-24], the authors presented a Hyperledger Fabric-based infrastructure in which blockchain participants or entities themselves are responsible for administering access permissions, identity verification, and other security-related tasks. The system's emphasis on user and institution anonymity is a major selling point. It aids in making data more trustworthy and secure.

## 3. Proposed System

The system architecture of proposed system is illustrated in figure 2. The two main steps in the proposed system are encryption and Re-Encryption are discussed in this section.

### *3.1 Process of encryption:*

- Evidence Owner would like to store the evidence.
- First step is to register the evidence into the blockchain. A transaction record will be stored into the blockchain.
- Now the owner will encrypt the evidence
  - Owner’s identity, private key and timestamp to given to encryptor.
  - Encryptor will generate the output C. This will be stored into the secured cloud storage.

### *3.2 Process of re-encryption:*

- The investigator would like to have access to the Evidence. He would request the Evidence Owner to pass him the delegation rights.

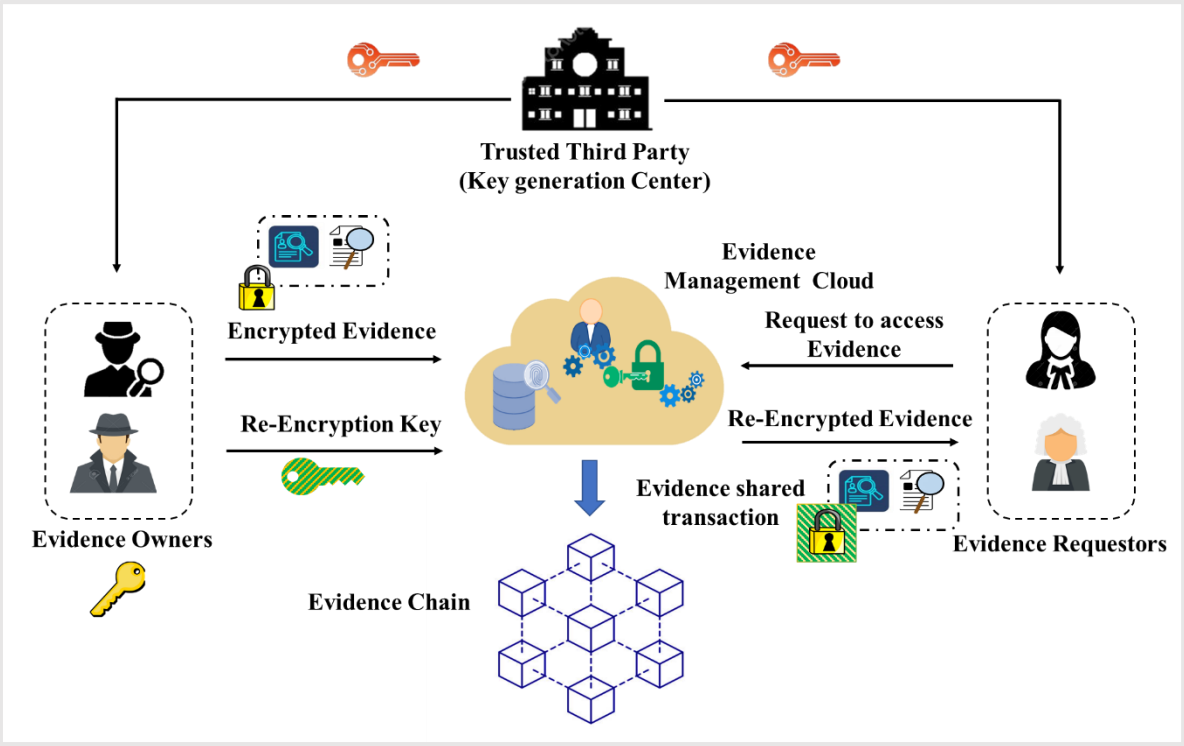


**Figure 2.** Proposed system

- First step, the smart contract is generated and transaction is stored into the blockchain.
- The investigator would request the Rekey Generator to generate the Re-Encryption Key
  - It is generated by using the C (original Output) and private key of the investigator (dB).
  - The rekey rAB is generated.
- The rAB is given to the proxy re-encryptor and the re-encryption of the evidence takes place and the new output is generated C'.
- Now this new output is received and decrypted by the investigator.
- Similarly, if the prosecutor wants the access to the evidence then same process will happen between the investigator and prosecutor.

## 4. Advantages of the Proposed System

- The current Systems are vulnerable to various attacks, which our system would tackle efficiently,
  - Man In the Middle Attack - It is a form of attack that allows attackers to listen to the conversation between two targets. The attack occurs between two properly communicating hosts, allowing the attacker to decipher the messages. An attack's purpose can be to steal personal information. Our system avoids this using the scheme of Proxy-Re-encryption.
  - Impersonification Attacks - User Authentication and delegation of rights help tackle the impersonification attacks making it hard for attacks to impersonify as a trusted authority.
  - Replay Attacks - In this attack the data transmission is maliciously repeated or delayed. This can be tackled by using timestamp as nonce value.
- Use of Cloud storage would provide remote access apart from its cloud computing benefits.

## 5. Challenges in Digital Evidence Management

- Security and integrity of evidence and protection against data breaches is a primary concern which may lead to leaked identities or loss of evidence.
- Data Storage and Volume -The digital evidence in the form of videos, images and other digital forms generates huge amounts of data. Due to storage constraints, it becomes difficult to retain the information and analyse it.
- Detection of tampering due to high risk of cyber-attacks, as these attacks seem to make the evidence intact.
- Access Management to restrict access to the authorized users according to their roles, which ensures a secured and controlled physical location.
- Errors and Mishaps which may affect the proceedings negatively like accessibility or modification of evidence due to errors.
- Transfer of Data between different entities, due to high vulnerability and exposure to hacking attacks or data breach during transfer.
- Presentation of evidence securely in court without the loss of integrity [25].

## 6. Conclusions

In this paper we have successfully analysed and compared various systems and their algorithms. We were able to identify the challenges present in the current systems and architectures. These challenges would form the base for further development and research of the system, which would guarantee security, integrity and authenticity of the evidence at all stages of the investigation process. This would bring transparency in court proceedings and trials.

## References

1. Patil, R.Y. and Devane, S.R., 2019. Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime. Journal of King Saud University-Computer and Information Sciences.
2. Yogesh, P.R. and Devane, S.R., 2018, July. Primordial fingerprinting techniques from the perspective of digital forensic requirements. In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
3. Patil, R.Y. and Devane, S.R., 2017, October. Unmasking of source identity, a step beyond in cyber forensic. In Proceedings of the 10th International Conference on Security of Information and Networks (pp. 157-164).
4. Ahmad, L., Khanji, S., Iqbal, F. and Kamoun, F., 2020, August. Blockchain-based chain of custody: towards real-time tamper-proof evidence management. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-8).
5. Rao, S., Fernandes, S., Raorane, S. and Syed, S., 2020. A Novel Approach for Digital Evidence Management Using Blockchain. Available at SSRN 3683280.
6. Ćosić, J. and Bača, M., 2010, May. (Im) proving chain of custody and digital evidence integrity with time stamp. In The 33rd International Convention MIPRO (pp. 1226-1230). IEEE.
7. Rajamäki, J. and Knuuttila, J., 2013, August. Law enforcement authorities' legal digital evidence gathering: Legal, integrity and chain-of-custody requirement. In 2013 European Intelligence and Security Informatics Conference (pp. 198-203). IEEE.
8. Rajamäki, J. and Knuuttila, J., 2013, August. Law enforcement authorities' legal digital evidence gathering: Legal, integrity and chain-of-custody requirement. In 2013 European Intelligence and Security Informatics Conference (pp. 198-203). IEEE.
9. Lone, A.H. and Mir, R.N., 2019. Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation, 28, pp.44-55.
10. Li, M., Lal, C., Conti, M. and Hu, D., 2021. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. Future Generation Computer Systems, 115, pp.406-420.
11. Petroni, B.C.A., Gonçalves, R.F., de Arruda Ignácio, P.S., Reis, J.Z. and Martins, G.J.D.U., 2020. Smart contracts applied to a functional architecture for storage and maintenance of digital chain of custody using blockchain. Forensic Science International: Digital Investigation, 34, p.300985.
12. Ahmad, L., Khanji, S., Iqbal, F. and Kamoun, F., 2020, August. Blockchain-based chain of custody: towards real-time tamper-proof evidence management. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-8).
13. Dr.S. Harihara Gopalan, S. Akila Suba, C. Ashmithashree,A. Gayathri, V. Jebin Andrews: Digital Forensics Using Blockchain. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S11, September 2019
14. Billard, D., 2018, May. Weighted forensics evidence using blockchain. In Proceedings of the 2018 International Conference on computing and data engineering (pp. 57-61).
15. Yunianto, E., Prayudi, Y. and Sugiantoro, B., 2019. B-DEC: Digital Evidence Cabinet based on Blockchain for Evidence Management. International Journal of Computer Applications, 975, p.8887.
16. Patil, R.Y. and Devane, S.R., 2020. Hash Tree-Based Device Fingerprinting Technique for Network Forensic Investigation. In Advances in Electrical and Computer Technologies (pp. 201-209). Springer, Singapore.
17. Yogesh, P.R., 2020. Formal verification of secure evidence collection protocol using BAN logic and AVISPA. Procedia Computer Science, 167, pp.1334-1344.
18. Al-Khateeb, H., Epiphaniou, G. and Daly, H., 2019. Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. In Blockchain and Clinical Trial (pp. 149-168). Springer, Cham.
19. Giuseppe Ateniese†, Kevin Fu‡, Matthew Green† and Susan Hohenberger‡. Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage. Published in ACM Transactions on Information and System Security (TISSEC).
20. D. Nu˜nez, I. Agudo, and J. Lopez, "Proxy Re-Encryption: Analysis of Constructions and its Application

to Secure Access Delegation", Journal of Network and Computer Applications, vol. 87, pp. 193-209, 2017.

21. W. Sharon Inbarani, G. Shenbagamoorthy, C. and Kumar Charlie Paul. Proxy Re-encryption Schemes for Data Storage Security in Cloud- A Survey. International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 1, January- 2013.
22. Jeong, J., Kim, D., Lee, B. and Son, Y., 2020. Design and Implementation of a Digital Evidence Management Model Based on Hyperledger Fabric. Journal of Information Processing Systems, 16(4).
23. Yogesh, P.R., 2020. Backtracking Tool Root-Tracker to Identify True Source of Cyber Crime. Procedia Computer Science, 171, pp.1120-1128.
24. Timothy, M., 2020. An Android Location-Based Crime Reporting System Using the Google Map Api. UNIVERSITY OF PITESTI SCIENTIFIC BULLETIN: ELECTRONICS AND COMPUTERS SCIENCE, 20(1).
25. Patil, R.Y., 2022. Digital forensics evidence management based on proxy re-encryption. International Journal of Computer Applications in Technology, 68(4), pp.405-413.

**Biographical notes**

**Rachana Yogesh Patil** received her Ph.D. degree from the University of Mumbai, India in 2020. Currently, she is an Associate Professor in the Department of Computer Engineering, Pimpri Chinchwad College of Engineering of Pune, India. Her research interests include cryptography, network security, cyber security and digital forensics (especially network forensics). She is a Member of ACM and IETE and IEEE.

**Yogesh H. Patil** received his Ph.D. degree from Sir Padampat Singhania University, Udaipur. He is an Assistant Professor at D.Y Patil Institute of Technology, Pune. He has worked as Assistant Professor at Department of Instrumentation Engineering, A.C. Patil College of Engineering, Kharghar, Navi Mumbai. India. Yogesh. H Patil received M.E. from University of Mumbai, India in 2004. He has published 10+ papers in international journals and conferences. His primary area of research is Sensors and Instrumentation especially Biomedical Instrumentation. I am a Life Time Member of IETE.