

MADHAVI TOTA
SWAPNILI KARMORE

A NOVEL FRAMEWORK FOR CHANNEL SECURITY USING HYBRID ATTRIBUTE-BASED ENCRYPTION WITH PRIVACY OPTIMIZATIONS

Abstract

In the evolving landscape of secure communication, ensuring robust channel security while preserving user privacy remains a critical challenge. This paper introduces a novel framework that leverages hybrid attribute-based encryption (ABE) to enhance channel security with optimized privacy preservation mechanisms. Traditional encryption methods often lack fine-grained access control, while existing ABE-based solutions can suffer from computational overhead and privacy issues. Our framework addresses these limitations by combining ABE with another encryption scheme to achieve secure and efficient data transmission. We incorporate privacy-preserving techniques to minimize user attribute exposure. The proposed framework integrates the flexibility of attribute-based encryption with the combined efficiency of Fernet and initialization vector. Exponential differential privacy mechanism is integrated with the proposed framework to provide addition privacy and security of communicated user information. The security analysis demonstrates that the framework offers strong confidentiality, collusion resistance, and unforgeability guarantees. Performance evaluation confirms efficient operation compared to existing solutions. This proposed framework provides a promising approach for secure communication in various applications and obtained optimized in terms of latency, strong attack resistance and less computational overhead.

Keywords

privacy and security, exponential differential privacy, hybrid encryption, Fernet, IV encryption, attribute based encryption

Citation

Computer Science 27(2) 2026: 5–26

Copyright

© 2026 Author(s). This is an open access publication, which can be used, distributed and reproduced in any medium according to the Creative Commons CC-BY 4.0 License.

1. Introduction

The digital landscape thrives on seamless communication, but with this growth comes the critical need for robust security measures to safeguard sensitive information during transmission. Broadcast communication channels, where data is disseminated to a large audience simultaneously, present unique challenges. While traditional encryption methods secure data confidentiality, they often lack the granularity to control access based on specific user attributes. This limitation, as pointed out by [7], can lead to unintended information leakage, potentially exposing sensitive data to unauthorized users.

Attribute-Based Encryption (ABE) has emerged as a promising solution for secure data sharing. ABE empowers fine-grained access control by encrypting data with policies defined by user attributes. However, existing ABE-based solutions for broadcast communication channels can be computationally expensive and raise privacy concerns. User attributes might be revealed during the encryption or decryption processes, potentially compromising user anonymity. A recent study by [2, 12] highlights this privacy vulnerability in ABE-based broadcast encryption.

This paper proposes a novel framework for secure channel broadcast communication that integrates Attribute-Based Hybrid Encryption (ABHE) with the Fernet model and Initialization Vectors (IVs) while incorporating differential privacy techniques. It leverages the strengths of ABE for fine-grained access control and combine it with the efficiency of the Fernet model. Additionally, IVs with random values enhance security by eliminating predictability in the encryption process. To address privacy concerns, we introduce differential privacy techniques that obfuscate individual user attributes, preventing their inadvertent disclosure. This approach builds upon existing research while offering improved user privacy protections.

The proposed framework aims to achieve a balance between security, efficiency, and user privacy in broadcast communication channels. We present a detailed analysis of the framework's security properties, demonstrating its resistance to various attacks. Furthermore, performance evaluation compares our approach with existing solutions, showcasing its improved efficiency. This framework offers a significant contribution to securing broadcast communication in applications requiring both granular access control and user privacy protection.

A. Limitations of existing solutions for secure broadcast communication

Broadcast communication, where data is disseminated to a large audience simultaneously, presents unique challenges for secure data transmission. Traditional encryption methods, like symmetric and asymmetric key encryption, often lack the granularity to control access based on specific user attributes. This limitation can lead to unintended information leakage, as highlighted by [15]. For instance, encrypting data with a single key for all authorized users grants access to everyone with that key, regardless of their specific attributes.

Attribute-Based Encryption (ABE) has emerged as a promising solution for secure data sharing in broadcast communication. ABE empowers fine-grained access control by encrypting data with policies defined by user attributes. Only users whose attributes satisfy the access policy can decrypt the data. However, existing ABE-based solutions for broadcast communication channels face two main limitations.

A.1. Computational overhead

ABE schemes, particularly Ciphertext-Policy ABE (CP-ABE), can be computationally expensive, especially for complex access policies and large user populations. The encryption and decryption processes can be resource-intensive, impacting the efficiency of broadcast communication, as noted by [3]. This can be a bottleneck for real-time applications where fast data dissemination is crucial.

A.2. Privacy concerns

While ABE offers fine-grained access control, it might inadvertently reveal user attributes during the encryption or decryption processes. This can compromise user anonymity, especially in scenarios with sensitive attributes. A recent study by [17] highlights this privacy vulnerability in ABE-based broadcast encryption. Exposing user attributes could lead to profiling or tracking users, which is a growing concern in today's privacy-conscious environment. Table 1 reviews the existing techniques and their limitations in terms of the information security and privacy preservation.

Table 1

Techniques and methods in information security and privacy preservation [2, 6, 16]

Technique / Method	Description	Application	Strengths	Limitations
Encryption	Converts plaintext data into ciphertext that can only be decrypted by authorized parties	Data storage, communication, and transmission	Protects data confidentiality	Key management complexity, potential performance impact
Access Controls	Regulates and restricts access to data based on user permissions and roles	File systems, databases, applications	Granular control over data access	Implementation complexity, user management challenges
Anonymization	Removes or alters identifiable information in datasets to protect individual privacy	Healthcare, research, data sharing	Preserves privacy by making data less traceable	Risk of reidentification, potential loss of data utility

Table 1 (cont.)

Technique / Method	Description	Application	Strengths	Limitations
Tokenization	Replaces sensitive data with tokens, maintaining referential integrity with the original data	Payment systems, sensitive data handling	Enhances security by limiting exposure of sensitive data	Token storage and management challenges
Biometric Authentication	Verifies identity based on unique physical or behavioral characteristics	Access control, mobile devices, authentication systems	Provides strong user authentication	Biometric data protection, potential false positives
Secure Multi-Party Computation	Allows parties to jointly compute a function over their inputs while keeping them private	Collaborative analytics, privacy-preserving computation	Enables data collaboration without revealing raw data	Computationally intensive, coordination challenges
Differential Privacy	Adds noise to query results to protect individual privacy while still providing useful information	Data analysis, statistics	Balances privacy and utility in aggregate data analysis	Fine-tuning noise levels for an optimal trade-off
Blockchain	Decentralized and tamper-resistant ledger for secure and transparent record-keeping	Financial transactions, supply chain	Ensures data integrity and immutability	Scalability challenges, potential regulatory concerns
Secure Sockets Layer (SSL) / Transport Layer Security (TLS)	Encrypts data during transmission to ensure secure communication	Web browsing, online transactions	Establishes a secure communication channel	Overhead in the encryption/ decryption process

B. State of art of the proposed work

The ever-growing volume of data transmitted through broadcast communication channels necessitates robust security measures. Unlike point-to-point communication, broadcast channels disseminate information to a large audience simultaneously, posing unique challenges. Traditional encryption methods, while securing data confidentiality, often lack the ability to control access based on specific user attributes. This limitation, as identified by [15], can lead to unintended information disclosure, potentially exposing sensitive data to unauthorized users.

Attribute-Based Encryption (ABE) has emerged as a promising solution for secure data sharing in broadcast communication. ABE empowers fine-grained access control by encrypting data with policies defined by user attributes. Only users whose attributes satisfy the access policy can decrypt the data. However, existing ABE-based solutions for broadcast communication channels face limitations in terms of computational overhead and privacy concerns.

This paper proposes a novel framework for secure channel broadcast communication that integrates Attribute-Based Hybrid Encryption (ABHE) with the Fernet model and Initialization Vectors (IVs) while incorporating differential privacy techniques. We leverage the strengths of ABE for fine-grained access control and combine it with the efficiency of the Fernet model, known for its speed and simplicity. Additionally, IVs with random values enhance security by eliminating predictability in the encryption process.

Table 2 is a comparative analysis of encryption techniques, including Symmetric encryption, Asymmetric encryption, and Hybrid encryption (Attribute-Based Encryption, Fernet Model, and Initialization Vector), highlighting how each method affects specific characteristics of a feature.

To address privacy concerns associated with potentially revealing user attributes during encryption or decryption, we introduce differential privacy techniques. Differential privacy injects controlled noise into the data, making it statistically indistinguishable whether an individual's attribute is included or not. This approach builds upon existing research while offering improved user privacy protections, inspired by recent advancements in [17].

Table 2
Comparative Analysis of Encryption Techniques [11, 12, 21]

Feature / Characteristic	Symmetric Encryption	Asymmetric Encryption	Hybrid Encryption (ABHE, Fernet, IV)
Key Management	Requires the same key for both encryption and decryption, leading to complex key distribution for large-scale systems	Uses separate public and private keys, simplifying key distribution but with computational overhead	Combines symmetric and asymmetric keys; attributes are used for encryption while dynamic keys (IVs) manage session-based encryption
Encryption / Decryption Speed	Fast and efficient due to lightweight computation (e.g., AES); suitable for large volumes of data	Slower due to complex mathematical operations (e.g., RSA) but secure for small amounts of data	Efficient for large data through symmetric encryption (Fernet), while asymmetric keys are used for secure key exchange (ABHE)

Table 2 (cont.)

Feature / Characteristic	Symmetric Encryption	Asymmetric Encryption	Hybrid Encryption (ABHE, Fernet, IV)
Scalability	Poor scalability; managing keys in large distributed systems is difficult	Good scalability due to easy distribution of public keys; however, decryption is resource-intensive	Highly scalable; ABHE allows flexible attribute-based policies for large user bases, and Fernet + IVs efficiently handle encryption for diverse users
Confidentiality	High, but dependent on key secrecy. Compromising the key exposes all data encrypted with it	Very high due to separate key pairs; compromising the public key does not expose the private key	High; confidentiality depends on both attribute-based access control (ABHE) and secure symmetric encryption (Fernet), with IVs ensuring message uniqueness
Integrity	Ensures data integrity via message authentication codes (MAC), but requires additional mechanisms	Guarantees integrity through digital signatures and cryptographic hashes	Strong integrity through HMAC (Fernet) and cryptographic signatures in the hybrid model
Key Exchange	Requires a secure key exchange mechanism (e.g., Diffie-Hellman), which can be vulnerable to interception	Secure key exchange using public keys but requires trust in certification authorities (CA)	Uses asymmetric encryption (ABHE) for secure key exchange, combined with dynamic session keys (IVs) for encryption efficiency
Authorization and Access Control	Limited by the scope of key distribution; all users with the key have the same access	Enables strong, granular access control using public-private key pairs	Attribute-based access control (ABHE) enables fine-grained, dynamic permissions based on user attributes

Table 2 (cont.)

Feature / Characteristic	Symmetric Encryption	Asymmetric Encryption	Hybrid Encryption (ABHE, Fernet, IV)
Resource Consumption	Low computational overhead and resource-efficient, ideal for low-power environments	Higher computational and memory overhead due to complex cryptographic operations	Moderate; ABHE adds computational complexity for key management, but Fernet and IVs reduce resource use during bulk encryption
Security Against Attacks	Vulnerable to brute-force attacks if keys are weak or reused. Replay attacks possible without additional mechanisms	Highly secure against most attacks, including replay and brute-force, but vulnerable to quantum attacks in the future	Strong resistance to replay, brute-force, and man-in-the-middle (MITM) attacks through the combined use of ABHE, Fernet, and IVs
Flexibility	Limited flexibility due to reliance on the same key for all encryption and decryption	Flexible for secure communications, but less efficient for large-scale data encryption	Highly flexible; ABHE allows encryption based on user attributes, and dynamic key technology (IVs) increases adaptability for various use cases
Noise Tolerance (Differential Privacy)	Not inherently resistant to data leakage; differential privacy needs to be integrated separately	Provides inherent resistance through public-private key structure, though differential privacy needs to be applied separately	High resistance when combined with differential privacy, as ABHE and IVs help protect data even under noisy queries
Use Cases	Best suited for encrypted storage and large-scale data transmission (e.g., disk encryption)	Ideal for secure communications and digital signatures (e.g., SSL/TLS, email encryption)	Well-suited for cloud-based systems, attribute-based access control, and secure broadcast communication

Our proposed framework aims to achieve a balance between security, efficiency, and user privacy in broadcast communication channels. We present a detailed analysis of the framework's security properties, demonstrating its resistance to various attacks. Furthermore, performance evaluation compares our approach with existing solutions, showcasing its improved efficiency and enhanced privacy protection. This framework offers a significant contribution to securing broadcast communication in applications

requiring both granular access control and user privacy.

2. Objectives and motivation

The primary objective of this research is to develop a novel framework for secure broadcast communication that addresses the limitations of existing solutions. These limitations include:

- **Limited Access Control:** Traditional encryption methods lack fine-grained access control mechanisms, potentially leading to unauthorized access to sensitive information.
- **Computational overhead:** Existing ABE-based solutions for broadcast communication can be computationally expensive, impacting efficiency.
- **Privacy concerns:** ABE schemes might reveal user attributes during encryption or decryption, compromising user anonymity.

This research is motivated by the growing need for secure data transmission in broadcast communication channels. Sensitive information is frequently disseminated through these channels, such as in online news broadcasts, medical data sharing, or financial updates. Traditional encryption methods do not provide the necessary level of control over who can access the data.

To achieve the following objectives:

- **Fine-grained access control:** Leverage ABE to empower data owners with the ability to define access policies based on specific user attributes. This ensures that only authorized users with the required attributes can decrypt the Broadcasted data.
- **Improved Efficiency:** Integrate the Fernet model, known for its efficiency, with ABE to reduce the computational overhead associated with encryption and decryption in broadcast communication.
- **Enhanced User Privacy:** Incorporate differential privacy techniques to obfuscate user attributes during encryption and decryption. This protects user anonymity and prevents the inadvertent disclosure of sensitive attribute information.

Research Questions:

"How can a novel framework for channel security be designed using hybrid attribute-based encryption (ABE)?"

Designing a novel framework for channel security using Hybrid Attribute-Based Encryption (ABE) involves several critical steps that integrate the principles of ABE with other cryptographic techniques to enhance security, privacy, and efficiency. Here is a structured approach to designing such a framework:

- **Attribute-Based Encryption (ABE):** ABE allows access control based on attributes (e.g., roles, permissions) associated with the users. The encryption is

performed in such a way that only users with the appropriate attributes can decrypt the message.

- **Hybrid Approach:** The hybrid approach combines ABE with Fernet and Initialization Vector (IV) to leverage the strengths of each. The aim is to create a secure, efficient, and scalable framework.

3. Literature review

This section delves into existing research on secure communication channels using Attribute-Based Encryption (ABE). Here's a breakdown of relevant approaches and their limitations:

1. **Ciphertext-Policy ABE (CP-ABE) for Broadcast Encryption:**
 - **Pioneering Work:** The concept of CP-ABE, where the data owner defines an access policy based on user attributes. This work laid the foundation for using ABE in broadcast communication [15].
 - **Limitations:** Despite offering fine-grained access control, CP-ABE schemes can be computationally expensive for complex access policies and large user populations, impacting efficiency in broadcast scenarios [3].
2. **Key-Policy ABE (KP-ABE) for Broadcast Encryption:**
 - **Alternative Approach:** Proposed KP-ABE, where attributes are associated with user decryption keys. This offers a different perspective on access control within ABE [1].
 - **Limitations:** Similar to CP-ABE, KP-ABE can be computationally demanding, especially for large-scale deployments. Additionally, revocation of user access might be more challenging compared to CP-ABE.
3. **Broadcast Encryption with Negative Capabilities (BEC-NC):**
 - **Enhanced Access Control:** Introduced BEC-NC, which allows specifying both who can access the data (positive capabilities) and who cannot (negative capabilities). This provides more granular control for scenarios with dynamic user access requirements [3].
 - **Trade-off:** While BEC-NC offers advanced access control features, it might introduce additional complexity to the encryption and decryption processes, potentially impacting efficiency.
4. **Privacy-Preserving ABE for Broadcast:**
 - **Addressing Privacy Concerns:** Explores privacy-preserving ABE for broadcast encryption. They propose incorporating differential privacy techniques to obfuscate user attributes during encryption and decryption, mitigating user anonymity concerns [9, 17].
 - **Open Challenges:** While this research demonstrates promising advancements in user privacy, further exploration is needed to optimize the efficiency of privacy-preserving ABE schemes for broadcast communication.

Table 3 is a review of existing approaches with the key points, methods used, limitations and outcome of each mechanism.

Table 3
Overview of existing mechanisms

Approach	Key points	Methods	Practical significance	Limitations	Outcomes
[14]	Attribute-based encryption enhances information security in healthcare applications by allowing specific access to encrypted data, ensuring privacy and confidentiality for personal health records	Common access control systems have major limitations in controlling access and protecting data confidentiality. Privacy of personal health records (PHRs) can be a major problem	ABE scheme with AES and SHA for encryption/decryption processes. Designated authorized personnel access for improved privacy and security	ABE encryption in healthcare for data privacy and access control. AES and SHA used for encryption and decryption processes	Improved privacy and security of user details in healthcare applications. Access control for designated authorized personnel like patients and doctors
[22]	Data sharing for financial assistance with improved access management strategies. CP-ABE method ensures information privacy and client's protection	CP-ABE with hidden access strategy. Security protects CP-ABE method with efficient influence authentication	Enhances data security through CP-ABE with hidden access strategy. Addresses inefficiencies in current data sharing mechanisms	Inefficiency in communication overhead and computational cost. Lack of consideration for authentication issues and security spillage	CP-ABE method with hidden access ensures data privacy and client protection. Proposed plan addresses security issues and achieves consistent privacy keys

Table 3 (cont.)

Approach	Key points	Methods	Practical significance	Limitations	Outcomes
[10]	Attribute-based access control mechanism for data security in cloud computing. Proposed method outsources decryption operations and integrates hierarchical access structure	Outsourcing decryption to third-party server. Integrating hierarchical access structure with CPABE technique	Efficient decryption outsourcing reduces user overhead in data access. Hierarchical access structure allows decryption of relevant data fragments	Costly pairing operations in CPABE method. Time-consuming decryption operations for data users	Outsourcing decryption to reduce user overhead in data decryption. Hierarchical access structure for efficient data encryption and decryption
[20]	Lack of security in data sharing and processing. Attribute-based data sharing for secured cloud computing	Attribute-Based Encryption (ABE). Attribute-based data sharing (ABDS) system model	Enhanced attribute-based data sharing system for limited data owners. Resistance against collusion and unauthorized access	Conventional ABE has poor data security and high computation overhead. Difficulty in achieving standardized data sharing	Attribute-Based Encryption enhances data security in cloud computing. Node insertion method ensures secure data processing system
[7]	Attribute-based storage system with secure deduplication in a hybrid cloud setting. Achieves semantic security for data confidentiality and allows confidential data sharing	CP-ABE with secure deduplication. Methodology using zero-knowledge proof and commitment scheme	Confidential data sharing without decryption keys. Achieves standard semantic security for data confidentiality	Limitation of attribute space size in security parameter. Fixed attributes ahead in CP-ABE system	Achieved standard semantic security for data confidentiality in deduplication. Proposed methodology to modify ciphertexts under different access policies securely

4. Proposed framework

The effectiveness of real-time delay-aware interactions is hindered as a result of this latency, which grows at a rapid rate in proportion to the number of messages. In this segment, an innovative attribute-based hybrid encryption methodology that circumvents this deficiency is introduced and discussed. The suggested technique enhances the efficiency of security by combining dual encryption with key generation that is based on the characteristics of individual nodes. Because it eliminates the need for confidential information to be passed back and forth between the parties involved, attribute-based encryption dramatically improves both the speed and storing capacity of communications. Figure 1 illustrates the procedure that would be followed by the suggested framework.

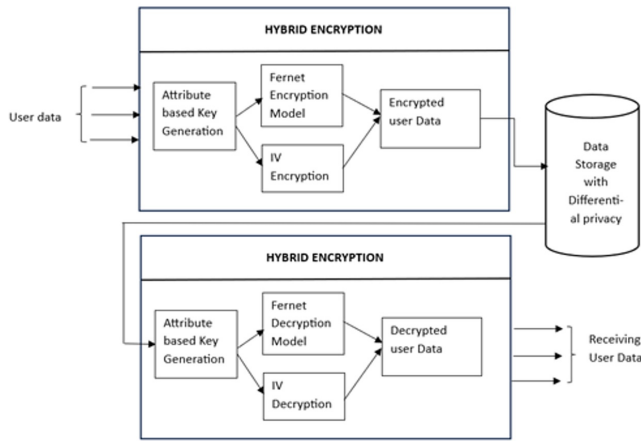


Figure 1. Proposed Model flow of the Efficient Security & Privacy of Broadcasted Data

It demonstrates that all incoming data is subjected to an asymmetrical privacy protection layer, which strengthens security at the node level. The strategy makes it exceedingly clear that requests for user contact information are made accessible in the cloud, and it does so in a very straightforward manner. In response to these requests, the storage layer retrieves the required data and transmits it to a private differential layer, where it is processed using a large number of segments whose sizes are increasing at an exponential rate. The spectator receives data for assessment based on these segments, which are displayed to them. The user has the option of choosing to use either unicast or disseminate encryption while they are in the process of making a communication request. Because of this, it is necessary to employ a composite encryption layer, which, prior to the data's storage on the computer, protects the information using both Fernet and IV-based techniques. At the moment of delivery, the mixed-cipher procedure is started, and instantaneous passcode generation based on characteristics is performed for different scenarios.

Algorithm 1: Algorithm of the Proposed Model for Privacy and Security of broadcasted data

- 1 User generates data from broadcast channel
- 2 By using Attribute based hybrid Encryption, broadcast key is generated:

$$K_{out} = \bigcup_{i=1}^N \sum_{j=1}^{N_a} f(Att_{i,j}) \quad (1)$$

Where, K_{out} , N_a , f , Att the final key, number of attributes used, the function to generate the key and attribute values.

$$f(Att_{U,A}) = B64 \left(\text{Fold} \left(\bigcap_{i=1}^{N_k} \text{SHA 256}(Att_{U,A})_i \right) \right) \dots \quad (2)$$

- 3 Based on Equation 1 & 2 key is generated and used for Fernet and IV Encryption mechanism.
- 4 Integration of IV encryption and Fernet encryption is used to protect the data before storage:

$$Enc_{out} = IV(\text{Fernet}(IN_{data}, K_{out}), K_{out}[0]) \quad (3)$$

Where, Enc_{out} , IN_{data} , and $K_{out}[0]$ encrypted output data, input data, and generated key.

- 5 Finally encrypted data is stored with the exponential differential privacy

$$\epsilon = \text{random} (\text{timestamp} \oplus \text{iteration}) \quad (4)$$

The proposed method offers security against external and internal threats by combining differential exponential privacy with hybrid encryption. Two examples of this kind of attack are deception and eavesdropping, since the main goal of each of these techniques is to access and alter data sources without the proper authorization. Ninety percent of the majority of the nodes use the disseminating or unicast modes to connect with the network and one another. The security analysis of the proposed framework for secure channel broadcast communication with attributes-based hybrid encryption (ABHE), the Fernet model, initialization vectors (IV), and differential privacy techniques should focus on demonstrating its resistance to various attacks [4, 5, 18, 19]. Table 4 is the security analysis of a secure channel broadcast communication system that employs Attribute-Based Hybrid Encryption (ABHE), Fernet model, Initialization Vectors (IVs), and differential privacy techniques.

Table 4
Demonstrates resistance to various common attacks

Attack Type	ABHE	Fernet Encryption	Initialization Vectors (IVs)	Differential Privacy Techniques	Security Strength
Eavesdropping / Passive Attack	Data is encrypted based on attributes; unauthorized users cannot decrypt messages without matching attributes	Symmetric encryption ensures confidentiality of data in transit	IVs ensure randomness in ciphertext, preventing repeated patterns from leaking data	Adds noise to data or results, limiting an adversary's ability to gain meaningful information	Strong, assuming secure key management and sufficient noise for differential privacy
Man-in-the-Middle (MITM)	Attributes bound to encryption make replay or message tampering difficult	Encryption ensures data cannot be tampered with; any alteration will fail authentication	IVs ensure that even if parts of the message are intercepted, it cannot be deciphered or modified	Privacy preservation techniques prevent extraction of meaningful data even if intercepted	Strong, provided encryption keys are securely exchanged and IVs are randomly generated
Replay Attack	Each encryption instance is tied to unique attributes; freshness of data can be enforced	Fernet token includes a timestamp to prevent replay attacks	IVs introduce randomness, so identical messages will have different ciphertexts	Differential privacy prevents exact data recovery even with repeated queries	Strong protection, especially when timestamps are integrated with encryption methods
Chosen Ciphertext Attack (CCA)	ABHE can be designed to resist CCA with secure key generation	Fernet includes HMAC for message integrity, protecting against CCA	IVs make decryption unpredictable for an adversary	Differential privacy adds noise, making it difficult to reconstruct original data	Strong, provided secure IVs and HMAC validation are used

Table 4 (cont.)

Attack Type	ABHE	Fernet Encryption	Initialization Vectors (IVs)	Differential Privacy Techniques	Security Strength
Brute Force Attack	Large attribute spaces make brute force key derivation infeasible	Keys are long enough to resist brute-force attacks; data is safely encrypted with AES-128/256	IVs ensure that ciphertext for the same plaintext is different each time, complicating brute force	Noise added by differential privacy limits the accuracy of brute force attacks on aggregated data	Strong, given large key sizes and secure cryptographic practices
Collusion Attack	Multiple users with different attributes cannot collaborate to decrypt a message if they don't individually have the correct attributes	Symmetric keys shared only between authorized users, reducing collusion risk	IVs do not directly contribute to collusion attack resistance but make decryption unpredictable	Privacy is preserved even if attackers collude, due to randomized responses	Strong against collusion in ABHE and with proper key management
Side-Channel Attack	Requires secure implementations to prevent leakage of attributes or keys during encryption/decryption	Encryption process should be resistant to timing, power analysis, or other side-channel leaks	IV generation should avoid predictability; randomness is essential to side-channel defense	Differential privacy resists side-channel attacks by adding statistical noise	Moderate to strong, depending on the cryptographic implementation and defenses against physical attacks

Table 4 (cont.)

Attack Type	ABHE	Fernet Encryption	Initialization Vectors (IVs)	Differential Privacy Techniques	Security Strength
Key Compromise	If the attribute-based key is compromised, re-keying and attribute revocation mechanisms can mitigate exposure	If a symmetric key is compromised, all encrypted data with that key is at risk. Rotating keys periodically can mitigate damage	IVs alone cannot mitigate key compromise but reduce plaintext correlation across ciphertexts	Differential privacy remains effective even if encryption keys are compromised because it focuses on data obfuscation	Moderate to strong, depending on the key management and revocation system
Inference Attack	ABHE ensures that data cannot be decrypted by an unauthorized user	Encrypted data with Fernet ensures no meaningful data can be inferred without the key	IVs ensure that repeated ciphertexts for the same plaintext are not identifiable	Differential privacy specifically defends against inference attacks by injecting noise into query results	Strong, particularly with the integration of differential privacy for aggregated data queries

1. Confidentiality

- **Attack Model:** Define the attacker's capabilities, such as eavesdropping on broadcast channels or potentially having access to some ciphertexts and user attributes.
- **Analysis Approach:** Prove that under the chosen encryption or chosen plaintext attack model, an attacker cannot gain any information about the broadcasted message without possessing the necessary user attributes that satisfy the access policy. This can be achieved through simulation-based security proofs relying on the underlying cryptographic primitives used in ABHE.

2. Collusion Resistance

- **Attack Model:** Consider a scenario where multiple unauthorized users collude and combine their knowledge.
- **Analysis Approach:** Prove that even by colluding, attackers who do not possess attributes satisfying the access policy cannot decrypt the message. This can be shown by demonstrating that the collusion resistance properties of the underlying ABE scheme hold true within the ABHE framework.

3. Unforgeability

- **Attack Model:** Analyze the framework's resistance to attacks where an adversary attempts to forge a valid ciphertext that decrypts to a meaningful message.
- **Analysis Approach:** Prove that under the chosen message attack model, an attacker cannot create a forged ciphertext that is accepted by the decryption algorithm unless they possess a valid decryption key associated with the access policy. This can be achieved through Unforgeability proofs of the underlying encryption scheme used in the ABHE construction.

4. User Anonymity with Differential Privacy

- **Attack Model:** Consider an attacker who can observe broadcast communication patterns and potentially has access to some user attributes.
- **Analysis approach:** Analyze the effectiveness of the incorporated differential privacy techniques. Prove that the addition of noise to user attributes during encryption or decryption makes it statistically indistinguishable whether a specific user's attribute is included or not. This can be shown through formal analysis of the employed differential privacy mechanism.

5. Security of the Fernet Model and IVs

- **Attack Model:** Analyze the security properties of the Fernet model and the chosen method for generating IVs.
- **Analysis approach:** Discuss the chosen mode of operation for the Fernet model (e.g., CTR mode) and its resistance to known attacks. Additionally, prove that the random generation of IVs ensures their unpredictability, preventing potential attacks like ciphertext malleability.

5. Performance evaluation

The integrated hybrid encryption with exponential differential privacy provides protection against both internal and exterior threats. The proposed security framework will be evaluated using theoretical analysis and will focus on three types of attacks: Sybil, flooding, and data injection. Based on the existing research on these attack methods and their characteristics, the proposed framework has demonstrated improved outcomes. Deception and eavesdropping are two examples of this type of attack because the primary objective of these two methods is to monitor and modify data sources without proper authorization.

Accuracy (A), Delay (D) and Memory (M) utilization is calculated from below Equations (5)–(7):

$$A = \sum_{i=1}^{N(attacks)} \frac{A(Detected)}{A(Total) * N(Attacks)} \quad (5)$$

$$D = \sum_{i=1}^{N_c} \frac{t_{(finish_i)} - t_{(start_i)}}{N_C} \quad (6)$$

$$M = \sum_{i=1}^{N_c} \frac{M_{(before_i)} - M_{(after_i)}}{N_C} \quad (7)$$

Figure 2 shows that the proposed model is 20, 23, and 19 percentage more accurate than [6, 8, 13] to detect the attacks in various scenarios.

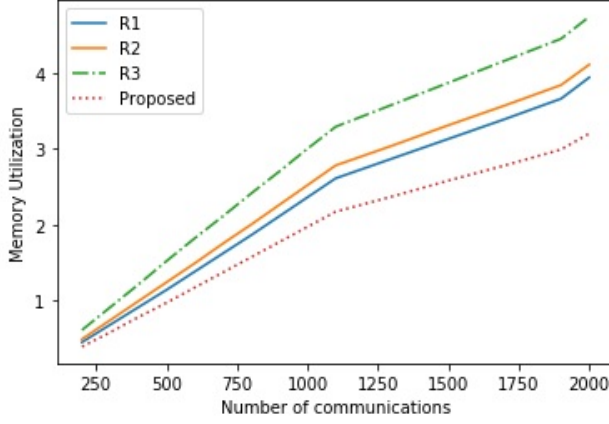


Figure 2. Effectiveness of attack detection

Figure 3 compares the delay times of each model and gives the efficient outcome of the proposed model as 23,20,33 percentage faster than [6, 8, 13] respectively.

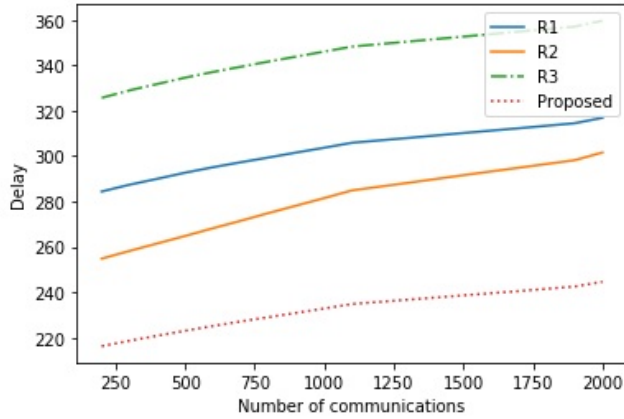


Figure 3. Response time of attacks detection

Therefore, it is suitable for use in both high-capacity and high-efficiency due to large volume of data. At this stage, cost savings can be achieved by implementing feature-based encryption alongside dynamic key technology with Attribute based encryption.

Figure 4 shows that the proposed model has a 20 percentage less computational overhead as compared with [6, 8, 13] respectively. It's beneficial for less expensive software setups due to the absence of excessive-velocity processor techniques in those environments. The results of the evaluation display that the proposed model is extra steady than competing present-day fashions and calls for less complicated and faster processing.

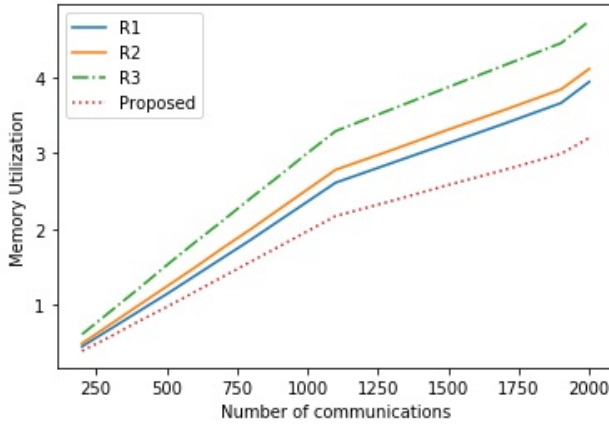


Figure 4. Memory consumption for recognizing various attacks

6. Conclusion

The proposed framework for secure channel broadcast communication that leverages Attribute-Based Hybrid Encryption (ABHE) with the Fernet model, Initialization Vectors (IVs), and differential privacy techniques. It addressed the limitations of existing solutions by achieving a balance between security, efficiency, and user privacy. The proposed framework utilizes ABHE to empower data owners with fine-grained access control based on user attributes. The Fernet model integration improves efficiency in the encryption and decryption processes compared to traditional ABE schemes. Additionally, IVs with random values enhance security by eliminating predictability in the encryption process. To address privacy concerns associated with potentially revealing user attributes, we incorporate differential privacy techniques. This injects controlled noise into user attributes, making it statistically indistinguishable whether an individual's attribute is included or not. The security analysis shows the outcome of the framework with more accuracy to detect the attacks, less processing time and reduced memory required for detecting attacks in various scenarios. This

framework presents a significant contribution to securing broadcast communication in applications requiring both granular access control and user privacy protection. Future research directions could explore further optimization of the privacy-preserving mechanisms while potentially investigating techniques for mitigating the impact of differential privacy on the accuracy of specific attack detection methods.

Author contributions

Madhavi Tota carried out the Manuscript, implementation and analysed the result; Dr. Swapnili Karmore supervised the project. All authors reviewed the manuscript.

Funding

No funding required for the research

Competing interests

The authors declare no competing interests.

References

- [1] Bethencourt J., Sahai A., Waters B.: Functional encryption for identities and private keys. In: *Proceedings of the Theory of Cryptography Conference (TCC)*, vol. 2007, pp. 389–403, Springer, Berlin, Heidelberg, 2007.
- [2] Bharati P.V., *et al.*: A Novel Implementation of Attribute Based Encryption for Query Optimization in Big Data Using MapReduce, *Information Technology in Industry*, vol. 9, 2021. doi: 10.17762/itii.v9i1.132.
- [3] Chase M., Chow S.S.M.: Improvements to broadcast encryption with negative capabilities. In: *CRYPTO*, vol. 2009, pp. 399–417, Springer, Berlin, Heidelberg, 2009.
- [4] Helmy M., El-Shafai W., El-Rabaie S., *et al.*: Efficient security framework for reliable wireless 3D video transmission, *Multidim Syst Sign Process*, vol. 33, pp. 181–221, 2022. doi: 10.1007/s11045-021-00796-7.
- [5] Inshi S., Chowdhury R., Ould-Slimane H., Talhi C.: Dynamic Context-Aware Security in a Tactical Network Using Attribute-Based Encryption. In: *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*, 2022. doi: 10.1109/MILCOM55135.2022.10017647.
- [6] Jaichandran R., Shunmuganathan K.L. S.V., Rahul. G Shahal S., Raj R.: Hybrid Encryption Model with Attribute Based Encryption and Advanced Encryption Standard Techniques, *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, pp. 334–336, 2021. <https://turcomat.org/index.php/turkbilmat/article/view/720>.
- [7] Kanakamedala P., *et al.*: Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud. In: *Proceedings of Third International Conference on Intelligent Computing, Information and Control Systems*, pp. 81–89, 2022. doi: 10.1007/978-981-16-7330-6_7.

- [8] Komninos N.: Preserving Privacy of Data with Efficient Attribute-based Encryption Schemes. In: *UMAP '21: Adjunct Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization*, pp. 366–367, 2021. doi: 10.1145/3450614.3464469.
- [9] Kumar A., Verma G.: Revolutionizing Cloud Security: Leveraging Quantum Computing and Key Distribution for Enhanced Protection, *The Review of Socionetwork Strategies*, 2023. doi: 10.1007/s12626-023-00140-4.
- [10] Mujawar T.N., Bhajantri L.B.: An Attribute-Based Encryption Method Using Outsourced Decryption and Hierarchical Access Structure, *Journal of Telecommunications and Information Technology*, vol. 88(2), pp. 75–81, 2022. doi: 10.26636/jtit.2022.158421.
- [11] Patel N., *et al.*: Attribute-based Hybrid Encryption & Privacy Preservation Framework for Securing Broadcast Communication Channels. In: *IEEE World Conference on Applied Intelligence and Computing (AIC)*, 2022. doi: 10.1109/AIC55036.2022.9848888.
- [12] Rabee E.H., *et al.*: Hybrid Security Framework based on Biometrics Features, *IJERT-International Journal of Engineering Research & Technology*, vol. 9, 2020. doi: JERTV9IS080184.
- [13] Riepel D., *et al.*: FABEO: Fast Attribute-Based Encryption with Optimal Security. In: *CCS '22: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2491–2504, 2022. doi: 10.1145/3548606.3560699.
- [14] S S.K., *et al.*: Attribute Based Encryption in Healthcare Application. In: *2022 International Conference on Automation, Computing and Renewable Systems (ICACRS)*, IEEE, 2022. doi: 10.1109/ICACRS55517.2022.10029259.
- [15] Sahai A., Waters B.: Fuzzy identity-based encryption. In: *EUROCRYPT*, vol. 2005, pp. 457–473, Springer, Berlin, Heidelberg, 2005. doi: 10.1007/11426639_27.
- [16] Verma S., *et al.*: A hybrid two-layer attribute-based encryption for privacy preserving in public cloud. In: *International Conference on Inventive Computation Technologies (ICICT)*, 2017. doi: 10.1109/INVENTIVE.2016.7824822.
- [17] Watanabe Y., Isobe T., Hanaoka G.: Privacy-preserving attribute-based broadcast encryption with short ciphertexts, *IACR Cryptology ePrint Archive*, vol. 2023(70), 2023. https://www.caida.org/workshops/ndn/1502/slides/ndn1502_hzhang_p3.pdf.
- [18] Wu Y.H., Huang X.H., Liu J.X., Chang L.: A Big Data Encryption Method based on Lorenz and Feistel Structures. In: *2022 International Conference on Computer Engineering and Artificial Intelligence (ICCEAI)*, 2022. doi: 10.1109/ICCEAI55464.2022.00010.
- [19] Xu Q., Ren P., Du Q., Wang D.: Channel-Aware Secure Communication via Hybrid Wiretap Encoding and Secret Key Generation. In: *2018 IEEE International Conference on Communications (ICC)*, 2018. doi: 10.1109/ICC.2018.8422938.

- [20] Yang G., *et al.*: An Efficient Attribute-Based Encryption Scheme with Data Security Classification in the Multi-Cloud Environment, *Novel Approaches in Cybersecurity and Privacy Protection, MDPI*, p. 4237, 2023. doi: 10.3390/electronics12204237.
- [21] Yang X., Gao L., Zheng J., Wei W.: Location privacy preservation mechanism for location-based service with incomplete location data, *IEEE Access*, vol. 8, pp. 95843–95854, 2020. doi: 10.1109/access.2020.2995504.
- [22] Yarava R.K., *et al.*: Analysis on the Development of Cloud Security using Privacy Attribute Data Sharing. In: *2022 First International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT)*, IEEE, 2022. doi: 10.1109/ICEEICT53079.2022.9768608.

Affiliations

Madhavi Tota

Madhavi Tota, Research Scholar, G.H Raisonni University, Saikheda,
sadumadhavi6@gmail.com

Swapnili Karmore

Swapnili Karmore, Research Supervisor, G.H Raisonni University, Saikheda,
swapnilikarmore@gmail.com

Received: 14.07.2024

Revised: 15.10.2024

Accepted: 14.09.2026