ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

IOPE:Improved Order Preserving Encryption Scheme For Mobile Cloud Environment

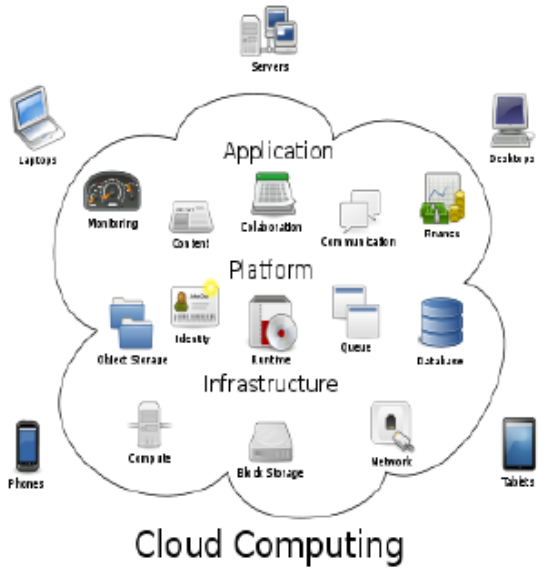
[1] Banuchandhar J [2] Saravanan S
[1] PG Scoholar [2] Asst.Professor
[1][2]Department of Computer Science and Engineering
M.Kumarasamy College Of Engineering, Karur

Abstract:-- **Cloud computing inflates its presence within the public sector, people and organizational bodies that are searching for cloud services to enhance security,productivity and scale back costs. With the exception of communication, file storage is that the main demand for people. Ancient DC(Data Centers) comprises massive collections of server farms implementing and preserving security measures. Cloud offers a multi-tenant service, during which the construct of the network perimeter vanishes. For the previous concern, encryption before outsourcing is that the easiest way to shield data privacy. However encryption additionally makes applying ancient data utilization services — a troublesome. This drawback on the way to search encrypted data has recently inflated attention and led to the event of searchable encryption techniques. During this work we are try and implement Improved Order preserving Encryption (IOPE), a primitive that permitting an economical standard vary queries on encrypted docs. This can be a sort of Searchable encryption scheme. IOPE improves the protection of OPE within the sense, because it doesn't leak the data regarding the placement of plaintext, Boldyvera et.al. The main objective of this work is to boost the protection provided by the present IOPE approaches with the assistance of variable Mobile cloud environment.**

Index Terms:— **Order Preserving Encryption, Deterministic Encryption, Multi-Keyword, Improved OPE, Mobile Cloud, Searchable Encryption**

I. INTRODUCTION

In the generation of computer technology, information science has moved from workstations to private computing devices to server-centric computing to the online. Today, several organizations are seriously considering adopting cloud computing, consecutive notable achievements in technology and business integration[1]. Cloud computing model has been outlined by NIST(National Informatics Science and Technology) as a model for enabling convenient, on-demand network access to a shared storage of configurable computing resources (e.g., servers, storage, applications,networks and services) that may be quickly provisioned and discharged with lowest management effort or cloud provider interaction. Cloud Computing remains a work in progress [2]. Although cloud computing edges are tremendous, security and privacy issues are the first obstacles to wide adoption [3]. As a outcome of Cloud Service Providers (CSPs) are separate admin entities, migrating to the business cloud deprives users of direct management over the systems that manage the applications and data.



Fig(a)Cloud Architecture

Although CSPs‘ infrastructure and management capabilities are way more powerful and reliable than those of private computing devices, the cloud platform still faces each

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

internal and external security and privacy threats, as well as media failures, software system bugs, malware, administrator errors and malicious insiders. Noteworthy outages and security breaks to cloud services appear from time to time[3]. as a result of users don‘t have access to the cloud‘s internal operational details, CSPs may additionally voluntarily examine users‘ data for varied reasons while not detection[4].Although it inflates resource utilization, this unique multitenancy feature additionally presents new security and privacy vulnerabilities for user interactions[5].Hence, we tend to argue that the cloud is per se insecure from a user‘s viewpoint. while not providing a robust security and privacy guarantee, we tend to can‘t expect users to show management of their data and computing applications over to the cloud primarily based entirely on economic savings and service flexibility[3]. consistent with users involved within the cloud may be classified in to a few classes.

A public cloud is one during which the infrastructure and different computational resources that it contains are created obtainable to general public over the web. it's owned by a cloud provider commercialism cloud services and by definition is external to a corporation greater control over the infrastructure and machine resources than does a public cloud [2].As individuals and enterprises turn out additional and more data that has to be stored and utilised , they‘re motivated to source their local complicated data management systems to the cloud attributable to its larger flexibility and cost-efficiency. However, once users now not physically possess their data, its confidentiality and integrity may be at risk[4].Traditionally, to regulate the disperse nature of privacy-sensitive data, users establish a trustworthy server to store data regionally in clear, and so control that server to visualize whether or not requesting users present proper certification before belongings them access the data[8]. From a security position, this access management architecture isn't any longer applicable once we source data to the cloud. Data encryption before outsourcing is the easiest way to guard data privacy and combat uninvited access within the cloud and on the far side. however encryption additionally makes deploying ancient data utilization services — like plaintext keyword search over textual data or question over information — a troublesome task.

The trivial resolution of downloading all the info and decrypting it regionally is clearly impractical, owing to the massive bandwidth cost ensuing from cloud-scale systems. Moreover, apart from eliminating local storage management, storing data within the cloud serves no purpose unless individuals will simply search and utilize that data. Another vital issue that arises once outsourcing data service to the cloud is protective data integrity and semi-permanent storage correctness. though outsourcing data to the cloud is economically attractive for semi-permanent, large scale storage, it doesn‘t immediately guarantee data integrity and availability. This drawback, if not properly addressed , will impede the successful preparation of a cloud architecture. providing users no longer locally possess their data, they can’t utilize ancient cryptographic primitives to guard its correctness[5].

Such primitives typically need local copy of the data for integrity verification, which isn‘t viable when storage is outsourced. moreover, the large quantity of cloud data and the user‘s unnatural computing capabilities build data correctness auditing in a very cloud environment expensive and even formidable [5].Other challenging security issues embrace assured data deletion and remote assessment of fault tolerance that's, the remote detection of hard-drive failure vulnerabilities in the cloud[7].

Ultimately, the cloud is neither smart nor bad: it‘s simply a replacement paradigm with its own benefits and drawbacks. Over time, a number of these issues are resolved or the risks are reduced to acceptable levels. For now, these issues have unbroken cloud adoption at a modest pace.[6] the remainder of the paper is organized as follows: Section two List, a number of the Searchable encryption techniques. Existing works so as protective encryption is listed in Section three. Section 4, list the planning goals of this work .Section five justify concerning our projected work. Performance analysis is discussed in section six. Section seven presents a security analysis of our approach. Finally Section eight offers the conclusion of the complete work exhausted this paper.

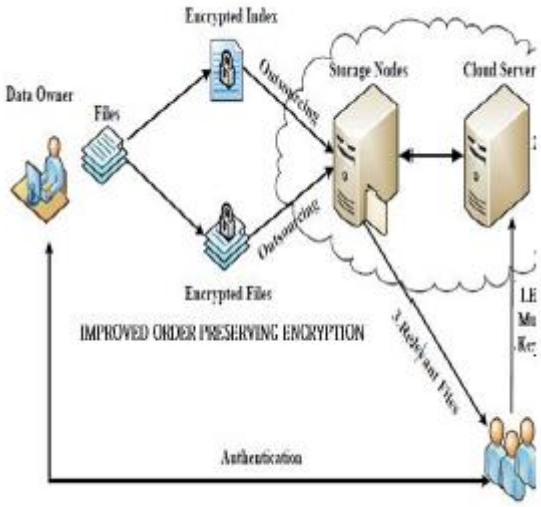
II. PROPOSED METHOD

A. Using Improved Order preserving encryption

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

Improved order-preserving encryption (IOPE), due to Boldyreva et al. [8], could be a promising extension that increases the protection of the essential OPE by introducing a secret improved offset to every data worth before encrypting it. However, execution vary queries via IOPE in a very native way permits the individual to be told this offset, negating any potential security gains of this approach. We tend to attempt to implement Improved order-preserving encryption (IOPE), during which the scheme of variable Mobile Cloud Area (MCA) prepended with a OPE. IOPE with MCA improves the potency of IOPE during a sense, because it manufacture coins that are additional sophisticated to brute force.



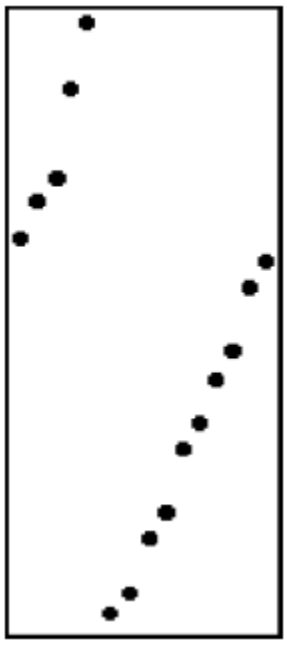
Fig(a) Encrypted Search Architecture of IOPE

An Improved order-preserving encoding (IOPE) scheme is an extension to OPE that increases its security. Rather than process such a scheme generally, we tend to outline a change to get it from a given OPE scheme. The transformation. Let OPE = (Kg′; EncA′; DecA′) be an OPE scheme. We tend to outline the associated Improved OPE scheme IOPE [OPE] = (Kg; EncA; DecA) wherever

Notations used

Kg = Key generator
EncA = Encryption Algorithm
DecA =Decryption Algorithm
MK = Group size
D = Subgroup size
n =Sample size

* Kg generates K ←$ Kg′ and j← $[I]; it outputs (K; j).
* EncA on inputs a key Kg and a plaintext m outputs Enc′ (K, I + j mod I).
* Dec on inputs a key Kg and a cipher text c outputs DecA (K; c) ─ j mod I. Above, the value j in the secret key of IOPE [OPE] is called the secret offset or displacement.



Fig(b)IOPE (Encrypted Value Distribution).

Using variable hyper geometric Distribution

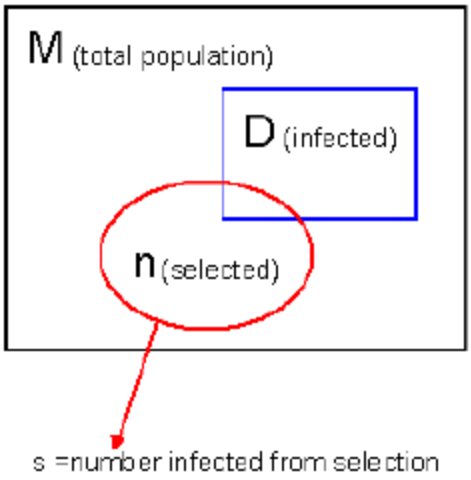
Discrete distributions will solely take a separate variety of values. This variety could also be infinite or finite. In HGD, Models the amount of things of a specific sort there'll be during a sample of size n wherever that sample is drawn from a population of size _M‘ of that _D‘ also are of that specific sort. An extension of the hyper geometric distribution wherever over two sub-populations of interest exist is termed variable hyper geometric distribution. Multivariate distributions describe many parameters whose values are probabilistically joined in some way [23]. The MHGD is formed by extending the arithmetic of the HGD. For the HGD with a sample of size n, the chance of observant

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

s people from a sub-group of size M, and so (n-s) from the remaining variety (M-D):

$$f(x) = \frac{\binom{D}{x}\binom{M-D}{n-x}}{\binom{M}{n}}$$



Fig(c) Multivariate Hyper geometric distribution and results in the probability distribution for s:

The dividend is that the variety of various sampling mixtures (each of that has an equivalent chance as a result of every individual has identical chance of being sampled) wherever one would have precisely s from the sub-group D and by implication (n-s) from the sub-group (M-D). The divisor is that the total variety of various mixtures one may have in choosing n individuals from a gaggle of size M. therefore the equation is simply the proportion of various attainable situations, every of that has an equivalent chance that will provide us s from D [23]. The variable hyper geometric chance equation is simply an extension of this concept. D1, D2, D3 and then on are the amount of people of different sorts during a population, and x1, x2, x3, ... are the quantity of successes. And leads to the chance distribution for:

$$f(x) = \frac{\binom{D_1}{x_1}\binom{D_2}{x_2}\cdots\binom{D_k}{x_k}}{\binom{M}{n}}$$

$$\sum_{i=1}^{k} D_i = M, \sum_{i=1}^{k} x_i = n$$

Pseudo code for encryption algorithm

Existing IOPE methodology, use a HGD methodology for coin generation. We tend to alter that in an exceedingly easy way to victimization MHGD methodology for coin generation. Below mentioning psudocode describe the notations and logic that are wont to implement MHGD in IOPE. See encryption algorithm for the formal descriptions of Enc, wherever as before l1 = l(D,R,y) is that the variety of coins required by MHGD on inputs D,R, y, and lR is that the range of coins required to select part of R uniformly randomly.

Encryption Algorithm for Using MHGD for IOPE
Encryption $_{Key}$ (H, S, I)

1. Assign |H| to I and |R| to N.
2. Compute min (H)-1 and assign it to d;
3. Compute min(S)-1 and assign it to r;
4. Compute [N/2], add with 2 and assign it toy;
5. Verify whether |H| = 1 then
A. Call Tape Gen function with parameters K, 1l1, (H, S, 0||Y)) assign the result to cc.
b. Assign S to c.
c. Return c.
6. Return Encrypted values.
1. Compute parameters H, S, y,n;cc and assign the result to x.
2. Verify if I is less than are equal to x then
a. Assign {d+1 ...x} to H.
b. Assign {r+1 ...y} to S.
3. Else
a. Assign {x+1,.....,d+I} to H.
b. Assign {y+1,.....,r+N} to S.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

The potency of our scheme follows from our previous analyses. encryption and decryption need the time for at the most logN + three invocations of MHGD on inputs of size at the most logN and at the most (5 logM + 14) . (5 logN + λ‘ + 1)=128 invocations of AES on the average for λ‘within the theorem. 5.

Security Analysis

We tend to show that a random commonplace OPF, not sort of a random OPF, absolutely hides the locations of the information points. we are going to to boot arrange to project escape with relevancy distance and window-distance one-wayness. On the opposite hand, if the individual is prepared to recover one far-famed plaintext-cipher text mix, security falls back thereto of a random OPF in Previous theme but our planned methodology not exactly reveal the plaintext - Cipher text strive. we tend to tend to propose a changes to Associate in Nursing existing IOPE theme that collectively improves the protection performance of any OPE. the following theme isn't to any extent further strictly order-preserving, but it still permits vary queries. However, presently the queries ought to be commonplace vary queries. consumer vary queries are not supported, as only ―improved order‖ rather than order is leaked. The changes in IOPE is simple, generic, and primarily free computation-wise. Notice that a IOPE is acceptable for normal vary question support as follows. To request the cipher texts of the messages at intervals the vary [m1;m2] (if money supply 9 m2), or [m1;M][[1;m2] (if money supply > m2), the user computes c1 Encm(K;m1); c2 Encm(K;m2) and submits cipher texts (c1; c2) as a result of the question. The server returns the cipher texts at intervals the interval [c1; c2] (if c1 9 c2) or [c1; N] [[1; c2] (if c1 > c2).Note that Associate in Nursing IOPF might instead be made public with a MHGD following the OPF rather than a random plaintext shift preceding it. The advantage of the upper than definition is that the map from (OPF, cipher text offset) pairs to IOPFs is objective whereas at intervals the varied it is not matched.

III. PERFORMANCE ANALYSIS

We tend to propose a way that improves on the efficiency of any IOPE theme whereas not sacrificing security. ROPF analysis reveals information leak in OPE not alluded to by [9], specifically regarding the locations of the information points instead of merely the distances between them. we tend to propose a modification to Associate in Nursing IOPE theme that overcomes this. The modification to the theme is easy and generic: the coding formula merely adds a secret offset to the message before coding. The key offset is that an equivalent for all messages. we tend to tend to use a way MHGD for improved OPE theme, and generalize the protection notion: the proper object is presently a random improved OPF (RIOPF), i.e. a random OPF applied to messages with a haphazardly picked offset. It’s straightforward to visualize that any IOPE theme, victimization MHGD yields a cost-effective style for the on prime of transformation.

IV. CONCLUSION

We revisited security of symmetrical order-preserving schemes made public in [9]. we tend to tend to formally clarify the strengths and limitations of any OPE theme established to be a pseudorandom order-preserving function(POPF), and particularly, the economical OPE theme planned in [9]. Namely, for any POPF-secure OPE our analysis beside the results of [9] provides higher bounds on the advantages of any adversaries assaultive the unidirectional land and distance unidirectional land, (2) lower bounds on the window unidirectional land and window distance unidirectional land edges. we tend to tend to hope our results facilitate practitioners to estimate the risks and security guarantees of using a secure OPE in their applications. Our analysis collectively provides directions in selecting the scale of the cipher text house. Finally we tend to tend to propose a straightforward and economical transformation that may be applied to any IOPE theme. Our analysis shows that the transformation yields a theme with improved efficiency during this the theme resists the one-wayness and window one-wayness attacks.

REFERENCES

[1] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds: towards a cloud definition,” ACM SIGCOM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[2] X. Yu and Q. Wen, "Design of security solution to mobile cloud storage," in Knowledge Discovery and Data Mining. Springer, 2012 pp. 255–263.

[3] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011.

[4] O. Mazhelis, G. Fazekas, and P. Tyrvainen, "Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage," in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012, pp. 646–653.

[5] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, "Virtualized in-cloud security services for mobile devices," in Proceedings of the First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35.

[6] J. Oberheide and F. Jahanian, "When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments," in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications. ACM, 2010, pp. 43–48.

[7] A. A. Moffat, T. C. Bell et al., Managing gigabytes: compressing and indexing documents and images. Morgan Kaufmann Pub, 1999.

[8] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44– 55.

[9] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology- Eurocrypt 2004. Springer, 2004, pp. 506–522.

[10] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.

[11] Y. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Applied Cryptography and Network Security. Springer, 2005, pp. 391–421.

[12] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, "Zerber+ r: Topk retrieval from a confidential index," in Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology. ACM, 2009, pp. 439–449.

[13] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 8, pp. 1467–1479, 2012.

[14] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. IEEE, 2010, pp. 253–262.

[15] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[16] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in INFOCOM, 2014 Proceedings IEEE.

[17] J. Zobel and A. Moffat, "Inverted files for text search engines," ACM Computing Surveys (CSUR), vol. 38, no. 2, p. 6, 2006.

[18] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proceedings of the 2004 ACM SIGMOD international conference on Management of data. ACM, 2004, pp. 563–574.

[19] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent dirichlet allocation," the Journal of machine Learning research, vol. 3, pp. 993–1022, 2003.

[20] J. Ramos, "Using tf-idf to determine word relevance in document queries," Technical report,Department of Computer Science, Rutgers University, 2003.
[21] D. Hiemstra, "A probabilistic justification for using tf idf term weighting in information retrieval," International Journal on Digital Libraries, vol. 3, no. 2, pp. 131–139, 2000.

[22] K. Jones, "Index term weighting," Information storage and retrieval, vol. 9, no. 11, pp. 619–633, 1973.

[23] Q. Chai and G. Gong, "Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers," in Communications (ICC), 2012 IEEE International Conference on. IEEE, 2012, pp. 917– 922.

[24] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography and Data Security. Springer, 2010, pp. 136– 149.

[25] M. Li, S. Yu, K. Ren, W. Lou, and Y. T. Hou, "Toward privacyassured and searchable cloud data storage services," Network, IEEE, vol. 27, no. 4, pp. 56–62, 2013.

[26] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, ser. ASIA CCS '13. New York, NY, USA: ACM, 2013, pp. 71–82.

[27] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in INFOCOM, 2011 Proceedings IEEE. IEEE, 2011, pp. 829–837.

[28] S. Hou, T. Uehara, S. Yiu, L. C. Hui, and K. Chow, "Privacy preserving multiple keyword search for confidential investigation of remote forensics," in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on. IEEE, 2011, pp. 595–599.

[29] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Applied Cryptography and Network Security. Springer, 2004, pp. 31–45.

[30] A. Aizawa, "An information-theoretic perspective of tf-idf measures," Information Processing and Management, vol. 39, pp. 45–65, 2003.

[31] G. Salton and M. J. McGill, "Introduction to modern information retrieval," McGraw-Hill, Inc.,New York, NY, 1986.
[32] E. Han and G. Karypis, "Centroid-based document classification: Analysis and experimental results," Principles of Data Mining and Knowledge Discovery, pp. 116–123, 2000.

[33] L. Baker and A. McCallum, "Distributional clustering of words for text classification," in Proceedings of the 21st annual international ACM SIGIR conference on Research and development in information retrieval. ACM, 1998, pp. 96–103.

[34] A. Boldyreva, N. Chenette, Y. Lee, and A. O´ neill, "Orderpreserving symmetric encryption," Advances in Cryptology- EUROCRYPT 2009, pp. 224–241, 2009.

[35] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," Advances in Cryptology–EUROCRYPT 2010, pp. 24–43, 2010.

[36] C. Gentry and S. Halevi, "Implementing gentry´s fullyhomomorphic encryption scheme," Advances in Cryptology– EUROCRYPT 2011, pp. 129–148, 2011.

[37] A. Swaminathan, Y. Mao, G. Su, H. Gou, A. Varna, S. He, M. Wu, and D. Oard, "Confidentiality-preserving rank-ordered search," in Proceedings of the 2007 ACM workshop on Storage security and survivability. ACM, 2007, pp. 7–12

[38] C. O¨ rencik and E. Savas¸, "Efficient and secure ranked multikeyword search on encrypted cloud data," in Proceedings of the 2012 Joint EDBT/ICDT Workshops. ACM, 2012, pp. 186–195.

[39] K. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage," in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 187–198.

[40] J. Zhang, B. Deng, and X. Li, "Additive order preserving encryption based encrypted documents ranking in secure cloud storage," Advances in Swarm Intelligence, pp. 58–65, 2012.

[41] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

[42] D. Stehl´e and R. Steinfeld, "Faster fully homomorphic encryption," Advances in Cryptology-ASIACRYPT 2010, pp. 377–394, 2010.

[43] K. Kumar and Y. Lu, "Cloud computing for mobile users: Can offloading computation save energy?" Computer, vol. 43, no. 4, pp. 51–56, 2010.

[44] A.Miettinen and J. Nurminen, "Energy efficiency of mobile clients in cloud computing," in Proceedings of the 2nd USENIX conference on Hot topics in cloud computing, 2010, pp. 21–28.

[45] A. Carroll and G. Heiser, "An analysis of power consumption in a smartphone," in Proceedings of the 2010 USENIX conference on USENIX annual technical conference. USENIX Association, 2010, pp. 271–284.

[46] Wikipedia, http://en.wikipedia.org/wiki/tf-idf.

[47] J. Zobel and A. Moffat, "Exploring the similarity space," in ACM SIGIR Forum, vol. 32, no. 1. ACM, 1998, pp. 18–34.

[48] A. Schulman, T. Schmid, P. Dutta, and N. Spring, "Demo: Phone power monitoring with battor." MobiCom, 2011.