International Journal of Engineering Research and Sustainable Technologies
Volume 2, No.3, Sep 2024, P 16-22
ISSN: 2584-1394 (Online version)

IDENTITY-BASED ENCRYPTION: A SECURE SOLUTION FOR PROTECTING SENSITIVE DATA

[1]Shermina, [2]Latha R, [3]Sreenithi R
[1]Assistant Professor, Muscat College, University of Stirling, Sultanate of Oman
[2]SRM Institute of Science and Technology, Kattankulathur, India
[3]Ignitho, TN, India
*** Corresponding author email address**: shermina@muscatcollege.edu.om

DOI: https://doi.org/10.63458/ijerst.v2i3.88 | ARK: https://n2t.net/ark:/61909/IJERST.v2i3.88

Abstract

Identity-Based Encryption (IBE) is a fundamental cryptographic technology that provides a powerful answer to the problems associated with protecting sensitive information in contemporary digital settings. In contrast to conventional encryption techniques, which depend on pre-existing public keys linked to certain entities, IBE uses distinct identifiers, like usernames or email addresses, as public keys. This method not only makes encrypted communication more flexible and accessible, but it also streamlines the key management procedure. Identity-Based Encryption is covered in detail in this study, which also explores its fundamental ideas, essential elements, and real-world uses. To provide a better understanding of IBE's cryptographic methods, the theoretical underpinnings of the algorithm—including its utilization of bilinear pairings and mathematical constructs—are clarified. In addition, the article investigates IBE's security features, testing its resistance to different kinds of intrusions and weaknesses. To illustrate the efficacy and adaptability of IBE in protecting data privacy across a range of industries, including healthcare, finance, and cloud computing, real-world deployment scenarios and case studies are given. Furthermore, new developments and trends in IBE studies are examined, providing insight into prospective directions for investigation and creativity in the future. For scholars, practitioners, and policymakers looking to use Identity-Based Encryption for strong data protection in the digital age, this paper is a great resource.

Keywords— *Identity-Based Encryption, IBE, Data Security, Cryptography, Public Key Infrastructure, Secure Communication,Bilateral Pairings, Privacy Protection, CryptographicTechniques,DigitalIdentity,Key, Management, Cybersecurity, Data Privacy, Secure Messaging, Access Control.*

1. Introduction

Safeguarding sensitive data's integrity, confidentiality, and authenticity is crucial in the field of cyber-attacks, Phaneendra, H. D. [1]. Identity-Based Encryption (IBE) is a cornerstone of contemporary cryptographic methods, providing a flexible and effective means of safeguarding data and facilitating secure communication. By leveraging user identities as public keys—such as email addresses or domain names—IBE expedites the encryption process in contrast to conventional public key infrastructure (PKI), which is dependent on laborious certificate management systems. By doing away with the requirement for pre-distributed public keys [2], this novel method improves the scalability of secured communication systems while streamlining key management.Adi Shamir first proposed the idea of identity-based encryption in 1984 as a substitute for traditional public key infrastructure. IBE's core principle is to extract public keys from user identities that can be independently verified, doing away with the requirement for a centralized body to issue certificates. Increased flexibility, lower overhead, and improved usability are only a few benefits of this paradigm shift [3]. IBE uses user IDs to enable secure messaging, data exchange, and access control across a range of industries, including cloud service providers, government agencies, and financial institutions.

The application of bilinear pairings, a mathematical concept that permits effective cryptographic operations on elliptic curve groups, is one of the essential elements of identity-based encryption. IBE systems achieve advanced functionalities such as delegation, revocation, and key escrow without compromising security by utilizing the peculiarities of bilinear pairings [4]. Recent developments in cryptography have also resulted in pairing-based protocols that provide verifiable security guarantees and defense against new threats like quantum attacks.

It is more important than ever to protect sensitive data from malicious actors and illegal access in this age of ubiquitous connectivity and digital transformation. Identity-Based Encryption shows promise as a means of addressing the changing security challenges in the globalized world of today [5]. IBE offers a strong foundation for developing private and secure communication systems by fusing cutting-edge key management and access control strategies with cryptographic concepts. This study examines Identity-Based Encryption's foundations, uses, and developments to highlight how it will influence cybersecurity going forward.

2. Literature Review

While Identity-Based Encryption (IBE) uses public key and certificate management, PKI (public key infrastructure) offers an alternative to public key encryption. The extra computation at the private key generator is the primary drawback of IBE compared to revocation (PKG). This work aims to explore many approaches to address the fundamental problem of identity renunciation. We also discuss our suggested work, which offers an intriguing way to incorporate outsourced computations into IBE and suggests a reversible IBE strategy in a server-assisted environment. With the use of a Key Update Cloud Services Provider, our proposal offloads most of the key generation-related procedures between key-issuing and key-redesign processes, enabling PKG and clients to handle only a consistent number of basic tasks locally. Furthermore, we suggest an additional advancement that may be verified securely using the recently defined Refereed Handover of Computation paradigm [2].

[6] Identity-Based Encryption (IBE) improves message secrecy by eliminating the requirement for key certificates, allowing users to generate public keys from random strings, such as names or email addresses. This work provides an extensive overview of different IBE schemes, ranging from the novel pairing function-based Boneh-Franklin scheme to more modern lattice-based IBE methods. Depending on their settings, fundamental primitives, security concerns, and computational difficulties, these schemes are categorized in the review. This review does not cover variations like fuzzy IBE and hierarchical IBE [6]. The report also addresses issues related to implementation, current developments in IBE research, and recommendations to improve future scheme designs [6].

[1] Identity-Based Cryptography (IBC) research is reviewed and contrasted with conventional public key encryption techniques in this paper. Identity-Based Cryptography (IBC) is a newly developed field in public key cryptography that is investigated through an analysis of basic concepts such as Identity-Based Signature (IBS) schemes and Identity-Based Encryption (IBE). The review focuses on significant IBE methods that make use of bilinear pairings, a common computational foundation for many IBE systems. IBE and conventional public key encryption are compared and contrasted. In conclusion, the research highlights the importance of IBC in contemporary cryptographic systems while delving into its advantages, disadvantages, and applications.Keywords: public key infrastructure, identity-based cryptography.

[7] This study provides a thorough analysis of Identity-Based Cryptography (IBC), including its practical applications and security implications. We start with the fundamental concepts of security and cryptography and then explore IBE, following its development and scientific breakthroughs. Along with in-depth security evaluations, we offer insights into Identity-Based Signature (IBS) and IBE techniques [7]. Furthermore, we investigate and assess the security models and constructions of Revocable Identity-Based Encryption (RIBE) schemes and Hierarchical Identity-Based Encryption (HIBE) in both standard and random oracle models. We examine several encryption techniques and highlight their advantages, disadvantages, effectiveness, and security implications.

[8] Using any IBE method, we suggest new and effective CCA-secure public-key encryption techniques that are protected from adaptive chosen-ciphertext attacks. There are significant practical and theoretical consequences to our constructs. First, they provide a new paradigm that achieves CCA-security without requiring the "proofs of well-formedness" that were necessary in earlier constructions. Second, we generate CCA-secure encryption algorithms with competitive performance, on par with the state-of-the-art, by employing well-established IBE constructs [8]. Moreover, our methods easily translate to strengthening hierarchical IBE schemes against adaptive chosen-ciphertext attacks. In conjunction with other studies, this marks the beginning of effective architectures for CCA-secure IBE systems. Table 1 shows a survey of the various papers with results.

3. System Methodology

A basic mathematical technique used in many **IBE** designs is bilinear pairings. Bilinear pairings are essential for building secure and effective **IBE** systems and allow computations in cryptographic protocols to be completed quickly. These pairings are used in a variety of cryptographic primitives, such as identity-based encryption, attribute-based encryption, cryptographic protocols like digital certificates, and key agreement [9]. They simplify interactions between elements in distinct groups. Because bilinear pairings allow operations on encrypted files and support additional cryptographic capabilities, they enhance the security and effectiveness of **IBE** systems.

3.1 Trusted Third Party (Private Key Generator - PKG)

A Trusted Third Party, referred to as a Private Key Generator (PKG) [10], is essential to IBE (Figure 1). The PKG is responsible for creating private keys that correspond to users' identities. It is trusted to provide users with private keys upon request and holds the master secret key.

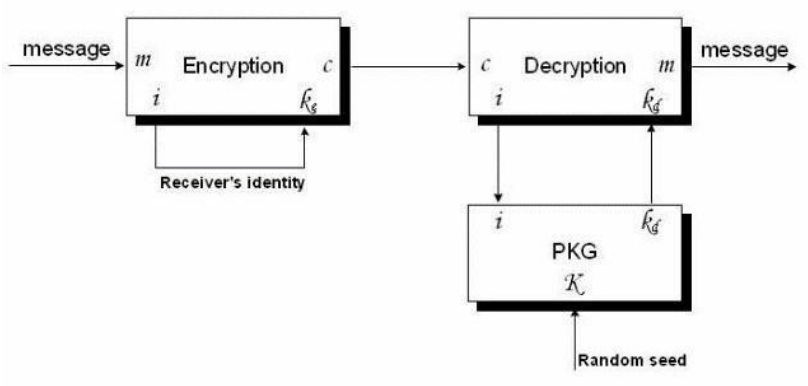

Fig.1. Identity-Based Encryption

3.2 Identities

In IBE, user-specific data, including email addresses, domain names, and other distinctive identifiers, are referred to as identities. These identities are used to generate public keys and facilitate the encryption and decryption processes

3.3 Public Keys

In classical public key cryptography, users create their own public-private key pairs. However, in IBE, public keys are generated from identities [11]. Users no longer need to generate or exchange public keys, as the PKG generates them based on user IDs.

3.4 Private Keys

In IBE, private keys are linked to specific user identities and are generated by the PKG. Upon registration or request, users receive a private key from the PKG. Messages encrypted with the corresponding public key can be decrypted using the private key.

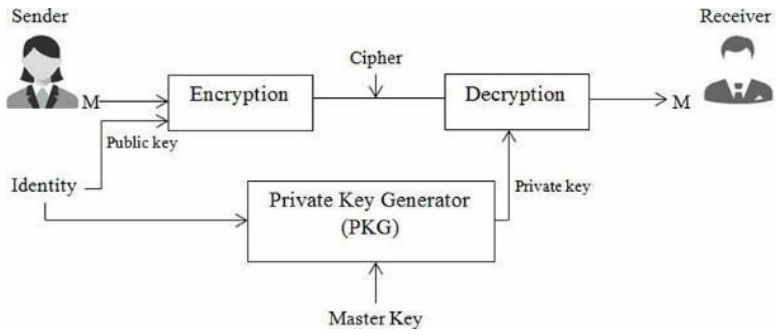

Fig. 2. Encryption and Decryption

3.5 Encryption/Decryption Process

A recipient's identity (e.g., e-mail address or username) is used by the sender as the public key in the IBE encryption procedure (Figure 2). It is not necessary for the sender to explicitly know the receiver's public key [12]. Only the recipient, who possesses the corresponding private key, can decrypt the message. The recipient must use their private key, which they can obtain from a PKG, to decrypt a message that has been encrypted using their identity as the public key.

3.5.1 Basic IBE

In Basic IBE, the recipient's identity serves as the public key, which the sender uses to encrypt a message.

Subsequently, the recipient decrypts the message using their private key, which they have obtained from the PKG. Functionality: By utilizing user identities as public keys directly and eliminating the need for key distribution, Basic IBE streamlines the encryption process. It provides a simple method for secure communication. Applications: Basic IBE is commonly used for email encryption, messaging apps, secure file sharing, and other scenarios where individual users need to communicate securely over an untrusted network.

3.5.2 BroadcastIBE

By enabling the sender to secure a message for multiple recipients at once, Broadcast IBE expands on the capabilities of Basic IBE [13]. The message is encrypted once, and the sender designates a set of identifiers as the recipients. Instead of encrypting the message individually for each recipient, Broadcast IBE facilitates efficient and secure transmission to multiple recipients. It enhances communication scalability and simplifies the encryption process.

Applications: Broadcast IBE is useful in scenarios such as group messaging, secure multicast communication, and organizational announcements, where a sender needs to distribute updates or sensitive information to a predefined group of recipients.

Table 1. Survey Table

S.no	Paper name	Technique	Advantage	Disadvantage	Result
1	Fast Digital Identity Revocation	Identity Revocation	Better Efficient verification	Infeasible to generate a signature	The results were displayed that the proof from user to vendor of the validity of user's ID remains very small as per the micalimethod
2	Certificate revocation using Fine Grained Certificatespace partitioning	Certificate Revocation System	More Method Efficient	Not Suitable In case of a Distributed query answering System	The result displays that right balance between query CAtodirectory communication costsand query costs by carefully selectingthe number of partitions
3	Quasi Modo: Efficient Certificate validation and revocation	Tree based variant And NOVOMODO System	Improvement in Relevant time and Communication Complexity	Limited Validity	A result displayed that the direct improvement in both the overall verification complexity, as well as the communication complexity, over previous Tree-based schemes.
4	Two Protocols For Delegation Of Computation	Round statistically Sound protocol and arithemetization techniques	Easier to Implement for general Computations, Less efficient	Un trusted Server And week client	As extension of this protocol that somewhat reduces The work load of the Client at the price of a comparable increase in the number of rounds

5	Outsourcing Encryptionof Attribute based Encryption with map reduce	Attribute based encryption (ABE) Graphic Tool is used	Computational Cost at user side During encryption is reduce	Complexity of access	The reducer executes reduce Function on the set of intermediate pairs(k',v')with the same key and outputs the final result
6	Privacy-Assured Outsourcing of image Reconstruction service in cloud	OIRS scheme is Used for design the framework	Source and efficient	In secure data sensitive data While enabling Outsourced image service	The System effectiveness and efficiency and Speed up of OIRS through hardware built-in system design.

3.5.3 Identity-Based Signature (IBS)

Using user IDs, Identity-Based Signature (IBS), a cryptographic primitive, enables the verification of a message's origin. Users can use their private keys to sign messages [14], and the legitimacy of the signature can be confirmed by anyone with access to the corresponding public key, which is the user's identity.

Functionality: Without explicitly exchanging public keys, IBS provides a method for authenticating the origin of messages. In digital communication, it ensures message integrity, non-repudiation, and identity verification.

Applications:IBS is widely used in secure email correspondence, document signing, payment authentication, and trusted authentication protocols for digital signatures.

3.5.4 Security properties of IBE

3.5.4.1 Indistinguishability of ciphertexts (IND- CCA2)

A basic security feature known as IND-CCA2 guarantees the privacy of a message encrypted with an IBE scheme. It ensures that, even with access to a decryption oracle, an adversary cannot distinguish between two ciphertexts created from the same raw message [15]. Within the framework of IBE, IND-CCA2 implies that an adversary, even with access to decryption oracles, cannot deduce any significant information about the plaintext message from its encrypted form.

3.5.4.2 Unforgeability

Another crucial security criterion for IBE schemes is unforgeability, especially when it comes to Identity-Based Signatures (IBS). It ensures that only authorized individuals can legitimately sign messages, preventing unauthorized parties from altering or forging signatures [16]. Message integrity and authenticity are ensured by unforgeability, which makes it computationally impossible for an attacker to create a legitimate signature without the corresponding private key (identity).

3.5.5 Construction of IBE Schemes

3.5.5.1 Mathematical Framework

Numerous IBE methods make use of mathematical constructs like bilinear pairings [17], which make cryptographic operations more secure and efficient. To maintain security, these schemes frequently rely on mathematical assumptions and characteristics, such as the difficulty of solving the Decisional Bilinear Diffie-Hellman (DBDH) problem.

3.5.5.2 Boneh-Franklin (BF) Scheme

Bilinear pairings over elliptic curves are used in the well-known BF IBE technique to provide IND-CCA2 security. It builds a system in which users' private keys are generated by an authorized Key Generation Center (PKG) in accordance with their identities [18]. To provide resistance against attacks, BF IBE carefully designs algorithms for key generation, encryption, and decryption to address any vulnerabilities.

3.5.5.3 WeilPairingSchemes

Weil pairings, a type of bilinear pairing, are used by another class of IBE schemes to create reliable encryption and decryption processes [19]. To ensure the integrity and security of communications, these techniques sometimes involve complex mathematical transformations and cryptographic protocols [20].

4. Result and Discussions

Secure Communication in Sensor Networks: IBE facilitates effective and secure interaction between node sensors and data aggregation points in sensor networks set up for monitoring and data collection. IBE simplifies key management and authentication by leveraging identity as public keys, which strengthens sensor networks' resistance to tampering and eavesdropping attempts.

Access Control in Cloud Computing: In cloud computing environments, IBE enables fine-grained access control techniques that allow users to safely access resources via their identities. Cloud providers can utilize IBE to scale and flexibly encrypt data dynamically for individual users or groups, protecting privacy and confidentiality.

E-commerce and Digital Rights Management: By encrypting data with user identities, IBE facilitates secure transactions and content dissemination in online shopping sites and multimedia distribution systems. By utilizing IBE, content providers can safeguard digital assets such as software, documents, and media files, ensuring that only individuals with permission can access or use them.

Secure Messaging in Mobile Applications: IBE can be used by mobile applications for secure messaging and communication, such as social media platforms, email clients, and instant messaging apps. Even in insecure network contexts, IBE enables users to exchange secure communications via their identities, ensuring end-to-end security and authentication.

5. Conclusion and Future Work

Conclusively, Identity-Based Encryption (IBE) offers a robust cryptographic framework with numerous applications and ongoing research challenges. Although IBE schemes are highly adaptable, there are still areas that require further research and development to improve their efficiency, security, and usability. Enhancing efficiency is a crucial topic for further investigation. Existing IBE systems often result in high computational and bandwidth overhead, especially when there are a large number of users or frequent changes to important parameters. Addressing these efficiency issues is imperative for making IBE more practical and scalable for real-world use.

The development of efficient revocation mechanisms represents a significant area for research. Revocation in IBE systems refers to the secure deactivation of compromised private keys to prevent unauthorized access and maintain system integrity. Designing reliable and effective revocation processes remains challenging, particularly in dynamic environments where users frequently join and leave the system.

Additionally, to encourage broader adoption of IBE across various platforms and contexts, standardization and interoperability initiatives are essential. Greater trust and interoperability among a variety of stakeholders can be fostered through standardized protocols and interoperable implementations, enabling the smooth integration of IBE into existing systems.

References

1. Phaneendra, H. D. ‘Identity-based cryptography and comparison with traditional public key encryption: A survey’. International Journal of Computer Science and Information Technologies, 5(4), 5521-5525., 2014.
2. Chatterjee, S., & Sarkar, P. ‘Identity- based encryption’. Springer Science & Business Media. 2011.
3. Boneh, D., & Franklin, M. ‘Identity-based encryption from the Weil pairing’. In Annual international cryptology conference (pp. 213-229). Berlin, Heidelberg: Springer Berlin Heidelberg. 2001.
4. Sahai, A., & Waters, B. ‘Fuzzy identity- based encryption. In Advances in Cryptology–EUROCRYPT 2005’: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus,Denmark,May22-26,2005.Proceedings 24 (pp. 457-473). Springer Berlin Heidelberg. 2005.
5. Horwitz, J., & Lynn, B. ‘Toward hierarchical identity-based encryption’. In International conference on the theory and applications of cryptographic techniques (pp. 466-481). Berlin, Heidelberg: Springer Berlin

Heidelberg. 2002.
6. Boldyreva, A., Goyal, V., & Kumar, V. 'Identity-based encryption with efficient revocation'. In Proceedings of the 15th ACM conference on Computer and communications security (pp. 417-426). 2008.
7. Gentry, C. 'Practical identity-based encryption without random oracles. In Advances in Cryptology-EUROCRYPT 2006': 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28- June 1, 2006. Proceedings 25 (pp. 445-464). Springer Berlin Heidelberg. 2006.
8. Canetti, R., Halevi, S., & Katz, J., 'Chosen-cipher text security from identity-based encryption. In Advances in Cryptology- EUROCRYPT 2004': International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23 (pp. 207-222). Springer Berlin Heidelberg. 2004.
9. Boneh, D., Canetti, R., Halevi, S., & Katz, J. 'Chosen-cipher text security from identity-based encryption'. SIAM Journal on Computing, 36(5), 1301-1328. 2007.
10. Boneh, D., Raghunathan, A., & Segev, G. 'Function-private identity-based encryption: Hiding the function in functional encryption'. In Advances in Cryptology–CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II (pp. 461-478). Springer Berlin Heidelberg.
11. Fan,C.I.,Huang,L.Y.,&Ho,P.H.'Anonymous multi receiver identity-based encryption'. IEEE Transactions on Computers, 59(9), 1239-1249.2010.
12. Galindo, D.'Boneh-Franklin identity- based encryption revisited'. In Automata, Languages and Programming: 32nd InternationalColloquium,ICALP2005,Lisbon, Portugal, July 11-15, 2005. Proceedings 32 (pp. 791-802). Springer Berlin Heidelberg. 2005.
13. Lynn, B. 'Authenticated identity-based encryption'. Cryptology ePrint Archive. 2002.
14. Seo, J. H., &Emura, K. 'Revocable identity-based encryption revisited: Security model and construction'. In Public-Key Cryptography–PKC 2013: 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26–March 1, 2013. Proceedings 16 (pp. 216- 234). Springer Berlin Heidelberg.2013.
15. Libert,B.,&Vergnaud,D.'Adaptive-ID secure revocable identity-based encryption'. In Topics in Cryptology–CT-RSA 2009: The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009. Proceedings (pp. 1-15). Springer Berlin Heidelberg.2009.
16. Gentry, C., & Halevi, S. 'Hierarchical identity-based encryption with polynomially many levels' . In Theory of Cryptography Conference (pp. 437-456). Berlin, Heidelberg: Springer Berlin Heidelberg. 2009.
17. Cao, C., Tang, Y., Huang, D., Gan, W., & Zhang, C. 'IIBE: an improved identity- based encryption algorithm for WSN security. Security and Communication Networks', 2021, 1-8.2021.
18. Baek, J., Susilo, W., & Zhou, J. 'New constructions of fuzzy identity-based encryption'. In Proceedings of the 2nd ACM symposium on Information, computer and communications security (pp. 368-370).2007.
19. Abdalla, M., Birkett, J., Catalano, D., Dent, A. W., Malone-Lee, J., Neven, G., ... & Smart, N.P. 'Wild carded identity-based encryption. Journal of Cryptology', 24, 42-82.2011.
20. Deng, H., Qin, Z., Wu, Q., Guan, Z., Deng, R. H.,Wang,Y.,&Zhou,Y., 'Identity-based encryption transformation for flexible sharing of encrypted data in public cloud'. IEEE Transactions on Information Forensics and Security, 15, 3168-3180.2020.