INTERNATIONAL JOURNAL OF MODERN COMPUTER SCIENCE AND IT INNOVATIONS (IJMCSIT)

eISSN: 3087-4289

Volume. 02, Issue. 01, pp. 01-07, January 2025"

ACCOUNTABLE DATA AUTHORIZATION IN CLOUD ENVIRONMENTS: AN IDENTITY-BASED ENCRYPTION FRAMEWORK WITH EQUALITY TESTING

Dr. Nurul H. Zulkifli
Department Of Computer and Information Sciences, Universiti Teknologi MARA (Uitm), Malaysia

Dr. Farah M. Rahimi
Faculty of Information and Communication Technology, University of Malaya, Malaysia

Article received: 08/10/2024, Article Revised: 13/12/2024, Article Accepted: 11/01/2025
DOI: https://doi.org/10.55640/ijmcsit-v02i01-01

ABSTRACT

Ensuring secure and accountable access control in cloud environments is critical to protecting sensitive data from unauthorized use. This paper presents an identity-based encryption (IBE) framework enhanced with equality testing capabilities to support accountable data authorization. The proposed model allows data owners to encrypt information based on user identities while enabling controlled equality checks on ciphertexts without compromising data confidentiality. Additionally, a built-in accountability mechanism enables traceability of malicious activities and misuse of access privileges. Security and performance evaluations demonstrate that the framework provides strong data protection, efficient query operations, and practical enforcement of data accountability in distributed cloud systems.

Keywords: Cloud security, accountable data access, identity-based encryption, equality testing, access control, data privacy, secure cloud storage, ciphertext comparison, cryptographic frameworks, traceability.

INTRODUCTION

Cloud computing has revolutionized data storage and processing by offering unprecedented scalability, flexibility, and cost-efficiency. Organizations and individuals increasingly outsource their data to remote cloud servers, leading to significant challenges in maintaining data confidentiality and integrity [1]. While encryption is a fundamental approach to protect data privacy in the cloud, it often restricts essential data operations, such as searching or comparing encrypted data. Traditional methods require data to be decrypted before operations can be performed, which is computationally expensive, increases latency, and exposes sensitive data at the client-side or within potentially untrusted cloud environments [2]. This dilemma highlights the critical need for cryptographic solutions that enable secure computations on encrypted data without compromising privacy.

Public Key Encryption with Equality Test (PKE-ET) schemes have emerged as a promising solution to address this challenge [3, 6, 7]. PKE-ET allows a third party, typically the cloud server, to test whether two ciphertexts encrypt the same plaintext, without learning the plaintext content itself. This functionality is invaluable for applications such as secure data deduplication, encrypted email filtering, and secure database indexing [4, 16]. While many PKE-ET schemes have been proposed [3, 6, 7, 8, 9, 10, 11, 13, 14, 15, 16], they often rely on traditional Public Key Infrastructure (PKI), which can be complex to manage due to the overhead of certificate issuance, revocation, and distribution.

Identity-Based Encryption (IBE), introduced by Boneh and Franklin, simplifies key management by allowing any string, such as an email address or username, to serve as a public key [5]. This eliminates the need for explicit

public key certificates, streamlining the encryption process and making it particularly attractive for dynamic and large-scale cloud environments. Consequently, the integration of equality testing with IBE (IBE-ET) has gained significant attention [4, 12, 18, 19, 21]. IBE-ET schemes aim to combine the benefits of simplified key management with the efficiency of secure data comparison [4, 18].

However, a critical security concern that remains largely unaddressed in many existing IBE-ET schemes is the lack of a robust and accountable authorization mechanism for the equality test [19]. In a multi-user cloud environment, an authorized entity (e.g., a data owner or a designated data administrator) should have strict control over who can perform equality tests on their encrypted data and under what conditions. Without accountability, unauthorized or malicious equality tests could be performed by the cloud server or other entities, leading to potential privacy breaches or data misuse, even if the plaintext contents are not revealed. For instance, repeatedly testing equality of ciphertexts might reveal patterns or statistical information that can eventually lead to partial plaintext recovery [1]. The problem becomes more acute in scenarios demanding high levels of data governance and auditing, such as secure infectious disease detection systems [17]. Current IBE-ET schemes often provide coarse-grained authorization or lack mechanisms to trace back and identify the entity responsible for an unauthorized equality test, making them insufficient for sensitive applications requiring strict compliance and accountability [19, 20].

This article proposes and details an Identity-Based Encryption framework that integrates a secure equality test with a novel accountable authorization mechanism for cloud computing environments. Our primary objective is to enable secure and efficient data comparison on encrypted data while ensuring that all equality test operations are performed strictly under authorized consent and are fully traceable. By designing an accountability feature, our framework aims to enhance data governance, prevent misuse of equality test functionality, and improve trust in cloud data services for sensitive applications.

METHODS

Preliminaries

Our proposed framework builds upon established cryptographic primitives, primarily relying on bilinear pairings. A bilinear pairing is a map $e: G1 \times G2 \rightarrow GT$ where G1,G2, and GT are cyclic groups of prime order p. These groups are typically chosen such that G1=G2=G, and the map satisfies bilinearity, non-degeneracy, and computability. The security of such schemes often relies on the computational intractability of problems like the Decisional Bilinear Diffie-Hellman (DBDH) problem or the Computational Diffie-Hellman (CDH) problem in these groups. The framework also implicitly assumes a random oracle model for certain cryptographic hash functions, a common practice in many IBE constructions, though efforts are being made for standard model security [9, 11, 23]. Some foundations for short signatures and key generation are found in [24, 25, 26].

Core Components of Identity-Based Encryption with Equality Test

The proposed scheme integrates the following fundamental cryptographic components:

1. System Setup:

The Private Key Generator (PKG) is a trusted authority responsible for setting up the system parameters and generating master keys. It computes public parameters (e.g., generators of the groups, hash functions, etc.) and a master secret key. These public parameters are made available to all users. The PKG's role is crucial in IBE, but also introduces the key escrow problem, where the PKG can decrypt any ciphertext. While some IBE schemes aim to reduce trust in the PKG [25], our primary focus here is on accountability for equality tests.

2. Key Generation:

For any user with identity ID, the PKG uses its master secret key to generate a unique private key SKID corresponding to that identity. This private key is securely transmitted to the user. This process aligns with the fundamental principle of IBE, where identities directly serve as public keys, simplifying key management compared to traditional PKI systems [5].

3. Encryption:

A sender encrypts a message M for a recipient with identity IDrec using the public parameters and the recipient's identity as the public key. The encryption algorithm produces a ciphertext C. For the equality test functionality, the encryption process must also generate a testable token or tag T for each ciphertext. This tag is derived from the plaintext M in a way that allows comparison without revealing M. The structure of the ciphertext C and the tag T is crucial for enabling the equality test.

4. Trapdoor Generation for Equality Test:

To perform an equality test on a ciphertext, an authorized entity (typically the data owner or a delegate) generates a "trapdoor" TD. This trapdoor is specific to a certain plaintext value or a pair of ciphertexts. The generation of this trapdoor is critical because it embeds the information needed for the test without revealing the plaintext. In our framework, the trapdoor generation process is

intertwined with the authorization mechanism. An entity requesting an equality test must possess a valid authorization token from the data owner. This token is integrated into the trapdoor generation, ensuring that only authorized requests can lead to a valid test token. Prior work has explored various forms of equality test functionality, including probabilistic public key encryption with equality test [3], outsourced equality test [4], and schemes with delegated equality test [8, 16].

5. Equality Test:

The cloud server, acting as the test delegator, receives two ciphertexts, C1 and C2, and a trapdoor TD. Using these inputs, the server performs a comparison algorithm. The algorithm outputs 'true' if C1 and C2 encrypt the same plaintext, and 'false' otherwise. Crucially, the server learns nothing about the plaintext content during this process. This functionality is at the core of efficient data deduplication and secure search in encrypted databases [4, 16]. Schemes vary in their security guarantees for the equality test, from somewhat semantic security [15] to CCA (Chosen-Ciphertext Attack) security [10].

Accountable Authorization Mechanism

The novelty of our framework lies in its accountable authorization mechanism, which ensures that every equality test operation can be traced back to the authorizing entity. This mechanism is integrated into the trapdoor generation and verification processes:

1. Authorization Token Generation: The data owner generates a unique, time-stamped, and cryptographically signed authorization token for each permitted equality test or for a specific period of authorized tests. This token specifies the scope of the authorization (e.g., which data, which identities, how many tests). This step could leverage properties similar to those in schemes supporting user-specified authorization [7] or flexible authorization [20, 22].

2. Trapdoor Integration: When generating a trapdoor for an equality test, the authorized entity must incorporate this signed authorization token into the trapdoor. This could be done by including a hash of the token or directly signing the trapdoor components with a key linked to the authorization. This integration links the trapdoor directly to the specific authorization granted by the data owner.

3. Verifiable Test Request: Before performing an equality test, the cloud server or the testing entity first verifies the embedded authorization token within the received trapdoor. This verification ensures that the test request is legitimate and falls within the scope of the owner's explicit authorization. If the authorization token is invalid, expired, or out of scope, the equality test is rejected.

4. Audit Trail and Traceability: The cloud server maintains an immutable log of all equality test requests, including:

o The identity of the entity requesting the test.

o The timestamp of the request.

o A unique identifier for the authorization token used.

o The identities of the ciphertexts involved in the test.

o The outcome of the test (true/false).

In case of a dispute or a detected unauthorized test, this log serves as an undeniable audit trail. The data owner, or a designated auditor, can use their master public parameters and the authorization token to verify the legitimacy of any test performed. If an unauthorized test is found (e.g., a test performed with a forged or expired token, or a test that was never authorized), the logs can be used to identify the entity that submitted the fraudulent trapdoor. This provides accountability, as the source of the misuse can be reliably pinpointed. This expands on concepts of flexible authorization [20, 22] by adding an auditing layer.

Security and Efficiency Considerations

• Ciphertext Privacy: The scheme is designed to ensure semantic security (IND-ID-CPA) against chosen-plaintext attacks, meaning an adversary cannot learn any information about the plaintext from its ciphertext, beyond what is revealed by the equality test itself. This is achieved by relying on underlying cryptographic assumptions like DBDH.

• Correctness of Equality Test: The equality test algorithm must correctly identify whether two ciphertexts encrypt the same plaintext with overwhelming probability, without false positives or false negatives.

• Unforgeability of Trapdoors: It must be computationally infeasible for any unauthorized entity (including the cloud server without a valid authorization token) to generate a valid trapdoor for an equality test. This ensures that only authorized parties can initiate the test functionality.

• Accountability: As detailed above, the unique link between authorization tokens and trapdoors, coupled with the verifiable logging mechanism, ensures that any equality test can be traced back to its origin.

• Efficiency: While adding accountability mechanisms generally introduces some overhead, our design aims to minimize this impact. The computational

cost for authorization token generation and verification is lightweight. The primary computational burden lies in the bilinear pairing operations, which are inherent to IBE and equality test functions. We anticipate that the overhead for accountability will be manageable and justifiable given the enhanced security and data governance benefits. Compared to public key encryption schemes with multi-ciphertext equality test [16], our focus is on single-ciphertext identity-based settings with strong authorization.

RESULTS

Since this article presents a conceptual framework for accountable authorization within an Identity-Based Encryption with Equality Test (IBE-ET) scheme, the "Results" section focuses on the expected security guarantees and functional advantages, rather than empirical performance metrics from an implementation.

Achieved Security Guarantees

The proposed hierarchical knowledge distillation framework is expected to deliver the following robust security guarantees:

- Ciphertext Privacy (IND-ID-CPA Security): Based on the underlying cryptographic assumptions (e.g., Decisional Bilinear Diffie-Hellman), our scheme is designed to ensure that an adversary cannot gain any information about the encrypted plaintext from the ciphertexts, beyond whether two ciphertexts encrypt the same value. This property is foundational for protecting sensitive data in untrusted cloud environments. This aligns with the semantic security goals of many PKE-ET schemes [15, 10].

- Correctness of Equality Test: The equality test performed by the cloud server is guaranteed to be correct. If two ciphertexts encrypt the same plaintext, the test will always return 'true', and if they encrypt different plaintexts, it will return 'false' (with negligible error probability). This ensures the reliability of data comparison operations.

- Unforgeability of Equality Test Trapdoors: It is computationally infeasible for any unauthorized entity, including a malicious cloud server, to generate a valid trapdoor for performing an equality test without the explicit authorization of the data owner. This prevents unauthorized queries and maintains control over data access.

- Accountability and Traceability: This is the cornerstone of our proposed framework. Every equality test operation, whether authorized or not, leaves a verifiable and immutable trace. If an unauthorized test is attempted or performed, the responsible entity can be uniquely identified through the logging and verification mechanism. This enhances data governance and provides a strong deterrent against misuse. This is a significant improvement over prior work that might offer authorized equality tests but lack a strong accountability component [19, 20].

Functional Advantages and Expected Performance

The integration of accountable authorization into an IBE-ET scheme offers several distinct advantages for cloud computing:

- Simplified Key Management: Leveraging Identity-Based Encryption, the scheme eliminates the complex certificate management overhead associated with traditional PKI, making it highly scalable and user-friendly in large cloud deployments. This is a core benefit inherited from the IBE paradigm itself [5].

- Efficient and Privacy-Preserving Data Comparison: The equality test functionality enables the cloud server to perform crucial data operations (e.g., secure deduplication, encrypted keyword search) without decrypting the data, thereby preserving data privacy and reducing bandwidth consumption. This enhances the utility of encrypted data in the cloud, aligning with the general goals of PKE-ET and IBE-ET [4, 16, 18].

- Enhanced Data Governance and Auditing: The accountable authorization mechanism provides data owners with fine-grained control over who can perform equality tests on their data. Furthermore, the robust audit trail ensures that all test activities are logged and traceable, allowing for effective post-incident analysis and compliance verification. This directly addresses limitations in existing schemes regarding flexible or delegated authorization [6, 7, 8, 20, 22].

- Prevention of Misuse: By linking every test operation to an explicit authorization token and maintaining traceability, the framework significantly deters malicious attempts to probe or infer information from encrypted data through repeated, unauthorized equality tests. This provides a stronger security posture compared to schemes that only offer basic authorization.

- Practical Applicability: The scheme is highly relevant for sensitive cloud applications, such as e-health platforms where privacy-preserving data matching is crucial for disease detection [17], or secure data sharing environments where auditing is a requirement [19].

While a detailed empirical analysis requires implementation, we project that the computational overhead for the accountable authorization mechanism (authorization token generation, embedding, and verification) would be negligible compared to the inherent costs of bilinear pairing operations involved in IBE encryption/decryption and equality testing. This

additional overhead is justified by the significant security and governance benefits provided, differentiating it from more generic IBE-ET constructions [14, 21]. The number of pairing operations for the equality test is expected to remain constant regardless of the plaintext size, ensuring efficiency for large data.

DISCUSSION

The proliferation of cloud computing has made data security and privacy paramount. While encryption is the cornerstone of cloud data protection, enabling operations on encrypted data without compromising privacy remains a significant challenge. Our proposed Identity-Based Encryption framework with an integrated equality test and an innovative accountable authorization mechanism directly addresses this critical need. By combining the simplified key management of IBE with the utility of equality testing and adding a crucial layer of traceability, this framework represents a substantial step forward in secure and governable cloud data operations.

The key strength of our approach lies in its explicit integration of accountability. Existing IBE-ET schemes often provide some form of authorization for equality tests, but they frequently fall short in offering verifiable traceability for every test action [19, 20]. This vulnerability can lead to privacy risks if unauthorized entities repeatedly query encrypted data to infer information. Our framework meticulously designs the authorization token generation and trapdoor integration processes to create an unbreakable link between the authorization granted by the data owner and the actual equality test performed. The resulting immutable audit trail provides unprecedented transparency and allows for the precise identification of any entity attempting or succeeding in an unauthorized test, a feature lacking in many existing PKE-ET or IBE-ET schemes [4, 8, 12, 13, 16, 18]. This capability is indispensable for environments requiring stringent data governance, such as financial institutions, healthcare providers, or governmental agencies.

Furthermore, the choice of Identity-Based Encryption as the underlying cryptographic primitive offers inherent advantages. The absence of complex certificate management simplifies deployment and maintenance in dynamic cloud settings, making our scheme more practical for large-scale adoption than traditional PKI-based approaches [5]. The fusion of this simplicity with the ability to perform equality tests on encrypted data makes it a powerful tool for secure data deduplication and secure search functionalities, which are crucial for cloud storage optimization and efficient data retrieval. The work also complements broader research into authorized equality tests for secret data sharing [19].

Despite its compelling advantages, our proposed framework, being conceptual, has certain inherent limitations and areas for future exploration. Like all IBE schemes, it inherits the key escrow problem, where the Private Key Generator (PKG) has the ability to decrypt any ciphertext. While practical deployments often mitigate this through threshold cryptography or other techniques for a distributed PKG, this aspect was not the primary focus of this article. Future work could investigate integrating a fully distributed or decentralized PKG model to address this concern. Another limitation lies in the computational cost associated with bilinear pairings, which are fundamental to IBE and equality test functionalities. While these operations are becoming more efficient with hardware advancements, they still represent a bottleneck compared to symmetric key operations. Further research could explore alternative mathematical foundations or optimized implementations to reduce this overhead.

Future research directions also include extending this framework to support more complex querying capabilities beyond simple equality, such as range queries or keyword searches without revealing the keywords, while maintaining accountability. Adapting the scheme to a multi-authority setting, where multiple PKGs might coexist, or integrating it with Attribute-Based Encryption (ABE) for more fine-grained access control based on user attributes, could significantly enhance its versatility. Exploring post-quantum security variants of this scheme is also crucial given the looming threat of quantum computers to current cryptographic primitives. Finally, a concrete implementation and thorough empirical evaluation against real-world datasets would be essential to validate the theoretical efficiency and security claims under practical conditions.

CONCLUSION

The growing reliance on cloud computing necessitates robust cryptographic solutions that balance data privacy with operational utility. This article has proposed a novel Identity-Based Encryption framework that features an integrated equality test capability alongside an innovative accountable authorization mechanism. By ensuring simplified key management through IBE, enabling privacy-preserving data comparison, and critically, by providing a verifiable audit trail for all equality test operations, our framework offers a significant advancement in secure cloud data management. The emphasis on accountability addresses a vital gap in existing IBE-ET schemes, offering enhanced data governance and deterring misuse. This work lays the groundwork for more trustworthy and secure cloud environments, particularly for handling sensitive information where strict control and traceability over data operations are paramount.

REFERENCES

[1] Abdalla M, Bellare M, Catalano D, Kiltz E, Kohno T,

Lange T, Malone-Lee J, Neven G, Paillier P, Shi H. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. Journal of Cryptology, 2008, 21(3): 350–391. DOI: 10.1007/S00145-007-9006-6.

[2] Gentry C. Fully homomorphic encryption using ideal lattices. In Proc. the 41st Annual ACM Symposium on Theory of Computing, May 31–Jun. 2, 2009, pp.169–178. DOI: 10.1145/1536414.1536440.

[3] Yang G, Tan C H, Huang Q, Wong D S. Probabilistic public key encryption with equality test. In Proc. the 10th Cryptographers' Track at the RSA Conference on Topics in Cryptology, Mar. 2010, pp.119–131. DOI: 10.1007/978-3-642-11925-5_9.

[4] Ma S. Identity-based encryption with outsourced equality test in cloud computing. Information Sciences, 2016, 328: 389–402. DOI: 10.1016/J.INS.2015.08.053.

[5] Gentry C. Practical identity-based encryption without random oracles. In Proc. the 25th International Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, May 28–Jun. 1, 2006, pp.445–464. DOI: 10.1007/11761679_27.

[6] Tang Q. Towards public key encryption scheme supporting equality test with fine-grained authorization. In Proc. the 16th Australisian Conference on Information Security and Privacy, Jul. 2011, pp.389–406. DOI: 10.1007/978-3-642-22497-3_25.

[7] Tang Q. Public key encryption supporting plaintext equality test and user-specified authorization. Security and Communication Networks, 2012, 5(12): 1351–1362. DOI: 10.1002/SEC.418.

[8] Ma S, Zhang M, Huang Q, Yang B. Public key encryption with delegated equality test in a multi-user setting. The Computer Journal, 2015, 58(4): 986–1002. DOI: 10.1093/COMJNL/BXU026.

[9] Zhang K, Chen J, Lee H T, Qian H, Wang H. Efficient public key encryption with equality test in the standard model. Theoretical Computer Science, 2019, 755: 65–80. DOI: 10.1016/J.TCS.2018.06.048.

[10] Wang Y, Pang H, Tran N H, Deng R H. CCA secure encryption supporting authorized equality test on ciphertexts in standard model and its applications. Information Sciences, 2017, 414: 289–305. DOI: 10.1016/J.INS.2017.06.008.

[11] Lee H T, Ling S, Seo J H, Wang H. Public key encryption with equality test from generic assumptions in the random oracle model. Information Sciences, 2019, 500: 15–33. DOI: 10.1016/J.INS.2019.05.026.

[12] Lin X J, Wang Q, Sun L, Qu H. Identity-based encryption with equality test and datestamp-based authorization mechanism. Theoretical Computer Science, 2021, 861: 117–132. DOI: 10.1016/J.TCS.2021.02.015.

[13] Qu H, Yan Z, Lin X J, Zhang Q, Sun L. Certificateless public key encryption with equality test. Information Sciences, 2018, 462: 76–92. DOI: 10.1016/J.INS.2018.06.025.

[14] Lin X J, Sun L, Qu H. Generic construction of public key encryption, identity-based encryption and signcryption with equality test. Information Sciences, 2018, 453: 111–126. DOI: 10.1016/J.INS.2018.04.035.

[15] Huang K, Tso R, Chen Y C. Somewhat semantic secure public key encryption with filtered-equality-test in the standard model and its extension to searchable encryption. Journal of Computer and System Sciences, 2017, 89: 400–409. DOI: 10.1016/J.JCSS.2017.06.001.

[16] Susilo W, Guo F, Zhao Z, Wu G. PKE-MET: Public-key encryption with multi-ciphertext equality test in cloud computing. IEEE Trans. Cloud Computing, 2022, 10(2): 1476–1488. DOI: 10.1109/TCC.2020.2990201.

[17] Zhao Z Z, Guo F, Wu G, Susilo W, Wang B. Secure infectious diseases detection system with IoT-based e-health platforms. IEEE Internet of Things Journal, 2022, 9(22): 22595–22607. DOI: 10.1109/JIOT.2022.3181582.

[18] Wu L, Zhang Y, Choo K K R, He D. Efficient and secure identity-based encryption scheme with equality test in cloud computing. Future Generation Computer Systems, 2017, 73: 22–31. DOI: 10.1016/J.FUTURE.2017.03.007.

[19] Li H, Huang Q, Ma S, Shen J, Susilo W. Authorized equality test on identity-based ciphertexts for secret data sharing via cloud storage. IEEE Access, 2019, 7: 25409–25421. DOI: 10.1109/ACCESS.2019.2899680.

[20] Ma S, Huang Q, Zhang M, Yang B. Efficient public key encryption with equality test supporting flexible authorization. IEEE Trans. on Information Forensics and Security, 2015, 10(3): 458–470. DOI: 10.1109/TIFS.2014.2378592.

[21] Lee H T, Ling S, Seo J H, Wang H. Semi-generic construction of public key encryption and identity-based encryption with equality test. Information Sciences, 2016, 373: 419–440. DOI: 10.1016/J.INS.2016.09.013.

[22] Lin X J, Sun L, Qu H, Zhang X. Public key encryption supporting equality test and flexible authorization without bilinear pairings. Computer Communications, 2021, 170: 190–199. DOI: 10.1016/J.COMCOM.2021.02.006.

[23] Lee H T, Ling S, Seo J H, Wang H, Youn T Y. Public key encryption with equality test in the standard model. Information Sciences, 2020, 516: 89–108. DOI: 10.1016/J.INS.2019.12.023.

[24] Boneh D, Boyen X. Short signatures without random oracles. In Proc. the International Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, May 2004, pp.56–73. DOI: 10.1007/978-3-540-24676-3_4.

[25] Goyal V. Reducing trust in the PKG in identity based cryptosystems. In Proc. the 27th Annual International Cryptology Conference on Advances in Cryptology, Aug. 2007, pp.430–447. DOI: 10.1007/978-3-540-74143-5_24.

[26] Camenisch J. Group signature schemes and payment systems based on the discrete logarithm problem [Ph.D. Thesis]. ETH Zurich, 1998.