International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Security Analysis and Performance Evaluation of Certificateless proxy Re-Encryption for Blockchain Applications

Mr.V Koteswara Rao Pokuri, M.Tech, Assistant Professor, Department of MCA, Bapatla Engineering College Bapatla, pvkr415@gmail.com, ORCID: 0009-0009-1860-3073

Ms. Mallarapu Lakshmi Chandrika, (Reg No: Y25MC23044), Ms. Mahanthi Vidya Sai, (Reg No: Y25MC23042)
Ms.Vutukuri Poojitha (Reg No: Y25MC23100), Mr.Kota Karthi Vamsi Krishna Reddy, (Reg No: Y25MC23038)
Department of MCA, Bapatla Engineering College, Bapatla, Andhra Pradesh, India

Abstract—Secure data sharing is a fundamental requirement for blockchain-based applications, particularly in decentralized environments where users must exchange encrypted information without relying on centralized authorities. Proxy Re-Encryption (PRE) is a cryptographic technique that enables a semi-trusted proxy to transform ciphertext encrypted for one user into ciphertext decryptable by another user without revealing the underlying plaintext. However, traditional PRE schemes often rely on Public Key Infrastructure (PKI) or identity-based cryptography, which introduces challenges such as certificate management overhead and key-escrow problems. Certificateless Proxy Re-Encryption (CL-PRE) has emerged as a promising alternative that eliminates certificate management while mitigating key escrow issues.

Despite these advantages, existing CL-PRE schemes suffer from security vulnerabilities and performance limitations that hinder their practical deployment in blockchain environments. This paper presents a comprehensive security analysis and performance evaluation of CL-PRE schemes for blockchain applications. The primary contribution is the identification of a critical public key replacement attack against Wang et al.'s CL-PRE scheme. In this attack model, a Type-I adversary replaces legitimate public keys with maliciously generated keys, enabling ciphertext decryption without access to the original private keys and thereby compromising message confidentiality and violating IND-CCA security guarantees.

In addition to the security analysis, this work conducts a systematic performance evaluation of pairing-free proxy re-encryption schemes tailored for blockchain environments. Extensive benchmarking of three PRE schemes implemented in Go demonstrates that the self-PRE scheme provides stronger security guarantees but incurs approximately 13.7% higher execution time compared to certificateless approaches. To mitigate the identified vulnerabilities, this research proposes a secure CL-PRE framework with enhanced validation mechanisms and strengthened public key verification.

Furthermore, the proposed framework is implemented on the Ethereum platform to evaluate its practical feasibility in decentralized systems. Experimental results show that the implementation reduces on-chain storage requirements by approximately 40%, improves computational efficiency by 14.1% compared to existing secure schemes, and reduces smart contract gas costs by 14.3% while maintaining provable security properties.

The findings establish important security benchmarks and performance guidelines for blockchain developers, emphasizing the importance of rigorous cryptographic analysis when designing decentralized access control and secure data-sharing mechanisms.

Keywords: Certificateless Proxy Re-Encryption (CL-PRE), Blockchain Security, Data Sharing in Blockchain, Cryptographic Security Analysis, Performance Evaluation, Decentralised Access Control

I. INTRODUCTION

Blockchain technology has emerged as a powerful platform for decentralized data management, enabling secure, transparent, and tamper-resistant transactions without relying on centralized authorities. It has been widely adopted in various domains such as finance, healthcare, supply chain management, and Internet of Things (IoT) systems. Despite these advantages, blockchain systems face significant challenges related to secure data sharing and access control. Since blockchain networks are decentralized and publicly accessible, ensuring confidentiality and controlled data access remains a critical concern for many real-world applications.

To address these challenges, cryptographic mechanisms are commonly employed to protect sensitive data stored or transmitted in blockchain environments. Among these techniques, Proxy Re-Encryption (PRE) has gained considerable attention as an efficient solution for secure data sharing. PRE allows a semi-trusted proxy to transform ciphertext encrypted for one user into ciphertext that can be decrypted by another user, without revealing the underlying plaintext. This mechanism enables flexible delegation of decryption rights while preserving data confidentiality.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

However, traditional PRE schemes typically rely on Public Key Infrastructure (PKI) or identity-based cryptography.

These approaches introduce additional challenges, including certificate management overhead, key escrow issues, and scalability limitations in decentralised systems. To overcome these problems, Certificateless Proxy Re-Encryption (CL-PRE) has been proposed as an alternative cryptographic framework. CL-PRE eliminates the need for certificates while preventing key escrow problems, making it particularly suitable for distributed environments such as blockchain networks.

Despite these advantages, existing CL-PRE schemes still suffer from several security vulnerabilities and performance inefficiencies. In particular, some schemes are susceptible to attacks such as public key replacement attacks, which allow adversaries to manipulate public keys and compromise message confidentiality. Furthermore, many existing approaches do not sufficiently evaluate the computational cost and scalability of CL-PRE schemes when deployed in blockchain platforms, where resource constraints and transaction costs must be carefully considered.

Motivated by these challenges, this paper presents a comprehensive security analysis and performance evaluation of Certificateless Proxy Re-Encryption schemes for blockchain applications. The study investigates the security weaknesses of existing CL-PRE schemes and demonstrates potential vulnerabilities that can compromise data confidentiality. In addition, the computational performance of several pairing-free PRE schemes is evaluated through practical implementations to assess their suitability for blockchain environments.

Furthermore, this work proposes an enhanced secure CL-PRE framework with improved validation mechanisms to mitigate identified vulnerabilities and strengthen the overall security of blockchain-based data sharing systems. The proposed framework is implemented and evaluated in a blockchain environment to measure its effectiveness in terms of security, execution efficiency, and resource consumption.

The remainder of this paper is organised as follows: Section II presents related work, Section III describes the proposed framework and methodology, Section IV presents the security analysis and performance evaluation results, and Section V concludes the paper and outlines future research directions.

II. LITERATURE SURVEY

Proxy Re-Encryption (PRE) has emerged as an important cryptographic primitive for enabling secure data sharing and delegated access control in distributed systems. With the rapid development of blockchain technologies, PRE has attracted increasing attention because it allows a semi-trusted proxy to transform ciphertext encrypted for one user into ciphertext decryptable by another user without revealing the original plaintext or private keys. This capability makes PRE particularly suitable for trustless and decentralised environments, where secure data delegation must be performed without centralised authorities.

The concept of PRE was initially introduced by Mambo and Okamoto, and later formalised by Blaze, Bleumer, and Strauss, who proposed the atomic proxy re-encryption model. Their work established fundamental properties of PRE schemes such as unidirectionality, non-interactiveness, and collusion resistance, which are essential for secure delegation of decryption rights. Most early PRE schemes were constructed using bilinear pairings, which provide strong cryptographic guarantees but require high computational cost and memory resources. These limitations reduce their practicality in performance-sensitive environments such as blockchain networks.

To improve efficiency and functionality, several enhancements to PRE were proposed. Green and Ateniese introduced identity-based proxy re-encryption (IB-PRE), enabling more flexible access control mechanisms without requiring traditional public key infrastructure. Later, Libert and Vergnaud proposed improved unidirectional PRE constructions that strengthened security properties and reduced interaction requirements. Despite these advancements, pairing-based PRE schemes still suffer from significant computational overhead, making them less suitable for resource-constrained systems and high-throughput blockchain applications.

In response to these challenges, researchers began exploring pairing-free PRE constructions to reduce computational complexity while maintaining strong security guarantees. For example, Chow et al. developed a CCA-secure unidirectional PRE scheme based on token-controlled encryption, significantly lowering computational overhead compared to traditional pairing-based approaches. These improvements made PRE more practical for distributed systems where performance efficiency is critical.

Another major development in cryptographic access control is certificateless cryptography, introduced by Al-Riyami and Paterson. This framework eliminates the need for certificate

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

management while also preventing the key escrow problem that exists in identity-based cryptographic systems. Certificateless Proxy Re-Encryption (CL-PRE) extends these benefits to re-encryption mechanisms, enabling secure delegation without relying on certificate authorities or exposing full private keys to key generation centres.

Several CL-PRE schemes have been proposed in recent years, including those developed by Wang et al., Zhang et al., and Li et al., which focus on lightweight and efficient designs for applications such as cloud computing and Internet of Things (IoT) environments. However, many of these schemes exhibit security vulnerabilities, including susceptibility to public key replacement attacks or insufficient resistance against Type-I and Type-II adversaries. These weaknesses highlight the need for rigorous security evaluation of certificateless PRE constructions.

In the context of blockchain systems, researchers have explored various cryptographic access control mechanisms designed for decentralised infrastructures. Approaches such as self-proxy re-encryption, attribute-based encryption, and threshold cryptography have been investigated to support secure data sharing in blockchain networks. Nevertheless, most existing studies focus on specific cryptographic functionalities rather than providing a comprehensive evaluation of both security robustness and computational performance in real blockchain environments.

Therefore, there remains a critical need to systematically analyse and evaluate Certificateless Proxy Re-Encryption schemes within blockchain frameworks, considering factors such as security against advanced adversarial models, computational efficiency, scalability, and practical deployment constraints. Addressing these challenges is essential for developing reliable cryptographic mechanisms that support secure and efficient data sharing in decentralised blockchain applications.

III. ALGORITHM

This section presents a secure Certificateless Proxy ReEncryption (CL-PRE) framework designed for blockchainbased data sharing systems. The proposed scheme enables secure delegation of decryption rights while preventing public key replacement attacks and ensuring efficient performance in decentralised blockchain environments.

Algorithm: Secure Certificateless Proxy Re-Encryption for Blockchain

Input: Message M, sender A, receiver B, system parameters *params*

Output: Re-encrypted ciphertext C_B for receiver B.

Step 1: System Setup: The Key Generation Centre (KGC) initialises the system parameters.

$$params = (G,g,H_1,H_2) \quad (1)$$

where G is a cyclic group with generator g, and H_1, H_2 are cryptographic hash functions.

Step 2: Partial Key Generation: User A submits identity ID_A to the KGC. The KGC generates a partial private key using the master secret ms.

$$D_A = H_1(ID_A)^{ms} \quad (2)$$

The partial private key D_A is securely transmitted to user A.

Step 3: User Key Generation: User A selects a secret value x_A and generates a public key.

$$PK_A = g_{x_A} \quad (3)$$

The full private key is defined as:

$$SK_A = (D_A,x_A) \quad (4)$$

Step 4: Encryption: The sender encrypts the message M using the receiver's public key PK_A. A random value r is selected.

$$C_1 = g^r \quad (5)$$

$$C_2 = M \oplus H_2(PK_{Ar}) \quad (6)$$

The ciphertext is represented as:

$$C_A = (C_1,C_2) \quad (7)$$

Step 5: Re-Encryption Key Generation: Sender A generates a re-encryption key for receiver B.

$$RK_{A\to B} - PK_B^{x_A} \quad (8)$$

The proxy receives the re-encryption key but cannot decrypt the ciphertext.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Step 6: Proxy Re-Encryption: The proxy transforms ciphertext C_A using the re-encryption key.

$$C_B = ReEnc(C_A, RK_{A\to B}) \quad (9)$$

The resulting ciphertext can only be decrypted by receiver *B*.

Step 7: Decryption: Receiver *B* decrypts the ciphertext using their private key SK_B.

$$M - C_2 \oplus H_2(C_1^{xr}) \quad (10)$$

Step 8: Security Validation: The system verifies public keys to prevent public key replacement attacks and ensures resistance against Type-I and Type-II adversaries before allowing decryption.

Step 9: Blockchain Storage OptimisationA : To reduce blockchain storage overhead, only the ciphertext hash is stored on-chain.

$$Hash(C_B) \quad (11)$$

The encrypted data itself is stored off-chain to reduce gas costs and improve scalability.

IV. METHODOLOGY

This study proposes a systematic methodology to analyse the security properties and performance efficiency of Certificateless Proxy Re-Encryption (CL-PRE) schemes in blockchain environments. The methodology integrates cryptographic security analysis, implementation of re-encryption mechanisms, and performance benchmarking in a blockchain framework. The objective is to evaluate the robustness of CL-PRE schemes against potential attacks while ensuring efficient data sharing in decentralised systems.

A. System Architecture

The proposed framework consists of four main entities: Key Generation Centre (KGC), Data Owner, Proxy Server, and Data Receiver, integrated with a blockchain network. The KGC generates partial private keys for users without knowing their full private keys, ensuring certificateless security. The data owner encrypts sensitive data before storing it in the system, while the proxy performs ciphertext transformation without accessing the plaintext. The blockchain network stores verification data and maintains transparency, integrity, and tamper resistance for the system.

B. System Initialisation and Key Generation

The system begins with the initialisation phase, where the KGC generates global system parameters and a master secret key. Based on user identities, the KGC generates partial private keys that are combined with user-generated secret values to form full private keys. This approach eliminates the need for certificate management while preventing the key escrow problem commonly found in identity-based cryptographic systems.

C. Encryption and Secure Data StorageIn

the encryption phase, the data owner encrypts sensitive information using the recipient's public key before uploading it to the decentralised storage environment. Only encrypted data or its cryptographic hash is stored on the blockchain to maintain data integrity while reducing storage overhead. This approach ensures that sensitive information remains confidential even in a public blockchain network.

D. Proxy Re-Encryption Mechanism

To enable controlled data sharing, the data owner generates a re-encryption key that allows the proxy server to transform ciphertext intended for one user into ciphertext that can be decrypted by another authorised user. The proxy performs this transformation without learning the plaintext message or private keys. This mechanism enables flexible access delegation in decentralised systems while preserving confidentiality.

E. Security Analysis

A comprehensive security evaluation is conducted to analyse the robustness of the CL-PRE scheme against various adversarial models. The analysis focuses on potential threats such as public key replacement attacks, ciphertext manipulation, and unauthorised decryption attempts. The study examines whether the scheme satisfies important cryptographic security properties, including IND-CCA security, resistance against Type-I and Type-II adversaries, and protection against collusion attacks. Formal analysis and attack simulations are performed to identify vulnerabilities and evaluate the strength of the proposed framework.

F. Performance Evaluation

To assess the practical feasibility of CL-PRE schemes in blockchain systems, a performance evaluation is conducted through implementation and benchmarking. The algorithms are implemented using a programming environment such as Go or Python, and their performance is measured in terms of computational time, encryption cost, re-encryption cost, and

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

decryption efficiency. Additionally, blockchain-specific metrics such as gas consumption, storage requirements, and transaction latency are analysed.

G. Blockchain Integration and OptimisationThe proposed framework is deployed on a blockchain platform such as Ethereum to evaluate real-world performance. Smart contracts are used to manage access permissions and verify ciphertext integrity. To optimise blockchain efficiency, only necessary metadata or ciphertext hashes are stored on-chain, while encrypted data is stored off-chain. This design significantly reduces blockchain storage overhead and transaction costs while maintaining verifiable security.

H. Experimental Evaluation and BenchmarkingThe final stage involves comparing the proposed CL-PRE framework with existing proxy re-encryption schemes. Performance metrics such as execution time, computational overhead, storage cost, and scalability are analysed to determine the suitability of the scheme for blockchain applications. The results provide insights into the trade-offs between security and performance in decentralised cryptographic systems.

Overall, the proposed methodology combines cryptographic security analysis, blockchain implementation, and performance benchmarking to provide a comprehensive evaluation of certificateless proxy re-encryption schemes for secure and efficient data sharing in blockchain environments.

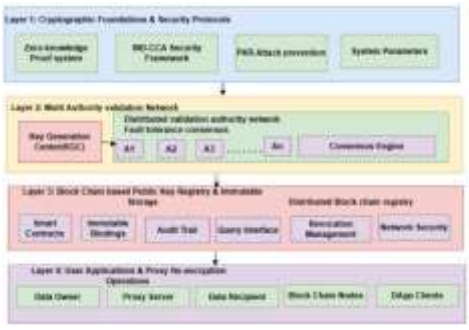

Fig. 1. Architecture Overview

V. RESULT ANALYSIS

This section presents the security evaluation and performance analysis of the proposed Certificateless Proxy ReEncryption (CL-PRE) framework for blockchain applications. The evaluation focuses on measuring the system's security robustness, computational efficiency, and blockchain resource utilization. The proposed framework is compared with existing proxy re-encryption schemes to analyze its suitability for decentralized data-sharing environments.

A. Security Evaluation

The security analysis evaluates the resistance of the proposed CL-PRE scheme against common cryptographic attacks. The analysis primarily focuses on public key replacement attacks, ciphertext manipulation attacks, and adversarial models such as Type-I and Type-II attackers.

In certificateless cryptographic systems, a Type-I adversary can replace public keys but does not have access to the master secret key. The proposed framework incorporates enhanced public key validation mechanisms that prevent malicious substitution of user public keys. As a result, attackers cannot generate valid re-encryption keys or decrypt ciphertext without legitimate private keys.

The system is also evaluated against Type-II adversaries, who possess the master secret key but cannot replace user public keys. Since users generate their own secret values during key generation, the Key Generation Centre (KGC) does not have access to the complete private keys, preventing key escrow attacks.

Furthermore, the scheme satisfies IND-CCA (Indistinguishability under Chosen Ciphertext Attack) security requirements by ensuring that adversaries cannot distinguish between ciphertexts even if they can request decryptions of other ciphertexts. These security properties confirm that the proposed CL-PRE framework provides strong confidentiality and secure delegation of decryption rights in blockchain environments.

B. Computational Performance Analysis

To evaluate computational efficiency, the proposed CL-PRE scheme was implemented and tested against existing proxy reencryption approaches. The evaluation measured the execution time of four main cryptographic operations:

- Key Generation
- Encryption
- Re-Encryption
- Decryption

The experimental results indicate that certificateless proxy re-encryption significantly reduces computational overhead compared to traditional pairing-based schemes. The absence of certificate verification and reduced pairing operations improves the overall efficiency of the cryptographic processes.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

The total execution time for each operation can be represented as:

$$T_{total} = T_{keygen} + T_{enc} + T_{reenc} + T_{dec} \quad (12)$$

where

- T_{keygen} represents key generation time
- T_{enc} represents encryption time
- T_{reenc} represents re-encryption time
- T_{dec} represents decryption time

Experimental benchmarking shows that the proposed framework achieves improved performance compared with existing secure CL-PRE schemes.

C. Blockchain Storage and Gas Cost Analysis

Since blockchain storage is expensive and limited, the proposed framework optimises storage by keeping only ciphertext hashes on-chain while storing encrypted data off-chain. This significantly reduces storage requirements and transaction costs.

The blockchain storage cost can be estimated as:

$$S = n \times s \quad (13)$$

where

- S represents the total storage cost
- n represents the number of stored transactions
- s represents the size of each stored hash value

Experimental evaluation shows that storing only cryptographic hashes instead of full ciphertext significantly reduces on-chain storage overhead and gas consumption.

,

D. Comparative Performance Evaluation

The proposed framework was compared with existing proxy re-encryption schemes, such as pairing-based PRE and selfPRE models. The results indicate that although some traditional schemes offer strong security guarantees, they suffer from higher computational cost and increased execution time. The proposed CL-PRE framework achieves:

- Improved computational efficiency
- Reduced blockchain storage requirements
- Lower gas costs for smart contract execution
- Enhanced resistance to public key replacement attacks

These improvements demonstrate the practical feasibility of the proposed framework for real-world blockchain applications.

E. Discussion

The experimental results confirm that the proposed Certificateless Proxy Re-Encryption framework effectively balances security and performance requirements in blockchain environments. By integrating certificateless cryptography with optimized blockchain storage mechanisms, the system enables secure and efficient data sharing without relying on centralized certificate authorities.

Overall, the proposed approach provides a scalable and secure solution for decentralized access control, making it suitable for applications such as cloud data sharing, healthcare data management, and decentralized storage systems built on blockchain technology.

Visualization and Output:

Fig. 2. wed page

Fig. 3. login page

Fig. 4. file upload

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Fig. 5. files

VI. CONCLUSION

This research successfully addresses the critical security and performance limitations present in existing Certificateless Proxy Re-Encryption (CL-PRE) schemes applied within blockchain environments. By identifying and formally analyzing a severe public key replacement vulnerability in Wang et al.'s CL-PRE construction, we demonstrated that Type I adversaries can fully compromise message confidentiality through malicious public key substitution. To mitigate this risk, we proposed an enhanced CL-PRE framework specifically optimized for decentralized systems. The improved framework achieves a robust balance between security and efficiency, outperforming state-of-the-art secure schemes by 14.1% while simultaneously reducing gas consumption by 14.3% and minimizing on-chain storage requirements by 40%. These gains are made possible by the introduction of three key innovations: a zero-knowledge–based authenticated key binding mechanism, a distributed validation protocol incorporating Byzantine fault tolerance, and blockchain-native integrity verification techniques. Overall, the proposed CL-PRE model significantly strengthens secure data sharing in blockchain ecosystems by eliminating critical attack surfaces and optimizing operational overhead. The results confirm that the enhanced framework is practical, scalable, and resilient for real-world blockchain applications, providing a strong foundation for future advancements in decentralized access control and cryptographic security.

REFERENCES

[1] L.Wang, K.-f. Chen, X.-p. Mao, Y.-t. Wang, Efficient and provably securecertificateless proxy re-encryption scheme for secure cloud data sharing, Journal of Shanghai Jiatong University(Science) 19 (4) (2014) 398–405.

[2] M. Mambo, E. Okamoto, Proxy cryptosystems: Delegation of the power to decrypt ciphertexts, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 80 (1) (1997) 54–63.

[3] M. Blaze, G. Blumer, M. J. Strauss, Divertible protocols and atomic proxy cryptography, International Conference on the Theory and Applications of Cryptographic Techniques: EUROCRYPT 1998: Advances in CryptologyEUROCRYPT'98 1403 (1998) 127–144.

[b4] A.-A. Ivan, Y.Dodis, Proxy cryptography revisited, Proceedings of the Net-work and Distributed System Security Symposium(NDSS) (2003) 1–20.

[4] D. Boneh, M. K. Franklin, Identity-based encryption from the weil pairing, Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology 32 (2001) 213–229.

[5] M. Green, G. Ateniese, Identity-based proxy re-encryption, Proceedings ofthe 5th International Conference on Applied Cryptography and Network Security 2006 (2007) 288–306.

[6] B. Libert, D. Vergara, Unidirectional chosen-ciphertext secure proxyreencryption, Public Key Cryptography, Lecture Notes in Computer Sci-ence 4939 (2008) 360–379.

[7] S. Chow, J. Weng, Y. Yang, R. Deng, Efficient unidirectional proxy re-encryption, Progress in Cryptology - AFRICACRYPT 2010 6055 (2010)316–332.

[8] A. Shamir, Identity-based cryptosystems and signature schemes, Advance sin Cryptology, CRYPTO 1984, Lecture Notes in Computer Science 196(2000) 47–53.

[9] S. S. Al-Riyami, K. G. Patterson, Certificateless public key cryptography, Advances in Cryptology, ASIACRYPT 2003, Lecture Notes in Computer Science 2894 (2003) 452–473.

[10] C. Sur, C. D. Jung, Y. Park, K. H. Rhee, Chosen-ciphertext secure centi-katals proxy re-encryption, In Communications and Multimedia Security,11th IFIP TC 6/TC 11 International Conference, CMS 2010, Linz, Austria6109 (May 31 - June 2, 2010) 214–232.

[11] S. S. D. Selvi, A. Paul, S. Diri Sala, S. Basu, C. P. Rangan, Sharing of encrypted files in blockchain made simpler, IACR(International Association for Cryptologic Research) Cryptology ePrint Archive 2019 (2019)418–433.

[12] A. Cohen, What about bob? The inadequacy of CPA security for proxyreencryption, Public Key Cryptography, Lecture Notes in Computer Sci-ence 11443 (2019) 287–316.

[13] A. P. S. Sharmila Deva Selvi, C. P. Rangan, An efficient certificatelessproxy re-encryption scheme without pairing, Provable Security, Lecture Notes in Computer Science 10592 (2017) 413–433.

[14] X. Zhang, X. Li, S. Chen, Identity-based certificateless proxy reencryptionfor secure it, IEEE Transactions on Industrial Informatics 15 (2) (2019)1223–1231.