Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 1 (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Attribute-Based Encryption for Secure Data Sharing in IOT Ecosystems

Sudhanshu Shekhar[1], Dr. Arvind Kumar Shukla[2]

[1]Research Scholar, School of Computer Science & Applications, IFTM University, Moradabad-244102, U.P., India
Email ID: shekharsystem2011@gmail.com

[2]Supervisor & Professor) School of Computer Science & Applications, IFTM University, Moradabad-244102, U.P., India
Email ID: arvindshukla@iftmuniversity.ac.in

Cite this paper as: Sudhanshu Shekhar, Dr. Arvind Kumar Shukla, (2025) Attribute-Based Encryption for Secure Data Sharing in IOT Ecosystems. *Journal of Neonatal Surgery*, 14 (1), 53-59.

ABSTRACT

The proliferation of Internet of Things (IoT) devices has led to unprecedented levels of data generation and sharing. However, ensuring data security and privacy in such dynamic and resource-constrained environments remains a critical challenge. Attribute-Based Encryption (ABE) has emerged as a promising cryptographic technique to enable fine-grained, flexible, and secure access control over shared data. This paper explores the applicability of ABE in IoT ecosystems, discussing its principles, architectures, advantages, and implementation challenges. Additionally, it reviews recent advances and outlines potential research directions to improve the performance and usability of ABE in IoT-based data-sharing scenarios.

Keywords: *Attribute-Based Encryption, IoT security, data sharing, access control, fine-grained encryption, privacy preservation.*

1. INTRODUCTION

The Internet of Things (IoT) envisions a world of interconnected devices that seamlessly share data and collaborate to improve various applications such as smart homes, healthcare, and industrial automation. However, the openness and heterogeneity of IoT systems expose them to significant security and privacy risks. Traditional access control mechanisms often struggle to cope with the scalability, resource constraints, and dynamic nature of IoT devices.

Attribute-Based Encryption (ABE) has emerged as a viable solution to address these challenges. Unlike conventional encryption schemes, ABE allows data owners to specify access policies based on user attributes, enabling more flexible and fine-grained access control. This paper delves into how ABE can be effectively leveraged to secure data sharing in IoT ecosystems.

The Internet of Things (IoT) represents a transformative technological paradigm that seamlessly integrates physical objects, sensors, and digital platforms to enable data-driven insights and smarter decision-making. As IoT continues to expand across domains such as healthcare, smart homes, transportation, and industrial automation, the volume and sensitivity of data generated and shared by these interconnected devices have grown exponentially.

However, the widespread adoption of IoT comes with significant challenges, particularly regarding data security and privacy. Traditional security mechanisms, including simple encryption and role-based access control models, often fall short in addressing the unique demands of IoT ecosystems. These demands include dynamic device join/leave behavior, fine-grained and flexible access control, and the resource-constrained nature of many IoT devices.

Attribute-Based Encryption (ABE) has emerged as a promising cryptographic approach to secure data sharing in IoT environments. Unlike conventional encryption schemes, ABE enables data owners to specify access policies based on descriptive attributes, ensuring that only authorized users or devices meeting the policy criteria can decrypt the data. This fine-grained access control paradigm aligns well with the dynamic and heterogeneous nature of IoT deployments.

This paper aims to explore the application of ABE in IoT-based data-sharing scenarios, highlighting its fundamental principles, advantages, and challenges. By analyzing the latest research advances and potential solutions to computational and management challenges, this work seeks to underscore ABE's viability as a foundation for secure and privacy-preserving IoT ecosystems.

2. OVERVIEW OF ATTRIBUTE-BASED ENCRYPTION

Attribute-Based Encryption (ABE) is an advanced public-key encryption scheme that extends traditional encryption models by introducing descriptive attributes and access policies. Unlike classical public-key cryptosystems that rely on user identities or roles, ABE enables access control decisions to be made based on sets of attributes, offering a more expressive and fine-grained control mechanism.

2.1. Fundamental Concepts

At its core, ABE associates cryptographic keys and ciphertexts with attributes and policies:

- **Attributes:** These are descriptive pieces of information that define user identities or device capabilities. Attributes could include device type (e.g., sensor, actuator), user roles (e.g., doctor, nurse), or contextual parameters (e.g., location, time).
- **Access Policy:** This defines the logical conditions that must be met for a user or device to decrypt the ciphertext. Policies are typically represented as Boolean formulas (e.g., "Role: Doctor AND Department: Cardiology").

2.2. Types of ABE

Two principal forms of ABE exist, each with a distinct approach to defining access policies:

- **Key-Policy Attribute-Based Encryption (KP-ABE):** In KP-ABE, the data is encrypted with a set of attributes, while the access policy is embedded within the user's decryption key. A user can decrypt the data only if the attributes associated with the ciphertext satisfy the access policy in the key.
- **Ciphertext-Policy Attribute-Based Encryption (CP-ABE):** In CP-ABE, the access policy is embedded within the ciphertext, while the user's decryption key is associated with a set of attributes. A user can decrypt the data only if their attributes satisfy the access policy specified in the ciphertext.

The distinction between KP-ABE and CP-ABE is critical in selecting the appropriate scheme for IoT applications, depending on whether the data owner or the user defines the access control.

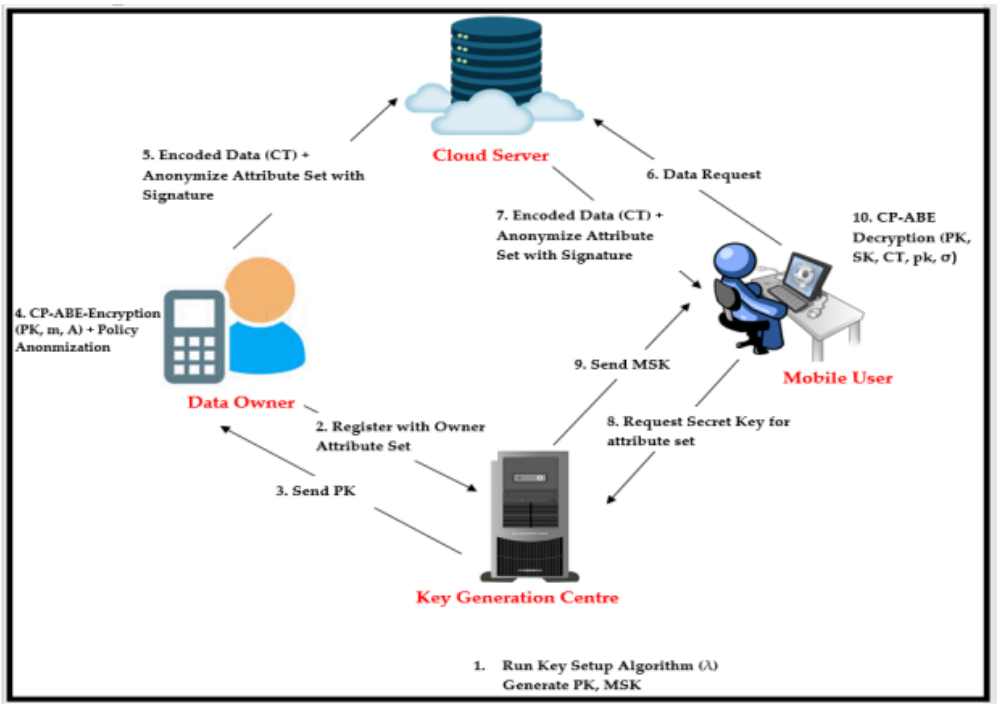

Figure 1 A system model of our proposed CP-ABE scheme

2.3. Advantages of ABE in IoT

ABE offers several significant advantages that align with the unique needs of IoT environments:

- **Fine-Grained Access Control:** Data owners can define detailed policies that govern who can access the data based on a combination of attributes.

- **Scalability and Flexibility:** ABE allows access policies to evolve and accommodate the dynamic nature of IoT devices and users.
- **Reduced Dependence on Central Authorities:** Unlike traditional models that rely heavily on central servers for access control, ABE distributes decision-making to the cryptographic layer, enhancing resilience and decentralization.

2.4. Cryptographic Foundations

ABE is typically built upon bilinear pairings and group theory, leveraging mathematical constructs such as elliptic curve cryptography for secure and efficient encryption and decryption processes. These cryptographic foundations ensure strong security guarantees while supporting the flexibility of attribute-based policies.

3. IOT ECOSYSTEM AND DATA SHARING CHALLENGES

The Internet of Things (IoT) represents a complex ecosystem composed of a vast array of interconnected devices—ranging from sensors and actuators to smart appliances and industrial machines. These devices continuously generate, process, and exchange data to support innovative services and applications. While the integration of these devices brings immense benefits, it also introduces significant challenges, especially in the context of data sharing and security.

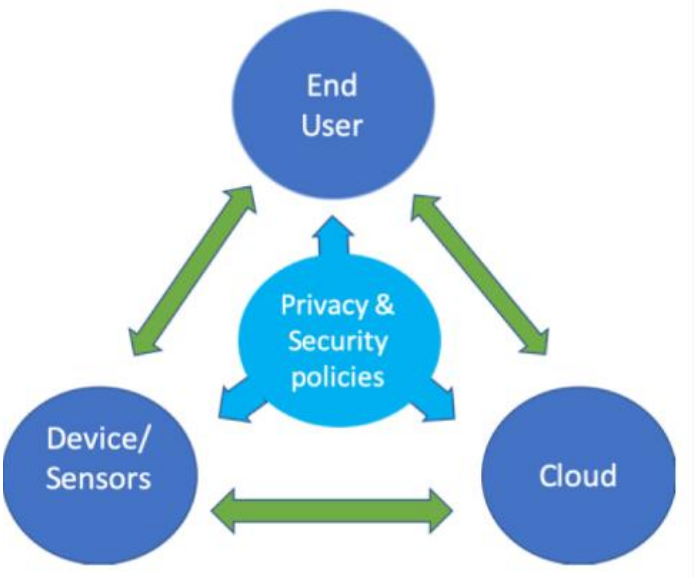

Figure 2 Internet of Things (IoT) generic model with privacy and security policies.

3.1. Characteristics of the IoT Ecosystem

Key features of the IoT ecosystem include:

- **Heterogeneity:** IoT devices vary widely in terms of hardware capabilities, communication protocols, and operating environments. This diversity complicates the design of a uniform security solution.
- **Resource Constraints:** Many IoT devices are constrained in terms of computation, memory, and power. These limitations impact the feasibility of deploying traditional security and cryptographic mechanisms.
- **Dynamic Topology:** IoT networks are inherently dynamic, with devices frequently joining, leaving, or moving within the network. Ensuring secure data sharing in such a fluid environment is challenging.
- **Data Sensitivity:** IoT devices often handle sensitive and private information, such as health data, personal preferences, or industrial process details, making data security paramount.

3.2. Data Sharing in IoT

Data sharing is fundamental to realizing the full potential of IoT. Examples include:

- **Smart Homes:** Data from smart thermostats and lighting systems is shared to optimize energy consumption.
- **Healthcare:** Wearable devices collect and share health-related data with healthcare providers for personalized treatment.

- **Industrial IoT (IIoT):** Sensors and control systems in smart factories share data to improve efficiency and reduce downtime.

While data sharing enhances operational efficiency and enables real-time decision-making, it also exposes sensitive data to risks if not properly secured.

3.3. Security and Privacy Challenges

Key challenges related to secure data sharing in IoT environments include:

- **Fine-Grained Access Control:** Traditional role-based or identity-based access control mechanisms are too rigid for the dynamic and context-aware nature of IoT applications.
- **Scalability:** With billions of connected devices, traditional centralized security models struggle to scale effectively and efficiently.
- **Trust Management:** Establishing trust between heterogeneous and autonomous IoT devices is complex, especially in open or partially trusted environments.
- **Data Confidentiality and Integrity:** Ensuring that data remains confidential and unaltered during transmission and storage is critical.
- **Efficient Key Management:** Secure distribution, storage, and revocation of cryptographic keys in dynamic IoT environments is challenging, particularly considering constrained device capabilities.

3.4. The Need for Advanced Cryptographic Solutions

Given these challenges, there is a clear need for advanced cryptographic techniques that can provide:

- **Flexible and Fine-Grained Access Control:** To allow only authorized users or devices to access specific data based on contextual attributes.
- **Low Computational Overhead:** To accommodate resource-constrained IoT devices without compromising performance.
- **Decentralized Security Mechanisms:** To reduce reliance on centralized authorities and enhance resilience against attacks.

Attribute-Based Encryption (ABE) has emerged as a promising solution that addresses many of these challenges by enabling flexible, scalable, and fine-grained access control suitable for dynamic IoT ecosystems.

4. ABE FOR SECURE DATA SHARING IN IOT

Aspect	Details
Definition	A cryptographic scheme that grants access to data based on user attributes rather than identities.
Purpose in IoT	Ensures secure data sharing among heterogeneous IoT devices with fine-grained access control.
Types of ABE	- **Key-Policy ABE (KP-ABE):** Access policies embedded in user keys; data encrypted with attributes. - **Ciphertext-Policy ABE (CP-ABE):** Access policies embedded in ciphertext; users hold attribute-based keys.
Key Features	- Fine-grained access control - Scalability for large IoT networks - Privacy-preserving data sharing - Reduced reliance on centralized servers
Security Goals	- Confidentiality: Unauthorized users cannot access data. - Integrity: Data remains untampered. - Access Control: Policies enforce who can decrypt data.
Advantages for IoT	- Supports dynamic user attributes

	- Efficient for resource-constrained devices - Enables multi-user collaboration without sharing keys directly
Challenges	- Computational overhead on IoT devices - Key management complexity - Revocation of user access can be difficult - Large-scale deployment may affect latency
Use Cases in IoT	- Smart healthcare: Protect patient records. - Smart cities: Secure sensor data sharing. - Industrial IoT: Control access to sensitive machine data. - Smart homes: Enforce selective device access.
Popular Implementations	- CP-ABE libraries: Charm, libfenc -KP-ABE frameworks: Java-based implementations for IoT gateway

4.1. How ABE Works in IoT

- Data owners encrypt data using an access policy expressed in terms of attributes.
- Only users whose attributes satisfy the policy can decrypt the data.
- This ensures that data is shared securely without constant involvement of the data owner.

4.2. Advantages

- **Fine-Grained Access Control:** Access can be controlled based on detailed attributes.
- **Scalability:** Suits the dynamic and expanding nature of IoT networks.
- **Privacy Preservation:** Reduces reliance on central authorities for access decisions.

5. IMPLEMENTATION CONSIDERATIONS AND CHALLENGES

5.1. Computational Overhead

IoT devices are resource-constrained, and ABE schemes can be computationally intensive.

5.2. Key Management

Secure and efficient key distribution and revocation are crucial for maintaining system security.

5.3. Policy Updating

IoT environments are dynamic, so attribute and policy updates need to be efficiently supported.

5.4. Lightweight ABE Variants

Recent research focuses on lightweight ABE schemes tailored for IoT (e.g., outsourced ABE decryption and hybrid cryptographic solutions).

6. RECENT ADVANCES AND RESEARCH DIRECTIONS

Recent research has focused on refining Attribute-Based Encryption (ABE) to better align with the unique constraints and requirements of IoT ecosystems. One notable advance is the development of outsourced ABE decryption, which offloads the computationally intensive parts of the decryption process to more powerful, semi-trusted servers or cloud platforms. This approach significantly reduces the computational burden on resource-constrained IoT devices, making ABE more practical in real-world applications.

Another important research direction is efficient attribute and key revocation. Since IoT environments are highly dynamic, attributes and access policies frequently change. Traditional ABE schemes struggle with timely and efficient revocation, which can compromise data security. Recent studies propose dynamic revocation techniques that leverage proxy re-encryption or update-friendly key management approaches, ensuring that revoked users or devices can no longer access sensitive data.

Efforts are also underway to design lightweight ABE schemes tailored for IoT. These schemes focus on optimizing

cryptographic operations, reducing ciphertext and key sizes, and simplifying attribute representations to fit within the limited processing and memory capacities of IoT devices. Techniques such as hybrid cryptographic systems that combine symmetric and asymmetric encryption have shown promise in maintaining security while minimizing computational costs.

Additionally, the integration of ABE with blockchain technology has gained significant interest. Blockchain's decentralized and tamper-evident ledger can provide robust and transparent attribute and policy management, enhancing trustworthiness and auditability in IoT data-sharing scenarios. Combining blockchain with ABE also helps address the single point of failure problem inherent in centralized key management models.

Finally, researchers are exploring context-aware ABE schemes that consider dynamic environmental factors—such as device location, time, or usage context—in access control decisions. Such context-aware adaptations align well with the fluid and adaptive nature of IoT ecosystems, allowing for more responsive and secure data sharing.

In summary, these recent advances highlight a concerted effort to bridge the gap between the theoretical strengths of ABE and the practical realities of IoT environments. Ongoing research in these areas is crucial to realizing secure, efficient, and scalable data sharing in the evolving landscape of the Internet of Things.

7. CONCLUSION

As the Internet of Things (IoT) continues to expand and evolve, ensuring secure and flexible data sharing has become a critical concern. Traditional access control and encryption methods often fall short in meeting the demands of dynamic, heterogeneous, and resource-constrained IoT environments. Attribute-Based Encryption (ABE) emerges as a promising solution, offering fine-grained, policy-driven access control that aligns well with the complex and evolving landscape of IoT systems.

This paper has explored the core principles and advantages of ABE, its suitability for IoT ecosystems, and the significant challenges that must be addressed for successful deployment. In particular, ABE's ability to provide scalable, attribute-driven access control makes it highly suitable for diverse IoT applications ranging from smart homes to industrial automation.

Nevertheless, realizing the full potential of ABE in IoT requires overcoming implementation challenges such as computational overhead, efficient key management, and dynamic policy updates. Recent advances—including outsourced decryption, lightweight ABE schemes, and blockchain integration—demonstrate the significant progress being made in this domain. These innovations aim to tailor ABE to the specific needs of IoT devices and networks, paving the way for more practical and robust security solutions.

In conclusion, ABE represents a significant step forward in securing data sharing within IoT ecosystems. Future research and development efforts should focus on further optimizing these schemes to balance security, scalability, and efficiency, ensuring that the benefits of IoT can be realized without compromising privacy or data integrity.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in Advances in Cryptology – EUROCRYPT 2005, Berlin, Germany: Springer, 2005, pp. 457–473.

[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2007, pp. 321–334.

[3] H. Li, Y. Dai, D. Tian, and C. Yu, "Achieving Secure and Efficient Dynamic Access Control in IoT Using Attribute-Based Encryption," IEEE Internet of Things Journal, vol. 4, no. 3, pp. 879–889, Jun. 2017.

[4] S. Yu, K. Ren, and W. Lou, "Attribute-Based Data Sharing with Attribute Revocation," in Proceedings of the 2010 ACM Conference on Computer and Communications Security (CCS), Chicago, IL, USA, 2010, pp. 261–270.

[5] T. Zhou, L. Yu, X. Chen, and Y. Zhang, "Blockchain-Based Secure Data Sharing in IoT with Attribute-Based Encryption," IEEE Access, vol. 7, pp. 117904–117917, 2019.

[6] M. Ambrosin, M. Conti, G. Dini, and R. T. Iacono, "On the Feasibility of Attribute-Based Encryption on IoT Devices," in Proceedings of the 2015 ACM Symposium on Information, Computer and Communications Security, Singapore, 2015, pp. 846–851.

[7] X. Liang, X. Li, T. H. Luan, R. Lu, X. Lin, and X. Shen, "Morality-Driven Data Forwarding with Privacy Preservation in Mobile Social Networks," IEEE Transactions on Vehicular Technology, vol. 61, no. 7, pp. 3209–3220, Sep. 2012.

[8] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-Based Access Control for Smart Grids," in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia, 2009, pp. 1–9.

[9] M. Joye and B. Libert, “A Scalable and Efficient Cryptographic Construction for Privacy-Preserving Data Sharing in Cloud Computing,” IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 468–480, Jul.–Sep. 2017.

[10] J. Hur and D. K. Noh, “Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221, Jul. 2011.