

# Security in the Cloud Era

**Dimitris Gritzalis**

**October 2011**

# Ασφάλεια στην εποχή του Cloud: Παράδοξο ή απλώς διαφορετικό;

**Δημήτρης Γκρίτζαλης**

Καθηγητής Ασφάλειας στις ΤΠΕ

Οικονομικό Πανεπιστήμιο Αθηνών

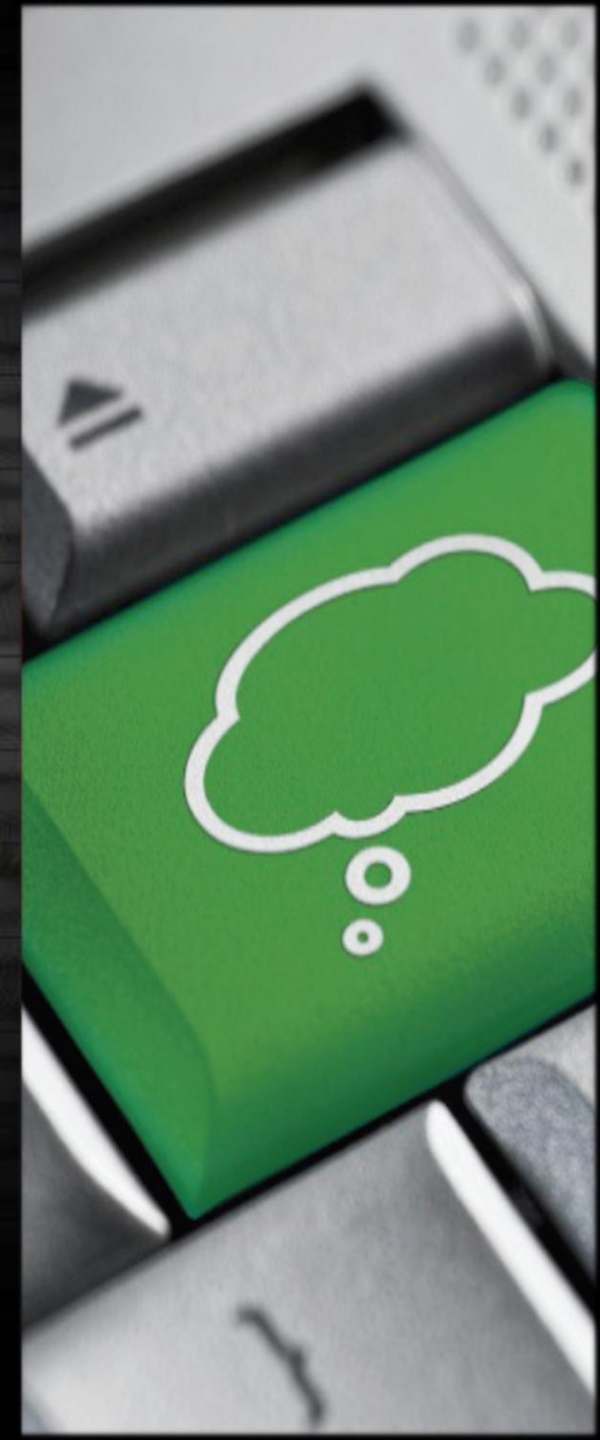
Πρόεδρος Δ.Σ. Ψηφιακές Ενισχύσεις Α.Ε.



## Το “Σύννεφο” ...

Το υπολογιστικό σύννεφο αποτελεί ένα **νέο οικονομικό μοντέλο** για παροχή υπολογιστικών υπηρεσιών.

Δεν αποτελεί μια νέα τεχνολογία.



# Το “Σύννεφο” ...

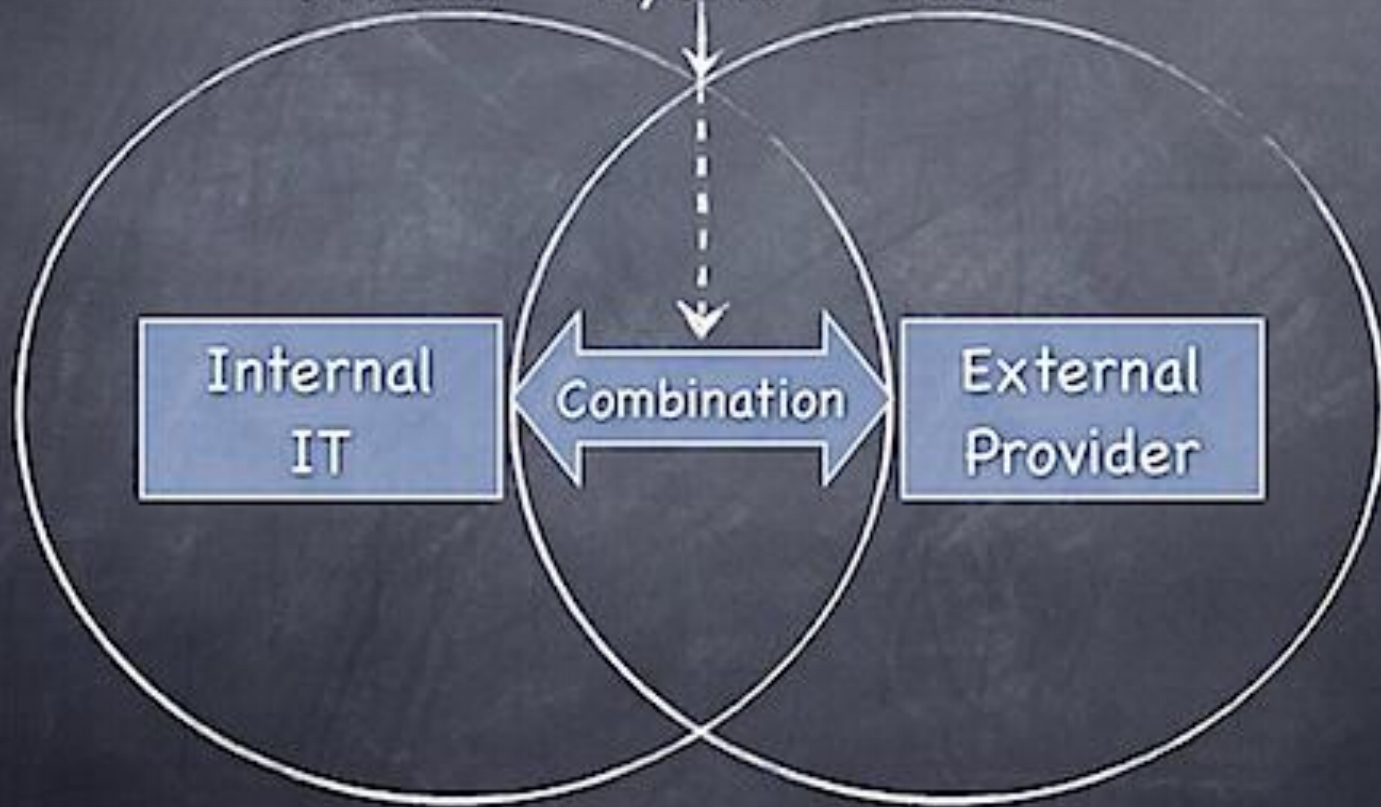
## Βασικά χαρακτηριστικά κατά NIST:

- Αυτοεξυπηρέτηση κατόπιν απαίτησης (On-demand Self-Service)
- Ευρεία δικτυακή πρόσβαση (Ubiquitous network access)
- Δυναμική εκχώρηση πόρων (Dynamic Resource Allocation)
- Ταχεία ελαστικότητα (Rapid elasticity)
- Μετρήσιμη υπηρεσία (Measured Service)

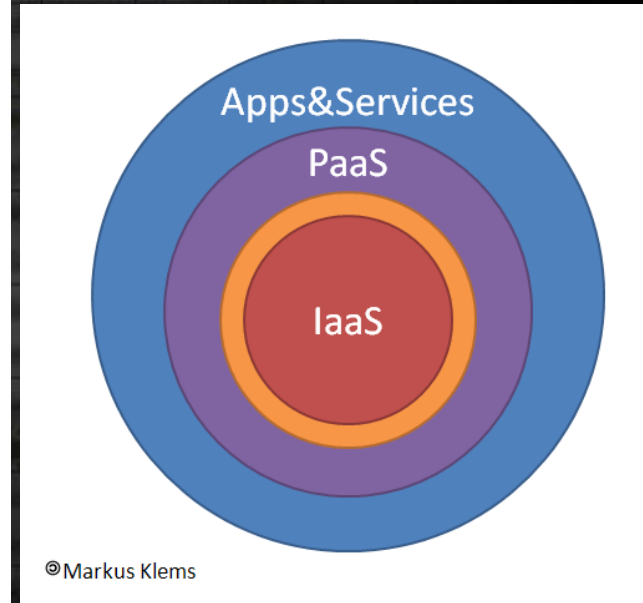
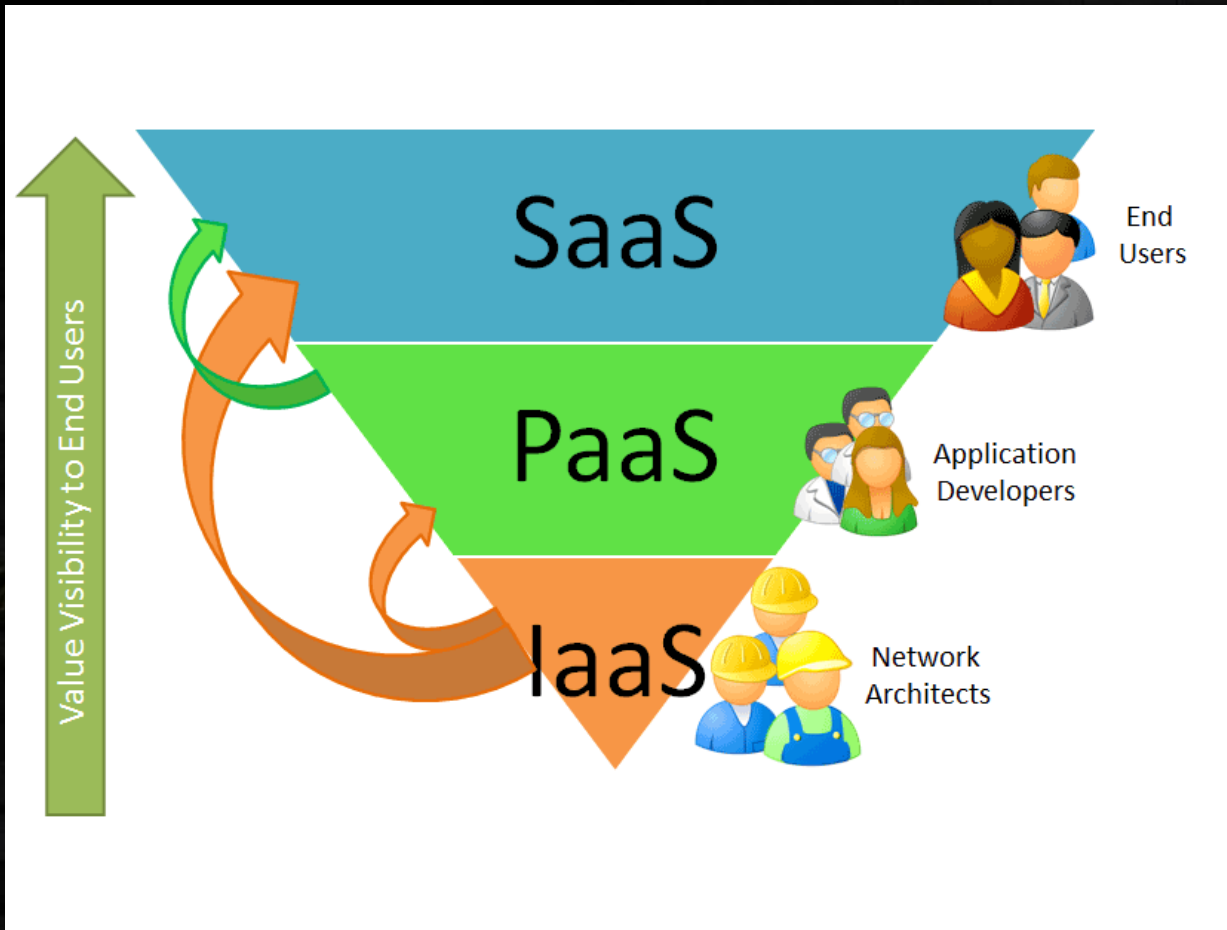
# Τρία βασικά είδη

## Types of Clouds

Private      Hybrid      Public



# Everything as a Service



Gartner<sup>1</sup>: To 2011 θα είναι η χρόνια του PaaS.

<sup>1</sup> <http://www.gartner.com/it/page.jsp?id=1586114>

# It's all about Money

Επιχειρήσεις + Cloud = Μειωμένο κόστος  
(Αγοράς, Συντήρησης, Ανάπτυξης)



# Επενδύσεις στο Σύννεφο

## Προϋπολογισμός Η.Π.Α. 2012<sup>1</sup>:

- **20 δις δολάρια** το χρόνο στο Cloud Computing.

## Ευρωπαϊκή Ένωση<sup>2</sup>:

- **€15.7 εκατομμύρια** για έρευνα στο Cloud, με έμφαση στο data mobility και τον έλεγχο πρόσβασης.

## UK's Centre for Economics and Business Research<sup>3</sup>:

- Υιοθέτηση του Cloud μπορεί να **εξοικονομήσει** περισσότερα από **€763 εκατομμύρια ευρώ** στις ευρωπαϊκές αγορές μεταξύ του 2010 και 2015.

<sup>1</sup> <http://fcw.com/articles/2011/02/28/buzz-cloud-computing-and-budget.aspx>

<sup>2</sup> <http://www.visioncloud.eu/>

<sup>3</sup> <http://www.redstor.com/downloads/cloud-dividend-report.pdf>

# Πόσο ασφαλές είναι το “Σύννεφο”?

ENISA<sup>1</sup>:

Οι βασικότερες ανησυχίες για την υιοθέτησή του σε επιχειρήσεις είναι η διασφάλιση:

1. Ιδιωτικότητας
2. Διαθεσιμότητας
3. Ακεραιότητας
4. Εμπιστευτικότητας

<sup>1</sup> <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-sme-survey>

# Πόσο ασφαλές είναι το “Σύννεφο”?

Cloud Security Alliance<sup>1</sup>:

## Κυριότερες Απειλές:

- Αδυναμίες λόγω κοινής χρήσης υπηρεσιών
- Data loss / Data leakage
- Επιθέσεις εκ των έσω
- Μη εξουσιοδοτημένη πρόσβαση σε πόρους (Account Hijacking)
- Μη ασφαλή API's
- Εκμετάλλευση του Cloud από κακόβουλους χρήστες (Spamming, Phishing, Password Cracking)

<sup>1</sup> <http://www.cloudsecurityalliance.org/>

## Παραχωρήσεις...

Υιοθετώντας cloud υπηρεσίες **παραχωρούμε τον έλεγχο** των δεδομένων μας στο πάροχο.

Τις περισσότερες φορές, δεν γνωρίζουμε καν τη φυσική τοποθεσία που βρίσκονται αποθηκευμένα.



Καλούμαστε να αντιμετωπίσουμε **νέα νομικά** και **τεχνικά ζητήματα**

# Νέα Ζητήματα

- 1. Διαχείριση κινδύνου:** Οι παραδοσιακές τεχνικές διαχείρισης κίνδυνου είναι δύσκολο ή ακόμα και αδύνατο να εφαρμοστούν.
- 2. Πρότυπα:** Η δυσκολία φυσικής πρόσβασης στο datacenter δημιουργεί προβλήματα συμμόρφωσης με ορισμένα πρότυπα (π.χ. PCI - Level 1).



# Νέα Ζητήματα

- 3. Διαχείριση συμβάντων:** Η τυπική διαδικασία της δικανικής πληροφορικής είναι εξαιρετικά πολύπλοκη σε ένα τέτοιο περιβάλλον.
- 4. Νομικά Κενά:** Αν χρησιμοποιήσουμε τα data centers της Amazon στην Ευρώπη σε ποια νομοθεσία υπόκεινται τα δεδομένα μας? Ευρωπαϊκή, Αμερικάνικη ή και τις δύο?



# Συμπεράσματα

Το Cloud αδιαμφισβήτητα αποτελεί μια **επανάσταση** για τις ΤΠΕ κυρίως χάρη στα **οικονομικά οφέλη**.

Η **ασφάλεια** όμως είναι ο **σημαντικότερος παράγοντας** που επηρεάζει τη διάδοση/υιοθέτηση του cloud computing.

Τα τεχνικά και νομικά κενά, θα πρέπει να αντιμετωπιστούν ορθά και με ακρίβεια, ώστε να γενικευτεί η χρήση cloud υπηρεσιών.



## References

1. Gritzalis D., *Secure Electronic Voting*, Springer, 2003.
2. Kandias M., Mylonas A., Virvilis N., Theoharidou M., Gritzalis D., "An Insider Threat Prediction Model", in *Proc. of the 7<sup>th</sup> International Conference on Trust, Privacy, and Security in Digital Business*, pp. 26-37, Springer, 2010.
3. Lekkas D., Gritzalis D., "e-Passports as a means towards a globally interoperable Public Key Infrastructure", *Journal of Computer Security*, Vol. 18, No. 3, pp. 379-396, 2010.
4. Lekkas D., Gritzalis D., Cumulative Notarization for Long-term Preservation of Digital Signatures, *Computers & Security*, Vol. 23, no. 5, pp. 413-424, 2004.
5. Soupionis Y., Dritsas S., Gritzalis D., "An adaptive policy-based approach to SPIT management", in *Proc. of the 13<sup>th</sup> European Symposium on Research in Computer Security*, Springer, 2008.
6. Spinellis D., Gritzalis D., "PANOPTIS: Intrusion detection using process accounting records", *Journal of Computer Security*, Vol. 10, No. 2, pp. 159-176, IOS Press, 2002.
7. Theoharidou M., Kotzanikolaou P., Gritzalis D., "A multi-layer criticality assessment methodology based on interdependencies", *Computers & Security*, Vol. 29, No. 6, pp. 643-658, 2010.
8. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk-based Criticality Analysis", in *Proc. of the 3<sup>rd</sup> IFIP International Conference on Critical Infrastructure Protection*, Springer, 2009.
9. Theoharidou M., Marias J., Dritsas S., Gritzalis D., "The Ambient Intelligence Paradigm: A review of security and privacy strategies in leading economies", in *Proc. of the 2<sup>nd</sup> IET Conference on Intelligent Environments*, Vol. 2, pp. 213-219, 2006.
10. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk assessment methodology for interdependent Critical Infrastructures", *International Journal of Risk Assessment and Management*, Vol. 15, Nos. 2/3, pp. 128-148, 2011.
11. Virvilis N., Dritsas S., Gritzalis D., "A cloud provider-agnostic secure storage protocol", in *Proc. of the 5<sup>th</sup> International Workshop on Critical Information Infrastructure Security*, pp. 104-115, Springer, 2010.