**International Journal of Emerging Research in Engineering and Technology**
Pearl Blue Research Group| AECTIC2025-Conference Proceeding
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.AECTIC-106

*Original Article*

# A Lightweight, Blockchain-Managed CP-ABE Scheme for Fine-Grained Access Control in the Automotive-Internet-of-Things (A-IoT)

Naresh Kalimuthu
Principal Engineer, Toyota, USA.

***Abstract*** *- The Automotive-Internet-of-Things (A-IoT) ecosystem produces large amounts of sensitive data from multiple stakeholders, leading to complex access control issues that traditional centralized systems cannot handle. This paper explores Lightweight Attribute-Based Encryption for Broadcast Cryptography (L-ABE-BC), a new, lightweight cryptographic system designed for precise access control in vehicles. Its architecture combines three main technologies: (1) a lightweight, pairing-free Ciphertext-Policy Attribute-Based Encryption (PF-CP-ABE) scheme using Elliptic Curve Cryptography (ECC) to reduce overhead on resource-limited ECUs; (2) an outsourced decryption process to reduce computational load on sensors; and (3) a permissioned blockchain that manages Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), ensuring decentralized, auditable, and quick management of attributes and revocations. This integrated system enables secure, policy-based encryption directly at the source, offering a practical approach for scalable, decentralized trust within the Automotive Internet of Things (A-IoT) environment.*

***Keywords*** *- Automotive IoT (A-IoT), Attribute-Based Encryption (ABE), Ciphertext-Policy (CP-ABE), Lightweight Cryptography, Elliptic Curve Cryptography (ECC), Blockchain, Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), Access Control, V2X.*

## 1. Introduction

### *1.1. The Automotive-Internet-of-Things (A-IoT) Data Ecosystem*

The Automotive Internet of Things (A-IoT) signifies a significant shift in the automotive sector, transforming vehicles from standalone mechanical systems into interconnected, cyber-physical entities. This ecosystem functions as a system-of-systems, integrating IoT components such as sensors, GPS devices, and cameras into the vehicle's main framework. These elements are managed by a network of specialized computers called Electronic Control Units (ECUs), which can number up to 100 in a luxury vehicle. This complex network produces a rapid stream of highly sensitive data, including real-time sensor logs, diagnostic trouble codes, predictive maintenance alerts (e.g., tire pressure, engine temperature), location history, driver behavior patterns, and safety messages for Vehicle-to-Everything (V2X) communication. While this data holds substantial value, its usefulness depends on a sophisticated access model involving multiple stakeholders:

- Original Equipment Manufacturers (OEMs): Need telemetric and diagnostic data for predictive maintenance, remote updates, and R&D.
- Vehicle Owners: Require access to their data and control over who else can see it.
- Technicians and Dealerships: Need temporary, privileged access to specific diagnostic systems for servicing.
- Fleet Managers: Require real-time tracking, fuel efficiency data, and operational logs to enhance routing and lower costs.
- Third Parties (e.g., Insurance): Seek data on driving behavior and vehicle health to develop dynamic, usage-based insurance models.

This multi-party setup highlights a key challenge in access control. A typical centralized system, where the OEM's cloud handles all data and permissions, creates a single point of failure and raises privacy concerns. A server breach could lead to complete data loss. Conversely, restricting all access to protect data can hinder crucial services like predictive maintenance. Consequently, an innovative security strategy is essential—one that is decentralized and governed by policies, enabling accurate access management without dependence on a single trusted authority.

### *1.2. Foundational Technology 1: Attribute-Based Encryption (ABE)*

Attribute-Based Encryption (ABE) is a sophisticated 'one-to-many' public-key cryptosystem. Unlike traditional encryption, which targets a specific recipient's public key, ABE encrypts data based on a description of the recipient. There are two main types of ABE:

*1.2.1. Key-Policy ABE (KP-ABE)*

In this model, the access policy is embedded in the user's private key (e.g., a key that can decrypt data labeled 'OEM' AND 'Diagnostics'). The data itself is encrypted with a set of attributes. KP-ABE is not suitable for A-IoT, as the data encryptor (the ECU) cannot control who accesses the data.

*1.2.2. Ciphertext-Policy ABE (CP-ABE)*

This model is ideal for A-IoT. Here, the access policy is embedded within the ciphertext by the encryptor. A user's private key is generated by an authority and linked to a set of attributes (e.g., {'Role:Technician', 'Affiliation:OEM', 'Region:EU'}). Decryption is only possible if the user's attribute set satisfies the ciphertext's policy (e.g., 'Role:Technician' AND 'Affiliation:OEM'). The foundational work on CP-ABE by Bethencourt, Sahai, and Waters was specifically designed to enforce complex access controls on encrypted data in untrusted environments, making it an excellent cryptographic primitive for the A-IoT challenge.

### *1.3. Foundational Technology 2: Blockchain and Decentralized Identity*

While CP-ABE offers a strong cryptographic framework, its traditional setup has a notable centralization flaw. It depends on a single, powerful Attribute Authority (AA) to generate the master key and distribute all private attribute keys. This AA becomes a security vulnerability. If compromised, the entire system's security is at risk. Additionally, this setup introduces a key-escrow problem, as the central AA can decrypt all ciphertexts, compromising privacy.

Blockchain technology, as a decentralized and immutable ledger, provides an effective solution. Instead of a single Attribute Authority (AA), a Multi-Authority ABE (MA-ABE) scheme can be used, where multiple organizations (such as OEMs, DMVs, and insurance providers) serve as independent authorities, managing their own attributes. A blockchain overseen by these stakeholders can serve as a transparent, auditable platform for managing public keys and permissions across these distributed actors. The most sophisticated implementation uses W3C standards for Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs).

- Decentralized Identifiers (DIDs): DIDs are unique, cryptographically verifiable identifiers controlled directly by the entity (vehicle, owner, or technician) and independent of any organization.
- Verifiable Credentials (VCs): VCs are tamper-evident, cryptographically signed claims issued by an authority (e.g., an OEM) to a holder (e.g., a technician). The VC resides in the user's private digital wallet, granting them control.
- The Ecosystem: The blockchain primarily functions as a Verifiable Data Registry (VDR), not storing personal data but enabling stakeholders to verify issuer signatures and check revocation statuses by querying it.

### *1.4. The Core Problem Statement and Our Contribution*

The A-IoT ecosystem needs a secure, decentralized, and detailed access control system. Simply combining the technologies described earlier won't work due to three main challenges:

- The Cryptography Issue: Standard CP-ABE schemes rely on bilinear pairings, which are computationally intensive, slow, and too resource-heavy for A-IoT devices.
- The Hardware Issue: Automotive ECUs are limited-resource devices, often based on low-power microcontrollers (such as ARM Cortex-M). They don't have enough processing power, memory, or energy to handle such demanding cryptography.
- The System Issue: Both traditional ABE, with its central Authorization Authority (AA), and public blockchains, with high-latency Proof-of-Work consensus mechanisms and high transaction costs, introduce performance bottlenecks and centralization risks that are unacceptable in real-time, large-scale IoT systems.

This paper introduces a new hybrid cryptosystem, L-ABE-BC (Lightweight ABE-Blockchain), designed to address all three challenges comprehensively. Our architecture combines: -

- A lightweight, pairing-free CP-ABE (PF-CP-ABE) scheme utilizing efficient Elliptic Curve Cryptography (ECC) to tackle cryptography issues.
- An outsourced decryption approach to alleviate hardware constraints by shifting heavy computations away from resource-limited ECUs.
- A hybrid, blockchain-managed DID/VC framework on a permissioned ledger that solves the system challenges by enabling decentralized, scalable, low-latency, and auditable trust.

## 2. Research Topics: Core Challenges in Securing A-IoT Data

Practical security architecture must be built upon a clear-eyed assessment of its operational constraints. The A-IoT environment presents a confluence of three distinct and formidable challenges that render standard cryptographic solutions non-viable.

### *2.1. Challenge 1: Computational Overhead of Pairing-Based Cryptography on Constrained ECUs*

The first challenge arises where cryptographic requirements meet hardware limitations.

#### *2.1.1. Hardware Constraints*

An automotive ECU is not a general-purpose computer but a highly specialized, resource-limited embedded system. Many ECUs belong to the Internet Engineering Task Force (IETF)'s constrained device classes (Class 1 or 2), which typically have only 10-50 KiB of RAM and 100-250 KiB of code storage. Often based on ARM Cortex-M microcontrollers, these devices prioritize reliability and low power use. Their main challenges are controlling power consumption and heat generation, as excess heat can harm the reliability of automotive electronics. Consequently, computationally intensive tasks are contrary to their primary design goals.

#### *2.1.2. Cryptographic Bottleneck*

Standard, secure Ciphertext-Policy Attribute-Based Encryption (CP-ABE) schemes, such as the widely referenced Bethencourt, Sahai, and Waters (BSW) Scheme, rely on a mathematical operation called a bilinear pairing (or bilinear map). A pairing is a function that takes elements from two cryptographic groups and maps them to a third group. This operation is known for being quite "expensive" in terms of computation. The time needed for a single bilinear pairing is roughly two to three times greater than performing a standard scalar multiplication on the same elliptic curve.

#### *2.1.3. The Scaling Problem*

This overhead is not a one-time expense. In CP-ABE, both encryption and decryption complexities grow linearly with the number of attributes in the access policy. A simple policy like "Role: Technician" AND "Region: EU" may be manageable, but a detailed, safety-critical data policy—such as (("Role: OEM-Engineer" AND "Subsystem: Brakes" AND "Level:5") OR ("Role: Regulator" AND "Event: Audit")) would involve many pairing operations, causing significant latency and increased power consumption.

This issue is also asymmetric. Although some decryption can be performed on powerful laptops, the encryption process must occur on a resource-constrained ECU. Additionally, in V2V communication, the decryptor is another ECU with limited capabilities. Consequently, any feasible solution must be lightweight for both encryption and decryption, which rules out the use of pairing-based cryptography altogether.

### *2.2. Challenge 2: Latency and Scalability of Blockchain in a Real-Time System*

The second challenge is the basic disconnect between how public blockchains perform and the real-time requirements of A-IoT.

- Real-Time Requirement: A-IoT systems are dynamic. V2X communications, used to share data to avoid collisions or alert about road hazards, are safety-critical and operate in real time. Access control decisions and even near-real-time diagnostic checks need to be made within seconds, not minutes.
- Latency and Throughput Mismatch: Public blockchains like Bitcoin and Ethereum rely on consensus mechanisms such as Proof-of-Work (PoW), which emphasize decentralization and resistance to censorship over other performance considerations.
- Latency: The "finality time"—the duration until a transaction becomes irreversible—can range from 10 to 60 minutes for PoW chains. Faster Proof-of-Stake (PoS) protocols typically vary from 2 to 15 minutes. This latency is too high for a technician waiting to access a vehicle, and it is impractical for V2V safety applications checks.
- Throughput: These public networks are known for their low transaction throughput (TPS) and are not built to manage the data volume generated by millions of IoT devices.

Systems and Cost Mismatch:

- Storage: ECUs with only 35 kilobytes of RAM cannot function as full nodes, as these require storing hundreds of gigabytes of ledger data.
- Cost: On public blockchains, each transaction, such as issuing a VC or revoking an attribute, requires a "gas fee"—a transaction cost you must pay to use the blockchain. For an A-IoT system managing millions of vehicles and potentially thousands of daily attribute updates (like technician certifications or fleet assignments), the operational expenses would be astronomical.

The "Blockchain Trilemma" states that a system can't optimize decentralization, security, and scalability simultaneously. Since A-IoT requires high performance and scalability, it must sacrifice public decentralization. This leads to using a permissioned consortium blockchain like Hyperledger Fabric, which employs fast, Byzantine Fault Tolerance (BFT)-based consensus. These platforms are built for industrial groups, providing high throughput, low latency, and importantly, no inherent transaction fees.

### *2.3. Challenge 3: Efficient, Dynamic Attribute Revocation*

The third and most crucial security challenge is revocation. In an A-IoT system, if a technician is terminated, a vehicle is stolen, or an ECU's key becomes compromised, its attributes must be revoked instantly. In traditional ABE, this is a well-known, complex, and costly challenge because attributes are cryptographically linked to a user's private key. Existing solutions all have significant flaws when applied to a large-scale IoT environment:

*2.3.1. Indirect Revocation (Re-Keying)*

The Attribute Authority (AA) regularly issues new attribute keys, often with timestamps, to all non-revoked users, such as daily updates. When a user is revoked, the AA stops issuing them new keys. This approach results in significant communication overhead, with O(N) key updates per user, leading to a large "update storm" that can overwhelm low-bandwidth wireless networks.

*2.3.2. Ciphertext Re-Encryption*

The data owner (or a proxy) must re-encrypt all data accessible to a revoked user with a new policy that excludes them. This process is computationally intensive and practically impossible for immutable, historical diagnostics logs.

*2.3.3. Direct Revocation (Revocation Lists)*

The encryptor appends a list of revoked user IDs to each ciphertext, leading to its growth over time and requiring the (limited) encrypting ECU to maintain a (possibly extensive) global revocation list continually.

The main issue is a misinterpretation of the problem: revocation should be treated as a state-management challenge, not a cryptographic one involving re-keying or re-encryption. Blockchain offers an elegant solution here. By leveraging the ledger as a trusted, immutable record of status, revocation can be performed with a single transaction. The decryption process is adjusted to include a final check: "Is the credential still valid for this decryption?" As a result, revocation becomes as straightforward and quick as flipping a bit in a smart contract.

## 3. Recommendations / Mitigation Strategies: The Proposed L-ABE-BC System Architecture

To address the three challenges outlined in Section II, this paper introduces the L-ABE-BC (Lightweight ABE-Blockchain) system. It features a hybrid, multi-component architecture designed to ensure security, scalability, and efficiency in the A-IoT environment.

### *3.1. System Core: A Pairing-Free, ECC-Based CP-ABE Scheme (Mitigating Challenge 1)*

To solve the "Pairing Bottleneck" (Challenge 1), the cryptographic core of Lightweight Attribute-Based Encryption for Broadcast Cryptography (L-ABE-BC) is a **Pairing-Free CP-ABE (PF-CP-ABE)** scheme.

*3.1.1. Mechanism*

This architecture employs standard Elliptic Curve Cryptography (ECC). It replaces the costly bilinear pairing operation with the more efficient ECC scalar multiplication. ECC scalar multiplication is significantly faster than pairings, is more mature, and is often hardware-accelerated on modern microcontrollers, including automotive-grade ARM Cortex-M processors.

*3.1.2. Security and Design*

The security of this PF-ABE scheme relies on the standard Elliptic Curve Decisional Diffie-Hellman (ECDDH) assumption, rather than complex pairing-based assumptions. However, caution is essential when designing such schemes, as several published "lightweight" ECC-based ABE schemes have been shown to be insecure. The proposed Lightweight Attribute-Based Encryption for Broadcast Cryptography (L-ABE-BC) scheme addresses the key-escrow issue at an architectural level by employing a multi-authority approach. This means no single authority, such as the OEM, can decrypt data that requires attributes from another authority, like the DMV. The key generation process is distributed across these authorities.

The formal construction consists of five algorithms:

$\text{GlobalSetup}(\lambda) \rightarrow \text{GP}$:

- What it does: It establishes the mathematical ground rules that everyone must agree on.
- A one-time, public function that determines global ECC parameters (e.g., the curve $\text{secp256r1}$, a generator G, and hash functions). This results in the Global Parameters (GP).

$\text{AuthSetup}(\text{Auth}_{\text{ID}}) \rightarrow (\text{SK}_{\text{A}}, \text{PK}_{\text{A}})$:

- What it does: This establishes the authorities trusted to endorse or verify people.
- Run by each Attribute Authority (e.g., OEM, DMV) to generate their master secret key ($\text{SK}_{\text{A}}$) and public key ($\text{PK}_{\text{A}}$). They publish $\text{PK}_{\text{A}}$ and their DID on the blockchain Verifiable Data Registry (VDR).

$\text{KeyGen}(\text{SK}_\text{A}, \text{User}_\text{DID}, \text{VC}) \rightarrow \text{SK}_{\text{user, attr}}$:

- What it does: A user, such as a mechanic, verifies their identity to gain access keys.
- A user presents their ID ($\text{User}_\text{DID}$), and a valid Verifiable Credential (VC) (e.g., "Role: Technician") to the issuing Authority (Issuer). The Issuer verifies the VC, then uses it $\text{SK}_\text{A}$to generate a partial attribute key ($\text{SK}_{\text{user,atttr}}$) for the user.

$\text{Encrypt}\ (\text{GP}, \{\text{PK}_\text{A}\}, \text{T}, \text{M}) \rightarrow \text{CT}$ :

- What it does: An Electronic Control Unit (ECU) inside a car wants to send sensitive data (Message M) only to authorized recipients.
- The ECU (Encryptor) generates a random symmetric key K. It encrypts the message M with K (e.g., AES-GCM) to get $\text{C}_\text{M}$ (this is hybrid encryption). It then encrypts K using PF-ABE scheme under a policy T (e.g., "Role: Technician" AND "Certified: OEM"). The policy T and the encrypted key K are output as the ciphertext CT.

$\text{Decrypt}(\text{GP}, \text{CT}, \{\text{SK}_{\text{user,attr}}\}) \rightarrow \text{M}$:

- What it does: The user tries to read the message.
- The user (Decryptor) first provides their set of partial attribute keys $\{\text{SK}_{\text{user,attr}}\}$. If the attribute set satisfies the policy T embedded in CT (and the attributes are not revoked), the ECC operations will combine to reconstruct the symmetric key K. K is then used to decrypt $\text{C}_\text{M}$and recover the plaintext M.

### *3.2. Hardware Mitigation: Outsourced Decryption (Mitigating Challenge 1, cont.)*

Even the rapid ECC operations in our PF-ABE scheme can be too demanding for the most constrained ECUs, like a basic sensor node. To address this, Lightweight Attribute-Based Encryption for Broadcast Cryptography (L-ABE-BC) uses an outsourced decryption approach. This approach splits the intensive decryption process into two parts, with the bulk of the work assigned to a powerful, semi-trusted proxy. In the A-IoT setting, this proxy is typically the vehicle's central Domain Control Unit (DCU) or a nearby Roadside Unit (RSU).

The mechanism works as follows:

- Modified KeyGen: The user's KeyGen algorithm is modified to produce two keys:
  - A private Secret Key (SK): This is a small, constant-size blinding factor z, which the user (or constrained device) keeps secret.
  - A public Transformation Key (TK): This is the original set of ABE attribute keys, blinded by $\text{z}^{-1}$ This TK is given to the proxy (e.g., the Domain Control Unit (DCU)).
- Transform (on Proxy): The proxy (DCU) receives the full, complex PF-ABE ciphertext CT. It uses the TK to perform all the "heavy" ECC scalar multiplications required by the policy. This "transforms" CT into a single, simple, and constant-size ElGamal-type ciphertext $\text{CT}'$.
- Security: During this transformation, the proxy (DCU) cannot learn any information about the plaintext message Mt; is simply performs a mathematical blinding operation.
- Final Decryption (on ECU): The proxy sends the tiny $\text{CT}'$to the constrained ECU. The ECU uses its private SK (the blinding factor z) to perform one single, lightweight ECC operation to recover the symmetric key K.

This model shifts over 99% of the decryption workload from the constrained ECU to the powerful DCU, enabling complex, policy-based decryption even on the most resource-poor IoT devices.

### *3.3. Trust & Performance Mitigation: A Hybrid On-Chain/Off-Chain Model (Mitigating Challenge 2)*

To address the issues of latency, throughput, and cost (Challenge 2), L-ABE-BC needs to be built on a Hybrid Smart Contract architecture. A "lightweight" cryptosystem is ineffective if it operates on a "heavy" (slow and costly) public blockchain. The system architecture also needs to be lightweight.

#### *3.3.1. On-Chain (The "Trust Layer"):*

- Ledger Choice: We select a Permissioned Consortium Blockchain such as Hyperledger Fabric.
- Rationale: Fabric is tailored for industrial consortia, such as groups of OEMs, suppliers, and regulators. Its BFT-based consensus ensures high throughput, handling thousands of TPS, and offers low-latency finality within seconds. Crucially, as a permissioned ledger, it does not incur "gas" or transaction fees, making it cost-effective for high-volume attribute management.
- On-Chain Data: The Fabric ledger functions solely as a Verifiable Data Registry (VDR), storing only the essential high-value metadata required to establish it trust:
  1. The DIDs of all registered entities (Vehicles, Owners, OEMs, Technicians).
  2. The DIDs and Public Keys of trusted Attribute Authorities (Issuers).
  3. A Smart Contract implementing the W3C "Status List 2020" for attribute revocation.

*3.3.2. Off-Chain (The "Data & Computation Layer"):*

- A-IoT Data: All high-volume, sensitive data such as sensor logs, GPS trails, and V2X messages is NEVER stored on-chain. Instead, it is encrypted at the source using our PF-ABE scheme and then stored in a standard, scalable, and cost-effective off-chain repository, like OEM cloud storage, an edge server, or the vehicle's on-board system storage).
- Verifiable Credentials: The VCs (attributes) are also stored off-chain in the user's private digital wallet, such as on their mobile device, ensuring control remains user-centric and private.

***3.4. Dynamic Access Mitigation: The L-ABE-BC Revocation Flow (Mitigating Challenge 3)***

This section integrates all architecture components to deliver an efficient, prompt, and cost-effective solution to the attribute revocation problem (Challenge 3), eliminating the need for extensive re-keying or re-encryption.

The full L-ABE-BC workflow is as follows:

- Setup: The OEM, DMV, and other trusted organizations (Issuers) register their DIDs and public keys on the Hyperledger Fabric ledger (the VDR).
- Issuance: Technician "Bob" completes an OEM certification. The OEM (Issuer) cryptographically signs a VC ({"type": "Technician", "level": "5", "issuer": "DID: OEM: Ford"}) and sends it to Bob's digital wallet (Holder).
- Encryption: A vehicle's ECU (Data Owner) generates a diagnostic log M. It encrypts M using the PF-ABE Encrypt function with the policy $T = (\text{"Technician" AND "level: 5" AND "Certified: OEM"})$ . The resulting ciphertext CT is uploaded to off-chain cloud storage.
- Decryption (Valid User): Bob (Data User) wants to access CT.
  a. His wallet (Holder) presents the required VCs to the Decrypt function (or its Verifier proxy).
  b. The Decrypt function (or proxy) uses the VCs to assemble the necessary attribute keys $\{SK_{user,attr}\}$.
  c. It then performs a mandatory, real-time check by querying the on-chain VDR (smart contract) to verify two things:
    i. Is the Issuer of the VC (DID: OEM: Ford) still a valid, trusted issuer in the consortium?
    ii. Is the serial number of Bob's VC present on the revocation "Status List"?
  d. The smart contract returns FALSE (not revoked).
  e. The decryption operation proceeds, and Bob successfully decrypts M.
- Revocation: Bob is fired from his job.
  a. The OEM (Issuer) executes one single, low-latency transaction on the Fabric blockchain, calling the "Status List 2020" smart contract to add Bob's VC serial number to the revoked list.
- Decryption (Revoked User): Bob attempts to use the same VCs and the same attribute keys to access CT again.
  a. Steps 4a and 4b proceed as normal. His keys still satisfy the policy cryptographically.
  b. At step 4c, the Decrypt function queries the on-chain "Status List."
  c. The smart contract now returns TRUE (revoked).
  d. The Decrypt function aborts. Access is denied.

This revocation scheme is immediate, auditable, and, most importantly, has an $O(1)$ complexity. Revoking a user's access incurs zero computational or communication overhead for any other user, any other data, or any other authority in the system.

## 4. Recommendations and Goals Achieved: A Comparative Analysis

The Lightweight Attribute-Based Encryption for Broadcast Cryptography (L-ABE-BC) system is designed to meet the objectives of lightweight computation, real-time scalability, and secure, dynamic revocation. This section compares how effectively these goals are accomplished.

***4.1. Goal Achievement: Lightweight Computation (Challenge 1)***

- Metric: Latency of cryptographic operations (ms).
- Analysis: Replacing "heavy" pairings with "light" ECC operations and adding an outsourcing layer significantly reduces the computational load on the constrained ECU. Performance improvements can be estimated by analyzing benchmark data for ABE on automotive-grade platforms and research on pairing-free schemes.

A baseline study on an automotive-compliant platform (Xilinx ZCU102) using a pairing-based CP-ABE library (PBC) found that ABE decryption took 38.38 ms for a simple policy with 1 attribute and 61.27 ms for 2 attributes. This highlights the poor $O(N)$ scaling of pairing-based decryption.

The L-ABE-BC architecture changes this completely. Most of the intensive computation—specifically, the faster ECC multiplication—is performed by the proxy (DCU). The only remaining on-device task for the limited ECU is a single, constant-time ElGamal-like decryption, which requires roughly the same amount of computation as one ECC operation.

**Table 1: Comparative Analysis of On-Device Decryption Overhead**

| Operation | System 1: Traditional Pairing-Based ABE (Baseline) | System 2: Proposed PF-ABE (ECC-based) (Estimate) | System 3: Proposed L-ABE-BC (PF-ABE + Outsourcing) |
|---|---|---|---|
| On-Device Decryption Task | Full policy-matching & pairing computations | Full policy-matching & ECC scalar multiplications | Single ECC operation (final decryption) |
| Computational Complexity (on-device) | $O(N)$ pairings (where N = attributes in policy) | $O(N)$ scalar multiplications | $O(1)$ scalar multiplication |
| Measured/Est. Latency (N=2 attributes) | ≈61.27 ms | ≈5-10 ms (est.) | < 1 ms (est.) |
| Scalability (on-device) | Poor: Latency grows with policy complexity. | Poor: Latency grows with policy complexity. | Excellent: Latency is constant, regardless of policy. |

As shown in Table 1, the L-ABE-BC system (System 3) is the only architecture that offers both lightweight computation and $O(1)$ (constant-time) on-device decryption.

### *4.2. Goal Achievement: System Scalability & Real-Time Performance (Challenge 2)*

- Metric: Transaction Throughput (TPS), Latency (s), and Cost (gas).
- Analysis: The hybrid on-chain/off-chain model, which is based on a permissioned ledger, directly addresses the scalability and latency issues common in public blockchains.
- Latency: Public PoW/PoS chains typically have a finality of several minutes. In contrast, our selected permissioned ledger (such as Hyperledger Fabric) employs BFT-based consensus, providing finality within 2 seconds. This speed is adequate for the near-real-time attribute and revocation checks needed for A-IoT.
- Cost: Public chains incur high, variable gas fees per transaction. In contrast, Hyperledger Fabric, a permissioned system, has no gas fees. This makes it a crucial enabler for high-volume IoT application systems.
- Footprint: A hybrid architecture that performs computation off-chain significantly lowers on-chain expenses. Case studies of comparable hybrid systems, such as those employing off-chain ZKPs and coordinators, have shown over 90% reductions in gas costs and end-to-end latency of about 3 seconds compared to entirely on-chain systems.

The L-ABE-BC architecture is characterized by this explicit separation of concerns, as summarized in Table 2.

**Table 2: L-ABE-BC Hybrid On-Chain vs. Off-Chain Data Management**

| Data / System Component | Storage/Execution Location | Technology Used | Rationale |
|---|---|---|---|
| Entity Identities (DIDs) | On-Chain | Hyperledger Fabric Ledger | Decentralized, immutable trust anchor for all entities. |
| Attribute Issuers (DIDs/Keys) | On-Chain | Fabric Smart Contract (VDR) | Publicly verifiable and auditable list of trusted issuers. |
| Attributes (VCs) | Off-Chain | User's Digital Wallet (e.g., mobile) | Ensures user-centric control, privacy, and sovereignty. |
| Attribute Revocation List | On-Chain | Fabric "Status List 2020" Smart Contract | Enables efficient, cheap, $O(1)$ real-time revocation. |
| A-IoT Data (Logs, V2X, etc.) | Off-Chain | Cloud / Edge Storage / Vehicle Storage | Solves storage/scalability; data is far too large for any ledger |
| ABE Encryption | Off-Chain | Vehicle ECU (using PF-ABE) | Data is encrypted at the source before storage or transmission. |
| ABE Decryption (Heavy Task) | Off-Chain | Proxy (DCU / RSU) | Offloads 99%+ of computation from constrained devices. |
| ABE Decryption (Final Task) | Off-Chain | Constrained ECU | Final step is a single, lightweight $O(1)$ operation. |

### *4.3. Goal Achievement: Secure & Dynamic Revocation (Challenge 3)*

- Metric: Revocation cost and system overhead.
- Analysis: The L-ABE-BC system fundamentally changes the revocation paradigm.
- Traditional (Failed) Model: Revocation requires either re-keying all $N$ non-revoked users or re-encrypting all $M$ accessible ciphertexts. The resulting overhead is proportional to $O(N)$ or $O(M)$ and is operationally infeasible.
- L-ABE-BC Model: Revocation involves a single blockchain transaction to update the "Status List" smart contract, with an overhead of $O(1)$. This process is immediate, auditable, and does not affect other users.

This architecture achieves its primary security goals:

- Decentralized Trust: The centralized AA acting as a single point of failure is removed and substituted with a consortium of trusted, independent issuers such as OEMs and DMVs etc.).
- Key Escrow Freeness: Using a multi-authority model and a secure key-issuance protocol ensures that no single authority, including the OEM, possesses all the keys needed to decrypt a multi-authority policy (e.g., "Role: Technician" AND "License: DMV"). This approach addresses the key-escrow issue common in simpler systems schemes.
- Auditability: All issuances and revocations of attributes are permanently and transparently recorded on the blockchain, ensuring a complete audit trail for compliance and incident tracking response.

## 5. Conclusion

This paper tackles three main challenges in securing the A-IoT data ecosystem: (1) the computational limitations of standard CP-ABE on constrained automotive ECUs, (2) the performance and scalability issues when using public blockchains in real-time systems, and (3) the security concerns and overhead associated with dynamic attribute revocation. The proposed L-ABE-BC architecture offers a comprehensive, integrated solution by combining three advanced approaches technologies.

- It addresses the computational challenge by employing a Pairing-Free (ECC) CP-ABE scheme along with Outsourced Decryption. This minimizes the cryptographic burden on a resource-limited ECU to a single, lightweight, constant-time operation.
- It addresses the systems challenge by using a Hybrid, On-Chain/Off-Chain approach based on a Permissioned Blockchain (such as Hyperledger Fabric). This offers the high throughput, low latency, and cost-free trust layer needed for a real-time industrial IoT system.
- It addresses the revocation challenge by combining DIDs and VCs with a blockchain-based "Status List" smart contract. This allows for instant, auditable, and $O(1)$ attribute revocation without expensive re-encryption or mass updates re-keying.

The Lightweight Attribute-Based Encryption for Broadcast Cryptography (L-ABE-BC) system design shows that a sophisticated, detailed, and decentralized access control model is both feasible and practical for resource-limited A-IoT environments. It offers a secure, scalable, and auditable framework that balances the demands of privacy, security, and functionality, supporting the next wave of secure, multi-stakeholder data sharing within connected systems vehicles.

## References

[1] S. Jadhav and D. Kshirsagar, "A Survey on Security in Automotive Networks," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-6, doi: 10.1109/ICCUBEA.2018.8697772.

[2] V. Rishiwal, U. Agarwal, A. Alotaibi, S. Tanwar, P. Yadav and M. Yadav, "Exploring Secure V2X Communication Networks for Human-Centric Security and Privacy in Smart Cities," in IEEE Access, vol. 12, pp. 138763-138788, 2024, doi: 10.1109/ACCESS.2024.3467002.

[3] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," 2007 IEEE Symposium on Security and Privacy (SP '07), Berkeley, CA, USA, 2007, pp. 321-334, doi: 10.1109/SP.2007.11.

[4] K. Sowjanya, M. Dasgupta, and S. Ray, "A lightweight key management scheme for key-escrow-free ECC-based CP-ABE for IoT healthcare systems," Journal of Systems Architecture, vol. 117, p. 102108, 2021. doi: 10.1016/j.sysarc.2021.102108.

[5] Y.-F. Tseng, "Cryptanalysis to Sowjanya et al.'s ABEs from ECC," in Proceedings of the International Conference on Advanced Information Networking and Applications, 2022. doi: 10.1007/978-3-031-05491-4_29

[6] U. Waheed, S. A. Khan, M. Masud, H. Jamshed, T. A. Jumani, and N. U. Rehman Malik, "Blockchain-Based, Dynamic Attribute-Based Access Control for Smart Home Energy Systems," Energies, vol. 18, no. 8, Apr. 2025. doi: 10.3390/en18081973

[7] R. Singh, D. Kukreja, and D. K. Sharma, "Blockchain-enabled access control to prevent cyber attacks in IoT: Systematic literature review," Frontiers in Big Data, vol. 5, p. 1081770, 2023. doi: 10.3389/fdata.2022.1081770

[8] B. Xie, P. Zhou, Y. Yi, and Y. Wang, "An Improved Multi-Authority Attribute Access Control Scheme Base on Blockchain and Elliptic Curve for Efficient and Secure Data Sharing," Electronics, vol. 12, no. 7, 2023. doi: 10.3390/electronics12071691

[9] C. Zhang, Z. Wang, L. Liu, G. Li, and H. Li, "A Decentralized Multi-authority Attribute-based Encryption Scheme via Blockchain for Smart Grid," in 2023 IEEE International Conference on Electrical, Automation and Computer Engineering (ICEACE), Changchun, China, 2023, pp. 269–274. doi: 10.1109/ICEACE60673.2023.10442268.

[10] E. Abdulrahman, S. Alshehri, A. Alzubaidy, and A. Cherif, "A Distributed Blockchain-based Access Control for the Internet of Things," arXiv preprint arXiv:2503.17873, Mar. 2025. [Online]. Available: https://arxiv.org/abs/2503.17873

[11] I. Bolychevsky, "Verifiable Credentials and Decentralised Identifiers: Technical Landscape," GS1, White Paper, Feb. 03, 2025. [Online]. Available: https://ref.gs1.org/docs/2025/VCs-and-DIDs-tech-landscape

[12] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, "A Survey on Decentralized Identifiers and Verifiable Credentials," IEEE Communications Surveys & Tutorials, 2025. doi: 10.1109/COMST.2025.3543197.
[13] M. Bany Taha, C. Talhi, and H. Ould-Slimane, "Performance Evaluation of CP-ABE Schemes under Constrained Devices," Procedia Computer Science, vol. 155, pp. 425–432, 2019. doi: 10.1016/j.procs.2019.08.059.
[14] M. Sporny, D. Longley, and M. Sabadello, Eds., "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, Jul. 2022. [Online]. Available: https://www.w3.org/TR/did-core/
[15] M. Sporny, G. Cohen, and D. Longley, Eds., "Verifiable Credentials Data Model v1.1," W3C Recommendation, Mar. 2022. [Online]. Available: https://www.w3.org/TR/vc-data-model/
[16] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology–EUROCRYPT 2005 (LNCS 3494), R. Cramer, Ed. Berlin, Heidelberg: Springer, 2005, pp. 457–473. doi: 10.1007/11426639_27.
[17] S. Ding, C. Li, and H. Li, "A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT," IEEE Access, vol. 6, pp. 27336–27345, 2018. doi: 10.1109/ACCESS.2018.2836350
[18] X. Yao, Z. Chen, and W. Tian, "A lightweight attribute-based encryption scheme for the internet of things," Future Generation Computer Systems, vol. 49, pp. 104–112, Aug. 2015. doi: 10.1016/j.future.2014.10.010
[19] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in Proceedings of the 20th USENIX Security Symposium, San Francisco, CA, USA, Aug. 2011. [Online]. Available: https://www.usenix.org/conference/usenixsecurity11/outsourcing-decryption-abe-ciphertexts
[20] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, Nov. 2018. doi: 10.1016/j.future.2018.05.046.