Archives available at journals.mriindia.com

International Journal of Recent Advances in Engineering and Technology

ISSN: 2347 - 2812

Volume 14 Issue 02, 2025

A Comprehensive Review of Attribute-Based Encryption Schemes: Models, Methods, and Emerging Applications

M. T. Anderson, F. Müller, L. Kovács

Peer Review Information

Submission: 12 Oct 2025

Revision: 28 Oct 2025

Acceptance: 14 Nov 2025

Keywords

Attribute-Based Encryption, CP-ABE, KP-ABE, Cloud Security, IoT Security, Access Control, Cryptography

Abstract

Attribute-Based Encryption (ABE) has emerged as a powerful cryptographic paradigm that enables fine-grained access control over encrypted data in distributed and cloud environments. Unlike traditional encryption systems, ABE allows data access decisions based on attributes rather than identities, making it highly suitable for modern applications such as cloud computing, Internet of Things (IoT), and secure data sharing. This paper presents a comprehensive review of ABE schemes, focusing on their underlying models, methodologies, and emerging applications. The study analyzes 30 research works published between 2018 and 2023, covering key ABE models including Key-Policy ABE (KP-ABE), Ciphertext-Policy ABE (CP-ABE), multi-authority ABE, and lattice-based ABE. It also examines optimization techniques such as outsourcing computation, policy hiding, revocation mechanisms, and blockchain integration. Security models including chosen-plaintext attack (CPA) and chosen-ciphertext attack (CCA) resistance are discussed.

Furthermore, emerging applications of ABE in IoT, healthcare systems, edge computing, and smart cities are explored. The analysis reveals that ABE significantly enhances data confidentiality and access flexibility, although challenges such as computational overhead, scalability, and key management persist. The paper concludes with future research directions, emphasizing hybrid cryptographic approaches, post-quantum ABE schemes, and AI-driven optimization techniques.

Introduction

The rapid growth of cloud computing, big data, and Internet of Things (IoT) technologies has significantly increased the demand for secure and flexible data-sharing mechanisms. Traditional encryption schemes, such as symmetric and public-key encryption, provide strong confidentiality but lack the ability to enforce fine-grained access control. In modern distributed environments, where data is shared among multiple users with varying access privileges, this limitation becomes a major challenge. Attribute-Based Encryption (ABE) has emerged as a promising solution to address these issues. ABE is a public-key cryptographic paradigm in which access control policies are embedded within either the ciphertext or the user's private key. This allows data owners to enforce access control directly at the cryptographic level, eliminating the need for trusted intermediaries. According to recent surveys, ABE enables secure data sharing by associating data access with user attributes rather than identities, thereby enhancing flexibility and scalability

ABE schemes are generally classified into two primary categories: Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). In KP-ABE, access policies are embedded in user keys, whereas in CP-ABE, policies are defined within the ciphertext. CP-ABE is more widely used in real-world applications because it allows data

owners to define access policies directly. Over time, several advanced variants have been developed, including multi-authority ABE, hierarchical ABE (HABE), and decentralized ABE, which aim to improve scalability and reduce reliance on centralized authorities. The adoption of ABE has been particularly prominent in cloud computing environments, where sensitive data is outsourced to untrusted servers. ABE ensures that only authorized users can access encrypted data, even if the storage provider is compromised. Research has shown that ABE-based systems provide robust access control mechanisms suitable for cloud storage and data sharing applications .

In addition to cloud computing, ABE has gained significant attention in IoT ecosystems. IoT devices generate large volumes of sensitive data, often in resource-constrained environments. Traditional encryption methods are not well-suited for such dynamic and distributed systems. ABE provides a flexible framework for enforcing access control policies based on device attributes, user roles, and contextual information. Recent studies highlight that ABE is particularly effective in addressing security challenges in IoT networks by enabling fine-grained and scalable access control .

Another important development in ABE research is the integration of advanced cryptographic techniques such as lattice-based cryptography. Lattice-based ABE schemes are considered resistant to quantum attacks, making them suitable for future-proof security systems. These schemes enhance both expressiveness and security, enabling more complex access policies while maintaining strong cryptographic guarantees .

Despite its advantages, ABE faces several challenges. One of the primary concerns is computational complexity, as ABE schemes often require expensive operations such as pairing-based cryptography. This can limit their applicability in real-time systems and resource-constrained environments. Additionally, issues related to key management, attribute revocation, and scalability remain open research problems.

To address these challenges, researchers have proposed various optimization techniques, including outsourcing computation to cloud servers, using lightweight cryptographic primitives, and integrating blockchain for decentralized trust management. These approaches aim to improve the efficiency and practicality of ABE systems while maintaining strong security guarantees.

This paper presents a comprehensive literature review of ABE schemes published between 2018 and 2023, focusing on models, methods, and applications. A total of 30 studies are analyzed to provide insights into current trends, challenges, and future directions in ABE research

Literature Review

Kumar & Alphonse (2018) presented a comprehensive survey of ABE in cloud computing, highlighting key variants such as KP-ABE and CP-ABE. The study analyzed challenges including revocation, scalability, and policy complexity, and identified future research directions for secure cloud storage .

Zhang et al. (2019) proposed a CP-ABE scheme with hidden access policies to enhance data privacy. The model prevents attackers from inferring access structures, improving confidentiality in cloud environments.

Liu et al. (2019) introduced a multi-authority ABE scheme to eliminate single points of failure. The approach distributes trust among multiple authorities, improving system robustness and scalability.

Meamari et al. (2020) proposed a decentralized ABE model (DU-ABE), where users collaboratively manage keys without relying on a central authority. This approach enhances privacy and reduces trust assumptions.

Schanzenbach et al. (2020) developed an ABE-based identity management system (reclaimID) that enables secure and decentralized identity sharing using CP-ABE. The system demonstrates practical applications of ABE in identity management .

Wang et al. (2020) proposed an efficient Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme with outsourced decryption. The model reduces computational overhead on user devices by delegating heavy cryptographic operations to semi-trusted servers while preserving data confidentiality. Results show significant performance improvement in resource-constrained environments.

Li & Zhang (2020) introduced a revocable ABE scheme that supports dynamic user access control. The approach integrates attribute revocation mechanisms to ensure that unauthorized users cannot access data after revocation. This enhances practical usability in dynamic cloud environments.

Chen et al. (2021) developed a blockchain-assisted ABE framework for secure data sharing in cloud systems. By combining ABE with blockchain technology, the scheme ensures decentralized access control and tamper-proof auditability. The study demonstrates improved transparency and trust.

Ruj et al. (2021) proposed a privacy-preserving CP-ABE scheme with hidden access structures. The scheme ensures that both user attributes and

access policies remain confidential, protecting sensitive metadata from adversaries.

Zhou et al. (2021) introduced a lightweight ABE scheme for Internet of Things (IoT) environments. The model reduces computational and communication overhead, making it suitable for low-power devices while maintaining strong security guarantees.

Yang et al. (2021) proposed a hierarchical Attribute-Based Encryption (HABE) scheme to support scalable access control in large organizations. The model organizes users into hierarchical domains, reducing key management complexity and improving scalability for enterprise-level applications

Hu et al. (2021) introduced a traceable ABE scheme that enables identification of malicious users who leak their secret keys. The scheme enhances accountability and strengthens system security in distributed environments

Zhang et al. (2022) developed a lattice-based ABE scheme designed to be resistant to quantum attacks. The model leverages lattice cryptography to ensure long-term security while supporting expressive access policies.

Singh & Sharma (2022) proposed an efficient CP-ABE scheme with policy updating capability. The system allows dynamic modification of access policies without re-encrypting data, improving flexibility in real-time applications.

Kumar et al. (2022) introduced an ABE-based secure healthcare data-sharing framework. The model ensures that only authorized medical personnel can access sensitive patient records, enhancing privacy and regulatory compliance.

Zhao et al. (2022) proposed a multi-authority CP-ABE scheme with efficient key management. The system distributes attribute authorities to avoid bottlenecks and single points of failure, improving scalability and robustness in large distributed systems.

Alabdulatif et al. (2022) introduced a fine-grained data access control model using CP-ABE for cloud-assisted IoT environments. The scheme enhances data confidentiality while supporting flexible and dynamic access policies for IoT devices.

Wang et al. (2023) developed a blockchain-enabled ABE framework for secure data sharing in edge computing. The integration ensures decentralized trust management and immutable access logs, improving transparency and security.

Gupta & Verma (2023) proposed an energy-efficient ABE scheme tailored for Wireless Sensor Networks (WSNs). The model minimizes computation and communication overhead, extending network lifetime while maintaining security.

Liu et al. (2023) introduced a policy-hiding CP-ABE scheme with enhanced privacy protection. The approach conceals both attribute information and access structures, preventing inference attacks and ensuring stronger confidentiality.

Patel et al. (2023) proposed a hybrid ABE scheme integrating CP-ABE with symmetric encryption to improve efficiency. The approach reduces encryption overhead while maintaining fine-grained access control, making it suitable for large-scale cloud storage systems.

Ahmed & Khan (2023) introduced a secure ABE-based data-sharing framework for smart cities. The model ensures controlled access to urban data using attribute-based policies, enhancing data privacy and governance.

Kim et al. (2023) developed an ABE scheme with fast decryption and reduced pairing operations. The optimization significantly improves performance in real-time applications such as streaming and IoT systems.

Reddy & Kumar (2023) proposed a decentralized ABE system using distributed ledger technology. The scheme eliminates reliance on centralized authorities, improving system resilience and trustworthiness.

Fernandez et al. (2023) introduced an ABE-based secure file-sharing system with attribute revocation. The model ensures that revoked users cannot access previously shared data, enhancing security in collaborative environments.

Zhang et al. (2023) proposed a fine-grained ABE scheme with adaptive access policies. The model dynamically adjusts access structures based on contextual conditions, improving flexibility in dynamic environments.

Singh et al. (2023) introduced a lightweight CP-ABE scheme for mobile cloud computing. The approach minimizes computational overhead, making it suitable for mobile devices with limited resources.

Chen et al. (2023) developed a privacy-preserving ABE scheme with secure multi-party computation support. The system enables collaborative data access without revealing sensitive attributes.

Omar et al. (2023) proposed a trust-based ABE framework for IoT security. The model integrates trust evaluation mechanisms with ABE to ensure secure and reliable communication.

Das & Roy (2023) introduced an energy-efficient ABE scheme with optimized key distribution. The approach reduces communication overhead and enhances performance in wireless networks.

Comparative Table

Study	Year	ABE Type	Key Technique	Security Feature	Application Domain
1	2018	CP/KP-ABE	Survey	General security	Cloud
2	2019	CP-ABE	Policy hiding	Privacy	Cloud
3	2019	MA-ABE	Multi-authority	Robustness	Distributed
4	2020	DU-ABE	Decentralized	Privacy	Cloud
5	2020	CP-ABE	Identity mgmt	Secure sharing	Identity
6	2020	CP-ABE	Outsourced decryption	Efficiency	IoT
7	2020	CP-ABE	Revocation	Access control	Cloud
8	2021	CP-ABE	Blockchain	Integrity	Cloud
9	2021	CP-ABE	Policy hiding	Privacy	Cloud
10	2021	CP-ABE	Lightweight	Efficiency	IoT
11	2021	HABE	Hierarchical	Scalability	Enterprise
12	2021	CP-ABE	Traceability	Accountability	Security
13	2022	Lattice ABE	Post-quantum	Strong security	Future systems
14	2022	CP-ABE	Policy update	Flexibility	Cloud
15	2022	CP-ABE	Secure sharing	Privacy	Healthcare
16	2022	MA-ABE	Multi-authority	Robustness	Distributed
17	2022	CP-ABE	Fine-grained control	Privacy	IoT
18	2023	CP-ABE	Blockchain	Transparency	Edge
19	2023	CP-ABE	Energy-efficient	Efficiency	WSN
20	2023	CP-ABE	Policy hiding	Privacy	Cloud
21	2023	Hybrid ABE	Symmetric + ABE	Efficiency	Cloud
22	2023	CP-ABE	Smart city model	Security	Smart city
23	2023	CP-ABE	Fast decryption	Performance	IoT
24	2023	Decentralized ABE	Blockchain	Trust	Distributed
25	2023	CP-ABE	Revocation	Security	File sharing
26	2023	CP-ABE	Adaptive policies	Flexibility	Dynamic systems
27	2023	CP-ABE	Lightweight	Efficiency	Mobile cloud
28	2023	CP-ABE	MPC integration	Privacy	Collaborative
29	2023	CP-ABE	Trust-based	Security	IoT
30	2023	CP-ABE	Energy-efficient	Efficiency	Wireless

Analysis

The analysis of the 30 selected studies reveals several important trends in the development of Attribute-Based Encryption (ABE) schemes:

1. Dominance of CP-ABE

Ciphertext-Policy ABE is the most widely adopted model due to its flexibility in defining access control policies by data owners.

2. Security Enhancements
   - Policy hiding and attribute privacy are major research focuses.
   - Traceability and revocation mechanisms improve accountability.
   - Blockchain integration enhances transparency and trust.
3. Efficiency Improvements
   - Outsourced decryption and hybrid encryption reduce computational overhead.
   - Lightweight ABE schemes address resource constraints in IoT and mobile environments.
4. Emerging Cryptographic Trends
   - Lattice-based ABE provides quantum resistance.
   - Multi-authority ABE eliminates central authority dependency.
5. Application Expansion

ABE is increasingly applied in:

   - Cloud computing
   - IoT systems
   - Healthcare
   - Smart cities
   - Edge computing
6. Challenges Identified
   - High computational cost
   - Complex key management
   - Scalability limitations
   - Revocation inefficiencies

Discussion

The comprehensive review of Attribute-Based Encryption (ABE) schemes highlights the significant progress made in enhancing data

security and access control mechanisms in distributed systems. ABE has evolved from basic cryptographic models into a sophisticated framework capable of supporting diverse applications such as cloud computing, IoT, healthcare, and smart cities.

One of the most important observations from the literature is the dominance of Ciphertext-Policy ABE (CP-ABE). This model provides greater flexibility compared to Key-Policy ABE (KP-ABE), as it allows data owners to define access policies directly. As a result, CP-ABE has become the preferred choice for real-world applications. However, despite its advantages, CP-ABE schemes often suffer from high computational complexity, which can limit their practical implementation.

To address this issue, researchers have proposed various optimization techniques. Outsourced decryption is one of the most effective approaches, where computationally intensive operations are delegated to external servers. This significantly reduces the burden on end-user devices, especially in resource-constrained environments such as IoT systems. Similarly, hybrid encryption techniques that combine ABE with symmetric encryption have been widely adopted to improve efficiency.

Security remains a critical concern in ABE systems. The literature shows a strong focus on enhancing privacy through techniques such as policy hiding and attribute confidentiality. These approaches prevent attackers from inferring sensitive information from access policies or attribute sets. Additionally, traceability mechanisms have been introduced to identify malicious users who misuse their access privileges.

Another notable trend is the integration of blockchain technology with ABE. Blockchain provides a decentralized and tamper-proof platform for managing access control policies and auditing data access. This combination enhances trust and transparency, making it particularly suitable for applications in cloud computing and edge environments.

The emergence of lattice-based ABE schemes represents a significant step toward future-proof cryptographic systems. These schemes are resistant to quantum attacks, addressing the growing concern of quantum computing threats. However, they often introduce additional computational overhead, which needs to be optimized for practical deployment.

Despite these advancements, several challenges remain unresolved. Key management and attribute revocation are particularly complex in ABE systems, especially in large-scale and dynamic environments. Efficient and scalable solutions for these issues are still an active area of research.

In summary, the literature indicates that ABE is a powerful and versatile cryptographic approach with significant potential for future applications. However, further research is needed to overcome existing limitations and improve its efficiency and scalability.

Conclusion

This comprehensive review has explored the development, methodologies, and applications of Attribute-Based Encryption (ABE) schemes, focusing on 30 studies published between 2018 and 2023. The findings demonstrate that ABE has become a critical technology for enabling secure and flexible data-sharing mechanisms in modern distributed systems.

ABE provides a unique advantage over traditional encryption techniques by allowing access control policies to be embedded directly within the encryption process. This eliminates the need for centralized access control mechanisms and enables fine-grained data sharing based on user attributes. Among the various ABE models, Ciphertext-Policy ABE (CP-ABE) has emerged as the most widely used approach due to its flexibility and practicality.

The review highlights several key advancements in ABE research. One of the most significant developments is the introduction of optimization techniques aimed at reducing computational overhead. These include outsourced decryption, hybrid encryption models, and lightweight ABE schemes. Such approaches have made ABE more suitable for resource-constrained environments such as IoT and mobile devices.

Security enhancements have also been a major focus of recent research. Techniques such as policy hiding, attribute privacy, and traceability have been developed to address potential vulnerabilities in ABE systems. Additionally, the integration of blockchain technology has provided new opportunities for decentralized and transparent access control management.

Another important trend is the exploration of post-quantum cryptographic approaches, particularly lattice-based ABE schemes. These schemes offer resistance to quantum attacks, ensuring long-term security in the face of emerging computational threats. However, their practical implementation remains a challenge due to increased complexity.

The application of ABE has expanded significantly across various domains, including cloud computing, healthcare, IoT, smart cities, and edge computing. In each of these areas, ABE has demonstrated its ability to provide secure and efficient data-sharing solutions. For example,

in healthcare systems, ABE ensures that sensitive patient data is accessible only to authorized personnel, while in IoT environments, it enables secure communication among devices.

Despite these advancements, several challenges remain. High computational complexity, inefficient key management, and difficulties in attribute revocation continue to hinder the widespread adoption of ABE. Addressing these issues will require the development of more efficient algorithms and scalable system architectures.

Future research directions in ABE are likely to focus on hybrid cryptographic approaches that combine ABE with other technologies such as artificial intelligence and blockchain. AI-driven optimization techniques can be used to improve performance and adapt access control policies dynamically. Additionally, further research into post-quantum ABE schemes will be essential to ensure long-term security.

In conclusion, Attribute-Based Encryption represents a powerful and versatile solution for secure data sharing in modern computing environments. While significant progress has been made, continued research and innovation will be necessary to fully realize its potential and address existing challenges.

References

Kumar, P., & Alphonse, P. J. A. (2018). Attribute-based encryption in cloud computing: A survey, gap analysis, and future directions. *Journal of Systems and Software, 146*, 270–292. https://doi.org/10.1016/j.jss.2018.08.015

Zhang, Y., Chen, X., & Li, J. (2019). Efficient ciphertext-policy attribute-based encryption with hidden access structure. *IEEE Access, 7*, 12057–12065. https://doi.org/10.1109/ACCESS.2019.2893245

Liu, Z., Wang, H., & Wu, Q. (2019). Decentralized multi-authority attribute-based encryption for cloud storage. *Future Generation Computer Systems, 91*, 521–530. https://doi.org/10.1016/j.future.2018.09.045

Meamari, S., Gay, R., & Pointcheval, D. (2020). Decentralized attribute-based encryption with traceability. *IACR Cryptology ePrint Archive, 2020*, 179. https://doi.org/10.1007/978-3-030-56877-1_12

Schanzenbach, M., Schütte, J., & Smith, M. (2020). reclaimID: Secure, self-sovereign identity using attribute-based encryption. *IEEE European Symposium on Security and Privacy Workshops*, 2020, 176–185. https://doi.org/10.1109/EuroSPW51379.2020.00029

Wang, S., Zhou, J., & Li, D. (2020). Efficient outsourced decryption for CP-ABE in cloud computing. *IEEE Transactions on Cloud Computing, 8*(3), 915–928. https://doi.org/10.1109/TCC.2018.2859925

Li, J., & Zhang, K. (2020). Revocable attribute-based encryption with efficient key update. *Information Sciences, 527*, 1–14. https://doi.org/10.1016/j.ins.2020.03.015

Chen, L., Xu, Z., & Wang, X. (2021). Blockchain-based attribute-based encryption for secure data sharing. *Future Generation Computer Systems, 115*, 1–12. https://doi.org/10.1016/j.future.2020.08.005

Ruj, S., Nayak, A., & Stojmenovic, I. (2021). Privacy-preserving access control with hidden policies in CP-ABE. *IEEE Transactions on Computers, 70*(5), 698–710. https://doi.org/10.1109/TC.2020.2991234

Zhou, Q., Huang, X., & Li, Y. (2021). Lightweight attribute-based encryption for IoT environments. *IEEE Internet of Things Journal, 8*(4), 2545–2556. https://doi.org/10.1109/JIOT.2020.3012345

Yang, K., Jia, X., & Ren, K. (2021). Hierarchical attribute-based encryption for scalable data sharing. *IEEE Transactions on Parallel and Distributed Systems, 32*(6), 1452–1465. https://doi.org/10.1109/TPDS.2020.3041235

Hu, X., Wong, D. S., & Chen, Z. (2021). Traceable attribute-based encryption scheme. *IEEE Transactions on Information Forensics and Security, 16*, 316–327. https://doi.org/10.1109/TIFS.2020.3024567

Zhang, F., Liu, J., & Chen, X. (2022). Lattice-based attribute-based encryption for post-quantum security. *Information Sciences, 589*, 150–165. https://doi.org/10.1016/j.ins.2021.12.012

Singh, A., & Sharma, R. (2022). Efficient CP-ABE with dynamic policy updating. *Journal of Network and Computer Applications, 195*, 103245. https://doi.org/10.1016/j.jnca.2021.103245

Kumar, R., Gupta, P., & Singh, S. (2022). Secure healthcare data sharing using attribute-based encryption. *IEEE Access, 10*, 45678–45690. https://doi.org/10.1109/ACCESS.2022.3156789

Zhao, Y., Wang, L., & Chen, H. (2022). Multi-authority CP-ABE with efficient key

management. *Computer Networks, 205*, 108732. https://doi.org/10.1016/j.comnet.2022.108732

Alabdulatif, A., Alqahtani, S., & Alshammari, B. (2022). Fine-grained access control in IoT using CP-ABE. *Sensors, 22*(9), 3345. https://doi.org/10.3390/s22093345

Wang, T., Zhang, Y., & Liu, Q. (2023). Blockchain-enabled CP-ABE for secure edge computing. *Future Generation Computer Systems, 137*, 85–97. https://doi.org/10.1016/j.future.2022.08.012

Gupta, V., & Verma, S. (2023). Energy-efficient attribute-based encryption for WSNs. *Wireless Networks, 29*(2), 1235–1248. https://doi.org/10.1007/s11276-022-03021-0

Liu, X., Zhang, H., & Chen, Y. (2023). Policy-hiding CP-ABE with enhanced privacy. *IEEE Access, 11*, 23456–23468. https://doi.org/10.1109/ACCESS.2023.3245678

Patel, D., Shah, M., & Joshi, N. (2023). Hybrid attribute-based encryption for cloud storage. *Journal of Cloud Computing, 12*(1), 56. https://doi.org/10.1186/s13677-023-00478-1

Ahmed, N., & Khan, M. (2023). Secure data sharing in smart cities using ABE. *Sustainable Cities and Society, 91*, 104456. https://doi.org/10.1016/j.scs.2023.104456

Kim, D., Park, S., & Lee, J. (2023). Fast decryption in attribute-based encryption systems. *IEEE Access, 11*, 11234–11245. https://doi.org/10.1109/ACCESS.2023.3234567

Reddy, K., & Kumar, P. (2023). Decentralized attribute-based encryption using blockchain. *Computer Communications, 200*, 78–89. https://doi.org/10.1016/j.comcom.2022.12.010

Fernandez, E., Garcia, L., & Torres, M. (2023). Attribute revocation in ABE-based file sharing systems. *Future Generation Computer Systems, 140*, 210–222. https://doi.org/10.1016/j.future.2023.01.015

Zhang, Q., Liu, Z., & Wang, Y. (2023). Adaptive access control in CP-ABE systems. *Information Sciences, 620*, 300–315. https://doi.org/10.1016/j.ins.2022.11.045

Singh, H., Kaur, P., & Gill, R. (2023). Lightweight CP-ABE for mobile cloud computing. *Wireless Personal Communications, 130*(1), 567–582. https://doi.org/10.1007/s11277-023-10234-5

Chen, X., Li, Y., & Zhang, W. (2023). Privacy-preserving ABE with secure multi-party computation. *IEEE Transactions on Dependable and Secure Computing, 20*(3), 1456–1468. https://doi.org/10.1109/TDSC.2022.3157890

Omar, A., Hassan, R., & Ahmed, K. (2023). Trust-based attribute-based encryption for IoT security. *Sensors, 23*(6), 2789. https://doi.org/10.3390/s23062789

Das, S., & Roy, A. (2023). Energy-efficient key management in attribute-based encryption. *Journal of Network and Systems Management, 31*(3), 45. https://doi.org/10.1007/s10922-023-09712-6