Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 215 (2022) 71–77

Procedia Computer Science

www.elsevier.com/locate/procedia

4th International Conference on Innovative Data Communication Technology and Application

Digital Evidence Management System for Cybercrime Investigation using Proxy Re-Encryption and Blockchain

Harshwardhan Chougule[a], Sunny Dhadiwal[b], Mehul Lokhande[c], Rohit Naikade[d], and Rachana Patil[e]*

[a,b,c,d,e] *Department of Computer Engineering,*
PCET's Pimpri Chinchwad College of Engineering,
Pune-411035, India.

Abstract

One of the most beneficial uses of the Internet of Things in cloud is data sharing. As tempting since this technology is, data security is still one of the issues it faces, as inappropriate data usage may lead to a range of issues. We offer a proxy re-encryption strategy to securely exchange data in cloud contexts in this paper. Data owners can utilize identity-based encryption to send encrypted data to the cloud, and legitimate users can access the data via proxy re-encryption. Because IoT devices have limited resources, an edge device functions as a proxy server to do complex calculations. We also make effective use of information-centric networking capabilities to supply cached data in the proxy, resulting in better service quality and more network capacity. Our system also uses block chain, a revolutionary technology that allows for decentralized data sharing. It improves centralized system efficiency and enables fine-grained data access control. The security analysis and assessment of our system show that it has the potential to offer privacy protection, authenticity, and dependability.

*Keywords:*Block chain, Cryptography Decentralized, Distributed Systems, Proxy Re-encryption;

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: rachana.y.patil@gmail.com

10.1016/j.procs.2022.12.008

1. Introduction

In today's rapidly growing world, we see there is a lot of development in technology, medical science, infrastructure, etc. On the other hand, we are able to see the surge in crimes and illegal activities. These activities are increasing at an alarming rate. Also, handling of the collected evidence is also a challenging task as there has been a rise in tampering and mishandling. Any corrupted official may change the evidence. In such a scenario, it becomes necessary to preserve the evidence. We aim to integrate blockchain with Evidence Management System along with Proxy Re-Encryption technique.

Roles and titles are always used to differentiate users' eligibility to use specific services. A method like this is the role-based access control (RBC) framework, which establishes permission limitations among users and services [1]. In RBAC, users are assigned to roles, and roles are assigned to role services. Many organizations and corporations utilize a framework like this to implement their internal access control needs for their computer systems [2]. Only if a company's programmer/developer has access to the full source code does the quality assurance team have access to the aforementioned source code. Although RBAC is extensively utilized within a company, it's vital to note that it's a flexible architecture; roles are frequently employed across organizations. For example, Students are frequently allowed to buy books at a discounted price. Users' responsibilities and titles frequently determine their eligibility to use particular services. Such a system has been molded by the role-based access management (RBAC) paradigm, which defines the access management connection between users and services. In RBAC, different roles are assigned to users, and roles are tied to services. To meet their internal access control requirements, many firms and organizations use such a framework in their computer systems. This access management is commonly adopted within a company; however it is essential to note that RBAC is a flexible architecture, and roles are routinely used between organizations.

2. Related Work

Smart Contracts are computer programs that transfer or regulate property or digital currents between parties. It may also carry out the policy or agreement in addition to setting the terms and conditions. Blockchain is used to store the generated smart contracts, which is an excellent system for storing these contracts due to its ambiguity and security. When a transaction is analyzed, the smart-contract helps to determine where to transfer the transaction and how long it has been since the transaction took place [3,4].

With [5], CSIRRO has introduced an innovative technique to integrate Block on IoT. He starts by experimenting with smart-home tech to see if IoT may be blocked. For the smart device transactions, the block wheels are the ideal access control mechanism. This search provides some additional security precautions when it comes to introducing BC technology into IoT. Furthermore, this technology is having not been able to assist with a generic form of block-chain solution in the case of IoT.

According to [6], is a multi-user system prototype for regulating access to datasets placed in virtual cloud settings. Cloud storage, similar to other insecure environments, necessitates the capability to securely transfer data. Access Control Mechanism is a feature-based encryption approach with dynamic properties. Our solutions use Block chain-based decentralized badgers to provide an irreversible record for any essential security circumstances, such as considerable funding, assignment, revision, or revocation of an access policy. [7,8] present a set of protocols that ensure the secret message, or the generated secret key used in cryptographic operations is kept private. Only the laser block transmits the sifter text's hash code. Ethereum Blockchain platforms and prototype smart contracts were used to test our solution.

[9] Proposes a four-level IoT Blockchain fusion model that covers several sorts of IoT devices. The concept envisions a distributed file system for storing enormous amounts of IoT data. The Ethereum blockchain is then used to present a M2M trading system which is autonomous is an example of a blockchain based IoT application. The suggested approach highlights how security, transparency and traceability are important in IoT applications.

The authors of [10], proposed Edgence a blockchain-enabled cloud computing (edge computing) platform for intelligently managing big decentralised apps (dApps) in IoT usecases. Edgence employs master-node technology to connect a locked blockchain-based system to the real world, allowing IoT-based dApps to benefit from blockchain. A master node is a blockchain full node with collateral that is deployed on a mobile edge computing edge cloud, allowing it to execute IoT dApps using the edge cloud's capabilities. HCloud is a reliable platform that uses a serverless computing strategy.

[11]. HCloud allows you to design an IoT server with several servers but fewer functionalities, and it distributes these services over multiple clouds using a scheduling method. The policy is defined by the client and contains, among other things, the desired functionality, execution resources, latency, and price. Based on scheduling criteria, HCloud gathers information about each cloud and to direct the serverless functions to the appropriate cloud system. Using blockchain technology, we can further assure that our system cannot spoof the cloud state or erroneously distribute the goal functions.

The idea of a decentralized gasified service exchange network, where providers (i.e solution providers) can dynamically supply and seek services from one another., is introduced in [12]. The proposed strategy uses blockchain technology to build a to-kenized market in which IoT solution providers may utilize smart contracts to implement gasification strategies to maximize profits while providing and receiving ser-vices.

According to [13] provides unique cryptosystems for distributing encrypted data correctly, which we refer to as key-policy attribute-based encryption. Cephet text is labeled with a bunch of attributes and commands related to private key access settings in our cryptosystem, allowing a user to decode the encryption. This method is companionable with encryption based on category identification used by private key providers (HIBE).

[14] Provide a block chain-based and proprietary cryptography-based electronic health record (EHR) solution. To acquire distinct properties of ABI, IBE, and IBS in cryptography, the authors propose a combined feature-based encryption and signature. It reduces the complexity of the system administration and removes the requirement of cryptographic systems to suit various security requirements to maintain the integrity and assessment of healthcare data a block chain based application for a medical insurance firm is proposed.

According to [15], block chain may be used to produce the seed required for key creation and to maintain the public key. Is it necessary to use a random seed generation approach to generate keys? Seeds are created via out-of-band transmission and device modification to avoid a man-in-the-middle attack and reverse contribution.

3. Proposed System Design

The below figure 1 shows Design and Implement a system for A Proxy Re-Encryption Approach to Secure Data Sharing using Block chain. The system contains following modules:

Registration and Authentication: All organizations may register during this step. Users, data owners, and service providers may all construct their own profiles.

Data Uploading: In the first step, the file is uploaded by the data owner. In that module, data encryption and encryption schemes are performed, and keys are sent to a database.

Data Sharing through Re-Encryption Approach: During this phase, the service provider may share any file with any user in the cloud group.

Access Control: With access control, every user may read or access a file that has been shared with him by another user. File request and download: the user may send a download request to databases, which will be verified using the key.

Distributed Block chain: A block chain is a distributed ledger that represents the current status of delegated access privileges in a system.

1. First of all, the IoT devices are registered on the secure cloud storage i.e. Block chain.
2.The data collected by the IoT devices, sensors, etc is then encrypted by the proxy and stored in the secure cloud storage.
3. The first user requests for the encrypted data collected by the IoT devices. The first user can access the data with the help of the public key associated with the user and the key generated by the proxy server. The user then sends the required information to the proxy for generating the re-encryption key for the next user.
4. In this manner, the users who need to access data need their public key registered within the blockchain and the re-encrypted key from the previous user and proxy server.
5. Data owner has rights to add users, update data and delete data.

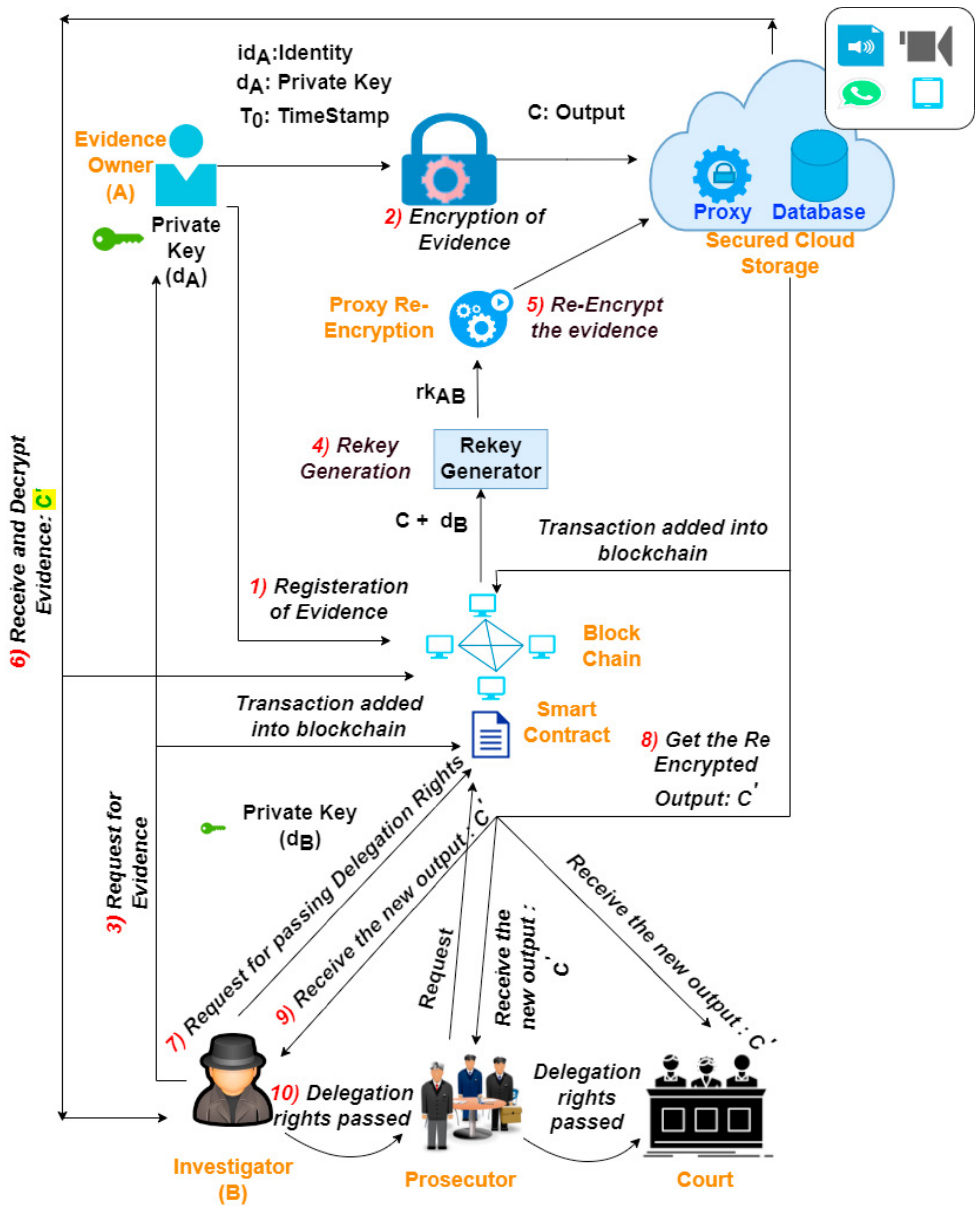
idA:Identity
dA: Private Key
T0: TimeStamp
C: Output
Evidence Owner (A)
Private Key (dA)
2) Encryption of Evidence
Proxy
Database
Secured Cloud Storage
Proxy Re-Encryption
5) Re-Encrypt the evidence
rkAB
4) Rekey Generation
Rekey Generator
C + dB
Transaction added into blockchain
1) Registeration of Evidence
Block Chain
6) Receive and Decrypt Evidence: C'
Transaction added into blockchain
Smart Contract
8) Get the Re Encrypted Output: C'
3) Request for Evidence
Private Key (dB)
7) Request for passing Delegation Rights
9) Receive the new output : C'
Request
Receive the new output : C'
Receive the new output : C'
10) Delegation rights passed
Delegation rights passed
Investigator (B)
Prosecutor
Court

Fig.1 System Architecture

3.1. Implementation Procedure

- Before committing a block, the system must validate the prior block.
- The data can be accessed over the internet at any time.
- The current block chain must be shown as invalid throughout the transaction if any block has been modified by an unauthorized user.
- With the support of the majority of trustiness, it can restore the faulty blockchain utilizing other data nodes.
- If the data is recorded and broadcast to the network by the node wishing to initiate a transaction.
- The node that gets the data confirms the data's validity in the network. The confirmed data is then written to a block.
- The transaction is validated by all nodes or users in the network that requires proof of work for validation.

- The data will be preserved in a block that is added to the block chain via the consensus process of the network. And all of the network's nodes accept the faulty block and utilize it to extend the chain.

4. Proposed algorithm for evidence management

Setup phase
Input:- Security parameters l
Output:- public system parameters P_{pub}
Choose < p, g, G, G_T, e>
G_1: - A cyclic additive group of prime order p.
G_T: - A cyclic multiplicative group of same order p.
g is generator of G
e: Bilinear map $e : G_1 \times G_1 \rightarrow G_T$.
Select $g \in G1$ and $Z = e(g, g) \in G_T$.

The Trusted third part KGC selects $\lambda \mathbf{1.} G1$ randomly

$\mathcal{H}_1 = \{0,1\}^* \mathbf{1.} G_1$

$\mathcal{H}_2 = G_T \mathbf{1.} G_1$
$M_{sk} = \lambda$

$P_{pub} = \{ G_{1,} G_T , \mathcal{H}_{1,} \mathcal{H}_{2,} g, \mathbf{1.} , \}$

Keygen phase
Input:-Identity of user, $P_{pub,}$ M_{sk}
Output:- Pk_{ID}
The user A with identity $ID_O \in \{0,1\}^*$
Private key of user A $(Pk_O) = \mathcal{H}_1(ID_O)^{\lambda}$

First level Encryption phase
Input:- $ID_{O,}$ M
Output:- C_O
$Select \alpha \leftarrow Z_p^*$
M- Message to be encrypted
$C_{1O} = g^r$
$C_{2O} = M * e\left(g^{\delta}, \mathcal{H}1(ID_O)\right)^{\alpha}$
$C_O = (C_{1O}, C_{2O})$

ReKey Gen phase
Input:- $P_{pub,} ID_U$
Output:- $rk_{O \rightarrow U}$
Original User O selects $\mu \leftarrow G_T$
Compute $\langle \sigma_1, \sigma_2 \rangle = Encrypt\ (P_{pub,} ID_U, \mu)$
Compute $\sigma_3 = Pk_U^{-1} * \mathcal{H}_2\ (\mu)$
$rk_{O \rightarrow U} = \langle \sigma_1, \sigma_2, \sigma_3 \rangle$

Re-encryption phase
Input:- $C_{O,}$ $P_{pub,} ID_U$
Output:- C_U

$C_{1U} = C_{1O} = g^r$
$C_{2U} = C_{2O} * e(C_{1O}, \sigma_3)$
$C_{3U} = \sigma_1$
$C_{4U} = \sigma_2$
$C_U = (C_{1U}, C_{2U}, C_{3U}, C_{4U})$

Decryption phase
Input:- C_O or C_U
Output:-M
For first level ciphertext decryption $M = \frac{C_{2O}}{e(C_{1O}, Pk_O)}$
Re-encrypted Ciphertext Decryption
Compute $C_U^{'} = (C_{1U}^{'}, C_{2U}^{'})$
Compute $\mu_2 = Decryption(\mathrm{Pk}_U, C_U^{'})$
Compute $\mu = \frac{C_{2U}}{e(C_{1U} * \mathcal{H}_2(\mu_2))}$
Compute $M = \frac{C_{2U}^{'}}{e\left(g^{\lambda}, \mathcal{H}_2(\mu)\right)}$

5. Results and Discussions

Figure 2 depicts the time it takes for four nodes to validate the blockchain using the consensus method The X axis shows the size of the blockchain, while the Y axis shows how long each of the four nodes takes in milliseconds.

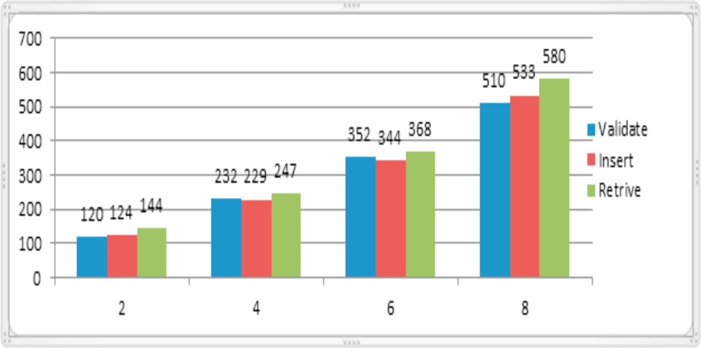

Fig .2 Time required (in milliseconds) for complete file encryption records block chain using 4 data nodes in P2P Network

We were able to bring system output to a satisfactory level after implementing some parts of the system. The results of the proposed PBEWithMD5AndDES and AES algorithm for plain text conversion and encryption and decryption are shown in Table 1.

Table.1 System Performance

File Data Size in KB	Encryption time (Milliseconds)		Decryption time (Milliseconds)	
	Encryption	Re- Encryption	Decryption	Re- Decryption
2	405	425	524	612
4	500	526	645	733
6	750	890	654	610
8	860	995	785	890

6. Conclusion

The main outcome of this work is a prototype of a software system that uses the access control paradigm to access data stored in unsaturated environments. For the implementation purpose of the algorithms for the system, acceptable, functionality, and implementation complexity were chosen. Customization of access policiesin order to define dynamic access policies; changing access policies requires no extra action from some another members of a social system, eliminating the need for frequent changes to user keys; the integrity of information about all transactions, including granting and changing access, facts improves. A blockchain-based system with configurable data encryption permission is proposed.

References

[1] Bannore, A., Patil, R.Y. and Devane, S.R., An Efficient Proxy Signature–Based Authority Delegation Scheme for Medical Cyber Physical Systems. In Cyber Security Threats and Challenges Facing Human Life (pp. 13-23). Chapman and Hall/CRC.

[2] Patil, R.Y. and Bannore, A., 2022. Provably Secure Role Delegation Scheme for Medical Cyber-Physical Systems. In Security Analytics (pp. 143-163). Chapman and Hall/CRC.

[3] Harshwardhan, C., Sunny, D., Mehul, L., Rohit, N. and Patil, R., 2021, June. Management of Digital Evidence for Cybercrime Investigation—A Review. In International Conference on Soft Computing and Signal Processing (pp. 133-143). Springer, Singapore.

[4] Patil, R.Y. and Patil, Y.H., 2022. Identity-based signcryption scheme for medical cyber physical system in standard model. International Journal of Information Technology, pp.1-9.

[5] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, \Querying in internet of things with privacy preserving: Challenges, solutions and opportunities," IEEE Network, vol. 32, no. 6, pp. 144{151, 2019.

[6] J. Li, H. Ye,W.Wang,W. Lou, Y. T. Hou, J. Liu, and R. Lu, Efficient and secure outsourcing of differentially private data publication," in Proc. ESORICS, 2019, pp. 187 206.

[7] 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*.

[8] Bhole, D., Mote, A. and Patil, R., 2016. A new security protocol using hybrid cryptography algorithms. International Journal of Computer Sciences and Engineering, 4(2), pp.18-22

[9] Gong, Xinglin, Erwu Liu, and Rui Wang. Blockchain-Based IoT Application Using Smart Contracts: Case Study of M2M Autonomous Trading. 2020 5th International Conference on Computer and Communication Systems (ICCCS). IEEE, 2020.

[10] Xu, Jinliang, et al Edgence: A blockchain-enabled edge-computing platform for intelligent IoT-based dApps. & China Communications 17.4 (2020): 78-87.

[11] Huang, Zheng, Zeyu Mi, and Zhichao Hua. & HCloud: A trusted JointCloud serverless platform for IoT systems with blockchain. & China Communications 17.9 (2020): 1-10.

[12] Gheitanchi, Shahin. & Gamified service exchange platform on blockchain for IoT business agility& 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2020.

[13] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, \Enabling efficient and geometric range query with access control over encrypted spatial data," IEEE Trans. Information Forensics and Security, vol. 14, no. 4, pp. 870{885, 2019.

[14] K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. Shen, Privacy preserving attribute- keyword based data publish-subscribe service on cloud platforms," Information Sciences, vol. 387, pp. 116{ 131, 2017.

[15] Choi, Jungyong, et al. &quot;Random Seed Generation For IoT Key Generation and Key Management System Using Blockchain.&quot; 2020 International Conference on Information Networking (ICOIN). IEEE, 2020.