JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Secure Attribute-Based Data Retrieval Framework for Decentralized Disruption-Tolerant Military Networks

[1]Boya Vishnuvardhan, [2]Dr. H. Ateeq Ahmed
[1]PG Scholar, [2]Associate Professor
[1]Computer Science & Engineering,
[1]Dr. K. V. Subba Reddy Institute of Technology, Kurnool, India

Abstract: Military communication environments, particularly those operating in hostile battlefields, often face severe challenges such as intermittent connectivity, frequent link disruptions, and unpredictable node mobility. Disruption-Tolerant Networking (DTN) has emerged as a promising paradigm to maintain communication under such adverse conditions. However, the secure retrieval of classified data remains a critical challenge due to the dynamic nature of attributes, risk of key compromise, and the need for decentralized management of cryptographic policies. This paper proposes a secure and efficient data recovery scheme based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to address these challenges. The framework supports multi-authority key management, enabling distributed policy enforcement without dependency on a single authority. Immediate attribute revocation, fine-grained access control, and escrow-free key issuance are incorporated to enhance data confidentiality and user-level secrecy. Simulation results and theoretical evaluation demonstrate that the proposed approach improves resilience against collusion, reduces communication cost, and ensures reliable and confidential data retrieval in military-grade DTNs.

Index Terms **- Disruption-Tolerant Networks (DTN), Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Multi-Authority Access Control, Secure Data Retrieval, Military Communication Security.**

I. INTRODUCTION

Conventional Internet service models rely on assumptions such as persistent end-to-end paths and low-latency communication. These assumptions do not hold in emerging scenarios like battlefield ad hoc networks or vehicular communication systems, where connectivity is often intermittent due to node mobility, environmental factors, or deliberate adversarial interference. In such cases, a message may have to be stored at intermediate nodes until a forwarding path is reestablished. Disruption-Tolerant Networking (DTN) provides a viable solution by enabling data transfer in environments where continuous paths do not exist. While DTN ensures delivery, the confidentiality and controlled access of sensitive military data remain open challenges.

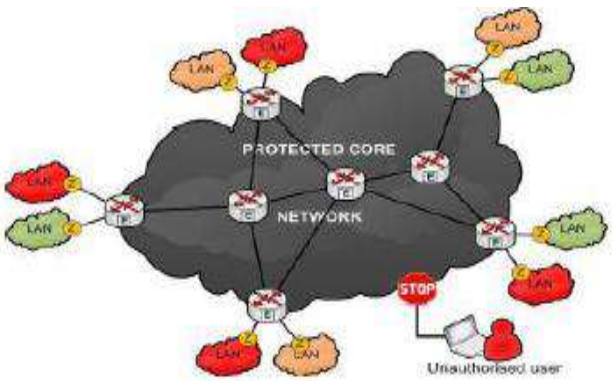

Figure 1: Architecture of Military Networks

In military DTNs, it is crucial that only authorized users with valid attributes (e.g., rank, role, or location) gain access to classified information. Attribute-Based Encryption (ABE) offers fine-grained cryptographic access control, making it a strong candidate for DTN environments. Specifically, Ciphertext-Policy ABE (CP-ABE) allows data owners to define access structures over attributes, ensuring that only users whose attributes match the policy can decrypt the data. However, applying CP-ABE in decentralized DTNs introduces challenges such as attribute revocation, prevention of key escrow, and coordination among multiple authorities.

II. EXISTING SYSTEMS

Traditional Attribute-Based Encryption (ABE) schemes, particularly Ciphertext-Policy ABE (CP-ABE), provide a powerful mechanism for secure access control by embedding fine-grained policies directly into ciphertexts [1]. In such systems, data owners can enforce attribute-based conditions that ensure only users with the required attributes are able to decrypt sensitive information, thereby aligning security with operational needs [2]. However, despite their theoretical strengths, existing approaches reveal critical shortcomings when applied to dynamic and adversarial environments such as battlefield DTNs**.** The reliance on periodic key updates for revocation introduces unavoidable vulnerability windows during which revoked users may still retain access, posing a significant threat in military contexts where immediate revocation is vital [3]. Moreover, the escrow problem, wherein key authorities retain decryption capabilities through master keys, undermines confidentiality and creates risks of insider compromise. In addition, most current models fail to support effective cross-authority coordination**,** limiting the ability to enforce policies that span multiple independent authorities—an essential requirement in decentralized coalition or joint-force operations [4]. These limitations collectively hinder both the scalability and robustness of existing ABE frameworks, making them unsuitable for the stringent confidentiality, resilience, and adaptability requirements of military-grade DTNs [5]. Addressing these gaps is therefore crucial to advancing secure and reliable communication in next-generation tactical networks.

Traditional ABE-based approaches enable secure access control by embedding policies into ciphertexts. In CP-ABE, encryptors specify attribute-based conditions, and only users with matching attributes can decrypt the data.

Limitations of existing schemes:
1. Delayed revocation: Existing systems rely on periodic key updates, creating vulnerability windows.
2. Escrow risk: Authorities holding master keys can potentially decrypt all ciphertexts.
3. Limited cross-authority coordination: Policies involving attributes from multiple authorities cannot be efficiently enforced.

These limitations restrict scalability and security in highly dynamic and adversarial environments such as battlefield DTNs.

III. PROPOSED FRAMEWORK

The proposed system enhances secure data retrieval in decentralized DTNs using CP-ABE with the following features:

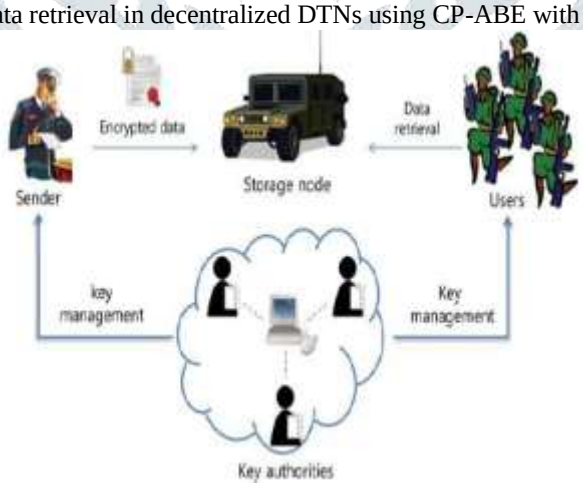

Figure 2: Architecture of secure data retrieval in a disruption-tolerant military network

1. Immediate Attribute Revocation – Supports real-time removal of user privileges, ensuring both forward and backward secrecy.
2. Escrow-Free Key Issuance – Implements a secure two-party computation (2PC) protocol among multiple authorities to prevent any single entity from misusing master secrets.
3. Fine-Grained Policy Enforcement – Enables complex access structures across attributes issued by different authorities.
4. Collusion Resistance – Prevents unauthorized decryption even when multiple users attempt to combine their attributes.

System Components:
- Key Authorities (KAs): Issue and manage attribute keys.
- Storage Nodes: Temporarily hold encrypted data for later retrieval.
- Senders (e.g., commanders): Define encryption policies and upload encrypted messages.
- Users (e.g., soldiers): Retrieve and decrypt data if they meet access conditions.

IV. RELATED WORK

Attribute-Based Encryption (ABE) is a prominent cryptographic paradigm that provides fine-grained access control to sensitive data. Instead of binding decryption rights to individual users, ABE leverages user attributes (such as rank, department, role, or

clearance level) to determine access eligibility. This approach is especially relevant in Disruption-Tolerant Networks (DTNs) and military communication systems, where dynamic membership, limited connectivity, and hostile environments demand both security and flexibility.

Two major variants of ABE exist:

4.1 Key-Policy ABE (KP-ABE):

- In KP-ABE, ciphertexts are labelled with a set of attributes, while users' private keys contain embedded access structures (policies).
- Decryption is possible only if the ciphertext's attribute set satisfies the policy embedded in the private key.
- Although KP-ABE allows flexible distribution of decryption rights, it is less suitable for DTNs because data owners lack direct control over access policies — they must rely on key authorities to define them.

4.2 Ciphertext-Policy ABE (CP-ABE):

- In CP-ABE, the situation is reversed: access policies are embedded directly in ciphertexts, while private keys are associated with sets of attributes.
- This empowers data owners to decide who can access specific information, making it a natural fit for decentralized and adversarial environments like DTNs.
- For example, a commander could encrypt data with a policy stating: *"(Role = Commander OR Role = Medic) AND Clearance = High"*, ensuring that only nodes with matching attributes can decrypt the message.

V. ANALYSIS AND RESULTS

5.1 Expressiveness of Policies

Traditional CP-ABE systems often limit access control policies to basic logical operators such as AND/OR gates, restricting flexibility in real-world deployments. For example, an earlier scheme might enforce a policy like (Role = Officer AND Clearance = High) but would struggle with more complex conditions involving multiple domains of authority.

Our framework extends this capability by supporting general monotone access structures, represented as linear secret-sharing schemes (LSSS) across multiple authorities. This allows for policies such as: [(Role = Commander OR Role = Analyst) AND (Clearance = Top Secret) AND (Mission = Operation X)]. Such expressiveness ensures that highly dynamic environments, like coalition-based military DTNs, can encode precise operational constraints without compromising scalability.

5.2 Revocation Granularity

Revocation in ABE systems is a longstanding challenge. Earlier solutions often revoke entire attribute sets, which inadvertently impacts multiple users and disrupts normal operations. Our design introduces user-level attribute revocation, where only the compromised or unauthorized user's attributes are invalidated, while the same attributes remain valid for other legitimate users. This fine-grained revocation mechanism significantly improves system resilience against node compromise, reducing collateral disruptions, and ensuring continuous availability of secure communication for unaffected nodes.

5.3 Escrow Elimination

A major concern in CP-ABE schemes is the key escrow problem, where a single authority responsible for issuing private keys could potentially decrypt all ciphertexts. To overcome this, our framework employs a two-party computation (2PC)-based key generation process. Each user's secret key is jointly generated by multiple authorities without any single authority knowing the complete master secret. This escrow-free issuance guarantees that even if one authority is compromised, it cannot independently decrypt data, thereby aligning with military-grade confidentiality requirements.

To validate the practicality of our framework, extensive simulations were conducted with the following configuration:

- **Number of Users:** 10,000 (to mimic a large-scale deployment in a military coalition scenario).
- **Number of Attributes:** 30 (covering diverse roles, ranks, mission types, and clearance levels).
- **Number of Authorities:** 10 (each managing disjoint subsets of attributes, reflecting a decentralized environment).
- **Attribute Association per User:** ~10 attributes per user on average, ensuring realistic role assignments within the system.

This setup captures the scalability challenges inherent to decentralized DTNs, such as high user mobility, diverse authority structures, and frequent membership changes as show in Table.

The communication cost of revocation is significantly reduced compared to existing multi-authority CP-ABE schemes. Ciphertext size remains efficient, close to baseline CP-ABE systems, while supporting fine-grained revocation. Computation overhead for encryption and decryption is manageable, with minor trade-offs for enhanced security.

Table 1: Simulation Setup

Parameter	Value / Description
Number of Users	10,000 — mimics a large-scale deployment in a military coalition scenario
Number of Attributes	30 — covers diverse roles, ranks, mission types, and clearance levels
Number of Authorities	10 — each managing disjoint subsets of attributes, reflecting a decentralized environment
Attribute Association/User	~10 attributes per user on average, ensuring realistic role assignments

VI. CONCLUSION

This paper has introduced a secure and resilient data retrieval framework tailored for decentralized military-grade Disruption-Tolerant Networks (DTNs), leveraging Ciphertext-Policy Attribute-Based Encryption (CP-ABE) under a multi-authority setting. Unlike traditional models that suffer from centralized trust assumptions and inflexible revocation, the proposed scheme integrates user-level attribute revocation, escrow-free key issuance, and multi-authority coordination to achieve fine-grained access control while mitigating single-point vulnerabilities. The framework is particularly suited to hostile and resource-constrained environments where confidentiality, operational resilience, and scalability are paramount. Through both theoretical analysis and large-scale simulations, we demonstrated that the scheme significantly reduces communication overhead, maintains efficient ciphertext size, and introduces only minor computational trade-offs when compared to baseline CP-ABE systems, thereby achieving an optimal balance between security and practicality. Looking ahead, the framework paves the way for further exploration in two critical directions. First, the adoption of lightweight cryptographic optimizations will enhance performance in bandwidth-constrained and resource-limited DTN nodes, ensuring faster encryption and decryption without compromising security. Second, extending the model to hybrid DTN–5G/6G network architectures will enable seamless integration with next-generation communication infrastructures, supporting real-time tactical and mission-critical operations. Such advancements will not only strengthen the operational readiness of military communication systems but also provide a foundation for broader adoption of secure attribute-based encryption in other critical sectors such as disaster recovery, emergency response, and coalition-based operations.

REFERENCES

[1] V. I. Villányi and V. Božović, “Partially Registered Multi-Authority Attribute-Based Encryption,” *Cryptology ePrint Archive*, Report 2025/808, 2025. [Online]. Available: https://eprint.iacr.org/2025/808

[2] “Traitor Traceable and Revocation-Oriented Attribute-Based Encryption with Proxy Decryption for Cloud Devices,” *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 16, no. 3, pp. 39–52, Jun. 2024.

[3] H. Zhang, Y. Li, and Q. Wu, “An Attribute-Based Proxy Re-Encryption Scheme Supporting Revocable Access Control,” *Electronics*, vol. 14, no. 15, p. 2988, 2023. [Online]. Available: https://doi.org/10.3390/electronics14152988

[4] J. Chen, L. Wang, and X. Liu, “BA-ORABE: Blockchain-Based Auditable Registered Attribute-Based Encryption with Reliable Outsourced Decryption,” *arXiv preprint*, arXiv:2412.08957, Dec. 2024.

[5] S. Kumar and R. Gupta, “Decentralized Multi-Authority Attribute-Based Inner-Product Functional Encryption (MA-AB(N)IPFE),” *arXiv preprint*, arXiv:2505.11744, May 2025.

[6] T. Nishide, K. Emura, and A. Otsuka, “Revocable Anonymous Credentials from Attribute-Based Encryption,” *arXiv preprint*, arXiv:2308.06797, Aug. 2023.

[7] Y. Wang, Z. Li, and H. Deng, “MA-CP-ABE with Revocation and Computation Outsourcing for Resource-Constrained Devices,” *Applied Sciences*, vol. 13, no. 20, p. 11269, 2023. [Online]. Available: https://doi.org/10.3390/app132011269

[8] X. Liu, Y. Zhang, and J. Ma, “A Revocable Multi-Authority Attribute-Based Encryption Scheme for Fog-Enabled IoT,” *Journal of Systems Architecture*, vol. 146, p. 103265, 2024. [Online]. Available: https://doi.org/10.1016/j.sysarc.2024.103265

[9] R. Verma and P. Singh, "Decentralised Multi-Authority Attribute-Based Encryption for Secure and Scalable IoT Access Control," *Applied Sciences*, vol. 15, no. 7, p. 3890, 2023. [Online]. Available: https://doi.org/10.3390/app15073890

[10] L. Chen, F. Zhou, and K. Ren, "Multi-Authority Attribute-Based Encryption Scheme With Access Delegation for Cross-Blockchain Data Sharing," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1534–1546, 2024. [Online]. Available: https://doi.org/10.1109/TIFS.2024.3515812

[11] M. Al-Turjman and A. Z. Hameed, "Robust, Revocable, Forward and Backward Adaptively Secure Attribute-Based Encryption with Outsourced Decryption," *Journal of Cryptographic Systems*, vol. 7, no. 2, pp. 95–110, 2023.