Ubiquitous Computing Laboratory
Kyung Hee University, Korea

경희대학교
KYUNG HEE UNIVERSITY

Oblivious Computation in Public Cloud *for* Privacy-aware Access Control Policies and Data Search

Ph.D. Dissertation Defense

Zeeshan Pervez

Department of Computer Engineering
Kyung Hee University, Global Campus, Korea
email: zeeshan@oslab.khu.ac.kr

Advisor: **Prof. Sungyoung Lee, Ph.D.**

October 08, 2012

Outline

Introduction

- Public cloud storage
- Oblivious computation - *background*
- Problem statement
- Taxonomy

Related work

Proposed methodologies

- Delegated private matching
- Oblivious access control policy evaluation – *O-ACE*
- Oblivious term matching – *OTM*

Thesis contributions

Conclusion and future directions

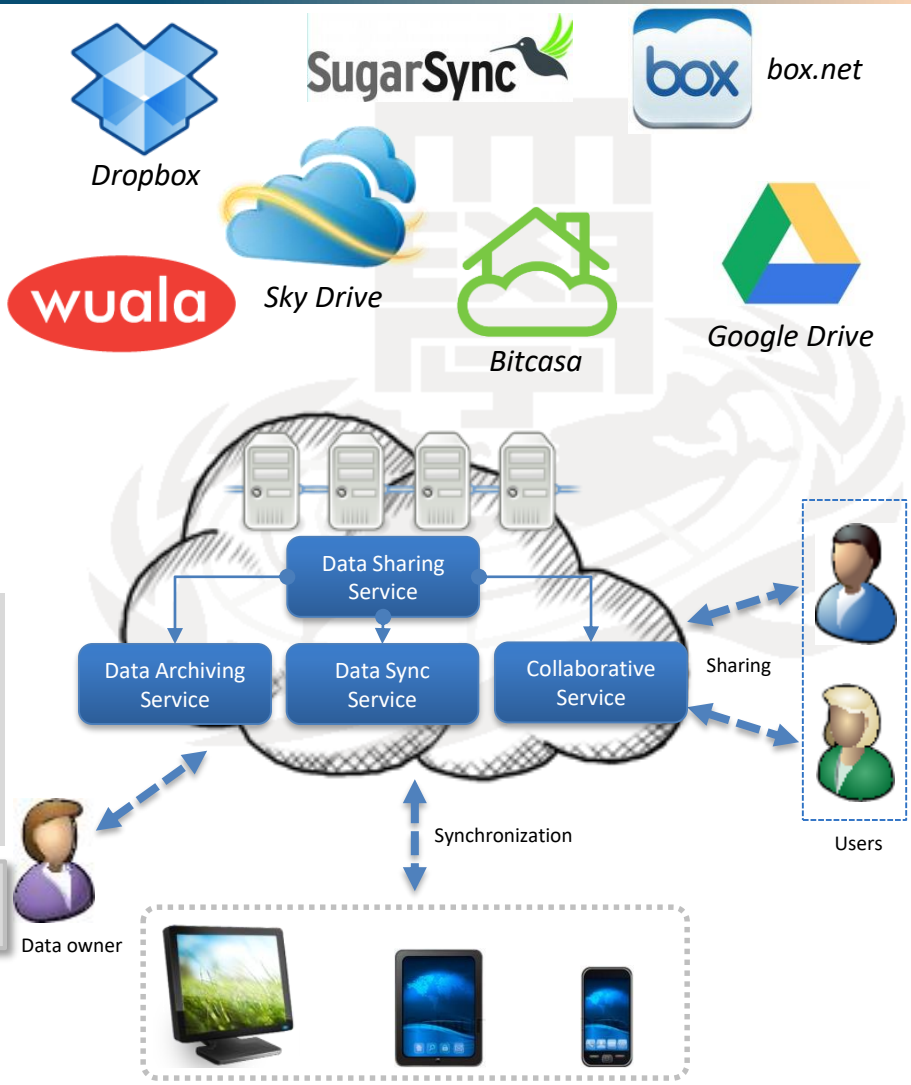
Achievements

Public cloud storage

- An **online storage** facility which is **owned**, **managed** and **operated** by a **cloud service provider**
- Cloud storage services are becoming **integral part** of our **computing environment**
  - Dropbox
  - Instragram
  - GoogleDocs
- Cloud based data sharing services are the most prevalent and adopted services – *enabling data owner to share data with multiple authorized users*

- ***Enforcement of access control policies*** *to ensure authorized data access*
- ***Data searching capabilities*** *to access relevant data* – avoid unnecessary bandwidth consumption: pay-as-you-use

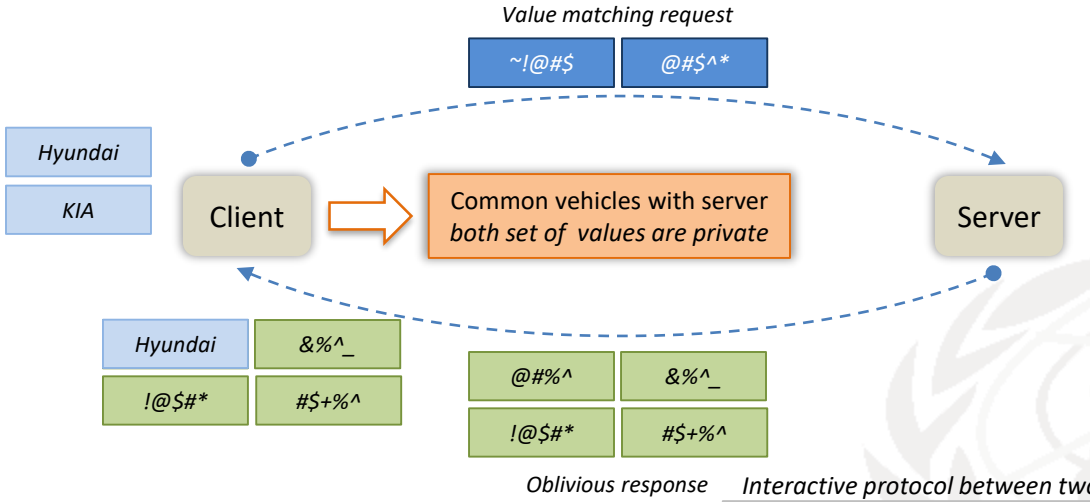
Oblivious computation



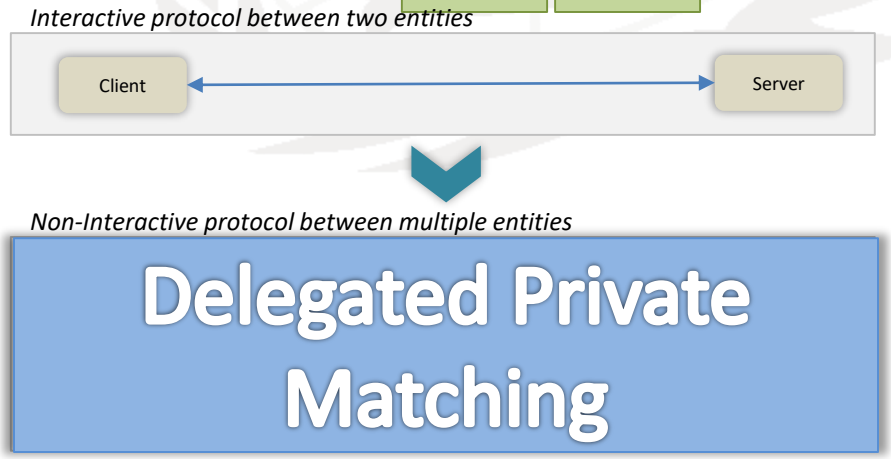
경희대학교 KYUNG HEE UNIVERSITY

Oblivious computation – *background*

- Private matching protocol: is an **interactive value matching protocol** between **server and client** over their private set of values



- **Client learns** nothing more than **common values** and **server remains oblivious** to client's private set
- *Nothing more than cardinality of client's private set is revealed*

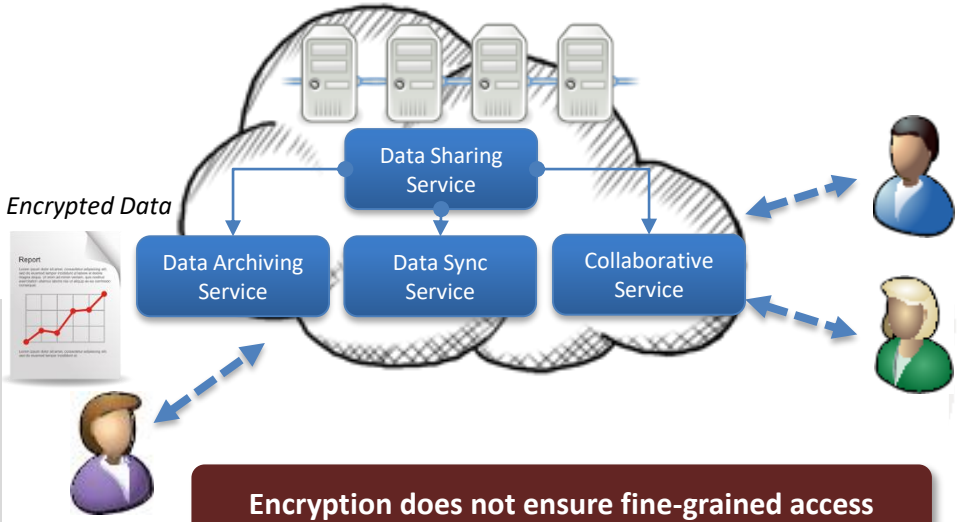


Problem statement

- Public cloud is **owned, managed and operated** by an **untrusted entity** – cloud service provider
- To **ensure data confidentiality** often **encrypted data** is outsourced to public cloud storage

- Conventional privacy enforcement and security frameworks
  - require some form of **data computation** to ensure authorized data access

    or
  - reliance on **trusted party** to govern data access
- Cloud service provider can **exploit data computation** operations to **compromise privacy** of the outsourced data



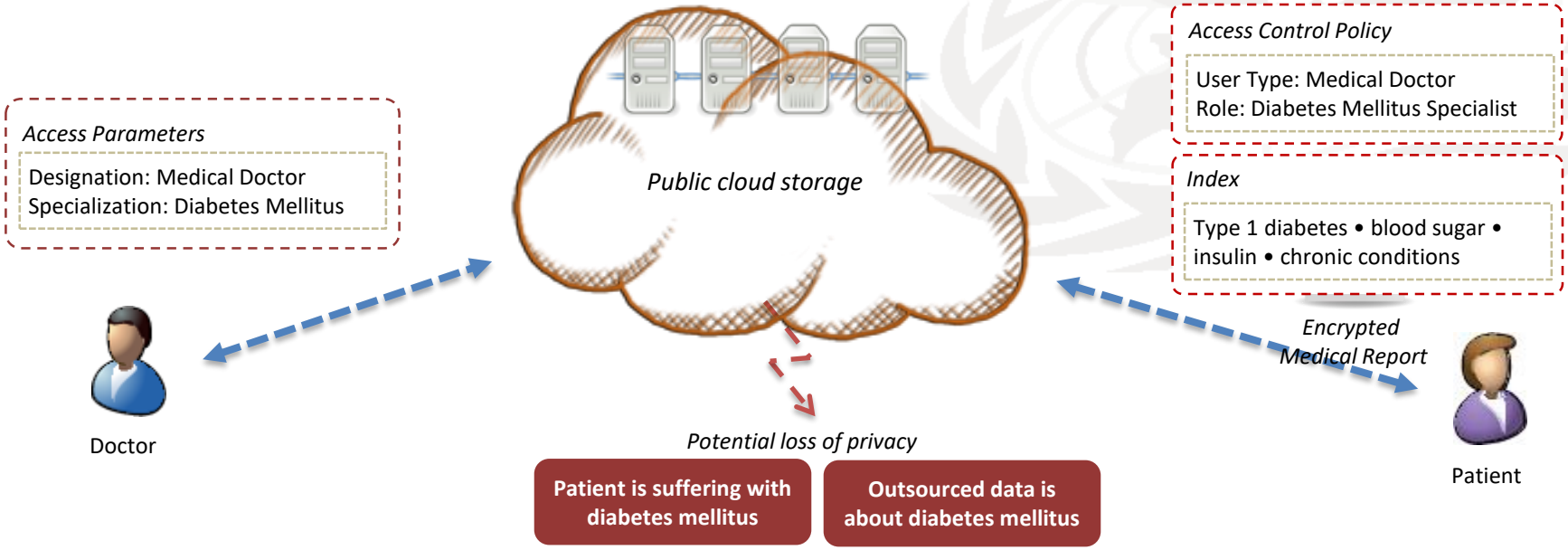
Encryption does not ensure fine-grained access control *over outsourced data*

Encrypted data cannot be processed – *standard search queries do not work for encrypted data*

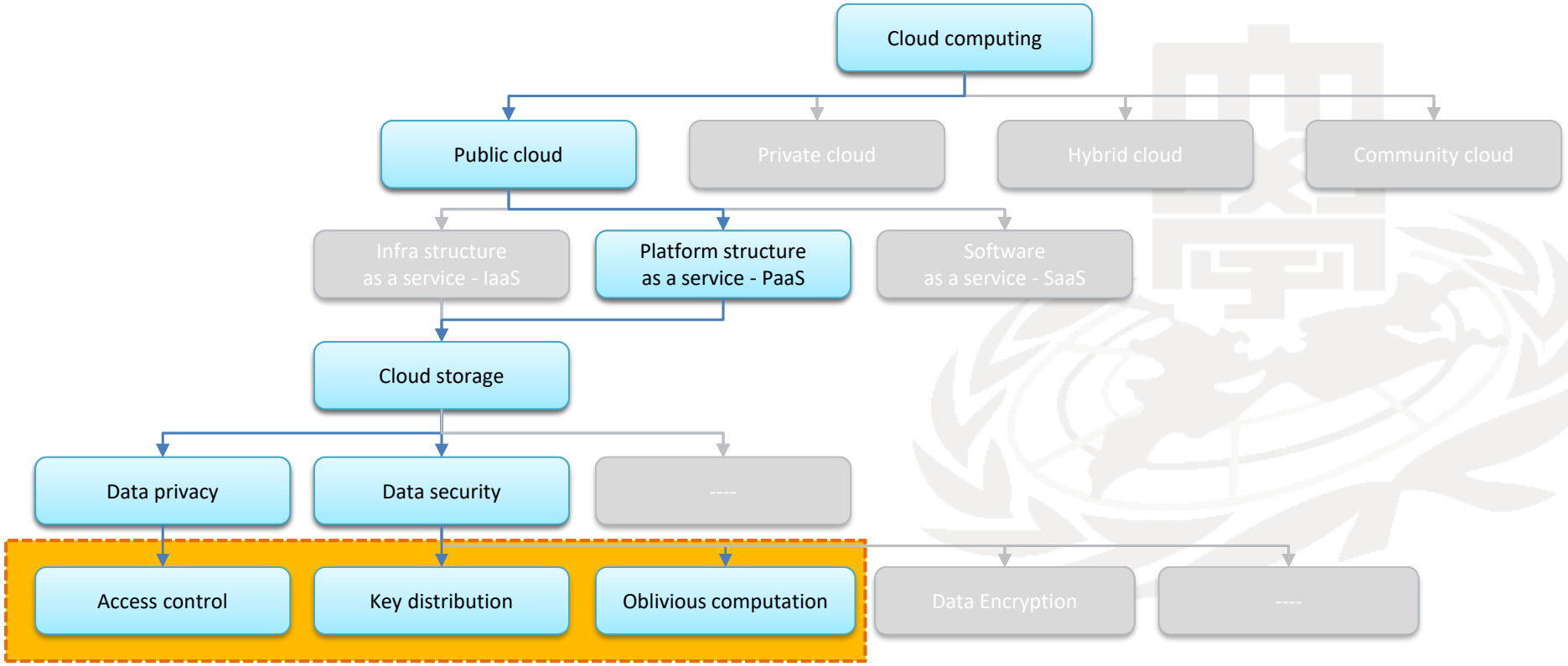
Utility of cloud public storage services is greatly affected – *availability of data owner, reliance on trusted third party, deployment of private cloud*

Problem statement

- **Access control policies can reveal confidential information** about the outsourced data and user's personal information
- Leveraging **search on outsourced data can be exploited** by public cloud service provider



Taxonomy


Cloud computing
Public cloud
Private cloud
Hybrid cloud
Community cloud
Infra structure as a service - IaaS
Platform structure as a service - PaaS
Software as a service - SaaS
Cloud storage
Data privacy
Data security

Access control
Key distribution
Oblivious computation
Data Encryption

Access control policies

Related work	Access control enforcement	Limitations
Cloud based data sharing system for massively large data [1]. Large data files are divided into multiple parts - each encrypted with different key.	Keys are managed by the data owner in a **binary tree** structure. **Security tokens** are issued by **data owner** and validated by cloud storage provider.	• Availability the data owner • Reliance of untrusted cloud service provider
FADE [2] is a secure cloud storage system. It is designed to share outsourced data in an untrusted domain and to assuredly delete it once the need of sharing is over.	**Data encryption key** encrypts the outsourced data. **Control keys** encrypts the data encryption key. Control keys are managed by **key manager**.	• Delegation of data governance to key manager • Poor utilization of cloud resources
TrustStore [3] is an Amazon S3 based storage service. It manages data as data-fragments and meta-data. Data-fragments are persisted at Storage Service Provider (SSP), whereas meta-object is managed by Key Management Service Provider (KMSP).	Utilizes a KMSP to generate and distribute decryption keys. **KMSP and SSP** are independent entities and **do not know each other**.	• Delegation of data governance to key manager • Impracticable assumption
Cryptographic Cloud Storage to outsource enterprise data [4]. Data Processor encrypts the outsourced data. Data Verifier verifiers the data integrity at cloud storage. Credential Generator generates manages credential of the users.	Utilizes **Attribute Based Encryption** (ABE). Data owner generates and disseminates ABE secret key to the authorized users.	• Availability the data owner • ABE reveals information about access control policy
SiRiUS [5], **Plutus** [6], and **CRUST** [7] are remote storage system	Utilizes **asymmetric encryption** to ensure authorized data access to the outsourced data.	• Poor utilization of cloud resources

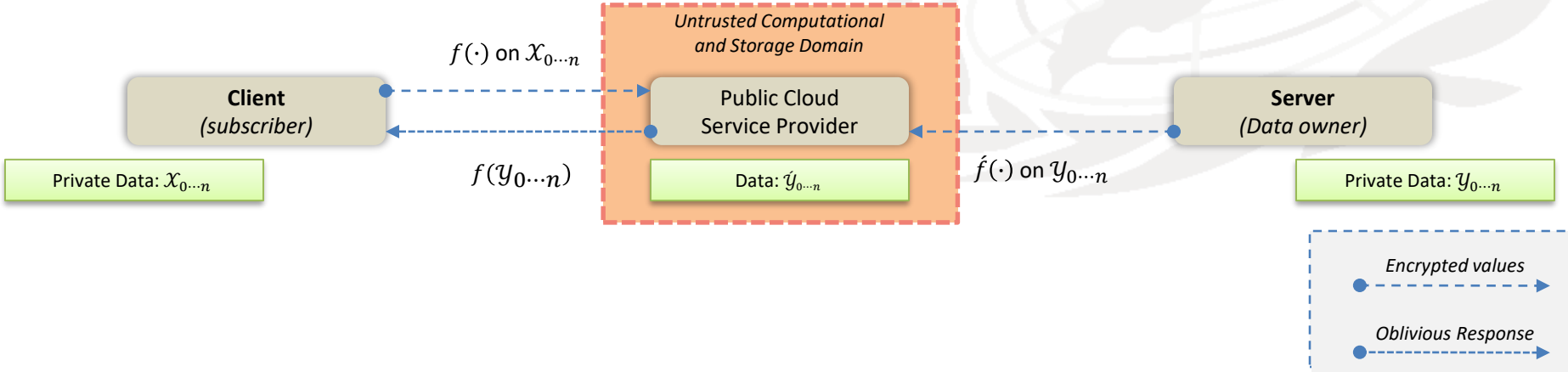
Encrypted data search

Related work	Encrypted data search	Limitations
Searchable symmetric key cryptography (SCK) [8], Privacy-preserving queries on encrypted data [9].	**Trapdoors based cryptography**. Utilizes untrusted storage provider to execute search query.	• Limited searching capabilities - search queries are confined to trapdoors. • Availability of data owner
Searchable public key cryptography (PKC) – based on the concept of asymmetric encryption [10].	**Trapdoors based cryptography**. Utilizes untrusted storage provider to execute search query.	• Limited searching capabilities - search queries are confined to trapdoors. • Availability of data owner
Authorized Private Keyword Search (APKS) on personal health record [11]	**Trapdoor based cryptography**. Utilizes untrusted storage provider to execute search query. **Trusted third party** was responsible for **distributing trapdoors**	• Limited searching capabilities - search queries are confined to trapdoors. • Reliance on trusted third party for authorized data search
Secure ranked search over encrypted data - Wang et al [12] .	**Trapdoor based cryptography**. Utilizes untrusted storage provider to execute search query. Search result are **sorted** according to frequency of **a single trapdoor**	• Limited searching capabilities - search queries are confined to trapdoors. • Can only search for single keyword at a time – cannot be utilized for complex queries.
Google search appliance [13], **Windows enterprise search** [14]	**Searchable data index** managed by **trusted entity** i.e., private cloud. Single enterprise wide centralized index.	• Poor utilization of cloud infrastructure

경희대학교 KYUNG HEE UNIVERSITY

Delegated private matching*

- Private matching is an **interactive protocol** between two entities – client and server
- **Availability of entities** cannot be assured in cloud storage system –it affects the utility of a cloud storage services
- Delegated private matching **delegates matching capabilities** to an **untrusted entity** – with privacy consideration
  - client, server & untrusted entity
- **Utilizes asymmetric encryption** to ensure privacy of delegated private set
- Holds **similar security properties as private matching**
  - Oblivious computation of information at untrusted entity
  - Minimized information deduction – not more than cardinality of sets



* Zeeshan Pervez, Asad Masood Khattak, Sungyoung Lee, Young-Koo Lee and Eui-Nam Huh, "***Oblivious Access Control Policies for Cloud Based Data Sharing Systems***", Computing, Springer.

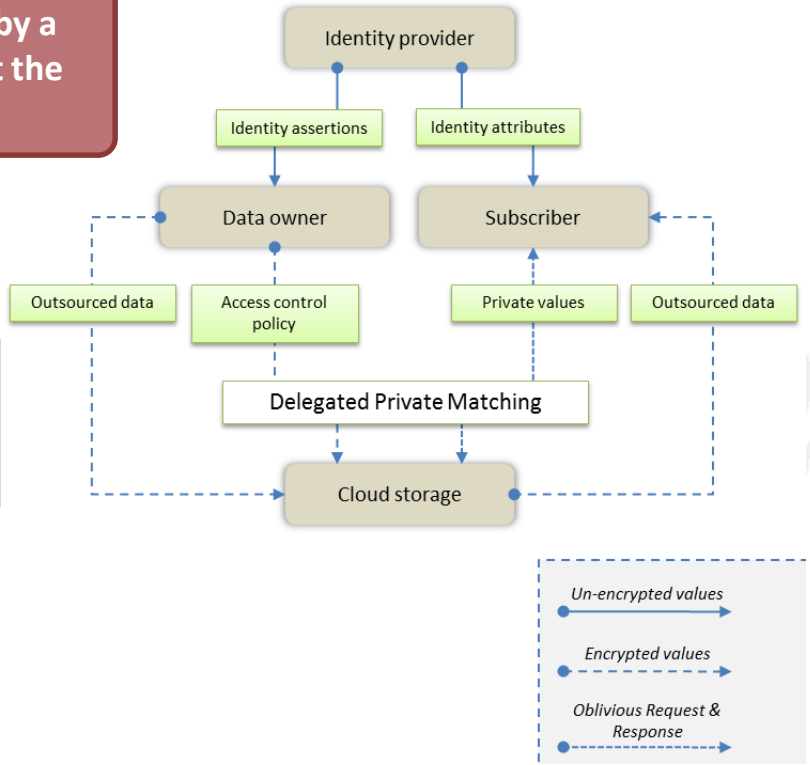
경희대학교 KYUNG HEE UNIVERSITY

Oblivious access control policy evaluation – O-ACE* 1/3

Access control policies and identity attributes can be exploited by a cloud service provider to deduce confidential information about the outsourced data and data owner

- O-ACE realizes **a privacy-aware access control policy enforcement** in public cloud services
- ***Concept:*** possession of **identity attributes** ensures **legitimacy** and **authenticity** of a subscriber
  - similar to password based authentication – *legitimacy*
  - similar to LDAP˜, user's role are defined by attributes – *authenticity*
- **Identity assertions** are utilized to encrypt outsourced data
- **Identity attributes** are utilized to derive data decryption key

˜*Light weight directory access protocol*

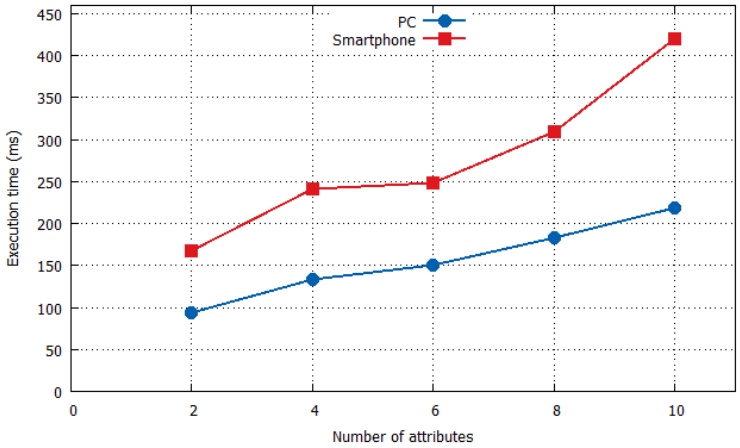


* Zeeshan Pervez, Asad Masood Khattak, Sungyoung Lee, Young-Koo Lee and Eui-Nam Huh, "***Oblivious Access Control Policies for Cloud Based Data Sharing Systems***", Computing, Springer.

Oblivious access control policy evaluation – O-ACE

- Evaluation
  - Cloud platform
    - **Google App Engine**
    - Node Specification 1.20 GHz
  - Desktop PC: 2.6 GHz dual core, 4.0 GB main memory
  - Smartphone: Android Gingerbread, 800MHz processor
  - Implementation: Java

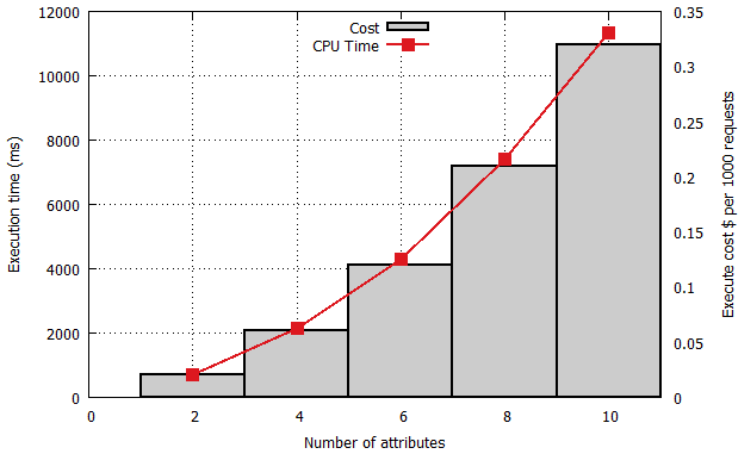
Attribute processing execution time



Polynomial modeling with root values

Homomorphic encryption

Policy evaluation on Google app engine execution time



Google datastore operation

Polynomial evaluation on legitimacy values

Homomorphic operation

Oblivious access control policy evaluation – O-ACE

- Evaluation

	Availability requirement			Access control enforcement			Privacy of access control policy
	Data owner	Cloud service provider	Third party services	Data owner	Storage service provider	Third party services	
Cloud based data sharing system [1]	●	●		●	●		
FADE [2]		●	●			●	
TrustStore [3]		●	●			●	
Cryptographic Cloud Storage	●	●	●			●	
SiRiUS [5]	●	●			◉		
Plutus [6]	●	●			◉		
CRUST [7]	●	●			◉		
O-ACE		●			●		●

● Complete dependency
◉ Partial dependency

경희대학교 KYUNG HEE UNIVERSITY

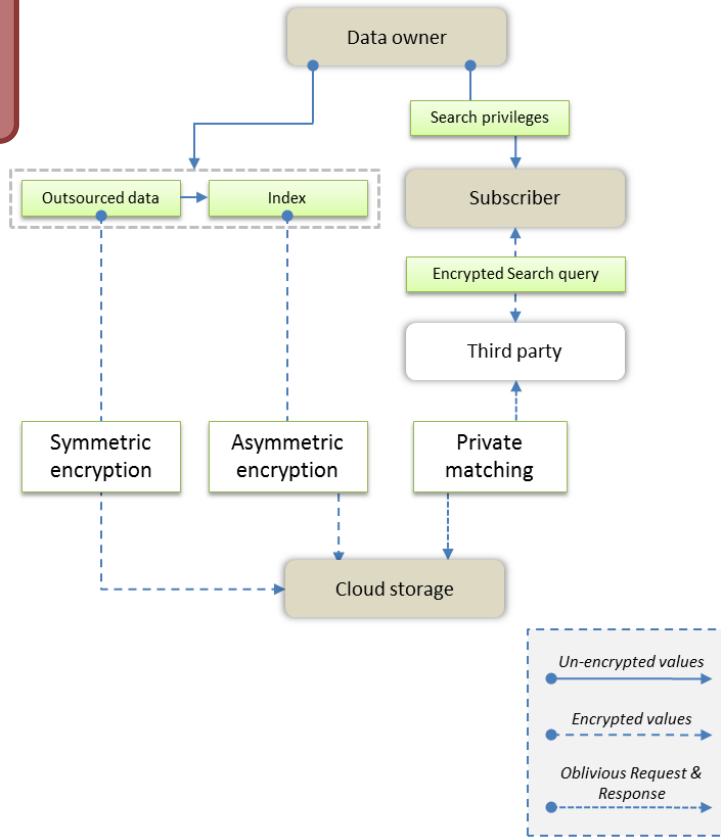
Privacy-aware searching with oblivious term matching – OTM* 1/3

Data search in cloud storage services can **assist cloud service provider** to **deduce confidential and personal** - compromising privacy of the outsourced data

- OTM leverages data owner to provision **privacy-aware searching capabilities** to subscribers
- **Authorized subscriber** can **define** their own **search criteria** instead of relying on trapdoors provided by the data owner
- Utilizes **index data structure** to evaluate search queries submitted by multiple authorized subscribers

- ***Concept:*** privacy-aware **term matching** between **index data structure** and **search criteria**

- Result of **query evaluation** is **oblivious** to cloud service provider
  - **Randomized result** for unauthorized subscribers

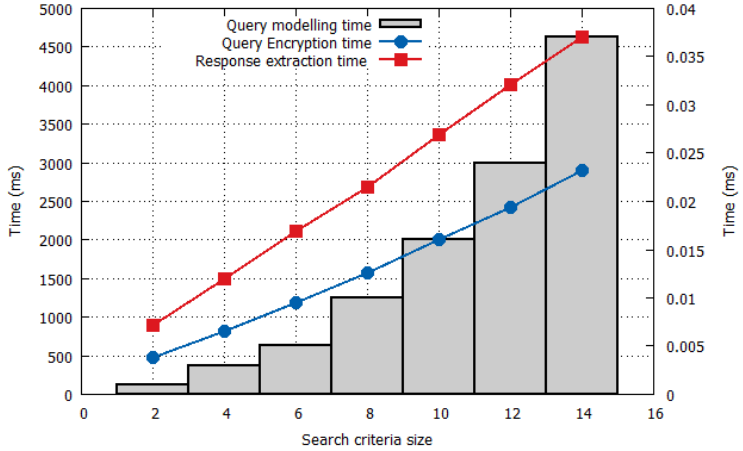


* Zeeshan Pervez, Ammar Ahmad Awan, Asad Masood Khattak, Sungyoung Lee, and Eui-Nam Huh, "***Privacy-aware Searching with Oblivious Term Matching for Cloud Storage***", Journal of Supercomputing, Springer,

Privacy-aware searching with oblivious term matching – OTM

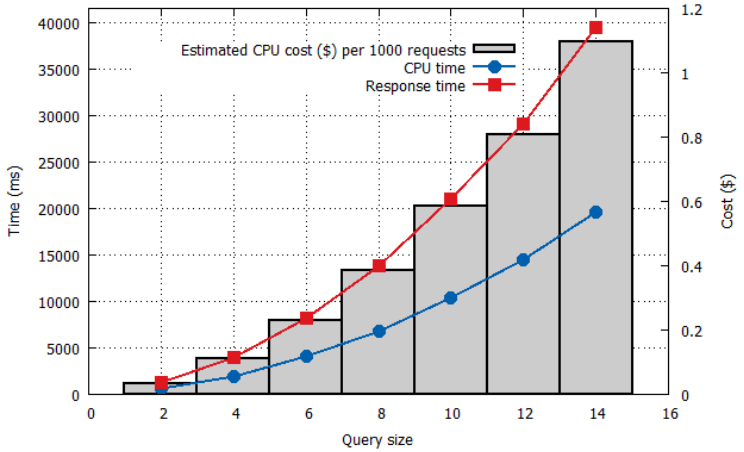
- Evaluation
  - Cloud platform
    - **Google App Engine**
  - Node Specification 2.40 GHz, 512 Main Memory
  - Desktop PC: 2.6 GHz dual core, 2.0 GB main memory
  - Trusted third party: 3.30 GHz Core i5 with 4 GB main memory
  - Implementation: Java

Query modeling, oblivious query generation encryption and response extraction time



Public encoding | Polynomial modeling with root values | Homomorphic encryption + decryption

Query evaluation, cloud server response time and estimated execution cost for 1000 requests



Google datastore operation | Polynomial evaluation on indexed values | Homomorphic operation

Privacy-aware searching with oblivious term matching – OTM

- Evaluation

	Availability requirement			Query execution		Unlimited search queries
	Data owner	Storage service provider	Third party services / dedicated resources	Storage service provider	Third party services	
Searchable symmetric key cryptography [8]	●	●		●		
Privacy-preserving queries on encrypted data [9]	●	●		●		
Searchable public key cryptography [10]	●	●		●		
Authorized Private Keyword Search [11]		●	●	●		
Secure ranked search over encrypted data [12]		●	●	●		
Google search appliance [13], Windows enterprise search [14]		●	●		●	
OTM		●		●		●

Contributions

Domain

Public cloud storage services – provisioned by untrusted entities

Research outcome

Proposed Methodologies

- **Privacy-aware access control enforcement**
  - without relying on any trusted third party – *Oblivious access control policy evaluation*
- **Privacy-aware encrypted data search**
  - without the need of trapdoor exchange – *Oblivious term matching*

Achieved

- **Oblivious computation** within untrusted domain i.e., public cloud storage
- Resilient against **conspired attack** of **cloud service provider** and **unauthorized subscribers**

Contributions

Restrain cloud service provider to deduce information about the encrypted data

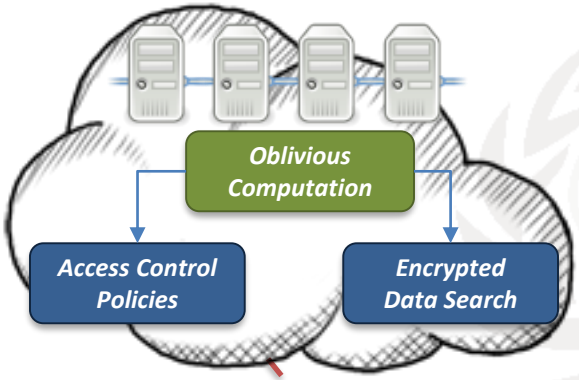
Encrypted Keywords

^&*(YUGBSDF^&
UY*GSDJ&^*GBD
$*(Yjhoiasf(&!a
....

Encrypted Access Control Policy

~@#$AkiQW|q2
*&^GS_)HS_A|J

enable authorized users to gain access to the encrypted data



Encrypted Medical Report

Doctor

Patient

Oblivious Computation – Randomized Response

Access Parameters

Designation: Medical Doctor
Specialization: Diabetes Mellitus

Conclusion

- We proposed **delegated private matching** to enforce authorized data access without relying on trusted third party
  - access control policies are **obliviously evaluated** by the cloud service provider
  - **maximizes utilization** of cloud storage services

- **Encryption** ensures **data confidentiality** within untrusted domain – however **encrypted data cannot be processed** (searched) without decrypting it
- We proposed **oblivious term matching** which enables authorized subscribers to search outsourced data without compromising privacy
  - authorized subscribers **define their own search queries**
  - **search queries** are **obliviously evaluated** by cloud service provider

Future directions

- Obliviously search encrypted data in **Hadoop environment**

- Incorporating **Garbled Circuits**
  - oblivious access control policy evaluation
  - oblivious term matching

Publications and Patents

Journal Publications: 07

SCI: 06		International Journal: 01
First Author: 03	Coauthor: 03	First Author: 01

Conference: 15

International: 14		Domestic : 01
First Author: 03	Coauthor: 11	First Author: 1

Patents: 01

Korean Patent: 01

Work in progress

- Sungyoung Lee, Zeeshan Pervez "**A method to obliviously search encrypted data in cloud storage services**" – *With patent officer*
- Zeeshan Pervez, Sungyoung Lee "**Searching Encrypted Data in Hadoop with Oblivious Term Matching**" - *In preparation*
- Zeeshan Pervez, Sungyoung Lee **"Privacy-aware Searching in Cloud Storage Services with Garbled Circuit Evaluation"** – *In preparation*

Selected References

1. Wang, W., Li, Z., Owens, R., Bhargava, B.: **Secure and efficient access to outsourced data**. In: Proceedings of the 2009 ACM workshop on Cloud computing security, CCSW'09, pp. 55–66. ACM, New York, NY, USA (2009).
2. Tang, Y., Lee, P.P.C., Lui, J.C.S., Perlman, R.: **Fade: Secure overlay cloud storage with file assured deletion**. In: SecureComm, pp. 380–397 (2010)
3. Yao, J., Chen, S., Nepal, S., Levy, D., Zic, J.: **Truststore: Making amazon s3 trustworthy with services composition**. In: Cluster, Cloud and Grid Computing (CCGrid), 2010 10th IEEE/ACM International Conference on, pp. 600 –605 (2010).
4. Kamara, S., Lauter, K.: **Cryptographic cloud storage**. In: Proceedings of the 14th international conference on Financial cryptograpy and data security, FC'10, pp. 136–149. Springer-Verlag, Berlin, Heidelberg (2010).
5. Goh, E.j., Shacham, H., Modadugu, N., Boneh, D.: **Sirius: Securing remote untrusted storage**. In: in Proc. Network and Distributed Systems Security (NDSS) Symposium 2003, pp. 131–145 (2003).
6. Kallahalla, M., Riedel, E., Swaminathan, R., Wang, Q., Fu, K.: **Plutus: Scalable secure file sharing on untrusted storage**. In: Proceedings of the 2nd USENIX Conference on File and Storage Technologies, pp. 29–42. USENIX Association, Berkeley, CA, USA (2003).
7. Geron, E., Wool, A.: **Crust: Cryptographic remote untrusted storage without public keys**. In: Security in Storage Workshop, 2007. SISW '07. Fourth International IEEE, pp. 3 –14 (2007).
8. Song, D. X., Wagner, D., and Perrig, A. (2000) **Practical techniques for searches on encrypted data**. Security and Privacy, 2000. S P 2000. Proceedings. 2000 IEEE Symposium on, pp. 44 –55.
9. Yang, Z., Zhong, S., and Wright, R. N. (2006) **Privacy-preserving queries on encrypted data**. In Proc. of 11th European Symposium On Research In Computer Security (Esorics), pp. 479–495.
10. Boneh, D., Crescenzo, G. D., Ostrovsky, R., and Persiano, G. (2004) **Public key encryption with keyword search**. EUROCRYPT, pp. 506–522.
11. Li, M., Yu, S., Cao, N., and Lou, W. (2011) **Authorized private keyword search over encrypted data in cloud computing**. Distributed Computing Systems (ICDCS), 2011 31st International Conference on, june, pp. 383 –392.
12. Wang, C., Cao, N., Li, J., Ren, K., and Lou, W. (2010) **Secure ranked keyword search over encrypted cloud data**. Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on, june, pp. 253 –262.
13. **Google search appliance**.
14. **Enterprise search server solutions**.

Selected References

15. Paillier, P. (1999) **Public key cryptosystems based on composite degree residuosity classes**. Proceedings of the 17th international conference on Theory and application of crypto graphic techniques, Berlin, Heidelberg, pp. 223–238, EUROCRYPT'99, Springer-Verlag.

16. Ateniese, G., Fu, K., Green, M., and Hohenberger, S. (2006) **Improved proxy re-encryption schemes with applications to secure distributed storage**. ACM Trans. Inf. Syst. Secur., 9, 1–30.

17. Paillier, P. (2000) **Trapdooring discrete logarithms on elliptic curves over rings**. Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, London, UK, pp. 573–584, ASIACRYPT '00, Springer-Verlag.

18. Freedman, M., Nissim, K., and Pinkas, B. (2004) **Efficient private matching and set intersection**. pp. 1–19, Springer-Verlag.

19. Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M (2010) **A view of cloud computing**. Commun ACM 53:50–58. doi:10.1145/1721654.1721672

20. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., and Brandic, I. (2009) **Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility**. Future Gener. Comput. Syst., 25, 599–616.

21. Yu, S., Wang, C., Ren, K., and Lou, W. (2010) **Achieving secure, scalable, and fine-grained data access control in cloud computing**. Proceedings of the 29th conference on Information communications, Piscataway, NJ, USA, pp. 534–542, INFOCOM'10, IEEE Press.

22. Goyal V, Pandey O, Sahai A, Waters B (2006) **Attribute-based encryption for fine-grained access control of encrypted data**. In: Proceedings of the 13th ACM conference on computer and communications security, CCS '06, ACM, New York, pp 89–98.

23. Holt JE, Bradshaw RW, Seamons KE, Orman H (2003) **Hidden credentials**. In: Proceedings of the 2003 ACM workshop on privacy in the electronic society, WPES '03. ACM, New York, pp 1–8. doi:10.1145/1005140.1005142

24. Pearson, S.: **Taking account of privacy when designing cloud computing services**. In: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, CLOUD '09, pp. 44–52. IEEE Computer Society, Washington, DC, USA (2009). DOI http://dx.doi.org/10.1109/CLOUD.2009.5071532. URL http://dx.doi.org/10.1109/CLOUD.2009.5071532

25. Sabrina, Foresti, S., Jajodia, S., Paraboschi, S., Samarati, P.: **Over-encryption: Management of Access Control Evolution on Outsourced Data**. In: VLDB, pp. 123–134 (2007)

26. Kaufman, L. M. (2009) **Data security in the world of cloud computing**, Piscataway, NJ, USA, July. vol. 7, pp. 61–64, IEEE Educational Activities Department.

27. Curino, C., Jones, E., Popa, R. A., Malviya, N., Wu, E., Madden, S., Balakrishnan, H., and Zeldovich, N. (2011) **Relational Cloud: A Database Service for the Cloud**. 5th Biennial Conference on Innovative Data Systems Research, Asilomar, CA, January.

28. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., and Molina, J. (2009) **Controlling data in the cloud: outsourcing computation without outsourcing control**. Proceedings of the 2009 ACM workshop on Cloud computing security, New York, NY, USA, pp. 85–90, CCSW '09, ACM.

Thank you