e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 12, December 2024

Impact Factor: 7.521

☎ 6381 907 438 6381 907 438 ijmrset@gmail.com www.ijmrset.com

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A Blended Cloud Email Looking and Separating Plan Thinking about Stowed away System

Mr.A.Lakshmipathi Rao[1], B.Revanth Kumar[2], B.Shanthi Priya[3], D.Deepika[4]

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India[1]

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India[2,3,4]

ABSTRACT: With the rapid growth of cloud email services, email encryption is beginning to be used more and more to alleviate concerns about cloud privacy and security. However, this increase in usage invites the problem of how to search and filter encrypted emails effectively. Searchable public key encryption is a popular technology to solve encrypted email searching, but encrypted email filtering is still an open problem. We propose a Blended cloud email looking and separating plan thinking about stowed away system as a new solution. It enables the recipient to search the encrypted cloud email keywords and allows the email filtering server to filter the encrypted email content when receiving the email, as the traditional email keyword filtering service. Our hidden policy scheme is constructed by Composite order bilinear groups and proven secure by dual system encryption methodology. Our scheme can be applied to other scenarios such as file searching and filtering and has certain practical value.

I. INTRODUCTION

The total number of business and consumer emails sent and received per day will exceed 319 billion in 2021 and is forecast to grow to over 376 billion by year-end 2025. Cloud-based email services are seeing rapid growth. The benefits of cloud adoption are clear to all organizations, and an increasing number of organizations, of all sizes, are choosing to migrate to cloud email and collaboration services. Cloud email providers are beginning to provide more security features, such as email encryption, archiving, and other security related services, which are helping to ease users concerns about cloud privacy and security. Email encryption also creates some problems, such as how users are to search for emails without needing bothersome decryption or how the relevant servers are supposed to filter the content of emails (email-related laws in every country or region require the filtering of emails, such as spam, spam containing malicious code, etc.). Moreover, in searching and filtering, cloud servers cannot obtain information about the content of emails. Thus, the main problem we are facing now is how to make it as easy for users to search and filter for encrypted email as it is to search and filter for unencrypted ones in the traditional system. Searchable public key encryption was proposed to address this problem. Searchable encryption is divided into searchable symmetric encryption and searchable public key encryption. Searchable public key encryption is suitable for encrypted email search scenarios. The first to put forward the notion of a public key encryption scheme with keyword search (PEKS), which has application in identity based encryption (IBE) email system. This scheme allows gateways in communication systems to retrieve and determine whether the received email contains keywords to be searched. This solution created the use of searchable encryption technology to solve the searching problem of encrypted email. Subsequently, many PEKS schemes claim to be used in encrypted email searching. Recently, there were some PEKS schemes for encrypted email. Xu et al. proposed an encrypted email multi-keyword search scheme with hidden structures. Li et al. Proposed a new notion called designated-server identity-based authenticated encryption with keyword search for encrypted emails. Proposed a scheme supporting conjunctive keywords search without keyword field. The main security problem of searchable public key encryption is offline keyword guessing attack (KGA) that defined for PEKS. Proved that the sufficient condition for resisting keyword guessing attack is the indistinguishability of trapdoor. All three schemes prove the security of keyword trapdoor so that they can resist KGA. However, these schemes did not consider the filtering of encrypted email. Now encrypted email filtering is still an open problem. There have also been some PEKS schemes that have claimed to support encrypted email filtering, but they did not provide a detailed explanation on how to do so. Proposed an abstract and general encrypted email filtering scheme model. Email users could use some partially trusted proxy servers to filter out all encrypted emails recognized as spam according to their own requirements with their scheme. This process achieves the seemingly conflicting goal of hiding the email content on the proxy server and allowing the proxy server to determine whether the email is spam according to the user's own settings.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Unfortunately, there are only two paragraphs of text description and a schematic diagram. However, we can see that their scheme model uses searchable encryption to solve this problem. Inspired by this, we came up with a solution. We only need to make the filtering server a particular recipient to solve the problem of encrypted email searching and filtering. Therefore, we decided to design an encrypted email searching and filtering scheme based on attribute-based encryption with keyword search (ABKS). Our Contribution: Under current circumstances, it would be difficult for an encrypted email to be searched by multiple recipients and filtered by a filter server. However, attribute-based encryption with keyword search, especially ciphertext-policy attribute-based encryption with keyword search (CPABKS), can solve this problem. Therefore, our solution is to design a CPABKS scheme for encrypted cloud email scenarios, aiming to enable both filtering and searching simultaneously. An additional recipient list is specially created when sending an email, and the filter server is added as the recipient. Attributes of users on this recipient list will form a set used as the access structure P of the encrypted keyword index. This way, only the recipients whose attributes meet the control policy can be successfully searched. The filter server can filter keywords within encrypted emails successfully, as the server is added to the additional recipient list. In order to resist KGA and make the scheme obtain full security, the Composite order bilinear groups are constructed to realize the policy hiding. According to this direction of thinking, we become the first to propose a hidden policy ciphertext-policy attribute-based encryption with keyword search (HPCPABKS) scheme to solve the problem of encrypted email searching and filtering. Our scheme is not filtering on the email gateway. Like some free email, it only provides recipient server-side filtering. Our scheme has the following advantages:

Innovatively applies the ABKS design to the encrypted cloud email scenario. The sender creates an additional list of recipients for searching and filtering and adds the recipient filtering server to this list of recipients. The user' attributes in this recipient list are used as the access control policy of the encrypted keyword index. Therefore, the recipients can search keywords by their attributes, and, in turn, the recipient filtering server can filter keywords by its own attributes. Our scheme supports copying and grouping multiple emails at the same time and uses only one encrypted keyword index without any additional encrypted index computation costs.

In our solution, we apply the dual system encryption methodology and the hidden policy to enhance privacy and obtain full security. It can resist KGA and satisfy the confidentiality of the encrypted email system.

Our scheme has certain practical application value and can further expand anti-virus email protection functions according to malicious email reporting, email attachment processing. It is not only more suitable for encrypted cloud email searching and filtering scenarios, but it can also be extended to encrypted file searching and filtering, as well as other application scenarios.

II. LITERATURE SURVEY

In their 2021 paper, D. Boneh and M. Franklin discussed the concept of identity-based encryption (IBE) to provide a fully functional encryption scheme. The proposed scheme is chosen ciphertext secure in the random oracle model and is on a variant of the computational Diffie-Hellman problem. Their system utilizes bilinear maps between groups, with the Weil pairing on elliptic curves as an example. They provide precise definitions for secure identity-based encryption schemes and highlight several practical applications of these systems.

In their 2021 paper, D. Boneh, G. Di Crescenzo, and R. Ostrovsky analysed the problem of searching encrypted data using public key systems. They introduced Public Key Encryption with Keyword Search (PEKS) to enable keyword-specific searches on encrypted emails without exposing other information. For instance, an email gateway can detect keywords like “urgent” in emails encrypted under a recipient’s public key. They presented several constructions for this mechanism, allowing scenarios where Alice could enable a mail server to identify emails with specific keywords while ensuring the server learns nothing beyond the presence based for those keywords.

In their 2021 paper, Q. Tang and L. Chen highlighted potential vulnerabilities in Public-key Encryption with Keyword Search (PEKS), such as the offline keyword guessing attack. To address this, they proposed Public-key Encryption with Registered Keyword Search (PERKS), which requires keyword preregistration. While this introduces some limitations, their approach enhances security by preventing offline keyword guessing. They also introduced a PERKS construction that supports batch processing of multiple tags, reducing computational complexity and proving its security.

In their 2021 paper, D. Boneh, A. Sahai, and B. Waters explored functional encryption as a transformative approach to public-key cryptography. They discussed how public-key encryption revolutionized secure communication, allowing two parties to exchange encrypted data without prior secret keys. They emphasized its widespread application in securing web communications, voice traffic, and storage systems. They traced its evolution, crediting foundational ideas to Diffie and Hellman, and highlighted the contemporary importance of these systems in secure information sharing.

In their 2021 paper, M. Bartoletti and L. Pompianu conducted an empirical analysis of smart contracts, focusing on their platforms, applications, and design patterns. They described smart contracts as tamper-resistant programs executed on networks of mutually distrusting nodes. Their study compared platforms like Bitcoin and Ethereum, quantifying smart contract usage across various domains. By analysing programming patterns in Ethereum, they provided insights into the design and implementation of smart contracts and their potential for applications such as financial services.

In their 2020 paper, S. Wang, D. Zhao, and Y. Zhang discussed a searchable attribute-based encryption scheme with attribute revocation tailored for cloud storage. Their scheme combines keyword search and access control to provide secure and flexible data retrieval. The keyword search mechanism is attribute-based, ensuring that only authorized users can decrypt retrieved ciphertexts. Supporting multiple keyword searches, their scheme is practical and secure under the decisional bilinear Diffie-Hellman exponent (q-BDHE) and decisional Diffie-Hellman (DDH) assumptions.

Existing System:

The total number of business and consumer emails sent and received per day will exceed 319 billion in 2021, and is forecast to grow to over 376 billion by year-end 2025. Cloud-based email services are seeing rapid growth. The benefits of cloud adoption are clear to all organizations, and an increasing number of organizations, of all sizes, are choosing to migrate to cloud email and collaboration services. Cloud email providers are beginning to provide more security features, such as email encryption, archiving, and other security related services, which are helping to ease users' concerns about cloud privacy and security. Email encryption also creates some problems, such as how users are to search for emails without needing bothersome decryption or how the relevant servers are supposed to filter the content of emails. Moreover, in searching and filtering, cloud servers cannot obtain information about the content of emails. Thus, the main problem we are facing now is how to make it as easy for users to search and filter for encrypted email as it is to search and filter for unencrypted ones in the traditional system.

Proposed System:

In this paper, we propose a Blended Cloud email looking and separating plan thinking about stowed away system as a new solution. It enables the recipient to search the encrypted cloud email keywords and allows the email filtering server to filter the encrypted email content when receiving the email, as the traditional email keyword filtering service. Our hidden policy scheme is constructed by Composite order bilinear groups and proven secure by dual system encryption methodology. Our scheme can be applied to other scenarios such as file searching and filtering and has certain practical value.

Proposed System Advantage:

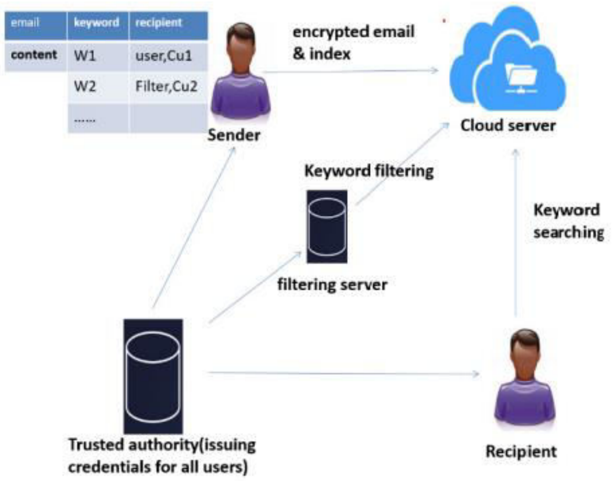
- Traditional email keyword filtering service.
- Scheme can be applied to other scenarios such as file searching and filtering and has certain practical value.
- Encrypted cloud email searching and filtering.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

System Architecture



email	keyword	recipient
content	W1	user,Cu1
	W2	Filter,Cu2
	......	

Figure 1: System Architecture

III. METHODOLOGY

The system is organized into key modules, each designed to handle distinct aspects of the process. The modules are as follows:Data Collection

- Sender
- Receiver
- Trusted Authority
- Filtering Server

3.1 Module Descriptions

1. Sender

To implement a system that allows a sender to register, send emails, and view emails, you can think about designing a simple email application.

2. Receiver

To build a system that allows a receiver to register, view emails, and read emails, you can follow a similar structure to the sender's system but with a focus on receiving and managing incoming emails.

3. Trusted Authority

Creating a system that involves a **trusted authority** to manage and oversee user email activities, while providing the ability to view user attributes and emails, requires a well-thought-out architecture. This setup typically focuses on security, privacy, and user management, often found in organizational or enterprise email systems

4. Filtering Server

Implementing a **filtering server** that can filter attributes for various purposes (such as data retrieval, analysis, or access control) involves creating a system that allows users or administrators to apply specific criteria to retrieve or manipulate data based on defined attributes.

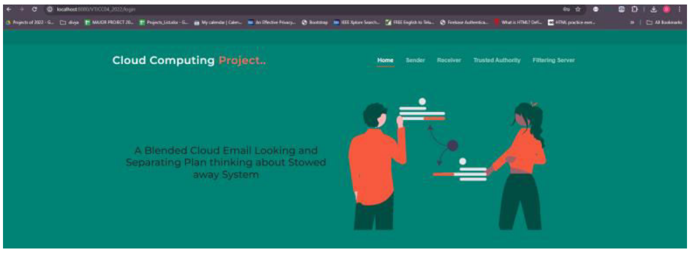
IV. IMPLEMENTATION

The system is implemented in web environment using struts framework. The apache tomcat is used as the web server and windows xp professional is used as the platform. Interface the user interface is based on Struts provides HTML Tag.

This project is implements like web application using Python and the Server process is maintained using the SOCKET & SERVERSOCKET and the Design part is played by Cascading Style Sheet.

V. EXPERIMENTAL RESULTS

Home page

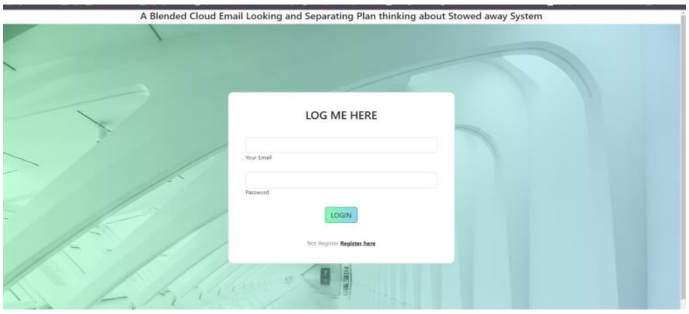


A Blended Cloud Email Looking and Separating Plan thinking about Stowed away System

Figure 2:Home Page

This is the default landing page, It provides an overview of the project and its purpose, highlighting the system's functionality related to cloud email management and data separation.

Login Page


A Blended Cloud Email Looking and Separating Plan thinking about Stowed away System

LOG ME HERE

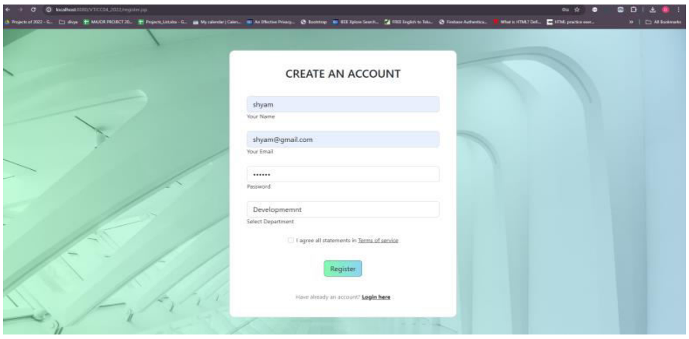
Your Email

Password

Figure 3:Login Page

In the login page user has to enter his/her username and password to login to the page.

User Register Page


CREATE AN ACCOUNT

shyam
Your Name

shyam@gmail.com
Your Email

••••••
Password

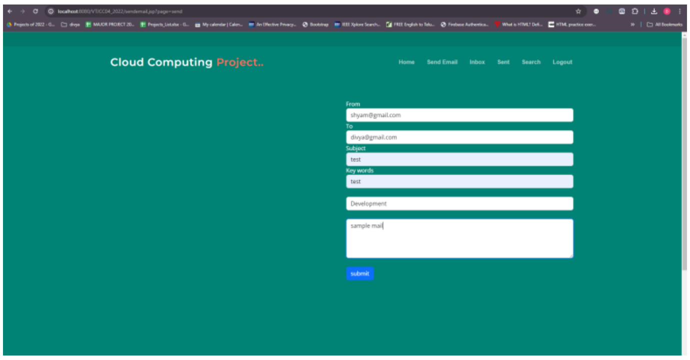
Developmemnt
Select Department

□ I agree all statements in Terms of service

Figure 4:User Register Page

Enter your details, including your full name, a valid email address, a strong password, and your department. Agree to the platform's terms of service and click "Register" to create your account. Existing users can click "Login here" to access their accounts with their credentials.

Send Email

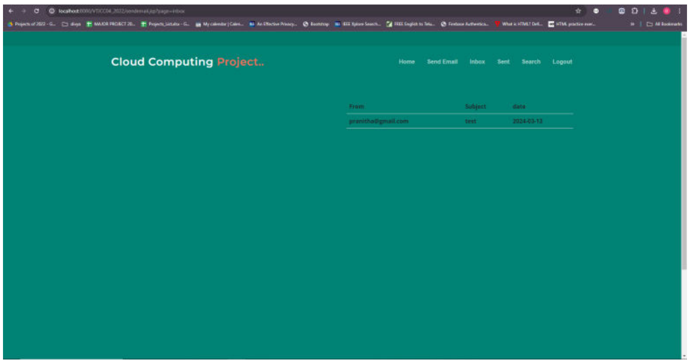


From: shyam@gmail.com
To: divya@gmail.com
Subject: test
Key words: test
Development
sample mail

Figure 5:Send Email

Enter the sender's email address in the "From" field and the recipient's email address in the "To" field, ensuring both are valid and accurate. Add a concise title in the "Subject" field to convey the purpose of the email. Include relevant keywords for filtering or organizing and write a message in the email content area. Click "Submit" to send the email, and you may receive a confirmation upon successful delivery.

View Email



From	Subject	date
pranitha@gmail.com	test	2024-03-13

Figure 6:View Email

Access the Inbox from the navigation bar to view all received emails. Each email is listed with details such as the sender's email address, subject line, and the date it was received. Click on any email to open it and view its full content, including the message body, attachments, and other details.

VI. CONCLUSION

Fake and clone profiles have become a very serious problem in online social networks. We hear some or the other threats caused by these profiles in everyday life. So a detection method has been proposed which can find both fake and clone Twitter profiles. For fake detection, a set of rules were used which when applied can classify fake and genuine profiles. Clone detection was carried out using Similarity Measures and C4.5 algorithm and a comparison was made to check the performance. Clone detection using Similarity Measures worked better than C4.5 and was able to detect most of the clones which were fed into the system.

VII. FUTURE ENHANCEMENT

In the future, we need to improve the scheme further to make it more rapid and straightforward without reducing the security. In addition, our next work will also focus on multi keyword search and other query expression capabilities.

REFERENCES

[1] Email Statistics Report, 2021-2025 Executive Summary. Accessed: Mar. 3, 2021. [Online]. Available: https://www.radicati.com/wp/ wpcontent/uploads/2020/12/
[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Proc. CRYPTO, vol. 2139, 2001, pp. 213–229.
[3] D. Boneh, G. Di Crescenzo, and R. Ostrovsky, "Public key encryption with keyword search," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Interlaken, Switzerland, 2004, pp. 506–522.
[4] Q. Tang and L. Chen, "Public-key encryption with registered keyword search," in Proc. Eur. Public Infrastructure. Workshop. Berlin, Germany: Springer, 2009, pp. 163–178.
[5] D. Boneh, A. Sahai, and B. Waters, "Functional encryption: A new vision for public-key cryptography," Common. ACM, vol. 55, no. 11, pp. 58–64, 2012.
[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. 24th Annu. Int. Conf. Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer, 2005, pp. 457–473.
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Compute. Common. Secure, 2006, pp. 89–98.
[8] N. Attrapadung and B. Libert, "Expressive key-policy attribute-based encryption with constant-size cipher texts," in Proc. 14th Int. Conf. Pract. Theory Public Cryptogr. Berlin, Germany: Springer, 2011, pp. 90–108.
[9] J. Li, Q. Yu, and Y. Zhang, "Key-policy attribute-based encryption against continual auxiliary input leakage," Inf. Sci., vol. 470, pp. 175–188, Jan. 2019.
[10] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," IEEE Trans. Services Comput., vol. 10, no. 5, pp. 785–796, Jan. 2016.
[11] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, "User collision avoidance CP-ABE with efficient attribute revocation for cloud storage," IEEE Syst. J., vol. 12, no. 2, pp. 1767–1777, Jun. 2018.
[12] J. Li, N. Chen, and Y. Zhang, "Extended file hierarchy access control scheme with attribute based encryption in cloud computing," IEEE Trans. Emerg. Topics Compute. vol. 9, no. 2, pp. 983–993, Apr./Jun. 2021.
[13] Q. Zheng, S. Xu, and G. Ateniese, "VABKS: Verifiable attribute-based keyword search over outsourced encrypted data," in Proc. IEEE Conf. Comput. Common. Toronto, ON, Canada, Apr. 2014, pp. 522–530.
[14] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," in Proc. IEEE Conf. Comput. Commun., Toronto, ON, Canada, Apr. 2014, pp. 226–234.
[15] S. Wang, D. Zhao, and Y. Zhang, "Searchable attribute-based encryption scheme with attribute revocation in cloud storage," PLoS ONE, vol. 12, no. 8, Aug. 2017, Art. no. e0183459. [16] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in Proc. 6th Int. Conf. Appl. Cryptogr. Netw. Secur., New York, NY, USA, 2008, pp. 111–129.
[17] J. Lai, R. H. Deng, and Y. Li, "fully secure ciphertext-policy hiding CPABE," in Proc. 7th Int. Conf. Inf. Secur. Pract. Exper., Guangzhou, China, 2011, pp. 24–39.
[18] X. Li, "Efficient ciphertext-policy attribute based encryption with hidden policy," in Proc. 5th Int. Workshop Internet Distrib. Comput. Syst., Melbourne, VIC, Australia, 2012, pp. 146–159.
[19] J. Lai, R. H. Deng, and Y. Li, "Expressive CP-ABE with partially hidden access structures," in Proc. 7th ACM Symp. Inf., Compute. Common. Secure. Seoul, South Korea, 2012, pp. 18–19.
[20] S. Qiu, J. Liu, Y. Shi, and R. Zhang, "Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack," Sci. China Inf. Sci., vol. 60, no. 5, May 2017, Art. No. 052105.
[21] A. Wu, D. Zheng, Y. Zhang, and M. Yang, "Hidden policy attributebased data sharing with direct revocation and keyword search in cloud computing," Sensors, vol. 18, no. 7, pp. 2–17, 2018.

[22] A. Lewko, "fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," Eurocrypt, vol. 6110, pp. 62–91, Dec. 2010.
[23] B. Waters, "Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 5677, S. Halevi, Ed. Berlin, Germany: Springer, 2009, pp. 619–636.
[24] A. Lewko and B. Waters, "new techniques for dual system encryption and fully secure HIBE wITH SHORT CIPHERtexts," in Theory of Cryptography (Lecture Notes in Computer Science), vol. 5978, D. Micciancio, Ed. Berlin, Germany: Springer, 2010, pp. 455–479.
[25] D. Boneh, E. J. Goh, and K. Nissim, "evaluating 2-DNF formulas on ciphertexts," in Theory of Cryptography, vol. 3378, J. Kilian, Ed. Berlin, Germany: Springer, 2005, pp. 325–341. [26] V. Goyal, A. Jain, and O. Pandey, "Bounded ciphertext policy attribute based encryption," in Proc. 35th Int. Colloq. Autom., Lang. Program., 2008, pp. 1–5.
[27] J. Byun, H. Rhee, and H. Park, "Off-line keyword guessing attacks on recent keyword search schemes over encrypted data," in Proc. Secure Data Manage., 2006, pp. 75–83.
[28] X. Liu, T. Lu, X. He, X. Yang, and S. Niu, "Verifiable attribute-based keyword search over encrypted cloud data supporting data deduplication," IEEE Access, vol. 8, pp. 52062–52074, 2020.
[29] Y. Zhang, Y. Li, and Y. Wang, "Efficient conjunctive keywords search over encrypted E-Mail data in public key setting," Appl. Sci., vol. 9, no. 18, p. 3655, Sep. 2019.
[30] H. Li, Q. Huang, J. Shen, G. Yang, and W. Susilo, "Designated-server identity-based authenticated encryption with keyword search for encrypted emails," Inf. Sci., vol. 481, pp. 330–343, May 2019.
[31] P. Xu, S. Tang, P. Xu, Q. Wu, H. Hu, and W. Susilo, "Practical multikeyword and Boolean search over encrypted E-mail in cloud server," IEEE Trans. Services Compute., vol. 14, no. 6, pp. 1877–1889, Nov. 2021.
[32] J. Chen, "Cloud storage third-party data security scheme based on fully homomorphic encryption," in Proc. Int. Conf. Netw. Inf. Syst. Comput. (ICNISC), Apr. 2016, pp. 155–159. [33] F. Han, J. Qin, H. Zhao, and J. Hu, "A general transformation from KPABE to searchable encryption," Future Gener. Compute. Syst., vol. 30, pp. 107–115, Jan. 2014.
[34] H. S. Rhee, W. Susilo, and H.-J. Kim, "Secure searchable public key encryption scheme against keyword guessing attacks," IEICE Electron. Exp., vol. 6, no. 5, pp. 237–243, 2009.
[35] J. Li, X. Lin, Y. Zhang, and J. Han, "KSF-OABE: Outsourced attribute based encryption with keyword search function for cloud storage," IEEE Trans. Services Compute., vol. 10, no. 5, pp. 715–725, Sep./Oct. 2017.
[36] J. Ulrich, G. Murray, and G. Carenini, "A publicly available annotated corpus for supervised email summarization," in Proc. AAAI Workshop, 2008, pp. 77–82.
[37] The Java Pairing Based Cryptography Library. Accessed: Jun. 18, 2021. [Online]. Available: http://gas.dia.unisa.it/projects/jpbc/.

.

INTERNATIONAL JOURNAL OF
MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com