**Journal of Convergence in Technology and Management: Global Nexus**

vol. 1, no. 1 (November, 2024) pp.1-18

# CONVERGENCE OF CRYPTOGRAPHY AND MANAGEMENT: EXPLORING ID-BASED AND ATTRIBUTE-BASED CRYPTOGRAPHY

**Malabika Das**

*Department of Mathematics, Heramba Chandra College, Kolkata, India*

**Dr. Rajdeep Chakraborty**

*Department of Computer Science and Engineering, Medi-Caps University, Indore, India*

## ABSTRACT

The advent of digital technologies has heightened the need for robust cryptographic solutions, necessitating the convergence of technical and managerial expertise. ID-based cryptography and attribute-based cryptography have emerged as vital alternatives to traditional public key cryptography, addressing key distribution and access control challenges. This paper provides an insightful exploration of these paradigms, examining their mechanisms, applications, advantages, and challenges.

We discuss the theoretical foundations of ID-based and attribute-based cryptography, including bilinear pairings and cryptographic primitives. Our analysis delves into the managerial implications of implementing these cryptographic solutions, considering factors such as scalability, security, and usability.

This study contributes to the understanding of cryptographic convergence, bridging the gap between technical and managerial perspectives. Our findings highlight the potential of ID-based and attribute-based cryptography in securing digital ecosystems, particularly in cloud computing, IoT, and big data environments.

***Keywords*****:** *ID-based cryptography, attribute-based cryptography, public key cryptography, bilinear pairings, encryption, identity, cryptographic convergence, digital security.*

# 1. INTRODUCTION

The convergence of cryptography and management has become imperative in today's digital landscape, where securing sensitive information and ensuring authorized access are paramount. Traditional public key cryptosystems rely on complex public key infrastructures (PKIs), necessitating trusted third-party certificate authorities **(Bubna & Jha, 1984)**. To address these limitations, Identity-Based Cryptography (IBC) and Attribute-Based Cryptography (ABC) have emerged as promising solutions **(Goyal *et al.* 2006, October; Anand, Khemchandani & Sharma, 2013, September)**.

In 1984, Shamir introduced IBC, leveraging users' identifier information as public keys, simplifying key management and reducing PKI complexities **(Baek *et al.* 2004, September)**. Constructing an identity-based encryption scheme was a challenging problem that remained unsolved until 2001. In that year, both Boneh and Franklin, as well as Cocks, independently found solutions to this issue. Their breakthroughs made significant contributions to the field of cryptography. These advancements paved the way for the development of practical identity-based encryption systems. As a result, the concept of identity-based encryption became a feasible and impactful solution in secure communication.

ABC offers a more flexible framework, enabling cryptographic keys to be generated based on user attributes rather than a single identity. This attribute-centric approach facilitates fine-grained access control and enhances privacy by allowing users to disclose only relevant attributes.

IBC and ABC have far-reaching implications for securing digital ecosystems, particularly in cloud computing, IoT, and big data environments. This paper provides a comprehensive review of IBC and ABC, comparing their underlying principles, strengths, and weaknesses. We explore their diverse applications across various sectors, highlighting how these cryptographic methods can enhance security in today's digital age.

The remainder of this paper is organized as follows:

**Section 2**: Technical Overview of IBC and ABC Algorithms

**Section 3**: Discussion on Applications, Merits, and Demerits of IBC and ABC, considering management applications and integration of cryptographic algorithms with management principles

**Section 4**: Key Findings based on content analysis and thematic analysis- Cross-Cutting Findings:

**Section 5**: Discussions in respect to investigation of IBC and ABC Applications in Emerging Technologies, further examination of security assumptions and vulnerability assessment and investigation of artificial intelligence and machine learning applications in IBC and ABC.

**Section 6**: Conclusion, and Future Directions

By examining the convergence of cryptography and management through IBC and ABC, this research aims to contribute to the development of robust and secure digital solutions.

## 2. TECHNICAL OVERVIEW OF IBC AND ABC ALGORITHMS

### 2.1 Identity-Based Cryptography (IBC)

IBC algorithms utilize users' identifier information as public keys **(Baek *et al.* 2004, September; Anand, Khemchandani & Sharma, 2013, September)**.

#### 2.1.1 Setup

The Private Key Generator (PKG) runs this algorithm once to create the IBE environment.

**Mathematically, this involves**:

- Choosing two cyclic groups, G1 and G2, of prime order q

- Selecting a generator g ∈ G1

- Defining a bilinear pairing e: G1 × G2 → GT

- Generating system parameters (G1, G2, e, g, n)

- Creating a master key (Km)

The master key is kept secret to derive user private keys, while system parameters are publicized.

**Clarification**: In IBC setup, the PKG generates system parameters and a master key, enabling efficient key management.

#### 2.1.2 Private Key Extraction

The PKG runs this algorithm when a user requests their private key.

**Mathematically, this involves**:

- Computing the user's private key d = Km × QID, where QID = H1(ID)

- Using the hash function H1: {0,1}* → G1

**Clarification**: Private key extraction involves computing the user's private key using the master key and the user's ID.

### 2.1.3 Encryption

This algorithm encrypts messages using the recipient's ID.

**Mathematically, this involves**:

- Computing ciphertext c = (rP, m × e(QID, Kpub)^r), where r ∈R Zq*

- Using the recipient's ID to compute QID = H1(ID)

**Clarification**: IBC encryption uses the recipient's ID to compute the ciphertext.

### 2.1.4 Decryption

This algorithm decrypts ciphertext using the private key **(Bethencourt, Sahai & Waters, 2007, May)**.

**Mathematically, this involves**:

- Computing plaintext m = c2 × e(dID, c1)^(-1), where c = (c1, c2)

- Using the private key dID to decrypt

**Clarification**: IBC decryption uses the private key to recover the plaintext.

## 2.2 Attribute-Based Cryptography (ABC)

ABC algorithms extend IBC by viewing user identities as sets of attributes **(Goyal *et al.* 2006, October; Das, Chakraborty & Banerjee, 2023)**.

### 2.2.1 Fuzzy Identity-Based Encryption (FIBE)

FIBE enables coarse-grained access control **(Sahai & Waters, (2005)**.

**Mathematically, this involves**:

- Defining a similarity metric between attribute sets

- Computing ciphertext c = (c1, c2), where c1 = rP and c2 = m × e(QID, Kpub)^r

**Clarification**: FIBE uses attribute similarity metrics for access control.

**2.2.2 Key-Policy Attribute-Based Encryption (KP-ABE)**

KP-ABE enables fine-grained access control **(Thakur, Ranga & Agarwal, 2024, February)**.

**Mathematically, this involves**:

- Defining an access structure (AS) as a Boolean formula

- Computing ciphertext c = (c1, c2), where c1 = rP and c2 = m × e(QID, Kpub)^r

**Clarification**: KP-ABE uses access structures for fine-grained access control.

**2.2.3 Ciphertext-Policy Attribute-Based Encryption (CP-ABE)**

CP-ABE introduces policy-based encryption.

**Mathematically, this involves**:

- Defining a policy (P) as a Boolean formula

- Computing ciphertext c = (c1, c2), where c1 = rP and c2 = m × e(QID, Kpub)^r

**Clarification**: CP-ABE uses policies for encryption.

**2.3 Integration with Management Principles**

*The integration of cryptographic algorithms with management principles enhances security, efficiency, and compliance. By aligning IBC and ABC with organizational policies, implementing robust identity and attribute management, and ensuring scalability, organizations can achieve robust security, streamlined operations, and effective access control. This convergence enables role-based access control, attribute-based access control, separation of duties, and least privilege principles, ultimately protecting sensitive information and ensuring authorized access.*

*Furthermore, integrating IBC and ABC with management principles facilitates:*

*- Automated key management and revocation*

*- Dynamic access control and policy updates*

*- Auditing and logging mechanisms*

- *Compliance with regulatory requirements*

*By leveraging these benefits, organizations can establish a secure, efficient, and compliant infrastructure for data protection and access control.*

# 3. DISCUSSION ON APPLICATIONS, MERITS, AND DEMERITS OF IBC AND ABC, CONSIDERING MANAGEMENT APPLICATIONS AND INTEGRATION OF CRYPTOGRAPHIC ALGORITHMS WITH MANAGEMENT PRINCIPLES

## 3.1 Applications of IBC and ABC in Management

**1. Secure Communication**: IBC enables secure email and messaging systems, ensuring confidentiality and authenticity. This is particularly important in management for sensitive information sharing. IBC-based secure communication prevents unauthorized access and protects against data breaches. Effective secure communication fosters trust among stakeholders. Management benefits from streamlined communication processes.

**2. Access Control**: ABC facilitates fine-grained access control in cloud storage, databases, and networks. Attribute-based policies ensure only authorized personnel access sensitive data **(Goyal *et al.* 2006, October)**. This prevents data breaches and unauthorized modifications. Management benefits from robust access control, ensuring compliance with regulatory requirements. ABC enables dynamic attribute updates, adapting to changing access needs.

**3. Identity Management**: IBC and ABC support robust identity management systems, verifying user identities. This prevents identity theft and impersonation. Management benefits from efficient identity verification, streamlining authentication processes. IBC and ABC enable secure identity management, protecting sensitive information **(Das, Chakraborty & Banerjee, 2023)**. Organizations ensure compliance with identity management regulations.

**4. Data Protection**: ABC ensures data confidentiality and integrity in data sharing and collaboration. Attribute-based encryption protects sensitive data from unauthorized access **(Goyal *et al.* 2006, October; Qiao *et al.* 2014, June)**. Management benefits from secure data sharing, enabling collaboration while maintaining data security. ABC facilitates secure data storage and transmission, preventing data breaches.

## 3.2 Merits of IBC and ABC in Management

### 3.2.1 IBC Merits

**1. Simplified Key Management**: IBC eliminates certificate requirements, streamlining key management. No certificate revocation or expiration issues arise. Management benefits from reduced key management complexity. IBC enables automated key generation and distribution.

**2. Automated Key Revocation**: IBC keys expire, eliminating revocation needs. This prevents compromised keys from being used. Management benefits from reduced key revocation complexity. IBC ensures secure key management.

**3. Postdating Messages**: IBC enables future decryption, allowing management to schedule message availability. This supports time-sensitive information sharing. IBC-based postdating ensures secure message transmission.

**4. Efficient Identity Verification**: IBC streamlines authentication, verifying user identities efficiently. Management benefits from reduced authentication complexity.

### 3.2.2 ABC Merits

**1. Fine-Grained Access Control**: ABC enables attribute-based policies, ensuring precise access control. Management benefits from robust access control.

**2. Scalable**: ABC suits large-scale systems, supporting numerous users and data objects. Management benefits from scalable and flexible access control.

**3. Flexible Attribute Management**: ABC enables dynamic attribute updates, adapting to changing access needs. Management benefits from efficient attribute management.

**4. Secure Data Sharing**: ABC facilitates secure data sharing, protecting sensitive information.

## 3.3 Demerits of IBC and ABC in Management

### 3.3.1 IBC Demerits

**1. Centralized Server Requirement**: IBC requires a centralized server, introducing single-point failure risks. Management must ensure server security.

**2. Secure Channel Needed**: IBC requires secure private key transmission channels. Management must establish trusted communication.

**3. Key Escrow**: Centralized key storage risks key compromise. Management must ensure secure key storage.

### 3.3.2 ABC Demerits

**1. Complexity**: ABC implementation and attribute structure can be challenging. Management must invest in expertise.

**2. Performance Overhead**: ABC introduces computational overhead. Management must balance security and performance.

**3. Attribute Revocation**: ABC attribute revocation can be complicated. Management must establish efficient revocation processes.

**4. Security Assumptions**: ABC relies on mathematical assumptions, potentially exposing vulnerabilities.

### 3.4 Integration of Cryptographic Algorithms with Management Principles

**Effective integration enhances**:

1. **Security**: Robust access control and data protection.

2. **Efficiency**: Streamlined key management and revocation.

3. **Compliance**: Adherence to regulatory requirements.

4. **Scalability**: Flexible attribute management.

**By converging cryptographic algorithms with management principles, organizations**:

1. Establish secure and compliant infrastructure.

2. Ensure data confidentiality and integrity.

3. Streamline access control and key management.

4. Support scalable and dynamic systems.

## 4. KEY FINDINGS- BASED ON CONTENT ANALYSIS AND RHEMATIC ANALYSIS - CROSS-CUTTING FINDINGS

Here are the key findings based on content analysis and thematic analysis:

### 4.1 Content Analysis Key Findings

1. IBC and ABC are crucial for secure communication, access control, identity management, and data protection.

2. IBC simplifies key management, automates key revocation, and enables postdating messages.

3. ABC facilitates fine-grained access control, scalable systems, flexible attribute management, and secure data sharing.

4. Challenges include centralized server requirements, secure channel needs, key escrow, complexity, performance overhead, attribute revocation, and security assumptions.

### 4.2 Thematic Analysis: Key Findings

**Theme 1: Security and Access Control**

- IBC and ABC ensure secure communication and data protection.

- Attribute-based policies enable fine-grained access control.

**Theme 2: Efficiency and Scalability**

- IBC simplifies key management and automates key revocation.

- ABC supports scalable systems and flexible attribute management.

**Theme 3: Compliance and Risk Management**

- IBC and ABC ensure compliance with regulatory requirements.

- Challenges include key escrow, complexity, and security assumptions.

**Theme 4: Management Applications**

- IBC and ABC support secure communication, access control, identity management, and data protection.

- Integration with management principles enhances security, efficiency, compliance, and scalability.

### 4.3 Cross-Cutting Findings

1. Integration of cryptographic algorithms with management principles is crucial.

2. Balancing security, efficiency, and scalability is essential.

3. Addressing challenges and limitations is vital for effective implementation.

### 4.4 Key Findings: Integration of IBC and ABC with Management Principles

**The integration of IBC and ABC with management principles yields several key benefits**:

- Enhanced security and compliance
- Streamlined key management and access control
- Improved scalability and flexibility
- Effective risk management and mitigation
- Alignment with organizational policies and objectives

### 4.5 Effective integration requires

- Alignment of cryptographic algorithms with management goals
- Implementation of robust identity and attribute management
- Continuous monitoring and evaluation of security assumptions
- Balancing security, efficiency, and scalability

*By converging IBC and ABC with management principles, organizations can establish a secure, efficient, and compliant infrastructure for data protection and access control.*

## 5. DISCUSSION

**I**nvestigation of IBC and ABC Applications in Emerging Technologies, further examination of security assumptions and vulnerability assessment and investigation of artificial intelligence and machine learning applications in IBC and ABC.

### 5.1 Investigation of IBC and ABC Applications in Emerging Technologies

The integration of Identity-Based Cryptography (IBC) and Attribute-Based Cryptography (ABC) with emerging technologies has the potential to revolutionize secure communication, access control, and data protection **(Baek *et al.* 2004, September; Anand, Khemchandani & Sharma, 2013, September)**. This study examines the use of IBC and ABC in emerging technologies like the Internet of Things (IoT), blockchain, and cloud computing. By exploring these applications, the investigation highlights how IBC and ABC can enhance the security and functionality of these technologies. The study also delves into the potential challenges and benefits of integrating these cryptographic approaches into IoT, blockchain, and cloud systems.

Understanding their role in these areas is essential for advancing secure and efficient solutions in the digital landscape. This research aims to provide insights into how IBC and ABC can support the growth and development of these technologies.

The Internet of Things (IoT) benefits from IBC and ABC through secure device authentication and communication, fine-grained access control for IoT devices, and scalable key management **(Feng *et al.* 2024)**. In blockchain, IBC and ABC enhance security and scalability for transaction verification, attribute-based access control for smart contracts, and decentralized identity management **(Ding *et al.* 2023)**. Cloud computing utilizes IBC and ABC for secure data storage and transmission, fine-grained access control for cloud resources, and scalable key management.

The integration of IBC and ABC with emerging technologies offers numerous benefits, including enhanced security and compliance, improved scalability and efficiency, simplified key management, and fine-grained access control. However, challenges arise from complexity and interoperability, performance overhead, and security assumptions and vulnerability assessment.

Future research should focus on optimizing IBC and ABC for IoT devices, investigating performance implications in blockchain, and ensuring secure data storage in cloud computing. Additionally, exploring artificial intelligence and machine learning applications in IBC and ABC will further enhance their potential.

This investigation demonstrates the potential of IBC and ABC in emerging technologies, highlighting the need for further research and development. Various industries, including healthcare, finance, government, and manufacturing, will benefit from the enhanced security, compliance, and efficiency provided by IBC and ABC applications.

To unlock the full potential of IBC and ABC in emerging technologies, it is essential to address the current challenges they face. By identifying and exploring future research directions, we can overcome these obstacles and enhance their capabilities. This will enable the development of secure and reliable communication systems. Additionally, focusing on these areas will help improve data protection, ensuring the integrity of information in an increasingly digital world. Through continued research and innovation, IBC and ABC can play a pivotal role in shaping the future of secure communication.

### 5.2 Further Examination of Security Assumptions and Vulnerability Assessment

The security assumptions underlying Identity-Based Cryptography (IBC) and Attribute-Based Cryptography (ABC) require rigorous examination to ensure their validity and effectiveness **(Baek *et al.* 2004, September; Goyal *et al.* 2006, October)**. detailed vulnerability assessment is vital for identifying potential weaknesses within a system. By conducting this assessment, organizations can pinpoint areas of concern that may pose risks. Addressing these vulnerabilities helps mitigate potential threats and enhance overall security.

This involves analyzing the cryptographic algorithms, key management systems, and attribute management protocols for vulnerabilities.

Effective vulnerability assessment involves evaluating the resistance of IBC and ABC to various attacks, such as side-channel attacks, quantum computer attacks, and key compromise impersonation attacks. Additionally, assessing the impact of compromised keys, attribute manipulation, and insider threats is essential. This examination should also consider the interplay between IBC and ABC with other security protocols and systems.

A comprehensive security assumption analysis should address questions such as: What are the implications of compromised master keys? How resilient are IBC and ABC to quantum computer attacks? What are the consequences of attribute manipulation or falsification? Answering these questions will facilitate the development of more robust and secure IBC and ABC solutions.

Moreover, ongoing monitoring and evaluation of security assumptions and vulnerability assessment are vital to maintaining the security and integrity of IBC and ABC systems. This ensures that emerging threats and vulnerabilities are promptly identified and addressed, safeguarding sensitive information and maintaining stakeholder trust.

### 5.3 Investigation of Artificial Intelligence and Machine Learning Applications in IBC and ABC

The integration of Artificial Intelligence (AI) and Machine Learning (ML) with Identity-Based Cryptography (IBC) and Attribute-Based Cryptography (ABC) has the potential to enhance security, efficiency, and scalability **(Anand, Khemchandani & Sharma, 2013, September; Goyal *et al.* 2006, October; Phaneendra, 2014)**. AI and ML can optimize cryptographic key management, improve attribute verification, and detect anomalies in access control.

***AI-powered IBC and ABC can:***

- ✓ Automate key generation and revocation
- ✓ Enhance attribute-based access control decisions
- ✓ Improve identity verification and authentication
- ✓ Detect and mitigate potential security threats

***ML algorithms can**:*

- ✓ Analyze patterns in access control data
- ✓ Identify potential security vulnerabilities
- ✓ Optimize cryptographic protocol performance

***Investigating AI and ML applications in IBC and ABC will enable**:*

- ✓ Intelligent key management systems
- ✓ Adaptive access control mechanisms
- ✓ Enhanced security and compliance

***Future research directions include:***

- ✓ Developing AI-driven cryptographic protocols
- ✓ Exploring ML-based attribute verification
- ✓ Investigating AI-powered security analytics

By leveraging AI and ML, IBC and ABC can provide more robust, efficient, and intelligent security solutions for emerging technologies, safeguarding sensitive information and protecting against evolving threats.

# 6. CONCLUSION, RESEARCH GAP, FUTURE DIRECTIONS AND RECOMMENDATIONS

## 6.1 Conclusion

This comprehensive analysis demonstrates the significance of Identity-Based Cryptography (IBC) and Attribute-Based Cryptography (ABC) in secure communication, access control, identity management, and data protection **(Phaneendra, 2014; Goyal *et al.* 2006, October)**. The integration of IBC and ABC with management principles enhances security, efficiency, compliance, and scalability. Our study highlights the crucial role of IBC and ABC in protecting sensitive information and ensuring secure communication. Effective implementation requires

balancing security, efficiency, and scalability, while addressing challenges such as key escrow and complexity.

The results of this study hold important implications for various stakeholders. Organizations aiming to improve security and compliance can benefit from the findings, as can developers of cryptographic solutions looking to enhance their technologies. Researchers exploring emerging technologies will gain valuable insights to guide their work. Additionally, policy-makers involved in regulating data protection and privacy will find the findings relevant to their efforts. Lastly, individuals concerned with secure communication and data protection will also benefit from the study's conclusions.

The integration of Artificial Intelligence (AI) and Machine Learning (ML) with Identity-Based Cryptography (IBC) and Attribute-Based Cryptography (ABC) revolutionizes secure communication and access control. AI-powered cryptographic key management, attribute verification, and anomaly detection enhance security and efficiency. ML algorithms optimize protocol performance, identify vulnerabilities, and improve access control decisions. This synergy enables intelligent key management, adaptive access control, and enhanced security compliance. Future research will further unlock AI- and ML-driven cryptographic potentials, safeguarding sensitive information and protecting against emerging threats in IoT, blockchain, cloud computing, and beyond. This innovative convergence secures the future of data protection.

***We may conclude that the integration of IBC and ABC with management principles is crucial for enhancing security, efficiency, and compliance. By addressing the research gaps and implementing the recommended strategies, organizations can establish a secure, efficient, and compliant infrastructure for data protection and access control.***

### 6.2 Research Gap/Limitations

Despite the comprehensive analysis, this study has some limitations. Future research should address:

- ✓ The lack of empirical studies on IBC and ABC implementation in real-world scenarios.
- ✓ Limited exploration of quantum-resistant IBC and ABC algorithms.
- ✓ The need for more efficient and scalable IBC and ABC algorithms.
- ✓ Future studies may focus on addressing these gaps to enhance the security, efficiency, and scalability of IBC and ABC solutions.

### 6.3 Future Directions

1. Investigate applications of IBC and ABC in emerging technologies (e.g., IoT, blockchain, cloud computing).

2. Develop more efficient and scalable IBC and ABC algorithms.

3. Improve key management and attribute management systems.

4. Explore artificial intelligence and machine learning applications in IBC and ABC.

5. Develop standards and guidelines for IBC and ABC implementation.

### 6.4 Recommendations

1. Organizations should prioritize IBC and ABC integration with management principles.

2. Implement robust identity and attribute management systems.

3. Continuously monitor and evaluate security assumptions.

4. Balance security, efficiency, and scalability.

5. Invest in research and development of more efficient and scalable IBC and ABC algorithms.

By addressing these research gaps, future directions, and recommendations, we can further enhance the security, efficiency, and compliance of IBC and ABC solutions.

## REFERENCES

Anand, D., Khemchandani, V., & Sharma, R. K. (2013, September). Identity-based cryptography techniques and applications (a review). In *2013 5th international conference and computational intelligence and communication networks* (pp. 343-348). IEEE. Doi: 10.1109/CICN.2013.78

Baek, J., Newmarch, J., Safavi-Naini, R., & Susilo, W. (2004, September). A survey of identity-based cryptography. In *Proc. of Australian Unix Users Group Annual Conference* (pp. 95-102). Retrieved from https://www.semanticscholar.org/paper/A-Survey-of-Identity-Based-Cryptography-Baek-Newmarch/2988b465ed8910c4ea07fe358330ef06d81084ff

Bethencourt, J., Sahai, A., & Waters, B. (2007, May). Ciphertext-policy attribute-based encryption. In *2007 IEEE symposium on security and privacy (SP'07)* (pp. 321-334). IEEE. Doi: 10.1109/SP.2007.11

Bubna, M. P., & Jha, P. B. (1984). Comparative analysis of Identity-based encryption with traditional public key encryption in wireless network. *IEEE Commun. Mag*, 196-205. Retrieved from https://www.semanticscholar.org/paper/COMPARATIVE-ANALYSIS-OF-IDENTITY-BASED-ENCRYPTION-Bubna-Jha/f07f6186ef395e2939d6041f75f626e86f772fde

Das, M., Chakraborty, R., & Banerjee, C. (2023). ID-Based Cryptography and Attribute-Based Cryptography: An Applied Mathematics Perspective. In *Intelligent Engineering Applications and Applied Sciences for Sustainability* (pp. 367-378). IGI Global. Doi: 10.4018/979-8-3693-0044-2.ch019

Ding, Y., Zhang, Y., Qin, B., Wang, Q., Yang, Z., & Shi, W. (2023). A scalable cross-chain access control and identity authentication scheme. *Sensors*, *23*(4), 2000. Doi: 10.3390/s23042000

Feng, L., Qiu, F., Hu, K., Yu, B., Lin, J., & Yao, S. (2024). CABC: A Cross-Domain Authentication Method Combining Blockchain with Certificateless Signature for IIoT. *Future Generation Computer Systems*, *158*, 516-529. Doi: 10.1016/j.future.2024.04.042

Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006, October). Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 89-98). Doi: 10.1145/1180405.1180418

Phaneendra, H. D. (2014). Identity-based cryptography and comparison with traditional public key encryption: A survey. *International Journal of Computer Science and Information Technologies*, *5*(4), 5521-5525. Retrieved from https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=9101ed4c951e367b20a1cf526a4d3be3cdff3c94

Qiao, Z., Liang, S., Davis, S., & Jiang, H. (2014, June). Survey of attribute based encryption. In *15th IEEE/ACIS international conference on software engineering, artificial intelligence, networking and parallel/distributed computing (SNPD)* (pp. 1-6). IEEE. Doi: 10.1109/SNPD.2014.6888687

Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In *Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings 24* (pp. 457-473). Springer Berlin Heidelberg. Doi: 10.1007/11426639_27

Thakur, A., Ranga, V., & Agarwal, R. (2024, February). Attribute-Based Encryption Scheme for Secure and Efficient Access in Blockchain. In *2024 IEEE International Conference for Women in Innovation, Technology & Entrepreneurship (ICWITE)* (pp. 653-658). IEEE. Doi: 10.1109/ICWITE59797.2024.10502721