International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Protection of Personal Privacy Data with Enhanced Encryption & Revocation (PEER)

Mr. K. Sairam[1], Tella Shiva Keerthi[2], Sutari Aishwariya[3], Elishetti Bhavya[4]

[1]Assistant Professor, Department of Computer Science and Engineering, Nalla Narasimha Reddy Education Society's Group of Institutions, Hyderbad, India
[2,3,4]Scholar, Department of Computer Science and Engineering, Nalla Narasimha Reddy Education Society's Group of Institutions, Hyderbad, India

Abstract:
In light of frequent non-public statistics breaches, safeguarding such facts is now greater crucial than ever. By combining Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with blockchain, stable facts storage and sharing are facilitated. However, in excessive-dimensional characteristic domains, existing schemes stumble upon issues like compromised safety, excessive computational overhead, and steeply-priced attribute revocation. This paper proposes a novel scheme to address those demanding situations. It includes 3 components: Fast High-dimensional Attribute Domain-based totally Message Encryption (HAD-FME) for more desirable protection and reduced computational charges, an Attribute Revocation Mechanism Based on Sentry Mode (SM-ARM) using clever contracts for green revocation, and a Blockchain-based totally Model for Personal Privacy Data Protection (BC-PPDP) integrating HAD-FME with SM-ARM. Security analysis confirms the effectiveness of HAD-FME beneath the DLIN assumption and the pride of forward and backward safety for attribute revocation. Experiments show advanced computational performance for HAD-FME and decrease revocation costs for SM-ARM as compared to present methods, with smart contracts and blockchain proving effective in making sure information safety and privateness.

Keywords: Confidential information, blockchain technology, attribute-centric encryption, data storage and distribution, attribute invalidation.

I. INTRODUCTION

The speedy advancement of technologies like cloud computing and the Internet of Things (IoT) has resulted inside the proliferation of substantial amounts of private information globally. Enterprises are continuously gathering and scrutinizing this private records, leveraging it to provide tailor-made offerings and reaping great financial gains, thereby fostering income in the facts technology for both customers and companies alike. Regrettably, in recent years, the absence of strong facts safety measures by using businesses, which include storing records in plaintext on centralized servers, has brought on a surge in non-public facts breach occurrences.

II. RELATED WORK

This paper examines current statistics safety strategies focused on blockchain and CP-ABE. It introduces numerous statistics protection schemes, including CP-ABE-primarily based characteristic revocation and verifiable ledger databases, as relevant to the study.

A. Data protection schemes

Numerous privateness facts security schemes, spanning fields like healthcare and clinical research, have emerged because of the growing series and utilization of consumer privacy information via agencies. These encompass green CP-ABE schemes for cloud storage supplied through Chen et al, and privateness and secrecy safety of blockchain by way of Lee et al. . Wang et al. proposed the RCP-ABE personal privateness data protection gadget, utilising smart contracts for get admission to control. Additionally, Kang et al. introduced a traceable and forward-steady attribute-primarily based signature scheme. While those schemes show promise, challenges which includes excessive computational overhead in excessive-dimensional attribute domain names persist.

B. CP-ABE-based attribute revocation

A focal point of CP-ABE studies is attribute revocation. Qian et al proposed a privacy-retaining private health record the usage of multi-authority attribute-based totally encryption with efficient revocation. Chen et al designed an characteristic-revocation-compliant cloud storage gadget, ensuring information get admission to rights are refreshed based on attribute revocation. Despite these advancements, schemes along with the ones proposed with the aid of Lian et al and Li et al. require computational value discount, particularly in attribute revocation eventualities related to IoT gadgets.

C. Verifiable ledger databases

Ledger databases can be categorised into permission blockchain-primarily based DLT and CLD-primarily based CLT. Gorbunova et al highlighted DLT's potential to provide an immutable and verifiable ledger

III. PROPOSED MODEL PROTECTION OF PERSONAL PRIVACY DATA WITH ENHANCED ENCRYPTION & REVOCATION (PEER)

This section deals with the proposed system, " Protection of personal privacy data with Enhanced Encryption & Revocation (PEER)" is designed with a modular structure comprising distinct modules is shown in Fig.1, each contributing to the system's overall functionality.

1. **Data Owner:** The information owner begins with the aid of registering with the software and acquiring an expert key from the trust server. Upon obtaining this key, the information proprietor proceeds to log in and receives a blockchain key from the trusted server. Using those keys, the information owner encrypts the facts and uploads it to the IPS (Information Processing System), at the same time as additionally granting permission for different customers to down load the statistics.
2. **Data User:** Utilizing this module, the user initiates registration with the software and obtains a key from the agree with server. Subsequently, the person logs in to get right of entry to documents uploaded through the proprietor and requests records from the agree with manager for blockchain attribute verification. Upon receiving the important facts, the user then requests get entry to from the IPS to down load the data, verifies the key, and proceeds with the down load process.

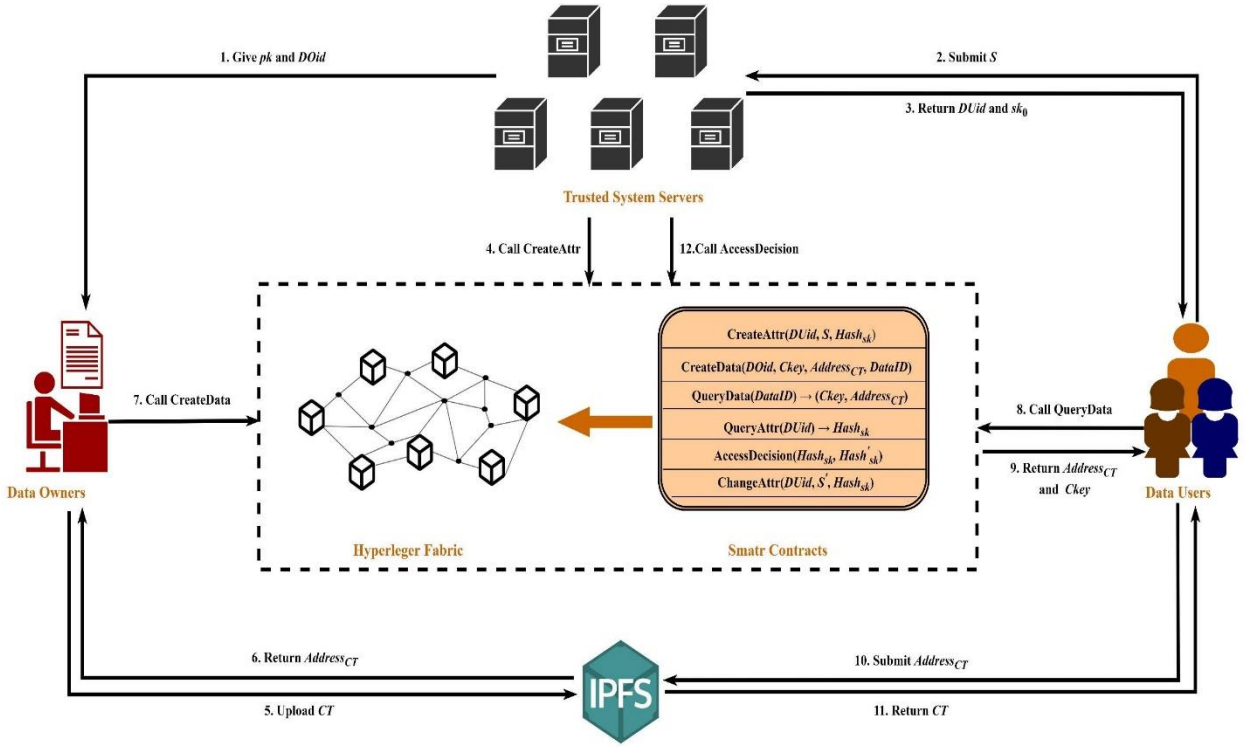

Fig1: system overview

3. **Trusted system server:** This depended on gadget server serves as the nexus wherein statistics owner and statistics consumer information are intricately related with the blockchain. Upon a success blockchain verification, users advantage get right of entry to upload records even as owners can retrieve requested statistics. Additionally, upon permission granting, the depended on machine server allows the relocation of user attributes inside the blockchain.
4. **IPFS Cloud :** Utilizing this IPFS cloud module, the proprietor uploads encrypted data to IPFS and receives down load requests from users. Subsequently, the owner gives the essential protection key to permit customers to securely download the data.

IV. Performance Test Results :

This phase covers experiments on cryptographic algorithm and blockchain overall performance. We conducted 3 schemes for overall performance trying out.

1. Experimental Environment:

Tests had been performed on an Intel Core i7-11700 processor with 16GB RAM, Ubuntu 20.04. The improvement setup used appeal-crypto0.50 for encryption, Hyperledger Fabric 2.3 for blockchain, and go-ipfs for IPFS integration.

2. Encryption Algorithm Performance Test:

We tested HAD-FME's encryption overall performance towards other schemes, watching linear growth in encryption instances with characteristic domain measurement growth. HAD-FME outperformed others for dimensions over 20. For information size effect, HAD-FME achieved high-quality for smaller facts volumes and dimensions.

3. Decryption Algorithm Performance:

Test HAD-FME exhibited advanced decryption times in comparison to scheme 1, with mild lag in the back of scheme For various facts volume, HAD-FME's decryption overhead remained decrease in comparison to scheme 1.

Schemes	Key size	Ciphertext size	Key generation
Scheme 1	$(T+1)_{\mathbb{G}} + T_{\mathbb{H}}$	$(n_1)_{\mathbb{G}} + (n_1+1)_{\mathbb{H}}$	$[(T+1)_{t_m}+(T+2)_{t_e} + T_{t_h}]_{\mathbb{G}} + (T_{t_e})_{\mathbb{H}}$
Scheme 2	$3(T+2)_{\mathbb{H}}$	$3(n_1+1)_{\mathbb{G}}$	$[3(T+2)_{t_e}]_{\mathbb{H}}$
HAD-FME	$3(T+1)_{\mathbb{G}} + 3_{\mathbb{H}}$	$(3n_1)_{\mathbb{G}} + 3_{\mathbb{H}}$	$[(8T+9)_{t_m} + (9T+9)_{t_e} + 6(T+1)_{t_h}]_{\mathbb{G}} + (3_{t_e})_{\mathbb{H}}$

Table1: schema evaluation for key size, ciphertext size and key generation.

Schemes	Encryption	Decryption
Scheme 1	$[(n_1)_{t_e} + (n_1)_{t_h}]_{\mathbb{G}} + [(n_1+1)_{t_e}]_{\mathbb{H}}$	$[(2I+1)_{\mathbb{G}_T}]_{t_m}+(2I+1)_{t_p}$
Scheme 2	$[(6n_1n_2)_{t_m} + (6n_1+9n_2)_{t_e}]_{\mathbb{G}}$	$[(3I)_{\mathbb{G}} + (3I)_{\mathbb{H}} + (6)_{\mathbb{G}_T}]_{t_m} + (6)_{t_p}$
HAD-FME	$[(12n_1n_2+6n_1)_{t_m} + (6n_1)_{t_e} + 6(n_1+n_2)_{t_h}]_{\mathbb{G}}+[(3)_{t_e}]_{\mathbb{H}}$	$[(6I+3)_{\mathbb{G}} + (6)_{\mathbb{G}_T}]_{t_m} + (6)_{t_p}$

Table2: Schema evaluation for Encryption and decryption

Schemes	Encrypt/ms	$KeyGen_{CP\text{-}ABE}$/ms	Decrypt/ms	Overall overhead/ms
Scheme 1	420.99	210.00	296.36	927.35
Scheme 2	741.10	550.28	22.30	1313.68
HAD-FME	360.96	240.00	24.43	**625.39**

Table 3: Phases and overall time overhead.

4. Key Generation Algorithm Performance Test:

HAD-FME showed competitive key technology instances, slightly slower than scheme 1 and quicker than scheme 2.

5. Phases And Overall Time Overhead:

HAD-FME tested better encryption, key generation, and general performance as compared to other schemes, particularly in high-dimensional characteristic domain names with small facts volumes.

6. Blockchain performance test

Hyperledger Calliper examined query and invoke transactions, showing applicable latency and throughput for specific transaction volumes.

7. Attribute revocation overhead test

SM-ARM exhibited green ciphertext replace with negligible overhead in comparison to Scheme 1.

Overall, our scheme outperformed others in various overall performance metrics, showcasing its suitability for excessive-dimensional attribute domains and small statistics volumes.

V. Two-line maps

Consider two multiplicative cyclic groups denoted G and G_T, both of which have the same prime order p. Let g be a generator of G . The bilinear map e: G × G → G_T satisfies the following three assumptions: Bilinearity: For any integer a, b in Z_p and elements x, y in G, it holds that e(x^a, y^b) = e(x, y)^(ab).

Irreducible: G contains elements x and y such that e(x, y) ≠ 1 .
Computational efficiency: For every x, y in G, e(x, y) can be computed efficiently.

Linear Secret-Sharing scheme (LSSS)

A linear secret-sharing scheme (LSSS) uses a method to convert access trees defined by Boolean formulas into LSSS-sharing matrices to simplify access control for multiparty scenarios Φ represents a secret-sharing scheme in a multiparty group P in, linearly defined on Z_p, satisfying the following conditions:
The proportion of all participants is a vector in Z_ p.
There exists a linear hidden shared structure (M, ρ), where M is a shared generation matrix of l × n dimensions, with l rows and n columns. Each M row is defined by M_ i Mi. The function ρ assigns the row index I to the location of the participant.
A random number r_2, …, r_ n ∈ Z_ p is chosen for the hidden value s, and a color vector v = (s, r_2, …, r_n) is generated. The latent part of s is computed as λ_ i = (M_ i · v), where λ_ i is related to ρ(i).
Moreover, LSSS exhibits linear reconstruction, where arbitrary licenses S in LSSS and A with access structure A, and the set I ⊂ {1, …, l}, with I = {i : ρ(i).) ∈ S} for. , . A linear combination of parts {λ_i} can naturally reconstruct the hidden s.

Edwards-Curve Digital Alphabet System (EdDSA): The Edwards Curved Digital Signature Algorithm (EdDSA) is an Edwards based deterministic signature algorithm. The initial parameters of the Edwards25519 curve, denoted as PP = (q, F_ q, c, d, B, n, H_1, H_2), include q = 2^255 - 19 as the F _q characteristic, where c, d ∈ F _q Define into the Edwards curve E_cd : cx^2 + y^2 = 1 + dx^2y^2 B represents the initial point in E_cd(F _q). The prime number n represents the configuration B of the basis point.
In addition, the cryptographic hash functions H_1: {0, 1}^K → {0, 1}^n and H_2: {0, 1}* → Z ^n are used, and the parameter b' is used to implement 2b handle ' - 100 . has been selected. 1 > q, the standard value of the Edwards25519 curve is 256

3. Knowledge Without Evidence (ZKP) 1.1.

To protect privacy, users use zero-knowledge proofs (ZKPs) to prove that lists of attributes are in different jurisdictions. In ZKP, a stonecutter chooses ω ∈ Z_R^*p and computes w = g^ω (mod p), c = H(a, g^S), and z = (cS + ω) mod q, where p and q are sufficiently large primes, and g is an integer of order q.
The estimator uses a nonzero knowledge proof ZKP = {w, g^S, z, c} to the power center, which determines whether w is equal to g^z · (g^-S)^c (mod p), or . . . . . where c'. = H(w, g^S).

System Definition

In this section, we demonstrate the design of a new privacy enhancement algorithm consisting of hierarchical data access control (HDAC) and attribute convergence confidentiality mechanism (ACCM), which culminates in the HD-MAC-DHE algorithm

Hierarchical access control based on LSSS:

The HDAC architecture enables the integration of multiple hierarchically connected access points into a cohesive function, facilitating multi-directional access control As shown expressed in the program, access methods such as A' and A" are merged into a compiled access method A _total. As a result, there are attributes that satisfy full access that enable users full decryption, while those that provide partial access get the satisfaction in restricted access.

S_3 = Ω*T/3* * λ = (0 - 1) * (-2 - 3) =
S_2 = Ω*T/2* * λ _ A = (-1-1) * (-2-3) =

Attribute convergence privacy policy based on convergence encryption:

The ACCM framework uses Convergent Encryption to mask access methods and user attributes, ensuring that advanced privacy protection is provided. In this approach, access methods and user attributes are hidden, represented as "secret" entities, replacing specific values with placeholders such as "*", "**", etc Convergence encryption, which relies on plaintext hash values as convergence keys , establishes a unique mapping between plaintext and ciphertext. Using this principle, the ACCM system encrypts the access policy and user attributes, allowing decryption if the accessed attributes are the user use it to match only if

k_i = KeyGen_SM3(S_i);

c_i = Enc_SM4(k_i, S_i);

S_CH_i = private_SM3(c_i) .

4.4.4.4. Algorithm definition

The HD-MAC-DHE framework contains seven specific policies that address privacy challenges in hierarchical data centric environments These policies include configuration policies implemented through user access (UAC) and attribute access so continuous (AAC), zero-knowledge proof generation, attribute convergence encryption , signature generation, key generation, encryption, decryption processes f are included Through these algorithms, HD-MAC-DHE ensures privacy protection robust, secure data transmission, and efficient access in hierarchical data ecosystems, providing a complete solution for deploying privacy-sensitive applications

3. Private key generation:

here are two important Private Key Generation Algorithms, namely UAC .KeyGen and AAC .KeyGen, which manage the private key generation part of the hierarchical data access control framework

UAC .KeyGen:

The UAC. KeyGen algorithm used by User Access Control (UAC) is central to generating a partial private key for users. Edwards25519 After receiving the curve parameter x, the UAC master key x1, and the signature information xd, the UAC begins the key generation process First, the UAC computes the l=c=2(x, xb)mod θm and verify the genuine signature by the x=x+1 equation θ θ θ θ. If the signature is valid and considered legitimate based on the users θ θ, the UAC proceeds to compute G=x1·d, generating a partial secret key x1, which is then used to the user

x1=(c=c1+b2·cb) 1 .

AAC.KeyGen:

Generated by Attribute Access Control (AAC), the AAC.KeyGen algorithm obtains a public key md and sets the user's private attribute θm as input AAC begins by binding each private attribute of x to a random number x a after the corresponding match associated with θM θ (. d)d, the AAC issues a portion of the private key x2, which is then sent to the user.

c2=(c=cb,∀c∈b:c==(c)d)

Once a partial secret key is obtained from the UAC and AAC, the user can combine them to obtain a complete secret key Xd.

x=(c,c,∀cj∈b:j))

VI. Conclusion and Future scope

Our proposed non-public privacy statistics safety scheme addresses the important thing demanding situations of low protection, excessive computational overhead, and exorbitant attribute revocation

costs generic in present schemes tailor-made for high-dimensional characteristic domain names. Leveraging HAD-FME, constructed upon FAME and SM4, guarantees strong protection even as minimizing computational burdens, thereby assembly the stringent demands of stable information storage and sharing in such domains. Additionally, our design of the Attribute Revocation Mechanism Based on Sentry Mode (SM-ARM) successfully reduces characteristic revocation prices by using updating best the consumer version key. Acknowledging positive assumptions made on this paper, consisting of barriers in STSS having access to complete DU private keys and performance constraints in blockchain systems, future research endeavours will recognition on exploring multi-authority-primarily based key era schemes to ensure DU protection. Moreover, we goal to analyse privacy data safety schemes based totally on high-overall performance tamper-evidence systems to decorate scheme throughput and overall performance further.

Future scope:

In addition to laying the basis for the CEDC problem, our research opens up diverse future studies directions. We intention to discover dynamic side server cache control, person mobility considerations, and advanced safety features. Specifically, we plan to integrate steganography into our gadget to decorate information security. By embedding statistics within pix, we will add an extra layer of safety in opposition to unauthorized get entry to. These efforts will ultimately improve system performance, adaptability, and security for better user reports.

VII. References:

1. Zhou, L., Qin, K., Torres, C. F., Le, D. V., & Gervais, A. (2021). High-frequency trading on decentralized on-chain exchanges. In Proc. IEEE Symp. Secur. Privacy (SP), pp. 428–445. Doi: 10.1109/sp40001.2021.00027.
2. Androulaki, E., et al. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proc. 13th EuroSys Conf., pp. 1–15. Doi: 10.1145/3190508.3190538.
3. Yang, X., et al. (2020). LedgerDB: A centralized ledger database for universal audit and verification. Proc. VLDB Endowment, 13(12), pp. 3138–3151. Doi: 10.14778/3415478.3415540.
4. Yue, C., et al. (2023). GlassDB: An efficient verifiable ledger database system through transparency. Proc. VLDB Endowment, 16(6), pp. 1359–1371. Doi: 10.14778/3583140.3583152.
5. Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. In Proc. IEEE Symp. Secur. Privacy (SP), pp. 321–334. Doi: 10.1109/SP.2007.11.
6. Agrawal, S., & Chase, M. (2017). FAME: Fast attribute-based message encryption. In Proc. ACM SIGSAC Conf. Comput. Commun. Secur., pp. 665–682. Doi: 10.1145/3133956.3134014.
7. Waters, B. (2011). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Proc. Int. Workshop Public Key Cryptogr., pp. 53–70. Doi: 10.1007/978-3-642-19379-8_4.
8. Chen, J., Gay, R., & Wee, H. (2015). Improved dual system ABE in prime-order groups via predicate encodings. In Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn., pp. 595–624. Doi: 10.1007/978-3-662-468036_20.
9. Zhang, Y., He, D., & Choo, K.-K.-R. (2018). BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT. Wireless Commun. Mobile Comput., pp. 1–9. Doi: 10.1155/2018/2783658.

10. Sharma, P., Jindal, R., & Borah, M. D. (2021). Blockchain-based decentralized architecture for cloud storage system. J. Inf. Secur. Appl., 62, Art. No. 102970. Doi: 10.1016/j.jisa.2021.102970.
11. Lu, X., & Fu, S. (2021). A trusted data access control scheme combining attribute based encryption and blockchain. Netinfo Secur., 21(3), pp. 7–8. Doi: 10.3969/j.issn.1671-1122.2021.03.002.
12. Yang, Z., Huang, S., & Zheng, C. Y. (2022). Study on crowdsourced testing intellectual property protection technology based on blockchain and improved CP-ABE. Comput. Sci., 49(5), pp. 325–332. Doi: 10.11896/jsjkx.210900075.
13. Liu, P., He, Q., & Liu, W. Y. (2020). CP-ABE scheme supporting attribute revocation and outsourcing decryption. Netinfo Secur., 20(3), pp. 90–97. Doi: 10.3969/j.issn.1671-1122.2020.03.012.