Secure Cloud Service

Student: Jiangshan Yu
Supervisor: Prof. Mark Ryan

School of Computer Science
University of Birmingham

Jan. 2013

Outline of Topics

1. Cloud Computing

2. Security Concerns

3. Current Solutions

4. Our Contributions

5. Reference

Cloud Computing

- Infrastructure as a service (IaaS)
  E.g. Amazon web services.
- Platform as a service (PaaS)
  E.g. Google App
- Software as a service (SaaS)
  E.g. Facebook, Gmail, Google Drive, Dropbox.

Security Concerns

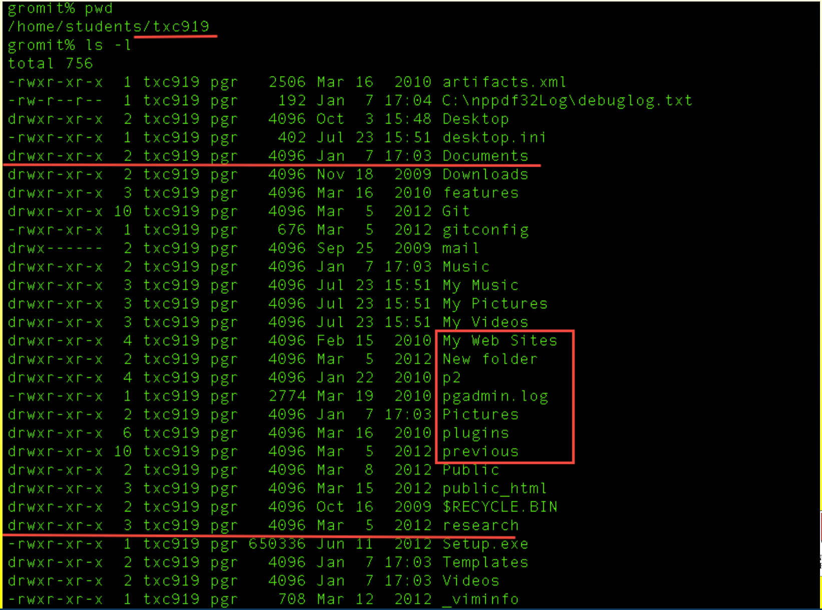
All about data.

- Confidentiality
- Integrity
- Availability

Some examples of data security with **weak adversary** are presented[1] in the following pages.

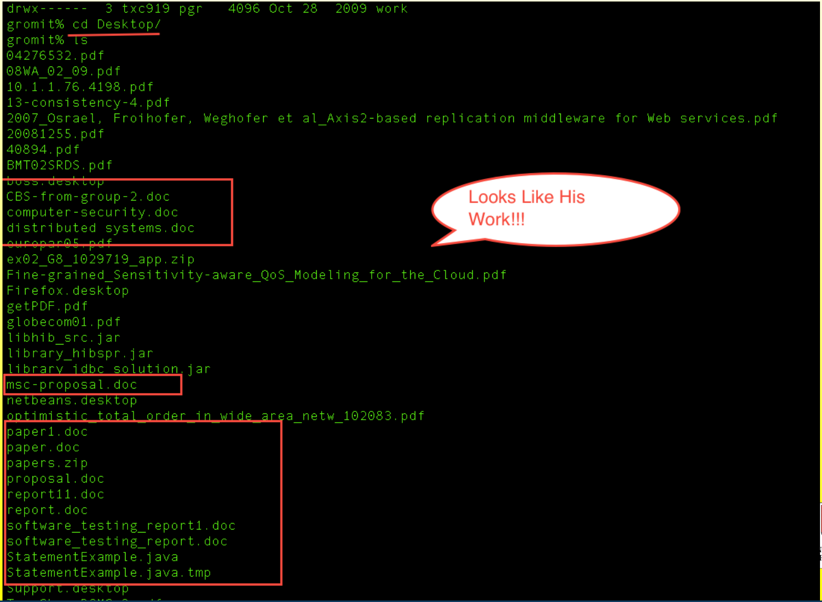
[1] Thanks Tao Chen, Wen-Chi Yang and Siti Mohd Shukri give me the permission to do it.

Tao Chen



```
gromit% pwd
/home/students/txc919
gromit% ls -l
total 756
-rwxr-xr-x  1 txc919 pgr   2506 Mar 16  2010 artifacts.xml
-rw-r--r--  1 txc919 pgr    192 Jan  7 17:04 C:\nppdf32Log\debuglog.txt
drwxr-xr-x  2 txc919 pgr   4096 Oct  3 15:48 Desktop
-rwxr-xr-x  1 txc919 pgr    402 Jul 23 15:51 desktop.ini
drwxr-xr-x  2 txc919 pgr   4096 Jan  7 17:03 Documents
drwxr-xr-x  2 txc919 pgr   4096 Nov 18  2009 Downloads
drwxr-xr-x  3 txc919 pgr   4096 Mar 16  2010 features
drwxr-xr-x 10 txc919 pgr   4096 Mar  5  2012 Git
-rwxr-xr-x  1 txc919 pgr    676 Mar  5  2012 gitconfig
drwx------  2 txc919 pgr   4096 Sep 25  2009 mail
drwxr-xr-x  2 txc919 pgr   4096 Jan  7 17:03 Music
drwxr-xr-x  3 txc919 pgr   4096 Jul 23 15:51 My Music
drwxr-xr-x  3 txc919 pgr   4096 Jul 23 15:51 My Pictures
drwxr-xr-x  3 txc919 pgr   4096 Jul 23 15:51 My Videos
drwxr-xr-x  4 txc919 pgr   4096 Feb 15  2010 My Web Sites
drwxr-xr-x  2 txc919 pgr   4096 Mar  5  2012 New folder
drwxr-xr-x  4 txc919 pgr   4096 Jan 22  2010 p2
-rwxr-xr-x  1 txc919 pgr   2774 Mar 19  2010 pgadmin.log
drwxr-xr-x  2 txc919 pgr   4096 Jan  7 17:03 Pictures
drwxr-xr-x  6 txc919 pgr   4096 Mar 16  2010 plugins
drwxr-xr-x 10 txc919 pgr   4096 Mar  5  2012 previous
drwxr-xr-x  2 txc919 pgr   4096 Mar  8  2012 Public
drwxr-xr-x  3 txc919 pgr   4096 Mar 15  2012 public_html
drwxr-xr-x  2 txc919 pgr   4096 Oct 16  2009 $RECYCLE.BIN
drwxr-xr-x  3 txc919 pgr   4096 Mar  5  2012 research
-rwxr-xr-x  1 txc919 pgr 650336 Jun 11  2012 Setup.exe
drwxr-xr-x  2 txc919 pgr   4096 Jan  7 17:03 Templates
drwxr-xr-x  2 txc919 pgr   4096 Jan  7 17:03 Videos
-rwxr-xr-x  1 txc919 pgr    708 Mar 12  2012 _viminfo
```

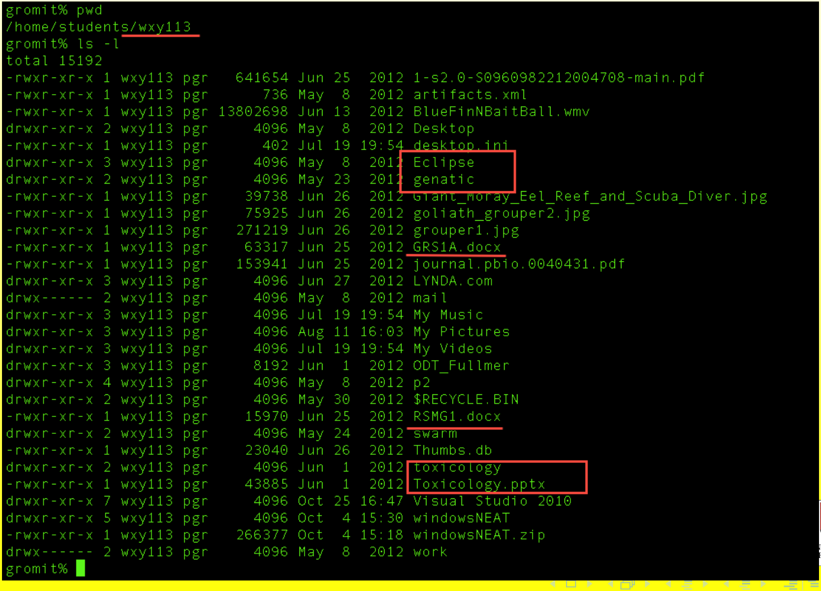
Tao Chen (Cont.)



```
drwx------  3 txc919 pgr   4096 Oct 28  2009 work
gromit% cd Desktop/
gromit% ls
04276532.pdf
08WA_02_09.pdf
10.1.1.76.4198.pdf
13-consistency-4.pdf
2007_Osrael, Froihofer, Weghofer et al_Axis2-based replication middleware for Web services.pdf
20081255.pdf
40894.pdf
BMT02SRDS.pdf
boss.desktop
CBS-from-group-2.doc
computer-security.doc
distributed systems.doc
europar05.pdf
ex02_G8_1029719_app.zip
Fine-grained_Sensitivity-aware_QoS_Modeling_for_the_Cloud.pdf
Firefox.desktop
getPDF.pdf
globecom01.pdf
libhib_src.jar
library_hibspr.jar
library_jdbc_solution.jar
msc-proposal.doc
netbeans.desktop
optimistic_total_order_in_wide_area_netw_102083.pdf
paper1.doc
paper.doc
papers.zip
proposal.doc
report11.doc
report.doc
software_testing_report1.doc
software_testing_report.doc
StatementExample.java
StatementExample.java.tmp
Support.desktop
```

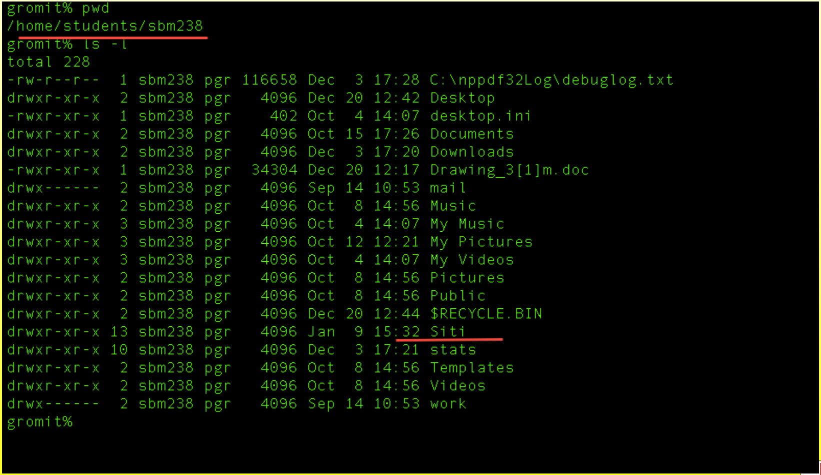
Looks Like His Work!!!

Wen-Chi Yang



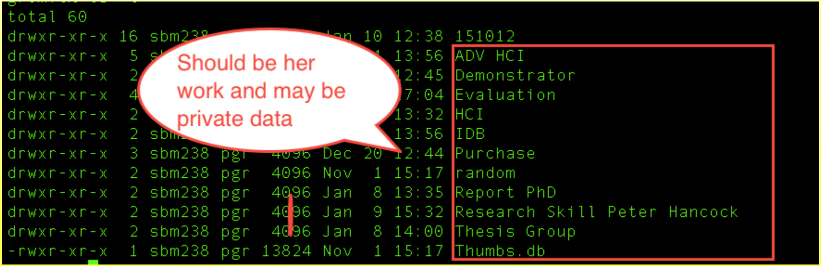
```
gromit% pwd
/home/students/wxy113
gromit% ls -l
total 15192
-rwxr-xr-x 1 wxy113 pgr   641654 Jun 25  2012 1-s2.0-S0960982212004708-main.pdf
-rwxr-xr-x 1 wxy113 pgr      736 May  8  2012 artifacts.xml
-rwxr-xr-x 1 wxy113 pgr 13802698 Jun 13  2012 BlueFinNBaitBall.wmv
drwxr-xr-x 2 wxy113 pgr     4096 May  8  2012 Desktop
-rwxr-xr-x 1 wxy113 pgr      402 Jul 19 19:54 desktop.ini
drwxr-xr-x 3 wxy113 pgr     4096 May  8  2012 Eclipse
drwxr-xr-x 2 wxy113 pgr     4096 May 23  2012 genatic
-rwxr-xr-x 1 wxy113 pgr    39738 Jun 26  2012 Giant_Moray_Eel_Reef_and_Scuba_Diver.jpg
-rwxr-xr-x 1 wxy113 pgr    75925 Jun 26  2012 goliath_grouper2.jpg
-rwxr-xr-x 1 wxy113 pgr   271219 Jun 26  2012 grouper1.jpg
-rwxr-xr-x 1 wxy113 pgr    63317 Jun 25  2012 GRS1A.docx
-rwxr-xr-x 1 wxy113 pgr   153941 Jun 25  2012 journal.pbio.0040431.pdf
drwxr-xr-x 3 wxy113 pgr     4096 Jun 27  2012 LYNDA.com
drwx------ 2 wxy113 pgr     4096 May  8  2012 mail
drwxr-xr-x 3 wxy113 pgr     4096 Jul 19 19:54 My Music
drwxr-xr-x 3 wxy113 pgr     4096 Aug 11 16:03 My Pictures
drwxr-xr-x 3 wxy113 pgr     4096 Jul 19 19:54 My Videos
drwxr-xr-x 3 wxy113 pgr     8192 Jun  1  2012 ODT_Fullmer
drwxr-xr-x 4 wxy113 pgr     4096 May  8  2012 p2
drwxr-xr-x 2 wxy113 pgr     4096 May 30  2012 $RECYCLE.BIN
-rwxr-xr-x 1 wxy113 pgr    15970 Jun 25  2012 RSMG1.docx
drwxr-xr-x 2 wxy113 pgr     4096 May 24  2012 swarm
-rwxr-xr-x 1 wxy113 pgr    23040 Jun 26  2012 Thumbs.db
drwxr-xr-x 2 wxy113 pgr     4096 Jun  1  2012 toxicology
-rwxr-xr-x 1 wxy113 pgr    43885 Jun  1  2012 Toxicology.pptx
drwxr-xr-x 7 wxy113 pgr     4096 Oct 25 16:47 Visual Studio 2010
drwxr-xr-x 5 wxy113 pgr     4096 Oct  4 15:30 windowsNEAT
-rwxr-xr-x 1 wxy113 pgr   266377 Oct  4 15:18 windowsNEAT.zip
drwx------ 2 wxy113 pgr     4096 May  8  2012 work
gromit%
```

Siti Mohd Shukri



```
gromit% pwd
/home/students/sbm238
gromit% ls -l
total 228
-rw-r--r--  1 sbm238 pgr 116658 Dec  3 17:28 C:\nppdf32Log\debuglog.txt
drwxr-xr-x  2 sbm238 pgr   4096 Dec 20 12:42 Desktop
-rwxr-xr-x  1 sbm238 pgr    402 Oct  4 14:07 desktop.ini
drwxr-xr-x  2 sbm238 pgr   4096 Oct 15 17:26 Documents
drwxr-xr-x  2 sbm238 pgr   4096 Dec  3 17:20 Downloads
-rwxr-xr-x  1 sbm238 pgr  34304 Dec 20 12:17 Drawing_3[1]m.doc
drwx------  2 sbm238 pgr   4096 Sep 14 10:53 mail
drwxr-xr-x  2 sbm238 pgr   4096 Oct  8 14:56 Music
drwxr-xr-x  3 sbm238 pgr   4096 Oct  4 14:07 My Music
drwxr-xr-x  3 sbm238 pgr   4096 Oct 12 12:21 My Pictures
drwxr-xr-x  3 sbm238 pgr   4096 Oct  4 14:07 My Videos
drwxr-xr-x  2 sbm238 pgr   4096 Oct  8 14:56 Pictures
drwxr-xr-x  2 sbm238 pgr   4096 Oct  8 14:56 Public
drwxr-xr-x  2 sbm238 pgr   4096 Dec 20 12:44 $RECYCLE.BIN
drwxr-xr-x 13 sbm238 pgr   4096 Jan  9 15:32 Siti
drwxr-xr-x 10 sbm238 pgr   4096 Dec  3 17:21 stats
drwxr-xr-x  2 sbm238 pgr   4096 Oct  8 14:56 Templates
drwxr-xr-x  2 sbm238 pgr   4096 Oct  8 14:56 Videos
drwx------  2 sbm238 pgr   4096 Sep 14 10:53 work
gromit%
```

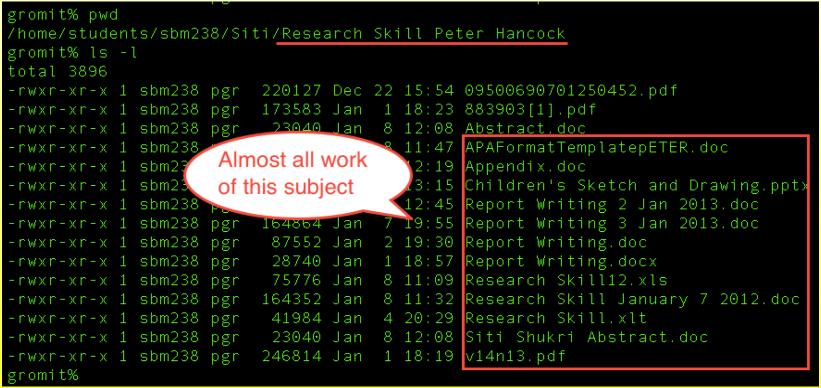
Siti Mohd Shukri (Cont. A)



```
total 60
drwxr-xr-x 16 sbm238             Jan 10 12:38 151012
drwxr-xr-x  5 s                     1 13:56 ADV HCI
drwxr-xr-x  2                        12:45 Demonstrator
drwxr-xr-x  4                         7:04 Evaluation
drwxr-xr-x  2                        13:32 HCI
drwxr-xr-x  2 sb                     13:56 IDB
drwxr-xr-x  3 sbm238 pgr  4096 Dec 20 12:44 Purchase
drwxr-xr-x  2 sbm238 pgr  4096 Nov  1 15:17 random
drwxr-xr-x  2 sbm238 pgr  4096 Jan  8 13:35 Report PhD
drwxr-xr-x  2 sbm238 pgr  4096 Jan  9 15:32 Research Skill Peter Hancock
drwxr-xr-x  2 sbm238 pgr  4096 Jan  8 14:00 Thesis Group
-rwxr-xr-x  1 sbm238 pgr 13824 Nov  1 15:17 Thumbs.db
```

Should be her work and may be private data

Siti Mohd Shukri (Cont. B)



```
gromit% pwd
/home/students/sbm238/Siti/Research Skill Peter Hancock
gromit% ls -l
total 3896
-rwxr-xr-x 1 sbm238 pgr  220127 Dec 22 15:54 09500690701250452.pdf
-rwxr-xr-x 1 sbm238 pgr  173583 Jan  1 18:23 883903[1].pdf
-rwxr-xr-x 1 sbm238 pgr   23040 Jan  8 12:08 Abstract.doc
-rwxr-xr-x 1 sbm238                        8 11:47 APAFormatTemplatepETER.doc
-rwxr-xr-x 1 sbm23                          2:19 Appendix.doc
-rwxr-xr-x 1 sbm23                          3:15 Children's Sketch and Drawing.pptx
-rwxr-xr-x 1 sbm238                          12:45 Report Writing 2 Jan 2013.doc
-rwxr-xr-x 1 sbm238 pgr  164864 Jan  7 19:55 Report Writing 3 Jan 2013.doc
-rwxr-xr-x 1 sbm238 pgr   87552 Jan  2 19:30 Report Writing.doc
-rwxr-xr-x 1 sbm238 pgr   28740 Jan  1 18:57 Report Writing.docx
-rwxr-xr-x 1 sbm238 pgr   75776 Jan  8 11:09 Research Skill12.xls
-rwxr-xr-x 1 sbm238 pgr  164352 Jan  8 11:32 Research Skill January 7 2012.doc
-rwxr-xr-x 1 sbm238 pgr   41984 Jan  4 20:29 Research Skill.xlt
-rwxr-xr-x 1 sbm238 pgr   23040 Jan  8 12:08 Siti Shukri Abstract.doc
-rwxr-xr-x 1 sbm238 pgr  246814 Jan  1 18:19 v14n13.pdf
gromit%
```

Almost all work of this subject

Security Concerns

All about data.

Confidentiality
Integrity
Availability

Strong adversary concerns (Key Escrow):

Security Concerns

All about data.

Confidentiality
Integrity
Availability

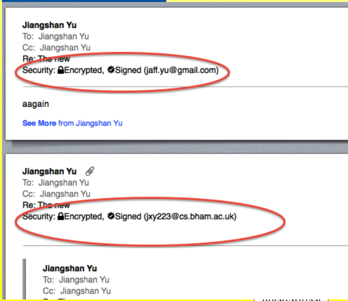
Strong adversary concerns (Key Escrow):
Dropbox (as well as Google Drive)

Security Concerns

All about data.

Confidentiality
Integrity
Availability

Strong adversary concerns (Key Escrow):
Dropbox (as well as Google Drive)
Email



Jiangshan Yu
To: Jiangshan Yu
Cc: Jiangshan Yu
Re: The new
Security: Encrypted, Signed (jaff.yu@gmail.com)

aagain

See More from Jiangshan Yu

Jiangshan Yu
To: Jiangshan Yu
Cc: Jiangshan Yu
Re: The new
Security: Encrypted, Signed (jxy223@cs.bham.ac.uk)

Jiangshan Yu
To: Jiangshan Yu
Cc: Jiangshan Yu

Current Solutions

- Fully homomorphic encryption
- Key translation
- Hardware based security

Fully homomorphic encryption

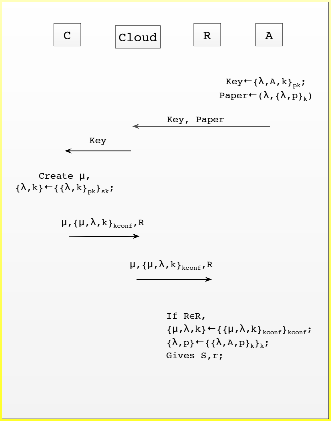
- $C_1 = Enc(pk, m_1)$
- $C_2 = Enc(pk, m_2)$

Fully homomorphic encryption

- $C_1 = Enc(pk, m_1)$
- $C_2 = Enc(pk, m_2)$
- $Enc(m_1 \cdot m_2) = C_1 \cdot C_2$

Key translation

ConfiChair[2]



C

Cloud

R

A

$\text{Key} \leftarrow \{\lambda, A, k\}_{pk}$;
$\text{Paper} \leftarrow (\lambda, \{\lambda, p\}_k)$

Key, Paper

Key

Create μ,
$\{\lambda, k\} \leftarrow \{\{\lambda, k\}_{pk}\}_{sk}$;

$\mu, \{\mu, \lambda, k\}_{kconf}, R$

$\mu, \{\mu, \lambda, k\}_{kconf}, R$

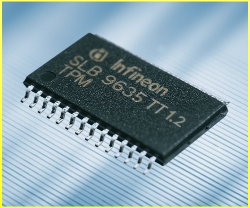
If $R \in R$,
$\{\mu, \lambda, k\} \leftarrow \{\{\mu, \lambda, k\}_{kconf}\}_{kconf}$;
$\{\lambda, p\} \leftarrow \{\{\lambda, A, p\}_k\}_k$;
Gives S,r;

[2] M. Arapinis,S. Bursuc,M. Ryan, "Privacy Supporting Cloud Computing: ConfiChair, a Case Study," *POST, 2012, pp. 89-108*

Hardware based security

Trusted Platform Module (TPM) (1.2, Mar. 2011).
Applications:

- **Intel's** trusted execution technology (TXT)
- **AMD's** secure virtual machine (SVM)
- etc.



Contributions

Previous:
Current:

[3] Guilin Wang, Jiangshan Yu, Qi Xie. Security Analysis of A Single Sign-On Mechanism for Distributed Computer Networks. IEEE Transactions on Industrial Informatics, July, 2012.(To appear)

[4] Jiangshan Yu, Guilin Wang, and Yi Mu. Provably Secure Single Sign-on Scheme in Distributed Systems and Networks. The 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, June 25-27 2012, Liverpool, UK.

Contributions

Previous: Single Sign-On (SSO)[3,4]
Current:

[3] Guilin Wang, Jiangshan Yu, Qi Xie. Security Analysis of A Single Sign-On Mechanism for Distributed Computer Networks. IEEE Transactions on Industrial Informatics, July, 2012.(To appear)

[4] Jiangshan Yu, Guilin Wang, and Yi Mu. Provably Secure Single Sign-on Scheme in Distributed Systems and Networks. The 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, June 25-27 2012, Liverpool, UK.

Contributions

Previous: Single Sign-On (SSO)[3,4]
Current: Not yet

[3] Guilin Wang, Jiangshan Yu, Qi Xie. Security Analysis of A Single Sign-On Mechanism for Distributed Computer Networks. IEEE Transactions on Industrial Informatics, July, 2012.(To appear)

[4] Jiangshan Yu, Guilin Wang, and Yi Mu. Provably Secure Single Sign-on Scheme in Distributed Systems and Networks. The 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, June 25-27 2012, Liverpool, UK.

M. Arapinis, S. Bursuc, and M. Ryan, “Privacy Supporting Cloud Computing: ConfiChair, a Case Study”,*POST 2012*, pp. 89-108, 2012.

G. Ateniese and R.Burns, “Provable data possession at untrusted stores”, *ACM CCS 2007*, pp. 598-609, 2007.

K. Bowers, M. Dijk, A. Juels, A. Oprea, and R. Rivest, “How to tell if your cloud files are vulnerable to drive crashes”, *Proc. of CCS 2011*, pp. 501-514, 2011.

R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility”, *Future Gener. Comput. Syst.*, vol. 25, No. 6, pp. 599-616, 2009.

R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, “Controlling data in the cloud: outsourcing computation without outsourcing control”,*Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW 2009)*, pp. 85-90, 2009.

M. Joshi and Y. S. Moudgil, “Secure Cloud Storage,” *International Journal of Computer Science & Communication Networks*, Vol. 1, No. 2, pp. 171-175, 2011.

S. Kamara and K. Lauter, “Cryptographic cloud storage,” *In Proceedings of the 14th international conference on Financial cryptograpy and data security (FC’10)*, Springer-Verlag, Berlin, Heidelberg, 136-149, 2010.

K. Lauter, M. Naehrig, and V. Vaikuntanathan, “Can homomorphic encryption be practical?” Manuscript at *http://eprint.iacr.org/2011/405*, 2011.

S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” *Journal of Network and Computer Applications*, Vol. 34, No. 1, Pages 1-11, January 2011.

Z. Wan, J. Liu and Robert H. Deng, “HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing,” . *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 2, pp. 743-754, 2012.

G. Wang, Q. Liu, and J. Wu, “Hierarchical attribute-based encryption for ?ne-grained access control in cloud storage services,” *ACM Conference on Computer and Communications Security*, pp. 735737, 2010.

K. Xi, Y. Tang, J. Hu, “Correlation Keystroke Verification Scheme for User Access Control in Cloud Computing Environment”, *Comput. J.*, Vol. 54, No. 10, pp. 1632-1644, 2011.

Z. Zhang, T. Plantard, and W. Susilo, “On the CCA-1 Security of Somewhat Homomorphic Encryption over the Integers”, *ISPEC 2012*, pp. 353-368, 2012.

Q&S Time!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!