Supporting Complex Queries and Access Policies for Multi-User Encrypted Databases

Muhammad **Rizwan** Asghar, Giovanni Russello, Bruno Crispo, Mihaela Ion

The 5th ACM Workshop on Cloud Computing Security Workshop (CCSW)

in conjunction with

The 20th ACM Conference on Computer and Communications Security (CCS),

Berlin, Germany

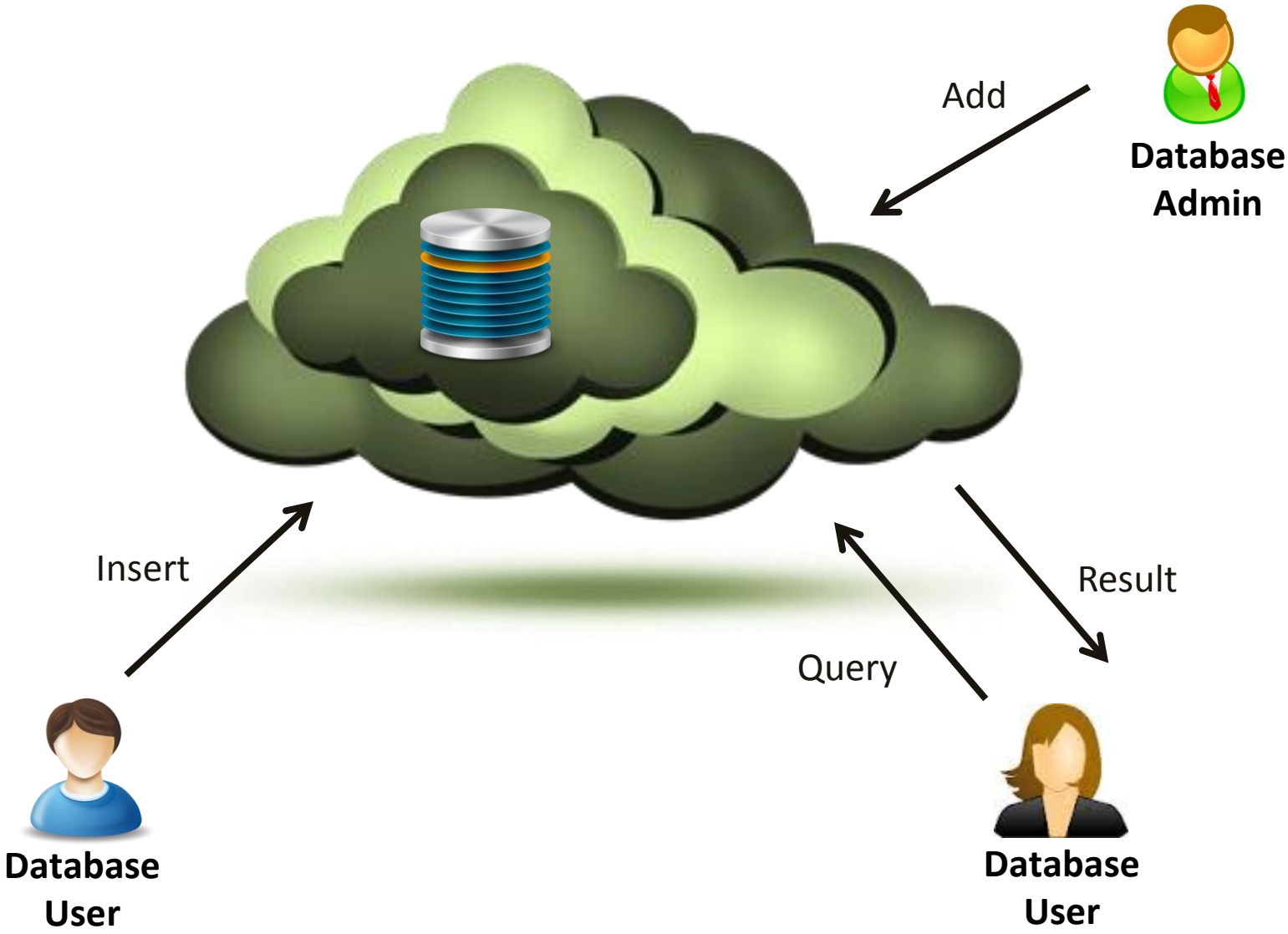
November 8, 2013

UNIVERSITÀ DEGLI STUDI DI TRENTO

Why Cloud Storage

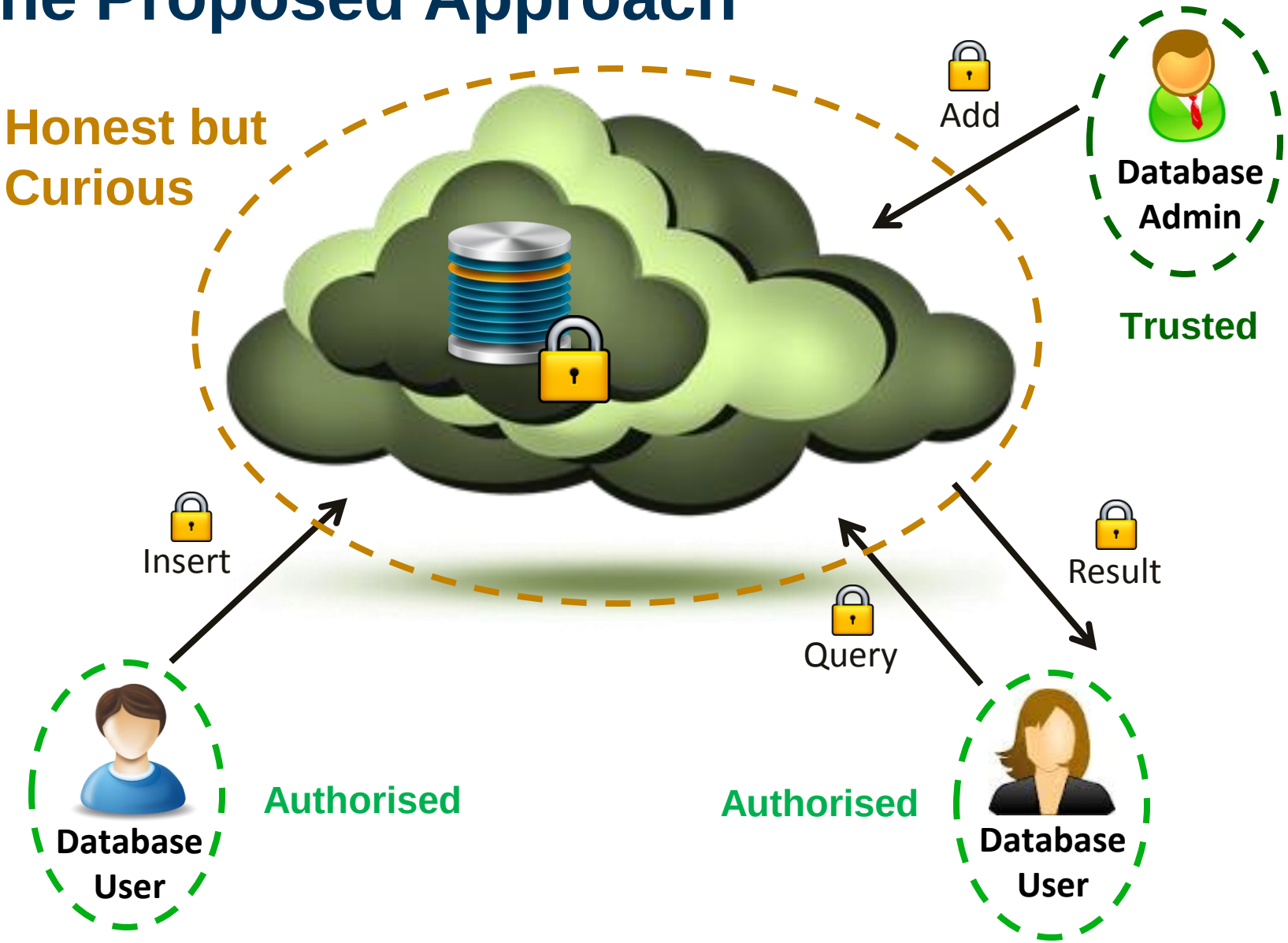
- Cost saving 
- Scalability 
- Efficiency 
- Availability 

Problem



End-to-end confidentiality/privacy

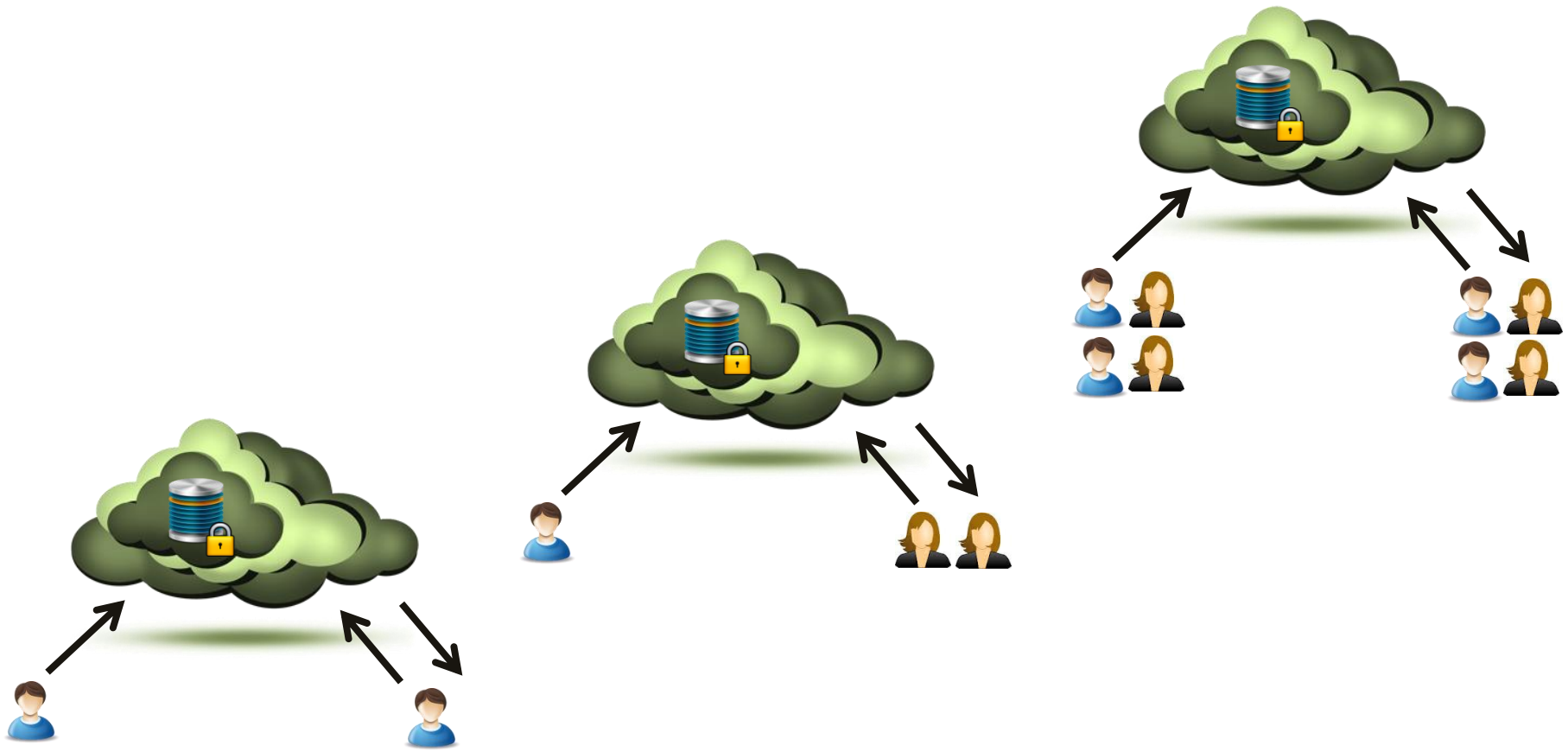
The Proposed Approach



Supported Queries

Keyword	**SELECT *name* FROM *Personnel* WHERE *position=manager***
Conjunction, Disjunction of Keywords	**SELECT *name* FROM *Personnel* WHERE *position=manager* AND *sex=female* OR *level=2***
Complex Queries (e.g., range queries)	**SELECT *name* FROM *Personnel* WHERE *position=manager* OR *age>30* AND *age<40***

State-of-the-Art Scheme Types



Single User	Semi-Fledged Multi-User	Full-Fledged Multi-User

State-of-the-Art

	Single User	Semi-Fledged Multi-User	Full-Fledged Multi-User
Keyword	Song et. al. (2000) Goh (2003) Chang and Mitzenmacher (2005) Hacigumus et. al. (2005)	Boneh et. al. (2004) Curtmola et. al. (2006) Zhu et. al. (2011)	Bao et. al. (2008) Dong et. al. (2008) Shao et. al. (2010)
Con/Dis-junction	Golle et. al. (2004) Bosh et al. (2011)	Baek et. al. (2008) Rhee et al. (2010) Cao et al. (2011)	Hwang et. al. (2007)
Complex	Hore et. al. (2004) Wang and Lakshmanan (2006) Popa et. al. (2011) Hore et. al. (2012)	Boneh and Waters (2007) Katz et. al. (2008) Yang et. al. (2011) Li et. al. (2011) Lu and Tsudik (2011)	**No Solution**

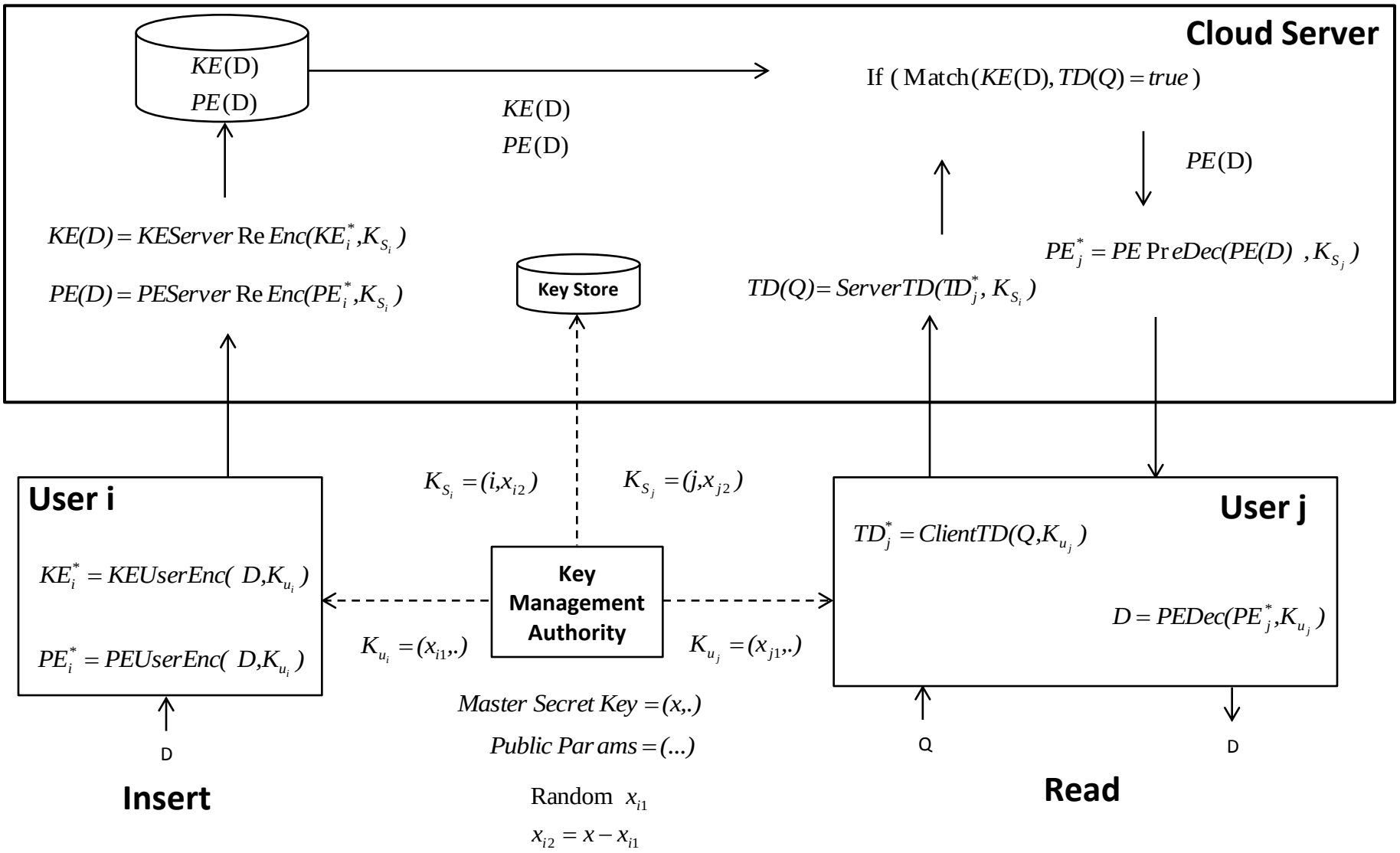
Our Proposed Solution

- We propose full-fledged multi-user scheme that supports complex queries
- Our proposed mechanism protects queries and data stored in the cloud
- We enable enforcement of access control policies
- Users do not share any keys and each user has her own key
- A user can be removed without requiring re-distribution of keys or re-encryption of stored data

Solution Overview

- For data insertion and ***retrieval***, we employ **Proxy Encryption (PE)**
  - Insert data → PE
  - Retrieve data → PE
- For making data ***searchable***, we use **Keyword Encryption (KE)**
  - Insert data → KE
  - Make query → Trapdoor (TD)
  - Perform matching → Match
- We protect access control policies using KE

Solution Details



Representation of Tables and Queries

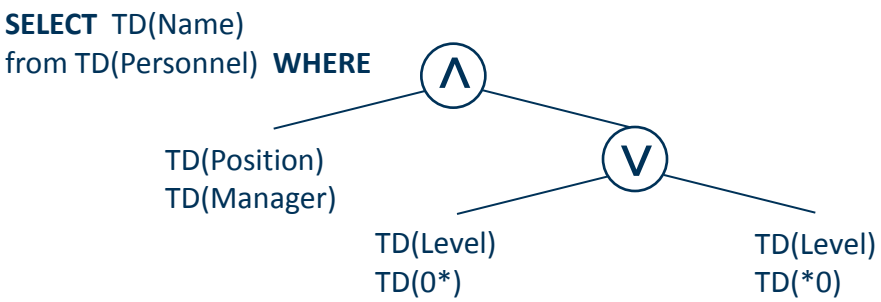
Personnel			
Name	***Gender***	***Position***	***Level***
Andy	Male	Manager	2

$\{Personnel\}_{KE}$			
$\{Name\}_{KE}$	$\{Gender\}_{KE}$	$\{Position\}_{KE}$	$\{Level\}_{KE}$
$\{Name\}_{PE}$	$\{Gender\}_{PE}$	$\{Position\}_{PE}$	$\{Level\}_{PE}$
$\{Andy\}_{KE}$	$\{Male\}_{KE}$	$\{Manager\}_{KE}$	$\{1^*\}_{KE}$, $\{^*0\}_{KE}$
$\{Andy\}_{PE}$	$\{Male\}_{PE}$	$\{Manager\}_{PE}$	$\{2\}_{PE}$

SELECT *name*

FROM *Personnel*

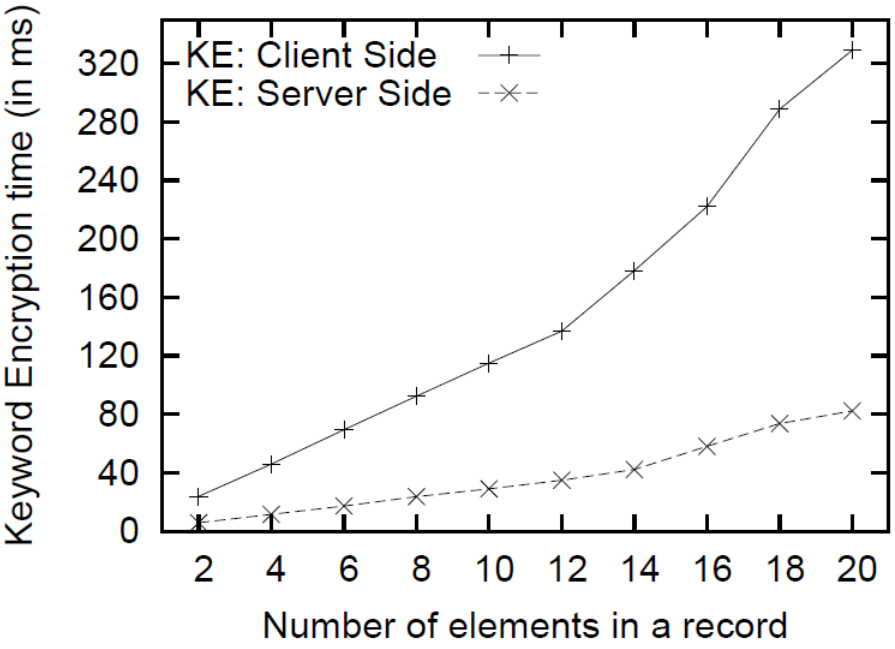
WHERE *position=manager* AND *level<3*

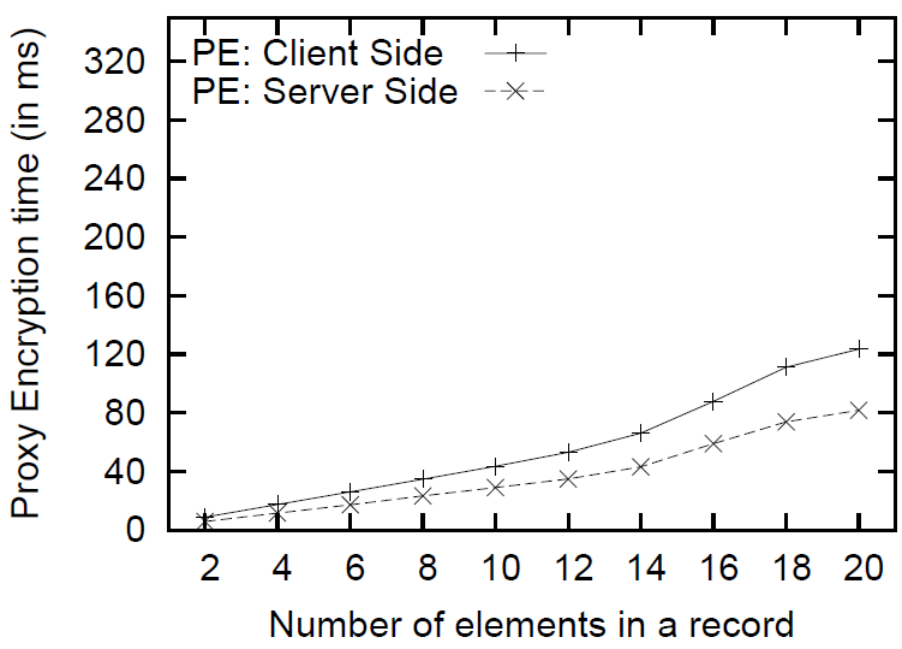


Performance Evaluation: Insert

A prototype implemented in Java

Tested on Intel 2.67 GHz with 4 GB RAM, Microsoft Windows 7

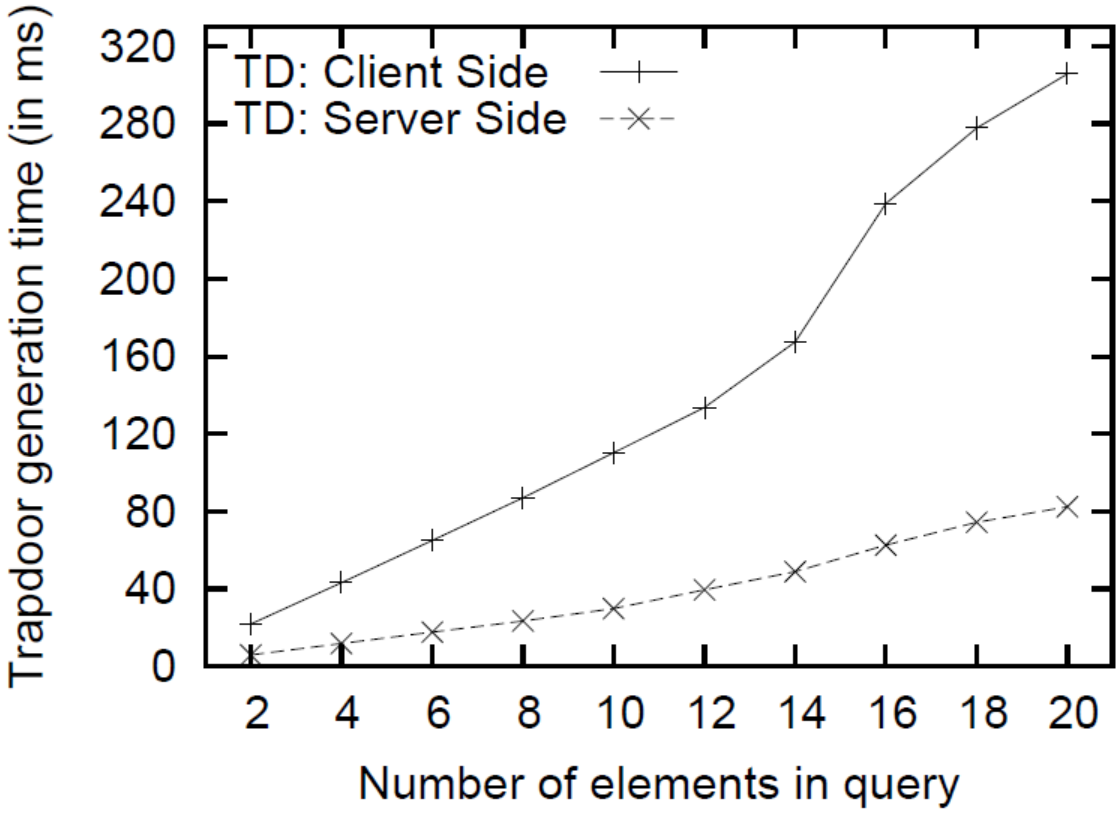




Complexity: $\Theta(n + ms)$

n is number of strings, m is number of integers, each of size s bits

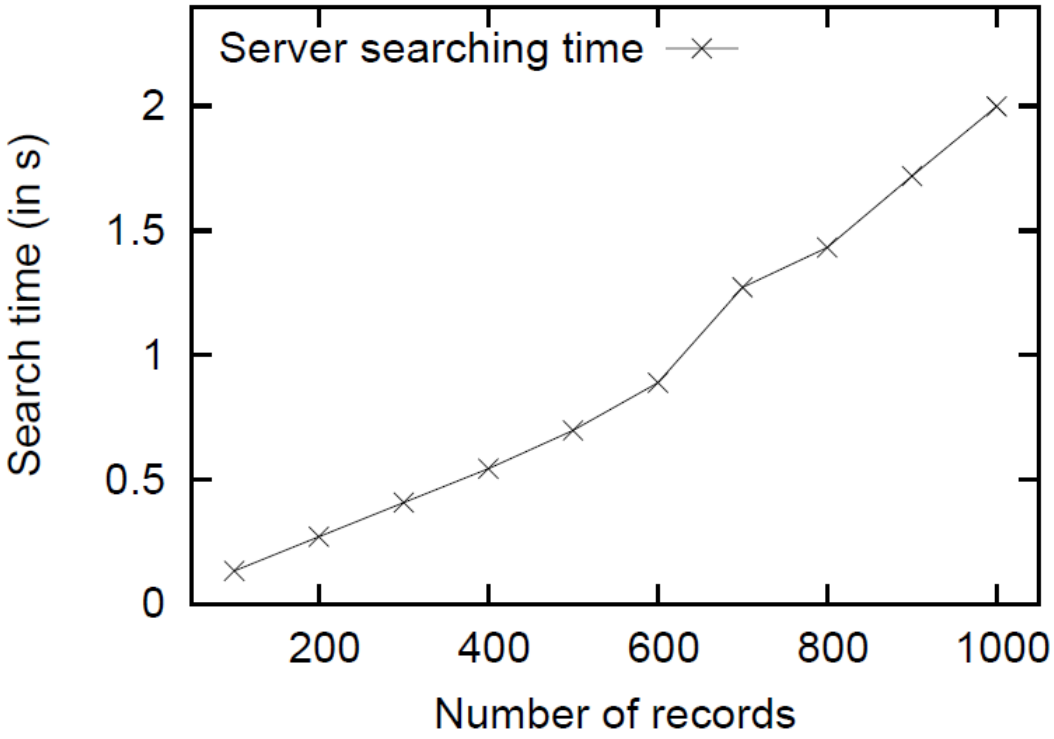
Performance Evaluation: Select (Query)



Complexity: $\Theta(n + ms)$

n is number of strings, m is number of integers, each of size s bits

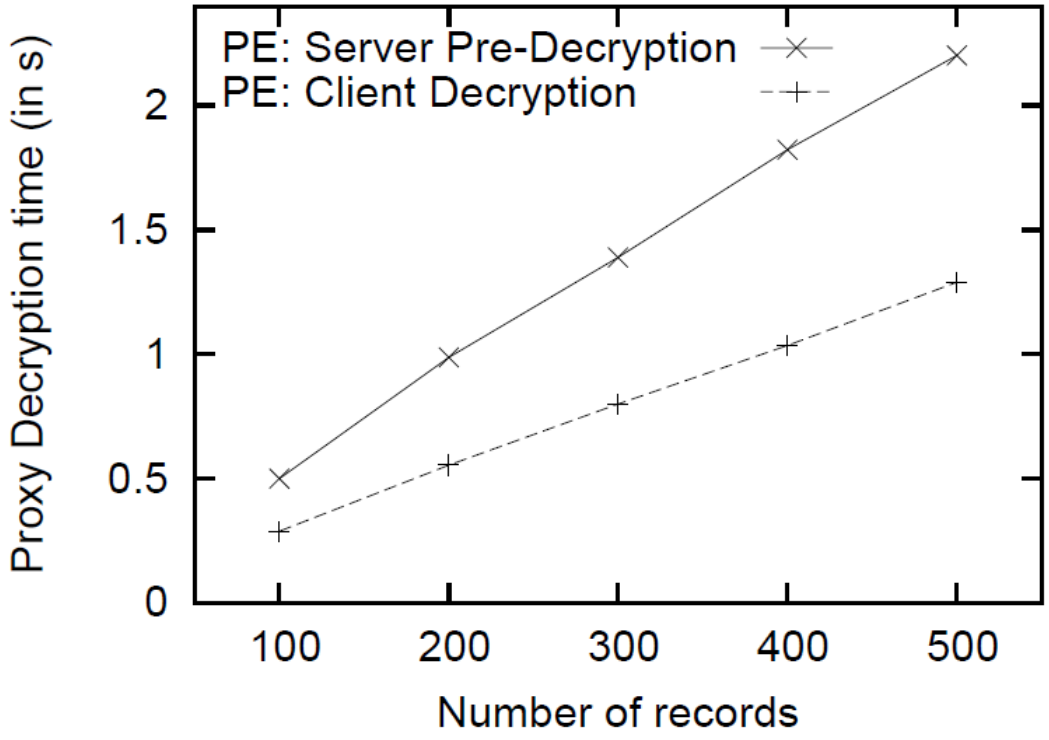
Performance Evaluation: Select (Server)



Complexity: $O(r*(n + ms^2))$

r is number of records, n is number of strings, m is number of integers, each of size s bits

Performance Evaluation: Select (Decryption)



Complexity: O(r*(n + m))

r is number of records, n is number of strings, m is number of integers

Summary

- We presented the first multi-user scheme that supports complex queries in the cloud
- Each user has her own key
- A compromised user is revoked without requiring re-distribution of keys or re-encryption of stored data
- In future, we would like to
  - make performance improvements
  - build indexes
  - apply the technique on very large database

Thank You!

asghar@create-net.org

http://disi.unitn.it/~asghar/

References

- H. Hacigumus, B. R. Iyer, C. Li, and S. Mehrotra, “Executing sql over encrypted data in the database-service-provider model,” in Proceedings of the 2002 ACM SIGMOD international conference on Management of data, SIGMOD ’02, pp. 216–227, ACM, 2002.
- E.-J. Goh, “Secure indexes.” Cryptology ePrint Archive, Report 2003/216, 2003. http://eprint.iacr.org/.
- P. Golle, J. Staddon, and B. Waters, “Secure conjunctive keyword search over encrypted data,” in Applied Cryptography and Network Security LNCS vol. 3089 pp. 31–45, Springer 2004.
- Y.-C. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data,” in Applied Cryptography and Network Security LNCS vol. 3531 pp. 442–455, Springer2005.
- H. Wang and L. V. S. Lakshmanan, “Efficient secure query evaluation over encrypted xml databases,” in Proceedings of the 32nd international conference on Very large data bases, VLDB ’06, pp. 127–138, 2006.
- C. Bosch, R. Brinkman, P. Hartel, and W. Jonker, “Conjunctive wildcard search over encrypted data,” in Secure Data Management, LNCS vol. 6933 pp. 114–127, Springer 2011.
- R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, “Cryptdb: protecting confidentiality with encrypted query processing,” in Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles, SOSP ’11, (New York, NY, USA), pp. 85–100, ACM, 2011.

References (2)

- 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, CCS ’06, pp. 79–88, ACM, 2006.
- D. Boneh and B. Waters, “Conjunctive, subset, and range queries on encrypted data,” in Theory of Cryptography, LNCS vol. 4392 pp. 535–554, Springer 2007.
- J. Baek, R. Safavi-Naini, and W. Susilo, “Public key encryption with keyword search revisited,” in Computational Science and Its Applications - ICCSA 2008 LNCS vol. 5072 pp. 1249–1259, Springer 2008.
- J. Katz, A. Sahai, and B. Waters, “Predicate encryption supporting disjunctions, polynomial equations, and inner products,” in Advances in Cryptology - EUROCRYPT 2008, LNCS vol. 4965 pp. 146–162, Springer 2008.
- H. S. Rhee, J. H. Park, W. Susilo, and D. H. Lee, “Trapdoor security in a searchable public-key encryption scheme with a designated tester,” Journal of Systems and Software, vol. 83(5), pp. 763 – 771, 2010.
- B. Zhu, B. Zhu, and K. Ren, “Peksrand: Providing predicate privacy in public-key encryption with keyword search,” in Communications (ICC), 2011 IEEE International Conference on, pp. 1–6, 2011.
- Y. Yang, H. Lu, and J. Weng, “Multi-user private keyword search for cloud computing,” 2011 IEEE Third International Conferencein Cloud Computing Technology and Science (CloudCom), on, pp. 264–271, 2011.

References (3)

- M. Li, S. Yu, N. Cao, and W. Lou, “Authorized private keyword search over encrypted data in cloud computing,” in Distributed Computing Systems (ICDCS), 2011 31st International Conference on, pp. 383–392, 2011.
- Y. Hwang and P. Lee, “Public key encryption with conjunctive keyword search and its extension to a multi-user system,” in Pairing-Based Cryptography - Pairing 2007 LNCS , vol. 4575 pp. 2–22, Springer 2007.
- F. Bao, R. Deng, X. Ding, and Y. Yang, “Private query on encrypted data in multi-user settings,” in Information Security Practice and Experience, LNCS vol. 4991 pp. 71–85, Springer 2008.
- J. Shao, Z. Cao, X. Liang, and H. Lin, “Proxy re-encryption with keyword search,” Information Sciences, vol. 180, no. 13, pp. 2576 – 2587, 2010.
- B. Hore, S. Mehrotra, and G. Tsudik, “A privacy-preserving index for range queries,” in Proceedings of the Thirtieth international conference on Very large data bases - Volume 30, VLDB ’04, pp. 720–731, VLDB Endowment, 2004.
- 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, pp. 829–837, 2011.
- D. X. 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, pp. 44–55, 2000.