Concealed Policy and Ciphertext Cryptography of Attributes with Keyword Searching for Searching and Filtering Encrypted Cloud Email

Hind Alhumaidi[†] and Hatim Alsuwat[†],
S44380050@st.uqu.edu.sa Hssuwat@uqu.edu.sa
[1] Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Saudi Arabia

Summary
There has been a rapid increase in the use of cloud email services. As a result, email encryption has become more commonplace as concerns about cloud privacy and security grow. Nevertheless, this increase in usage is creating the challenge of how to effectively be searching and filtering the encrypted emails. They are popular technologies of solving the issue of the encrypted emails searching through searchable public key encryption. However, the problem of encrypted email filtering remains to be solved. As a new approach to finding and filtering encrypted emails in the cloud, we propose a ciphertext-based encrypted policy attribute-based encryption scheme and keyword search procedure based on hidden policy ciphertext. This feature allows the user of searching using some encrypted emails keywords in the cloud as well as allowing the emails filter-based server toward filter the content of the encrypted emails, similar to the traditional email keyword filtering service. By utilizing composite order bilinear groups, a hidden policy system has been successfully demonstrated to be secure by our dual system encryption process. Proposed system can be used with other scenarios such as searching and filtering files as an applicable method.

Keywords:
Attribute accompanied by Keyword-based Searching, system of dual cryptography, filtering-based encrypted email, Policy of concealed.

1. Introduction

It is forecast that the total number of business and the email sent and received by consumers will be exceed 333 million in 2022 and will reach over 376.4 million by the end of 2025[1]. In recent years, there has been a rapid increase in the number of cloud-based email services. The benefits of adopting the cloud are well known to all organizations today. Therefore, more and more, all sizes organizations are being migrated to the email of cloud as well as services-based collaboration. There are numerous cloud email providers providing more security features, namely emails encryption, some archiving, and several other functions related to security, which help to alleviate users' concerns about their privacy and security in the cloud.

Additionally, encryption of email as well generates several issues, for instance in what way one is supposed in order to search for email in the absence of being bothered by annoying decryption efforts or how one should handle the environment in which email is served (all countries and regions have laws that require the distribution of certain types of email, as junk mail, junk mail that contain several malicious code, and so forth).Furthermore, the cloud servers in somewhat situations do not be able to determine information regarding content of emails, when searching and filtering. As a result, the main issue that are being faced at the present time is in what way is make it as easy as possible to users for searching and filtering the encrypted email messages which it is being searched and is being filtered unencrypted it as in the traditional systems. In order to tackle this dilemma, the concept of searchable public key encryption had been proposed. Two principal encryption types, searchable symmetric encryption and searchable public key encryption can be divided into two sections. Searchable public key encryption is an ideal candidate for searching encrypted emails. Among the headmost to propose the concept of (PK) a public-key cryptographic system that also incorporates keyword search (PEKS), Boneh et al. [2] were the first to implement an encryption (IBE) email system based on identity. The scheme is being allowed the gateway in the sense of systems-based communication for retrieving and identifying if any keywords are contained in the received email. For the purpose of solving the problem of searching encrypted emails, searchable encryption technology was created by this solution. Afterwards, plenty of PEKS schemas are claimed that they can use as encrypted email searching. In the recent past, some PEAKS schemes were there [3],[4]to encrypted email messages. According to Xu et al [4], a hidden structure was used to implement a scheme for searching encrypted email messages involving multiple key words. A study by Li et al. [5] proposed a new idea for encrypting emails with a server-based design according to identity authentication cryptography method that also included keyword searches. The study Zhang et al. [3] has proposed a method that can support conjunctive keyword search without requiring a keyword field to be provided. Byun et al. [6] identified for PEKS what they termed the keyword guessing attacks according to offline mode (KGA) being one of the security mean security problems

Manuscript received June 5, 2022
Manuscript revised June 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.6.30

surrounding searchable public key encryption. The indistinguishability of the trapdoor has been proved by [7] to be a sufficient condition for resisting keyword guessing attacks. As in [3], [4], all of the three schemas can resist KGA, proving that the keyword trapdoor provides security. In spite of this, the filtering of the encrypted email messages was not being taken into consideration by these schemas. As such, this is still an issue that has not been resolved yet. Besides these PEKS schemes, there have also been some others [8], [9] that claim advocates encrypted emails filter, but they did not present a full explanation in what manner this would be achieved. A generalized encryption email filtering scheme model was proposed by Bonneh et al. [10] through the use of an abstract methodology. In a plausible scenario, some partially trusted proxy servers are used by email users in order to filter out encrypted email messages that were identified as junk mail as part of their own requirements for their schema. As a result, the proxy server manages to achieve the seemingly contradictory objective to hide the content of the email on the server of proxy and same time specify if the current email is junk mail based on the settings of the user. A description of the schematic diagram can be found in only two paragraphs of the text. Nevertheless, to solve this issue, they use searchable encryption to create a scheme, which is clearly demonstrated in their scheme model. From this, this schema was developed. in order to figure out the encrypted emails searching and filtering issue, we want to making filtering-based server a specific receiver. In light of this, we were motivated for designing the encrypted email based on searching and filtering schema according to encryption referring to attributes and keyword search.

Currently, it is hard for multiple recipients to search about encrypted email and as well as a filter it uses filtering server. In contrast, encryption based on attribute and search using keyword, particularly policy of ciphertext encryption based on attribute and search using keyword, be able to help address this issue. In order to achieve this objective, we propose the (Cpabks) system to encrypt cloud emails scenario is proposed to allow both filtering and searching at the same time. Whenever emails are sent, the additional lists of receivers are created, as well as the filtering-based server is added on the manner of the recipient. As a result of the users' attributes on this list of recipients being part of this set, then that set will act that the structure of access B of the index of the encrypted keyword. thus, just those recipients who fulfil required attributes for the policy of control could effectively search. By adding the filtering server to a list of additional recipients, the server will be able to filter the encrypted emails through keywords in a successful manner. It was necessary of constructing order bilinear groups in a composite way in order of hiding the data policy to be able to provide resisting in the (KGAs) as well as making system has a complete security. Toward solving this issue of encrypted emails search and filter, a secret-based policy ciphertexts-based policy attributes-based encryption system over keyword searching "HPCPABKS" [11] is proposed. In this proposed system, emails gateway does not provide any level of filtering. Instead, the recipient server-side filtering is provided only, which is same as some free email services.

This scheme is distinguished by the following benefits:

- Applying the KSBA design to the encrypted cloud email story in an innovative way. A sender can additionally create recipients list for search and filter as well as can include the recipient filtering-based server in this list as well. Users' attributes that are listed in this list of recipients are being used such as the policy of access control for the encrypted index of keyword. Hence, the recipients could be searched about keywords via searching by their own attributes, and the server of recipient filtering in turn could sort keywords using filtering keywords by their possess attribute.
- This schema allows multiple emails simultaneously to be copied and grouped using a single encrypted keyword index, sans incurring additional encryption index costs-based computation.
- The proposed result utilizes a system which known as dual system cryptography approach with a concealed policy with the aim of enhancing privacy and providing full security and privacy. It is capable of resisting KGA and is able to maintain the confidentiality of the encrypted email system.
- The proposed schema can facilitate several practical applications for email protection, including the detection of malicious e-mails, the processing of email attachments, and the reporting of malicious emails. It has a particular advantage of being able to be searched and filtered encrypted email more efficiently because it is generally excess adequate to the encrypted cloud-based email searches and filters stories however it could be expanded into encrypted file-based searches and filters besides other stories.

2. Related Work

A system of "HPCPABKS" traces its origins of encryption depending on Attribute (EBA), which is the schema that presented by Sahai and Waters [11]. Essentially, traditional public-key encryption is the root of the EBA. By expressing how the user desires of sharing the data in the algorithm of the encryption, the user can create several policies based on the receiving user attributes as well as the data sharing based on such policies. Accordingly, EBA can be classified in policy of ciphertext EBA (CPEBA) as well as policy-based key EBA (PBKEBA).CP-EBA schemas for

example[12] – [14], consist of attribute sets for which the key of the receiver is related, and ciphertexts for where the access policy for the sets of the attribute is set if the set of the attribute related with the key of the receiver matches the policy of the access included in the message of the ciphertext only then could be able to decrypt. According to [15]-[17], in the PBKEBA schemas the ciphertext have a group of attributes. Whenever a key is related to a policy of the access based on attribute group, it could be decrypted on the condition that the set of the attribute that forms ciphertext is compatible with the policy-based access related to the key. With the EBA, in a cloud platform environment, it is possible for the privacy of data sharing, as well as the security, to be maintained effectively. For the sake of ensuring that sensitive information is not disclosed in the access structure, however, under certain conditions, the EBA scheme must Providing support for an anonymous access system to successfully implement a hidden-based policy. In conjunction accompanied by a concealed control policy-based access, Nishide et al. [18] offered two CPABE schemas. By hiding a subgroup of each possible value of the attribute in the policy of the ciphertext, the user is able to hide some or all of the policy. It has also been realized in later work by [19]-[21] that access control policies can be hidden, data confidentiality protection can be maintained, as well as fine-grained access-based control can be implemented in cloud-based storages. All of the systems that have been mentioned so far are based on the selective model. As a result of the selective model, the attacker will need of specifying which of the access control policies are challenged before the system will start generating some public limits. This problem was first solved by Lewko et al. [22]. They suggested implementing an EBA system with a full security using the encryption approach of the dual system according to Waters [23] as well as the approaches developed via Lewko et al. [24]. Despite this, these encryption systems cannot be able to promote keyword-based search as well as search the ciphertexts data. With the goal of effectively supporting one-to-many stories in the storage of the cloud, in [25] [26], they have combined encryption based on attribute (EAB) technique with searchable encryptions technique. A new encryption based on attribute approach along with search-based keyword schema has been presented, that is applicable for the precise control of the access for ciphertext data as well as the retrieval of ciphertext data quickly, which will significantly improve productivity by sharing the data of the ciphertext over cloud. With a Cloud KSBA structure [27], [28], data regarding the keyword and data is not retrieved by the cloud server in any way. The [30] and [31] proposed KSBA schema accompanied by the policy of the access with a hidden mode, as well as they developed methodologies that were capable of resisting Keyword guessing attacks. Moreover, Liu et al. [32] suggested that the "HPCPABKS"[11] system is able to be supporting the integrity of the data as well as verification them then deduplication as well. Although the majority of these systems are validated using the selective model, there are still several insecure schemas. It is assumed in the adversary creates a Selective security model based on the information that they seek decides which access-based structure for attacks prior to that the system is initialized. Considering this, with a focus on resisting the keyword guessing attack (KGA), as well as selective security models as shown in [29], [30], [33] have to verify which the ciphertext is incomprehensible to the opponent at first, afterward, they have to verify the keyword trapdoor is incomprehensible to the opponent. On the other hand, the complete security scheme has a high security enough [34] demonstrated that the keyword-based ciphertexts to ABC'S schema converted at the complete security EBA is incomprehensible because of adversary's ciphertext addition, Trapdoor incomprehensibility can be proven in conjunction within a proof of the security, that assures that the security proof is stronger and more trustworthy. They have developed a HPCPABKS schema with full security in order to bilinear groups in a composite way, to effectively manage encrypted cloud email stories as well as increase their security. As compared to several of the PEKS for encrypted email schemes [35]– [36] introduced in the previous section, (Abks) system with multiple keywords as well as some other kinds of keywords are complex enough in implementation. As a result, the proposed system presently solely assists searching using a separate keyword. Each technique used which related to the proposed system is described in detail as shown in Fig 1.

System	Approach used	Hidden control policy-based access	Cloud storage-based access control	Selective model	Encryption approach of the dual system	Partial policy hiding	Resisting (KGA)	Search-based keyword	keyword trapdoor	Search ciphertext data	Full security model	Encrypted email schemes	Only supports searching using a single keyword.
[18]	two CPABE schemas	Yes	No	Yes	No	Yes	No	No	No	No	No	No	No
[19],[21]	two CPABE schemas	Yes	Yes	Yes	No	No	No	No	No	No	No	No	No
[22],[23], [24]	EBA system	No	No	No	Yes	Yes	No	No	No	No	Yes	No	No
[25], [26]	EBA.SE	Yes	Yes	No	No	No	No	Yes	No	Yes	No	No	No
[27],[28]	KSBA	No	No	No	No	No	No	Yes	No	No	No	No	No
[29],[30], [31],[33]	KSBA schema	Yes	Yes	No	No	No	Yes	Yes	No	Yes	No	No	No
[32]	HPCPABKS schema	No	Yes	Yes	No	No	Yes	No	No	Yes	No	No	No
[34]	HPCPABKS schema	No	Yes	No	No	No	Yes	No	No	Yes	Yes	No	No

Fig. 1 Comparison of Related Work

The rest of paper is organized as follows. In section 3, all the groundwork is given, including complexity Presumption, the structure of the access. Searching and filtering of encrypted cloud emails in the cloud system along its complete security is defined and provide the particular system at section 4. The section 5 presented the proof of the security in the system as well as comparison with other some other researches is given. Lastly, the paper states the conclusion in section 6.

3. Groundwork

3.1 Basic Concepts of Composite Order Bilinear Group

The first order bilinear in a composite way algorithm was proposed by [36]. The system is being built on the basis of N-order groups, and in this case, the N variable is a sum of 3 distinct prime numbers. Let δ be the generator of the group, the algorithms which can gets some security element 1λ such as an income as well as the outcomes as a tuple (q, r,s, H, HU , f). δ outputs (q, r,s, H, HU , f) where q, rs are being prime numbers, H as well as HU cycles of order N belong to these groups = qrs. f : H × H → HU where is the map contains such a feature:

1) Bilinear. $\forall$ s, i ∈ H, and $\forall$ b, c ∈ YN, f(g , i c) = f(g, i) bc

2) Non-degenerate. $\exists$ s ∈ H, f(s, s) has the order n at HU ,

3) amplification H as well as HU, and the procedures of these maps of Bilinear f of all polynomial-time towards λ are being fully computable.

Hq, Hr and Hs indicate all subsets of group H which the order is q, r and s r individually. Based on the orthogonality of subsets, as we can see that if $\forall$ iq ∈ Hq and $\forall$ ir ∈ Hr then f (iq, ir) = 1.

3.2 Presumption

Presumption 1 (Subset Decision issue for three Primes [37]): δ means the creator of H. They specify distribution as follows:

(r, s, t, H, HU, f) ← δ(1λ)
N = qrs, sq ← Hq, ss ← Hs,
K = (H, HU , N, f, sq, ss),
V1 ← Hqr, V2 ← Hq

They specify the benefit of the algorithm We specify the benefit of the algorithm *A* in breaking 1 to be:

Adv1A| Pro[a(d, t1) = 1] − Pro[a(d, t2) = 1]|

Definition number 1 says : δ fulfills Presumption number 1 if and only if for any polynomial time of the algorithm *A*, Adv1A is being minimal.

Assumption number 2: a generator group δ like above.

They defined the distribution as follows:

(q, r, s, H, HU , f) ← δ (1 λ),
N = qrs, sq, Y1 ← Hq, Y2 ← Hr,
ss ← Hs,
D = (H, HU, N, f, sq, Y1Y2, ss)
T1 ← Gpq, T2 ← Gp

They specify the algorithm *A* benefits to break the Presumption two to be:

Adv2*A*| Pro[a(d, t1) = 1] − Pro[a(d, t2) = 1]|

Definition number 2: They said δ fulfils Presumption number 2 if and only if for that polynomial time algorithm, *A*, Adv2 *A* is minimal.

Presumption 3: shown set creator δ as mentioned previously. The distribution is defined as:

(Q, R, s, H, HU, f) ← δ (1 λ)
N = qrs, α ∈ AN, sq ← Hq, sr,
J, J1, J2 ← Hr
ss, W0, W1, W ← Hs
K = (H, HU, N, f, sqW0, s
αBW1,
sBJ1, s1/αB J2, sr, ss)
V1 = sα qJE, V2 ← HU

They specify the algorithm *A* benefit to break Presumption three as:

Adv3 A| Pro[a(d, t1) = 1] − Pro[a(d, t2) = 1]|

Definition number 3: As seen the δ fulfills Presumption number 3 which says Adv3A is minimal to the algorithm A to all polynomial time.

3.3 Framework of the access

The expression capability of the control policy of the access is specified by the access framework itself. The structure of the access has various types to deal with the policies such as threshold structure (TS), tree-based structure (TBS), linear secret sharing structure (LSSS), and AND gate. The proposed system is used the AND gate and applied it to multivalued attributes [38] such a proposed framework. Therefore, an AND gate is used to get a connection between different attributes while an OR gate is used to get a connection between the same attribute with different values. The paper takes the developer as a position, and if the department: G& C AND indicates Seniority: Junior whereas OR indicates Seniority: Senior as shown in Fig 3.

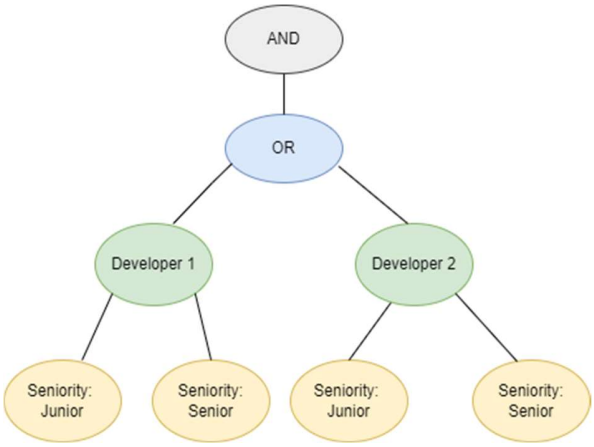


Fig. 3 Control Policy of the Access.

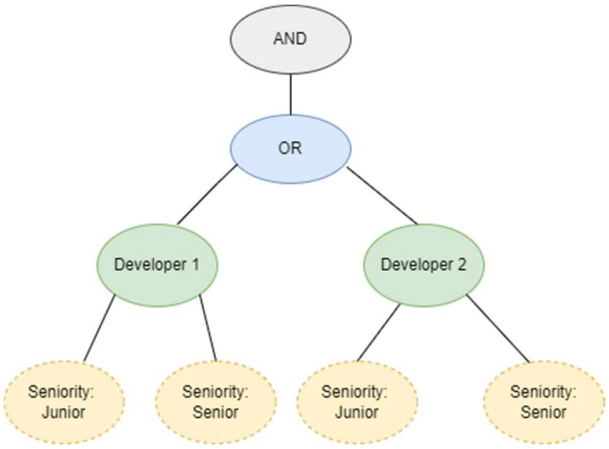


Fig. 4 Fully hidden access policy

Thus, an attribute of the list of one user's list is Ls = {Ls1, Ls2, . . ., Lsn}. while the structure of the access is A = {A1, A2, . . ., An}. If the Lsi ∈ Ai, i ∈ [1, . . . , n] then the attributes fulfill the structure of access control, and the structure of access is motivated by the inner product encryption which hides the policy of the access as much as possible as shown in Fig 4 which the hidden information can be appeared with dotted node.

3.4 The Policy of Ciphertext EBA

There are four main algorithms that describes the CPEBA system in general:

- ***Setup.*** Which sets a security parameter λ as long as description of attributes as input to get (PK) public key plus (MSK) master secret key as output.
- ***KeyGe.*** Which sets (MSK) master secret key, (S) list of attributes, and (PK) public key as input to get (SK) secret key related to (S).
- ***Encrypt.*** Which sets (A) the structure of the access, msg (M), and (PK) as input to get (CT) coded msg. The hidden policy of CPEBA along with policy. At some point in time there may also be a point when the access will be hidden from sight in the CT.
- ***Decrypt.*** Which sets ciphertext and secrete key as input. Furthermore, the msg (M) is returned by it. The user deciphers the ciphertext if and only if the (S) list of the attribute fulfils the structure of the access A that identified to ciphertext.

4. Searching and Filtering Schema for Encrypted Cloud Email

The system model, some security definitions, and the process of the system are described in this section

4.1 Proposed System Design

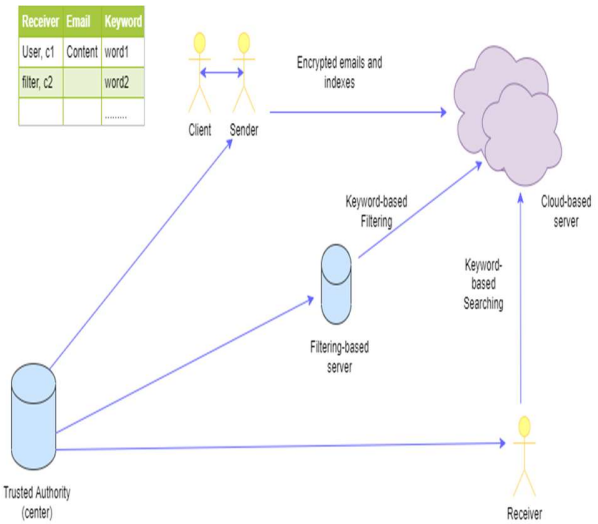


Fig. 2 system model

The system is clarified based on the following proposed structure which determines fives basic elements including trusted authority, email and keyword filtering server, sender, receiver, and cloud-based server as shown in Fig 2. Firstly, trusted authority which also known as the center of authorization creates master key, to the receiver filtering server and all of the users' emails is a public key and a private attribute key. Secondly, email and keyword filtering server (i.e., search) own a set of keywords to filter and put them in a list called blacklist. Based on the blacklist that it had, it creates trapdoors keyword as well as give them to the cloud-based server for running the algorithm-based filtering and make the new emails filtered. Thirdly, In the sender side, the sender's client responsible for dividing the email contents to set of keywords as long as the sender responsible for generating the additional list of receivers as well as adding the filtering-based server and all the receivers to that list. Thus, the sender uses the policy of the access to encrypt the index of the keyword by specifying the policy of the access, based on the receivers' attributes, and the server of the filter. This makes the email encrypted by the same original encryption approach. Moreover, the index of the ciphertext and the content of the email are sent by the sender to the cloud-based server. Fourthly, the receiver creates the trapdoor as a keyword and the keyword is sent to the searching cloud-based server, if and only if the receiver searches about an email with its keyword at the previous receiving email. Finally, the cloud-based server store all the encrypted emails as long as the index of the keyword that is received by the receiver. The cloud-based server presents either the services of the filters or searchable keyword if it gets a Trapdoor-based keyword due to the emails searchable servers or due to receivers themselves. The cloud-based server is done the processing of the email if and only if matching the keyword.

The proposed system focuses on only the encryption of encrypted emails regardless encryption of the plain email that presents the decryption process.

Assume that the adversary can distinguish the trapdoor-based keyword, this makes the cloud-based server untrusted to search and filter the encrypted emails.

4.2 System Algorithms

There are five main algorithms that explain the system in detail. They are presented in this fashion:

As shown in Table 1, the five algorithms are used to build the proposed system in order to describe the workflow of the system.

Algorithm	Characterization
Setup algorithm → (PK, MKS)	When the system uses the setup algorithm, it indicates that the trusted authority implements the entire system and that can be done according to the quality of the algorithm as well as the algorithm itself. Thus, it uses the basis of security parameter that presented as ʎ as input to produce PK and MSK as output.
KeyGen → (SK)	The trusted authority uses the KeyGen algorithm to execute the S the attribute list of the email of the user and MSK as input to produce of the SK secret key of the user email that is relative to the attribute list of the email of the user S.
Encindex → KWCT)	The encindex algorithm focuses on Encryption process that is done on the index-based keyword by sender. The sender encrypts the index-based keyword which enter the PK, as well as the structure of the access (A) to the system as input to make the algorithm produces the KWCT index-based keyword ciphertext.
Trapdoor → (trap)	The trapdoor algorithm focuses on the trapdoor-based keyword to filter (search) that is done by the receiver or filtering-based server. It enters the SK private (secret) key and keyword-based filter KF as input to make the trapdoor algorithm produces (trap) trapdoor-based keyword as output.
Verify → (0 or 1)	The search/filter (verify) algorithm focuses on the email index-based keyword that is done by a cloud-based server. The verify algorithm enters the KWCT index-based keyword ciphertext as well as trap as input. That produces potential outputs. When the attributes of the receiver fulfil the structure of the access as long as the keyword-based trapdoor meets the keyword-based ciphertext, the output is 1. In other respects, the output is 0. The filter (verify) algorithm is likewise the search (verify) algorithm in some points such as meeting the blacklist within the keywords-based email contents. If the algorithm produces the identification 1 of the email, The meeting is successfully done, and it generates the next process. Otherwise, if the meeting is unsuccessfully done, the algorithm produces 0.

Table 1: The system algorithms
Table 3 : proposed system vs. related systems

System	Trapdoor operation	Verification operation	Encryption operation	Email filtering
[4]	3E	4P	2E +P	NO
[34]	2E1 + E	2P	2E1 + E2	NO
[35]	E1 +E2 + P	2E1 +2P	2E1+E2+2P	NO
Proposed system	E(n + 1)	(n+1)P + (n+2)ET	(2*n*m +1)E+ET	Yes

4.3 Proposed Security Concept

The security concept can be defined in the proposed system as a case study (game). In the game, there are two main factors which are a challenger X and an adversary Y.

- In the setup level, to create the MSK maser private (secret) key as well as the PK public key, the challenger X calls the algorithm setup. Afterward, the adversary Y can obtain the public key, as well as the master private (secret) key is saved by the challenger X as shown in Fig 5.

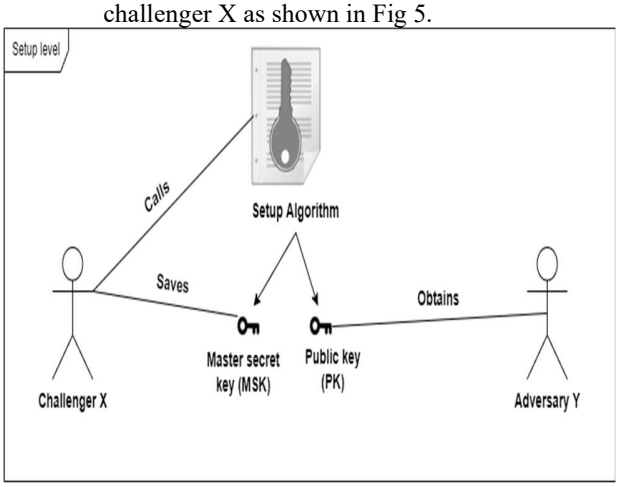


Fig. 5 Setup level

- The phase 1 says that the challenger X can obtain the secret key SK using KeyGen algorithm to create secret key as well as trapdoor (trap) to obtain the trapdoor-based keyword to send them to the adversary Y whereas the adversary Y creates n times queries of the secret key based on its attributes and the trapdoor-based keyword queries.
- The big challenge here is the A determines 2 keywords word0, word1 as well as 2 structures of the access A0, A1 and send them to challenger X to specify an arbitrary binary bit 0 or 1 value.
- Afterward, the challenge ciphertext using Encindex algorithm to get CT and It should be sent to the adversary Y.
- By the end of phase 2, the phase 1 queries have been repeated by the Y. Moreover, the Y guesses the keywords and the structure of the access according to the inverse of the arbitrary bit value. If it is equals, the adversary Y guessing is true, and it wins the game.

From this game, the proposed system can accomplish full security if and only if the adversaries with a polynomial-time mostly had minimal profit within the game.
Now, if the game is applied to non-discrimination on the trapdoor-based keyword then,

- The setup level is like the above concept as well as phase 1. However, the Y enters 2 keywords word 0, word 1 as well as the previous challenge in the structure of the access A and post them to the challenger X. on the other hand, the X specifies an arbitrary bit execute them using trapdoor algorithm and send the trap value of the algorithm to the Y.
- In the phase 2, repeating the phase 1 queries. As long as the adversary Y guesses the inverse of the arbitrary bit value. Therefore, the A wins again.

From all of this, the proposed system can fulfill the trapdoor-based keyword in non-discrimination if and only if the adversaries with a polynomial-time mostly had minimal profit within the game.

4.4 The proposed system

To make the system have full security, this paper has constructed the composite order bilinear groups method, which hide the data policy so the schema will be secure and comply with the KGA. Thus, assume that the user X has an email, and that email has let say n of attributes as well as each of these have Z potential values which are corresponding of a several item-based attribute. As mentioned above, five algorithms are used to build this system using this kind composite order bilinear groups method. The consequence of the process as follows:

Gp refers to subgroup which can used to verify from two functions: encrypt and verify. Whereas the Gr ensuring that the parameters are arbitrary. It helps to make the system accomplish the full security. Furthermore, there is Gq which responsible for affecting a space in a semi-functional way

not for the actual system. These five algorithms defined according to proposed system as shown in Fig 2:

Algorithm	Equation
Setup => PK, MSK	PK = {A0, {Ai,j}1≤i≤n,1≤j≤m, gr, Y } MSK = {gp,{ai,j}1≤i≤n,1≤j≤m, ω}.
KeyGen => SK	Sk = (xu, D0, {Di}1≤i≤n)
Encindex => CT	CT = (C˜, C0, {Ci,j}1≤i≤n,1≤j≤m)
Trapdoor => trap	Trap = (T˜, T0,{Ti}1≤i≤n)
Verify => 0 orl	If the attributes of the user fulfill the policy of the access control, the equation used is : E = e (gp, gp) tsd . If kw = tw, the cloud-based server is passes the validation as well as the outputs is one and the equation used is: C˜ T˜ · CU = Y s(xu+d) · Y −sxu = Y sd = e(gp, gp) ωsd

Fig 2: The algorithms of the proposed system based on composite order bilinear groups

5. Security Verification

To acquire full security of the system, the encryption of the dual system is applied in the proposed scheme. Therefore, a semi-functional keywords Trapdoor as long as semi-functional ciphertexts as well as semi-functional keys. Those who use traditional keyword trapdoors can check regular ciphertexts as well as semi-functional ciphertexts. On other hand, the semifunctional keyword trapdoors, however, can only be used to verify normal ciphertext, but cannot verify semifunctional ciphertext.s will also be used to demonstrate the security of proposed system. For example, all the ciphertexts and keywords used by the trapdoors in the first game normally occur. Unlike game two only the ciphertexts are semi-functional and the whole keyword trapdoors are in a regular state. Let imagine that there are several keywords-based trapdoor queries conducted by an adversary. In Game x, the rest of keyword-based trapdoors are in regular state while that the first x keyword-based trapdoors are semi-functional. However, In Game z, the whole keyword-based trapdoors cannot check the challenge-based ciphertext if the whole keyword-based trapdoors as well as ciphertexts arrived at the adversary Y as long as all challenge ciphertexts will not be able to be verified if keyword trapdoors are semi-functional By using this technique keywords trapdoors of this proposed system will not distinguishable due to this adversary Y.

5.1 Performance comparison

The computational comparison is done with some related systems as shown in Table 3. The pairing operation is defined as P where the group of exponentiation in G is defined as E,E1,E2, and ET. In Table 2, traditional PEKS systems [4],[34], and [35] are less computationally intensive, thus they do not support email filtering. For that reason, if they are going to send a mass mailing to many recipients, they have to provide a unique encryption index for each recipient in their systems, as well as encrypt multiple times. Hence, the index must be encrypted once in this system. In contrast to other systems, add only a list of recipients, which makes the scheme quite feasible. On the other hand, in order to ensure the security of this system, it is protected by a complete security model, which ensures that it has high security than other schemes. Because of this, the keywords trapdoors in the system is not distinguishable against the adversary side. Therefore, It is capable of resisting KGA. Comparatively, as a result of this system, functionality and security are improved at the expense of higher computing costs.

5.2 Evaluation of the performance

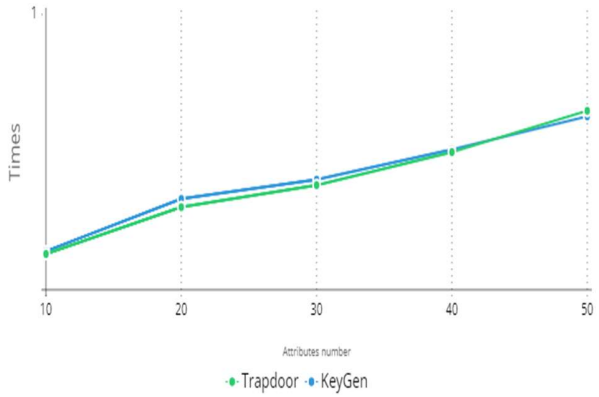
- After making a performance comparison between the proposed system with related ones, this performance must be evaluated. An email dataset is used as the basis for testing the proposed system's performance. There are more than 36 emails in the BC3-Email Corpus [39], and each email has an average of five keywords. A single type A1 algorithm from the Java Pairing Based Cryptography Library is used for generating all five algorithms [41] as well as its core modules such as:
- **jpbc-api** : used for the Application Program Interfaces (API).
- **jpbc-plaf** : used for the port implementation of the API.
- **jpbc-pbc** : used for the wrapper implementation of the API.

The experiment is conducted on an Intel(R) Core (TM) i7-5500U CPU @ 2.40GHz 2.39 GHz
and Windows 10 OS.
A security parameter of 192 bits is used in the experiments, In addition to increasing the number of attributes to 50 and setting the number of possible values for each attribute to twenty, all keywords have been encrypted to the same level. The average time was

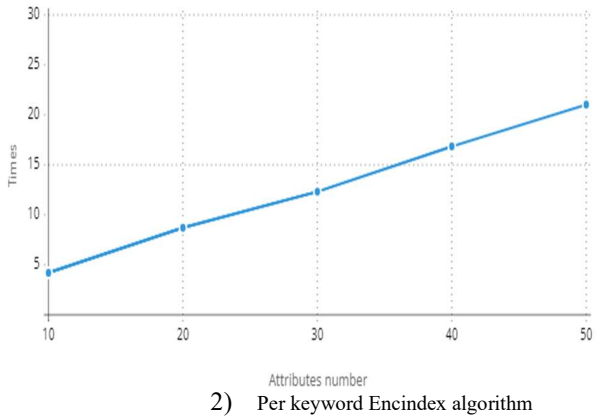
determined by performing each experiment ten times. In Table 3, each algorithm is shown by its average execution time.

Algorithms	Attributes number				
	10	20	30	40	50
Setup algorithm	4.10	9.73	12.40	16.8	20.44
Trapdoor algorithm	0.13	0.3	0.38	0.5	0.65
Per Keyword Encindex algorithm	4.2	8.71	12.32	16.85	21.03
KeyGen algorithm	0.14	0.33	0.4	0.51	0.63
Verify algorithm	0.38	0.54	0.84	1.04	1.29

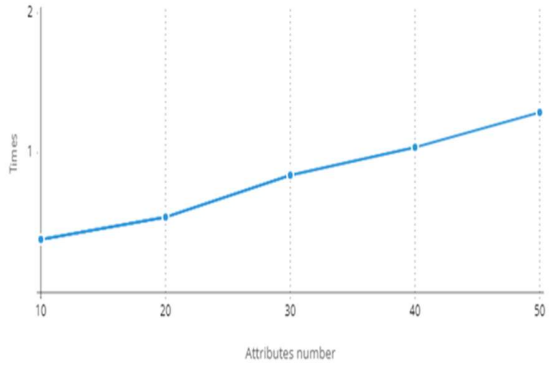
Table 3: five algorithms' Average Execution Times



1) Trapdoor and KeyGen algorithms



2) Per keyword Encindex algorithm



3) Verify algorithm

Fig 6: proposed system performance

Based on Fig 6, the attributes number generates a positive relationship between the cost of computation for every algorithm contained within proposed system. Additionally, we can see from the figures below that Encindex costs a lot more per keyword than is the case with the Verify/Search algorithm.

There is a good reason for this, and that is that from a computational standpoint, Policy hiding can be implemented by composite order bilinear groups and additional recipient lists, but it is very expensive to implement. Accordingly, as part of the proposed system, the security and functionality have been improved, but at the cost of significantly increased computation costs.

6. Conclusion

This paper presents a modern method to search as well as filter encrypted cloud emails using the "HPCPABKS"[11] algorithm. The recipient can search for keywords through our system, as well as the receiver's filtering-based server is able to filter-based keyword for including the additional receivers' lists in keyword. In this system, the total security can be proven to be achieved through dual-system encryption method as well as the resistance to offline key guessing attack is proven. Searching and filtering in this system are as easy for users as in the traditional email system that we used to it. It is possible that the scheme needs to be expanded in order to fully realize the function of protection of virus email in the future. Furthermore, this method can also be used in other applications, such as searching and filtering encrypted file systems.

As a consequence of the performance of this system is somewhat limited due to the usage of composite order bilinear groups. This system needs to be improved in future in order to be faster and direct in a way that does not compromise the security at any point in the future. Further, we also intend to develop multi-keyword search capabilities and other features that will enable the user to search more effectively.

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, 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.

[3] 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.

[4] 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 Comput., vol. 14, no. 6, pp. 1877–1889, Nov. 2021.

[5] 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.

[6] 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.

[7] 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.

[8] Q. Tang and L. Chen, ''Public-key encryption with registered keyword search,'' in Proc. Eur. Public Infrastruct. Workshop. Berlin, Germany: Springer, 2009, pp. 163–178.

[9] 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.

[10] D. Boneh, A. Sahai, and B. Waters, ''Functional encryption: A new vision for public-key cryptography,'' Commun. ACM, vol. 55, no. 11, pp. 58–64, 2012.

[11] 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.

[12] 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.

[13] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, ''User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage,'' IEEE Syst. J., vol. 12, no. 2, pp. 1767–1777, Jun. 2018.

[14] J. Li, N. Chen, and Y. Zhang, ''Extended file hierarchy access control scheme with attribute based encryption in cloud computing,'' IEEE Trans. Emerg. Topics Comput., vol. 9, no. 2, pp. 983–993, Apr./Jun. 2021.

[15] 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. Comput. Commun. Secur., 2006, pp. 89–98.

[16] N. Attrapadung and B. Libert, ''Expressive key-policy attribute-based encryption with constant-size ciphertexts,'' in Proc. 14th Int. Conf. Pract. Theory Public Cryptogr. Berlin, Germany: Springer, 2011, pp. 90–108.

[17] 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.

[18] 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.

[19] J. Lai, R. H. Deng, and Y. Li, ''Expressive CP-ABE with partially hidden access structures,'' in Proc. 7th ACM Symp. Inf., Comput. Commun. Secur., 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] Q. Zheng, S. Xu, and G. Ateniese, ''VABKS: Verifiable attribute-based keyword search over outsourced encrypted data,'' in Proc. IEEE Conf. Comput. Commun., Toronto, ON, Canada, Apr. 2014, pp. 522–530.

[26] 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.

[27] 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.

[28]] 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 Comput., vol. 10, no. 5, pp. 715–725, Sep./Oct. 2017.

[29] 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.

[30]] 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.

[31] 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.

[32] 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.

[33] F. Han, J. Qin, H. Zhao, and J. Hu, ''A general transformation from KPABE to searchable encryption,'' Future Gener. Comput. Syst., vol. 30, pp. 107–115, Jan. 2014.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] J. Gao and F. Zhou, "An Encrypted Cloud Email Searching and Filtering Scheme Based on Hidden Policy Ciphertext-Policy Attribute-Based Encryption With Keyword Search," in IEEE Access, vol. 10, pp. 8184-8193, 2022, doi: 10.1109/ACCESS.2021.3136331.
[39] Ulrich, Jan. Supervised machine learning for email thread summarization. Diss. University of British Columbia, 2008.
[40] J. Ulrich, G. Murray, and G. Carenini, ‘‘A publicly available annotated corpus for supervised email summarization,’’ in Proc. AAAI Workshop, 2008, pp. 77–82
[41] The Java Pairing Based Cryptography Library. Accessed: Apr. 23, 2022. [Online]. Available: http://gas.dia.unisa.it/projects/jpbc/