AN ENCRYPTED CLOUD EMAIL SEARCHING AND FILTERING SCHEME BASED ON HIDDEN DATA WITH KEYWORD SEARCH

Wajeeha Samreen Saleem[1], Jothikumar. R[2], Sridhar Gummalla[3]
[1]Research Scholar, Department of Computer Science and Engineering, SCET, Hyderabad, Telangana
perky.charm@yahoo.com
[2]Professor, Department of Computer Science and Engineering, SCET, Hyderabad, Telangana.
drjothikumarr@gmail.com
[3]Professor, Department of Computer Science and Engineering, SCET, Hyderabad, Telangana.
Sridhar_gummalla@yahoo.com

ABSTRACT

With the speedy advancement of cloud email organizations, email encryption is beginning to be used progressively more to moderate stresses over cloud insurance and security. In any case, this extension being used invites the issue of how to look and channel mixed messages, as a matter of fact. Available public key encryption is a notable development to handle mixed email looking; yet encoded email isolating is at this point an open issue. We propose a mixed cloud email looking and filtering plan considering hidden away procedure cipher text methodology trademark-based encryption with watchword search as another game plan. It enables the recipient to glance through the encoded cloud email watchwords and licenses the email isolating server to channel the mixed email content while receiving the email, as the standard email expression filtering organization. Our mysterious course of action contrive is worked by composite solicitation bilinear social affairs and showed secure by twofold system encryption approach. Our arrangement can be applied to various circumstances, for instance, record looking and filtering and has explicit realistic worth.

1. INTRODUCTION

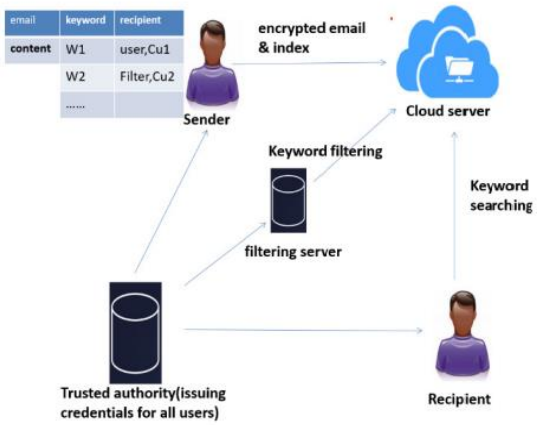
The complete number of business and shopper messages sent and got each day will surpass 319 billion of every 2021, and is estimate to develop to more than 376 billion by year-end 2025. Cloud-based email administrations are seeing quick development. The advantages of cloud reception are obvious to all associations, and a rising number of associations, everything being equal, are deciding to relocate to cloud email and coordinated effort administrations. Cloud email suppliers are starting to give greater security highlights, like email encryption, documenting, and other security related administrations, which are assisting with facilitating clients' interests about cloud protection and security. Email encryption additionally makes a few issues, for example, how clients are to look for messages without requiring troublesome decoding or how the important servers should channel the substance of messages (email-related regulations in each nation or locale require the sifting of messages, for example, spam, spam containing noxious code, and so on.). Also, in looking and sifting, cloud servers can't get data about the substance of messages. Consequently, the primary issue we are confronting now is the means by which to make it as simple for clients to look and channel for encoded email for all intents and purposes to look and channel for decoded ones in the conventional framework. Accessible public key encryption was proposed to resolve this issue. Accessible encryption is separated into accessible symmetric encryption and accessible public key encryption. Search capable public key encryption is appropriate for scrambled email search situations. Bonehet al. were quick to advance the thought of a public key encryption plot with catchphrase search (PEKS), which has application in character-based encryption (IBE) email framework. This plan permits doors in correspondence frameworks to recover and decide if they got email contains watchwords to be looked. This arrangement made the utilization of accessible encryption innovation to take care of the looking through issue of scrambled email. Along these lines, numerous PEKS plans guarantee to be utilized in encoded email looking. As of late, there were some PEKS plans for encoded email. Proposed a scrambled email multi-catchphrase search conspire with stowed away designs. Li et al. proposed another idea called assigned server personality based confirmed encryption with catchphrase look for encoded messages. Zhang et al. proposed a plan supporting conjunctive watchwords search without catchphrase field. The primary security issue of accessible public key encryption is disconnected catchphrase speculating assault (KGA) that Byun et al. characterized for PEKS. Rhee et al. demonstrated that the adequate condition for opposing watchword speculating assault is the in noticeability of hidden entrance. Every one of the three plans demonstrate the security of watchword hidden entryway so they can oppose KGA. Nonetheless, these plans didn't think about the sifting of encoded email. Presently scrambled email sifting is as yet an open issue. There have likewise been some PEKS plans that have professed to help scrambled email separating, yet they didn't give an itemized clarification on the most

proficient method to do as such. Boneh et al. proposed a theoretical and general scrambled email separating plan model. Email clients could utilize some somewhat confided in intermediary servers to sift through undeniably encoded messages perceived as spam as per their own necessities with their plan. This cycle accomplishes the apparently clashing objective of concealing the email content on the intermediary server and permitting the intermediary server to decide if the email is spam as indicated by the client's own settings. Tragically, there are just two passages of text portrayal and a schematic outline. Nonetheless, we can see that their plan model purposes accessible encryption to take care of this issue. Roused by this, we thought of an answer. We just have to make the separating server a specific beneficiary to tackle the issue of encoded email looking and sifting. Thusly, we chose to plan an encoded email looking and separating plan in light of characteristic based encryption with catchphrase search (ABKS).

2. RELATED WORK

The foundation of HPCPABKS can be followed back to Ascribe based encryption (ABE) proposed by Sahai and Waters. ABE is an expansion of customary public key encryption. The client can communicate how the person needs to share the information in the encryption calculation, make a few strategies as per the properties of the getting client, and offer the information as per these arrangements. The ABE plot is separated into ciphertext-strategy ABE (CPABE) and key-arrangement ABE (KPABE). In the CP-ABE plans, the beneficiary's key is related with the characteristic set, while the ciphertext contains the entrance strategy on the trait set. Just when the trait set related with the collector's key meets the entrance strategy contained in the ciphertext could it at any point be decoded. In the KPABE plans, the code text contains a bunch of traits. The key is related with the quality set's admittance strategy and must be decoded on the off chance that the property set of the ciphertext fulfills the entrance strategy related with the key. ABE is a viable answer for understand the protection of information sharing and security in the cloud stage climate. Be that as it may, in specific situations, to not uncover any delicate data in the entrance structure, the ABE plan ought to help a mysterious access design to ealize the secret strategy. Nishide et al. proposed two CPABE plans with a secret access control strategy. The client can conceal a subset of each characteristic's potential qualities in the ciphertext strategy to acknowledge fractional approach stowing away. Later work (for example likewise understood the stowing away of access control strategy, taking care of information classification assurance issues, and fine-grained admittance control in distributed storage. The past plans are totally founded on the particular model. In the specific model, the enemy needs to choose the entrance control pol cold to be tested before the framework instates the public boundaries. Lewko et al. first tackled this issue. They proposed a completely protected ABE framework utilizing the double framework encryption philosophy presented by Waters and methods utilized by Lewko et al. Nonetheless, these encryption plans don't uphold watchword search and can't look through information ciphertext.

3. METHODOLOGIES



System Architecture

We represent the based engineering of our plan in Figure 1. Our plan includes five elements: Believed power, Source, Email sifting server, Beneficiary, Cloud server. Every substance is presented as follows:

1. Confided in power: The Approval place creates a public key and expert key for the plan and produces a confidential property key for the beneficiary channel server and all the email clients. The client's confidential key is connected with his credits.

2. Shipper: from the beginning, the client of source fragments the con tents of an email into watchwords. The shipper then, at that point, makes an extra beneficiary rundown and adds all beneficiaries and the relating channel server to this beneficiary rundown. The shipper decides the entrance strategy as indicated by the properties of the beneficiaries and channel servers and utilizations the entrance strategy to scramble the watchword list. The email content is as yet scrambled with the first framework's encryption technique. At long last, the source sends the cipher text of the file and email to the cloud server.

3. Email sifting server: The email channel server keeps a boycott of catchphrases to be separated. It produces catchphrase hidden entrances as per the boycott and sends them to the cloud server to run the separating calculation to channel the recently gotten messages. The channel here really looks.

4. Beneficiary: to look for an email with a watchword in the as of late gotten email, the beneficiary will produce a catchphrase secret entryway and afterward send the catchphrase secret entrance to the cloud server for looking. On the off chance that the email contains catchphrases to look, the cloud server will present the email to the beneficiary.

4. PROPOSED ALGORITHM

➢ ENCRYPTED EMAIL FILTERING

Theoretical and general encoded email sifting plan model. Email clients could utilize some somewhat confided in intermediary servers to sift through completely encoded messages perceived as spam as per their own prerequisites with their plan. This cycle accomplishes the apparently clashing objective of concealing the email content on the intermediary server and permitting the intermediary server to decide if the email is spam as per the client's own settings. Sadly, there are just two passages of text portrayal and a schematic graph. Nonetheless, we can see that their plan model purposes accessible encryption to take care of this issue. Propelled by this, we thought of an answer. We just have to make the sifting server a specific beneficiary to tackle the issue of scrambled email looking and separating. Along these lines, we chose to plan a scrambled email looking and sifting plan in light of property-based encryption with watchword search (ABKS).

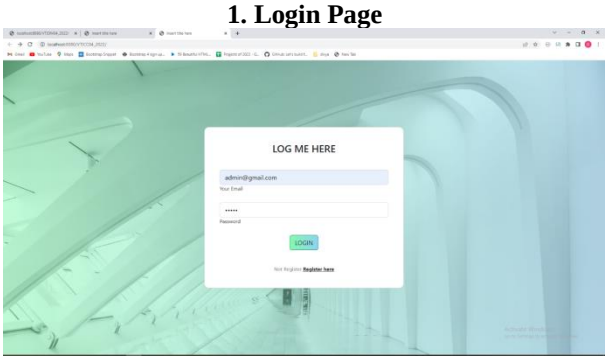
ATTRIBUTE-BASED KEYWORD SEARCH

The foundation of HPCPABKS can be followed back to Attribute based encryption (ABE) proposed by Sahai and Waters ABE is an expansion of customary public key encryption. The client can communicate how the person needs to share the information in the encryption calculation, make a few strategies as per the traits of the getting client, and offer the information as per these approaches. The ABE plot is separated into cipher text-strategy ABE (CPABE) and key-arrangement ABE (KPABE). In the CP-ABE plans, the beneficiary's key is related with the trait set, while the cipher text contains the entrance strategy on the property set. Creatively applies the ABKS plan to the scrambled cloud email situation. The source makes an extra rundown of beneficiaries for looking and separating and adds the beneficiary sifting server to this rundown of beneficiaries. The client' credits in this beneficiary rundown are utilized as the entrance control strategy of the encoded watchword file. Subsequently, the beneficiaries can look through watchwords by their properties, and, thusly, the beneficiary separating server can channel catchphrases by its own traits.

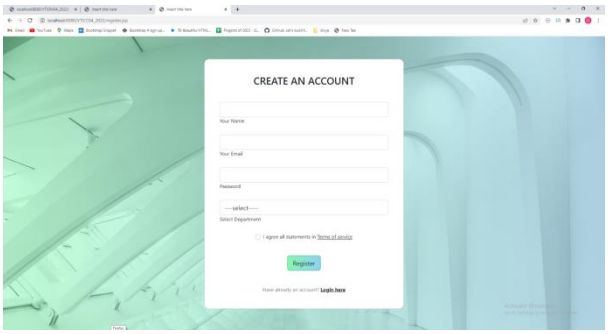
DATA MINING WITH PRIVACY

In this paper, we mainly focus on the integrity checking for data shared within a group. Suppose there is a scenario that a software engineer starts an open source project and calls on volunteers from the world to join the project. They work as a temporary team. All the codes of the project are stored on certain cloud server so that all the team members upload and modify the source code by Internet. The team may be very big, so it should be set up and managed efficiently. The volunteers may leave the team at any time, so the problem of user revocation from the team should be considered. The most important thing is that there need some way to guarantee the integrity of source codes on cloud sever. Motivated by such requirement, we propose a new RDPC scheme for data shared in a group. Different from previous work, our scheme is based on the certifcateless signature technique to avoid the problems of certificate management and key escrow. In our scheme, the group creator generates the partial key for each group user on behalf of key generation center. Each user selects a secret value privately. The private key of each group user contains two parts: a partial key and a secret value. All the data blocks are signed by group user to get corresponding authentication tags. During the data verification, all the tags are aggregated to decrease the computation and communication cost. Based on CDH and DL assumptions, we prove the security of our scheme. Besides, our scheme supports public verification and efficient user revocation. We implement our scheme and perform some experiments. The experiment results indicate that our scheme has good efficiency.

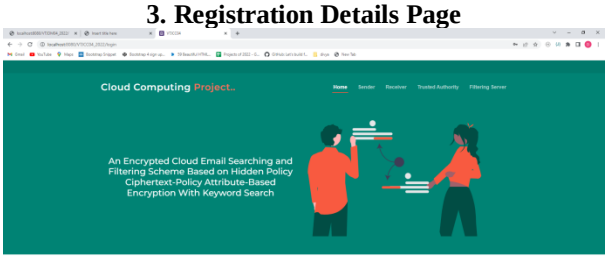
1. Login Page



2. Create Account Page



3. Registration Details Page



4. Email Search Page

5. Request Page

6. CONCLUSION AND FUTURE ENHANCEMENT

We introduce a new solution for searching and filtering encrypted cloud email based on HPCPABKS. Our scheme enables the recipients to search for keywords and the recipient filtering servers to filter keywords by adding the additional list of recipients. The scheme achieves full security proved by using dual system encryption methodology and can resist offline KGA. It can be as convenient for users to search and filter as the traditional email system. More extensions can be made to the scheme to realize the function of virus email protection in the future. It can also be easily extended to other application scenarios, such as the searching and filtering encrypted file systems. Because of the use of Composite order bilinear groups, the performance of our scheme is limited. 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. 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 attribute-based 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 multi-keyword 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/.