iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 Issue: VI Month of publication: June 2023

DOI: https://doi.org/10.22214/ijraset.2023.53709

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Enabling Encrypted Cloud Emails with Data Encryption using Advanced Encryption Techniques

Mr. Abhijeet Gosavi[1], Mr. Sakib Shaikh[2], Mr. Adnan Sayyed[3], Mr. Somesh Sapa[4], Mr. Ayan Shaikh[5], Prof. A. A. Pund[6]
[1, 2, 3, 4, 5, 6]*Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar*

Abstract: Cloud computing offers a flexible and convenient means of exchanging data, with several advantages for both society and individuals. With the widespread usage of cloud emails and frequent reports of large-scale email leakage occurrences, the security property known as forward secrecy has become desirable and necessary for both users and cloud email service providers to increase the security of cloud email systems. Typical techniques of attaining forward secrecy, such as Diffie-Hellman key exchange and forward-secure public-key encryption, have not been extensively authorized and used because they fail to meet the security and practicality requirements of email systems at the same time. We introduce a new cryptographic primitive called forward-secure puncturable identity-based encryption (fs-PIBE) in this paper to capture forward secrecy of encrypted cloud email systems without sacrificing practicability. It allows an email user to perform fine-grained decryption capacity revocation. In the standard model, we design a framework for encrypted cloud email systems and instantiate it with a concrete fs-PIBE structure that has constant ciphertext size and proved security. We enhance the proposed fs-PIBE scheme to provide end-to-end encryption and outsourced decryption, respectively, to improve the security and efficiency of the presented framework.
Keywords: Secure Cloud Email, Identity-based Encryption, Broadcast Encryption, Encrypted cloud emails, forward secrecy, puncturable encryption, identity-based encryption, end-to-end security.

I. INTRODUCTION

Despite the rise of various secure communications platforms, email remains one of the most popular ways to communicate. While mail server transit security is beneficial against some types of attackers, it does not provide reliable security guarantees for email confidentiality or authenticity. Reports of widespread data collecting operations by nation-state actors, large-scale email server breaches exposing millions of emails, and attackers accessing email accounts to search the emails for important data demonstrate that transport security alone is insufficient. In such cases, end-to-end encryption is used to protect user data. With end-to-end encryption, the email infrastructure becomes essentially a transportation service for opaque email data, and no compromise should affect the security of an end-to-end encrypted email — separate from the sender and receiver endpoints. Encryption is a simple way to protect data security and confidentiality. Because it uses a compact public key infrastructure, identity-based encryption is one of the most promising representative safe techniques. The data owner would like to share the identity-based encrypted data with others in specific instances when storing it in the cloud.

Email's widespread use provides great convenience to people's daily communications, but it also poses a serious threat to people's personal privacy. This is due to the fact that email messages frequently include sensitive information, and large-scale cyber-attacks on email networks are becoming more common. In recent years, email data breaches have been recognized as one of the leading causes of important data loss in financial, legal, and professional companies. OpenPGP and S/MIME, the standards for encrypting emails, have been around for more than two decades.

They use a hybrid encryption model. To put it another way, the email sender produces a random session key before using a symmetric encryption algorithm to encrypt the email content. Despite numerous improvements to the efficiency and security of these two protocols, most practical email systems do not use them due to the issue.\\ Public key infrastructures (PKIs) are required for their deployment, and each user must maintain a public key certificate issued by a trusted authority. The term "identity-based encryption" (IBE) was initially used to refer to key management in the context of public key encryption. It allows users to use any string as their public keys, such as identity numbers and email addresses, and therefore is closer to the practical scenario of email senders using a simple and meaningful string rather than a signed public key certificate to identify the intended receiver. IBE is recognized as an ideal building block for encrypted email systems due to its numerous features. To achieve forward secrecy of encrypted emails, early developments of secure email systems used this method. The difficulty of synchronization, however, limits this basic strategy. To put it another way, it necessitates that all players log on at the same time. The use of forward-secure public key encryption, as proposed by Canetti et al., is another appealing method for establishing forward secrecy in email systems.

The entire lifetime of an email system is divided into distinct time intervals using their technique, during which each email user utilizes various secret keys thanks to a key evolution process, but their public keys remain intact. This situation brings up the most serious issue we face in our work. How to enable forward secrecy in cloud emails that are encrypted.

A. Motivation

With the growing usage of cloud email and numerous instances of large-scale email leakage events, the risk of large-scale email leakage is increasing. While mail server transit security is beneficial against some types of attackers, it does not provide reliable security guarantees for email confidentiality and authenticity. Reports of widespread data gathering attempts by nation-state actors, large-scale email server breaches exposing millions of emails, or attackers accessing email accounts to search the emails for important data highlight the fact that transport security alone is insufficient. The forward secrecy can guarantee the confidentiality of those previously encrypted emails even if the user's secret key gets exposed. So that we introduce a new cryptographic primitive named forward-secure puncturable identity-based encryption (fs-PIBE) which enables an email user to perform fine-grained revocation of decryption capacity.

II. REVIEW OF LITERATURE

D. Poddebniak et al: In this paper, we describe new approaches for revealing the plaintext of encrypted emails based on a technique called malleability gadgets. To inject malicious plaintext snippets into encrypted emails, we use CBC/CFB devices. After decryption, these snippets take advantage of existing and standard complying backchannels to exfiltrate the complete plaintext. Using HTML, CSS, and X.509 functionality, we describe malleability gadgets for emails. The attack is started when the recipient decrypts a single maliciously designed email from the attacker, and it works even if the emails were acquired a long time ago.

P. Xu et al: This paper presented a Conditional Identity-based Broadcast Proxy Re Encryption (CIBPRE), as well as its IND-sID-CPA security definitions, is a novel sort of PRE idea. The CIBPRE is a generic notion that includes Conditional PRE (CPRE), Identity-based PRE (IPRE), and Broadcast PRE capabilities (BPRE). The IND-sID-CPA security definition of CIBPRE incorporated the CPRE, IPRE, and BPRE security standards.

H. Li et al: In this study, we presented a concrete dIBAEKS system and introduced the concept of designated-server identity-based authenticated encryption with keyword search. On the basis of a basic number-theoretic assumption, we demonstrated that it is secure against inside offline KGA and achieves required testability. To satisfy the CCA-type designated testability, the scheme could be slightly altered. We also demonstrated how to improve the scheme's efficiency by modifying it to operate with asymmetric bilinear pairing. To ensure users' privacy, dIBAEKS can be used with an encrypted email system. However, because both ciphertexts and trapdoors are linked to the identity of the sender, our dIBAEKS and dIBAEKS-3 schemes have the property that a trapdoor can only be used to search across ciphertexts received by a certain sender.

J. Wei et al: In this paper, We developed a concept called RS-IBE to build a cost-effective and secure data sharing system in cloud computing, which allows identity revocation and ciphertext update simultaneously, preventing a revoked user from accessing previously shared data as well as subsequent shared data. In addition, a concrete RS-IBE construction is shown. Under the decisional l-DBHE assumption, the suggested RS-IBE technique is shown to be adaptively safe in the standard model.

C. Ge et al: In this work, we defined revocable identity-based broadcast proxy re-encryption, proposed a concrete construction under the definition and proved our scheme is CPA secure in the random oracle model. Our proposed solution is efficient and practicable, as evidenced by the property and performance comparison. Furthermore, our RIB-BPRE technique can be used to facilitate key revocation in a cloud context for a data-sensitive system, such as a volunteer-based genome research system. While this research has solved the problem of key revocation for data sharing, it has also raised several fascinating open questions, such as how to design a RIB-BPRE scheme without random oracles and how to support more expressive identities.

D. Derler et al: In this paper, We presented Bloom filter encryption as a type of puncturable encryption that tolerates a non-negligible correctness mistake. We demonstrated a variety of BFKEM structures. The first is a straightforward and highly efficient design based on concepts from the Boneh–Franklin IBE. It creates public keys with a fixed size. The second is a generic ciphertext construction based on CP-ABEs, in which a proper choice of CP-ABE results in constant size ciphertexts. However, in existing systems, those constant-size ciphertexts come at the expense of larger keys. The third is a general IBBE-based architecture that can be created with Delerablée's IBBE. This instantiation simultaneously yields constant size ciphertexts and compact public keys.

S. Krenn et al: In this study, We look at forward secrecy, which is an appealing cryptographic characteristic for PRE. The proxy in our forward-secret PRE (fs-PRE) specification updates the re-encryption keys on a regular basis and permanently deletes previous copies, while the delegator's public key remains constant.

As a result, ciphertexts from previous periods can no longer be re-encrypted and, more importantly, cannot be decrypted at the delegatee's end. Delegators' secret keys evolve as well, therefore they won't be able to decrypt old ciphertexts after their key material from previous periods has been lost. This has direct use in short-term data/message-sharing contexts, as we will demonstrate.

T. V. X. Phuong et al: In this paper, We introduce a Puncturable Proxy Re-Encryption Scheme for asynchronous communication that supports forward secrecy. Because a participant safely delegated computational demand operations to interact with numerous parties to a proxy, the proposed technique is well-suited to many-to-many communication, such as a group messaging service (i.e. a message server). As a result, it enables a large number of people to communicate effectively in a group setting.

S.-F. Sun et al:In this study,A generic method for creating public-key puncturable key encapsulation mechanisms is proposed. By combining it with the usual decapsulation approach, we gain the first modular way of constructing full-blown puncturable encryption with minor correctness issues. Finally, we offer a key-homomorphic identity-based revocable key encapsulation mechanism with expanded correctness, which is a new notion in identity-based revocable encryption. We also describe a number of different implementations of the novel concept, resulting in four distinct public-key puncturable encryption systems.

S. Garg et al: In this work,We introduce the concept of registration-based encryption (RBE), which aims to eliminate the necessity for parties to invest trust in the private-key generator in an IBE scheme. Users sample their own public and secret keys in an RBE scheme. There will also be a "key curator" whose sole responsibility will be to collect all of the registered users' public keys and update the "short" public parameter whenever a new user joins the system. Encryption of a specific recipient can still be done using the recipient's identification as well as any public parameters published after the recipient's registration. Decryption necessitates the usage of certain supplementary data to link users' public (and secret) keys to public parameters.

III. PROPOSED SYSTEM

1) Designated-server identity-based authenticated encryption.
2) Keyword search for encrypted emails is not construct a more flexible proposed scheme in which a trapdoor can be used to search over multiple users' encrypted data.
3) Adaptive security is not used in Puncturable Proxy Re-Encryption supporting to Group Messaging Service.
4) Revisiting Proxy Re-encryption: Forward Secrecy, Improved Security,and Applications in that also does not have to be online when ciphertexts are re-encrypted for her by the proxy & not cover the third dimension.

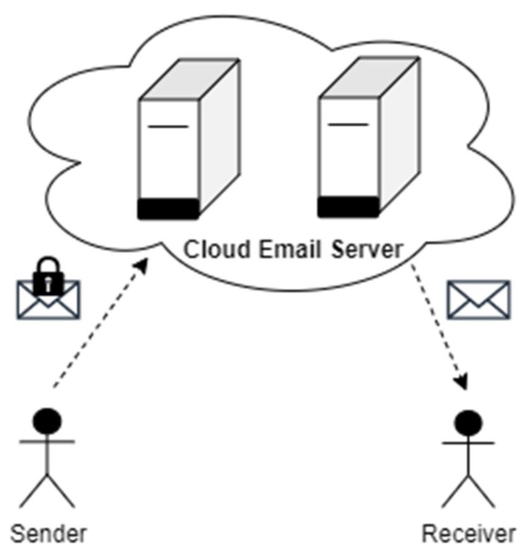

Figure 1. System Architecture

The above framework encrypted email service is made much easier for users. Users can encrypt cloud emails using their email accounts. The correctness of the underlying fs-PIBE scheme and symmetric encryption scheme is the source of its correctness. Furthermore, the security of our framework can be decreased to that of fsPIBE and SE by correctly implementing the hybrid encryption pattern. As a result, even if the cloud email server is corrupted, all cloud emails maintain their confidentiality. Our approach differs from past encrypted email systems in that it delivers practical forward secrecy while maintaining usability.

IV. METHODOLOGY

Identity based encryption

1) IBE.Setup: A fully trusted PKG runs the setup algorithm. This technique generates bilinear groups with a random exponent given a security parameter, the total number of time intervals, and the maximum number of tags allowed to attach to each ciphertext.
2) IBE.KeyGen:The PKG also manages the secret key generation algorithm.
3) IBE.Puncture: A user runs the puncture algorithm without interacting with it.
4) IBE.Update: A user can also run the secret key update procedure without interacting with it.
5) IBE.Encrypt: A sender who wants to send a message to a recipient with an identification ID uses this algorithm.
6) IBE.Decrypt: A receiver with an identification ID performs this algorithm

Algorithm

AES (advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys.

Rijendeal was founder. In this drop we are using it to encrypt the data owner file.

Input:

128_bit /192 bit/256 bit input (0, 1)

Secret key (128_bit) +plain text (128_bit).

Process:

10/12/14-rounds for-128_bit /192 bit/256 bit input

Xor state block (i/p)

Final round:10,12,14

Each round consists: sub byte, shift byte, mix columns, add round key.

Output:

cipher text(128 bit)

V. RESULTS AND DISSCUSSION

Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i3-2120 CPU @ 3.30GHz, 4GB memory, Windows 7, MySQL 5.1 backend database and Jdk 1.8. The application is web application used tool for design code in Eclipse and execute on Tomcat server.

In this subsection, our System evaluates the performance of the proposed scheme by several experiments.

1) *Results 1:*

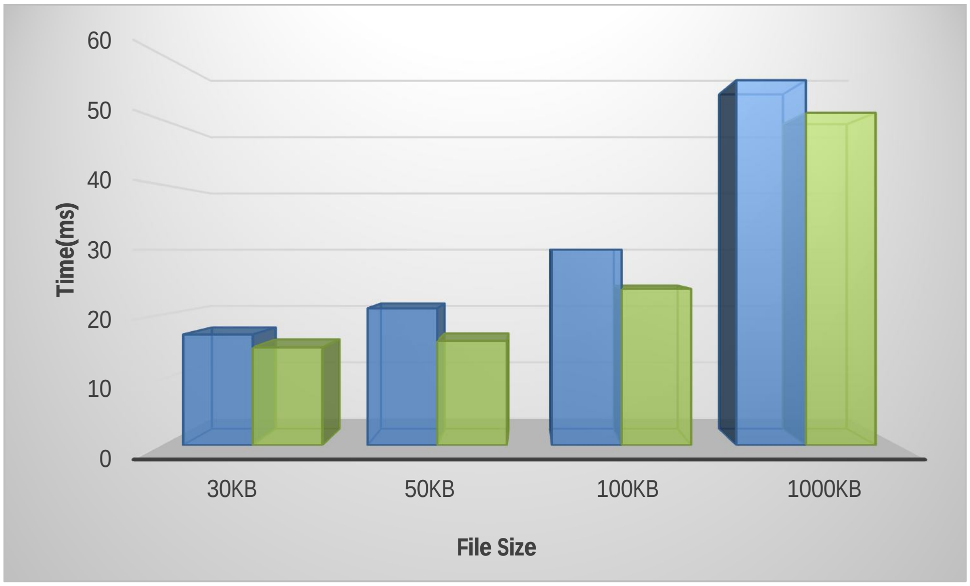

Figure 1: Encryption and Uploading Time

Table 1: Show File Size and Encryption and Uploading Time

Index Number	size (KB)	RSA	IBE
1	30	31ms	28ms
2	50	36ms	31ms
3	100	63ms	58ms
4	1000	102ms	93ms

2) Results 2:

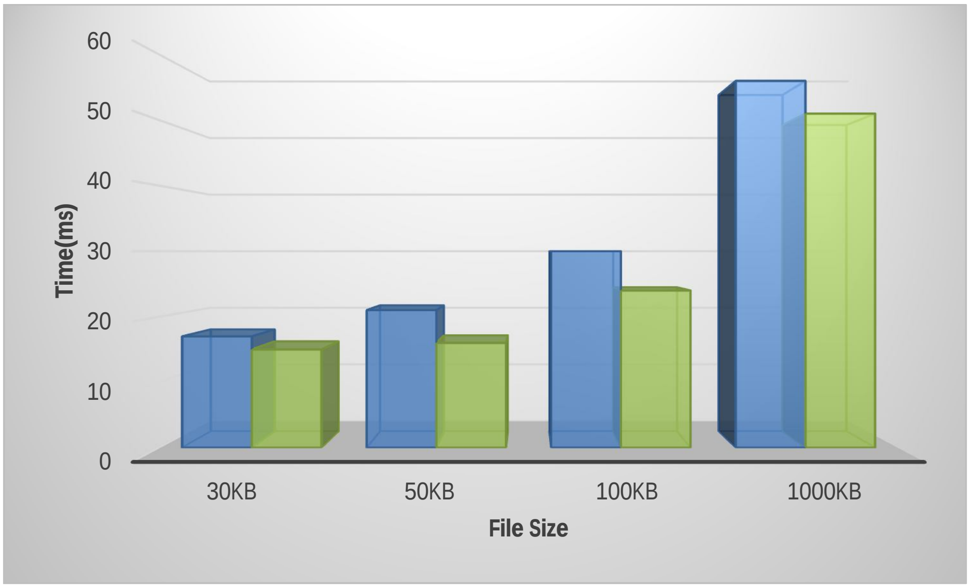

Figure 2: Decryption and Downloading Time

Table 2:Decryption and Downloading Time

Index Number	size (KB)	RSA	IBE
1	30	12ms	9ms
2	50	16ms	12ms
3	100	26ms	21ms
4	1000	52ms	46ms

VI. CONCLUSION

In this paper, we offer a novel cryptographic fundamental called forward-secure puncturable identity-based encryption technique to capture practical forward secrecy of cloud email systems, which does not require the assistance of PKIs or the synchronisation of the email sender and receiver. To be more specific, we clarify the syntax and security concept of fs-PIBE before presenting a framework for encrypted cloud email systems.

REFERENCES

[1] D. Poddebniak, C. Dresen, J. Müller, F. Ising, S. Schinzel, S. Fried berger, J. Somorovsky, and J. Schwenk, "Efail: breaking s/mime and openpgp email encryption using exfiltration channels," in 27th USENIX Security Symposium, 2018, pp. 549–566.

[2] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, "Conditional identity based broadcast proxy re-encryption and its application to cloud email," IEEE Transactions on Computers, vol. 65, no. 1, pp. 66–79, 2016.

[3] H. Li, Q. Huang, J. Shen, G. Yang, and W. Susilo, "Designated server identity-based authenticated encryption with keyword search for encrypted emails," Information Sciences, vol. 481, pp. 330–343, 2019.

[4] J. Wei, W. Liu, and X. Hu, "Secure data sharing in cloud com puting using revocable-storage identity-based encryption," IEEE Transactions on Cloud Computing, vol. 6, no. 4, pp. 1136–1148, 2018.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

[5] C. Ge, Z. Liu, J. Xia, and L. Fang, “Revocable identity-based broadcast proxy re-encryption for data sharing in clouds,” IEEE Transactions on Dependable and Secure Computing, pp. 1–1, 2019.
[6] D. Derler, T. Jager, D. Slamanig, and C. Striecks, “Bloom filter encryption and applications to efficient forward-secret 0-rtt key exchange,” in Advances in Cryptology–EUROCRYPT 2018. Springer, 2018, pp. 425–455.
[7] D. Derler, S. Krenn, T. Lorünser, S. Ramacher, D. Slamanig, and C. Striecks, “Revisiting proxy re-encryption: forward secrecy, improved security, and applications,” in IACR International Conference on Public-Key Cryptography–PKC 2018. Springer, 2018, pp. 219–250.
[8] T. V. X. Phuong, W. Susilo, J. Kim, G. Yang, and D. Liu, “Puncturable proxy re-encryption supporting to group messaging service,” in 24th European Symposium on Research in Computer Security (ESORICS 2019). Springer, 2019, pp. 215–233.
[9] S.-F. Sun, A. Sakzad, R. Steinfeld, J. K. Liu, and D. Gu, “Public-key puncturable encryption: Modular and compact constructions,” in IACR International Conference on Public-Key Cryptography–PKC 2020. Springer, 2020, pp. 309–338.
[10] S. Garg, M. Hajiabadi, M. Mahmoody, and A. Rahimi, “Registration-based encryption: Removing private-key generator from ibe,” in Theory of Cryptography–TCC 2018. Springer, 2018, pp. 689–718.