AN SECURE DATA PROTECTION IN CLOUD STORAGE WITH ESPP APPROACH

Charla Venkata Lakshmi Lalitha

PG Student, Department Of Computer Science And Technology, GITAM School Of Technology, Hyderabad Campus,

GITAM Deemed To University, Hyderabad.

EMail id :- lakshmilalitha.charla@gmail.com

ABSTRACT

Thanks to its potential to deliver low-cost, pay-as-you-go IT infrastructure, outsourcing data into the cloud has become an important practice in modern-day computering. Though cloud-based platforms provide several advantages, outsourced data protection is a major concern. It is possible to outsource confidential data in an encrypted form to alleviate this issue, but the complexity of the encryption method will raise the high computing overhead on thin clients such as resource-constrained mobile devices. Many encryption schemes searchable for keywords have been identified in the literature recent.Nonetheless, these systems are not suitable for resource-constrained mobile apps, because not only does the implemented encryption method allow keyword search over encrypted files, but also have high performance. In this article, we are suggesting an effective and safe approach to privacy protection for outsourced data from resource-constrained mobile devices in cloud computing. Our solution uses a probabilistic, public-key encryption algorithm to encrypt the data, and uses graded keyword search over encrypted data to retrieve files from the cloud. We are working to achieve an effective data protection framework without compromising data privacy.In addition, our ranked keyword search significantly enhances device efficiency by enabling ranking for a search result based on a relevance score, submitting top most important files instead of submitting all files back, and guaranteeing the consistency of the file retrieval. As a consequence, data protection guarantees the decrease of storage, communication overheads. A detailed review of safety and efficiency, we show our method is semi-secure and effective.

KEYWORDS:

Cloud computing, Privacy-preserving, Outsourced data, Probabilistic public-key encryption, Ranked keyword search, Mobile devices.

I. INTRODUCTION

Cloud infrastructure is an evolving form of infrastructure, where computer owners outsource their data to cloud servers. Through transferring data files into the cloud, it offers big organizations as well as individual customers many advantages as they can automatically expand their storage capacity if needed when necessary without purchasing any storage equipment. These are: (1) users can view centrally encrypted data at any time, from anywhere, which enables approved users to share the data. (2) Users should be freed from the local data management pressure, (3) reduction of hardware and device spending, etc.

In fact, all these benefits of outsourced data in the cloud still pose certain major problems. Some of the key concerns is the protection of outsourced data in the cloud, i.e. personal information such as email, health reports and government data that leak or even be compromised to unauthorized users (Cloud Protection Alliance, 2009). Because the cloud is an open network, it can be vulnerable to threats by malicious insiders as well as outsiders The cloud service providers (CSPs) typically offer data protection by mechanisms such as firewalls and virtualization.

These systems, however, are untrusted because of remote cloud storage services, which do not protect user privacy from the CSP itself. A logical solution to protecting confidential data protection is to encrypt data before exporting it to the cloud and retrieve data with a keyword-based scan of encrypted data. Although encryption protects against unauthorized entry, it significantly increases data owners' overhead computing particularly when they have resource-constrained mobile devices and large data file sizes. In addition, the approved users need to download those files from the cloud, connect with the CSPs and allow them to function over the encrypted data.

To order to ensure successful data recovery, it is best to get the most important files instead of getting all files, i.e. the files should be rated and only the most applicable files will be sent back to the customers, which is extremely advantageous to

the "pay-as-you-use" cloud model. Nonetheless, it is a daunting job that safely and effectively retrieves the data back without being able to collect valuable cloud information.

Owner of records, provider of cloud services (CSP), and registered users. Data Owner (DO): is an organization with a vast volume of data to be stored in the cloud, may be human users of limited mobile devices like iphones, PDAs, TPM chips, etc. Cloud Service Provider (CSP): is an organization that automatically delivers data storage and computing services to the data owner and consumers Registered Consumers (AU): the data owner allows authorized users to access their files and exchange any of the key materials with the data owner. The approved users would download the data from the cloud in an encrypted form and get the original data by decrypting it.

Cloud is a storage point where the data is processed by various data providers, i.e. owners for availability and stability. The data owners require the permitted data user to access their data for privacy protection purposes. For example, to have government health-care programs that are adequate or to research the study in medical institutions. Some volunteer patients will consent to share their health information in the cloud for that reason. Data owners must encrypt their data with the hidden key in support of privacy issues.

By this solitary approved association can play out a protected search over encoded data. Considering the above situation building up the multi-proprietor framework is entangled when contrasted with a solitary proprietor framework. In a solitary proprietor framework, data proprietors need to remain online to produce trapdoors (encoded keywords) for data clients. At whatever point an enormous number of data proprietors are included, it for all intents and purposes outlandish that, to request that they remain on the web. Besides, No one needs to share our emit key with others. In the interim, various data proprietors will encode their data with an alternate key so it will turn out to be extremely hard to play out a protected search over the data scrambled with various keys. Then again, side when numerous data proprietors are included, and productive client enrolment and denial instrument is required for framework versatility

The key commitments of our work can be summed up as follows:

1. We propose a productive and secure privacy-preserving approach; it utilizes probabilistic public-key encryption procedures to lessen computational overhead on proprietors while encryption and unscrambling process without releasing any data about the plaintext.

2. Our methodology utilizes ranked keyword search on encoded data to recover the records back. It empowers the cloud server to decide if a given document contains certain keywords and related pertinence scores without knowing any data about both the keywords and the records. It incredibly lessens the correspondence overhead during the record recovery process. It additionally confirms the uprightness of data put away in the cloud

3. Through examination of security exhibits that the proposed plan can be demonstrated semantically secure under various assaults. Besides, the presentation investigation and experiential outcomes show that our plan is productive and it outflanks contrasted and existing plans

II. LITERATURE REVIEW

The primary inspiration driving data redistributing is that the accessibility of data anytime with privacy-preserving. Data security is accomplished utilizing encryption of data before redistributing. While accessibility is a great idea to have an exact outcome. For that reason, D. Tune, D. Wagner, A. Perrig proposed as down to earth methods for searches on encoded data[2]. The untrusted would anything be able to about the plaintext is the upside of this framework. The subjective word search without the client's validation is beyond the realm of imagination.

"Secure Indexes" Secure record is the best answer for the issue of building data structures with privacy ensures, for example, those gave by unaware and history free data structures[3]

Another randomized data structure Bloom channels for speaking to a set to help enrollment questions are disclosed to take care of a verity of system issues to give a bound together numerical and pragmatic system for them and invigorate their utilization in future applications[4].

The private key encryption permits the data proprietor to re-appropriate data for a constrained client with symmetric encryption likewise the private key encryption forestalls searching over encoded data to accomplish the Reza Curtmola purposed Searchable Symmetric Encryption technique[5]. This paper manages the multi-client framework and permits a keyword-based search. For increasingly proficient yield search result the positioning of records gave in made sure about ranked keyword search over encoded cloud data.

It is beneficial for a cloud server to assume liability for delicate data protection from untrusted cloud specialist organizations (CSP) by permitting unscrambling just confided in the client. The framework bolsters keyword-dependent on encoded

data as well as gives superior. Attributes of cloud administrations are concentrated well in this paper and proposed a novel framework for secure and privacy-preserving keyword searching (SPKS)scheme which permits CSP to take an interest in the decipherment and return just records containing certain keywords determined by the client. Keyword search lessens both the computational overhead required to search on scrambled data and correspondence overhead required to share got records. It is demonstrated that a proposed framework semantic protection from versatile picked plaintext attacks.[6]

Ranked search upgrades the framework ease of use by getting the coordinating documents in a ranked request with respect to certain significance criteria[7]. Cong Wang characterizes a request preserving symmetric encryption(OPSE) strategy. The framework very much took a shot at a positioning of records But it won't support multi-keyword search

Wei Zhang proposed a framework that manages upgrading security over keyword and trapdoors. Alongside positioning office added substance request and privacy-preserving capacity family(AOPPF) [8]

Numerous methodologies have been demonstrated to empower searching for encoded data. Most of these methodologies are restricted to a solitary keyword search or a Boolean search yet not a multi-keyword search. A Multi-keyword search gives a progressively pertinent outcome which will builds productivity. For that, a searchable encoded file is changed in the paper. Likewise, the quantity of pertinence scores is considered for the positioning of the archive. Other than that, a little temporary work must be finished in regards to incorrectly spelled keyword search since the paper just arrangement with likeness keyword coordinate search.[9]

Privacy-preserving multi-keyword fluffy search over scrambled data in the cloud "Propose a novel multi-keyword fluffy search conspire by misusing the area touchy hashing procedure. Our proposed plot accomplishes fluffy coordinating through algorithmic plan as opposed to growing the list document. It additionally disposes of the requirement for a predefined word reference and viably underpins numerous keyword fluffy search [10]

"A proficient and secure privacy-preserving approach for outsourced data of asset obliged mobile devices in cloud computing"[11]proposed a strategy Public key encryption calculation for encoding the data and summon ranked keyword search over the scrambled data to recover the documents from the cloud. We mean to accomplish a productive framework for data encryption without relinquishing the privacy of data. Further, our ranked keyword search incredibly improves the framework ease of use by empowering positioning dependent on a pertinence score for a search result, sends top most important documents as opposed to sending all records back, and guarantees the document recovery exactness. we propose an Efficient and Secure Privacy-Preserving approach(ESPPA) utilizing probabilistic public-key encryption and ranked keyword search. In addition, our plan likewise confirms the respectability of the data. we will improve ESPP calculation to help productive powerful data activities and ranked keyword search over the scrambled enormous data in the cloud as future work.

III. EXISTING SYSTEM

Cloud computing is an rising computing model where the facts proprietors are outsourcing their data into cloud storage. By outsourcing the information documents into the cloud, it offers many advantages to the large businesses as well as man or woman customers because they can dynamically make bigger their storage area as and when required barring buying any storage devices

They are:

(1) the users can get right of entry to the remotely saved statistics at any time, from anywhere, and approves approved users to share the data.

(2) The users can be relieved from the burden of storage administration at locally,

(3) Avoidance of capital expenditure on hardware and software program costs etc. To date, there are countless cloud storage services: Amazon easy storage Space (S3), Rack space, Google, Microsoft, etc.

Besides, all of these advantages of outsourced facts in the Cloud, there are additionally some good sized issues.

3.1. Searchable encryption schemes primarily based on symmetric key encryption

The symmetric key encryption scheme lets in a data proprietor to outsource its records symmetrically encrypted to an untrusted server and later to search for a particular file in the server with the aid of a trapdoor.

Although normal searchable symmetric encryption schemes allow a user to securely search over encrypted facts through key-words and retrieve the files of their interest, these strategies assist only the genuine key-word search. That is there is no tolerance of minor kinds and format inconsistencies. This sizable drawback makes present strategies unsuitable in Cloud computing as

it considerably impacts gadget usability, rendering consumer looking experiences are very irritating and machine efficiency is very low.

However, all these schemes are working based on symmetric key encryption, the place a single key used to encrypt and decrypt the data. If the information proprietor desires to share the secrete-key, which is used in trapdoor era to all licensed users. Sharing a secret key by means of several users forms a high-security danger on account that it can effortlessly leak to the unauthorized parties. Once the unauthorized parties examine the secret key, they can break the machine and access the data.

3.2. Searchable encryption based on public-key encryption

To keep away from key leakage problems, the public-key encryption is used in a comparable state of affairs with two keys: one key is for encryption and some other for decryption.

However, now not all these schemes support for resource-constrained devices. This is due to their encryption and the decryption manner creates system overhead on the system.

To avoid the above problems, Liu et al. (2012), proposed a invulnerable and privacy-preserving key-word looking scheme for cloud storage services the usage of ElGamal public-key encryption based on Elliptic Curve Cryptography (ECC) over Fp. It permits the CSP to participate in the decipherment, and return the encrypted documents containing certain key-words barring knowing any information. However, this scheme may disclose facts to the cloud service provider due to the fact it approves the CSP to take part in the encryption process. Furthermore, like previous schemes (Song et al., 2000; Goh, 2003; Chang and Mitzenmacher, 2005; Curtmola et al., 2006; Li et al., 2010; Kuzu et al., 2012; Lu, 2012), this scheme does not support the ranked search technique. To guide ranked key-word search with less efficiency, Yu et al., (2013) proposed a Two-Round Searchable Encryption (TRSE) scheme that supports top-k multi-keyword retrieval based on ranking. the TRSE scheme used a vector space mannequin and homomorphic encryption techniques, it allows customers to involve in the ranking technique whilst the majority of computing works accomplished at the server-side through operations only on the ciphertext. As a result, statistics leakage can be eliminated and protection is ensured. However, the computation and conversation charges of this method are pretty massive due to the fact each search term in a question requires quite a few homomorphic encryption operations both on the server and on the user side. Further, it uses a two-round conversation method to retrieve the information from the server.
One of the foremost troubles is the privateness of outsourced information in the cloud (Jaeger and Schiffman, 2010) i.e., the touchy records such as e-mail, health records, and government data may additionally leak to unauthorized customers (Slocum, 2009; Krebs, 2009) or even be hacked (Cloud Security Alliance, 2009). Since the cloud is an open platform; it can be subjected to assaults from both malicious insiders and outsiders (Haclgiimfi et al., 2002). Cloud provider vendors (CSPs) typically provide statistics protection through mechanisms like firewalls and virtualization. However, these mechanisms do now not defend users' privateness from the CSP itself due to far off cloud storage servers are untrusted.

IV. PROPOSAL SYSTEM

In this paper, we propose a productive and secure privacy-preserving way to deal with keep away from all the above issues while preserving the privacy and respectability of outsourced data in the cloud. In our plan, the data proprietor first forms the list for record assortment, encodes both list and data documents, and stores them in the cloud. Afterward, to recover the put away documents from the cloud server, the approved client produces a trapdoor for keywords and sends it to the server. After accepting the trapdoor, the cloud server searches for a rundown of coordinated record sections and their relating encoded significance scores.

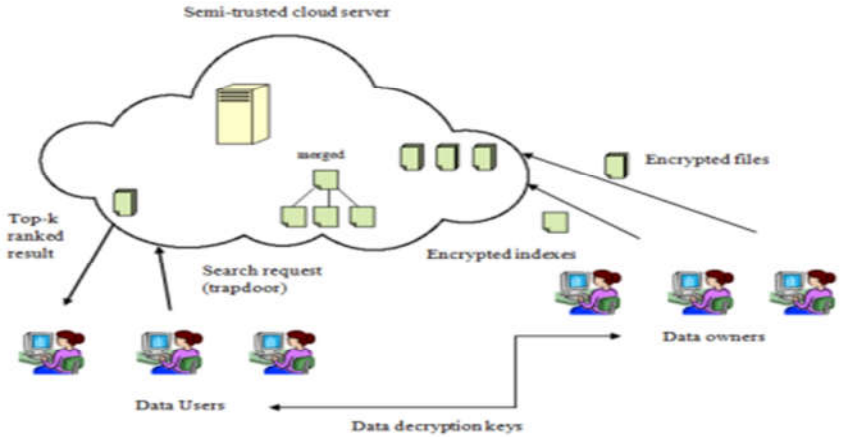

Figure 1 System Model

As Fig.1 shows, there are three elements in which two are entertainers i.e., data proprietors and data clients where third is cloud stockpiling. Data proprietors have a huge assortment of documents F to redistribute. To empower proficient multi-keyword searches on the scrambled records, every data proprietor first forms a protected searchable tree-based list I which is required for effective searching. The activity of data proprietors is to scramble their data records F with their keys and redistribute both the encoded tree-based list and data documents to the cloud server. While accepting the tree-based lists, the cloud server combines different scrambled lists without bargaining data proprietors' privacy. At the point when the data client searchest keywords over the scrambled records and get k encoded documents, he initially processes the trapdoors T and submits T and k to the cloud server. While getting the trapdoors T and k, the cloud server starts searching the blended file tree I and returns the comparing assortment of the top-k ranked encoded records.

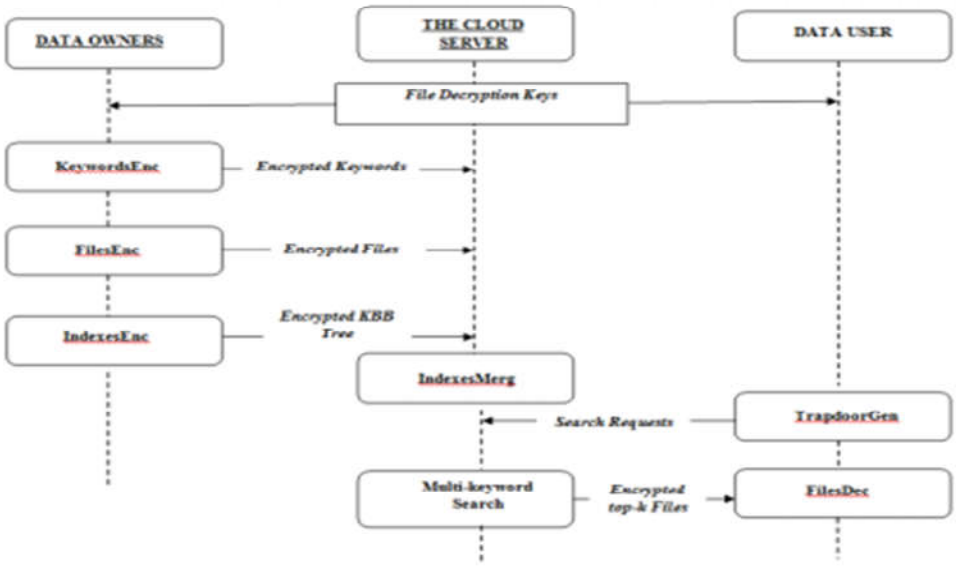

Fig2 working process

The job of these three substances are as given underneath:

• Data Proprietors

1) keywords encodes the keyword with data proprietors' mystery key koi,w;

2) FilesEnc uses the customary symmetric encryption calculation to scramble data proprietors' records;

3) Files Enc constructs the tree-based record for every data proprietor and encodes the KBB-tree with AOPPF.

4) data proprietors transfer encoded keywords, documents, and KBB-trees to the cloud server.

• Data Clients

1) TrapdoorGen produces trapdoors with data clients' mystery key kui,w, and afterward submits trapdoors and the quantity of removed records k to the cloud server;

2) FilesDec decodes scrambled records.

• Cloud Server

1) Files Merg blends numerous encoded trees;

2) Multi-keyword Search runs the DFS calculation to discover the comparing records and returns the adjusted top-k scrambled documents to data clients.

V. EFFICIENT AND SECURE PRIVACY-PRESERVING APPROACH(ESPPA)

The current TRSE conspire has been proposed dependent on completely homomorphic encryption and positioned catchphrase look for the protection of re-appropriated information. Be that as it may, homomorphic encryption builds the overwhelming computational weight on the information proprietor side of portable asset compelled cell phones, and positioned catchphrase search procedure would expand the high correspondence overhead because of the two-round correspondence between the cloud server and the approved client for record recovery.

To ease the calculation and correspondence overhead and guarantee the protection of re-appropriated information of asset compelled cell phones in the cloud, we propose an Efficient and Secure Privacy-Preserving approach (ESPPA) utilizing probabilistic open key encryption and positioned catchphrase search. In our plan, the information proprietor makes a list for document assortment at that point scrambles both files and records. Afterward, the approved client creates an inquiry and sends it to the server. At the point when the cloud server gets an inquiry, it scans for comparing records and sends top-k coordinated documents to the approved client. At that point, the client decodes the documents and gets the first information. The ESPPP comprises of three stages: (1) Setup stage, (2) Retrieval Phase and (3) Integrity check

In the arrangement stage, the information proprietor initially produces open and private key sets. At that point constructs the record from numerous catchphrases removed from document assortment, at that point figure the pertinence score and add to list post list. At that point, to guarantee the protection of the list and record assortment, the information proprietor scrambles both. At last, the information proprietor circulates the encoded records and lists to the cloud server.

Afterward, in the recovery stage, the information proprietor or approved client produces trapdoor for a lot of watchwords and send it to the server. At that point, the server scan for the coordinated documents and their corre-sponding pertinence scores dependent on trapdoor. On the off chance that watchwords coordinate with record, the server positions the coordinated documents based pertinence score and send the documents to the client in a positioned arranged way. At that point the information proprietor or client unscrambles the record utilizing private key.

VI. RESULT ANALYSIS

In this segment, we present a presentation investigation of the ESPPA, in which correspondence and calculation costs are broke down independently. Particularly, low calculation costs on the data proprietor and approved clients side are urgent for rendering the ESPP approach is achievable for mobile applications where the data proprietor and clients as a rule play out all calculations through asset compelled mobile devices, for example, cell phones.

We have directed the trial assessment of the proposed ESPPP plot on the genuine data set: Request For Comments (RFC) database (RFC, 2012). Our analysis condition incorporates the client and server. The client utilizes the C programming language on a Linux machine with double Intel Xeon CPU running at 2.0 GHz and calculations utilize both open ssl and MATLAB libraries and the server use C programming on a Linux machine with Xeon E5620 CPU running at 2.4 GHz. The client goes about as a data proprietor, approved client, and the server goes about as a

CSP. The presentation of our plan assessed proficiency regarding calculation and correspondence costs.

Calculation cost

In this area, we assess the calculation cost of the data proprietor, approved client, and cloud server.

Data Owner

Here, we measure the calculation cost of the data proprietor during the arrangement stage, which incorporates key age, encryption, and file assemble calculations. We principally focus on the calculation cost of the data proprietor for scrambling the document assortment and contrast the trial results and the current plan.

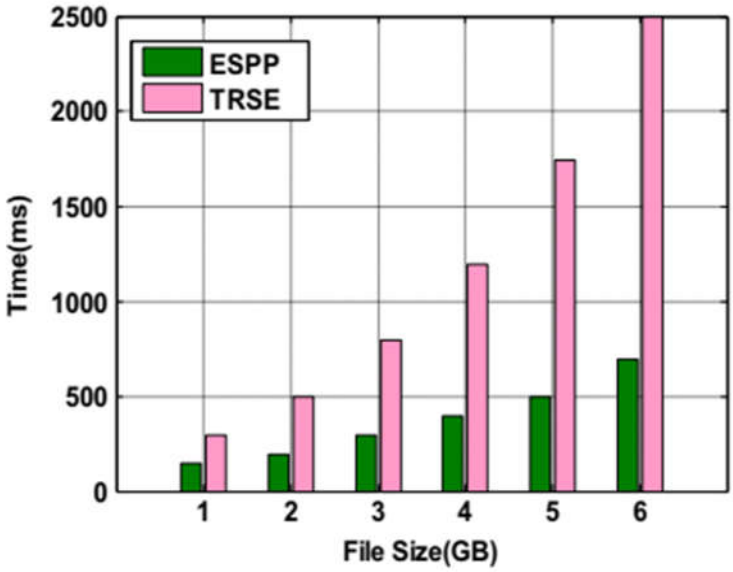

Fig. 3. Computation cost of Data Owner for Encrypting the File.

Fig. 3 shows that ESPPA encryption process is quite efficient because it takes only 1 modular multiplication to encrypt h bits of plaintext. By comparing TRSE encryption technique (Yu et al., 2013), the ESPPA encryption takes less computation cost for longer files (GB).

Conclusions

In this paper, we tended to the issue of supporting proficient and secure privacy-preserving ranked keyword search over the encoded data for accomplishing viable data use of out-sourced scrambled data of asset compelled mobile devices in the cloud. The client's data ensured against privacy infringement. We initially introduced a fundamental review on existing plans and indicated that those are extremely wasteful to accomplish privacy of outsourced data and not appropriate for asset compelled mobile devices. At that point, we proposed an Efficient and Secure Privacy-Preserving approach dependent on probabilistic public-key encryption and ranked multi-keyword search. We initially made a record for document assortment and put away both list and record assortment in the cloud in a scrambled structure. Afterward, to recover data documents, the approved client makes a trapdoor and sends it to the server. At that point, the server begins to search for comparing records over the encoded data by means of a trapdoor. The server restores the coordinating records back to the client if any document matches with keywords. We fittingly increment the proficiency of our plan by utilizing probabilistic public key encryption tech-nique instead of other encryption strategy for document encryption. In addition, our plan likewise confirms the honesty of the data. At long last, we have demonstrated that ESPPA fulfills the security and proficiency prerequisites through security and execution analysis.ESPPA is a component that permits a client to search by ranked keywords on

scrambled data. It targets preserving the privacy of the outsourced data of the proprietor while giving a way that permits a client to search productively without the need of decoding the ciphertext. In this manner, ESPPA has gotten increasingly significant away and recovery of encoded outsourced data of asset obliged mobile devices in cloud computing

REFERENCES

1. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, A. Konwinski A, Lee G, Patterson DA, Rabkin A, Stoica I, Zaharia M. Above the clouds: a Berkeley view of cloud computing, Technical Report UCB-EECS-2009-28. Berkeley: University of Cali-fornia; 2009. p. 1–23.

2. Attrapadung N, Li Bert B. Functional encryption for inner product: achieving con-stant size cipher text switch adaptive security or support for negation. In: Nguyen P, Pointcheval D, editors. Public Key Cryptography, 6056 LNCS. Springer Berlin/Heidelberg; 2010. p. 384–402.

3. Bao F, Deng R, Ding X, Yang Y. Private query on encrypted data in multi-user set-tings. In: Proceedings of 4th international conference on information security practice and experience. Sydney; 2008. p. 71–85.

4. Bellare M, Boldyreva A, Neill AO. Deterministic and efficient searchable encryption. In: Menezes A, editor. Advances in Cryptology-CRYPTO 2007, 4622 LNCS. Berlin/ Heidelberg: Springer; 2007. p. 535–52.

5. Boldyreva A, Chenette N, Lee Y, O'Neill A. Order-preserving symmetric encryption. In: Proceedings of 28th annual international conference on theory and appli-cations of cryptography techniques. Springer, Germany; 2009. p. 224–41.

6. Boneh D, Crescenzo GD, Ostrovsky R, Persiano G. Public key encryption with key-word search. In Proceedings of international conference on theory and appli-cations of cryptographic techniques: advances in cryptology. Switzerland; 2004. p. 506–22.

7. Cao N, Wang C, Li M, Ren K, Lou W. Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Trans Parallel Distrib Syst 2014;25(1):222–33.

8. Chang Y-C, Mitzenmacher M. Privacy preserving keyword searches on remote encrypted data. In: Proceeding of Third International Conference on Applied Cryptography and Network Security. New York; 2005. p. 442–55.

9. Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing; 2009. ⟨http://www.cloudsecurityalliance.org⟩.

10. Curtmola R, Garay JA, Kamara S, Ostrovsky R. Searchable symmetric encryption:improved definitions and efficient constructions. In: Proceedings of 13th ACM conference on computer and communication security. Alexandaria; 2006. p. 79–88.

11. Haclgiimfi H, Iyer B, Li C, Mehrotra S. Executing SQL over encrypted data in database-service-provider model, Technical Report TR-DB 02 02. Irvine: Database Research Group at University of California; 2002.

12. Jaeger PT, Lin J, Grimes JM. Cloud computing and information policy: computing in a policy cloud? J Inform Technol Polit 2009;5(3):269–83.
13. Jaeger T, Schiffman J. Outlook: Cloudy with a chance of security challenges and improvements. IEEE Secur Priv 2010;8(1):77–80.
14. Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Proceedings of 27th annual international conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg; 2008. p. 146–62.

15. Kuzu M, Saiful Islam M, Kantarcioglu M. Efficient similarity search over encrypted data. In: Proceedings of IEEE international conference on data engineering. Washington; 2012. p. 1156–67.

16. Li J, Wang Q, Wang C, Cao N, Ren K, Lou W. Fuzzy keyword search over encrypted data in cloud computing. In: Proceedings of of IEEE 29th international con-ference on computer communications. San Diego; 2010. p. 441–5.

17. Liu Q, Wang G, Wu J. Secure and efficient privacy preserving keyword searching for cloud services. J Netw Comput Appl, 35. Elsevier; 927–33.

18. Menezes Alfred J, van Oorschot Paul C, Vanstone Scott A. A hand book of applied cryptography. FL: CRC Press; 1996.

19. Shi E, Bethencourt J, Chan H, Song D, Perrig A. Multi-dimensional range query over encrypted data. In: Proceedings of IEEE symposium on security and privacy. California; 2007. p. 350–64.

20. Slocum Z. Your Google docs: soon in search results?; 2009. ⟨http://news.cnet.com/ 8301-17939_109-10357137-2.html⟩.

21. Song D, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Proceedings of the IEEE symposium on security and privacy. California; 2000. p. 44–55.

22. Wang C, Cao N, Ren K, Lou W. Enabling secure and efficient ranked keyword search over outsourced cloud data. IEEE Trans Parallel Distrib Syst 2012;23
23. (8):1467–79.

24. Waters B, Balfanz D, Durfee G, Smetters D. Building an encrypted and searchable audit log. In: Proceedings of annual network and distributed security symposium. California; 2004.

25. Yu J, Lu P, Zhu Y, Xue G, Li M. Toward secure multi-keyword top-k retrieval over encrypted cloud data. IEEE Trans Depend Secur Comput 2013;10(4):239–50.