International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Survey on Feature Extraction Techniques for Outsourced Encrypted Multimedia Content Data Analysis

Pranjali M Marne, Prof. P.M.Kamde
Department of Computer Network, Sinhgad College of Engineering, Savitribai Phule, Pune University, Pune, 411041, Maharashtra, India.

ABSTRACT

Currently, most data owners are interested in outsourcing their large amount of personal multimedia data in the cloud. In such cases, sometimes these outsourced multimedia data may disclose the private information of the owner of the information. Therefore, there is a need for a strong protocol. Currently, most of the techniques have been developed to support the efficient and safe extraction of functions over the outsourced multimedia data. These surveys also make comparative analysis of such techniques, which represents the advantages and limitations. Also after analyzing the techniques, the authors provide a general framework of the system that will be better than the proposed system.

Keywords : Personal multimedia data, Outsourced Multimedia data, Cloud computing.

I. INTRODUCTION

Increasing the cloud-based data services, data owners are store their huge amount of personal multimedia data files and computationally expensive task onto remote cloud server. While taking part in the plentiful storage and computation assets for price saving and flexibility, the outsourcing of statistics garage and computation to the cloud moreover increases great safety and privacy worries due to the diverse trust domains the facts proprietor and the cloud belong to .

As Cloud Computing gets to be fundamental, increasingly more sensitive statistics are being centralized into the cloud, as an instance, emails, non-public fitness records, private films and pix, agency finance information, government documents, and so forth. The aid of putting away their information into the cloud, the facts owners can be relieved from the load of records garage and maintenance so as to enjoy the on-demand excessive quality records storage carrier. anyways, the manner that information proprietors and cloud server are not inside the identical relied on domain may positioned the outsourced information at danger, because the cloud server may additionally now not be absolutely confided in this kind of cloud situation, due to numerous reasons: the

Cloud server might also leak information data to unauthorized entities or be hacked. It follows that sensitive information typically should be encrypted previous to outsourcing for facts private ness and preventing unsolicited accesses.

However, information encryption makes effective facts use an exceptionally tough challenge given that there could be quite a few outsourced statistics documents. Additionally, in

Cloud Computing, information proprietors may also percentage their outsourced facts to an extensive number of customers. The person clients may additionally need to most effective retrieve certain unique facts documents they're desirous about amid a given consultation. one of the maximum popular methods is to specially facts documents thru keyword-based search in preference to retrieving all of the encrypted documents returned which is definitely impractical in cloud computing eventualities. Such keyword-based seek approach allows clients to mainly retrieve files of hobby and has been usually implemented in plaintext search situations, for example, Google search. Tragically, information encryption confines customer's capacity to carry out keyword search and hence makes the conventional plaintext seek techniques unsuitable for Cloud Computing. other than this, data encryption additionally requests the warranty of protection of keyword privacy when you consider that keywords commonly comprise crucial information associated with the statistics files. Despite the fact that encryption of key phrases can defend key-word privacy, it in addition renders the traditional plaintext seek systems vain on this scenario.

In the existing literature, efforts on private ness-maintaining outsourcing calculation have been dedicated to unique numerical issues such as modular exponentiation, linear equations and kNN search. These works in the main focus on engineering computation issues over numerical facts or textual content records. Simplest in latest years, private ness-maintaining facts search in the cipher textual content domain has been extended to content material-based multimedia retrieval, face popularity and fingerprint identity.

The researcher investigated the way to allow secure photograph search inside the facts outsourcing surroundings. All things considered, all of them accept that the snap shots were pre-processed by means of some feature extraction algorithms to get their vector representations [18, 19]. Due to the importance of picture function extraction in multimedia records processing and its widespread operations on massive records, particularly for satellite facts for its great length and expansive variety of characteristic points, the extraction or identification of picture functions from the cipher text area has begun to attract increasingly more studies hobby.

Organization of the paper:

Paper begins via offering the associated work in phase II.Our machine is defined in phase III. phase IV gives a few discussion of the proposed device. At final phase V concludes the paper.

II. LITERATURE SURVEY

In paper [1] Hu S.et. Al. proposed an effective and realistic private ness-keeping computation outsourcing protocol for the triumphing scale-invariant feature rework (SIFT) over huge encrypted picture records. They first show that the previous solutions to this problem have both performance/protection or expediency reasonableness troubles, and none can well store the imperative qualities of the unique SIFT in terms of strong point and robustness.

Then present a brand new scheme design that achieves performance and security necessities concurrently with the upkeep of its key traits, through randomly splitting the authentic picture statistics, designing two novel powerful conventions for secure duplication and examination, and deliberately conveying the characteristic extraction computations onto two independent cloud servers.

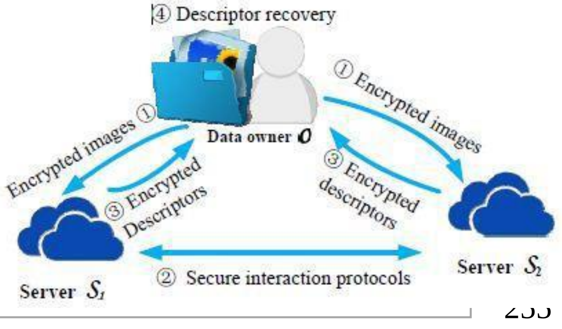


Fig.1 System Architecture [1]

In paper [2] Q. Wang ET. Al. supplied a new and novel privateness preserving SIFTS outsourcing protocol. Authors carefully analyze and substantially evaluate the security and effectiveness of our design. Also experimental outcomes indicate that our protocol outperforms the modern-day and plays comparably to the authentic SIFT and is practical for actual-world applications.

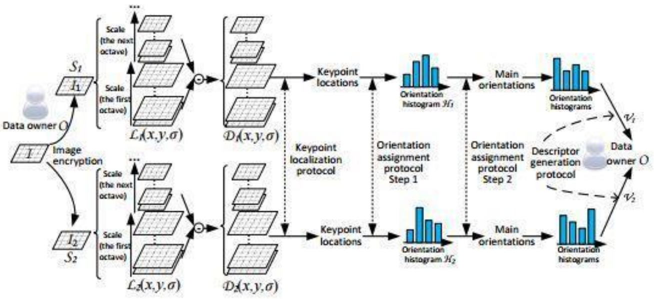


Fig.2 System Architecture [2]

In paper [3] the k. Ren et.al. Define several crucial protection demanding situations and motivate in addition investigation of protection solutions for a honest public cloud environment.

In paper [4] Z. Fu et al studied and solve the problem of personalized multi-key-word ranked search over encrypted records (PRSE) whilst keeping privacy in cloud computing. To tackle the regulations of the model of "one size healthy all" and key-word specific seek, they suggest PRSE schemes for distinct search intentions.

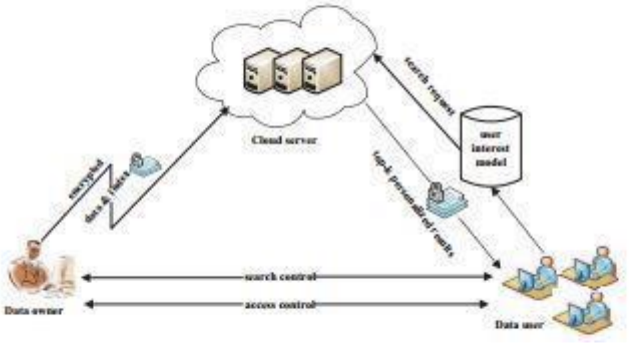


Fig.3 System Architecture [4]

In paper [5] Z. Xia et al built a special tree-primarily based index structure and advice a "Greedy Depth-first Search" algorithm to provide green multi-keyword ranked search. The proposed plan can accomplish sub-direct search time and manipulate the deletion and insertion of documents flexibly.

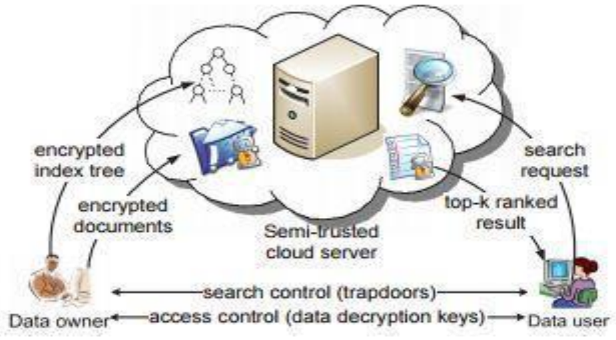
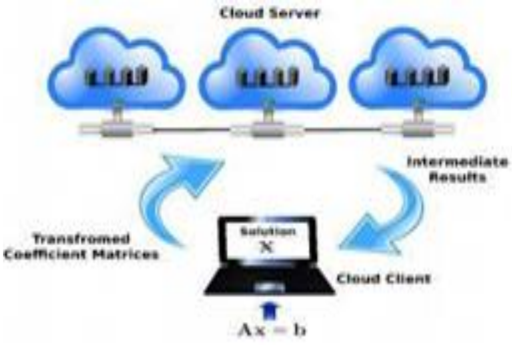


Fig.4 System Architecture [5In paper [6] S. Salinas et al develop an efficient and practical secure outsourcing algorithm for solving large-scale LSEs, which has both low computational complexity and low memory I/O complexity and can secure clients' privacy well. Author actualizes their calculation on a real-world cloud server and a portable workstation. They find that the proposed algorithm offers significant time savings for the client (up to 65%) compared to previous algorithms.



In paper [7] L. Weng et al introduce the idea of tunable privacy, where the private ness protection level can be adjusted according to coverage. It is acknowledged through hash-based piecewise rearranged indexing. Two unique developments of robust hash calculations are utilized. The outcomes demonstrate that the security upgrade marginally enhances the recovery execution.

the discrete logarithm problem and RSA that PPSIFT is secure against cipher text only attack and known plaintext attack.

In paper [9] Z. Brakerski and V. Vaikuntanathan present a relatively holomorphic encryption scheme that is each quite simple to demonstrate and observe, and whose security (quantumly) reduces to the worst-case hardness of troubles on ideal lattices. They then transform it into a totally holomorphic encryption scheme the usage of standard “squashing” and “bootstrapping” strategies introduced by means of Gentry (STOC 2009).

In paper [10] Z. Ren et al given In paper [7] L. Weng et al introduce the idea of tunable privacy, where the private ness protection level can be adjusted according to a coverage. It is acknowledged through hash-based piecewise rearranged i

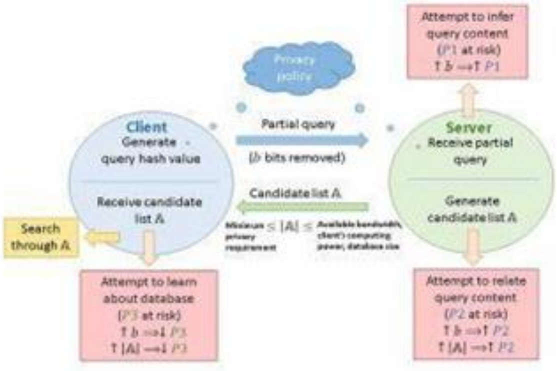

Privacy policy
Attempt to infer query content (P1 at risk) ↑b ⟶↑ P1
Client
Generate query hash value
Receive candidate list A
Partial query
(b bits removed)
Candidate list A
Minimum privacy requirement ≤ |A| ≤ Available bandwidth, client's computing power, database size
Server
Receive partial query
Generate candidate list A
Search through A
Attempt to learn about database (P3 at risk) ↑b ⟶↓ P3 ↑|A| ⟶↓ P3
Attempt to relate query content (P2 at risk) ↑b ⟶↑ P2 ↑|A| ⟶↑ P2

Fig.6 System Architecture [7]

In paper [8] C.-Y. Hsu et al propose a privacy-preserving awareness of the SIFT approach primarily based on holomorphic encryption. They display via the security analysis based on the discrete logarithm problem and RSA that PPSIFT is secure against cipher text only attack and known plaintext attack.

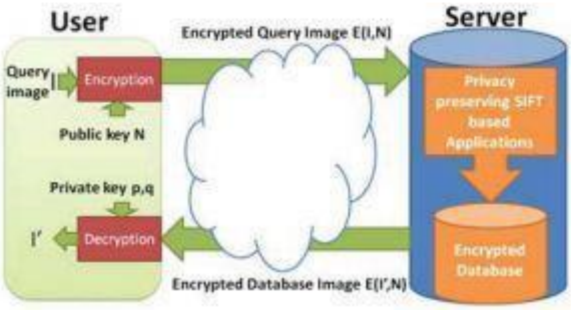

User
Server
Encrypted Query Image E(I,N)
Query image
I
Encryption
Public key N
Private key p,q
I'
Decryption
Privacy preserving SIFT based Applications
Encrypted Database
Encrypted Database Image E(I',N)

Fig.7 System Architecture [8]

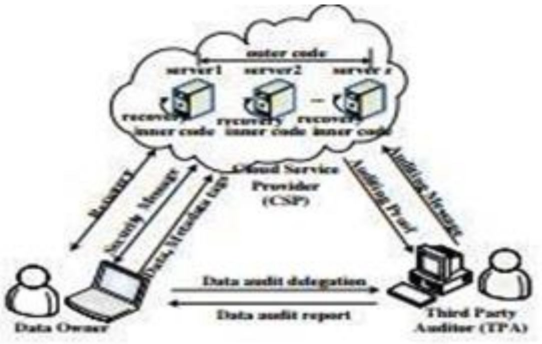
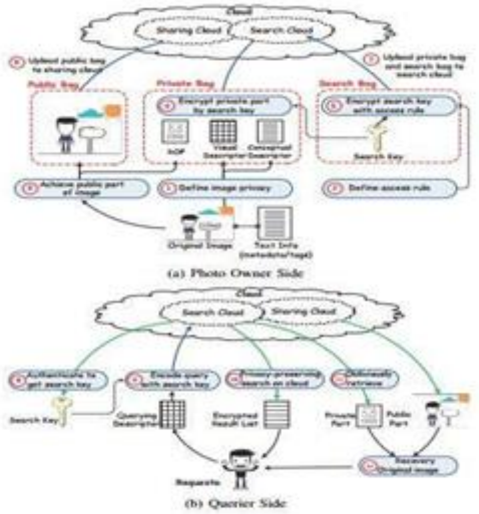


Fig.8 System Architecture [10]

In paper [11] Y. Elmehdwi et al proposed SkNN protocols on encrypted information in the cloud. the primary protocol, which acts as a basic answer, leaks some records to the cloud. Additionally authors say that developed 2nd protocol is completely comfortable, which is, it protects the confidentiality of the records, consumers enter query, also hides. The data access patterns. the second protocol is extra steeply-priced in comparison to the primary protocol. In paper [12] M. Osadchy et al developed SCiFI, a device for at ease Computation of Face identification. The gadget performs face identification which compares faces of subjects with a database of registered faces. The identity is carried out in a comfortable way which protects both the private ness of the subjects and the confidentiality of the database. a specific utility of SCiFI is reducing the private ness impact of camera primarily based surveillance.

Fig.9 Examples of variation in test images

In paper [13] L. Zhang et al introduced gadget POP that allows cloud servers to give privacy-preserving photo sharing and searching carrier to cell device customers who intend to outsource picture management while protecting their private ness in pictures. Given machine no longer simplest protects the outsourced snap shots so that no unauthorized customers can get entry to them, but additionally enables users to encode their image search so that the hunt also can be outsourced to an un-trusted cloud server obliviously without leakage at the question contents or results.



(a) Photo Owner Side

(b) Querier Side

Fig. 10: POP System Overview

In paper [14] L. Zhang et al have given a system known PIC towards privacy preserving content-based search on large-scale outsourced photographs. With our careful layout, most people of the computationally in depth image matching jobs are outsourced to the cloud in a non-interactive way, but the photograph and query privateness is preserved.

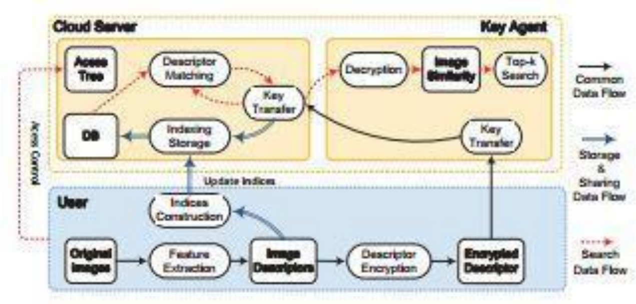


Fig.11 System Architecture [14]

In paper [15] C.-Y. Hsu et al given a homomorphic encryption-based totally privacy preserving SIFT (PPSIFT) approach to solve with the privacy preserving problem found in a cloud computing surroundings, where the server can end the tasks of SIFT primarily based programs without learning anything to breach the user's privateness. In PPSIFT, the maximum hard hassle, i.e., homomorphic comparison has been solved in this paper. Authors also demonstrated that the implemented Paillier cryptosystem-based PPSIFT systems achieve provable security depending on DLP and RSA.

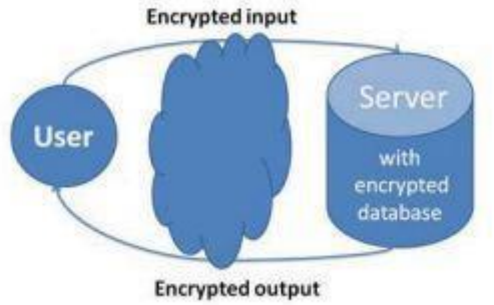


Fig.12 System Architecture [15]

II. PROPOSE SYSTEM

In latest maximum of the information proprietors interested by outsourcing their huge amount of private multimedia records onto the cloud as it's far the cost efficient and flexible solution. Such records is utilized by most of the provider companies or some other programs for diverse purpose such as getting to know, searching or for behavioral advertising. In such instances every so often this outsourced multimedia records may expose the information owner's non-public information.

So on this paper authors will use the protocol of privacy maintaining computation over outsourced multimedia records

When Scale-Invariant feature Transform (SIFT) function extraction approach follow on encrypted image records. in this paper, next they uses those extracted feature descriptors in content based searching by using third party users with high level of security over encrypted image statistics. To check the performance of gadget, they use Breast cancer image dataset and analyze our proposed machine.

Experimental effects will prove that the proposed solution is very green and effective for image seek over encrypted photo records and achieves excessive degree private ness maintenance with SIFT characteristic descriptors.

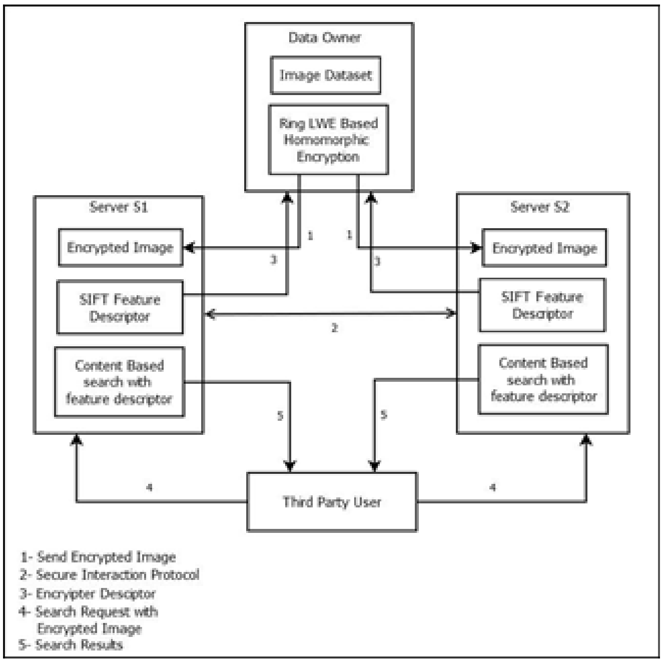


Fig.13: System Architecture for proposed system

III. CONCLUSION

This paper provides a secure framework for the private ness keeping outsourced storage, their search, and retrieval in those huge-scale outsourced image repositories. Such repositories are dynamically up to date. This survey shows a few recent strategies has been evolved for supporting thee efficient and comfortable function extraction over outsourced multimedia statistics. Also gives the constraints of all techniques with purpose to be in addition useful for new improvements in a same area.

This survey shows some recent techniques has been developed for supporting the efficient and secure feature extraction over outsourced multimedia data. Also presents the limitations of all techniques that will be further useful for new improvements in same area.

IV. REFERENCES

[1]. Hu S, Wang Q, Wang J, Qin Z, Ren K. SecSIFT: Privacy-preserving Outsourcing Computation of Feature Extractions over Encrypted Image Data," in IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411-3425, July 2016.

[2]. Q. Wang, S. Hu, K. Ren, J. Wang, Z. Wang, and M. Du,

[3]. "Catch me in the dark: Effective privacy-preserving outsourcing of feature extractions over image data,- in Proc. of INFOCOM'16, Accepted to appear, 2016.

[4]. K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud,- IEEE Internet Computing, vol. 16, no.1, pp. 69–73, 2012.

[5]. Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement,- IEEE Transactions on Parallel and Distributed Systems, 2015, DOI: 10.1109/TPDS.2015.2506573

[6]. Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data,- IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340–352, 2015.

[7]. S. Salinas, C. Luo, X. Chen, and P. Li, "Efficient secure outsourcing of large-scale linear systems of equations,- in Proc. of INFOCOM'15.IEEE, 2015, pp. 1035–1043.

[8]. L. Weng, L. Amsaleg, A. Morton, and S. Marchand Maillet, "A privacy-preserving framework for large-scale content-based information retrieval,- IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 152–167, 2015.

[9]. C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, "Image feature extraction in encrypted domain with privacy-preserving sift,- IEEE Transactions on Image Processing, vol. 21, no. 11, pp. 4593–4607, 2012.

[10]. Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-lwe and security for key dependent messages,- in Proc. Of CRYPTO'11. Springer, 2011, pp. 505–524

[11]. Z. Ren, L. Wang, Q. Wang and M. Xu, "Dynamic proofs of retrievability for coded cloud storage systems", IEEE Trans. Services Computing, vol. PP, no. 99, pp. 1, Sep. 2015.

[12]. Y. Elmehdwi, B. K. Samanthula and W. Jiang, "Secure k-nearest neighbor query over encrypted data in outsourced environments", Proc. IEEE ICDE, pp. 664-675.

[13]. M. Osadchy, B. Pinkas, A. Jarrous and B. Moskovich, "SCiFI-A system for secure face identification", Proc. IEEE S&P, pp. 239-254.

[14]. L. Zhang, T. Jung, C. Liu, X. Ding, X.-Y. Li and Y. Liu, "POP: Privacy-preserving outsourced photo sharing and searching for mobile devices", Proc. IEEE ICDCS, pp. 308-317.

[15]. L. Zhang, T. Jung, P. Feng, K. Liu, X.-Y. Li and Y. Liu, "PIC: Enable large-scale privacy preserving content-based image search on cloud", Proc. IEEE ICPP, pp. 949-958.

[16]. C.-Y. Hsu, C.-S. Lu and S. Pei, "Image feature extraction in encrypted domain with privacy-preserving SIFT", IEEE Trans. Image Process., vol. 21, no. 11, pp. 4593-4607, Nov. 2012.

[17]. http://www.webopedia.com/TERM/C/cloud_computing.html

[18]. M. I. M. Almanea, "A Survey and Evaluation of the Existing Tools that Support Adoption of Cloud Computing and Selection of Trustworthy and Transparent Cloud Providers," Intelligent Networking and Collaborative Systems (INCoS), 2014 International Conference on, Salerno, 2014, pp. 628-634.

[19]. M.K. Khan and Q. Malluhi, "Establishing trust in cloud computing", IT Professional, vol. 12, no. 5, pp. 20-27, 2010.

[20]. M.R. Savola, A. Juhola and I. Uusitalo, "Towards wider cloud service applicability by security privacy and trust measurements", 4th International Conference on Application of Information and Communication Technologies, 2010. Lambo, Why You Need A Cloud Rating System, 2013.

[21]. S. Gagnono, V. Nabelsi, K. Passerini and K. Calisi, "The next web apps architecture: Challenges for saas vendors", IT Professional, vol. 13, no. 5, pp. 44-50, 201

[22]. W. Pauley, "Cloud provider transparency: An empirical evaluation", IEEE Security and Privacy, vol. 8, no. 6, pp. 32-39, 2010.

[23]. K.S. Garg, S. Versteeg and R. Buyya, A Framework for Ranking of Cloud Computing Services, 2012.