International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 1
January 2019

An Enhanced and Reliable Over Encrypted Data in Cloud

Cherukuri Alekhya & A.Hanumath Prasad
[1] PG Scholar Department of CSE, GVR & S College Of Engineering & Technology, Guntur (D.T),Andhra Pradesh
[2]Associate Professor&HOD, Department of CSE , GVR & S College Of Engineering & Technology, Guntur (D.T),Andhra Pradesh

Abstract:-
Accessible encryption enables a cloud server to direct watchword seek over scrambled information in the interest of the information clients without taking in the fundamental plaintexts. Nonetheless, most existing accessible encryption plots just help single or conjunctive watchword seek, while a couple of different plans that can perform expressive catchphrase look are computationally wasteful since they are worked from bilinear pairings over the composite-arrange gatherings In this paper, we present a safe multi-watchword positioned look conspire over scrambled cloud information, which at the same time bolsters dynamic refresh activities like erasure and inclusion of records. In particular, the vector space display and the generally utilized TF_IDF demonstrate are consolidated in the list development and question age. We build a unique tree-based file structure and propose an "Avaricious Depth-first Search" calculation to give productive multi-catchphrase positioned seek. The safe kNN calculation is used to scramble the list and question vectors, and in the interim guarantee exact importance score count between encoded record and inquiry vectors. With the end goal to oppose measurable assaults, apparition terms are added to the list vector for blinding indexed lists. Because of the utilization of our exceptional tree-based list structure, the proposed plan can accomplish sub-direct hunt time and manage the cancellation and addition of records adaptably. Broad tests are directed to exhibit the productivity of the proposed plan.

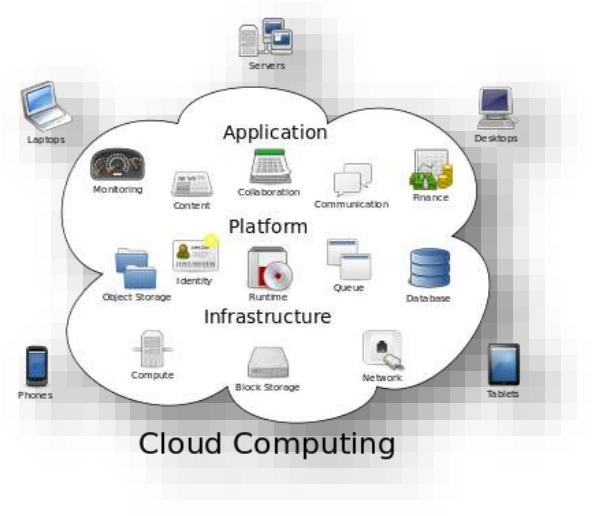
KeyWords:- Searchable encryption, cloud computing, expressiveness, attribute-based encryption.

I.INTRODUCTION

What is cloud computing?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over

a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.



Structure of cloud computing

How Cloud Computing Works?

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

- **On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without

requiring human interaction with each service's provider.

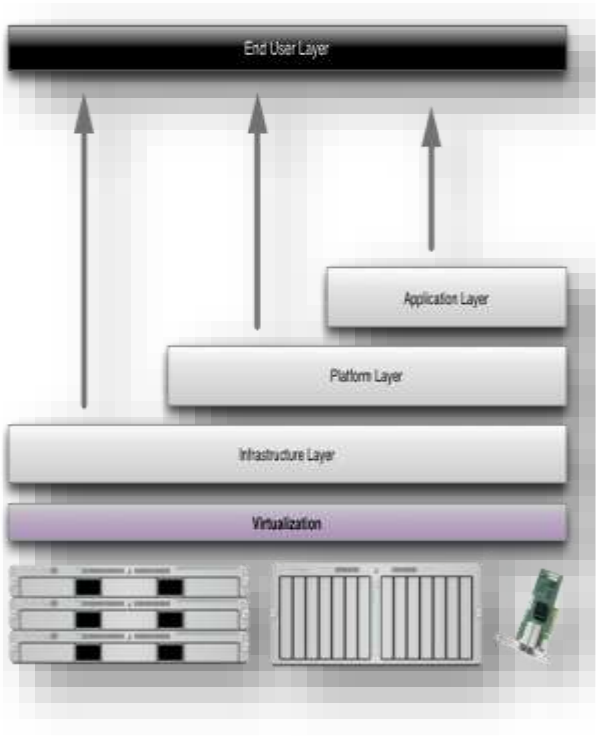
- **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity**: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Services Models:

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 1
January 2019

below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.



Structure of service models

Benefits of cloud computing:

1. **Achieve economies of scale** – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
2. **Reduce spending on technology infrastructure.** Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
3. **Globalize your workforce on the cheap.** People worldwide can access the cloud, provided they have an Internet connection.
4. **Streamline processes.** Get more work done in less time with less people.
5. **Reduce capital costs.** There's no need to spend big money on hardware, software or licensing fees.
6. **Improve accessibility.** You have access anytime, anywhere, making your life so much easier!
7. **Monitor projects more effectively.** Stay within budget and ahead of completion cycle times.
8. **Less personnel training is needed.** It takes fewer people to do more work on a cloud, with a minimal

learning curve on hardware and software issues.

9. **Minimize licensing new software.** Stretch and grow without the need to buy expensive software licenses or programs.
10. **Improve flexibility.** You can change direction without serious "people" or "financial" issues at stake.

Advantages:

1. **Price:** Pay for only the resources used.
2. **Security**: Cloud instances are isolated in the network from other instances for improved security.
3. **Performance:** Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's core hardware.
4. **Scalability:** Auto-deploy cloud instances when needed.
5. **Uptime:** Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
6. **Control:** Able to login from any location. Server snapshot and a software library lets you deploy custom instances.
7. **Traffic:** Deals with spike in traffic with quick deployment of additional instances to handle the load.

2. LITERATURE SURVEY

1) Security challenges for the public cloud

AUTHORS: K. Ren, C.Wang, Q.Wang et al.,

Cloud computing represents today's most exciting computing paradigm shift in information technology. However, security and privacy are perceived as primary obstacles to its wide adoption. Here, the authors outline several critical security challenges and motivate further investigation of security solutions for a trustworthy public cloud environment.

2) **A fully homomorphic encryption scheme**

AUTHORS: C. Gentry

We propose the first fully homomorphic encryption scheme, solving an old open problem. Such a scheme allows one to compute arbitrary functions over encrypted data without the decryption key—i.e., given encryptions E(m1), ..., E(mt) of m1, ..., m t,

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 1
January 2019

one can efficiently compute a compact ciphertext that encrypts f(m1, ..., m t) for any efficiently computable function f.

Fully homomorphic encryption has numerous applications. For example, it enables encrypted search engine queries—i.e., a search engine can give you a succinct encrypted answer to your (boolean) query without even knowing what your query was. It also enables searching on encrypted data; you can store your encrypted data on a remote server, and later have the server retrieve only files that (when decrypted) satisfy some boolean constraint, even though the server cannot decrypt the files on its own. More broadly, it improves the efficiency of secure multiparty computation.

In our solution, we begin by designing a somewhat homomorphism "boostrappable" encryption scheme that works when the function f is the scheme's own decryption function. We then show how, through recursive self-embedding, bootstrappable encryption gives fully homomorphism encryption.

3) Public key encryption with keyword search

AUTHORS: D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano

We study the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

4) Practical techniques for searches on encrypted data

AUTHORS: D. X. Song, D. Wagner, and A. Perrig,

It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality. We describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms presented are simple, fast (for a document of length n, the encryption and search algorithms only need O(n) stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today .

5) Privacy preserving keyword searches on remote encrypted data

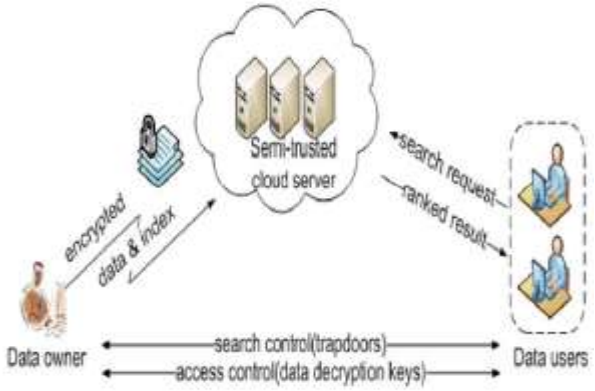
AUTHORS: Y.-C. Chang and M. Mitzenmacher

We consider the following problem: a user U wants to store his files in an encrypted form on a remote file server S. Later the user U wants to efficiently retrieve some of the encrypted files containing (or indexed by) specific keywords, keeping the keywords themselves secret and not jeopardizing the security of the remotely stored files. For example, a user may want to store old e-mail messages encrypted on a server managed by Yahoo or another large vendor, and later retrieve certain messages while travelling with a mobile device.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 1
January 2019

In this paper, we offer solutions for this problem under well-defined security requirements. Our schemes are efficient in the sense that no public-key cryptosystem is involved. Indeed, our approach is independent of the encryption method chosen for the remote files. They are also incremental, in that U can submit new files which are secure against previous queries but still searchable against future queries.

Architecture Diagram:-



III. Related Work:-

Public-Key Encryption with Keyword Search. After Boneh et al. [7] initiated he study of public-key encryption with keyword search (PEKS), several PEKS constructions were put forth using different techniques or considering different situations [8], [11], [12], [13], [14], [15], [22], [23], [24], [25], [26], [27], [28], [29]. They aim to solve two cruces in PEKS: (1) how to make PEKS secure against offline keyword dictionary guessing attacks; and (2) how to achieve expressive searching predicates in PEKS. In terms of the offline keyword dictionary guessing attacks, which requires that no adversary (including the cloud searching server??)

can learn keywords from a given trapdoor, to the best of our knowledge, such a security notion is very hard to be achieved in the public-key setting [30]. Regarding the expressive search, there are only few works in PEKS [8], [13], [14], [15]. Unfortunately, the construction in [13] is built on the basis of inner-product predicate encryption [16], and the constructions in [8], [14], [15] are built from the pairings in composite-order group. Therefore, they are not sufficiently efficient to be adopted in the practical world [16], [17]. Moreover, the number of keywords allowed in these searchable schemes are predefined in the system setup phase. We

compare our scheme to other keyword search schemes in Table 1. It is straightforward to see that compared to the existing ones, our construction make a good balance in that it allows unbounded keywords, supports expressive access

structures, and is built in the prime-order groups.

Private-key Searchable Encryption. In a private-key SE setting, a user uploads its private data to a remote database and keeps the data private from the remote database administrator. Private-key SE allows the user to retrieve all the records containing a particular keyword from the remote database [1], [2], [3]. However, as the name suggests, private-key SE solutions only apply to scenarios where data

owners and data users totally trusted each other.

Private Information Retrieval. With respect to public database such as stock quotes, where the user is unaware of it and wishes to search for some data-item without revealing to the database administrator which item it is, private information retrieval (PIR) [4], [5], [6] protocols were introduced, which allow a user to retrieve data from a public database with far smaller communication then just downloading the entire database. Nevertheless, in our context, the database

is not publicly available, the data is not public, so the PIR solutions cannot be applied.

IV. CONCLUSION

In order to allow a cloud server to search on encrypted data without learning the underlying plaintexts in the public key setting, Boneh [7] proposed a cryptographic primitive called public-key encryption with keyword search (PEKS). Since then, considering different requirements in practice,e.g., communication overhead, searching criteria and security enhancement, various kinds of searchable encryption systems have been put forth. However, there exist only a few public-key searchable encryption systems that support expressive keyword search policies, and they are all built from the inefficient composite-order groups [17]. In this paper, we focused on the design and analysis of public-key searchable encryption systems in the prime-order groups that can be used to search multiple keywords in expressive searching formulas. Based on a large universe key-policy attribute-based encryption scheme given in [18], we presented an expressive searchable encryption system in the prime order group which supports expressive access structures expressed in any monotonic Boolean formulas. Also, we proved its security in the

standard model, and analyzed its efficiency using computer simulations.

V.BIBLIOGRAPHY

References Made From:-

[1] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," J. ACM, vol. 43, no. 3, pp. 431–473, 1996.

[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in 2000 IEEE Symposium on Security and Privacy, Berkeley, California, USA, May 14-17, 2000. IEEE Computer Society, 2000, pp. 44–55.

[3] E. Goh, "Secure indexes," IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[4] C. Cachin, S. Micali, and M. Stadler, "Computationally private information retrieval with polylogarithmic communication," in Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding, ser. Lecture Notes in Computer Science, vol. 1592. Springer, 1999, pp. 402–414.

[5] G. D. Crescenzo, T. Malkin, and R. Ostrovsky, "Single database private information retrieval implies oblivious transfer," in Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding, ser. Lecture Notes in Computer Science, vol. 1807. Springer, 2000, pp. 122–138.

[6] W. Ogata and K. Kurosawa, "Oblivious keyword search," J. Complexity, vol. 20, no. 2-3, pp. 356–371, 2004.

[7] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings, ser. Lecture Notes in Computer Science, vol. 3027. Springer, 2004, pp. 506–522.

[8] J. Lai, X. Zhou, R. H. Deng, Y. Li, and K. Chen, "Expressive search on encrypted data," in 8th ACM Symposium on Information,Computer and Communications Security, ASIA CCS '13, Hangzhou, China - May 08 - 10, 2013. ACM, 2013, pp. 243–252.

[9] P. Golle, J. Staddon, and B. R. Waters, "Secure conjunctive keyword search over encrypted data," in Applied Cryptography and Network Security, Second International Conference, ACNS 2004, Yellow Mountain, China, June 8-11, 2004, Proceedings, ser. Lecture Notes in Computer Science, vol. 3089. Springer, 2004, pp. 31–45.

[10] D. J. Park, K. Kim, and P. J. Lee, "Public key encryption with conjunctive field keyword search," in Information Security Applications, 5th International Workshop, WISA 2004, Jeju Island, Korea, August 23-25, 2004, Revised Selected Papers, ser. Lecture Notes in Computer

Science, vol. 3325. Springer, 2004, pp. 73–86.
[11] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in Pairing-Based Cryptography - Pairing 2007, First International Conference, Tokyo, Japan, July 2-4, 2007, Proceedings, ser. Lecture Notes in Computer Science, vol. 4575. Springer, 2007, pp. 2–22.
[12] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," J. Network and Computer Applications, vol. 34, no. 1, pp. 262–267, 2011.
[13] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007, Proceedings, ser. Lecture Notes in Computer Science, vol. 4392. Springer, 2007, pp. 535–554.
[14] Z. Lv, C. Hong, M. Zhang, and D. Feng, "Expressive and secure searchable encryption in the public key setting," in Information Security - 17th International Conference, ISC 2014, Hong Kong, China, October 12-14, 2014. Proceedings, ser. Lecture Notes in Computer Science, vol. 8783. Springer, 2014, pp. 364–376.
[15] J. Shi, J. Lai, Y. Li, R. H. Deng, and J. Weng, "Authorized keyword search on encrypted data," in Computer Security - ESORICS 2014 -19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part I, ser. Lecture Notes in Computer Science, vol. 8712. Springer, 2014, pp. 419–435.
[16] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," J. Cryptology, vol. 26, no. 2, pp. 191–224, 2013.
[17] D. M. Freeman, "Converting pairing-based cryptosystems from composite-order groups to prime-order groups," in Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings, ser. Lecture Notes in Computer Science, vol. 6110. Springer, 2010, pp. 44–61.
[18] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in 2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013. ACM, 2013,
pp. 463–474.
[19] A. B. Lewko and B. Waters, "Unbounded HIBE and attribute based encryption," in Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings,ser. Lecture Notes in Computer Science, vol. 6632, 2011, pp. 547–567.
[20] X. Boyen and B. Waters, "Anonymous hierarchical identity-based encryption (without random oracles)," in Advances in Cryptology - CRYPTO 2006, 26th Annual

International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings, ser.
Lecture Notes in Computer Science, vol. 4117. Springer, 2006, pp. 290–307.
[21] J. Lai, R. H. Deng, and Y. Li, "Expressive CP-ABE with partially hidden access structures," in 7th ACM Symposium on Information, Compuer and Communications Security, ASIACCS '12, Seoul, Korea, May 2-4, 2012. ACM, 2012, pp. 18–19.
[22] H. S. Rhee, J. H. Park, W. Susilo, and D. H. Lee, "Improved searchable public key encryption with designated tester," in Proceedings of the 2009 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2009, Sydney, Australia, March 10-12, 2009. ACM, 2009, pp. 376–379.
[23] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings, ser. Lecture Notes in Computer Science, vol. 4622. Springer, 2007, pp. 535–552.
[24] C. Gu, Y. Zhu, and H. Pan, "Efficient public key encryption with keyword search schemes from pairings," in Information Security and Cryptology, Third SKLOIS Conference, Inscrypt 2007, Xining, China, August 31 - September 5, 2007, Revised Selected Papers, ser. Lecture Notes in Computer Science, vol. 4990. Springer, 2007, pp. 372–383.
[25] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in Computational Science and Its Applications - ICCSA 2008, International Conference, Perugia, Italy, June 30 - July 3, 2008, Proceedings, Part I, ser. Lecture Notes in Computer Science, vol. 5072. Springer, 2008, pp. 1249–1259.
[26] Q. Tang and L. Chen, "Public-key encryption with registered keyword search," in Public Key Infrastructures, Services and Applications - 6th European Workshop, EuroPKI 2009, Pisa, Italy, September 10-11, 2009, Revised Selected Papers, ser. Lecture Notes in Computer Science, vol. 6391. Springer, 2009, pp. 163–178.
[27] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in 2011 International Conference on Distributed Computing Systems, ICDCS 2011, Minneapolis, Minnesota, USA, June 20-24, 2011. IEEE Computer Society, 2011, pp. 383–392.
[28] H. S. Rhee, J. H. Park, and D. H. Lee, "Generic construction of designated tester public-key encryption with keyword search," Inf. Sci., vol. 205, pp. 93–109, 2012.
[29] W. Yau, R. C. Phan, S. Heng, and B. Goi, "Keyword guessing attacks on secure searchable public key encryption schemes with a designated tester," Int. J. Comput. Math., vol. 90, no. 12, pp. 2581–2587, 2013.
[30] E. Shen, E. Shi, and B. Waters, "Predicate privacy in encryption systems," in Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009, San

Francisco, CA, USA, March 15-17, 2009. Proceedings, ser. Lecture Notes in Computer Science, vol. 5444.
Springer, 2009, pp. 457–473.
[31] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in CRYPTO, ser. Lecture Notes in Computer Science, vol. 2139. Springer-Verlag, 2001, pp. 213–219.
[32] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings, ser. Lecture Notes in Computer Science, vol. 3152. Springer, 2004, pp. 41–55.
[33] A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings,ser. Lecture Notes in Computer Science, vol. 6632. Springer, 2011, pp. 568–588.
[34] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive , efficient, and provably secure realization," in Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9,
2011. Proceedings, ser. Lecture Notes in Computer Science, vol. 6571. Springer, 2011, pp. 53–70.
[35] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 – November 3, 2006. ACM, 2006, pp. 89–98.
[36] R. Ostrovsky, A. Sahai, and B.Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007. ACM, 2007, pp. 195–203.
[37] A. B. Lewko, A. Sahai, and B. Waters, "Revocation systems with very small private keys," in 31st IEEE Symposium on Security and Privacy, S&P 2010, 16-19 May 2010, Berleley/Oakland, California, USA. IEEE Computer Society, 2010, pp. 273–285.
[38] A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, Israel Institute of Technology, Israel Institute of Technology, June 1996.