JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Data Access Control In Cloud Computing: Flexible and Receiver Extendable

1st Abhilasha M B
M.Tech Student
Dept of Computer Science EnggUVCE, Bangalore University Bengaluru, India

2nd Kumaraswamy S
Asst Professor
Dept of Computer Science EnggUVCE, Bangalore University Bangaluru, India

***Abstract*—Broadcast encryption presents a workable approach of controlling data access for certain users in cloud computing. A data uploader can generate a ciphertext for a particular user group in order to guarantee intended users have access to the data. However, the capacity of the receiver set should be increaseddue to the rapidly increasing number in order to promote user collaboration. The current broadcast encryption solutions cannot allow receiver extension. For the first time, authors address this problem in this project and provide a resolution. We suggest the concept of EIBBE, a broadcast encryption - based flexible with access control with extendable receiver for cloud computing,taking into account the benefits of identity-based cryptography. It enables the authorised user to enlarge the receiver set S definedin the IBBE ciphertext by adding a new receiving set without re-encrypting it. The data is effectively accessible to users in S and S0. The data uploader also chooses the highest limit of extended receivers. Provide a full construction of a EIBBE after that, and do a comprehensive security analysis of the proposed scheme. Finally, demonstrate the plan's practicality and effectiveness.**

***Index Terms*—Broadcast Encryption, Receiver Extendable, Cloud Computing, Access Control**

I. Introduction

A. Overview

The most promising technology has been touted as CLOUD computing[1] method for dealing with the a never-ending supply of data of user. Typically, cloud has strong computation capabilities, storage, affordability and flexibility. To avoidthe expense of managing local data, It can be delegated to a distant cloud server by the user, where it can then be shared with collaborators. when the information is delicate, like military secrets or individual medical records, preventing their exposure is preferable. One of the most effective waysto protect data confidentiality is to encrypt this type of data using cryptographic techniques prior to submitting it

to a cloud server. Nonetheless, because the data has been converted into cypher data, using it as plaintext is unsettling.

Techniques for flexible in data access control are expected in cloud for encrypt the data so that only users who meet the encrypted data is accessible to select individuals.

The primary goal of developing such a plan is for provide a key encapsulation which is flexible method that protects the encrypted key message.

The vocabulary and ideas used to define "cloud computing" frequently need to be clarified as it is a concept that is constantly changing and evolving. Press reports on How companies make their products accessible via the "cloud" or how "cloud computing" is the future's method areoccasionally unclear or may not fully reflect the scope ofwhat cloud computing encompasses or signifies. Forward without carefully considering the traits, theories, and services need to understand cloud computing and its potential.

This project introduces cloud computing that is based on the internet and looks at its properties, service models, deployment patterns, advantages, and disadvantages. Along with cloud communications services, Also highlighted are the needs for scalability and flexibility in a cloud-based system(including access points to the cloud like media control interfaces and online APIs.) The choices of interface, thatare suitable for a variety of applications and developers of services, as well as Enterprises wanting to use communication services should be aware of, as well as Web APIs, control and java XML-based interfaces, enterprises intending to use communication services should be aware of this.

Network designs that represented the internet or various parts of it as schematic clouds are thought to be the originof the term "cloud." The phrase "cloud computing" is usedto explain what occurs when services and programs are transferred to the cloud of the internet. It is possible thatthe roots of cloud computing can be found at an era when computers were utilised remotely. Cloud computing did not just appear out of nowhere.

Apps and computer resources shared over time. But more recently, the term "cloud computing" has come to refer to the wide range of services and applications that are now offered through the internet cloud, as well as that many of the devices being used to access these services and apps don't require any specialized software.

Many characteristics of cloud computing exist, however the following stand out:

- Shared Infrastructure – Makes use of a virtualized software approach to share networking, storage, and physical resources. Regardless of the deployment technique, the cloud architecture attempts to maximize the utilization of the available infrastructure across a number of users.
- Dynamic Provisioning – This feature enables the deliv- ery of services based on the demands of the moment. Software automation enables the automatic growth and contraction of service capability as necessary. High levelsof reliability and security must be upheld when doing this dynamic scaling.
- Network Connection – Requires internet access via a variety of devices, including desktop computers, using standards-based APIs, laptops and mobile devices.

B. Motivation of the project

Broadcast encryption is a practical way to limit access to specific users' data in cloud computing[2][3]. Ciphertext is generated by a data uploader for them to ensure that only a specific user group can read the data. To grant additional users direction to decryption rights, receiver set should be expanded in light of the constantly increasing level of user collaboration live transmission Receiver extension is not supported by encryption systems. To address this issue, we were inspired to launch this project. Utilizing the identity-based broadcast proxy reencryption (IBPRE) method is one potential fix [9]. In essence, It allows a proxy (cloud) to change the original ciphertext meant for one group of users into a new one meant for a different group of users. However, due to the simplicity of the encryption, not only does the data uploader create anew secret keys for the cloud, but still the cloud is also able to re-encrypt all of the ciphertexts that were created by the data uploader. For real-world applications, it is not desirable. A re-encryption key is created via the data uploader also needs to be aware of the set S0 of IDs of each new recipient. Given that firm X chose the new receiver set in a way that makes the earlier instance challenging to accomplish and seem impossible. To the to our knowledge, the literature does not currently use any solutions that can deal with the aforementioned issue.

II. RELATED WORK

A. Maintaining the Integrity of the Specifications

Broadcast encryption (BE) [1] was developed to provide effective access control on data which is encrypted for a large number of users. It enables a user (encrypt) to distribute a one piece of data to select users from the group while ensuring that only those user is permitted to obtain data access and encapsulated ke. No information is shared with other users. When the compared access control for standard public key encryption in single user situations. BE shows a significant improvement in efficiency.

There has been a lot of discussion on the broadcast encryption identity-based (IBBE) [2] approach the literature [2, 10, 11, and 12]. It does away with certificates in the established public key from encryption scheme. When receiver is known before the encryption process, BE is particularly helpful for implementing access control.

Goyal et al. [14] and Sahai and Waters [13] created attribute-based encryption (ABE), which view user identification as sets of attributes. For encrypted data, ABE offers precise access control and scalability. Depending whether it involves the creation of user private keys or wrapped ciphertext, the access policy is split into two categories.

Key ABE and policy-ABE with ciphertext policy (CP-ABE) (KP-ABE). Only particular conditions allows for the decryption from ciphertext. The core layout of Access (encoded in CP-ciphertext ABE's and KP-private ABE's key, respectively). Due to its error and tolerance property, ABE is frequently been utilized to make flexible key encapsulation methods for data access and control.

To obtain different results, a variety of ABE techniques in different models and applications have been developed [15], [16], [17], [18], [19], [20]. The ABE system's receivers are fuzzy in comparison to IBBE since one characteristic can be utilised to feature numerous individuals. Proxy re-encryption (PRE) [21] is required for cloud and data communication. A data upload cane be done by uploader may add its data in an encrypted manner on a remote cloud server to preserve its confidentiality. The user provides a reencryption key connected from the cloud to the receiver, which is shown as proxy, in case receiver is recognized in the future. With the provided re-encryption value key, the proxy re-encrypts original cipher-text to create a new one. This process ensures that the data is kept private in cloud server and that only the given receiver may access to it. Preparation of work has been done. PRE for new challenges and requirements.

An IPRE PRE method was presented by Green and Ateniese [22] to handle the certificate issue in the context of identity-based systems. Contrarily, only one receiver can be used at a time by PRE and IPRE. The relevant system needs to be run many times if there are multiple intended receivers. Chu et al. created broadcast proxy's re-encryption (BPRE), sometimes referred as proxy broadcast reencryption in other sources [23], to solve this problem.

The benefits of proxy re-encryption and broadcast encryption are combined this strategy. The data uploader develops a re-encryption value key in given number of collection targeted receiver rather than using a single receivers. Using the re-encryption value key, the new ciphertext will be decrypted by most of the intended recipients.

It should be emphasised that in PRE schemes, The ciphertexts can all be encrypted by the proxy, none of them are generated by the delegator. Conditional proxy re-encryption (CPRE) is proposed [23, 24] as a solution to this issue. Instead of having to generate the re-encryption secret for every ciphertext, the data uploader can specify which ciphertexts are allowed to be re-encrypted. In order to catch multiple receivers, CPRE is naturally expanded to condition proxy broadcast re-encryption (CPBRE). [23], [25].

A CPBRE technique for the identity-based environment was given by Xu et al. [9]. Whether in a single user scenario or a multi-user one, each of these PRE methods requires the uploader to be aware of the receiver before producing the encryption key. Firm X, not uploader, chooses the new extension receiver sets in the aforementioned scenario. Therefore, the PRE primitive is unable to resolve the aforementioned issue. Lai et al. [26] employ receiver extension for this. To enable anonymous revocation of many receivers, they created an broadcast encryption identity-based approach with authorizations.

An original ciphertext may be altered by a third party using a new receiver that has been set up anonymously. Only someone who can verify both identity sets can decipher the ciphertext. In order to offer multi-user access control, the study in [27] combines proxy re-encryption and homomorphic encryption algorithms.

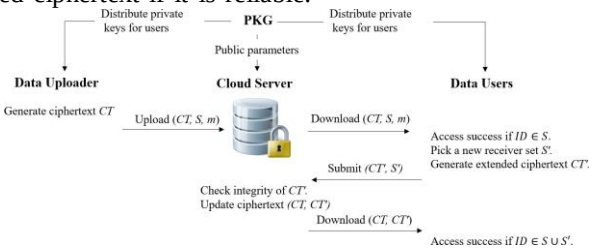
However, the data service provider and access control server (ACS) both need to generate the ciphertext (DSP). DSP uses each data user's public value key to re-encrypt ciphertextwithin transmitting in the finished product to ACS. The result-ing result is then once again encrypted by ACS using the user's public key. The ACS and DSP must do the aforementioned procedure for each and every receiver in a group of receivers. For a large number of users, broadcast encryption (BE) was de-veloped to offer effective on encrypted data for access control. It will allow a data encrypt to send only one piece of encrypted data to a chosen set of users, who can only view the data after getting the encapsulating key. Nothing is communicated to other users. For access control in single user scenarios,B E performs noticeably better than conventional public key encryption. Researchers are interested in the identity-based broadcast encryption identity-based (IBBE) method because usual public value key encryption method requires a certificate. When the receivers are known before the encryption process, BE is particularly helpful for implementing access control.

III. PROPOSED SYSTEM

Model for a broadcast encryption system that can be ex-panded based on identification (EIBBE).

A. Frame work of EIBBE

- The PKG, which oversees the entire EIBBE system, is a reliable body. PKG will create system's public parameter and configure first system. PKG generates a private key for each user after confirming user identity information, enabling new data users to decrypt data. In actuality, the PKC can be a reputable organisation the user is engaged with, like our government or a business' data centre.
- It is considered that the cloud (server) is enquiring yet trustworthy (In other words, it will conduct the procedure honestly while adhering to the algorithms, but it also triesto decrypt the data.) It will have strong calculating and also storing capabilities. This offers a stage for the storageof data user. Any user may download the encrypted data that is kept on the server (cloud) for free of cost. When cloud receives an expanded ciphertext for a receiver extension, integrity testing is also done. The server will add the expanded ciphertext if it is reliable.



- Before uploading to the cloud, the data uploader encrypts the original data (message) in their possession by select-ing an authorised receiver set. The information for limited receiver set extension is contained in the cypher data.
- The user may freely get the encrypted information of their choice from the cloud platform. Each user must register for the systems and get a private key associated with their identification from PKG before they can access data. The intended (authorised) receivers may add a new users set towards the receiver set without having to re-encrypt the data.
-

B. Methodologies

Receiver extension, data access, integrity check, data sharing and user registration, are the six steps of an EIBBE system. Each step is described by the algorithms called polynomial-time, in that sequence.

Set-up: After receiving as inputs an integer N and a system security parameter denoting the maximum number of receivers set, the setup operation carried out by the PKG outputs a system public parameter SP and a master secret key msk. The msk is kept as secret while the SP is made to public. Key key = generatekey();

Key-Gen: An identity ID and the system key pair (msk; SP) and are inputs into the key for generation process employed by PKG, which results in a key which is private skID for ID.

Encryption: The inputs of the receiver identities S and system public parameter SP a are used by the data uploader's encrypted procedure to create a tuple of three parameters (CT; K; m), where m is the highest amount of extended receivers and K is an encryption key for the message. Inthis case, we always consider m to be a part of CT. Thedata uploader creates (CT), (K), and (m) by performing Encrypt prior to disseminating M to consumers in S. (SP;M; S). After that, it transmits the crypt data CM of M that was created using a symmetrical encryption method and key
K. (CT;CM; S). CT can be considered a header, with CM serving as the broadcast body. String encryptedValue = new BASE64Encoder().encode(encVal);

```
c.init(Cipher.ENCRYPTMODE, key);
byte[] encVal =
c.doFinal(Data.getBytes());
```

String encryptedValue = new BASE64Encoder() encode(encVal);

Decrypt: The identity set S, its corresponding private key skID, its corresponding ciphertext CT, and the system's public parameter SP as inputs. The data user's decryption method generates a data encryption key K if ID 2 S. It stands to reason that the user might employ obtain the data M and K to crack CM. If ID = 2 S, it produces.

```
c.init(Cipher.DECRYPTMODE, key);
byte[] decordedValue = new
BASE64Decoder().decodeBuffer(encryptedData1);byte[]
decValue = c.doFinal(decordedValue);
```

Extend: After taking the public parameter SP, an extended identification set S0 with the inputs jS0j m and ciphertext C T with identity sets S and m, the extended operation carried out by authorized user data provides an extension ciphertext CT for S [S0 for S] S0, which may be using for extract agiven key K0.

Check: The integrity checking algorithm used by the cloud produces 1 to show whether K0 = K and accept CT0 whenever provided the systems public variable SP, a cipher
- text CT connected with just an identification sequence, an expanded cipher - text CT0 connected with just an expanded identification set S0, and the private key sk0 of the cloud. Otherwise, CT0 cannot be the result.

Using the setting algorithm for each (SP; msk), skidby calling the algorithms KeyGen(SP; msk; ID) and Encrypt(SP;M; S), respectively, for (CT;K) and ID for a set of S, and (CT0; S0), through using the algorithm Extend(SP;CT; S0), for S and ID, we obtain, if ID 2 S, Decrypt (S;CT; SP;)

We have added extra feature that is revocation of an account. If a user want to delete the account by himself/herself or user is no longer using the account or user is no longer needed this service then user can revoke itself. Admin can also revoke the account in this.

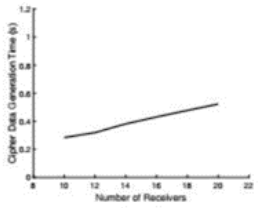


Fig. 2: Cipher Data Generation Time($m = 8$).

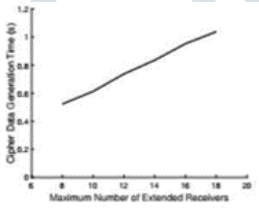


Fig. 3: Cipher Data Generation Time($n = 20$).

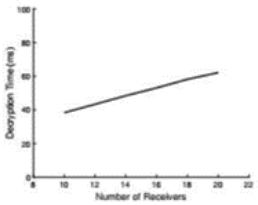


Fig. 4: Decryption Time.

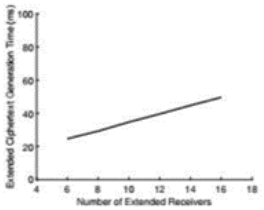


Fig. 5: Extended Ciphertext Generation Time ($n = 20$).

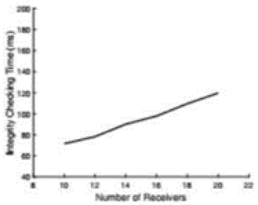


Fig. 6: Integrity Checking Time($l = 8$).

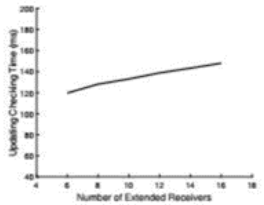


Fig. 7: Integrity Checking Time($n = 20$).

in the ciphertext for the purpose of simplicity. The expenses of communication are summarised in Table 2. The communication costs incurred during User Registration phase are a result of the distribution of user private keys following PKG creation. In our example, the costof PKG distributing private keys to users is constantand it has a size of 4—G—, such as Alice, firm X,and manufacturers. The data which is uploaded, whosends encrypted data to the server(cloud), is primarily responsible for the communication costs in the Shared Data phase. The price for Alice to outsource her cloud ciphertext is (5 + m)—G—. The only communication the data user must send to other entities during in the Data Access phase is to the cloud server's ciphertext can be downloaded. The cost of connectivity from the cloud server to the data user (such as firm X or manufacturers) is therefore (5 + m) —G—. By delivering the expanded ciphertext to the cloud in during Receiver Extension phase, the data owner

RESULT ANALYSIS

A. *Theoretical Analysis*

In terms of communication and computing complexity, the proposed strategy is theoretically analysed in this sub- section. The earlier example illustrates the communication costs associated with each contact between entities. The latter summarises each phase's computing expense.

- Communication Complexity

With the exception of System Initialization and Identity Check, which contain no inter-entity connections, we take into account four phases when evaluating communication overhead. The symbol —G— designates the size of group —G— elements. We presume that The largest amount of extended receivers is m. We ignore the size of the number m and the length of the identities that are associated Communicational Complexity Regardless of m, the expense of communication between firm X and the cloud is 5—G—. At the startup of both the system, exponentiations in group G. A data user must make five calculations for PKG to start the service. Use exponentiations to create the private key of the user in group G. The data uploading (Alice) must do O(m n) possible in group (G) in order to produce crypto data which to n number of receivers and m at the very extra receivers. For each user, the computation of five pairing and O (n) exponentiations in group is required. Any additional l receivers in group G will be accepted by the receiver extension as O(l) exponentiations. Ten pairings plus an O(n) exponentiations group comprise the computation cost for the cloud integrity checks.

B. *Experimental Analysis*

The planned approach is then put into practise to see how long the fundamental algorithms take. The tests are done on a computer that has a 16 GB RAM and an Intel(R) Cpu (central processing unit) i7-8550U processors that operates at 1.80GHz and 2.00GHz. The OS in use is Windows 1064-bit. The curves are Type A with —G— = 160 bits, and the libraries is Pairing-Based Cryptography (PBC). The scripting lang used is C++. Stressing that the simulator isnot prototype execution rather gauges how long each phaseof our suggested

strategy will take to complete. In the tests,we change the dimensions of the S, the number of available original receiver sets, the number of expanded receivers, and the duration of the expanded receiver set S 0. If a phase's running time is dependent on two factors, we fix one factor component and change the other variable element separatelyto evaluate the computation time. Instead of just computingthe time-consuming operations, the cost time is acquired from the random element selection through algorithm execution. During in the Sharing Data, Data Accessing, Receiver Extensions, and Integrity Check phases, we evaluate the running time.

We do not take into account the Systems Initializingand User Registration phases because the PKG handles these and their computing time is independently of the variables indicated above. Our architecture shows that time needed to generate cypher data during in Shared Data phase is related to both n and m. We first set m = 8 in the studies, and then we changed n between 10 and 20. Then, m is changed from 8 to 18 while n is adjusted to 20. During the access stage, evaluate the decrypted times for various cipher-texts. Particularly, look at computations times as ciphertext specifies between 10 and 20 original receivers. Because the updated information (CT0, S0) is calculated using the initial ciphertext CT as well as the expanded receiver set S, evaluate calculation time changing one from 6 to 16. Way of maintaining time during in the Integrity Check phase depends on size of bothS and S". After setting one to 8, we change n between 10and 20. Next, n is set to 20 and l is varied from 6 and 16.20 algorithm runs are performed and then take the average. The experiment's findings are displayed in Figures 2–7. In essence, the experiment's findings support the theoretical analysis by demonstrating that each phase's running time rises roughly linearly even as underlying variable component rises. // Here are the few clips of the view of the project. It

Fig. 1. Screenshot

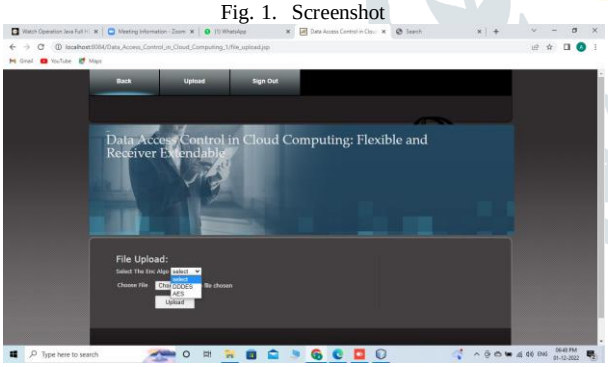
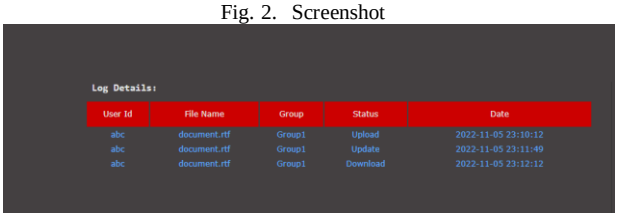


Fig. 2. Screenshot



basically done with HTML PHP and CSS for Styling. The below figure shows detailed page for frontend. It contains File details, File upload, file download, Account Revoke. These are the tab contained in After Login page i.e after the user is logged in with the correct credentials and Signature Key. Signature key is sent through the mail to the users mail ID from the cloud server login. The signature key willbe different for each and every user. It is a string which is contained of twelve characters which will include alphabets, numbers and symbols so that it will be unique for each and every user and not easy to remember or guess.

- Above figure shows that when user uploads data to the Server Cloud, user have to select either of two among algorithms that is DDDES and AES. So data will be encrypted by using one of these algorithm method.
- So once we login through login details and verify by giving group signature key user can see the log file details that is shown in the below screenshot.

IV. CONCLUSION

Introduced a brand-new idea for flexible data access and control in cloud computing called extendable encryption based on user identity (EIBBE). It accomplishes receiver extended for the very first time in an identity based broadcasting encryption method. The receivers set can be expanded from any authorised user, enabling other users to access the same data without having to re-encrypt it. The data uploader determines the maximum number of extended receivers. The cloud will reject an extend ciphertext that will be created for large receivers than the m. presented a concrete EIBBE structure. Access for control and a small amount of receiver extensions for same data are primary design objectives of EIBBE. The suggested scheme's capacity to capture soundness, semantic security and accountability has been proven. Finally, assessed by the computational overhead and transfer bandwidth performance of our EIBBE system. Our examples show that our EIBBE scheme may offer adaptable access control for group applications.

ACKNOWLEDGMENT

I am grateful to all of those with whom I have hadthe pleasure to work during this and other related projects specially Kumaraswamy S sir. Each of the members of my Dissertation Committee has provided me extensive personal and professional guidance and taught me a great deal about both scientific research and life in general.

REFERENCES

[1] A. Fiat and M. Naor, "Broadcast encryption," in CRYPTO '93, Lecture Notes in Computer Science. Springer, 1994, pp. 480-491, Computer Science, D. R. Stinson, Ed.
[2] C. Delerablee, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in ASIACRYPT 2007, ser. LNCS, edited by K. Kurosawa, vol. 4833. Springer, pp. 200-215, 2007.
[3] Sakai, R., and Furukawa, J., "Identity-based broadcast encryption," IACR Cryptology ePrint Archive, vol. 2007, p. 217, 2007
[4] "Identity-based broadcast encryption with continuous authentication," J. Li, Q. Yu, and Y. Zhang. The resilience of leakage," Inf. Sci., vol. 429, pp. 177-193, 2018.
[5] J. Lai, Y. Mu, F. Guo, P. Jiang, and S. Ma, "Identity-based broadcast encryption for inner products," Comput.
[6] P. Jiang, F. Guo, and Y. Mu, "Efficient identity-based broadcast encryption with public key cryptography," "Keyword search for database systems against insider attacks," Theor. Computer Science, vol. 767, pp. 51–72, 2019
[7] "Identity-based broadcast encryption with efficient revocation," A. Ge and P. Wei, in Public-Key Cryptography - PKC 2019, D. Lin and K. Sako, Eds., Lecture Notes in Computer Science, vol. 11442. 405-435, Springer, 2019.
[8] "EACSIP: extendable access control system with integrity protection for enhancing cloud collaboration," W. Susilo, P. Jiang, F. Guo, G. Yang, Y. Yu, and Y. Mu. IEEE International Journal of Information Forensics and Security, vol. 12, no. 12, pp. 3110-3122, 2017.

[9] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, ”Conditional identity-basedbroadcast proxy re-encryption and its application to cloud email,” IEEE Transactions on Computers, vol. 65, no. 1, pp. 1–5. no. 1, pp. 66–79, 2016

[10] D. Boneh, C. Gentry, and B. Waters, ”Collusion resistant broadca st encryption with short ciphertexts and private keys,” in CRYPTO 2005, ser. Lecture Notes in Computer Science, pp. 59-64. Science, Springer, 2005, pp. 258-275, edited by V. Shoup.

[11] B. Libert, K. G. Paterson, and E. A. Quaglia, ”Adaptive security and efficient constructions in the standard model,” in PKC 2012, ser. M. Fischlin, J. A. Buchmann, and M. Manulis, Eds., Lecture Notes inComputer Science, vol. 7293. Springer, pp. 206-224, 2012

[12] ”Adaptively secure identity-based authentication,” J. Kim, W. Susilo, M. H. Au, and J. Seberry.”Broadcast encryption with a constant-sized ciphertext,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, 2015, pp. 679-693.

[13] A. Sahai and B. Waters, ”Fuzzy identity-based encryption,” EURO- CRYPT 2005, pp. 1–5.Springer, R. Cramer, Ed., Ser. LNCS, vol. 3494, pp. 457-473, 2005.

[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ”Attribute-based en- cryption for fine-grained access control of encrypted data,” in ACM Conference on Computer and Communications Security, CCS 2006, Eds.ACM, 2006, pp. 89-98.

[15] B. Waters, ”Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realisation,” in PKC 2011, ser. LNCS, Eds. D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi. Springer, pp. 53-70,2011.

N. Attrapadung, B. Libert, and E. de Panafieu, ”Expressive key-policy attribute-based encryption with constant-size ciphertexts,” LNCS, D.Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Eds., vol. 6571. Springer, pp. 90-108, 2011.

[16] J. Herranz, F. Laguillaumie, and C. R’afols, ”Constant size ciphertextsin threshold attribute-based encryption,” in PKC 2010, ser. LNCS, P. Q. Nguyen, and D. Pointcheval, ”Constant size ciphertexts in threshold attribute-based encryption,”

[17] C. Chen, J. Chen, H. W. Lim, Z. Zhang, D. Feng, S. Ling, and H.Wang, ”Fully secure cryptography.” ”Attribute-based systems with shortciphertexts/signatures and threshold access structures,” in CT-RSA 2013,ser. LNCS, Ed. E. Dawson, vol. 7779. Springer, pp. 50-67, 2013.

[18] Verifiable and exculpable outsourced labor,” H. Ma, R. Zhang, Z. Wan, Y. Lu, and S. Lin. Attribute-based encryption for cloud computing access control,” IEEE Transactions on Dependable Systems Computing, vol. 14,no. 6, pp. 679-692, 2017. Forensics and Security, vol. 13, no. 1, 2018, pp. 94-105.

[19] ”Auditable -time outsourced attribute-based encryption for access con- trol in cloud computing,” J. Ning, Z. Cao, X. Dong, K. Liang, H. Ma, and L. Wei. IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, 2018, pp. 94-105.

[20] M. Blaze, G. Bleumer, and M. Strauss, ”Divertible protocols and atomicproxies,” Springer Cryptography,” in EUROCRYPT ’98, Lecture Notes in Computer Science, vol. 1403 Springer, 1998, pp. 127-144.

[21] Green, M., and Ateniese, G., ”Identity-based proxy re-encryption,” in ACNS 2007, ser. J. Katz and M. Yung, Eds., Lecture Notes in ComputerScience, vol. 4521. 288-306 (Springer, 2007).

[22] Chu, C., J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng, ”Conditionalproxy broadcast re-encryption,” in ACISP 2009, Lecture Notes in Computer Science, vol. C. Boyd Springer, 2009, pp. 327-342. and J. M. G. Nieto, Eds.

[23] ”Conditional proxy reencryption,” J. Weng, R. H. Deng, X. Ding, C. Chu, and J. Lai. secure against chosen-ciphertext attack,” in ASIACCS 2009, edited by W. Li, W. Susilo, and U. K.ACM, 2009, pp. 322-332, Tupakula, R. Safavi-Naini, and V. Varadharajan, Eds.

[24] ”A conditional proxy,” K. Liang, Q. Huang, R. Schlegel, D. S. Wong, and C. Tang. ”Broadcast re-encryption scheme with timed release,” in ISPEC 2013, ser. Lecture Notes in Computer Science, Eds. R. H. Deng and T. Feng, Springer, 2013, pp. 132-146.

[25] J. Lai, Y. Mu, F. Guo, and R. Chen, ”Fully privacy-preserving id-based broadcast encryption with authorization,” Comput.

[26] ”Encrypted data processing with homomorphic re-encryption,” Inf. Sci.,vol. 409, pp. 35-55, 2017.

[27] R. Chen, Y. Mu, G. Yang, and F. Guo, ”BL-MLE: block-level message locked encryption for secure large file deduplication,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, 2015, pp. 2643- 2652.

[28] Cambridge English Dictionary, ”RAM.” taken from 11 July 2019.

[29] ”RAM”. Oxford Advanced Learner’s Dictionary. Retrieved 11 July 2019.

[30] NetBeans.org provides ”A Brief History of NetBeans.” taken down on May 17, 2008.