IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303282 |

Identity-Based Encryption Transformation for Flexible Sharing of Encrypted Data in Cloud

G Bhavana[1],C Poojitha[2], M Kullai Swami[3] , K Mounika[4], G Madhusudhan[5]

Assistant Professor, Department of CSE, Faculty, AITS, Tirupati, India [1]

Student, Department of CSE, Annamacharya Institute of Technology and Sciences, Tirupati, India [2, 3,4,5]

ABSTRACT: Identity-Based Encryption (IBE) extends the concept of public-key encryption (PKE) by allowing a user's identity string to serve as their public key. This eliminates the need for a separate public key infrastructure. The first IBE scheme utilized a bilinear map and demonstrated its security in the random oracle model. Since then, numerous IBE schemes have been developed using bilinear maps. For real-world applications, a Revocable IBE (RIBE) scheme is necessary to effectively revoke a user's private key when needed. Various RIBE schemes have been proposed to enhance security or performance. Generic methods for designing RIBE schemes using binary trees have been introduced. The key principle behind this generic RIBE design is to associate the path of a binary tree with a ciphertext rather than with a private key. However, generic RIBE designs require larger binary trees compared to direct RIBE design methods, leading to inefficiencies in terms of update key size. To alleviate the computational burden on the key generation center in RIBE, a scheme was proposed where the generation of update keys is delegated to a cloud server. Nevertheless, this approach results in update keys increasing in size proportionally to the number of users.

KEYWORDS: Identity-based encryption, key revocation, subset cover, update key delegation, public verifiability

I. INTRODUCTION

Revocable Identity-Based Encryption (RIBE) has become crucial in efficiently managing keys within distributed systems. Traditionally, RIBE relies on trusted authorities to generate and distribute decryption keys based on user identities. However, in environments where user privileges change regularly, managing update keys becomes vital for maintaining system security and adaptability. Our paper introduces a novel approach for Delegate and Verify the Update Keys of Revocable Identity-Based Encryption. We address the need for securely managing key updates by proposing a protocol that allows a trusted authority to delegate update key management to specific entities. This delegation is done securely to ensure the integrity and authenticity of the update process. The ability to delegate and verify update keys is critical for maintaining the security and efficiency of distributed systems, especially in dynamic environments where user privileges evolve frequently. Our proposed approach aims to bridge this gap by offering a flexible and secure mechanism for managing update keys within RIBE schemes. Overall, our solution aims to enhance the resilience and adaptability of distributed systems by providing a robust method for managing update keys in RIBE schemes.

II. RELATED WORKS

In the [1] The paper titled "Identity-based encryption from the Weil pairing" by D. Boneh and M. K. Franklin, published in 2001, introduced the concept of Identity-Based Encryption (IBE) based on bilinear pairings, specifically the Weil pairing. Identity-based encryption allows encryption and decryption operations to be performed directly using identities (such as email addresses or usernames) as public keys, eliminating the need for public key certificates. The use of bilinear pairings in cryptography has opened up new possibilities for constructing efficient cryptographic schemes, including identity-based encryption and other advanced cryptographic primitives.

[2] The paper titled " Identity-based encryption with efficient revocation," authored by A. Boldyreva, V. Goyal, and V. Kumar, published in 2008, provides a scheme for Identity-Based Encryption (IBE) that incorporates efficient mechanisms for revocation. Revocation is a crucial aspect of cryptographic systems, especially in scenarios where users' access privileges need to be revoked in a timely and secure manner. The work addresses the challenge of

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303282 |

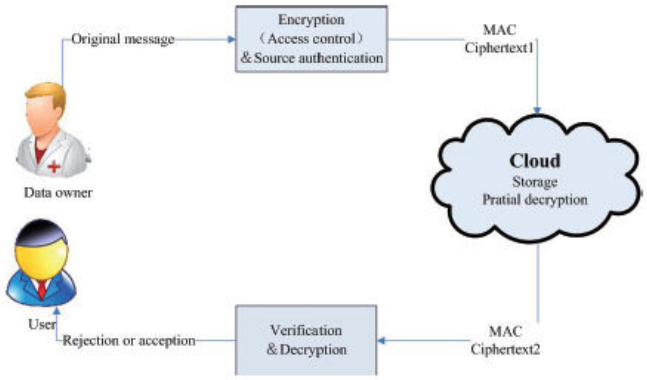
efficiently managing revocation in IBE schemes, which is essential for maintaining the security and integrity of the system.

[3] The paper by B. Libert and D. Vergnaud ,titled "Adaptive-ID secure revocable identity-based encryption" published in 2009, introduces a cryptographic scheme for Identity-Based Encryption (IBE) that is both revocable and resistant to adaptive chosen identity attacks. Adaptive-ID security is a desirable property in identity-based encryption schemes, ensuring that an adversary cannot obtain decryption keys for arbitrary identities of their choosing, even if they have access to decryption oracles.

[4] The paper titled " Revocable identity-based encryption revisited: Security model and construction," authored by J. H. Seo and K. Emura , published in 2013, revisits the concept of revocable identity-based encryption (IBE) and presents advancements in its security model and construction. Revocable IBE is a cryptographic primitive that allows for efficient management of access control in dynamic environments, where the ability to revoke access privileges of users is essential.

III. PROPOSED SYSTEM

we examine a way to make a decryption key greater effective inside the experience that it permits decryption of more than one cipher texts, without growing its size.To design an green public-key encryption scheme which helps flexible delegation within the experience that any subset of the cipher texts (produced by means of the encryption scheme) is decry table through a regular-length decryption key (generated by the proprietor of the grasp-secret key).” We remedy this hassle via introducing a special form of public-key encryption which we name key-combination cryptosystem (KAC). In KAC, customers encrypt a message no longer best below a public-key, however also underneath an identifier of cipher text called elegance. Meaning the cipher texts are in addition categorized into one-of-a-kind training. The important thing proprietor holds a master-secret known as grasp-mystery key, which can be used to extract mystery keys for exclusive classes. Extra importantly, the extracted key have can be an aggregate key that's as compact as a mystery key for a single elegance, but aggregates the electricity of many such keys, i.e., the decryption vigor for any subset of cipher textual content classes.



IV. IMPLEMENTATION

Data Encryption Standard:

The Data Encryption Standard (DES) is a symmetric-key block cipher encryption algorithm that operates on fixed-size blocks of data, typically 64 bits in length. Developed in the 1970s, DES was established as a federal standard by the U.S. National Bureau of Standards (now NIST) in 1977 and was widely adopted for securing sensitive information in electronic communications and storage. DES employs a Feistel cipher structure, where the input block is divided into two halves and undergoes a series of alternating encryption and decryption rounds using a shared secret key. Each round involves permutation, substitution, and mixing operations to produce the ciphertext.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303282 |

AI-NN-Fuzzy Algorithm for decission Making:

AI-NN-Fuzzy algorithm for decision making in cryptography offers a versatile and adaptive approach to address the evolving challenges and complexities of cryptographic systems. By combining AI, NNs, and Fuzzy Logic techniques, it enables the development of more robust, efficient, and secure cryptographic solutions for protecting sensitive information and ensuring the confidentiality, integrity, and authenticity of data.

Rivest-Shamir-Adleman Algorithm (RSA)

The RSA algorithm, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is a widely used asymmetric cryptographic algorithm for secure communication and digital signatures. It relies on the mathematical difficulty of factoring large prime numbers into their constituent primes. RSA is widely used in various applications, including secure communication protocols like SSL/TLS, digital signatures, key exchange, and secure email. It provides a secure method for exchanging information over insecure channels and for verifying the authenticity of messages and digital documents. However, its security relies on the difficulty of factoring large numbers, and it is vulnerable to attacks if the underlying mathematical problem becomes solvable by quantum computers.

V. RESULTS AND DISCUSSION

The series of visuals presented below showcase the sequential development of our project, which involved the establishment of a Flask framework.

Login: A login page is where users enter credentials to access restricted content or services on a website.

Fig1.Login page.

Registration: Here we will register the details.

Fig2. Registration page.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303282 |

Upload File: To upload the file in the cloud.

Fig3.upload file page

View the Files: After successfully uploading the file we will see all the files in the cloud

Fig4. View Files Page

Access Other Users Files: If you want to see the other user files then we will enter the two keys such as Private key and cloud key.Private key is generated by Group Manager and cloud key is generated by cloud server.

Fig5.Acess Other User Files

VI. CONCLUSION

In conclusion, delegating and verifying the update keys of revocable identity-based encryption (RIBE) systems is a critical aspect in ensuring the security and efficiency of these cryptographic schemes. By allowing authorized parties to delegate their update keys, RIBE systems can accommodate dynamic environments and evolving access control requirements. Moreover, the verification of update keys plays a pivotal role in maintaining the integrity and

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303282 |

authenticity of the delegated privileges. Through this delegation and verification process, organizations can effectively manage access control policies, revoke compromised or outdated keys, and streamline cryptographic operations without sacrificing security. However, it is imperative to implement robust verification mechanisms to prevent unauthorized or malicious key delegations. Overall, the successful deployment of delegate and verify mechanisms in RIBE systems enhances their flexibility, scalability, and resilience to security threats, thereby facilitating secure data sharing and communication in diverse applications and environments. Moreover, the verification of update keys serves as a crucial checkpoint in the RIBE ecosystem, safeguarding against unauthorized modifications or manipulations of access control policies. Through rigorous verification procedures, organizations can uphold the integrity and trustworthiness of the delegated privileges, thereby ensuring that only legitimate updates are accepted and enforced.Overall, the implementation of delegate and verify mechanisms in RIBE systems underscores a balanced approach to access control, combining flexibility, security, and efficiency.

REFERENCES

1. D. Boneh and M. K. Franklin, ‘‘Identity-based encryption from the Weil pairing,’’ in Advances in Cryptology— CRYPTO 2001, vol. 2139. Berlin, Germany: Springer, 2001, pp. 213–229.
2. A. Boldyreva, V. Goyal, and V. Kumar, ‘‘Identity-based encryption with efficient revocation,’’ in Proc. 15th ACM Conf. Comput. Commun. Secur., Oct. 2008, pp. 417–426.
3. B. Libert and D. Vergnaud, ‘‘Adaptive-ID secure revocable identity-based encryption,’’ in Topics in Cryptology—CT-RSA 2009, vol. 5473. Berlin, Germany: Springer, 2009, pp. 1–15.
4. J. H. Seo and K. Emura, ‘‘Revocable identity-based encryption revisited: Security model and construction,’’ in Public-Key Cryptography—PKC 2013, vol. 7778. Berlin, Germany: Springer, 2013, pp. 216–234.
5. S. Park, K. Lee, and D. H. Lee, ‘‘New constructions of revocable identitybased encryption from multilinear maps,’’ IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1564–1577, Aug. 2015.
6. K. Lee, D. H. Lee, and J. H. Park, ‘‘Efficient revocable identity-based encryption via subset difference methods,’’ Des., Codes Cryptogr., vol. 85, no. 1, pp. 39–76, Oct. 2017
7. Y. Watanabe, K. Emura, and J. H. Seo, ‘‘New revocable IBE in primeorder groups: Adaptively secure, decryption key exposure resistant, and with short public parameters,’’ in Topics in Cryptology—CT-RSA 2017, vol. 10159. Berlin, Germany: Springer, 2017, pp. 432–449.

BIOGRAPHY

Mrs. G Bhavana, M.Tech., is currently working as Assistant Professor in the department of CSE, Annamacharya Institute of Technology and Sciences, Tirupati.

Ms. C Poojitha is currently pursuing B. Tech in the stream of Computer Science and Engineering from Annamacharya Institute of Technology and Sciences, Tirupati.

Mr. M Kullai Swami is currently pursuing B. Tech in the stream of Computer Science and Engineering from Annamacharya Institute of Technology and Sciences, Tirupati.

Ms. K Mounika is currently pursuing B. Tech in the stream of Computer Science and Engineering from Annamacharya Institute of Technology and Sciences, Tirupati.

Mr. G Madhusudhan is currently pursuing B. Tech in the stream of Computer Science and Engineering from Annamacharya Institute of Technology and Sciences, Tirupati.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details