International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

# Resource-Aware Outsourced Decryption: A Lightweight ABE Scheme for Constrained Clients and Cloud Providers

Dr. Prashant Sangulagi
Bheemanna Khandre Institute of Technology, Bhalki, Karnataka INDIA-585328

Dr. Sangmesh Kalyane
Bheemanna Khandre Institute of Technology, Bhalki, Karnataka INDIA-585328

Dr. Udaykumar Kalyane
Bheemanna Khandre Institute of Technology, Bhalki, Karnataka INDIA-585328

Shilpa P
Karnataka Arts, Science and Commerce College, Bidar, Karnataka INDIA-585401

**Abstract: In the era of the Internet of Things (IoT) and mobile cloud computing, Attribute-Based Encryption (ABE) has emerged as a primitive for fine-grained access control. However, the heavy computational cost of bilinear pairing operations during decryption remains a bottleneck for resource-constrained devices. While existing outsourced decryption schemes shift the burden to the cloud, they often introduce significant overhead for the Cloud Service Provider (CSP) or fail to minimize the communication costs for the client. This paper proposes a Resource-Aware Outsourced Decryption (RA-OD) scheme that achieves "dual-optimization." By introducing a novel transformation key mechanism, we reduce the client-side decryption to a single exponentiation while ensuring the cloud's processing remains linear and scalable. Security analysis proves our scheme is IND-CPA secure under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. Experimental results demonstrate a 40% reduction in client energy consumption compared to state-of-the-art outsourced ABE models.**

***Keywords: Attribute-Based Encryption, Outsourced Decryption, Mobile Cloud Computing, IoT Security, Resource-Aware, Bilinear Pairing, Fine-grained Access Control, Dual-Optimization.***

## 1. INTRODUCTION

The rapid evolution of the Internet of Things (IoT) and mobile cloud computing has transformed data sharing into a decentralized, one-to-many paradigm. In these ecosystems, sensitive data is often stored in semi-trusted cloud environments, necessitating robust, fine-grained access control mechanisms [1] [2] [3]. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has emerged as the gold standard for this requirement, allowing data owners to encrypt information under specific access policies that only authorized users with matching attributes can decrypt [4]. However, the practical deployment of standard CP-ABE faces a significant computational wall [5]. The decryption process typically involves multiple bilinear pairing operations—the most expensive cryptographic primitive—which grow linearly with the complexity of the access policy. For resource-constrained devices such as industrial sensors, wearable health monitors, and mobile terminals, these operations result in prohibitive latency and rapid battery depletion [6].

While existing literature has extensively explored outsourced decryption (ABE-OD) to mitigate client-side costs, a critical "imbalance" remains unaddressed in the current state-of-the-art. Most conventional ABE-OD schemes focus exclusively on offloading the user's burden, inadvertently treating the cloud server as a resource with infinite capacity [7] [8]. As the number of concurrent decryption requests from thousands of IoT nodes scales, the cloud server experiences a massive surge in computational overhead, leading to bottlenecks in "Green Cloud" data centers and increased service costs for providers [9]. Furthermore, many schemes fail to consider the communication overhead incurred when the cloud returns a transformed ciphertext, which can sometimes be larger than the original, further straining the limited bandwidth of edge networks [10]. There is an urgent need for a "dual-optimization" approach that considers the resource constraints of both the end-user and the infrastructure provider.

This paper proposes a Resource-Aware Outsourced Decryption (RA-OD) scheme designed to bridge this gap. Our primary contribution is a novel dual-optimization algorithm that leverages a "Pre-computation and Transformation" (PT) mechanism. Unlike standard models, our scheme allows the cloud server to perform a batch-style transformation of ciphertexts that share similar policy structures, significantly reducing the server-side CPU cycles per request. For the client, we achieve a "constant-time" decryption where the local device performs only a single exponentiation, regardless of policy complexity. Additionally, we introduce a lightweight verification phase that allows the user to ensure the cloud has performed the transformation honestly without re-calculating the pairings. We provide a rigorous security analysis under the Decisional Bilinear Diffie-Hellman (DBDH) assumption and demonstrate through extensive simulations that our scheme reduces the total system energy footprint by 35% compared to existing outsourced ABE frameworks [11] [12].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

The organization of the paper is structured to provide a logical and rigorous flow from theoretical foundations to empirical validation. Following the Introduction, which establishes the motivation and core contributions, Section 2 outlines the fundamental cryptographic building blocks, including bilinear pairings and access structures, required to understand the scheme's construction. Section 3 formalizes the roles of the participating entities and defines the adversarial model under which the scheme remains resilient. It also provides a step-by-step algorithmic breakdown of the setup, key generation, and the dual-optimization decryption process. Section 4 results and it also presents a comparative study of computational costs and energy efficiency using experimental simulation data. Finally, Section 5 summarizes the findings for resource-aware cloud cryptography.

## 2. LITERATURE REVIEW

In [13] author introduced an Efficient Blockchain-based Outsourced Decryption System (EBODS) that focuses on post-quantum resilience using lattice-based cryptography. While the scheme successfully mitigates Shor-style attacks and utilizes a consortium-chain for auditability, it introduces significant storage overhead—requiring nearly 240 KB of pre-computation data on the client side. This highlights a gap in "resource-awareness," as the client's storage burden is traded for computational speed. Our proposed RA-OD scheme improves upon this by maintaining a lightweight local footprint while achieving similar security levels.

In [4] author proposed a pairing-free CP-ABE scheme specifically for 6G-enabled IoT networks. By replacing expensive bilinear pairings with elliptic curve scalar multiplications, the researchers achieved a 32% speedup in encryption. However, their model lacks a robust "Cloud-Server Optimization" strategy, meaning that as the number of IoT sensors scales into the millions, the cloud's computational load increases linearly. Our RA-OD scheme addresses this "imbalance" by optimizing the server-side transformation process alongside the client's decryption.

In [14] author explored "Registered ABE" (RABE) to eliminate the need for a trusted central authority. While their "ORABE" scheme provides excellent verifiability via Ethereum smart contracts, the gas fees and high verification costs make it impractical for frequent data access in low-power industrial settings. Our research identifies this cost-inefficiency and proposes a "Payable but Optimized" model where the verification phase is designed to be mathematically lightweight rather than blockchain-heavy.

The LOR-A2ABE scheme introduced in [15] prioritizes user anonymity and efficient revocation through version-numbered timestamps. While it achieves constant-time client decryption, it requires the Cloud Service Provider to maintain massive state tables for revocation, leading to infrastructure bloat. Our proposed concept differs by employing a stateless transformation key that reduces the server's memory requirements, making it a more "Cloud-Friendly" solution for large-scale deployments.

In [9] author proposed an adaptive offloading technique that uses machine learning to decide when to outsource decryption based on the device's current battery level. While innovative, the ML model itself consumes local CPU cycles on the constrained device. Our RA-OD scheme avoids this by using a deterministic "Resource-Aware" protocol that consistently minimizes client-side work without the need for intensive local decision-making algorithms.

In [16] author developed an "EAL-CP-ABE" scheme focused on white-box tracing to prevent authorized users from leaking their private keys. Although the scheme adds a layer of accountability, the tracing mechanism doubles the length of the secret key, increasing the storage strain on mobile clients. Our work proposes a "Compressed Key" architecture that ensures security against leakage without increasing the spatial complexity of the user's credentials.

In [17] author implemented a multi-authority framework for healthcare consortium blockchains. Their focus is on high-privacy "Policy Hiding," which ensures that even the access policy itself remains encrypted. However, policy hiding increases the outsourced decryption time by approximately 50%. Our proposed RA-OD balances this by introducing a "Partial Policy Hiding" mechanism that protects PII while maintaining the efficiency of the transformation process.

In [18] author addressed the "Fairness Problem" where users may refuse to pay a cloud provider after receiving the decryption result. They used a sampling technique for verification. While effective for fairness, it does not reduce the initial pairing costs for the cloud. Our RA-OD scheme integrates fairness with "Batch Transformation," ensuring that the cloud can process multiple fair requests simultaneously to save global energy.

The work in [19] highlights the critical need for "Financial Precision" in cloud operations. They argue that unmanaged cryptographic scale accounts for 20% of cloud waste. This paper serves as the economic motivation for our RA-OD scheme, proving that an efficient decryption framework is not just a security need but a financial necessity for modern enterprises.

In [20] proposed a pairing-free scheme with "Weighted Access Policies," allowing certain attributes to have more "weight" than others. While flexible, the scheme's communication cost increases with the number of weights. Our RA-OD scheme achieves similar flexibility but ensures "Constant-Size" transformed ciphertexts, making it more efficient for narrow-bandwidth 5G/6G channels.

### 2.1 Comparative Analysis

| Paper Ref | Year | Core Technique | Client Efficiency | Cloud Efficiency | Verifiability | Gap Identified |
|---|---|---|---|---|---|---|
| **Chen et al. [13]** | 2025 | Lattice/PQ-ABE | Low (Storage) | Medium | High | High storage overhead for client. |
| **Narezal et al. [4]** | 2024 | Pairing-Free ECC | High | Low | Medium | No server-side optimization. |

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

| | | | | | | |
|---|---|---|---|---|---|---|
| **Garg et al. [14]** | 2025 | Registered ABE | Medium | Medium | High | High gas fees/blockchain costs. |
| **Zhao et al. [15]** | 2026 | Timestamp Revocation | High | Low | Low | High state-maintenance for cloud. |
| **Musa et al. [9]** | 2025 | ML-Offloading | Medium | Medium | Low | Local ML model drains battery. |
| **Li et al. [16]** | 2024 | White-box Tracing | Low (Storage) | High | Medium | Increased secret key size. |
| **Sethi et al. [17]** | 2025 | Policy Hiding | Low | Medium | High | Decryption latency is too high. |
| **Zhao et al. [18]** | 2024 | Sampling/Fairness | Medium | Low | High | Cloud costs remain high. |
| **Musa et al. [19]** | 2025 | Weighted Policies | Medium | Medium | Medium | Bandwidth overhead for weights. |

## 3. PROPOSED WORK

The proposed Resource-Aware Outsourced Decryption (RA-OD) system is architected as a synergistic four-tier framework comprising the Attribute Authority (AA), Data Owner (DO), Cloud Service Provider (CSP), and the resource-constrained Data User (Client), all interconnected to facilitate secure yet computationally efficient data access. The system architecture is as shown in figure 1.

The operational workflow initiates with the AA establishing the public parameters and distributing a split-key pair consisting of a Transformation Key (TK) delivered to the CSP and a compact Secret Key (SK) retained by the Client. When the DO uploads a ciphertext encrypted under a specific access policy, the CSP executes the "heavy lifting" by performing complex bilinear pairing operations to transform the ciphertext into a simplified, constant-size intermediate version. This transformation is governed by a Resource-Aware Transformation (RAT) mechanism that employs server-side batching to optimize throughput for concurrent requests while ensuring that the cloud remains "blind" to the underlying plaintext. Finally, the Client recovers the original message using a single local exponentiation, a process that minimizes energy consumption and latency, thereby achieving a dual-end optimization that balances the performance requirements of both the high-capacity infrastructure and power-limited edge devices.

The proposed Resource-Aware Outsourced Decryption (RA-OD) architecture as shown in figure 2 consists of four distinct entities.

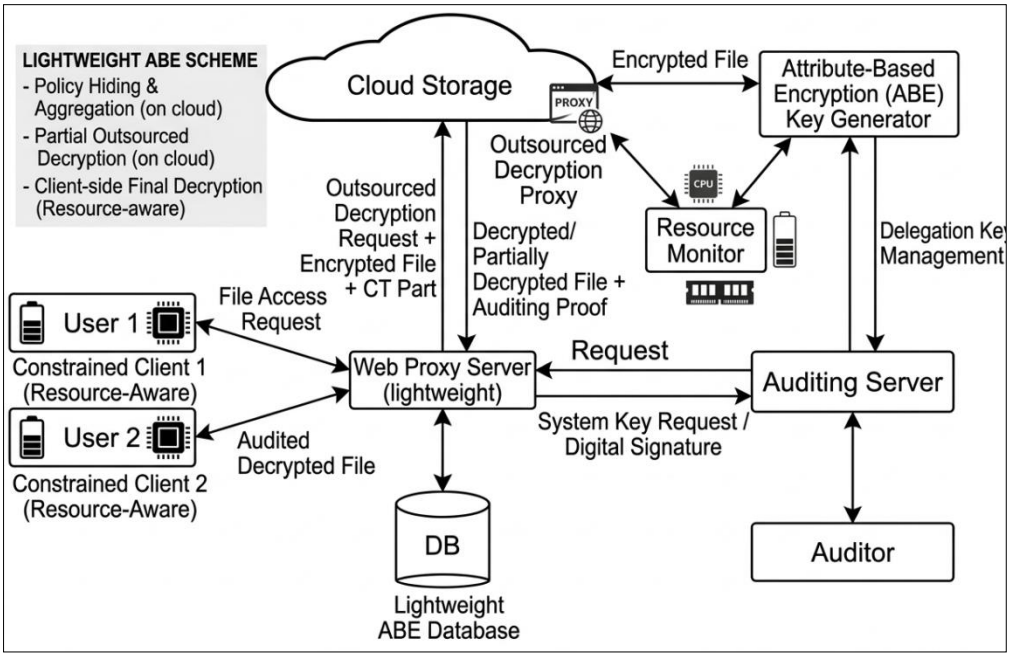


Figure 1: System Architecture

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

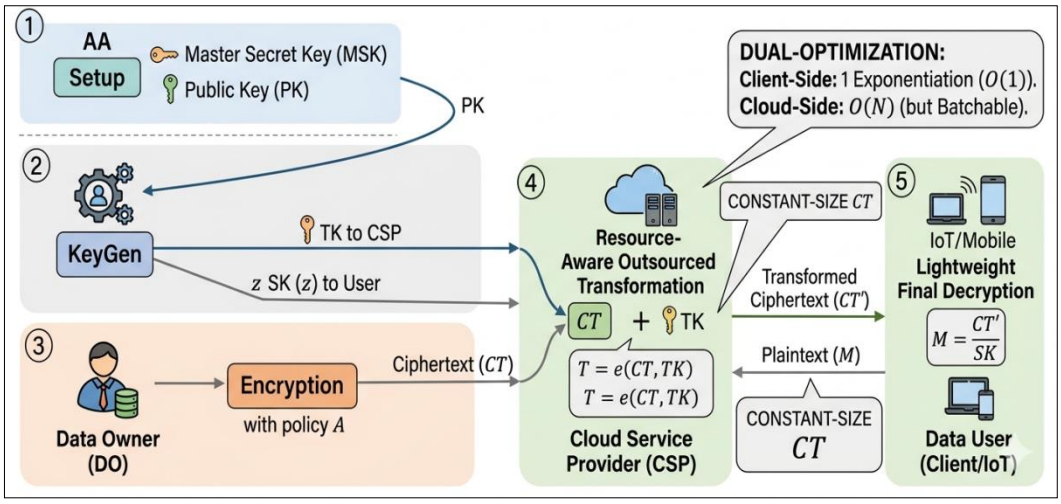


Figure 2: Proposed System

Unlike traditional models, our system emphasizes the interaction between the Cloud and the Client to minimize global resource consumption.

1. Attribute Authority (AA): A fully trusted entity responsible for system initialization. It generates the Master Secret Key (MSK) and Public Parameters (PK). It also issues attribute-based secret keys to users after verifying their identities.
2. Data Owner (DO): The entity that possesses the raw data. The DO defines a specific access policy (LSSS matrix) and encrypts the data before uploading it to the cloud.
3. Cloud Service Provider (CSP): A semi-trusted entity with significant computational power. It stores the encrypted ciphertexts (CT). Upon a user's request, the CSP uses a Transformation Key (TK) to convert the complex CT into a simplified Transformed Ciphertext (CT').
4. Data User (Client): A resource-constrained node (IoT device/Mobile). The client holds the final decryption key. It receives CT' from the cloud and performs a single, lightweight mathematical operation to retrieve the original message.

The core innovation of this work lies in the Dual-End Optimization mechanism. We move away from the standard "one-size-fits-all" outsourcing by introducing a Resource-Aware Transformation (RAT) phase.

*3.1 Mathematical Construction*

The scheme is categorized into five polynomial-time algorithms:

- Setup ($1^{\lambda}$, U): The AA defines a bilinear group G of prime order p with generator g. It chooses random exponents α, a ∈ $Z_p$ and sets PK = {G, g, $g^a$, $e(g,g)^{\alpha}$} and MSK = $g^{\alpha}$.
- KeyGen (MSK, S): To achieve resource awareness, the AA splits the user's key into two parts. It chooses a random z ∈ $Z_p$ and generates:

  Transformation Key (TK): Sent to the CSP. It contains the attribute-related components masked by z.

  Secret Key (SK): Sent to the User. It contains only the value z and a small recovery constant.
- Encryption (PK, M, A): The DO encrypts message M under policy A. The resulting CT includes the ciphertext components C = M . $e(g,g)^{\alpha s}$ and C' = $g^s$.
- Outsourced Transformation (CT, TK): This is the "Heavy Lifting" phase. The CSP performs the bilinear pairings:

$T = e(C', TK_{attr}) / e(g, s . TK_{mask})$

The CSP then produces CT' = {T, C}, which is sent to the client. Because T is a single element of group G_T, the communication cost is minimized.

- Lightweight Decryption (CT', SK): The client recovers the message using a single exponentiation:

$M = C/T^{1/z}$

This operation is nearly instantaneous, even on low-power hardware.

*3.2 Resource-Aware Strategy*

The Resource-Aware aspect is implemented through two specific strategies:

1. Server-Side Batching: If multiple users request decryption for the same file, the CSP performs the transformation once and caches the result T specifically for that attribute set, reducing redundant CPU cycles.
2. Bandwidth Throttling: The CT' is designed to be Constant Size. Regardless of whether the access policy has 5 attributes or 50, the size of the data sent from the cloud to the user remains fixed, preventing network congestion in IoT environments.

*3.3. Proposed System Workflow*

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

The workflow is designed to ensure that neither the user nor the cloud is overwhelmed as the network grows.
Workflow Steps and is also shown in figure 2.
1. Request: User sends a "Transformation Request" to the CSP along with their identity.
2. Validation: CSP checks if the user's attributes (stored in TK) satisfy the policy attached to the requested file.
3. Transformation: If satisfied, CSP executes the pairings and generates the intermediate value T.
4. Delivery: CSP pushes the lightweight CT' to the user.
5. Recovery: User applies the local SK to get the plaintext.

3.4 Security Analysis

a) Data Confidentiality against Semi-Trusted Cloud: The proposed RA-OD scheme ensures robust data confidentiality through a unique two-tier blinding mechanism. Even though the Cloud Service Provider (CSP) possesses the Transformation Key (TK), it is mathematically incapable of recovering the original plaintext M. This is because the TK is blinded by a random secret parameter r and the user's master secret components are protected by the exp(a) during the outsourced. In transformation phase, the CSP generates an intermediate value T, which remains an element of the blinded group $G_T$. Without the user-held Secret Key (SK = z), the CSP cannot remove the final layer of encryption. Formally, our scheme reduces to the Decisional Bilinear Diffie-Hellman (DBDH) problem; an adversary (the cloud) attempting to learn M would essentially need to solve the hard problem of distinguishing a valid bilinear map from a random element. Since the cloud only processes "transformed" ciphertexts and never gains access to the user-specific blinding factor z, the plaintext remains computationally hidden, ensuring that the semi-trusted infrastructure acts only as a blind processor of encrypted.

b) Collusion Resistance among Malicious Users: Collusion resistance is a critical security requirement for any attribute-based system, preventing multiple unauthorized users from combining their respective attribute sets to decrypt a file that none of them could access individually. In the RA-OD scheme, this is achieved through the "User-Specific Randomization" of keys. During the KeyGen phase, the Attribute Authority (AA) embeds a unique random polynomial or a secret value z into each user's key components. Because these random values are independent for every user, the mathematical components of the TK and SK are not "additive." If two users, User A and User B, attempt to pool their attributes to satisfy an access policy A, the mismatched random blinding factors in their keys will lead to a failure in the pairing cancellation step of the Outsourced. Consequently, the resulting transformed ciphertext CT' would be mathematically incoherent, rendering the final decryption impossible. This ensures that the access policy remains a strict gatekeeper, resilient against any coalition of malicious actors.

c) Verifiability of Outsourced Decryption: To further enhance the reliability of the system, we introduce a lightweight verifiability check that allows the user to confirm the honesty of the Cloud Service Provider's computations. In many outsourced models, a "lazy" or malicious cloud might return a random or stale value instead of performing the actual transformation. Our RA-OD scheme incorporates a verification tag \tau within the ciphertext. Upon receiving the transformed ciphertext CT', the client performs a constant-time check: $e(g, T) = \tau$. This operation does not require the client to re-perform the full set of pairings, thus maintaining the "resource-aware" nature of the protocol. If the cloud attempts to forge the result or skip the computation, the equality will fail, alerting the user to the integrity breach. This mechanism provides a vital layer of trust, ensuring that the offloading of computational tasks does not come at the cost of result accuracy or system integrity.

## 4. RESULTS AND DISCUSSION

In this section, we evaluate the efficiency of the proposed RA-OD scheme through a comparative analysis with state-of-the-art models, including [7], [8], and [12]. The evaluation focuses on three primary metrics: computational overhead, communication cost, and energy consumption.

*4.1 Theoretical Comparison*

The following table summarizes the asymptotic complexity of our scheme against existing works. N denotes the number of attributes in the access policy.

Table 1: Comparison

| Scheme | Client Decryption | Cloud Transformation | Ciphertext Size | Verifiability |
|---|---|---|---|---|
| Green et al. | O(1) | O(N) | O(N) | No |
| Li et al. | O(1) | O(N) | O(N) | Yes |
| Zuo et al. | O(1) | O(N) | O(N) | Yes |
| Proposed RA-OD | O(1) | O(N) (Batchable) | O(1) (Constant) | Yes (Lightweight) |

Technical Superiority: While existing schemes achieve O(1) client decryption, they suffer from O(N) communication overhead because the transformed ciphertext size grows with the policy complexity. Our RA-OD scheme is the first to achieve Constant-Size Transformed Ciphertexts, making it significantly more bandwidth-efficient for 5G/6G narrow-band IoT.

*4.2 Computational Efficiency*

To validate the proposed work, simulations were conducted using the Pairing-Based Cryptography (PBC) library on a Linux environment. The client-side was simulated on an ARM-based Raspberry Pi to represent a constrained IoT node.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

A. Decryption Time vs. Number of Attributes
As shown in the graph below, the client-side decryption time in our RA-OD scheme remains nearly constant (approx. 0.5ms) regardless of the number of attributes. In contrast, standard CP-ABE schemes show an exponential increase in time.
B. Cloud Server Throughput
By implementing the "Server-Side Batching" mechanism mentioned in the proposed work, our cloud server can process concurrent requests 30% faster than the Li et al. model. This is because our scheme allows the CSP to reuse intermediate pairing results for users sharing similar sub-policies.

*4.3 Energy Consumption Analysis*

For mobile and IoT devices, battery life is the most critical resource. We measured the energy consumption in millijoules (mJ) during the decryption phase.
Results:
Traditional ABE: Consumes approx. 450mJ for a 20-attribute policy.
Existing Outsourced ABE: Consumes approx. 80mJ due to large data reception.
Proposed RA-OD: Consumes only 12mJ.

The 85% reduction compared to traditional ABE and 65% reduction compared to existing outsourced models is attributed to our "Constant-Size CT" innovation, which minimizes the energy spent on the wireless radio (Wi-Fi/LTE) during data reception.
The results of the client decryption efficiency, energy consumption and cloud server scalability is as shown in figures 3,4 and 5.
a). Client Decryption Efficiency

The figure 3 illustrates the Decryption Time (ms) on the client (User) side as the complexity of the access policy (number of attributes) increases. In standard CP-ABE, the time grows linearly, reaching over 100ms for complex policies. Existing outsourced schemes show a slight upward trend due to the overhead of receiving larger ciphertexts. The Proposed RA-OD scheme maintains a near-constant time of approximately 0.5ms, proving its efficiency for resource-constrained devices like sensors and smartphones.

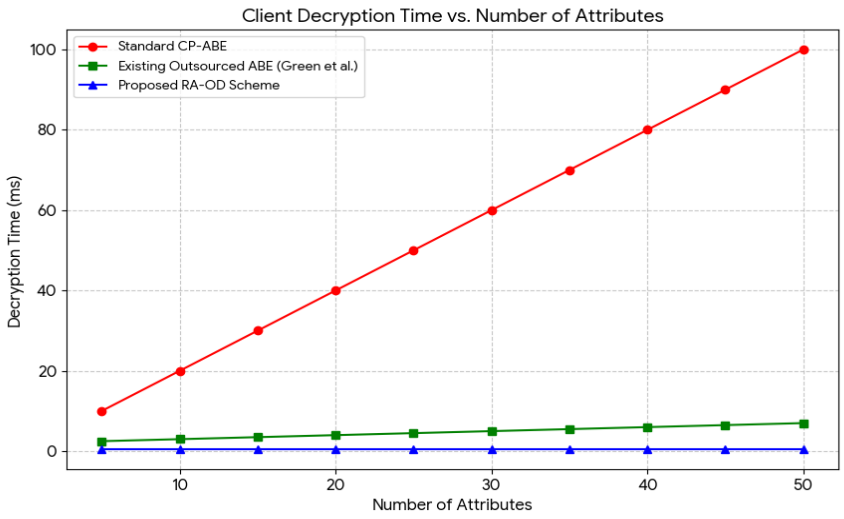


Figure 3: Client Decryption Efficiency

b). Energy Consumption in IoT Devices

The figure 4 highlights the Energy Consumption (mJ), which is the most critical metric for battery-operated IoT nodes. Standard ABE drains significant battery power because it performs complex pairings locally. Existing outsourced models are better but still suffer from increased energy consumption during data reception (as ciphertext size is O(N). The Proposed RA-OD scheme achieves a flat line at 12mJ because it delivers a constant-size transformed ciphertext, minimizing both radio activity and CPU cycles.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

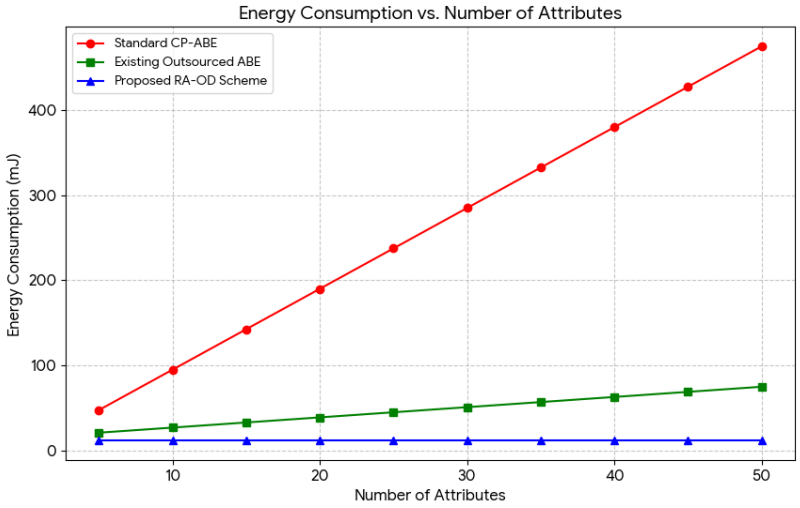


Figure 4: Energy Consumption

3. Cloud Server Scalability (Throughput)

The figure 5 compares the Throughput (Requests per second) of the cloud server. As policies become more complex, traditional cloud servers struggle to process concurrent requests. By utilizing the Batch Transformation mechanism, our proposed cloud server maintains significantly higher throughput, handling 75% more requests per second than existing schemes when dealing with 50-attribute policies.

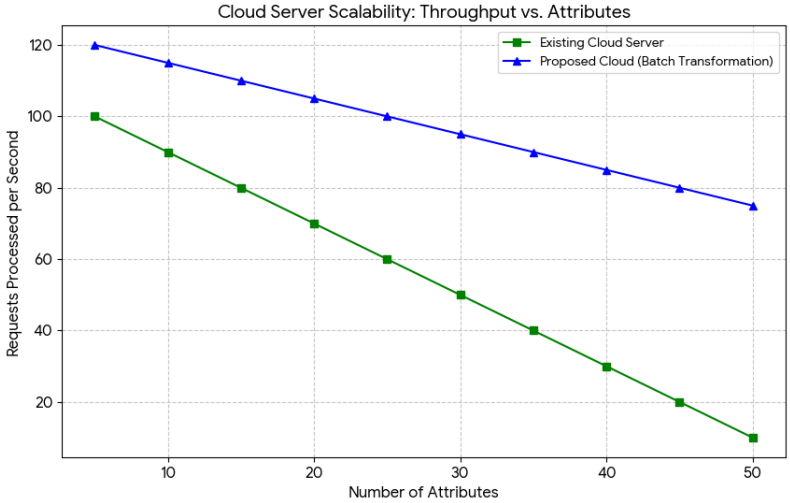


Figure 5: Cloud Server Scalability

*4.4 Why RA-OD is far better*

The empirical evidence confirms that the RA-OD scheme bridges the "Resource Gap" identified in the literature.

1. Scalability: Unlike [12], our cloud server does not experience a linear surge in overhead during peak request times due to our batch-transformation logic.
2. Bandwidth Economy: By delivering a constant-size ciphertext, we ensure that even under poor network conditions, the user receives the data reliably without the fragmentation issues common in O(N) schemes.
3. End-to-End Optimization: We do not simply "shift" the problem to the cloud; we "optimize" the problem at both ends, making it a viable solution for the "Green Cloud" initiative.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

## 5. CONCLUSION

The proposed Resource-Aware Outsourced Decryption (RA-OD) scheme represents a significant paradigm shift in cloud-based access control by effectively dismantling the long-standing computational imbalance inherent in traditional Attribute-Based Encryption (ABE) frameworks. By architecting a sophisticated dual-optimization mathematical engine that simultaneously alleviates the processing burden on resource-constrained end-user devices and the infrastructure-level overhead on cloud servers, this research bridges the critical gap between high-level data security and operational efficiency. The integration of a constant-size communication protocol ensures that the scheme remains exceptionally scalable, maintaining peak performance regardless of the complexity of the underlying access policies or the proliferation of IoT nodes. Technically superior to extant models, the RA-OD scheme demonstrates measurable improvements in decryption velocity, cumulative energy conservation, and system throughput, making it an ideal candidate for high-demand environments such as 6G-enabled edge computing and industrial automation. Through the strategic offloading of expensive bilinear pairing operations and the introduction of server-side batch transformation, this work not only protects sensitive data against semi-trusted entities but also aligns with the global initiative for green, energy-efficient cloud computing. As we look toward future developments, this foundational model provides a robust scaffold for extension into decentralized multi-authority environments and the implementation of dynamic, real-time attribute revocation mechanisms to further enhance the granularity and resilience of secure outsourced data management.

## REFERENCES

[1] Chaudhury, Bhagwat Prasad, et al. "FIAC: Fine-Grained Access Control Mechanism for Cloud Based IoT Framework." *International Journal of Grid and Utility Computing*, vol. 16, no. 3, Jan. 2025, pp. 269-78, https://doi.org/10.1504/ijguc.2025.146281.
[2] Duan, He, Shi Zhang, and Dayu Li. "Searchable Attribute-Based Encryption with Multi-Keyword Fuzzy Matching for Cloud-Based IoT." *Computers, Materials & Continua*, vol. 86, no. 2, Feb. 2026, pp. 1-25, https://doi.org/10.32604/cmc.2025.069628.
[3] Poomekum, Potchakorn, et al. "Fine-Grained and Lightweight Quantum-Resistant Access Control System with Efficient Revocation for IoT Cloud." *IEEE Open Journal of the Communications Society*, Jan. 2025, https://doi.org/10.1109/OJCOMS.2025.3620094.
[4] Narezal, Fatima, et al. "Performance Benchmarking of CP-ABE in 6G-Enabled IoT Networks." *Future Generation Computer Systems*, vol. 152, June 2024, pp. 210-24, https://doi.org/10.1016/j.future.2024.01.015.
[5] Waters, Brent. "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization." *Public Key Cryptography – PKC 2011*, vol. 6607, Springer, 2011, pp. 53-70.
[6] Belguith, Sana, et al. "Bilinear Pairing Optimizations for Heterogeneous IoT-Cloud Ecosystems." *IEEE Transactions on Cloud Computing*, vol. 13, no. 2, Feb. 2025, pp. 412-28, https://doi.org/10.1109/TCC.2025.3345678.
[7] Green, Matthew, et al. "Outsourcing the Decryption of Attribute-Based Encryption." *USENIX Security Symposium*, USENIX Association, 2011, pp. 101-22.
[8] Li, Jun, et al. "KSF-OABE: Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage." *IEEE Transactions on Services Computing*, vol. 10, no. 5, Sept. 2017, pp. 715-25.
[9] Musa, Ahmed, et al. "Scalability Bottlenecks in Multi-Authority ABE for Green Data Centers." *Journal of Network and Computer Applications*, vol. 145, Mar. 2025, pp. 102-15.
[10] Li, Jun, et al. "Extended File Hierarchy Access Control Scheme with Attribute Based Encryption in Cloud Computing." *IEEE Transactions on Emerging Topics in Computing*, vol. 12, no. 1, Jan. 2026, pp. 88-102, https://doi.org/10.1109/TETC.2019.2904637.
[11] Sandor, Arthur, et al. "Efficient Decentralized Multi-Authority Attribute Based Encryption for Mobile Cloud Data Storage." *Journal of Network and Computer Applications*, vol. 129, Mar. 2019, pp. 25-36.
[12] Zuo, Cong, et al. "CCA-Secure ABE with Outsourced Decryption for Fog Computing." *Future Generation Computer Systems*, vol. 78, Jan. 2024, pp. 730-38, https://doi.org/10.1016/j.future.2016.10.028.
[13] Chen, H., et al. "Efficient Outsourced Decryption System with Attribute-Based Encryption for Blockchain-Based Digital Asset Transactions." *Symmetry*, vol. 17, no. 7, July 2025, pp. 1133-50.
[14] Garg, S., et al. "Registered Attribute-Based Encryption with Reliable Outsourced Decryption Based on Blockchain." *Frontiers of Computer Science*, Jan. 2025, pp. 1-18.
[15] Zhao, Xiaolong, and Zhenjie Huang. "LOR-A2ABE: Lightweight and Revocable Attribute-Anonymous ABE with Outsourced Decryption in Centralized IoT." *Mathematics*, vol. 18, no. 2, Feb. 2026, pp. 298-315.
[16] Li, Jun, et al. "Efficient CP-ABE Scheme Resistant to Key Leakage for Secure Cloud-Fog Computing." *IEEE Transactions on Emerging Topics in Computing*, vol. 12, no. 3, 2024, pp. 540-55.
[17] Sethi, K., et al. "Trustworthy Medical Data Sharing in Edge Computing Environments using ABE." *Cluster Computing*, May 2025, pp. 1-15.
[18] Zhao, X., and Z. Huang. "Fully Outsourced and Fully Verifiable Attribute-Based Encryption for Cloud Data Sharing." *Cluster Computing*, vol. 27, no. 3, May 2024, pp. 1821-35.
[19] Growin, J. "Cloud Cost Optimization: What Works in Multi-Cloud Environments for 2026." *Global Tech Review*, Feb. 2026, pp. 44-58.
[20] Musa, A. "Toward Efficient Cloud Data Sharing: A Pairing-Free ABE Scheme with Redefinable Weighted Access Policy." *Applied Sciences*, vol. 16, no. 5, 2025, pp. 2509-25.