



**ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ**

**UNIVERSITY OF MACEDONIA**

**ΔΠΜΣ Πληροφοριακά Συστήματα**

**Master Information Systems**

**Δίκτυα Υπολογιστών**

**Computer Networks**

**Καθηγητής: Α.Α. Οικονομίδης**

**Professor: A.A. Economides**

**ΕΡΓΑΣΙΑ / TUTORIAL:**

**SURVIVABILITY AND RELIABILITY IN CLOUD NETWORKING**

**ΙΚΑΝΟΤΗΤΑ ΕΠΙΒΙΩΣΗΣ ΚΑΙ ΑΞΙΟΠΙΣΤΙΑ ΣΤΗ ΔΙΚΤΥΩΣΗ  
ΝΕΦΟΥΣ**

**ΕΙΣΗΓΗΤΡΙΑ / STUDENT:**

**ΕΥΓΕΝΙΑ ΠΟΠΗ / EUGENIA POPI (MIS 1311)**

**ΘΕΣΣΑΛΟΝΙΚΗ / THESSALONIKI**

**ΙΑΝΟΥΑΡΙΟΣ / JANUARY 2014**

## ΠΕΡΙΕΧΟΜΕΝΑ:

ΠΕΡΙΛΗΨΗ / ABSTRACT.....	σελ. 1
ΠΑΡΟΥΣΙΑΣΗ ΘΕΜΑΤΟΣ.....	σελ. 2
1. Ορισμός της υπολογιστικής νέφους (Cloud Computing).....	σελ. 3
Θεμελιώδη χαρακτηριστικά νέφους.....	σελ. 4
Μοντέλα υπηρεσιών.....	σελ. 4
Μοντέλα ανάπτυξης (Deployment models).....	σελ. 6
Δικτύωση νέφους (Cloud Networking).....	σελ. 7
2. Τα πλεονεκτήματα και μειονεκτήματα της υπολογιστικής νέφους.....	σελ. 8
Πλεονεκτήματα δικτύωσης νέφους.....	σελ. 8
Μειονεκτήματα δικτύωσης νέφους.....	σελ. 10
3. Αξιοπιστία (reliability) στη δικτύωση νέφους.....	σελ. 12
Εξάρτηση από το διαδίκτυο.....	σελ. 13
Βλάβες κατά την παροχή στο νέφος (cloud provider outages).....	σελ. 14
Δυσκολίες εξέτασης αξιοπιστίας.....	σελ. 15
4. Ικανότητα επιβίωσης (survivability) στη δικτύωση νέφους.....	σελ. 17
Ο ρόλος των ιδεατών δικτύων στην ικανότητα επιβίωσης μιας δικτύωσης νέφους.....	σελ. 17
Κίνδυνοι επιβίωσης και ασφάλειας των πληροφοριών.....	σελ. 18
ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ.....	σελ. 19
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	σελ. 20

## ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία αποτελεί μια εισαγωγική παρουσίαση του ραγδαία αναπτυσσόμενου τομέα της υπολογιστικής νέφους, επικεντρώνοντας την ανάλυση στο ζήτημα της αξιοπιστίας (reliability) και της ικανότητας επιβίωσης (survivability) στην παροχή υπηρεσιών μέσω τη δικτύωσης νέφους. Η εργασία ξεκινάει με την παρουσίαση της υπολογιστικής νέφους, τις μορφές και τα είδη των υπηρεσιών που παρέχονται, αναλύοντας στη συνέχεια τα πλεονεκτήματα, καθώς και τα μειονεκτήματα – κινδύνους που ελλοχεύουν κατά τη χρήση της τεχνολογίας αυτής. Στη συνέχεια αναπτύσσονται τα ζητήματα της αξιοπιστίας της δικτύωσης κατά την παροχή των υπηρεσιών νέφους, καθώς και η ικανότητα επιβίωσής της παράλληλα με τη ραγδαία ανάπτυξή της.

## ABSTRACT

The current tutorial is an introduction to the rapidly developing technology of cloud computing, focusing in cloud networking reliability and survivability. In the first part of the essay are presented the basic elements of cloud computing such as the types and forms of the services that are provided. In the second part are analyzed the benefits as well as the risks and disadvantages that arise in the use of the cloud and finally in the last part we discuss the issues of reliability and survivability in cloud networking which occur nowadays.

## ΠΑΡΟΥΣΙΑΣΗ ΘΕΜΑΤΟΣ

Η δικτύωση νέφους αποτελεί το πλαίσιο μέσω του οποίου δίνεται η δυνατότητα παροχής πόρων και υπηρεσιών μέσω του διαδικτύου (Internet). Ο στόχος στη σχεδίαση και υλοποίηση του μοντέλου αυτού είναι η καλύτερη χρήση των πόρων και η ορθή συνεργασία αυτών ώστε να επιτευχθεί η υψηλότερη δυνατή απόδοση, διαθεσιμότητα, αξιοπιστία και δυνατότητα επέκτασης (extensibility) (Wang L., Ranjan R., Chen J., Benatallah B. 2012). Το κύριο χαρακτηριστικό των συστημάτων υπολογιστικής νέφους (Cloud Computing Systems – CCS), το οποίο τα διαχωρίζει άλλα είδους συστήματα όπως η υπολογιστική πλέγματος (Grid) και η υπολογιστική Cluster είναι ο διαμοιρασμός ενός πλήθους υπηρεσιών, τη χρήση των οποίων δύναται να αιτηθούν καταναλωτές από όλο τον κόσμο (Shojaee R., Faragardi H. R., Alae S. and Yazdani N. 2012).

Λόγω του χαρακτηριστικού της μεγάλης κλίμακας διαμοιρασμού των υπηρεσιών καθώς και των ετερογενών συστατικών της δικτύωσης αυτής, τόσο σε επίπεδο λογισμικού (software) όσο και σε επίπεδο φυσικών πόρων (hardware), ο κίνδυνος ύπαρξης σφαλμάτων είναι μεγάλος. Προκειμένου να υπάρχει η εγγύηση στην παροχή αξιόπιστων υπηρεσιών (reliable services) και στην ικανότητα επιβίωσης (survivability) στη δικτύωση νέφους, η ανάπτυξη των σχετικών μοντέλων από τις επιχειρήσεις παροχής υπηρεσιών νέφους είναι ένα από τα φλέγοντα ζητήματα που τις απασχολούν (Gu F., Alazemi H., Rayes A., Ghani N. 2013).

## 1. Ορισμός της υπολογιστικής νέφους (Cloud Computing)

Η υπολογιστική νέφος (cloud computing) είναι μια έννοια η οποία έκανε την εμφάνισή της τα τελευταία χρόνια, παρόλα αυτά, οι αρχές και τα μοτίβα στα οποία βασίζεται η τεχνολογία αυτή, χρησιμοποιούνται από τις απαρχές της χρήσης των ηλεκτρονικών υπολογιστών (Christopher M. Moyer 2011).

Στις μέρες μας, η πλειοψηφία των χρηστών του διαδικτύου, ηθελημένα ή μη, κάνει χρήση των υπηρεσιών του νέφους, π.χ. επιλέγοντας το διαδίκτυο για την αποθήκευση των δεδομένων του αντί για τον σκληρό δίσκο του υπολογιστή τους, χρησιμοποιώντας το webmail και συμμετέχοντας σε σελίδες κοινωνικής δικτύωσης. Στις περιπτώσεις των επιχειρήσεων και οργανισμών, επιλέγεται η χρήση μιας διαδικτυακής υπηρεσίας (π.χ. στον τομέα της διαχείρισης πελατών - CRM), έναντι της επιλογής αναβάθμισης της ήδη υπάρχουσας εγκατεστημένης εφαρμογής που η ίδια η επιχείρηση χρησιμοποιεί.

Στη βιβλιογραφία, ο επίσημος - ευρέως αποδεκτός και ολοκληρωμένος ορισμός της έννοιας της υπολογιστικής νέφους δόθηκε το 2011 από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (National Institute of Standards and Technology – NIST) και είναι ο ακόλουθος: «Υπολογιστική νέφος είναι ένα μοντέλο το οποίο επιτρέπει την ευρέως διαδεδομένη, κατάλληλη, κατ' εντολή, διαδικτυακή πρόσβαση σε μια κοινή δεξαμενή σύνθετων υπολογιστικών πόρων (resources) (όπως δίκτυα, διακομιστές, μνήμη, εφαρμογές και υπηρεσίες) οι οποίοι μπορούν να παρασχεθούν γρήγορα και να διακοπούν με την ελάχιστη δυνατή διοικητική προσπάθεια ή ανάμειξη του πάροχου της υπηρεσίας. Αυτό το μοντέλο νέφους συντίθεται από πέντε θεμελιώδη χαρακτηριστικά, τρία μοντέλα εξυπηρέτησης και τέσσερα μοντέλα ανάπτυξης» (Mell, Grance 2011)

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models”

## Θεμελιώδη χαρακτηριστικά του νέφους

Σύμφωνα με τον ανωτέρω ορισμό, τα θεμελιώδη χαρακτηριστικά του νέφους είναι τα ακόλουθα:

- Κατ' εντολή αυτό-εξυπηρέτηση (On-demand self-service): Οι χρήστες έχουν μονομερώς και αυτόματα τη δυνατότητα να κάνουν χρήση των υπηρεσιών του νέφους
- Ευρεία δικτυακή πρόσβαση (Broad network access): Οι υπηρεσίες είναι διαρκώς διαθέσιμες και προσεγγίζονται μέσω ειδικών συσκευών με πρόσβαση στο διαδίκτυο (π.χ. κινητά τηλέφωνα, ταμπλέτες, lap-top, και τερματικοί σταθμοί).
- Διάχυση πόρων (Resource pooling): Οι υπολογιστικοί πόροι του παρόχου διατίθενται για την εξυπηρέτηση πολλαπλών πελατών, χρησιμοποιώντας ένα μοντέλο πολύ-μίσθωσης, με διαφορετικούς φυσικούς και εικονικούς πόρους οι οποίοι δυναμικά εκχωρούνται κατ' επανάληψη στους χρήστες. Παράλληλα, υπάρχει η αίσθηση της ανεξαρτησίας στην τοποθεσία, καθώς ο πελάτης δεν ασκεί έλεγχο και δεν έχει ακριβή γνώση σχετικά με την τοποθεσία από την οποία προωθούνται οι παρεχόμενες υπηρεσίες.
- Ταχεία ελαστικότητα (Rapid elasticity): Οι υπηρεσίες στον χρήστη παρέχονται άμεσα, ανάλογα με τη ζήτηση, οποιαδήποτε στιγμή και σε οποιαδήποτε ποσότητα.
- Μετρούμενη υπηρεσία (Measured Service): Τα υπολογιστικά συστήματα νέφους αυτομάτως ελέγχουν και βελτιστοποιούν τη χρήση των πόρων, παρέχοντας τη δυνατότητα μέτρησης των παρεχόμενων υπηρεσιών, σύμφωνα με το είδος της υπηρεσίας αυτής, (όπως παροχή μνήμης, επεξεργασία, εύρος σύνδεσης, λογαριασμοί ενεργών χρηστών). Τυπικά αυτό πραγματοποιείται με την πληρωμή με βάση τη χρήση. Η χρήση των πόρων δύναται να ελεγχθεί και να καταγραφεί, παρέχοντας διαφάνεια τόσο στον πάροχο της υπηρεσίας, όσο και στον χρήστη (Mell, Grance 2011).

## Μοντέλα υπηρεσιών

Αντίστοιχα, τα μοντέλα υπηρεσιών που προκύπτουν μέσω του υπολογιστικού νέφους είναι τα ακόλουθα:

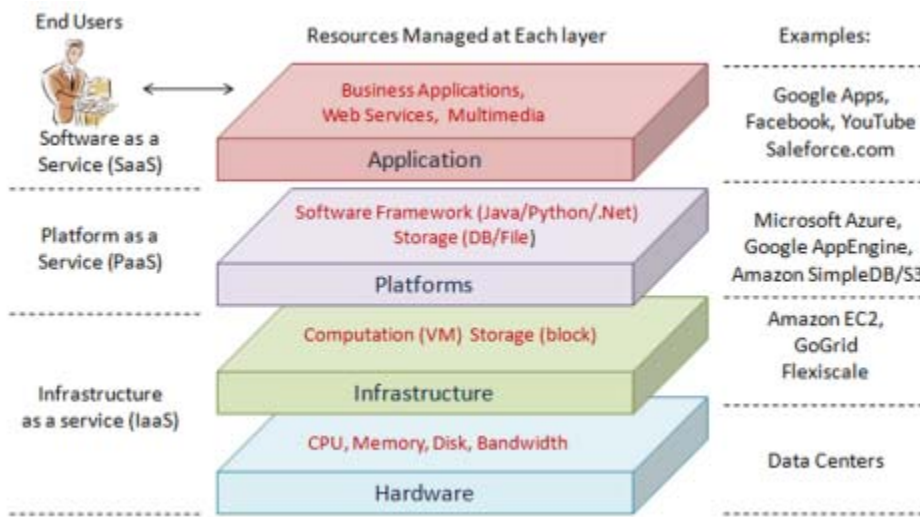
- Λογισμικό ως υπηρεσία (Cloud Software as a Service - SaaS): Πρόκειται για εφαρμογές οι οποίες αναπτύσσονται ως δανειζόμενες υπηρεσίες (hosted services) και οι οποίες

είναι προσβάσιμες μέσω του διαδικτύου. Η υποδομή νέφους περιλαμβάνει τόσο τη φυσική έννοια των εξαρτημάτων hardware, όπως τον διακομιστή (server), τη μνήμη (storage) και τα συστατικά μέρη του δικτύου (network components), όσο και την αφηρημένη έννοια της υποδομής που αποτελούν τα λειτουργικά συστήματα και η ίδια η εφαρμογή, η οποία καταδεικνύει τα θεμελιώδη χαρακτηριστικά του νέφους, όπως αναλύθηκαν ανωτέρω. Χρήστες των υπηρεσιών αυτών είναι Οργανισμοί οι οποίοι παρέχουν στα μέλη ή τους υπαλλήλους τους πρόσβαση σε τυπικές εφαρμογές λογισμικού, (όπως π.χ. το email και το CRM) και τελικοί χρήστες οι οποίοι απευθείας χρησιμοποιούν εφαρμογές λογισμικού. Παραδείγματα αυτής της υπηρεσίας είναι οι εφαρμογές που παρέχουν οι: Salesforce, LinkedIn, Workday, ServiceNow, NetSuite. (<http://www.onbile.com/info/top-10-software-as-a-service-saas-companies/>, Last access: 31/12/2013).

- Πλατφόρμα ως υπηρεσία (Cloud Platform as a Service – PaaS): Μέσω της υπηρεσίας αυτής ο χρήστης δύναται να αναπτύξει στο νέφος εφαρμογές, χρησιμοποιώντας γλώσσες προγραμματισμού και εργαλεία τα οποία υποστηρίζονται από τον πάροχο της υπηρεσίας. Κύριοι χρήστες της υπηρεσίας αυτής είναι επιχειρήσεις και ειδικοί ανάπτυξης εφαρμογών (application developers). Παραδείγματα τέτοιας εφαρμογής αποτελούν οι online πλατφόρμες: AppScale ([www.appscale.com](http://www.appscale.com)), Google App Engine (GAE) (<https://developers.google.com/appengine/>), AppFog (<https://www.appfog.com/>), Cloud Bees (<http://www.cloudbees.com/>).
- Υποδομή ως υπηρεσία (Cloud Infrastructure as a Service – IaaS): Μέσω της εν λόγω υπηρεσίας παρέχονται υποδομές επεξεργασίας, αποθήκευσης, δικτύωσης και άλλων θεμελιωδών υπολογιστικών πόρων, τους οποίους ο χρήστης χρησιμοποιεί προκειμένου να αναπτύξει και να τρέξει λογισμικό, όπως λειτουργικά συστήματα και εφαρμογές. Στην περίπτωση αυτή ο τελικός χρήστης δεν διαχειρίζεται ούτε ελέγχει την υποδομή, διατηρεί όμως τον έλεγχο στα λειτουργικά συστήματα, τη μνήμη, τις αναπτυσσόμενες εφαρμογές και πιθανώς ένα περιορισμένο μέρος της δικτύωσης, όπως τον τοίχο προστασίας. Κύριοι χρήστες της υπηρεσίας αυτής είναι διαχειριστές συστημάτων (System administrators) και αρχιτέκτονες δικτύου (Network architects). Παραδείγματα



πάροχων υπηρεσιών IaaS είναι οι: Amazon (EC2) (<http://aws.amazon.com/ec2/>), Rackspace (<http://www.rackspace.com/>), Gogrid (<http://www.gogrid.com/>).



Εικόνα 1: Η αρχιτεκτονική της υπολογιστικής νέφους  
(Πηγή: Zhang Q., Cheng L., Boutaba R. 2010)

### Μοντέλα ανάπτυξης (Deployment models)

Τα μοντέλα ανάπτυξης (deployment models) των ανωτέρω υπηρεσιών νέφους είναι τα ακόλουθα:

- **Ιδιωτικό νέφος (Private Cloud):** Η υποδομή παρέχεται για αποκλειστική χρήση από έναν οργανισμό ο οποίος αποτελείται από πολλαπλούς χρήστες, (π.χ. επιχειρήσεις). Η υποδομή δύναται να ανήκει και να διευθύνεται από τον οργανισμό ή έναν τρίτο ή με κάποιον συνδυασμό αυτών.
- **Κοινοτικό νέφος (Community Cloud):** Όμοια με το ιδιωτικό νέφος, η υποδομή στην περίπτωση αυτή παρέχεται για αποκλειστική χρήση από οργανισμούς που έχουν κοινές υποθέσεις, όπως αποστολές, απαιτήσεις ασφάλειας και πολιτική.
- **Δημόσιο νέφος (Public Cloud):** Στην περίπτωση αυτή, οι υποδομές παρέχονται ανοιχτά στο ευρύ κοινό. Κάτοχος και διαχειριστής των υποδομών ενός δημόσιου νέφους δύναται να είναι μια επιχείρηση, ένας ακαδημαϊκός ή κρατικός οργανισμός

ή ακόμα ένας συνδυασμός αυτών. Η υποδομή του δημόσιου νέφους βρίσκεται στο χώρο του παροχέα της υπηρεσίας.

- Υβριδικό νέφος (Hybrid Cloud): Η υποδομή είναι ένας συνδυασμός δύο ή περισσότερων υποδομών (ιδιωτικό, κοινοτικό ή δημόσιο) οι οποίες παραμένουν διαχωρισμένες αλλά δένονται μέσω μιας τυποποιημένης ή ιδιόκτητης τεχνολογίας η οποία επιτρέπει τη μεταφορά δεδομένων (Wang L., Ranjan R., Chen J., Benatallah B. 2012).

### **Δικτύωση νέφους (Cloud Networking)**

Η υιοθέτηση της υπολογιστικής νέφους δημιουργεί πολύ σημαντικές απαιτήσεις και προκλήσεις οι οποίες αφορούν τη δικτύωση. Σε αναγνώριση των απαιτήσεων αυτών, η έννοια δικτύωση νέφους (cloud networking), αναφέρεται στα Τοπικά Δίκτυα Υπολογιστών (Local Area Network - LAN), τα Δίκτυα ευρείας περιοχής (Wide Area Network – WAN) και τις διαχειριστικές λειτουργίες (Network Management) τις οποίες οι οργανισμοί των τεχνολογιών πληροφορικής (IT organizations) πρέπει να διευθετήσουν προκειμένου να υλοποιηθεί η υπολογιστική νέφους. Ως πιο απαιτητική, η δικτύωση νέφους θα πρέπει να είναι πολύ πιο ευκίνητη και αποδοτική από ότι είναι ένα παραδοσιακό δίκτυο (Metzler J., Metzler A. & Associates 2011).

Η αρχιτεκτονική της δικτύωσης νέφους περιλαμβάνει το Σύστημα Διαχείρισης Νέφους (Cloud Management System – CMS) το οποίο συντίθεται από έναν αριθμό διακομιστών (servers) οι οποίοι είναι είτε αποκεντρωμένοι, είτε συγκεντρωμένοι σε ένα κεντρικό σημείο. Το σύστημα αυτό εκπληρώνει τέσσερις διαφορετικές λειτουργίες:

- 1) Διαχειρίζεται μια σειρά αιτημάτων (request queue) από διαφορετικούς χρήστες για την εκτέλεση εργασιών που αφορούν τις υπηρεσίες νέφους
- 2) Διαχειρίζεται τους υπολογιστικούς πόρους, όπως υπολογιστές, Clusters και υπερ-υπολογιστές σε όλο το διαδίκτυο.
- 3) Διαχειρίζεται τους πόρους δεδομένων, όπως οι βάσεις δεδομένων, δημοσιευμένη πληροφορία, περιεχόμενα URL σε όλο το διαδίκτυο
- 4) Ρυθμίζει ένα αίτημα, διαχωρίζοντάς το σε διαφορετικές διεργασίες (subtasks) και αναθέτει τις διεργασίες αυτές σε διαφορετικούς υπολογιστικούς πόρους, οι οποίοι

δύνата να έχουν πρόσβαση σε διαφορετικούς πόρους δεδομένων. (Dai Y. S., Yang B., Dongarra J., Zhang G. 2010)

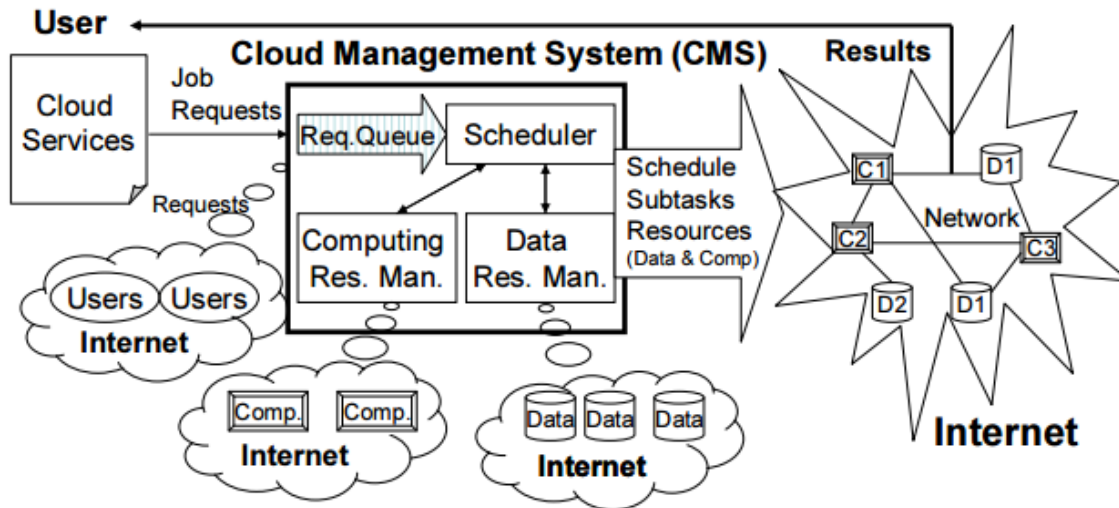


Fig. 1. Cloud Service System.

Εικ 2: Σύστημα διαχείρισης νέφους  
(Dai Y. S., Yang B., Dongarra J., Zhang G. 2010)

## 2. Τα πλεονεκτήματα και μειονεκτήματα της υπολογιστικής νέφους

### 1. Πλεονεκτήματα δικτύωσης νέφους

Το νέφος μεταμορφώνει τις δικτυακές υποδομές δίνοντας τη δυνατότητα σε επιχειρήσεις κάθε μεγέθους να υιοθετούν και να λειτουργούν εφαρμογές χωρίς το κόστος, την πολυπλοκότητα και τους περιορισμούς των παραδοσιακών δικτύων. Η δικτύωση νέφους μοιράζεται πολλά από τα πλεονεκτήματα των υπηρεσιών του νέφους, όπως υψηλή επεκτασιμότητα, εύκολη διαχείριση, μείωση του κόστους από την μη αγορά υποδομής και ενημέρωσης λογισμικού ή ετήσιας συντήρησης, συνδρομή με βάση τη χρήση, ενσωματωμένη αναβάθμιση και πρόσβαση από παντού μέσω του Διαδικτύου.

- Μείωση κόστους: Οι υπηρεσίες νέφους είναι δημοφιλείς για τις επιχειρήσεις και τους καταναλωτές, καθώς μειώνουν το κόστος κτήσης και λειτουργίας της φυσικής υποδομής του δικτύου, όπως η αγορά και κατοχή συσκευών αποθήκευσης και διακομιστών. Επιπλέον, καθώς η διαφύλαξη των δεδομένων και το μεγαλύτερο μέρος της επεξεργασίας γίνεται από τις κεντρικές μονάδες επεξεργασίας (CPUs) του παρόχου, οι τελικοί χρήστες δεν υποχρεώνονται να αγοράσουν ακριβούς Η/Υ προκειμένου να επεξεργαστούν τις εφαρμογές του νέφους. Επίσης, η μη αγορά λογισμικού μειώνει το κόστος βραχυπρόθεσμα, ενώ σε πολλές περιπτώσεις οι εφαρμογές νέφους παρέχονται δωρεάν στους τελικούς χρήστες (J. Dale Prince 2011).
- Υψηλή επεκτασιμότητα (scalability): Οι πάροχοι υποδομών διαχέουν ένα μεγάλο όγκο πόρων από τα κέντρα δεδομένων, τα οποία παρέχουν στους πελάτες με εύκολα προσβάσιμο τρόπο. Την ίδια στιγμή, κάποιος πάροχος υπηρεσιών μπορεί με εύκολο τρόπο να επεκτείνει την υπηρεσία του σε μεγάλες κλίμακες ώστε να αντιμετωπίσει την ταχεία αύξηση στις απαιτήσεις της υπηρεσίας (π.χ. flash-crowd effect) (Armbrust M et al 2009).
- Εύκολη πρόσβαση: Οι υπηρεσίες που φιλοξενούνται στο νέφος βασίζονται γενικά στο διαδίκτυο. Για το λόγο αυτό, είναι εύκολα προσβάσιμες μέσω μιας ποικιλίας συσκευών με πρόσβαση στο διαδίκτυο. Οι συσκευές αυτές περιλαμβάνουν τόσο τους Η/Υ, όσο και τα κινητά τηλέφωνα και τους Προσωπικούς Ψηφιακούς Οδηγούς (PDAs) (Zhang Q., Cheng L., Boutaba R. 2010).
- Μείωση του επιχειρηματικού κινδύνου και των εξόδων συντήρησης: Με την ανάθεση των υπηρεσιών υποδομής στο νέφος, ένας πάροχος υπηρεσιών μετατοπίζει τους επιχειρηματικούς κινδύνους (όπως τις βλάβες στον τεχνικό εξοπλισμό) στους πάροχους υποδομών, οι οποίοι συνήθως έχουν καλύτερη εξειδίκευση και είναι καλύτερα εξοπλισμένοι για την αντιμετώπιση των κινδύνων αυτών. Επιπλέον, ένας πάροχος υπηρεσιών δύναται να μειώσει τα έξοδα συντήρησης του τεχνικού εξοπλισμού και τα έξοδα εκπαίδευσης του προσωπικού (Zhang Q., Cheng L., Boutaba R. 2010).

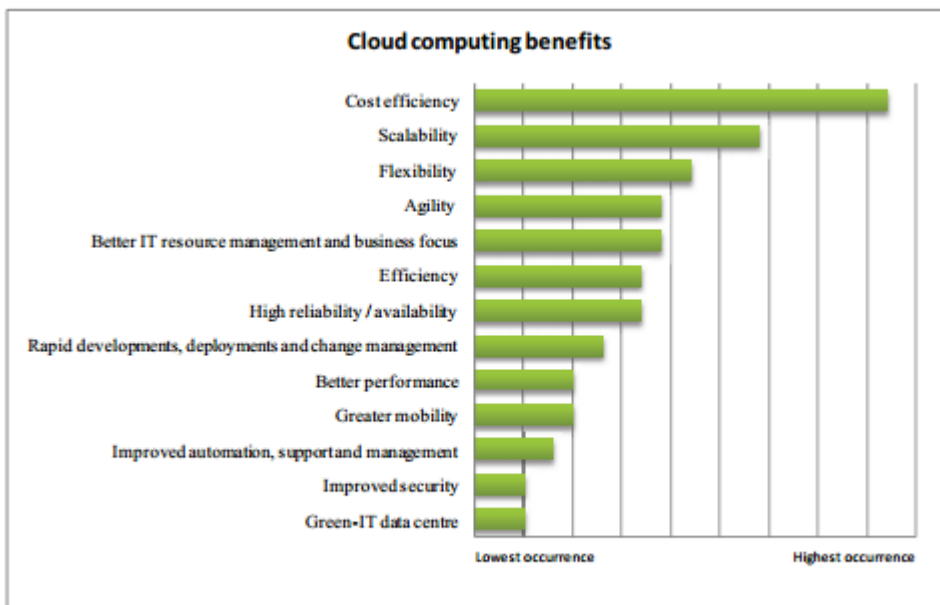


Figure 1. Cloud computing benefits.

Εικόνα 2: Πλεονεκτήματα υπολογιστικής νέφους (Carroll M., Van der Merwe A., Kotze P. 2011)

## 2. Μειονεκτήματα δικτύωσης νέφους

Τα μειονεκτήματα της δικτύωσης νέφους περιλαμβάνουν τους κινδύνους που ελλοχεύουν κατά την παροχή των διαφόρων υπηρεσιών. Οι κίνδυνοι αυτοί είναι ιδιαίτερα σημαντικοί όταν οι υπηρεσίες αυτές αφορούν τη λειτουργία ολόκληρων επιχειρήσεων ή κρατικών οργανισμών.

Στην αναφορά του, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST) (Badger L., Grance T., Patt-Corner R., Voas J. 2012), σημειώνει την ύπαρξη 23 “ανοιχτών ζητημάτων” τα οποία αφορούν την υπολογιστική νέφους στο σύνολό της. Τα ανοιχτά ζητήματα τα οποία θα πρέπει να απασχολούν τους χρήστες της τεχνολογίας αυτής, σχετίζονται με μειονεκτήματα πολλά από τα οποία δεν εμφανίζονται μόνο στο νέφος, αλλά αφορούν γενικότερα υπηρεσίες της τεχνολογίας πληροφοριών που δρουν ως ξενιστές (IT hosted services). Τα θέματα προς διευθέτηση κατατάσσονται σε πέντε κατηγορίες:

1. Υπολογιστική απόδοση (Computing performance): Ανάμεσα στα ζητήματα που αφορούν την υπολογιστική απόδοση, ο συγχρονισμός δεδομένων εκτός σύνδεσης είναι από τα πιο κρίσιμα. Στην περίπτωση που οι τελικοί χρήστες δεν διαθέτουν σύνδεση στο διαδίκτυο,

τα έγγραφα και τα δεδομένα δεν δύναται να συγχρονιστούν με τις εκδόσεις οι οποίες φιλοξενούνται στο νέφος. Αποτέλεσμα αυτού, είναι ο έλεγχος των εκδόσεων (versions) και η συνεργασία των μελών μιας ομάδας να γίνονται κρίσιμα ζητήματα.

2. Αξιοπιστία του νέφους (cloud reliability): Ανάμεσα στα άλλα, η εξάρτηση από τη σύνδεση στο διαδίκτυο για την ομαλή λειτουργία των εφαρμογών, κρίνεται ως το πιο κρίσιμο μειονέκτημα του νέφους. Το διαδίκτυο θα πρέπει να είναι μονίμως διαθέσιμο για τον χρήστη προκειμένου να έχει πρόσβαση στις υπηρεσίες του νέφους, αλλιώς δεν δύναται να παρασχεθούν οι υπηρεσίες του.
3. Οικονομικοί στόχοι (economic goals): Στην περίπτωση των δημοσίων συστημάτων νέφους οι χρήστες των υπηρεσιών εξαρτώνται από την παροχή σε πραγματικό χρόνο της υπηρεσίας. Στην περίπτωση που η εταιρία παροχής κλείσει, ο χρήστης βρίσκεται εκτεθειμένος, γεγονός που στην περίπτωση των επιχειρήσεων είναι ένα κρίσιμο οικονομικό ζήτημα. Τον κίνδυνο αυτό οι επιχειρήσεις τον μειώνουν μέσω των υβριδικών νεφών.
4. Συμμόρφωση (Compliance): Οι χρήστες δύναται να έχουν έλλειψη ορατότητας σχετικά με το πώς λειτουργεί το νέφος. Στην περίπτωση αυτή δεν θα είναι σε θέση να γνωρίζουν αν οι υπηρεσίες είναι εγγυημένες, διανέμονται με ασφαλή τρόπο και συμμορφώνονται με τις ισχύουσες κατά τόπους νομοθεσίες.
5. Ασφάλεια πληροφοριών: Η ασφάλεια της πληροφορίας αναφέρεται στην προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων και τη διασφάλιση της διαθεσιμότητας των δεδομένων. Όταν μια επιχείρηση γίνεται συνδρομητής σε μια υπηρεσία του νέφους, όλα τα δεδομένα που παράγονται βρίσκονται σε φυσική μορφή σε κτίρια τα οποία ανήκουν και λειτουργούν σύμφωνα με τον πάροχο. Το γεγονός αυτό προκαλεί ανησυχία, καθώς πολλά δεδομένα, ιδιαίτερα σε περιπτώσεις επιχειρήσεων και κρατικών οργανισμών θα πρέπει να είναι πλήρως διασφαλισμένα τόσο από ξένους εισβολείς, όσο και από λάθη τα οποία δύναται να συμβούν μέσω των μηχανισμών διαμοιρασμού (risk of isolation failure).

Σχετικά με το θέμα της ασφάλειας, η αναφορά του Κέντρου Στρατηγικών και Διεθνών Σπουδών (Center for Strategic and International Studies – CSIS) (Baker S., Waterman S., Ivanov G. 2010) η οποία βασίστηκε στις απαντήσεις 600 ειδικών σε θέματα ασφάλειας από επιχειρήσεις σε 14 χώρες, αναφέρει ότι το 60% των ερωτηθέντων είχαν βιώσει απόπειρες (επιθέσεις) κλοπής

υπηρεσίας (theft-of-service attacks), ενώ σχεδόν το 90% είχε μολυνθεί από ιούς και άλλα κακόβουλα λογισμικά. Όμως τα ποσοστά εξαπάτησης ξεπερνούσαν το 70% σε ένα μεγάλο εύρος και άλλων επιθέσεων, οι οποίες περιλαμβάνουν μικρής έκτασης επιθέσεις άρνησης υπηρεσιών (DDOS - Distributed denial-of-Service Attack) και βανδαλισμό, απειλές από άτομα εντός του οργανισμού ή υπαλλήλους, απώλεια ή διαρροή ευαίσθητων δεδομένων και ηλεκτρονικό ψάρεμα (phishing) και pharming (Greer M. 2010).

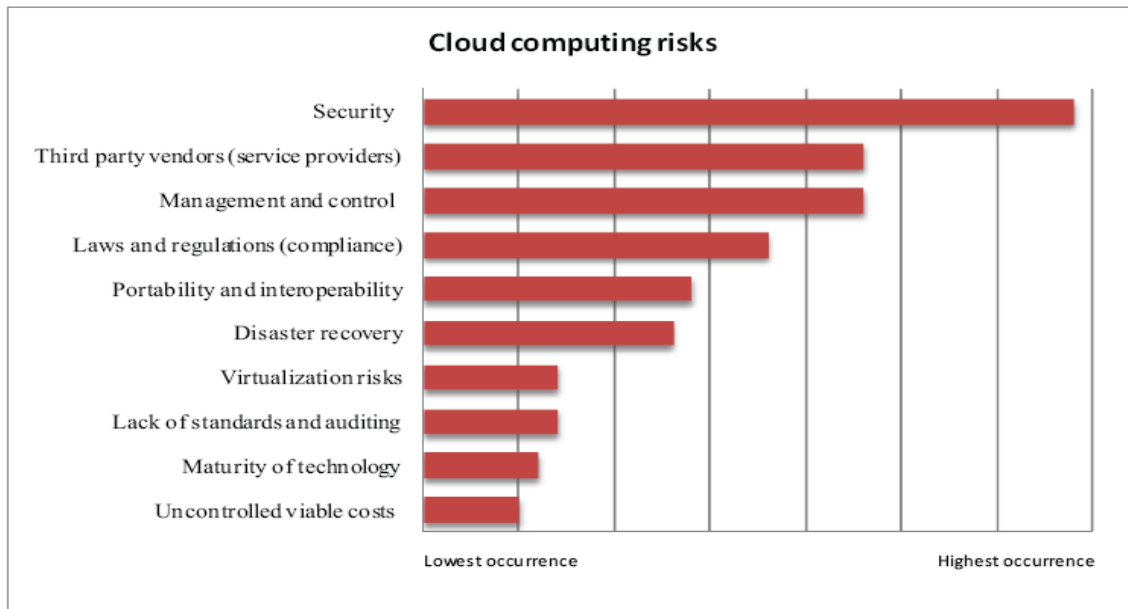


Figure 2. Cloud computing risks.

Εικόνα 3: Μειονεκτήματα - κίνδυνοι υπολογιστικής νέφους (Carroll M., Van der Merwe A., Kotze P. 2011)

### 3. Αξιοπιστία (reliability) στη δικτύωση νέφους

Ο τύπος και η ποιότητα των υπηρεσιών και των απαιτήσεων στην υπολογιστική νέφους, διατυπώνονται στις περισσότερες των περιπτώσεων στη βάση μιας συμφωνίας επιπέδου υπηρεσιών (Service Level Agreement - SLA), ανάμεσα στον πάροχο και τους πελάτες. Η συμφωνία αυτή προσδιορίζει τις απαιτήσεις του πελάτη και τη δέσμευση του πάροχου απέναντι σε αυτές (Carroll M., Van der Merwe A., Kotze P. 2011). Η αξιοπιστία και η ποιότητα των υπηρεσιών (Quality of Service – QoS) είναι δύο βασικά ζητήματα τα οποία συνομολογούνται

μέσω της συμφωνίας αυτής. Ο πάροχος υποχρεούται να εκτελεί τα αιτήματα υπηρεσίας (service requests) του πελάτη στο πλαίσιο της συμφωνημένης ποιότητας υπηρεσιών και αξιοπιστίας σε αντάλλαγμα ενός συγκεκριμένου ποσού χρημάτων (Faragardi H. R., Shojaee R., Tabani H. and Rajabi A. 2013).

Με τον όρο αξιοπιστία (reliability), αναφερόμαστε στην πιθανότητα ενός συστήματος να παρέχει υπηρεσία χωρίς σφάλματα (failure - free service) για μια δεδομένη περίοδο χρόνου μέσα στο πλαίσιο ενός συγκεκριμένου περιβάλλοντος (Badger L., Grance T., Patt - Corner R., Voas J. 2012). Στα δημόσια δίκτυα (public clouds), η αξιοπιστία προβάλλεται ως μια προκαθορισμένη παράμετρος της υπηρεσίας. Η Amazon σε δημοσίευσή της το 2008 ανέφερε ότι οι χρήστες των υπηρεσιών της μπορούν να αναμένουν 99,95% χρόνο λειτουργίας (uptime) σε όρους αξιοπιστίας, το οποίο αντιστοιχεί αναλογικά σε ένα σφάλμα ανά εβδομάδα (Limrungsi N., Zhao J., Xiang Y., Lan T., Huang H.H., Subramaniam S. 2012).

Στις μέρες μας, όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, εξακολουθούν να υπάρχουν μειονεκτήματα και κίνδυνοι οι οποίοι απειλούν την αξιοπιστία των υπηρεσιών του νέφους. Η εξάρτηση από τη συνδεσιμότητα στο διαδίκτυο και οι βλάβες κατά την παροχή στο νέφος (cloud provider outages), είναι δύο λόγοι που μειώνουν τον βαθμό αξιοπιστίας των υπηρεσιών αυτών.

### **Εξάρτηση από το Διαδίκτυο**

Ένα σημαντικό ζήτημα που σχετίζεται με την αξιοπιστία στη χρήση των υπηρεσιών νέφους αφορά την εξάρτησή τους από τη συνδεσιμότητα με το διαδίκτυο (network dependence). Το γεγονός ότι οι υπηρεσίες του νέφους είναι διαθέσιμες μόνο μέσω της σύνδεσης στο διαδίκτυο, έχει ως αποτέλεσμα την άμεση εξάρτηση από την ικανότητα και την ποιότητα της σύνδεσης σε αυτό. Αυτό σημαίνει ότι οι εφαρμογές του νέφους δύναται να μην είναι προσβάσιμες σε περίπτωση που οι δυνατότητες σύνδεσης στο διαδίκτυο είναι περιορισμένες και είναι ευάλωτες σε διασπάσεις του διαδικτύου (network disruptions) (Badger L., Grance T., Patt - Corner R., Voas J. 2012).



## **Βλάβες κατά την παροχή στο νέφος (cloud provider outages)**

Οι επιχειρησιακές εφαρμογές είναι πλέον μέσω του νέφους τόσο ουσιώδεις ώστε θα πρέπει να μπορούν να υποστηρίξουν τη λειτουργία της επιχείρησης αδιαλείπτως. Στην περίπτωση μιας αποτυχίας ή βλάβης, ο σχεδιασμός έκτακτης ανάγκης θα πρέπει να δραστηριοποιείται με ομαλό τρόπο, ενώ στην περίπτωση καταστροφικής βλάβης, σχέδια ανάκαμψης θα πρέπει να τίθενται σε εφαρμογή με την ελάχιστες δυνατές ελλείψεις. Κάθε όψη αξιοπιστίας θα πρέπει να σχεδιάζεται προσεκτικά και να δοκιμάζεται σε περιπτώσεις βλάβης. Για την επιχείρηση, η επίτευξη των επιθυμητών επιπέδων αξιοπιστίας απαιτεί την αύξηση του αντίστοιχου κόστους, ώστε να μειωθούν οι κίνδυνοι και το κόστος της αποτυχίας. Η τήρηση ενός αρχείου αξιοπιστίας αποτελεί ένα προαπαιτούμενο προσόν προς ευρεία υιοθέτηση (Mather T., Kumaraswamy S., Latif S. 2009).

Σύμφωνα με τους Dai Y. S., Yang B., Dongarra J., Zhang G. (2010), υπάρχει μια ποικιλία σφαλμάτων τα οποία δύναται να επηρεάσουν την επιτυχία / αξιοπιστία μιας υπηρεσίας νέφους. Στα σφάλματα αυτά περιλαμβάνονται τα εξής:

- 1) Υπερχείλιση (Overflow): η σειρά αναμονής αιτημάτων (request queue) στο δίκτυο θα πρέπει να έχει ένα όριο όσον αφορά το μέγιστο αριθμό των αιτήσεων σε αναμονή. Στην αντίθετη περίπτωση, οι νέες αιτήσεις θα πρέπει να αναμένουν πολύ ώρα, με αποτέλεσμα τη δημιουργία σφάλματος λήξης χρόνου (Timeout failure). Για το λόγο αυτό, εφόσον η ουρά είναι υπερπλήρης και υπάρχει αίτημα για καινούργια εργασία, το καινούργιο αίτημα αποβάλλεται και ο χρήστης αδυνατεί να εξυπηρετηθεί.
- 2) Λήξη χρόνου (Timeout): ο χρόνος προσπέλασης (due time) της υπηρεσίας νέφους συνήθως καθορίζεται από τον χρήστη ή το αντίστοιχο όργανο παρακολούθησης (service monitor). Στην περίπτωση που η αναμονή του αιτήματος στην ουρά είναι μεγαλύτερη του χρόνου αυτού, εμφανίζεται το σφάλμα της λήξης χρόνου. Αποτέλεσμα του σφάλματος αυτού είναι τα αιτήματα αυτά να απορριφθούν από την ουρά ώστε να μην επηρεάσουν τις ακολουθούμενες αιτήσεις.
- 3) Απώλεια δεδομένων (Data resource missing): σε ένα σύστημα διαχείρισης νέφους (Cloud Management System), ο διαχειριστής δεδομένων (Data resource manager - DRM) καταγράφει όλους τους πόρους των δεδομένων. Κατά τη διαδικασία αυτή είναι πιθανό κάποια δεδομένα που είχαν καταχωρηθεί παλαιότερα να έχουν διαγραφεί αλλά

να μην έχει ενημερωθεί ο διαχειριστής. Ως αποτέλεσμα του, στην περίπτωση που τα δεδομένα αυτά αναζητηθούν σε ένα συγκεκριμένο αίτημα εργασίας, να εμφανιστεί το εν λόγω σφάλμα.

- 4) Απώλεια υπολογιστικών πόρων (Computing resource missing): παρόμοια με το προηγούμενο σφάλμα, η απώλεια υπολογιστικών πόρων δύναται να εμφανιστεί στην περίπτωση της διακοπής λειτουργίας ενός Η/Υ χωρίς την ενημέρωση του συστήματος διαχείρισης νέφους.
- 5) Σφάλμα λογισμικού (Software failure): οι διεργασίες (subtasks) είναι λογισμικά προγράμματα τα οποία εκτελούνται σε διαφορετικούς υπολογιστικούς πόρους. Τα προγράμματα αυτά, ως λογισμικό υλικό, δύναται να εμφανίσουν σφάλματα κατά την εκτέλεσή τους (Dai Y.S., Xie M., Poh. K.L. 2006)
- 6) Σφάλμα βάσης δεδομένων (Database failure): η βάση δεδομένων που αποθηκεύει τους υπό αίτηση πόρους δεδομένων δύναται επίσης να εμφανίσει σφάλμα, με αποτέλεσμα κατά την εκτέλεση των διεργασιών να μην είναι δυνατή η πρόσβαση στα δεδομένα.
- 7) Σφάλμα τεχνικού εξοπλισμού (Hardware failure): οι υπολογιστικοί πόροι και οι πόροι δεδομένων περιέχονται στον τεχνικό εξοπλισμό ο οποίος επίσης δύναται να εμφανίσει βλάβη κατά τη λειτουργία του
- 8) Σφάλμα δικτύου (Network failure): τα κανάλια επικοινωνίας δύναται να είναι ατελή είτε κατά φυσική, είτε κατά λογική έννοια, προκαλώντας το σφάλμα δικτύου, ειδικά στις περιπτώσεις μετάδοσης μεγάλου όγκου δεδομένων (Dai Y.S., Xie M., Poh. K.L. 2002)

### **Δυσκολίες εξέτασης αξιοπιστίας**

Η ανάλυση της αξιοπιστίας ενός συστήματος νέφους συναντά δυσκολίες, λόγω της περιπλοκότητας του. Για το νέφος, η αξιοπιστία είναι κατά μια γενική έννοια, η αξιοπιστία τεσσάρων ξεχωριστών συνιστωσών:

- 1) Των φυσικών υποδομών (hardware) και των υποδομών λογισμικού (software) οι οποίες προσφέρονται από τον πάροχο
- 2) Του προσωπικού του πάροχου
- 3) Της σύνδεσης στις συνδρομητικές υπηρεσίες

- 4) Του προσωπικού της επιχείρησης – πελάτη της υπολογιστικής νέφους (Badger L., Grance T., Patt - Corner R., Voas J. 2012)

Χαρακτηριστικά της δικτύωσης νέφους, όπως αυτό του διαμοιρασμού σε μαζική κλίμακα, της ετερογένειας των φυσικών εξαρτημάτων και του λογισμικού, καθώς και της περίπλοκης αλληλεπίδρασης ανάμεσά τους, δεν επιτρέπουν σε μοντέλα τα οποία έχουν αναπτυχθεί για τα συμβατικά δίκτυα να εφαρμοσθούν στην εξέταση της αξιοπιστίας σε μια δικτύωση νέφους (Dai Y. S., Yang B., Dongarra J., Zhang G. 2010). Η εξέταση της αξιοπιστίας ενός συγκεκριμένου νέφους από τον πάροχο ή τον πελάτη αντιμετωπίζει εμπόδια κυρίως για δύο βασικούς λόγους. Πρώτον, ένα νέφος είναι η σύνθεση ποικίλων συστατικών μερών, το καθένα από τα οποία κληρονομεί ένα συγκεκριμένο βαθμό αξιοπιστίας κατά τη μέτρησή του ως ξεχωριστή μονάδα. Όταν τα συστατικά μέρη συνδυάζονται, η συνδυασμένη αξιοπιστία είναι δύσκολο να προβλεφθεί. Δεύτερον, η μέτρηση της αξιοπιστίας σχετίζεται με τη λειτουργία ενός περιβάλλοντος και η πλήρης κατανόηση του περιβάλλοντος στο οποίο λειτουργεί το νέφος δύναται να μην είναι εφικτή (Badger L., Grance T., Patt-Corner R., Voas J. 2012).

Σχετικά με την αντιμετώπιση του προβλήματος της αξιοπιστίας και του μετριασμού των κινδύνων του νέφους, έχουν προταθεί ποικίλες στρατηγικές (βλ. Atighetchi M., Pal P. (2009), Dai Y. S., Yang B., Dongarra J., Zhang G. (2010), Faragardi H. R., Shojaee R., Tabani H. and Rajabi A. (2013) και Carroll M., Van der Merwe A., Kotze P. (2011)). Σε μια κοινή προσέγγιση σε εσωτερικό επίπεδο (intra - site level) έχει προταθεί η προσθήκη εφεδρικής ισχύος σε διακομιστές/μνήμη για τη μεταστροφή της μετά-σφάλματος κατάστασης. Οι μέθοδοι αυτοί παρέχουν ταχεία ανάκαμψη, αλλά επειδή έχουν τοπική ισχύ δεν είναι κατάλληλες στις περιπτώσεις σφαλμάτων ευρείας κλίμακας, όπως στην περίπτωση φυσικών καταστροφών ή επιθέσεων από άλλα άτομα οι οποίες δύναται να οδηγήσουν σε πολλαπλές υποκείμενες βλάβες κόμβου / συνδέσεων (Gu F., Shaban K., Ghani N., Hayat M., Assi C. 2013).

#### **4. Ικανότητα επιβίωσης (survivability) στη δικτύωση νέφους**

Ως ικανότητα επιβίωσης, εννοούμε την ικανότητα που παρουσιάζει ένα δίκτυο για τη αδιάλειπτη παροχή υπηρεσιών στην περίπτωση εμφάνισης σφαλμάτων και βλαβών. Η ικανότητα επιβίωσης σχετίζεται τόσο με τον τρόπο σχεδίασης του δικτύου, όσο και με τη λειτουργικότητα αυτού (Kennington, J.L., Olinick, E.V., and Spiride, G. 2006). Από σχεδιαστικής άποψης, η ικανότητα επιβίωσης περιλαμβάνει διάφορα σχέδια προστασίας της διανομής της διαθέσιμης δυναμικότητας στο δίκτυο, τα οποία χρησιμοποιούνται στην περίπτωση της εμφάνισης κάποιου σφάλματος. Από την άποψη της λειτουργικότητας του δικτύου, τα σχέδια προστασίας εκτελούνται δια των μηχανισμών αποκατάστασης, οι οποίοι ενεργοποιούνται για την αποκατάσταση των σφαλμάτων (failures) οι οποίες προσβάλλουν τους τελικούς χρήστες (Luo B. and Liu W. 2011).

#### **Ο ρόλος των ιδεατών δικτύων στην ικανότητα επιβίωσης μιας δικτύωσης νέφους**

Από σχεδιαστικής άποψης, καθώς οι υπηρεσίες της υπολογιστικής νέφους εξαπλώνονται, η βιωσιμότητα των δικτύων αυτών δημιουργεί την ανάγκη της κατανομής των διάφορων λειτουργιών ανάμεσα σε πολλαπλά κέντρα δεδομένων τα οποία συνδέονται μεταξύ τους μέσω των βασικών δικτύων (Rimal B., et al 2009). Στην περίπτωση αυτή, η δημιουργία της ιδεατής δικτύωσης (network virtualization) είναι θεμελιώδης, καθώς με αυτόν τον τρόπο επιτρέπεται στους διαχειριστές των υπηρεσιών να φιλοξενούν τα πολλαπλά ιδεατά δίκτυα (virtual networks – VN) των χρηστών σε κοινά υποστρώματα νέφους (Sun G., et al 2012). Την ίδια στιγμή, πολλοί χρήστες υιοθετούν υπηρεσίες νέφους με στόχο την επέκταση εφαρμογών ανάμεσα σε διασυνδεδεμένα κέντρα δεδομένων. Τέτοιες περιπτώσεις απαιτούν τον διαμοιρασμό κοινών δεδομένων και απαιτούν και πάλι από τους διαχειριστές τη σχεδίαση εικονικών δικτύων.

Ένα από τα βασικά βήματα στη σχεδίαση των ιδεατών δικτύων είναι η χαρτογράφηση των απαιτήσεων στις φυσικές υποδομές. Κάθε κόμβος (node) ιδεατού δικτύου απαιτεί συγκεκριμένους πόρους υπολογιστικής ισχύος και μνήμης προκειμένου να τρέξουν οι εφαρμογές του πελάτη του δικτύου. Όμοια, κάθε άκρη (edge) του ιδεατού δικτύου απαιτεί συγκεκριμένα επίπεδα δυναμικότητας εύρους ζώνης (bandwidth) προκειμένου να υποστηρίξουν

την επικοινωνία ανάμεσα στους κόμβους. Επομένως, το ζήτημα της χαρτογράφησης των ιδεατών δικτύων απαιτεί διαχειριστές που να φροντίζουν τους υποκείμενους κόμβους, να συνδέουν τους πόρους και να χαρτογραφούν τους κόμβους των ιδεατών δικτύων σε φυσικά υποκείμενες θέσεις κέντρων δεδομένων και τις συνδέσεις των δικτύων σε υποκείμενες (underlying) συνδέσεις (Gu F., Shaban K., Ghani N., Hayat M., Assi C. 2013).

### **Κίνδυνοι επιβίωσης και ασφάλειας των πληροφοριών**

Από λειτουργικής άποψης, σύμφωνα με τον Greer M. B. (2010), στους κινδύνους επιβίωσης μιας δικτύωσης νέφους περιλαμβάνονται οι εξής:

- 1) Κίνδυνος ελέγχου (Risk Testing): δεν είναι εύκολο να προσδιοριστεί εάν ο πάροχος μιας υπηρεσίας νέφους μετριάζει τους βασικούς κινδύνους που διέπουν το νέφος, καθώς ο έλεγχος είναι δύσκολο να πραγματοποιηθεί από την πλευρά του πελάτη.
- 2) Κίνδυνος τοποθεσίας δεδομένων (Data Location Risk): αντίστοιχα είναι δύσκολο να προσδιοριστεί η ακριβής τοποθεσία όπου αποθηκεύονται τα δεδομένα. Στην Ε.Ε. έχουν νομοθετηθεί κανόνες προστασίας προσωπικών δεδομένων για τη χρήση μέσα στη χώρα των δεδομένων αυτών.
- 3) Κίνδυνος μεταφοράς δεδομένων και κωδικών (Data and Code Portability Risk): μετά την αποθήκευση των δεδομένων σε μια υπηρεσία νέφους, είναι δύσκολη η επιστροφή των δεδομένων αυτών.
- 4) Κίνδυνος απώλειας δεδομένων (Data Loss Risk): η απώλεια δεδομένων μπορεί να οφείλεται είτε στη διακοπή λειτουργίας στην πάροχο, είτε λόγω τεχνικών βλαβών
- 5) Κίνδυνος ασφάλειας προσωπικών δεδομένων (Data Security (privacy) risk): η αποθήκευση δεδομένων στο διαδίκτυο είναι πιο ευάλωτη στις επιθέσεις που γίνονται μέσω του διαδικτύου (cyber attacks)
- 6) Βιωσιμότητα πάροχου (Vendor Viability Risk): όντας επιχείρηση, ο πάροχος δύναται να απωλέσει την βιωσιμότητά του και αντίστοιχα την ιδιότητά του και να σταματήσει την παροχή υπηρεσιών νέφους.

## ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ

Με το πέρασμα των χρόνων, αναμένεται σημαντική επέκταση της χρήσης της υπολογιστικής νέφους ανά τον κόσμο. Οι προβλέψεις για την ανάπτυξη της αγοράς των υπηρεσιών νέφους κυμαίνονται μεταξύ των 46,3 δισεκατομμυρίων δολαρίων τα οποία σημειώθηκαν το 2008, σε \$148,8 δις το 2014 και \$222,5 δις το 2015. Τα έξοδα (spending) για την υπολογιστική νέφους προβλέπεται να αυξηθούν από \$16 δις το 2008 σε περίπου \$55 δις το 2014 (Carroll M., Van der Merwe A., Kotze P. 2011). Αυτές οι προβλέψεις ανάπτυξης βασίζονται στη συνειδητοποίηση των σημαντικών πλεονεκτημάτων που παρουσιάζει η υπολογιστική νέφους.

Παρόλα αυτά, οι κίνδυνοι που διατρέχουν την τεχνολογία αυτή είναι ακόμα αρκετοί και οφείλονται στην ευρύτητα που την χαρακτηρίζει και τους πολλούς παράγοντες που τη συνθέτουν. Οι έρευνες για τη διασφάλιση των χρηστών από τους επικείμενους κινδύνους της υπολογιστικής νέφους και την εξασφάλιση της αξιοπιστίας και της βιωσιμότητας των υπηρεσιών του εξελίσσονται παράλληλα με την επέκταση της χρήσης του διαδικτύου.

Ενδιαφέρον παρουσιάζουν οι έρευνες οι οποίες προσανατολίζονται στο συνδυασμό της βελτίωσης της βιωσιμότητας των υπηρεσιών του νέφους και της μείωσης της ενέργειας που καταναλώνεται παγκοσμίως στον τομέα της τεχνολογίας της πληροφορικής και των επικοινωνιών (Information and Communication Technology – ICT). Μέσω της λεγόμενης Πράσινης Υπολογιστικής (Green Computing) επανασχεδιάζονται τα δικτυακά πρωτόκολλα και οι αρχιτεκτονικές με σκοπό να τοποθετήσουν τις απαιτήσεις μείωσης της κατανάλωσης ενέργειας στο σχεδιασμό της μελλοντικής αρχιτεκτονικής των δικτύων, ώστε η μελλοντική δικτύωση νέφους να είναι αξιόπιστη, βιώσιμη και ενεργειακά αποδοτική (Luo B., Liu W. 2011).

## **ΒΙΒΛΙΟΓΡΑΦΙΑ:**

Armbrust M et al (2009): “*Above the clouds: a Berkeley view of cloud computing*” UC Berkeley Technical Report No. UCB/EECS-2009-28

<http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html>

Last access: 30/12/2013

Badger L., Grance T., Patt-Corner R., Voas J., National Institute of Standards and Technology – NIST (2012) “*Cloud Computing Synopsis and Recommendations – Recommendations of the National Institute of Standards and Technology, Special Publication 800-146*”. Gaithersburg. U.S. Department of Commerce

Baker S., Waterman S., Ivanov G. (2010) “*In the Crossfire: Critical Infrastructure in the Age of Cyber War*” Center for Strategic and International Studies (CSIS). Washington, DC. USA

Carroll M., Van der Merwe A., Kotze P. (2011): “*Secure cloud computing: Benefits, risks and controls*”, [Information Security South Africa \(ISSA\)](#), pp: 1 – 9, DOI: [10.1109/ISSA.2011.6027519](https://doi.org/10.1109/ISSA.2011.6027519)

CloudTimes.org (11/2011): “*Top PaaS, SaaS and IaaS Cloud companies by CloudTimes*” <http://cloudtimes.org/2011/11/30/top-paas-saas-and-iaas-cloud-companies-by-cloudtimes/>, Last access: 31/12/2013

Dai Y. S., Yang B., Dongarra J., Zhang G. (2010) “*Cloud Service Reliability: Modeling and Analysis*”. University of Tennessee. Knoxville, TN, USA

Dai Y.S., Xie M., Poh. K.L. (2002): “*Reliability Analysis of Grid Computing Systems*” The 9<sup>th</sup> IEEE Pacific Rim Symposium on Dependable Computing (PRDC2002), IEEE Computer Press, pp. 97-103

Dai Y.S., Xie M., Poh. K.L. (2006): “*Reliability of grid service systems*” *Computers & Industrial Engineering*, 50(1-2), 130-147

Faragardi H. R., Shojaee R., Tabani H. and Rajabi A. (2013) “[An analytical model to evaluate reliability of cloud computing systems in the presence of QoS requirements](#)” Computer and Information Science (ICIS) IEEE/ACIS 12<sup>th</sup> International Conference on, pp. 315 - 321, DOI: [10.1109/ICIS.2013.6607860](#)

Greer M. (2010) “*Survivability and Information Assurance in the Cloud*” International Conference on [Dependable Systems and Networks Workshops \(DSN-W\)](#), pp. 194-195, DOI: [10.1109/DSNW.2010.5542595](#)

Gu F., Alazemi H., Rayes A., Ghani N. (2013) “*Survivable Cloud Networking Services*” International Conference on Computing, Networking and Communications (ICNC), pp. 1016 – 1020, DOI: [10.1109/ICCNC.2013.6504230](#)

Gu F., Shaban K., Ghani N., Hayat M., Assi C. (2013) “*Regional Failure Survivability for Cloud Networking Services Using Post Fault Restoration*” 8th International Conference on [System of Systems Engineering \(SoSE\)](#), pp. 229 – 234, DOI: [10.1109/SYSoSE.2013.6575272](#)

J. Dale Prince (2011) “*Introduction to Cloud Computing*” Journal of Electronic Resources in Medical Libraries, 8:4, 449-458, DOI: [10.1080/15424065.2011.626360](#)

Kennington, J.L., Olinick, E.V., and Spiride, G. (2006) “*Basic mathematical programming models for capacity allocation in meshbased survivable networks*”, Int. J. Manage. Sci., pp.1-16.

Limrungsi N., Zhao J., Xiang Y., Lan T., Huang H.H., Subramaniam S. (2012): “*Providing reliability as an elastic service in cloud computing*” ICC (p./pp. 2912-2917), : IEEE. ISBN: 978-1-4577-2052-9



Luo B., Liu W. (2011): “*The Sustainability and Survivability Network Design for Next Generation Cloud Networking*” [\*\*Dependable, Autonomic and Secure Computing \(DASC\), 2011 IEEE Ninth International Conference on\*\*](#), pp. 555-560 DOI: [\*\*10.1109/DASC.2011.103\*\*](#)

Mather T., Kumaraswamy S., Latif S. (2009) “*Cloud Security and Privacy - An Enterprise Perspective on Risks and Compliance*” .Sebastopol. O’Reilly Media, Inc.

Mell P., Grance T., National Institute of Standards and Technology – NIST (2011) “*The NIST Definition of Cloud Computing – Recommendations of the National Institute of Standards and Technology, Special Publication 800-145*”. Gaithersburg. U.S. Department of Commerce

Metzler J., Metzler A. & Associates Distinguished Research Fellow and Co - Founder Webtorials Analyst Division (2012) “*The 2012 Cloud Networking Report*” <http://www.webtorials.com/content/2012/11/2012-cloud-networking-report.html> Last Accessed: 28-12-2013

Metzler J., Metzler A. & Associates Distinguished Research Fellow and Co - Founder Webtorials Analyst Division (2011) “*The 2011 Cloud Networking Report*” <http://www.webtorials.com/content/2011/11/2011-cloud-networking-report.html> Last Accessed: 28-12-2013

Moyer Christopher M. (2011) “*Building Applications in the Cloud - Concepts, Patterns and Projects*”. Boston. Pearson Education, Inc.

Onbile.com (8/3/2013): “Top 10 Software as a Service (SaaS) Companies” <http://www.onbile.com/info/top-10-software-as-a-service-saas-companies/>  
Last access: 31/12/2013

Rimal B., et al (2009) “*A Taxonomy and Survey of Cloud Computing Systems*” International Joint Conference on INC, IMS and IDC (NCM).Korea.

Shojaee R., Faragardi H. R., Alaei S. and Yazdani N. (2012) “A New Cat Swarm Optimization based Algorithm for Reliability-Oriented Task Allocation in Distributed Systems” 6<sup>th</sup> International Symposium on Telecommunication, pp. 861-866.

SMART 2020, Enabling the low carbon economy in the information age, <http://www.theclimategroup.org>, 2009.

Sun G., et al (2012) “Optimal Provisioning for Virtual Network Request in Cloud - based Data - centers” Photonic Network Communications, Vol. 24, No. 2, pp. 118-131.

Walker Bernhart M. (31/5/2012) “NIST: Cloud reliability, information security remain ‘open issues’”. FierceGovernmentIT. <http://fiercegovernmentit.com>, Last Accessed: 18/12/2013

Zhang Q., Cheng L., Boutaba R. (2010): “Cloud computing: state-of-the-art and research challenges” The Brazilian Computer Society, J Internet Serv Appl 1: 7–18 DOI: 10.1007/s13174-010-0007-6