ΚΑΠΑΚΟΠΟΥΛΟΥ ΠΑΡΑΣΚΕΥΗ

ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΠΑΡΑΛΛΗΛΟΥ ΥΠΟΛΟΓΙΣΜΟΥ ΒΑΣΙΣΜΕΝΕΣ ΣΕ ΥΠΟΛΟΓΙΣΤΙΚΑ ΠΛΕΓΜΑΤΑ ΚΑΙ Ο ΡΟΛΟΣ ΤΟΥΣ ΣΤΟ ΣΧΕΔΙΑΣΜΟ ΣΥΣΤΗΜΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ ΨΗΦΟΦΟΡΙΑΣ

Πτυχιακή Εργασία

Εισηγητής: *Ν. Βώρος*

ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΜΕΣΟΛΟΓΓΙΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ **ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗΝ ΔΙΟΙΚΗΣΗ ΚΑΙ ΣΤΗΝ ΟΙΚΟΝΟΜΙΑ**

ΝΟΕΜΒΡΙΟΣ 2006

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΕΧΟΜΕΝΑ 1
ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ 3
ΠΡΟΛΟΓΟΣ 4
1. ΕΙΣΑΓΩΓΗ 5
1.1 Τι είναι ικανό να κάνει το υπολογιστικό πλέγμα 7
1.1.1 Εκμετάλλευση αχρησιμοποίητων υπολογιστικών πόρων 7
1.1.2 Παράλληλη επεξεργαστική ισχύς 8
1.1.3 Ιδεατοί Οργανισμοί και πόροι (Virtual Organizations and Resources) 8
1.1.4 Πρόσβαση σε επιπλέον Πήγες και Πόρους 9
1.1.5 Ισορροπία πόρων 10
1.1.6 Αξιοπιστία (reliability) 11
1.1.7 Διαχείριση 12
1.2 Τα συστατικά και οι αρχές του grid 13
1.2.1 Τύποι υπολογιστικών πόρων 13
1.2.2 Εργασίες και Εφαρμογές 15
1.2.3 Δυναμικός Προγραμματισμός Πόρων 16
1.2.4 Intragrid σε Intergrid 17
1.3 Κατασκευάζοντας ένα grid 20
1.3.1 Σχέδιο ανάπτυξης 20
1.3.2 Συστατικά λογισμικού 21
1.4 Η ΧΡΗΣΗ ΤΟΥ grid: Από την σκοπιά του χρήστη 24
1.4.1 Εγγραφή του χρήστη και εγκατάσταση λογισμικού υπολογιστικού πλέγματος 24
1.4.2 Σύνδεση στο υπολογιστικό πλέγμα 25
1.4.3 «Δήλωση» Εργασιών 25
1.4.4 Παραμετροποίηση δεδομένων 27
1.4.5 Διαδικασίες επίβλεψης προόδου και ανάκαμψης εργασιών 27
1.5 Η ΧΡΗΣΗ ΤΟΥ GRID: Από την σκοπιά του διαχειριστή 28
1.5.1 Σχεδιασμός 28
1.5.2 Εγκατάσταση 28
1.5.3 Διαχείριση των «Μελών» του grid 28
1.5.4 Αρχή Πιστοποίησης 29
1.5.5 Διαχείριση Υπολογιστικών πόρων 30
1.6 Η ΧΡΗΣΗ ΤΟΥ GRID: Από την σκοπιά του σχεδιαστή πληροφοριακών συστημάτων 30
2. GLOBUS TOOLKIT 31
2.1 Τρεις Πυραμίδες 31
2.2 Συστατικά του Globus Toolkit 32
2.2.1 Υποδομή Ασφάλειας του Υπολογιστικού Πλέγματος (Grid Security Infrastructure, GSI) 33
2.2.2 Διαχειριστής Δέσμευσης Υπολογιστικών Πόρων (Grid Resource Allocation Manager, GRAM) 33

2.2.3 Υπηρεσία Επίβλεψης και Εύρεσης Υπολογιστικών Πόρων (Monitoring and Discovery Service, MDS) 34
2.2.4 GridFTP 37
2.3 Υλοποίηση Αρχιτεκτονικών Υπολογιστικού Πλέγματος (Globus Toolkit) 38
2.3.1 Στόχοι Σχεδιασμού Υπολογιστικού Πλέγματος 38
2.4 Μοντέλα Αρχιτεκτονικής Υπολογιστικών Πλέγματος 41
2.4.1 Computational grid 42
2.4.2 Data grid 43
2.5 Τοπολογίες Υπολογιστικού Πλέγματος 43
2.5.1 Intragrid 45
2.5.2 Extragrid 45
2.5.3 Intergrid 46
2.5.4 E-utilities 47
2.6 Προτεινόμενη Μεθοδολογία και Βήματα 48
2.6.1 Βασική Μεθοδολογία 48
2.6.2 Προτεινόμενα Βήματα 49
3. Συγκριτική Παρουσίαση Προϊόντων Υπολογιστικού Πλέγματος 51
3.1 Avaki 51
3.2 Data Synapse 54
3.3 Entropia 56
3.4 United Devices 58
3.5 Platform Computing 60
3.6 Τελική Αξιολόγηση Προϊόντων (Final Evaluation) 62
4. ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΨΗΦΟΦΟΡΙΑΣ – ΑΞΙΟΠΟΙΗΣΗ ΤΕΧΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΠΛΕΓΜΑΤΟΣ 64
4.1 Εισαγωγή 64
4.1.1 Απαιτήσεις Ασφάλειας και Πρακτικότητας 66
4.1.2 Επιθέσεις σε Συστήματα Ηλεκτρονικής Ψηφοφορίας 67
4.1.3 Προϋποθέσεις για τη Διεξαγωγή Εκλογών μέσω Internet 68
4.1.4 Κρυπτογραφικά Μοντέλα Ασφάλειας 70
4.1.5 Πλεονεκτήματα Συστημάτων Ηλεκτρονικής Ψηφοφορίας 73
4.2 Θέματα Ασφαλείας Συστημάτων Ηλεκτρονικής Ψηφοφορίας 73
4.3 Αξιοποίηση Υπηρεσιών Ασφαλείας Υπολογιστικού πλέγματος σε Συστήματα Ηλεκτρονικής Ψηφοφορίας 75
4.3.1 Κρυπτογραφία Δημοσίου Κλειδιού σε Συστήματα Ηλεκτρονικής Ψηφοφορίας 77
4.3.2 Η Βασική Αρχιτεκτονική του Κεντρικού Συστήματος Ψηφοφορίας 78
4.3.3 Μέτρα Αντιμετώπισης Ανάκαμψης Συστήματος Ηλεκτρονικής Ψηφοφορίας 80
ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΟΠΤΙΚΕΣ ΓΙΑ ΤΟ ΜΕΛΛΟΝ 83
ΒΙΒΛΙΟΓΡΑΦΙΑ - ΑΝΑΦΟΡΕΣ 85

ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ

Σχήμα 1.1.3: Ο ιδεατός κόσμος του grid 9
Σχήμα 1.1.5: Διαμοίραση εργασιών 11
Σχήμα 1.1.6: Εφεδρική διάταξη grid 12
Σχήμα 1.1.7: Καθορισμός πόρων 13
Σχήμα 1.2.2: Εργασίες και εφαρμογές 16
Σχήμα 1.2.4(α): Τοπολογίες grid 19
Σχήμα 1.2.4(β): Εφαρμογές του grid σε όλο τον κόσμο 19
Σχήμα 1.4.3: Δήλωση εργασιών 26
Σχήμα 2.1: Τρεις πυραμίδες 31
Σχήμα 2.2: Το σύστημα Globus Toolkit 32
Σχήμα 2.2.2: Αρχιτεκτονική GRAM 34
Σχήμα 2.2.3: Αρχιτεκτονική MDS 35
Σχήμα 2.2.3(β): Μοντέλο client-server LDAP 36
Σχήμα 2.2.4 (α): "Βασική" μεταφορά δεδομένων 37
Σχήμα 2.2.4 (β): "Τρίτης οντότητας" μεταφορά δεδομένων 38
Σχήμα 2.4.2: "Ομοσπονδιακή" βάση δεδομένων 43
Σχήμα 2.5: Intragrids, extragrids και intergrids 44
Σχήμα 2.5.1: Intragrid 45
Σχήμα 2.5.2: Extragrid 46
Σχήμα 2.5.3: Intergrid 47
Σχήμα 3.1(β): Συγκριτικός Πίνακας: NFS – Avaki Grid 52
Σχήμα 3.1(γ): Avaki Computational Grid 54
Σχήμα 3.3: Αρχιτεκτονική DcGrid 57
Σχήμα 3.4: Αρχιτεκτονική MP Grid 59
Σχήμα 3.5(α): Αρχιτεκτονική LSF 61
Σχήμα 3.5(β): Δυνατότητες LSF πλατφόρμας 61
Σχήμα 3.6: Συγκριτικός Πίνακας Προϊόντων 63
Σχήμα4.1.4(α):Ένα παράδειγμα ενός δικτύου MIX-net με τρεις κόμβους MIX 71
Σχήμα4.1.4(β):Ένα παράδειγμα ηλεκτρονικής ψηφοφορίας με «τυφλές» υπογραφές 72
Σχήμα 4.3: Δομή ενός Συστήματος Ηλεκτρονικής Ψηφοφορίας 76
Σχήμα 4.3.1: Κρυπτογραφία Δημοσίου Κλειδιού για Συστήματα Ηλεκτρονικής Ψηφοφορίας 78
Σχήμα 4.3.2(α):Αρχιτεκτονική της Βασικής Οντότητας Ηλεκτρονικής Ψηφοφορίας 79
Σχήμα 4.3.3: Διαδικασίες Αντιμετώπισης Επιθέσεων DOS 81

ΠΡΟΛΟΓΟΣ

Τα τελευταία χρόνια όλο και περισσότερες εταιρίες, οι οποίες στηρίζονται στην υπολογιστική δύναμη, τις δικτυακές εφαρμογές και την εξωγενή δραστηριότητα για να επιτύχουν τα επιχειρηματικά σχέδια τους, καταφεύγουν στη λύση του υπολογιστικού πλέγματος (grid computing). Το grid έρχεται να δώσει τη λύσεις εκμεταλλευόμενο υπολογιστικούς πόρους και επεξεργαστική ισχύς όχι μόνο του πληροφοριακού συστήματος της εταιρίας, άλλα και όλων των άλλων εταιριών που συμμετέχουν στο υπολογιστικό πλέγμα.

Το υπολογιστικό πλέγμα είναι μια φόρμα κατανεμημένων υπολογιστών που περιλαμβάνει το συντονισμό και τη διαμοίραση υπολογισμών, εφαρμογών, δεδομένων, αποθηκευτικών χώρων και διαδικτυακών πηγών μεταξύ γεωγραφικά διασκορπισμένων οργανισμών. Το grid είναι διαδεδομένο σε πολλές χώρες παγκοσμίως, άλλα όχι τόσο διαδεδομένο στην Ελλάδα, όπου τώρα έχει αρχίσει δειλά - δειλά να αναπτύσσεται.

Σκοπός της πτυχιακής εργασίας είναι η μελέτη του υπολογιστικού πλέγματος και πως αυτό μπορεί να εφαρμοστεί σε ένα σύστημα "Ηλεκτρονικής ψηφοφορίας" (e-voting). Πιο συγκεκριμένα, το 1° κεφάλαιο εμπεριέχει μια εισαγωγή γύρω από το θέμα όπως τον ορισμό του υπολογιστικού πλέγματος, τις ανάγκες που έρχεται να καλύψει και τη βασική αρχιτεκτονική του. Στο 2° κεφάλαιο αναλύεται το Globus Toolkit το οποίο αποτελεί μία από τις πιο διαδεδομένες εφαρμογές παγκοσμίως στην αρένα του υπολογιστικού πλέγματος. Στο 3° κεφάλαιο γίνεται συγκριτική παρουσίαση των προϊόντων του υπολογιστικού πλέγματος και τέλος στο 4° κεφάλαιο αναλύονται μέθοδοι βελτίωσης αρχιτεκτονικών συστημάτων ηλεκτρονικής ψηφοφορίας, αξιοποιώντας τεχνικές υπολογιστικού πλέγματος.

"Η συγγραφή της πτυχιακής δεν θα ήταν εφικτή χωρίς την καθοδήγηση του επιβλέποντα καθηγητή μου, Κ. Ν.Βώρου. Τον ευχαριστώ θερμά για το χρόνο που αφιέρωσε."

1. ΕΙΣΑΓΩΓΗ

Στις αρχές του '70 ξεκίνησαν οι πρώτες προσπάθειες εγκατάστασης δικτύων υπολογιστών. Οι προσπάθειες αυτές δημιούργησαν την ανάγκη για την αξιοποίηση αχρησιμοποίητης υπολογιστικής ισχύς. Τα πρώτα επιστημονικά πειράματα στον τομέα των κατανεμημένων υπολογιστών περιλαμβάνουν τις εφαρμογές «Creeper» και «Reaper» [1], οι οποίες «τρέχανε» στο ARPAnet [1].

Το 1973, το ερευνητικό κέντρο «Xerox Palo Alto»(PARC) [1] εγκατέστησε το πρώτο «Ethernet» δίκτυο. Οι επιστήμονες John F.Shoch και Jon A.Hupp δημιούργησαν ένα σκουλήκι-ιό, όπως το ονόμασαν. Με σκοπό την παρακολούθηση του δικτύου, ο ιός μετακινούταν από υπολογιστή σε υπολογιστή χρησιμοποιώντας τους αναξιοποίητους υπολογιστικούς πόρους. Πολλές προσπάθειες ακολούθησαν στις δεκαετίες του '80 και του '90 για την αξιοποίηση των υπολογιστικών πόρων μέσω της υποδομής των κατανεμημένων υπολογιστών. Η κατανεμημένη υπολογιστική επιστήμη αναβαθμίστηκε με τον ερχομό του διαδικτύου στις αρχές του '90, αξιοποιώντας την «δύναμη» του διαδικτύου το πρώτο επαναστατικό project στους κατανεμημένους υπολογιστές ήταν η κρυπτανάλυση συγκεκριμένων αλγορίθμων κρυπτογράφησης. Το όνομα του ήταν "distributed.net", το δεύτερο και συνάμα το πιο δημοφιλές project στην κατανεμημένη υπολογιστική επιστήμη ήταν το "SETI@home". Περισσότεροι από 2 εκατ. άνθρωποι εγκατέστησαν το λογισμικό "SETI@home" στον υπολογιστή τους.

Πλέον, το 2005 έχει ξεκινήσει να υλοποιείται από διάφορους ερευνητικούς χώρους (για παράδειγμα Globus) το υπολογιστικό πλέγμα (Grid Computing) [2]. Το grid στηρίζεται στην αρχιτεκτονική των κατανεμημένων υπολογιστών και στοχεύει στην διαμοίραση επεξεργαστικής ισχύς, αποθηκευτικού χώρου, αποτελεσμάτων-δεδομένων και άλλων υπολογιστικών πόρων. Η ιδέα ήταν η κατασκευή ενός ενιαίου χώρου, τουλάχιστον έτσι θα το βλέπουν οι χρήστες του grid, για την συσσώρευση και την εκμετάλλευση ετερογενών υπολογιστικών πόρων.

Εισαγωγή στο υπολογιστικό πλέγμα (Grid Computing)

Το υπολογιστικό πλέγμα (Grid Computing) είναι ένας από τους πιο πολυσυζητημένους όρους στην βιομηχανία της πληροφορικής τελευταία. Το υπολογιστικό πλέγμα είναι μια καινοτομία που πλησιάζει στο ότι η υπάρχων δραστηριότητα στην υποδομή του πληροφοριακού συστήματος βελτιστοποιεί τις υπολογιστικές πήγες και τη διαχείριση δεδομένων. Κατά τον Gartner, "το grid είναι μια συλλογή από πηγές που κατέχεται από πολλαπλές οργανώσεις που είναι συντονισμένες για να λύσουν ένα κοινό πρόβλημα" [2]. Ο Gartner δίνει ακόμα τρεις κοινά αναγνωρισμένους ορισμούς για το grid

- Υπολογιστικό πλέγμα(Grid computing) – πολλαπλοί υπολογιστές για να λύσουν ένα πρόβλημα εφαρμογής

- Πλέγμα δεδομένων (Grid data)-πολλαπλά αποθηκευτικά συστήματα για να φιλοξενήσουν ένα μεγάλο φορτίο δεδομένων
- Πλέγμα συνεργασίας (Grid collaboration) – πολλαπλή συνεργασία συστημάτων για συνεργασία σε ένα κοινό θέμα.

Το υπολογιστικό πλέγμα δεν είναι απλώς μια καινούργια σκέψη άλλα είναι κάτι που έχει κερδίσει πρόσφατα το ενδιαφέρον για τους δυο παρακάτω λόγους:

- Τα οικονομικά ποσά για την ανάπτυξη των Π.Σ έχουν περιορισθεί σημαντικά. Οι διοικήσεις των εταιριών ψάχνουν εναλλακτικές λύσεις
- Τα πιο γνωστά υπολογιστικά προβλήματα στο χώρο των επιχειρήσεων και των βιομηχανιών είναι η συσσώρευση μεγάλου όγκου δεδομένων για επεξεργασία καθώς και οι απαιτήσεις σε επεξεργαστική ισχύ.

Μέρος από το σύνολο των παγκόσμιων βιομηχανιών ενδιαφέρονται για τη χρήση του υπολογιστικού πλέγματος στους παρακάτω τομείς:

- Επιστήμες ζωής (ιατρική, βιολογία)
- Υπολογιστική κατασκευή
- Βιομηχανική κατασκευή
- Οικονομικές υπηρεσίες, και κυβέρνηση

Βασικά στοιχεία του grid

Το υπολογιστικό πλέγμα είναι μια φόρμα κατανεμημένων υπολογισμών που περιλαμβάνει το συντονισμό και τη διαμοίραση υπολογισμών, εφαρμογών, δεδομένων, αποθηκευτικών χώρων και διαδικτυακών πηγών μεταξύ γεωγραφικά διασκορπισμένων οργανισμών. Οι τεχνολογίες του grid υπόσχονται να αλλάξουν τον τρόπο με τον οποίο οι οργανισμοί θα αντιμετωπίσουν τα σύνθετα υπολογιστικά προβλήματα. Εν τούτοις, το όραμα μιας μεγάλης κλιμακωτής πηγής διαμοίρασης δεν είναι πραγματικότητα σε πολλές περιοχές – Το υπολογιστικό πλέγμα είναι μια εξελισσόμενη περιοχή υπολογισμών, όπου η προαπαιτούμενη τεχνολογία είναι ακόμα αναπτυσσόμενη και δεν μπορεί να καταστήσει εφικτό το νέο όραμα (τουλάχιστον ακόμη).

Γιατί είναι σημαντικό;

Χρόνος και χρήμα. Οι οργανισμοί που στηρίζονται στην υπολογιστική δύναμη για να προοδεύσουν τα επιχειρηματικά σχέδια τους αναγκάζονται να αποσύρουν καινούργια project και ιδέες. Τα projects απαιτούν πολλές φορές μεγάλη υπολογιστική ισχύ, ακόμα και όταν ο οργανισμός έχει επενδύσει στους υπολογιστικούς πόρους.

Επιπλέον, οι υπολογιστικοί πόροι και οι δυνατότητες του Π.Σ μιας εταιρίας επιφέρουν οικονομικά οφέλη. Παρόλα αυτά, οι επιχειρήσεις δυσκολεύονται να ισορροπήσουν τις ανάγκες για επιπλέον υπολογιστική ισχύ με τον έλεγχο του κόστους. Η αναβάθμιση και η αγορά λογισμικού και υλικού από τις εταιρίες δεν αποτελεί πάντα μια συμφέρουσα πρόταση λόγω της ραγδαίας ανάπτυξης της επιστήμης της πληροφορικής. Το grid έρχεται να δώσει λύση σε αυτό το πρόβλημα εκμεταλλευόμενο τους υπάρχοντες υπολογιστικούς πόρους.

1.1 Τι είναι ικανό να κάνει το υπολογιστικό πλέγμα

Κατά τη διαδικασία ανάπτυξης ενός Υπολογιστικού πλέγματος (Grid Computing) στόχος είναι η πλήρης ικανοποίηση του συνόλου των απαιτήσεων των πελατών. Με τον όρο πελάτες εννοούμε το σύνολο των εταιριών, οργανισμών και οποιασδήποτε άλλη οντότητας αιτείται τη χρήση του διαδικτύου για τη βελτίωση των υπηρεσιών που προσφέρει. Στο κεφάλαιο 1 γίνεται παρουσίαση των δυνατοτήτων ενός υπολογιστικού πλέγματος. Αυτό που μας ενδιαφέρει είναι αν οι δυνατότητες του Grid ανταποκρίνονται στον παραπάνω στόχο που έχουμε θέσει.

1.1.1 Εκμετάλλευση αχρησιμοποίητων υπολογιστικών πόρων

Η πιο απλή χρήση του Υπολογιστικού πλέγματος είναι να τρέχει μια υπάρχουσα εφαρμογή σε ένα άλλο μηχάνημα. Το μηχάνημα, στο οποίο η εφαρμογή τρέχει κανονικά, μπορεί να έχει υψηλό φόρτο εργασίας. Για αυτό το λόγο το μηχάνημα δεν μπορεί να ανταποκριθεί στις απαιτήσεις της εφαρμογής. Η λύση που προτείνεται από την αρχιτεκτονική του Υπολογιστικού Πλέγματος είναι να «τρέξει» η εφαρμογή σε έναν «ιδεατό» υπολογιστή μέσα στο Πλέγμα.

Για την υλοποίηση ενός τέτοιου σεναρίου απαιτούνται οι παρακάτω προϋποθέσεις:

- Η εφαρμογή θα πρέπει να είναι εκτελέσιμη από απόσταση και χωρίς αδικαιολόγητο κόστος.
- Το απομακρυσμένο μηχάνημα πρέπει να συναντά τις απαιτήσεις της εφαρμογής σε λογισμικό, υλικό και υπολογιστικούς πόρους.

Ένας από τους επιμέρους στόχους του υπολογιστικού πλέγματος είναι η βελτιστοποίηση της αρχιτεκτονικής του συστήματος, έτσι ώστε οι πόροι του grid να είναι πλήρως εκμεταλλεύσιμοι. Για παράδειγμα, όταν μία εργασία (batch job) πρέπει να εκτελεσθεί μέσα στο πλέγμα από έναν απομακρυσμένο υπολογιστή τότε αυτό που μας ενδιαφέρει είναι η πλήρης εκμετάλλευση του συνόλου του grid για την ελαχιστοποίηση των καθυστερήσεων (delays) μέσα στο δικτυακό πλέγμα.

Από έρευνες που έχουν πραγματοποιηθεί στους περισσότερους οργανισμούς-εταιρίες, υπάρχει μεγάλο πλήθος αναξιοποίητων υπολογιστικών πόρων ανά πληροφοριακό σύστημα ανά εταιρία. Για παράδειγμα σε πολλές εταιρίες η επιτραπέζιοι υπολογιστές (Desktop Computers) των πληροφοριακών συστημάτων τους αξιοποιούν την υπολογιστική ισχύ τους λιγότερο από πέντε λεπτά του συνολικού χρόνου που τρέχουν. Ακόμα και η εξυπηρετητές σε μερικές από τις εταιρίες δεν αξιοποιούν την υπολογιστική τους δύναμη ούτε στο μισό. Το Υπολογιστικό πλέγμα παρέχει ένα πλαίσιο εργασίας για την εκμετάλλευση όχι μόνο τις αναξιοποίητης υπολογιστικής ισχύς των Π.Σ, αλλά του συνόλου των αναξιοποίητων υπολογιστικών πόρων.

Η υπολογιστική ισχύς δεν είναι ο μοναδικός αναξιοποίητος πόρος ενός υπολογιστικού συστήματος. Ο αποθηκευτικός χώρος (Storage Capacity) είναι μια άλλη μορφή υπολογιστικού πόρου και το υπολογιστικό πλέγμα πρέπει να είναι σε θέση να τον εκμεταλλευτεί. Βάση των προαναφερθεισών ερευνών στις περισσότερες εταιρίες υπάρχει τεράστιος όγκος αχρησιμοποίητου αποθηκευτικού χώρου. Για

παράδειγμα, αν μια εργασία πρέπει να εκτελεστεί σε απομακρυσμένο υπολογιστή και η συγκεκριμένη εργασία απαιτεί μεγάλο όγκο δεδομένων τότε το Υπολογιστικό Πλέγμα μπορεί να αποδώσει καλύτερα ή ακόμα και τα μέγιστα με την προϋπόθεση ο όγκος των δεδομένων να είναι αποθηκευμένος σε στρατηγικά σημεία (Key Points) του δικτύου.

1.1.2 Παράλληλη επεξεργαστική ισχύς

Ίσως το πιο ενδιαφέρον χαρακτηριστικό σε ένα δίκτυο πλέγματος (grid network) είναι η δυνατότητα για παροχή μαζικής παράλληλης επεξεργαστικής ισχύς. Πολλές εταιρίες και οργανισμοί από τους τομείς της ιατρικής, της επεξεργασίας εικόνας, του οικονομικού σχεδιασμού και πολλών άλλων έχουν δηλώσει έντονο ενδιαφέρον για τη χρήση μαζικής επεξεργαστικής ισχύς.

Βέβαια για να αξιοποιήσει το πλέγμα τη μαζική παράλληλη επεξεργασία πρέπει οι αλγόριθμοι που θα χρησιμοποιηθούν ανά εφαρμογή να χωρίζονται σε ανεξάρτητα «μέρη» τα οποία θα τρέχουν σε διαφορετικά σημεία μέσα στο Grid. Μια Grid εφαρμογή θα μπορούσε να θεωρηθεί «έξυπνη», αποδοτική μόνο αν αποτελείτε από πολλές μικρές υπό-διαδικασίες που τρέχουν σε διαφορετικά «μέρη» του δικτύου. Μια τέλεια βαθμωτή εφαρμογή (scalable) θα τελείωνε 5 φορές γρηγορότερα την εργασία της αν χρησιμοποιούσε και τους 5 επεξεργαστές της [2].

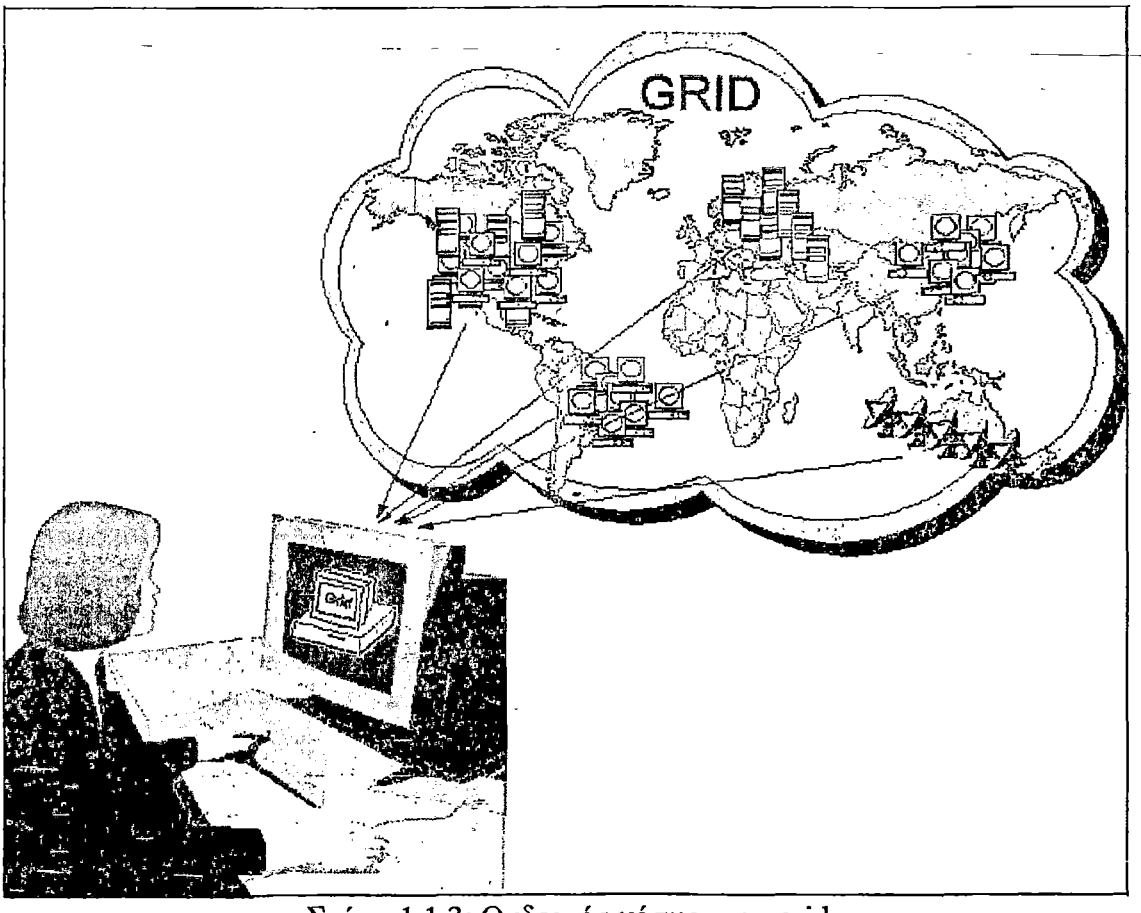
Συχνά συναντάμε εμπόδια ακόμα και σε μια τέλεια διαβάθμιση. Το πρώτο εμπόδιο που συναντάμε προέρχεται από την αδυναμία των αλγορίθμων να διαμοιράσουν την εφαρμογή στους υπόλοιπους επεξεργαστές. Αν ο αλγόριθμος μπορεί να διαμοιραστεί σε περιορισμένο αριθμό ανεξάρτητων επεξεργαστών τότε έχουμε το πρώτο εμπόδιο διαβάθμισης. Το δεύτερο εμπόδιο εμφανίζεται όταν οι επεξεργαστικές μονάδες δεν είναι πλήρως ανεξάρτητες, και ως αποτέλεσμα δημιουργείτε καθυστέρηση των οντοτήτων του δικτύου και γενικότερα περιορίζεται το επίπεδο τις διαβάθμισης της εφαρμογής. Για παράδειγμα, αν όλες οι υποδιεργασίες πρέπει να διαβάσουν ή να γράψουν δεδομένα από το ίδιο αρχείο ή βάση δεδομένων τότε οποιοσδήποτε περιορισμός πρόσβασης στο αρχείο ή στη βάση δεδομένων συνεπάγεται και περιορισμό στη διαβάθμιση της εφαρμογής. Άλλες πηγές προβλημάτων θα μπορούσαν να θεωρηθούν οι δυνατότητες του δικτύου, τα πρωτόκολλα συγχρονισμού (synchronization protocols) και γενικότερα οι καθυστερήσεις (latencies) που εμπλέκονται σε πραγματικού χρόνου απαιτήσεις [3].

1.1.3 Ιδεατοί Οργανισμοί και πόροι (Virtual Organizations and Resources)

Το υπολογιστικό πλέγμα συνεισφέρει στον τομέα των τηλεπικοινωνιών και των δικτύων απλοποιώντας τη διασύνδεση και τη συνεργασία ενός ευρύτερου κοινού. Στο παρελθόν, έχουν γίνει προσπάθειες στον τομέα των κατανεμημένων υπολογιστών και έχουν επιτευχθεί σημαντικά αποτελέσματα. Το υπολογιστικό πλέγμα, αξιοποιώντας τις προσπάθειες του παρελθόντος και εκμεταλλευόμενο τις σύγχρονες δυνατότητες του είναι σε θέση να στηρίξει ολόκληρα ετερογενή συστήματα με την τεχνική των ιδεατών οργανισμών και πόρων. Οι χρήστες του υπολογιστικού πλέγματος (π.χ. επιχειρήσεις διαδικτύου) κατανέμονται δυναμικά σε ιδεατούς οργανισμούς, ο κάθε ένας από αυτούς θέτει τη δικιά του πολιτική και τις δικές του

απαιτήσεις. Οι ιδεατοί οργανισμοί μπορούν να μοιράζουν τους πόρους τους συλλογικά σαν ένα «μεγάλο» υπολογιστικό πλέγμα.

Το πλέγμα δεδομένων είναι η πιο γνωστή εφαρμογή grid που χρησιμοποιεί την αρχιτεκτονική των ιδεατών οργανισμών. Τα αρχεία και οι βάσεις δεδομένων έχουν διπλότυπα τους σε διάφορα σημεία μέσα στο grid έτσι ώστε να επιτυγχάνεται η γρήγορη προσπέλασή τους από οποιοδήποτε ιδεατό οργανισμό. Η τεχνική διαμοίρασης δεν περιορίζεται μόνο σε αρχεία και βάσεις δεδομένων, αντιθέτως οι πόροι εμπεριέχουν λογισμικό, υπηρεσίες, άδειες κ.α. Οι πόροι μετατρέπονται σε «ιδεατή» μορφή για να επιτευχθεί η διαλειτουργικότητα μεταξύ περισσοτέρων συμμετεχόντων στο υπολογιστικό πλέγμα. Με τον όρο συμμετέχοντες εννοούμε τα μέλη διαφόρων πραγματικών ή ιδεατών οργανισμών. Η εικόνα 1.1.3 που ακολουθεί παρουσιάζει ένα χρήστη μέσα στον «ιδεατό» κόσμο του grid [4].



Σχήμα 1.1.3: Ο ιδεατός κόσμος του grid

1.1.4 Πρόσβαση σε επιπλέον Πήγες και Πόρους

Εκτός τις επεξεργαστικής ισχύς και των αποθηκευτικών δυνατοτήτων, το grid μπορεί να εξασφαλίσει πρόσβαση για να αυξηθούν οι ποσότητες των άλλων πόρων και των ειδικών εξοπλισμών, του λογισμικού και των υπόλοιπων υπηρεσιών. Οι επιπλέον πόροι μπορούν να εξασφαλίσουν επιπλέον χωρητικότητα. Για παράδειγμα, εάν ένας χρήστης χρειάζεται να αυξήσει την χωρητικότητα του στο διαδικτύου υλοποιεί μια μηχανή αναζήτησης δεδομένων(data mining search), η εργασία μπορεί να διαμοιραστεί μεταξύ των υπολογιστών του grid χωρίς να απαιτείται μεταξύ τους

σύνδεση. Σε αυτή την περίπτωση η ικανότητα αναζήτησης είναι πολλαπλή(multiplied), έτσι ο κάθε υπολογιστής έχει διαφορετική σύνδεση. Εάν οι υπολογιστές δεν είχαν διαφορετική σύνδεση και μοιράζονταν τη σύνδεση τότε θα υπήρχε πρόβλημα στο να αυξηθεί η χωρητικότητα.

Μερικοί υπολογιστές έχουν εγκατεστημένο ακριβό λογισμικό το οποίο ο χρήστης χρειάζεται. Η δουλειά του είναι να στέλνει σε αυτούς τους υπολογιστές περισσότερη εκμετάλλευση προς το λογισμικό. Άλλα μηχανήνατα στο grid έχουν κάποιες ιδιότητες. Όπως για παράδειγμα κάποιοι εκτυπωτές έχουν την ιδιότητα να έχουν καλύτερη ανάλυση χρωμάτων ή έχουν την ιδιότητα της γρήγορης εκτύπωσης.

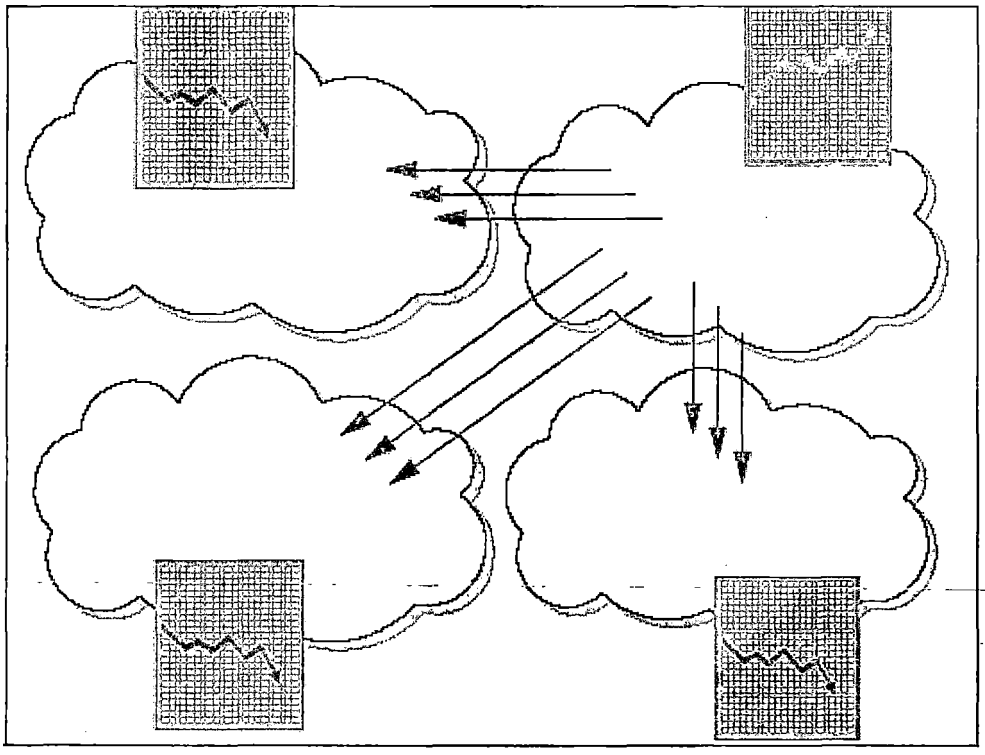
Ομοίως, το grid μπορεί να χρησιμοποιηθεί ώστε να κάνει χρήση ειδικού εξοπλισμού. Για παράδειγμα, ένας υπολογιστής μπορεί να έχει μεγάλη ταχύτητα και αυτόνομη τροφοδοσία. Ακόμα οι υπολογιστές μπορούν να είναι συνδεδεμένοι με ένα ηλεκτρονικό μικροσκόπιο το οποίο μπορούν να χειρίζονται εξ αποστάσεως. Σε αυτή την περίπτωση οι διαδικασίες προγραμματισμού είναι απαραίτητες. Το grid μπορεί να προσδώσει μια πιο εξειδικευμένη πρόσβαση, ενδεχομένως στην τηλεϊατρική με τις εξ αποστάσεως ιατρικές διαγνώσεις και στα ρομποτικά εργαλεία χειρουργείου.

1.1.5 Ισορροπία πόρων

Το grid έχει τη δυνατότητα να συνδέει ένα μεγάλο αριθμό πόρων, κυρίως υπολογιστών, που περιέχονται από ανεξάρτητους υπολογιστές και να τους μετατρέψει σε ένα συνολικά μεγάλο ιδεατό πόρο. Οι εφαρμογές μέσα στο grid έχουν την δυνατότητα να καθορίσουν ποια θα είναι τα μηχανήματα τα οποία θα εκτελέσουν μια εργασία του δικτύου. Η επιλογή αυτή γίνεται βάση του τρέχοντος υπολογιστικού φόρτου ανά μηχάνημα. Βέβαια, η τεχνική αυτή δεν θα μπορούσε να αποδώσει σε μια οποιαδήποτε αρχιτεκτονική δικτύου. Για παράδειγμα, ένας υπολογιστής στο δίκτυο που θεωρείται «ιδανικός» να τρέξει την εργασία μπορεί ξαφνικά να παρουσιάσει υψηλό φόρτο εργασίας. Ακόμη και αν το δίκτυο είναι πλήρες απασχολημένο πρέπει με κάποιον τρόπο να γίνει η ανάθεση της εργασίας και γενικότερα να καθοριστεί η προτεραιότητα ανά υπολογιστή και να εξασφαλιστεί ο κατάλληλος «χώρος» για την διεκπεραίωση της εργασίας. Οι παραπάνω αποφάσεις ονομάζονται «αποφάσεις ισορροπίας πόρων» (decision resource balancing) [4] και είναι δύσκολο να επιτευχθούν αν δεν ακολουθείται μια συγκεκριμένη υποδομή υπολογιστικού πλέγματος στο δίκτυο μας.

Σε πολλές επιχειρήσεις κρίνεται απαραίτητο η διεκπεραίωση ενός project να γίνει μέσα σε συγκεκριμένο χρονικό διάστημα (deadline). Όταν το χρονικό διάστημα είναι πολύ μικρό υπάρχει περίπτωση το πληροφοριακό σύστημα της εταιρίας να μην μπορεί να φέρει σε πέρας το project ακόμα και αν το ΠΣ βασίζεται πάνω σε μια αρχιτεκτονική grid. Παρόλα αυτά αν το μέγεθος του project είναι γνωστό, το project μπορεί να χωριστεί σε μικρές υποεργασίες και υπάρχουν αρκετοί πόροι στο grid τότε ένα δίκτυο με την υποδομή του grid μπορεί να δώσει λύσει το πρόβλημα.

Στο σχήμα 1.1.5 γίνεται η διαμοίραση των εργασιών βάση της τεχνικής «ισορροπίας πόρων».

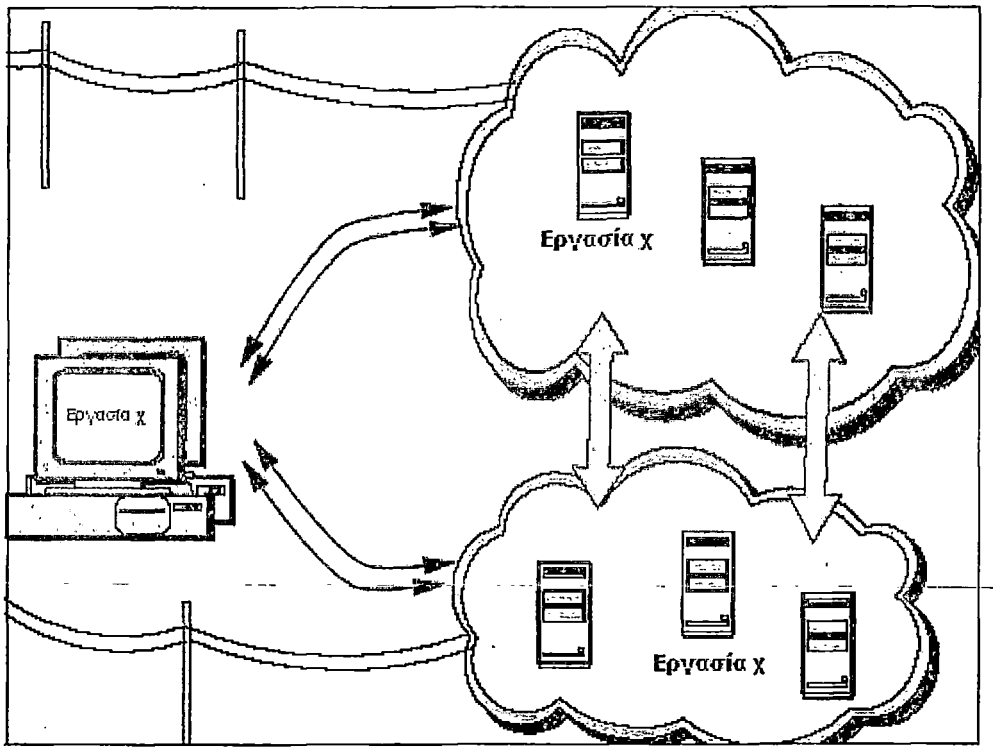


Σχήμα 1.1.5: Διαμοίραση εργασιών

1.1.6 Αξιοπιστία (reliability)

Τα προηγμένα υπολογιστικά συστήματα χρησιμοποιούν υλικό τελευταίας τεχνολογίας έτσι ώστε να πετύχουν υψηλή αξιοπιστία. Οι υπολογιστές του grid μπορούν να χρησιμοποιήσουν μέχρι και δύο όμοιους επεξεργαστές οι οποίοι έχουν πλήρη συμβατότητα μεταξύ τους. Σε περίπτωση που ένας από τους δύο τερματίσει αναπάντεχα ο δεύτερος θα πρέπει να ανταποκριθεί άμεσα και να υποστηρίξει τις λειτουργίες του υπολογιστή. Γενικότερα στο grid εφαρμόζεται το πλάνο αδιάκοπης λειτουργίας (continuity plan). Ένα τέτοιο πλάνο συνεχόμενης λειτουργίας εφαρμόζεται και στους επεξεργαστές. Οι παροχές ενέργειας και τα συστήματα ψύξης είναι σε συστοιχία των δύο. Τα συστήματα λειτουργούν με ειδικές ηλεκτρικές πηγές που βάζουν σε λειτουργία τη γεννήτρια αν το ρεύμα κοπεί. Όλα αυτά προσδίδουν ένα αξιόπιστο σύστημα, που είναι αρκετά δαπανηρό λόγω ότι τα συστήματα που αντιγράφουν έχουν υψηλής προστασίας συστατικά [5].

Στο μέλλον θα δούμε μία συμπληρωματική προσέγγιση στην αξιοπιστία που να βασίζεται στο υλικό και το λογισμικό. Το grid είναι απλός η αρχή αυτής της τεχνολογίας. Τα συστήματα που βρίσκονται στο grid μπορεί να είναι σχετικά φτηνά και διασκορπισμένα γεωγραφικά , έτσι εάν υπάρχει κάποιο είδος αποτυχίας σε κάποιο κομμάτι του grid τότε τα υπόλοιπα κομμάτια του grid δεν θα επηρεαστούν. Η διαχείριση του λογισμικού στο grid μπορεί κάλλιστα, με αυτόματες διαδικασίες να μεταφέρει εργασίες σε άλλες μηχανές στο grid όταν μία αποτυχία εντοπίζεται. Οι περιπτώσεις πραγματικού χρόνου, οι πολλαπλές αντιγραφές σημαντικών δουλειών μπορούν να τρέξουν σε διαφορετικές μηχανές οπουδήποτε στο grid. Τα αποτελέσματα τους μπορούν να ελεγχθούν για οποιαδήποτε είδος ανακολουθίας, όπως, αποτυχία, διαφθορά δεδομένων, ή παραποίηση. Στο σχήμα 1.1.6 διακρίνουμε την εφεδρική διάταξη του grid [4].



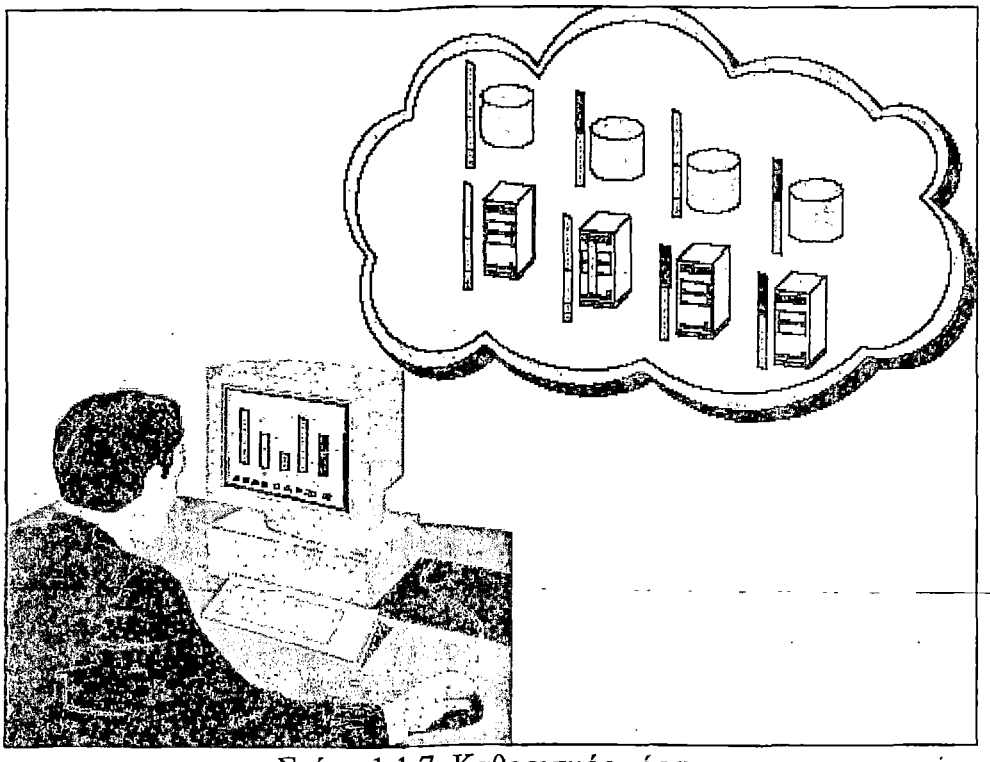
Σχήμα 1.1.6: Εφεδρική διάταξη grid

Αυτά τα συστήματα χρησιμοποιούν την τεχνολογική υποδομή "autonomic computing". Η τελευταία είναι ένα είδος λογισμικού το οποίο αυτόματα διορθώνει τα προβλήματα που προκύπτουν στο grid πιθανόν ακόμα και πριν ο χειριστής ή ο διαχειριστής είναι ενήμερος για αυτά.

1.1.7 Διαχείριση

Σκοπός είναι να μετατρέψουμε τους πόρους στο grid σε ιδεατή μορφή έτσι ώστε να αξιοποιήσουμε τα ετερογενή συστήματα και να εκμεταλλευτούμε καλύτερα την υποδομή των ΠΣ. Θα ήταν πιο αποδοτικό να απεικονίσουμε τη χωρητικότητα και τη χρησιμότητα διευκολύνοντας με αυτό τον τρόπο τα διαμερίσματα του ΠΣ να ελέγχουν τη δαπάνη για τους υπολογιστικούς πόρους σε μεγαλύτερους οργανισμούς.

Το grid είναι ικανό να διαχειρίζεται τις «προτεραιότητες» μεταξύ διαφορετικών έργων (projects). Στο παρελθόν, κάθε έργο απασχολούσε τους δικούς του υπολογιστικούς πόρους. Πολύ συχνά αυτοί οι πόροι ήταν αχρησιμοποίητοι και ταυτόχρονα κάποιο άλλο έργο είτε της ίδιας επιχείρησης είτε κάποιας άλλης χρειάζονταν περισσότερους υπολογιστικούς πόρους για να ολοκληρωθεί βραχυπρόθεσμα. Το grid παρέχει εκείνες τις υποδομές έτσι ώστε παρόμοιες συνθήκες να ελέγχονται και να διαχειρίζονται ευκολότερα. Στην εικόνα 1.1.7 βλέπουμε πως οι διαχειριστές έχουν τη δυνατότητα μέσω της υποδομής του grid να καθορίσουν πολιτικές για την καλύτερη διαχείριση και δέσμευση των υπολογιστικών πόρων [2,6].



Σχήμα 1.1.7: Καθορισμός πόρων

1.2 Τα συστατικά και οι αρχές του grid

Σε αυτή την παράγραφο θα γίνει αναλυτική παρουσίαση των όρων, των αρχών και των συστατικών που περιέχει το grid. Πιο συγκεκριμένα θα αναφερθούμε στους υπολογιστικούς πόρους, τις εφαρμογές, τις εργασίες που διέπουν το υπολογιστικό πλέγμα, τις τεχνικές προγραμματισμού, κράτησης και «καθαρισμού» (scheduling, reservation and scavenging) και τέλος τα είδη του grid [2,4,6].

1.2.1 Τύποι υπολογιστικών πόρων

Το grid όπως γνωρίζουμε είναι μια συλλογή από «υπολογιστικά μηχανήματα» και περιλαμβάνει «πόρους», «μέλη», «πελάτες», «εξυπηρετητές», «υπολογιστές» κ.α. Αμέσως τώρα ακολουθεί αναλυτική παρουσίαση των πόρων του grid.

Υπολογισμός: Ο πιο κοινός πόρος σε ένα υπολογιστικό πλέγμα είναι η υπολογιστική ικανότητα που παρέχεται από τους επεξεργαστές των μηχανημάτων. Βέβαια οι επεξεργαστές μέσα σε ένα grid ποικίλουν ανάλογα την ταχύτητα, την αρχιτεκτονική, την πλατφόρμα λογισμικού και βάση άλλων πολλών παραγόντων όπως η μνήμη, ο αποθηκευτικός χώρος και η συνδεσιμότητα. Υπάρχουν τρεις βασικοί τρόποι εκμετάλλευσης της υπολογιστικής ισχύς του grid. Ο πρώτος και συνάμα ο πιο απλώς είναι να «τρέξει» μια υπάρχουσα εφαρμογή σε ένα διαθέσιμο μηχάνημα του grid. Ο δεύτερος και περισσότερο πολύπλοκος από τον πρώτο είναι η εφαρμογή να είναι σχεδιασμένη με τέτοιο τρόπο ώστε να διαχωρίζεται σε πολλές υποδιεργασίες και οι τελευταίες να εκτελούνται παράλληλα σε διαφορετικούς επεξεργαστές. Ο τρίτος και τελευταίος τρόπος είναι να τρέξει η εφαρμογή πολλές φορές, σε πολλά διαφορετικά μηχανήματα του υπολογιστικού πλέγματος.

Η «διαβάθμιση» (scalability) είναι μια μεταβλητή με την οποία μετράμε την απόδοση των πολλαπλών επεξεργαστών μέσα στο grid. Για παράδειγμα, αν μια εφαρμογή χρειάζεται 100 sec για να παράγει το 100% του συνόλου των αποτελεσμάτων της με την χρήση ενός επεξεργαστή τότε θα είχαμε ιδανική διαβάθμιση (perfect scalability) αν με την χρήση ενός δεύτερου επεξεργαστή πετυχαίναμε η εφαρμογή να ολοκληρωθεί σε 50 sec (οι επεξεργαστές είναι ίδιου τύπου) [7].

Αποθηκευτικός χώρος: Ο δεύτερος σε σειρά πιο κοινός πόρος του grid είναι ο «αποθηκευτικός χώρος δεδομένων». Το υπολογιστικό πλέγμα που παρέχει μια «ενοποιημένη» όψη αποθηκευτικών δεδομένων ονομάζεται «Υπολογιστικό Πλέγμα Δεδομένων» (Data grid) [4]. Κάθε υπολογιστής του grid είναι σε θέση να παρέχει ένα κομμάτι αποθηκευτικού χώρου έστω και αν αυτό είναι προσωρινό. Ο αποθηκευτικός χώρος αυτός μπορεί να είναι είτε η μνήμη του επεξεργαστή είτε ένας δευτερεύον αποθηκευτικός χώρος όπως οι σκληροί δίσκοι. Στην πρώτη περίπτωση η μνήμη του επεξεργαστή έχει γρήγορη πρόσβαση αλλά περιορισμένη χωρητικότητα. Στη δεύτερη περίπτωση ο δευτερεύον αποθηκευτικός χώρος μπορεί να χρησιμοποιηθεί με διάφορους τρόπους όπως βελτίωση της απόδοσης του δικτύου, διαμοιρασμός των δεδομένων σε σύντομο χρονικό διάστημα μεταξύ των οντοτήτων του grid και διπλότυπες εγγραφές δεδομένων με στόχο την αξιοπιστία του δικτύου.

Ο αποθηκευτικός χώρος μπορεί να αυξηθεί χρησιμοποιώντας ένα κοινό αρχείο συστήματος, σκοπός είναι η ενοποίηση συστημάτων Βάσεων δεδομένων και ο περιορισμός του μεγέθους των αρχείων και των δεδομένων στο ιδανικό μέγεθος.

Τα πιο προοδευτικά συστήματα αρχείων δεδομένων μέσα στο grid μπορούν αυτόματα να αντιγράψουν μέρη δεδομένων και αρχείων, για να εξασφαλίσουν πλεονασμό για την αύξηση της αξιοπιστίας και της αποδοτικότητας. Ένας έξυπνος διαχειριστής του grid μπορεί να βοηθήσει στην επιλογή του κατάλληλου αποθηκευτικού χώρου για να κρατηθούν τα δεδομένα, βασιζόμενος σε ένα πρότυπο. Στην συνέχεια οι εργασίες μπορούν να είναι προγραμματισμένες πιο κοντά στα δεδομένα, κατά προτίμηση στις μηχανές που είναι συνδεδεμένες κατευθείαν στον αποθηκευτικό χώρο που κρατά τα απαιτούμενα δεδομένα.

Τα συστήματα αρχείων του grid μπορούν επίσης να υλοποιήσουν ένα σύστημα εντοπισμού δεδομένων έτσι ώστε αυτά να μπορούν να τα ανακαλούν με έναν αξιόπιστο τρόπο μετά από συγκεκριμένες αποτυχίες. Επιπλέον, κάποια συστήματα αρχείων υλοποιούν αναβαθμισμένους μηχανισμούς συγχρονισμού για τον περιορισμό τις «αντιδικίας» των χρηστών όταν οι τελευταίοι διαμοιράζουν και αναβαθμίζουν τα δεδομένα ταυτόχρονα [8,9].

Επικοινωνίες: Η άμεση επικοινωνία μεταξύ των υπολογιστικών μηχανών του δικτύου κάνει το υπολογιστικό πλέγμα πιο πρακτικό και αποδοτικό. Συνεπώς, δεν θα προκαλούσε έκπληξη αν μια ακόμα υπολογιστική πηγή για το grid είναι η χωρητικότητα του καναλιού επικοινωνιών. Αυτό περιλαμβάνει τις επικοινωνίες τόσο εντός του grid τόσο και με εξωτερικές οντότητες. Οι επικοινωνίες μεταξύ των οντοτήτων που ανήκουν στο grid πρέπει να χαρακτηρίζονται από ταχύτητα και αξιοπιστία. Μερικές εργασίες - projects απαιτούν μεγάλο όγκο δεδομένων και πολλές φορές η εργασία που τρέχει σε ένα μηχάνημα στο grid δεν μπορεί να προσπελάσει άμεσα τα αναγκαία δεδομένα. Επομένως, το εύρος ζώνης αποτελεί ένα κρίσιμο υπολογιστικό πόρο για την άμεση εκτέλεση των εργασιών στο grid. Αν το εύρος

ζώνης δεν αποδίδει στο μέγιστο τότε η απόδοση του υπολογιστικού πλέγματος πέφτει κατακόρυφα.

Η εξωτερική πρόσβαση στο διαδίκτυο, για παράδειγμα, μπορεί να είναι πολύτιμη όταν δημιουργείται μια μηχανή αναζήτησης. Οι μηχανές του grid μπορούν να έχουν επικοινωνία με το εξωτερικό διαδίκτυο και επιπλέον να έχουν σύνδεση μεταξύ των μηχανών του grid. Όταν αυτές οι συνδέσεις δεν μοιράζονται το ίδιο επικοινωνιακό κανάλι, τότε το συνολικό διαθέσιμο εύρος ζώνης επιβαρύνει το διαδίκτυο – δίκτυο. Το πλεόνασμα στα επικοινωνιακά κανάλια μερικές φορές χρειάζεται καλύτερη δυναμική διαχείριση στις αποτυχίες του δικτύου και την υπερβολική κίνηση δεδομένων. Σε πολλές περιπτώσεις, η μεγαλύτερη ταχύτητα του δικτύου πρέπει να εξασφαλιστεί για να συναντήσει τα αιτήματα των εργασιών που μεταφέρουν μεγαλύτερο όγκο δεδομένων. Το διαχειριστικό σύστημα του grid στοχεύει στην αποσυμφόρηση των καναλιών επικοινωνίας.

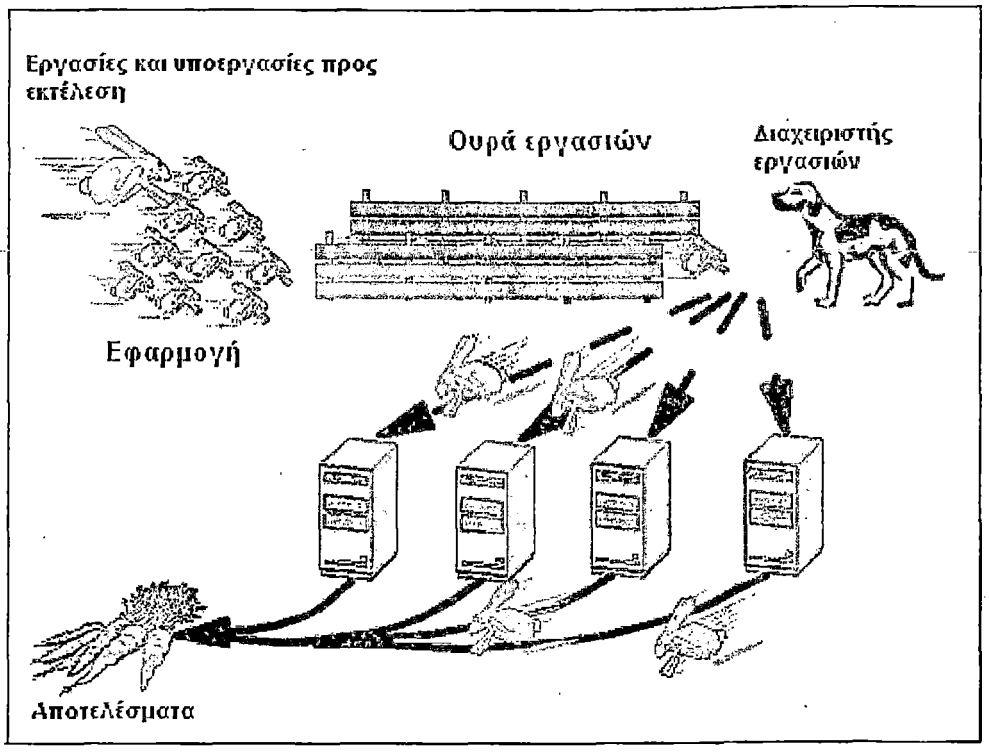
Λογισμικό και άδειες χρήσης: Το λογισμικό που απαιτείται για τη λειτουργία του grid μπορεί να είναι πολύ ακριβό για να εγκατασταθεί σε κάθε μηχάνημα του δικτύου, ευτυχώς το λογισμικό μπορεί να εγκατασταθεί μόνο σε ένα συγκεκριμένο υπολογιστή και οι «εργασίες» που απαιτούν το λογισμικό για την εκτέλεση τους στέλνονται σε εκείνο τον υπολογιστή. Οι επιχειρήσεις αγοράζουν άδειες χρήσης του λογισμικού και το κόστος μειώνεται σημαντικά. Το που θα δοθούν οι άδειες χρήσης, σε πόσα μηχανήματα θα εγκατασταθεί το λογισμικό καθώς και άλλες ενέργειες που αφορούν τη διαχείριση του λογισμικού και της άδειας χρήσης του κατά κόρον, καθορίζονται από την εταιρεία που παρέχει το λογισμικό [1].

Αρχιτεκτονικές, πολιτικές και ειδικός εξοπλισμός: Οι πλατφόρμες του grid από εταιρία σε εταιρία μπορούν να διαφέρουν στις αρχιτεκτονικές, στα λειτουργικά συστήματα, στις συσκευές και τον εξοπλισμό. Κάθε ένα από τα παραπάνω συστατικά αντιπροσωπεύει υπολογιστικούς πόρους του grid. Οι διαφορετικοί τύποι πόρων και οι διαφορετικές πλατφόρμες δημιουργούν προβλήματα συμβατότητας στο δίκτυο. Σε πολλές περιπτώσεις ο διαχειριστής του υπολογιστικού πλέγματος δημιουργεί έναν τεχνητό πόρο για την ανάθεση εργασιών βάση των κανόνων πολιτικής ή άλλων περιορισμών. Συγκεκριμένα, μια εργασία στο grid δεν μπορεί να προσπελάσει οποιοδήποτε υπολογιστικό πόρο, για παράδειγμα υπάρχουν πόροι στο grid οι οποίοι παρέχονται μόνο για project του στρατού. Αν μια εργασία η οποία είναι «άσχετη» με στρατιωτικά project, θελήσει να προσπελάσει ένα «στρατιωτικό πόρο» τότε θα απορριφθεί. Τα θέματα και οι πολιτικές ασφαλείας μπορούν να ακολουθούν διαφορετικούς κανόνες μέσα στο grid άλλα πρέπει να ακολουθούν κοινό σχεδιασμό.

1.2.2 Εργασίες και Εφαρμογές

Διαφορετικά είδη πόρων μέσα στο grid μπορούν να διαμοιραστούν και να χρησιμοποιηθούν, συνεπώς έχουν πρόσβαση δια μέσου της εκτέλεσης μιας εφαρμογής ή εργασίας. Χρησιμοποιούμε την έκφραση «εφαρμογή» σαν το υψηλότερο επίπεδο από ένα κομμάτι εργασίας του grid. Ωστόσο, μερικές φορές ο όρος «εργασία» χρησιμοποιείται ισοδύναμα. Οι εφαρμογές μπορούν να διαχωριστούν σε πολλές ξεχωριστές εργασίες, όπως θα φανεί και στην παρακάτω εικόνα. Στην συνέχεια αυτές οι εργασίες μπορούν να διαχωριστούν σε «υποεργασίες». Η βιομηχανία του grid χρησιμοποιεί άλλους όρους, όπως συναλλαγή (transaction), μονάδα εργασίας (work unit), ή υποταγή (submission).

Οι εργασίες – προγράμματα εκτελούνται σε συγκεκριμένες τοποθεσίες μέσα στο grid. Οι εργασίες είναι σε θέση να κάνουν υπολογισμούς, να εκτελούν μια ή περισσότερες εντολές του συστήματος, να μετακινούν ή να συλλέγουν δεδομένα, ή/και ακόμα και να διαχειρίζονται μηχανήματα από απόσταση. Μια εφαρμογή του grid, η οποία αποτελείται από μια συλλογή από εργασίες, συνήθως είναι με τέτοιον τρόπο σχεδιασμένη έτσι ώστε οι εργασίες να εκτελούνται παράλληλα σε διαφορετικές μηχανές του grid [6].



Σχήμα 1.2.2: Εργασίες και εφαρμογές

Οι εργασίες μπορούν να έχουν συγκεκριμένες απαιτήσεις οι οποίες να αποτρέπουν την εκτέλεση τους με παράλληλο τρόπο. Για παράδειγμα, οι εργασίες ίσως να απαιτούν συγκεκριμένα δεδομένα εισόδου και τα τελευταία θα πρέπει να αντιγράφουν στο μηχάνημα στο οποίο η εργασία τρέχει.

Επιπλέον, κάποιες εργασίες απαιτούν δεδομένα εξόδου που παράγονται από άλλες εργασίες. Τα δεδομένα εξόδου είναι προαπαιτούμενα έτσι ώστε οι πρώτες εργασίες να μπορούν να ολοκληρώσουν την εκτέλεση τους. Τέλος, οι εργασίες δημιουργούν επιπλέον «υποεργασίες», βασισμένες στα δεδομένα που επεξεργάζονται. Αυτή η λειτουργία παράγει ένα διάγραμμα ροής το οποίο είναι ιεραρχημένο από πάνω προς τα κάτω με «εργασίες» και «υποεργασίες».

1.2.3 Δυναμικός Προγραμματισμός Πόρων

Τα υπολογιστικά πλέγματα είναι υπεύθυνα για την αποστολή εργασιών σε συγκεκριμένα μηχανήματα για την εκτέλεση τους. Τα grid συστήματα στην απλή μορφή τους επιτρέπουν στο χρήστη να επιλέξει το μηχάνημα που είναι πιο κατάλληλο για την εκτέλεση της εργασίας του. Εν συνεχεία, ο χρήστης εκτελεί μια «εντολή» grid και στέλνει την εργασία προς εκτέλεση στο επιλεγόμενο μηχάνημα. Τα υπολογιστικά

πλέγματα ανώτερου επιπέδου εμπεριέχουν ένα πρόγραμμα που ονομάζεται «Διαχειριστής» (scheduler) [4,6]. Ο «Διαχειριστής» βρίσκει με αυτοματοποιημένες διαδικασίες το κατάλληλο μηχάνημα το οποίο είναι σε θέση να τρέξει οποιαδήποτε εργασία και αλληλεπιδρά με την τρέχουσα διαθεσιμότητα των υπολογιστικών πόρων μέσα στο grid. Σε αυτό το σημείο είναι σημαντικό να διαχωρίσουμε τον όρο «διαχείριση» με τον όρο «κράτηση». Η «κράτηση» πόρων στο υπολογιστικό πλέγμα βοηθάει στη βελτίωση της ποιότητας των υπηρεσιών, όμως δεν καθορίζει ποια εργασία θα τρέξει και σε ποιο μηχάνημα θα εκτελεστεί.

Άλλα συστήματα υπολογιστικού πλέγματος χρησιμοποιούν την πολιτική του «ρακοσυλλέκτη» (scavenging grid system) [10]. Όταν ένα μηχάνημα στο grid αποδεσμεύσει τους υπολογιστικούς πόρους του, τότε αναφέρει την τρέχουσα κατάσταση του στον κόμβο διαχείρισης. Ο κόμβος διαχείρισης θα αναθέσει εργασία στο μηχάνημα βάση των υπολογιστικών δυνατοτήτων του. Συνήθως η τεχνική του «ρακοσυλλέκτη» υλοποιείται με έναν αφανή τρόπο προς το χρήστη του μηχανήματος. Στην περίπτωση που το μηχάνημα απασχοληθεί με «τοπική-μη grid» εργασία, τότε η εργασία στο grid θα αναβληθεί και θα καθυστερήσει. Καταστάσεις σαν τις παραπάνω δημιουργούν μη προβλεπόμενους χρόνους ολοκλήρωσης των εργασιών του grid.

Για την επίτευξη προβλεπόμενων συμπεριφορών, τα μηχανήματα στο grid συχνά «αφοσιώνονται» πλήρως στο υπολογιστικό πλέγμα και δεν απασχολούνται με εξωτερικές εργασίες. Μια τέτοια προοπτική επιτρέπει στο διαχειριστή να καθορίσει τον ακριβή χρόνο ολοκλήρωσης των εργασιών. Επιπλέον, για τη βελτίωση της παραπάνω κατάστασης, οι υπολογιστικοί πόροι στο grid μπορούν να «διαφυλάσσονται» και να χρησιμοποιούνται για συγκεκριμένες εργασίες. Η τεχνική «κράτησης πόρων» απαιτείται έτσι ώστε οι εργασίες στο grid να ολοκληρώνονται μέσα σε συγκεκριμένο χρονικό διάστημα. Όταν η υποδομή του grid και οι πολιτικές επιτρέπουν έναν περίπλοκο συνδυασμό των τεχνικών της «διαχείρισης», «κράτησης» και του «ρακοσυλλέκτη» τότε επιτυγχάνονται μέθοδοι αξιοποιήσης των πόρων του grid [10].

1.2.4 Intragrid σε Intergrid

Το πραγματικό μέγεθος ενός υπολογιστικού πλέγματος δεν μπορεί να καθοριστεί. Ένα υπολογιστικό πλέγμα μπορεί να αποτελείται από ένα μονοψήφιο αριθμό μηχανημάτων μέχρι ενός συνόλου εταιριών – οργανισμών παγκοσμίως. Σε αυτή την παράγραφο ακολουθεί η περιγραφή παραδειγμάτων για την κλίμακα του μεγέθους των τοπολογιών ενός υπολογιστικού πλέγματος.

Ένα «μικρό» grid σύστημα αποτελείται από λίγα μηχανήματα, όλα χρησιμοποιούν κοινή αρχιτεκτονική υλικού και λειτουργικό σύστημα και είναι συνδεδεμένα σε ένα τοπικό δίκτυο. Σε ένα τέτοιο υπολογιστικό πλέγμα μπορούν να υπάρξουν πειραματισμοί μόνο σε επίπεδο λογισμικού. Συνήθως τα μηχανήματα είναι εγκατεστημένα σε ένα τομέα ενός οργανισμού και η χρήση τους δεν απαιτεί την υλοποίηση συγκεκριμένων πολιτικών ή θεμάτων ασφαλείας.

Η αμέσως επόμενη προσέγγιση εμπεριέχει ετερογενή υπολογιστικά συστήματα. Ένα τέτοιο υπολογιστικό πλέγμα σε σχέση με ένα ομογενές υπολογιστικό πλέγμα, πλεονεκτεί:

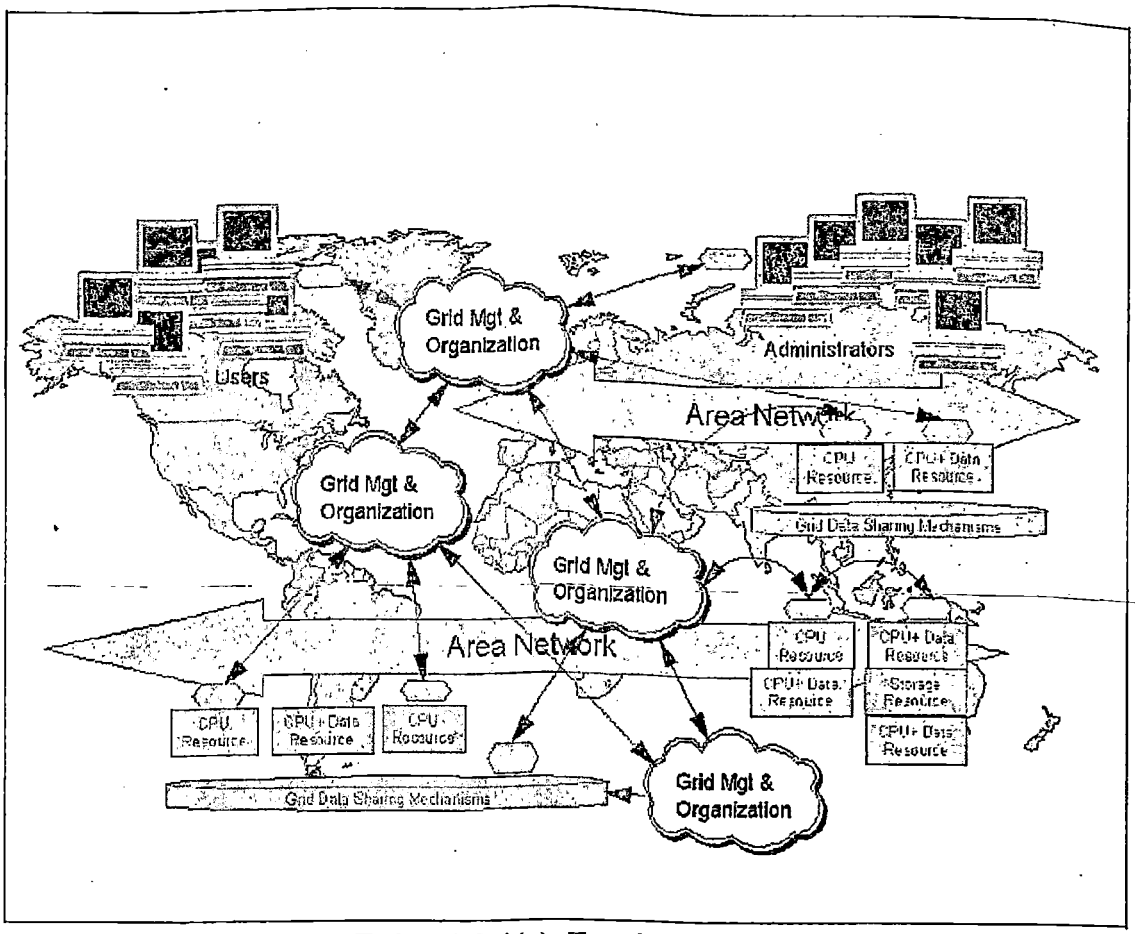
- Τύποι υπολογιστικών πόρων
- Οντότητες διαχείρισης
- Τεχνικές διαμοίρασης αρχείων
- Περισσότεροι υπολογιστικοί πόροι

Ένα ετερογενές υπολογιστικό πλέγμα, το οποίο ανήκει βέβαια στα πλαίσια του ίδιου οργανισμού, αναφέρεται με τον όρο «Intragrid» [2,10].

Βέβαια όσο το grid εξαπλώνεται, θέματα πολιτικών και θέματα ασφαλείας πρέπει να ληφθούν υπόψη. Για παράδειγμα, υπάρχουν πολιτικές για το ποια είδη εργασίας επιτρέπονται στο grid και σε ποια χρονική στιγμή αυτά θα εκτελεστούν. Ακόμα ίσως υπάρξουν προτεραιότητες κατά διαμέρισμα ή είδους εφαρμογής που θα μπορεί να έχει πρόσβαση στους πόρους του grid. Έτσι η ασφάλεια αποκτά μεγαλύτερη βαρύτητα όσο πιο πολύ οργανισμοί συμμετέχουν. Ευαίσθητα δεδομένα σε ένα διαμέρισμα του οργανισμού πρέπει να προστατεύονται ανάλογα με την οντότητα που προσπαθεί να τα προσπελάσει. Οι μηχανές του grid που είναι αφοσιωμένες σε αυτό συμβάλουν στη βελτίωση της ποιότητας των υπηρεσιών του υπολογιστικού πλέγματος και όχι τόσο να εξαρτώνται εξολοκλήρου από την τεχνική του «ρακοσυλλέκτη».

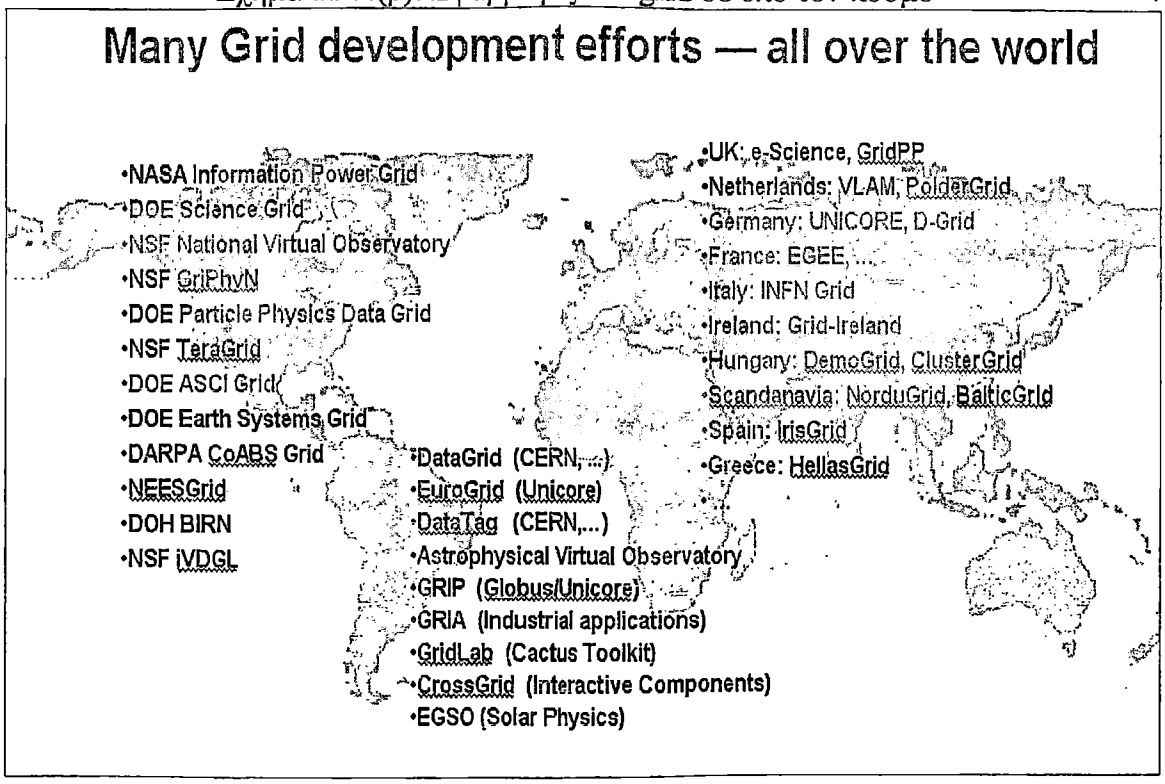
Το grid μπορεί να μεγαλώσει γεωγραφικά σε ένα οργανισμό που έχει εγκαταστάσεις σε διαφορετικές πόλεις υλοποιώντας συγκεκριμένες συνδέσεις μεταξύ των εγκαταστάσεων και του grid. Σε μερικές περιπτώσεις, τεχνολογίες δικτύου όπως «VPN Tunneling» [3] χρησιμοποιούνται πάνω από το διαδίκτυο για τη σύνδεση των διαφορετικών διαμερισμάτων του οργανισμού.

Στα σχήματα που ακολουθούν το grid ξεπερνάει τα όρια ενός οργανισμού και μπορεί να χρησιμοποιηθεί για την υλοποίηση projects κοινού ενδιαφέροντος, αυτό είναι γνωστό ως «Intergrid». Βέβαια απαιτείται υψηλό επίπεδο ασφάλειας για την αποτροπή επιθέσεων και παρακολουθήσεων [6,10].



Σχήμα 1.2.4(α): Τοπολογίες grid

Σχήμα 1.2.4(β): Εφαρμογές του grid σε όλο τον κόσμο



1.3 Κατασκευάζοντας ένα grid

Μερικοί προγραμματιστές εγκαθιστούν «αφηρημένα» δίκτυα με τοπολογία grid, άλλα όσο το grid εξαπλώνεται και οι χρήστες εξαρτώνται όλο και περισσότερο από αυτό για τις εργασίες τους, το σχέδιο για ένα πιο οργανωμένο grid γίνεται όλο και πιο απαραίτητο. Το καλύτερο θα ήταν να γίνουν κατανοητές οι απαιτήσεις των οργανισμών και οι τεχνολογίες του grid να επιλεχθούν βάση των απαιτήσεων αυτών. Στην παρακάτω ενότητα περιγράφονται οι βασικές σχεδιαστικές αρχές για τα συστατικά ενός υπολογιστικού πλέγματος και πως αυτά θα ανταποκρίνονται στις απαιτήσεις οργανισμών και χρηστών.

1.3.1 Σχέδιο ανάπτυξης

Η χρήση του grid, συχνά γεννιέται από την ανάγκη για αύξηση των υπολογιστικών πόρων. Ο πρώτος συλλογισμός που προκύπτει είναι η διαθεσιμότητα του υλικού και πως αυτό θα διασυνδεθεί μέσω τοπικού ή ευρύτερου δικτύου. Είναι σημαντικό να κατανοήσουμε τις εφαρμογές που θα χρησιμοποιηθούν στο υπολογιστικό πλέγμα. Τα χαρακτηριστικά τους μπορούν να επηρεάσουν τις αποφάσεις για το πώς θα επιλέξουν ή θα τροποποιήσουν καλύτερα το υλικό και τα δεδομένα σύνδεσης του.

Ασφάλεια: Η ασφάλεια είναι σημαντικός παράγοντας στη σχεδίαση και στην υποστήριξη ενός grid παρά στο συμβατικό κατανεμημένο υπολογισμό. Σε ένα grid, τα υπολογιστικά συστήματα είναι τροποποιημένα στο να εκτελούν προγράμματα από το να εκτελείται απλή μεταφορά δεδομένων. Αυτό δημιουργεί ένα μη ασφαλές grid και ενδεχομένως μια πιο εύφορη γη για ιούς και δούρειους ίππους. Για αυτό το λόγο, είναι σημαντικό να γίνουν κατανοητά ακριβώς ποια συστατικά του grid πρέπει να προστατευτούν αυστηρά έτσι ώστε να αποφευχθούν παραβάσεις. Επιπλέον, είναι σημαντικό να κατανοήσουμε θέματα που σχετίζονται με την αυθεντικοποίηση των χρηστών και με τη σωστή εκτέλεση των υπευθυνοτήτων μιας αρχής πιστοποίησης.

Οργανισμός: Τα θέματα των οργανισμών και των επιχειρήσεων είναι εξίσου κρίσιμα. Είναι σημαντικό να κατανοήσουμε πως τα διαμερίσματα ενός οργανισμού αλληλεπιδρούν, λειτουργούν και συνεισφέρουν στο σύνολο. Συχνά, δημιουργείται ένας ανταγωνισμός μεταξύ των τμημάτων ενός οργανισμού που αποβλέπει στην προστασία των υπολογιστικών πόρων του κάθε τμήματος με τελικό σκοπό την ολοκλήρωση των projects μέσα στο θεμιτό χρονικό διάστημα. Παρόλα αυτά, αν εξετάζαμε μια κατάσταση που επιτρέπεται η διαμοίραση των υπολογιστικών πόρων μέσα στον οργανισμό, θα παρατηρούσαμε ότι συνολικά ο οργανισμός θα επωφεληθεί.

Για παράδειγμα, ένα project το οποίο έχει μείνει πίσω χρονικά και έχει υπερβεί τον προϋπολογισμό του κατά πολύ, ίσως να μην καταφέρει να ανεχτεί τις πηγές που απαιτούνται έτσι ώστε να λύση το πρόβλημα. Το grid θα δώσει σε αυτά τα project ένα επιπλέον κίνητρο ασφαλείας, προσφέροντας ένα επιπλέον περιθώριο χωρητικότητας υπολογιστικών πόρων εωσότου υλοποιηθεί το project. Ομοίως, ένα project σε αρχικό στάδιο, όταν οι απαιτήσεις για υπολογιστικούς πόρους είναι χαμηλές, έχει τη δυνατότητα να αποδεσμεύσει πόρους και να τους διαθέσει σε άλλα projects με μεγαλύτερη πίεση χρόνου. Το grid επίσης προσφέρει τη δυνατότητα στις διοικήσεις των οργανισμών να έχουν άμεση άποψη για τις προτεραιότητες των projects. Με αυτό τον τρόπο αντιδρούν γρηγορότερα και αποτελεσματικότερα σχετικά με τη διαχείριση, την αξιοποίηση και την πολιτική των πόρων [11].

1.3.2 Συστατικά λογισμικού

Σε αυτή την παράγραφο παρουσιάζονται βασικά συστατικά που πρέπει να συζητηθούν προτού προχωρήσουμε στο σχεδιασμό της αρχιτεκτονικής του υπολογιστικού συστήματος.

Συστατικά διαχείρισης: Κάθε υπολογιστικό πλέγμα διαθέτει συστατικά διαχείρισης. Πρώτον, υπάρχει ένα συστατικό που κρατά πληροφορίες για τις διαθέσιμες πηγές στο grid και ποιοι χρήστες είναι μέλη του grid. Αυτή η πληροφορία χρησιμοποιείται αρχικά για να αποφασιστεί πως οι εργασίες στο grid θα κατανεμηθούν. Δεύτερον, υπάρχουν συστατικά μετρήσεων που καθορίζουν τόσο την χωρητικότητα των κόμβων-υπολογιστών όσο και τον τρέχον ρυθμό αξιοποίησης πόρων του grid.αυτή η πληροφορία χρησιμοποιείται για τον προγραμματισμό των εργασιών του grid. Επίσης, χρησιμοποιείται για να καθορίσει την «υγεία» του grid, ενημερώνοντας με αυτό τον τρόπο το προσωπικό των οργανισμών για πιθανή βλάβη ή υπερφόρτωση του υπολογιστικού συστήματος. Επιπλέον αξιοποιείται για την μελέτη στατιστικών αποτελεσμάτων όπως για παράδειγμα, η συνολική χρήση των υπολογιστικών πόρων ημερησίως. Τρίτον, το εξειδικευμένο λογισμικό διαχείρισης grid μπορεί αυτόματα να διαχειριστεί πολλές όψης του grid. Αυτό είναι γνωστό ως αυτόνομο υπολογιστικό σύστημα (autonomic computing). Το λογισμικό αυτό διαθέτει διαδικασίες «ανάρρωσης» από ιούς και άλλες τεχνικές αστοχίες, βρίσκοντας εναλλακτικούς τρόπους για να συνεχιστεί η ροή εργασίας (Continuous Planning).

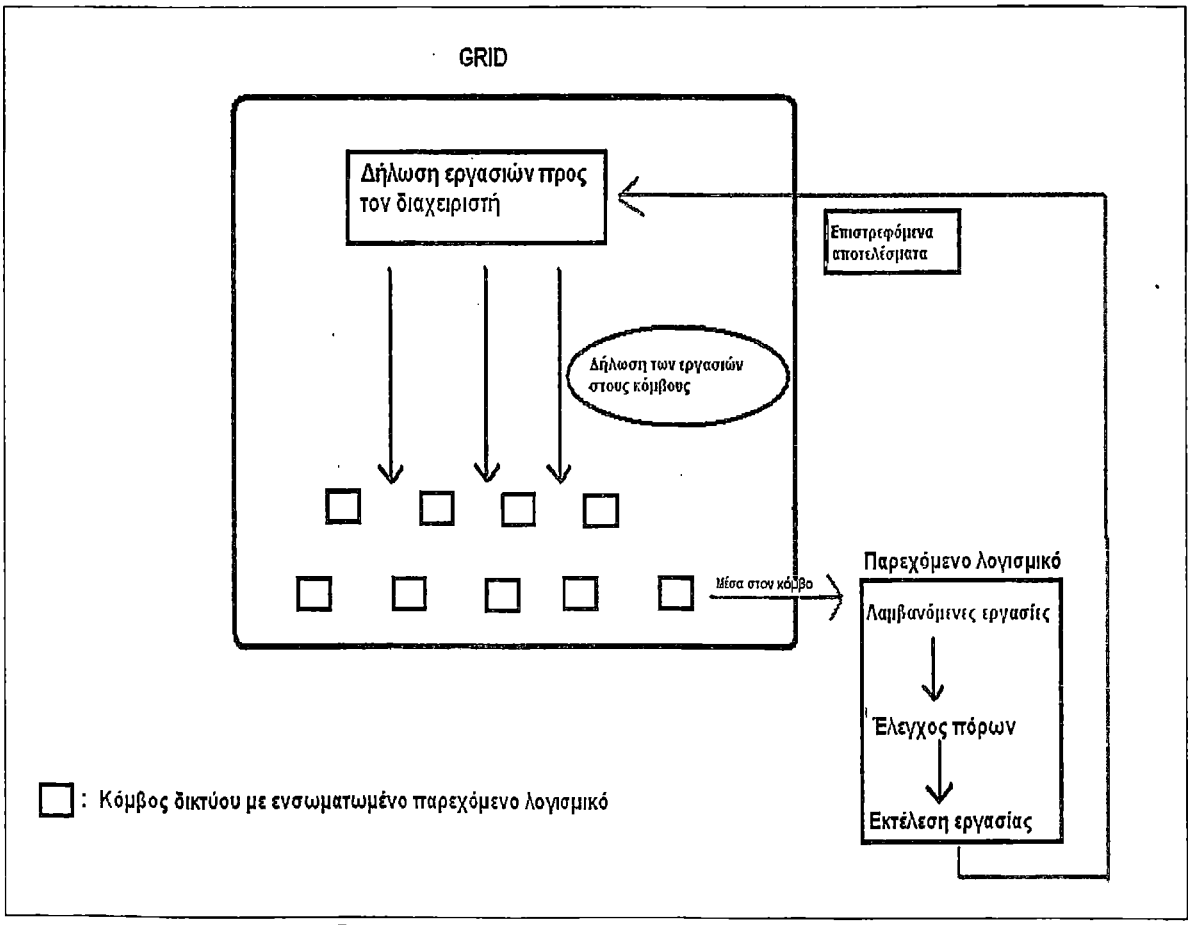
Λογισμικό παροχής πόρων: Κάθε υπολογιστής συνεισφέρει υπολογιστικούς πόρους στα πλαίσια ενός δικτύου grid. Αυτό αποτελεί απαραίτητη διαδικασία του grid. Συνήθως απαιτείται διαδικασία ταυτοποίησης και αυθεντικοποίησης πριν ένας υπολογιστής συνδεθεί στο grid. Ένα πιστοποιητικό αυθεντικότητας μπορεί να επαληθεύει την ταυτότητα του υπολογιστή που συνεισφέρει πόρους, όπως επίσης τους χρήστες και το ίδιο το υπολογιστικό πλέγμα [12].

Αρκετά πληροφοριακά συστήματα στηρίζονται σε βελτιωμένες διαδικασίες αυθεντικοποίησης, την ίδια ώρα που κάποια άλλα συστήματα εξαρτώνται από διαδικασίες αυθεντικοποίησης σε επίπεδο λειτουργικών συστημάτων. Στην τελευταία περίπτωση, ένα σύστημα εύρεσης χρηστών ίσως χρειαστεί να ελέγξει τα δικαιώματα του χρήστη σε διαφορετικούς υπολογιστές. Αυτό τυπικά συντηρείται χειροκίνητα από το διαχειριστή του grid. Ο τελευταίος καθορίζει ποιος κωδικός χρήστη θα χρησιμοποιηθεί και από ποια μηχανή, στη συνέχεια εισάγει αυτόν τον κωδικό χρήστη σε μια προστατευμένη βάση δεδομένων ή εγγραφή. Με αυτόν τον τρόπο, όταν οι εργασίες του grid έχουν διανεμηθεί σε διαφορετικές μηχανές για κάθε χρήστη, το αντίστοιχο τοπικό μηχάνημα καθορίζει και τα δικαιώματα των χρηστών.

Σε μερικά συστήματα στο grid δεν είναι δυνατό να συμμετέχουν χρήστες στο υπολογιστικό σύστημα χωρίς να χρειάζονται να αυθεντικοποιηθούν. Και σε κάποια άλλα είναι δυνατό για οποιοδήποτε χρήστη να υποβάλλει εργασίες στο grid χωρίς να απαιτούνται διαδικασίες εξουσιοδότησης. Τέτοιου είδους συστήματα παραμετροποιούνται πιο εύκολα, άλλα θα πρέπει να αποφεύγονται στην περίπτωση μεγάλης κλίμακας υλοποιήσεων λόγω των σοβαρών προβλημάτων ασφάλειας.

Ένα σύστημα grid δημιουργεί πληροφορίες σχετικά με τους πρόσφατα προστιθέμενους πόρους που είναι διαθέσιμοι στο grid. Το μηχάνημα – παροχέας πόρων στο grid συνήθως έχει μια οθόνη επίβλεψης ποσοτήτων ή ποιοτικών μεταβλητών. Τέτοιες μεταβλητές είναι ο τρέχον ρυθμός απασχόλησης των μηχανημάτων και το μέγεθος των πόρων που εκμεταλλεύονται την τρέχουσα στιγμή. Η πληροφορίες που κρατούνται από την οθόνη επίβλεψης αξιοποιούνται από το λογισμικό διαχείρισης του υπολογιστικού πλέγματος [10].

Ο χρήστης στο δίκτυο «δηλώνει» μια εργασία προς εκτέλεση στο υπολογιστικό πλέγμα. Το λογισμικό διαχείρισης επικοινωνεί με το λογισμικό παροχής πόρων για να σταλεί η εργασία στο τελευταίο. Το λογισμικό παροχής πόρων πρέπει να είναι έτοιμο να λάβει το εκτελέσιμο αρχείο ή να επιλέξει το κατάλληλο αντίγραφο που είναι προεγκατεστημένο στο μηχάνημα παροχής πόρων. Το λογισμικό εκτελείται και το αποτέλεσμα αυτού στέλνεται πίσω στον αιτούντα. Πιο εξειδικευμένες υλοποιήσεις μπορούν δυναμικά να καθορίσουν τη προτεραιότητα της τρέχουσας εργασίας, να την αναβάλλουν προσωρινά, να τη συνεχίσουν αργότερα ή/και να συνεχιστεί η εκτέλεση της σε διαφορετικό μηχάνημα. Τέτοιου είδους ενέργειες είναι απαραίτητες για θέματα προτεραιοτήτων, ισορροπιών και πολιτικών στο grid.



Σχήμα 1.3.2: Λογισμικό παροχής πόρων

Λογισμικό δέσμευσης εργασιών: Συνήθως οποιοδήποτε μηχάνημα μέσα στο grid μπορεί να «δηλώσει» μια εργασία προς εκτέλεση και να αρχικοποιήσει μια ουρά εργασιών. Όμως, στα περισσότερα υπολογιστικά πλέγματα η λειτουργία αυτή υλοποιείται ως ένα ξεχωριστό συστατικό-μέρος και εγκαθιστάτε στα ονομαζόμενα "submission nodes" ή "submission clients". Όταν ένα grid έχει υλοποιηθεί χρησιμοποιώντας την τεχνική των προκαθορισμένων πόρων παρά την τεχνική της εξεύρεσης πόρων, τότε το λογισμικό δέσμευσης πόρων εγκαθίσταται στον επιτραπέζιο υπολογιστή του χρήστη ή στο σταθμό εργασίας του.

Κατανεμημένη διαχείριση στο grid: Τα μεγάλα σε μέγεθος grid έχουν ιεραρχικό ή άλλο τύπο οργανωτικής τοπολογίας συνήθως ενοποιώντας ετερογενείς τεχνολογικά πλατφόρμες. Οι μηχανές συνδέονται μεταξύ τους τοπικά με δίκτυο LAN και αποτελούν μια «ομάδα». Το grid μπορεί να οργανωθεί βάση μίας ιεραρχίας αποτελούμενο από ομάδες "clusters" [11]. Η εργασία που έχει εμπλακεί στη διαχείριση του grid είναι κατανεμημένη να αυξάνει την κλίμακα του grid. Η συλλογή, η εφαρμογή του grid και οι πηγές δεδομένων όπως και η εργασία του προγραμματισμού είναι κατανεμημένα ώστε να ταιριάζουν στην τοπολογία του grid. Ομοίως, η συλλογή στατιστικών πληροφοριών είναι κατανεμημένη. Ομάδες "clusters" λαμβάνουν τρέχουσες πληροφορίες από τις υπολογιστικές μηχανές, τις συναθροίζουν, και τις στέλνουν στο υψηλότερο κομβικό επίπεδο διαχείρισης στην ιεραρχία.

Λογισμικό διαχείρισης εργασιών: Τα περισσότερα συστήματα του grid συμπεριλαμβάνουν λογισμικό διαχείρισης εργασιών. Αυτό το λογισμικό εντοπίζει το μηχάνημα όπου θα τρέξει η εργασία του grid η οποία έχει «δηλωθεί» από το χρήστη. Στην πιο απλή περίπτωση, μπορεί τυφλά να αναθέτει εργασίες στην επόμενη μηχανή που ταιριάζει στους πόρους που απαιτούνται. Ωστόσο, υπάρχουν πλεονεκτήματα στο να χρησιμοποιηθεί πιο αναβαθμισμένη έκδοση του λογισμικού.

Τα αναβαθμισμένα λογισμικά διαχείρισης εργασιών υλοποιούν ένα σύστημα προτεραιοτήτων εργασιών, χρησιμοποιώντας αρκετές εργασίες που είναι σε αναμονή, η κάθε μια με διαφορετική προτεραιότητα. Όταν οι μηχανές του grid είναι διαθέσιμές στο να εκτελέσουν εργασίες, η εργασία που είναι πρώτη σε προτεραιότητα στην ουρά εκτελείται πρώτη. Οι πολιτικές υλοποιούνται κάνοντας χρήση του λογισμικού διαχείρισης εργασιών. Συνήθως συμπεριλαμβάνουν περιορισμούς εργασιών, χρηστών, και πόρων. Για παράδειγμα, θα μπορούσε να υπάρχει μια πολιτική που να απαγορεύει στις εργασίες του grid να εκτελούνται σε συγκεκριμένη χρονική στιγμή κατά την διάρκεια της ημέρας.

Τα πιο ανεπτυγμένα λογισμικά διαχείρισης εργασιών θα παρακολουθούν την πρόοδο των εργασιών μέσω ενός ολοκληρωμένου διαγράμματος ροής. Αν οι εργασίες χαθούν μέσα στο σύστημα ή στο δίκτυο, το λογισμικό διαχείρισης εργασιών αυτόματα θα ξανά – δηλώσει την εργασία σε άλλο μηχάνημα. Εάν η εργασία εμφανιστεί να βρίσκεται σε ένα άπειρο βρόγχο, τότε αυτή η εργασία δεν θα πρέπει να ξανά – δηλωθεί . Τυπικά, οι εργασίες έχουν διαφορετικούς κώδικες ολοκλήρωσης, κάποιες από αυτές είναι ικανές να επαναδηλωθούν και κάποιες όχι [2].

Στα περισσότερα υπολογιστικά πλέγματα υλοποιείται ένα σύστημα εφεδρικών πόρων. Το σύστημα αυτό είναι ανώτερο από ένα λογισμικό διαχείρισης εργασιών. Καταρχάς είναι ένα «ημερολογιακό» σύστημα που δεσμεύει πόρους σε

συγκεκριμένες χρονικές περιόδους αποτρέποντας το λογισμικό ή άλλους χρήστες να δεσμεύσουν τον ίδιο πόρο την ίδια χρονική στιγμή. Επιπλέον, είναι σε θέση να διαγράφουν ή να σταματούν τρέχουσες εργασίες ανάλογα με τις προτεραιότητες.

Επικοινωνίες: Ένα σύστημα grid περιλαμβάνει λογισμικό, το οποίο είναι υπεύθυνο για την επικοινωνία των επιμέρους εργασιών. Για παράδειγμα, μια εφαρμογή μπορεί να διαχωριστεί σε μεγάλο αριθμό υποεργασιών. Η κάθε μια από τις υποεργασίες είναι μια διαφορετική εργασία για το υπολογιστικό πλέγμα. Η εφαρμογή ίσως να υλοποιήσει έναν αλγόριθμο που απαιτεί οι υποεργασίες να ανταλλάσουν πληροφορίες μεταξύ τους. Οι υποεργασίες πρέπει να είναι διαθέσιμες να εντοπίζουν άλλες υποεργασίες, να δημιουργήσουν κανάλια επικοινωνίας και να στέλνουν τα απαραίτητα δεδομένα. Το open standard Message Passing Interface (MPI) [3] και οποιαδήποτε άλλη παραλλαγή συχνά συμπεριλαμβάνεται σαν μέρος του grid για τέτοιου είδους επικοινωνία.

1.4 Η ΧΡΗΣΗ ΤΟΥ grid: Από την σκοπιά του χρήστη

Στην παράγραφο 1.4 και στις υπό – παραγράφους που ακολουθούν γίνεται αναφορά στη χρήση ενός υπολογιστικού πλέγματος από την πλευρά του χρήστη. Ο χρήστης ενός grid μπορεί να εκτελέσει τις παρακάτω ενέργειες:

- Εγγραφή στο Grid.
- Διαδικασία αυθεντικοποίησης.
- «Δήλωση» εργασίας προς εκτέλεση.
- Παρακολούθηση της προόδου και της κατάστασης των εργασιών που έχει «δηλώσει».
- Αξιοποίηση του γραφικού περιβάλλοντος ή της γραμμής εντολών.

Ακολουθεί αναλυτική περιγραφή των παραπάνω ενεργειών.

1.4.1 Εγγραφή του χρήστη και εγκατάσταση λογισμικού υπολογιστικού πλέγματος

Αρχικά ο χρήστης εγγράφεται στο υπολογιστικό πλέγμα και στη συνέχεια εγκαθιστά το διαθέσιμο λογισμικό στον υπολογιστή του. Κατά τη διάρκεια εγγραφής του λογισμικού δίνετε η δυνατότητα στο χρήστη να εγγράψει τον προσωπικό υπολογιστή του ως «υπολογιστής – παροχέας πόρων» στο υπολογιστικό πλέγμα που ανήκει. Για να εγγραφεί κάποιος στο grid απαιτείται αυθεντικοποίηση για προφανής λόγους ασφάλειας. Ο χρήστης έχει αποκτήσει ένα ηλεκτρονικό πιστοποιητικό μέσω μιας «Αρχής Πιστοποίησης» (Certificate Authority) [12]. Όμως η πιστοποίηση του χρήστη μέσω του διαδικτύου δεν αποτελεί την πιο ασφαλή λύση. Η αρχή πιστοποίησης πρέπει να πάρει μέτρα και να ενημερώσει το υπολογιστικό πλέγμα (συγκεκριμένα τον κόμβο διαχείρισης) για την «πραγματική» ταυτότητα του χρήστη. Επομένως, η αρχή πιστοποίησης συνεργάζεται με την εταιρεία σχεδιασμού του λογισμικού έτσι ώστε στο λογισμικό να ενσωματωθεί ένα ειδικό πιστοποιητικό που θα αυθεντικοποιεί το χρήστη. Ο χρήστης είναι υπεύθυνος να μην γνωστοποιήσει τα πιστοποιητικά του grid σε τρίτους.

Το λογισμικό που παρέχεται για εγκατάσταση στο χρήστη συνήθως είναι παραμετροποιημένο με τέτοιο τρόπο έτσι ώστε να γνωρίζει τις ηλεκτρονικές διευθύνσεις των κόμβων διαχείρισης στο υπολογιστικό πλέγμα. Η εγκατάσταση απαιτεί πολύ μικρή συμμετοχή από το χρήστη και όλες οι διαδικασίες της είναι αυτοματοποιημένες (πάντα βάση των πολιτικών που εφαρμόζονται στο εκάστοτε υπολογιστικό πλέγμα). Σε λιγότερο αυτοματοποιημένες εγκαταστάσεις λογισμικού, θα ζητηθεί από το χρήστη να αναγνωρίσει τον κόμβο διαχείρισης και θα του ζητηθούν πληροφορίες για την παραμετροποίηση του υπολογιστή του (για παράδειγμα, ο όγκος των πόρων που θα παρέχει προς το υπολογιστικό πλέγμα, τα χρονικά διαστήματα κατά τα οποία ο υπολογιστής θα είναι συνδεδεμένος στο υπολογιστικό πλέγμα και άλλοι παρόμοιοι περιορισμοί).

1.4.2 Σύνδεση στο υπολογιστικό πλέγμα

Για να χρησιμοποιηθεί το grid, θα πρέπει ο χρήστης να συνδεθεί στο σύστημα με τον προσωπικό κωδικό του που είναι εγγεγραμμένος στο grid. Άλλα συστήματα του grid έχουν το δικό τους κωδικό σύνδεσης ξέχωρα από αυτόν που έχει το λειτουργικό σύστημα, το οποίο είναι πιο βολικό για τους χρήστες του grid. Η χρήση κωδικών σύνδεσης στο grid θυμίζει περισσότερο ένα τεράστιο ιδεατό υπολογιστικό σύστημα παρά μια συλλογή από ανεξάρτητους υπολογιστές. Το Globus για παράδειγμα, υλοποιεί ένα μοντέλο σύνδεσης proxy που κρατάει το χρήστη συνδεδεμένο στο σύστημα για συγκεκριμένο χρονικό διάστημα, ακόμα και αν αποσυνδεθεί ή επανεκκίνηση το μηχάνημα.

1.4.3 «Δήλωση» Εργασιών

Ο χρήστης μπορεί να εκτελεί κάποια ερωτήματα για να ελέγχει πόσο απασχολημένο είναι το grid, να ελέγχει την πρόοδο των εργασιών του και να ψάξει για νέους υπολογιστικούς πόρους μέσα στο grid. Το υπολογιστικό σύστημα διαθέτει στη χειρότερη περίπτωση εργαλεία εντολών γραμμής και στην καλύτερη γραφικά περιβάλλοντα για την εκτέλεση των ερωτημάτων [4,12]. Τα εργαλεία εντολών γραμμής απευθύνονται σε εξειδικευμένους χρήστες οι οποίοι συνήθως γράφουν ένα κομμάτι κώδικα για να εκτελεστεί μια ακολουθία ενεργειών. Για παράδειγμα, ο χρήστης μπορεί να γράψει 10 γραμμές κώδικα και να ψάξει για διαθέσιμους πόρους, να δηλώσει μια εργασία προς αυτούς, να ελέγξει την πρόοδο της εργασίας και να παρουσιάσει τα αποτελέσματα της όταν αυτή ολοκληρωθεί.

Η δήλωση μιας εργασίας στο grid συνήθως απαιτεί το πάτημα ενός κουμπιού ή την εκτέλεση μιας εντολής αλλά ουσιαστικά αποτελείται από 3 ενέργειες. Πρώτον, τα δεδομένα εισόδου και το εκτελέσιμο αρχείο στέλνονται στο μηχάνημα που θα εκτελέσει την εργασία. Εναλλακτικά τα δεδομένα μπορεί να είναι "προ-εγκατεστημένα" στα μηχανήματα στο grid ή προσβάσιμα μέσω ενός διαδικτυακού συστήματος διαχείρισης αρχείων. Όταν το grid αποτελείται από ετερογενή μηχανήματα τότε θα υπάρξουν πολλαπλά εκτελέσιμα αρχεία, κάθε ένα από αυτά είναι συμβατά με την αντίστοιχη πλατφόρμα του μηχανήματος. Κάποιες τεχνολογίες του grid απαιτούν το πρόγραμμα και τα δεδομένα εισόδου να επεξεργαστούν σε πρώτο στάδιο από τους μηχανισμούς του grid. Το παραπάνω γίνεται με την προσθήκη προστατευτικών ελέγχων ή/και με τη συλλογή όλων των δεδομένων σε ένα αρχείο.

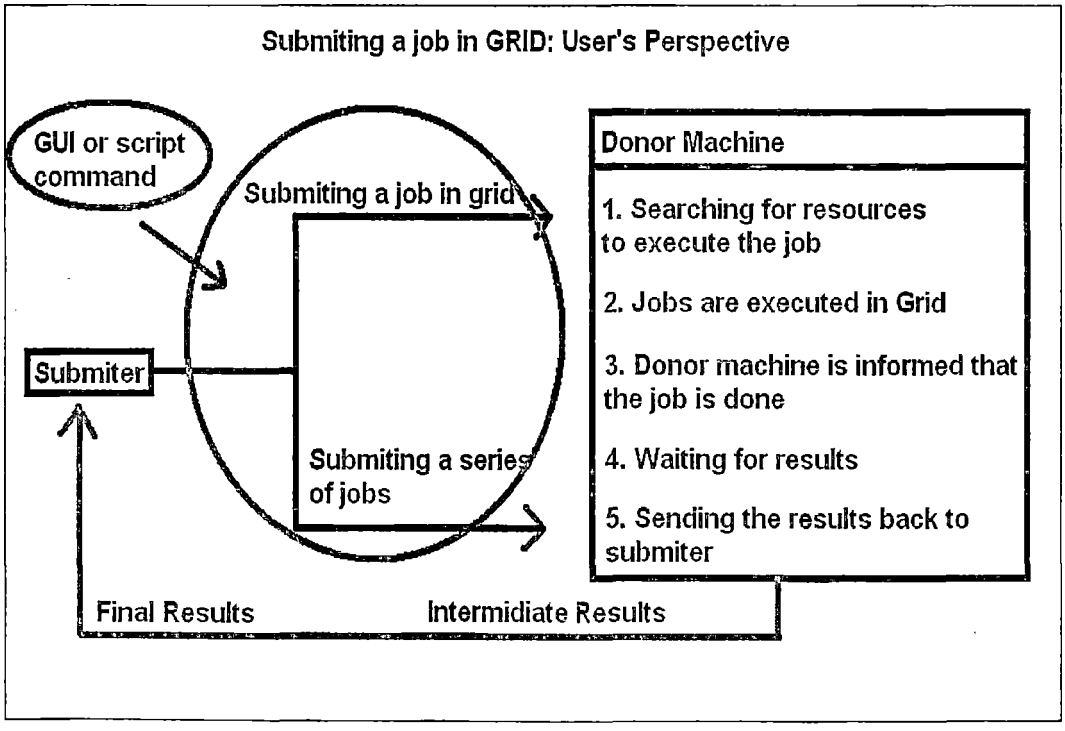
Στο επόμενο βήμα το λογισμικό του grid, το οποίο τρέχει στα μηχανήματα παροχής πόρων εκτελεί την εφαρμογή. Τα περισσότερα συστήματα υπολογιστικού πλέγματος υλοποιούν μια "προστατευτική αύρα" γύρω από την εφαρμογή έτσι ώστε να μην υπάρξει παρέμβαση προς το μηχάνημα παροχής πόρων.

Τρίτον, τα αποτελέσματα από τις εργασίες στέλνονται προς το μηχάνημα που δήλωσε την εργασία. Σε μερικές υλοποιήσεις ο χρήστης που δήλωσε την εργασία μπορεί να παρακολουθήσει τα ενδιάμεσα αποτελέσματα. Τέτοια αποτελέσματα είναι:

- Πλήθος μηχανημάτων που χρησιμοποιήθηκαν για την εκτέλεση της εργασίας
- Υπολογίσιμη ισχύ που καταναλώθηκε
- Χρόνος διεκπεραίωσης της εργασίας
- Πιθανά προβλήματα που παρουσιάστηκαν

Τα "scripts"(μικρές εφαρμογές κώδικα προς εκτέλεση) είναι χρήσιμα για τη "δήλωση" μιας σειράς εργασιών. Για παράδειγμα, κάποια υπολογιστικά προβλήματα αναζητούν ιδανικά αποτελέσματα βάση κάποιων παραμέτρων εισόδου. Ο στόχος είναι η εύρεση των κατάλληλων δεδομένων εισόδου που παράγουν το επιθυμητό αποτέλεσμα [8]. Για κάθε δεδομένο εισόδου μια ξεχωριστή εργασία εκτελείται και παράγει το αντίστοιχο αποτέλεσμα. Τα "scripts" χρησιμοποιούνται για την εκτέλεση αυτών των υποεργασιών.

Όταν ένα μεγάλο πλήθος υποεργασιών ολοκληρωθεί, τα αποτελέσματα συλλέγονται και παράγουν ένα τελικό αποτέλεσμα που στέλνεται στον χρήστη που δήλωσε τις εργασίες. Αν τώρα το πλήθος των υποεργασιών είναι υπερβολικά μεγάλο η διαδικασία συλλογής των αποτελεσμάτων μπορεί και αυτή να κατανεμηθεί.



Σχήμα 1.4.3: Δήλωση εργασιών

1.4.4 Παραμετροποίηση δεδομένων

Τα δεδομένα, που είναι προσβάσιμα από τις εργασίες του grid μπορούν απλά να ανεβαίνουν και να κατεβαίνουν βαθμίδες μέσα στο δίκτυο. Βάση του μεγέθους του υπολογιστικού πλέγματος και το πλήθος των εργασιών, υπάρχει περίπτωση η διαβάθμιση των δεδομένων να προκαλέσει "κυκλοφοριακό χάος". Για τον παραπάνω λόγο γίνονται προσπάθειες έτσι ώστε να επιτευχθεί η λιγότερη δυνατή κίνηση των δεδομένων μέσα στο grid.

Για παράδειγμα, όταν μια εφαρμογή "τρέχει" συνεχώς μέσα στο grid, τα δεδομένα που θα χρησιμοποιηθούν ως δεδομένα εισόδου της εφαρμογής θα αποθηκευτούν σε ένα διαδικτυακό σημείο στο grid έτσι ώστε να αποφευχθεί η επαναμετακίνηση τους. Υπάρχουν πολλές σκέψεις για το πώς θα κατασκευαστεί ένα σχέδιο που θα διαμοιράζει και θα διαχειρίζεται τα δεδομένα στο υπολογιστικό πλέγμα. Αυτός ο τύπος ανάλυσης είναι απαραίτητος για μεγάλου μεγέθους εργασίες και για την καλύτερη αξιοποίηση του grid έτσι ώστε να μην δημιουργηθούν άσκοπες καθυστερήσεις.

1.4.5 Διαδικασίες επίβλεψης προόδου και ανάκαμψης εργασιών

Ο χρήστης μπορεί να θέτει «ερωτήματα» προς το υπολογιστικό πλέγμα για να ενημερωθεί σχετικά με την πρόοδο της εφαρμογής και των υπο-εργασιών του. Όταν ο αριθμός των υπο-εργασιών είναι πολύ μεγάλος, τότε πολύ πιθανόν ένα γραφικό παράθυρο να αδυνατεί να τις χωρέσει. Για αυτό χρησιμοποιούνται γραφικές μπάρες για την καταμέτρηση των πληροφοριών. Ένα ακόμη σημαντικό ζήτημα είναι η παρακολούθηση εργασιών που βρίσκονται σε διαδικασία ανάκαμψης (rejuvenation procedure).

Συνήθως τα υπολογιστικά πλέγματα, σε συνεργασία με το «Διαχειριστή εργασιών», παρέχουν διαδικασίες ανάκαμψης για υπό-εργασίες που αποτυγχάνουν. Μια εργασία μπορεί να αποτύχει για τους παρακάτω λόγους:

- Προγραμματιστικό σφάλμα
- Υλικό ή ενεργειακό σφάλμα (για παράδειγμα, το μηχάνημα που εκτελεί την εργασία τερματίζει απρόσμενα)
- Διακοπή επικοινωνιών (για παράδειγμα, υπερφόρτωση του δικτύου)
- Υπερβολική καθυστέρηση (η εργασία έχει μπει σε άπειρο βρόγχο ή αναμένει την εκτέλεση εργασιών με μεγαλύτερη προτεραιότητα).

Οι «διαχειριστές εργασιών» κατηγοριοποιούν τις αστοχίες εργασιών ανά ομάδα σφαλμάτων. Επιπλέον, οι «διαχειριστές εργασιών» εκκινούν αυτόματες διαδικασίες «επαναδήλωσης» των εργασιών σε κάποιο σημείο στο grid. Οι χρήστες στα περισσότερα υπολογιστικά πλέγματα ενημερώνονται αυτόματα για την «ανανέωση» των υπο-εργασιών τους. Για να συμβεί αυτό απαιτείται η χρήση συναρτήσεων – μεθόδων από τα APIs (application programming interfaces).

1.5 Η ΧΡΗΣΗ ΤΟΥ GRID: Από την σκοπιά του διαχειριστή

1.5.1 Σχεδιασμός

Ο διαχειριστής πρέπει να κατανοήσει της ανάγκες του οργανισμού, και να επιλέξει την καλύτερη δυνατή τεχνολογία του grid που ικανοποιεί αυτές τις ανάγκες. Παρακάτω θα δούμε τα βήματα που πρέπει να ακολουθήσει ο διαχειριστής για την οργάνωση του grid. Το καλύτερο θα ήταν να δημιουργηθεί ένα μικρό grid αρχικά, έτσι ώστε ο διαχειριστής να εξοικειωθεί με τις διαδικασίες εγκατάστασης και διαχείρισης, προτού βρεθεί αντιμέτωπος με πολύπλοκα θέματα δικτύων και ασφάλειας που συμπεριλαμβάνονται σε ένα μεγαλύτερου μεγέθους grid.

1.5.2 Εγκατάσταση

Αρχικά, το επιλεγόμενο σύστημα του grid πρέπει να εγκαθίσταται σε κατάλληλα παραμετροποιημένα μηχανήματα. Ένα ζήτημα μεγίστης σπουδαιότητας είναι η αξιοποίηση των «σεναρίων αντιμετώπισης – ανάκαμψης σφαλμάτων». Στόχος είναι η αδιάλειπτη λειτουργία του υπολογιστικού πλέγματος ακόμη και αν αποτύχουν ένας ή παραπάνω κεντρικοί κόμβοι του συστήματος (για παράδειγμα οι μηχανές διαχείρισης). Τα μηχανήματα πρέπει να είναι παραμετροποιημένα και «συνδεδεμένα » έτσι ώστε τα σενάρια ανάκαμψης να είναι εφικτά.

Οποιοδήποτε άλλο κρίσιμο αγαθό στο υπολογιστικό πλέγμα (για παράδειγμα μία βάση δεδομένων που κρατάει πληροφορίες σχετικά με τις εργασίες στο grid) πρέπει να έχει άμεση πρόσβαση σε αντίγραφα ασφαλείας. Επιπλέον, τα πιστοποιητικά δημοσίου κλειδιού πρέπει να έχουν αντίγραφα (back up) στο σύστημα, ενώ αντιθέτως τα «ιδιωτικά κλειδιά» πρέπει να κρατούνται σε ασφαλή περιοχή, μη προσβάσιμη από καμία άλλη οντότητα εκτός του διαχειριστή.

Σε μερικά υπολογιστικά πλέγματα απαιτείται η εγκατάσταση του λογισμικού και στα μηχανήματα παροχής πόρων. Το λογισμικό που εγκαθίσταται στα μηχανήματα παροχής πόρων πρέπει να παραμετροποιηθεί από το διαχειριστή έτσι ώστε τα τελευταία να επικοινωνήσουν με αυτόματες διαδικασίες με τα μηχανήματα διαχείρισης του υπολογιστικού πλέγματος.

Από τη στιγμή που το υπολογιστικό πλέγμα μπαίνει σε λειτουργία, ο διαχειριστής θα πρέπει να εγκαταστήσει λογισμικό εφαρμογής στα μηχανήματα παροχής πόρων. Το λογισμικό αυτό εμπεριέχει «περιορισμούς πιστοποίησης» που πρέπει να γίνουν κατανοητοί. Πολλά υπολογιστικά πλέγματα ενσωματώνουν εργαλεία που υποστηρίζουν τις διαδικασίες διαχείρισης του πιστοποιητικού.

1.5.3 Διαχείριση των «Μελών» του grid

Ένα σημαντικό θέμα που προκύπτει για το διαχειριστή του υπολογιστικού πλέγματος είναι να οργανώσει τα «μέλη» του grid, τόσο τα μηχανήματα παροχής πόρων όσο και τους χρήστες. Ο διαχειριστής είναι υπεύθυνος για τον έλεγχο και την παραμετροποίηση των δικαιωμάτων των χρηστών του υπολογιστικού πλέγματος. Μία εργασία στο grid μπορεί να τρέξει σε ένα μηχάνημα παροχής πόρων βάση συγκεκριμένου κωδικού εξουσιοδότησης. Τα δικαιώματα πρόσβασης κάθε χρήστη

στο grid πρέπει να διαχειρίζονται με σύνεση έτσι ώστε να μην επιτρέπεται η πρόσβαση των χρηστών στα μη εξουσιοδοτημένα μέρη του grid.

Όταν οι χρήστες συνδεθούν στο grid για πρώτη φορά, η «ταυτότητα» τους στέλνεται σε μία Αρχή Πιστοποίησης (Certificate Authority). Ο κωδικός και τα πιστοποιητικά του χρήστη προστίθενται στη «λίστα χρηστών» βάση του λογισμικού που χρησιμοποιεί το εκάστοτε υπολογιστικό πλέγμα. Σε μερικές περιπτώσεις, ο διαχειριστής «δημοσιοποιεί» τις πληροφορίες του χρήστη σε μερικά ή και σε όλα τα μηχανήματα του gird [12].

Παρόμοια διαδικασία ακολουθείται και για τα μηχανήματα παροχής πόρων. Η «ταυτότητα» ενός μηχανήματος παροχής πόρων ενημερώνεται στην αρχή πιστοποίησης. Ο διαχειριστής του υπολογιστικού πλέγματος πρέπει να συμφωνεί με το διαχειριστή του αντιστοίχου μηχανήματος παροχής πόρων σε δεδομένα όπως:

- Οι κωδικοί των χρηστών.
- Συμβατότητα λογισμικού.
- Δικαιώματα πρόσβασης.
- Περιορισμοί πολιτικών.

Τέλος, οι διαδικασίες που αφορούν την απομάκρυνση – διαγραφή χρηστών, μηχανημάτων εκτελούνται μόνο από το διαχειριστή του υπολογιστικού πλέγματος.

1.5.4 Αρχή Πιστοποίησης

Στην παράγραφο 1.5.3 αναφερθήκαμε στην «Αρχή Πιστοποίησης». Σε αυτή την παράγραφο θα αναλύσουμε ποιες είναι οι βασικές ευθύνες μιας «Αρχής Πιστοποίησης» και πως η τελευταία αλληλεπιδρά με το υπολογιστικό πλέγμα. Το υπολογιστικό πλέγμα δεν στοχεύει μόνο στην διαμοίραση δεδομένων αλλά και στην εκτέλεση κώδικα. Υιοί, «Δούρειοι Ίπποι » και άλλες γνωστές επιθέσεις αποτελούν μεγάλη απειλή για το υπολογιστικό πλέγμα. Επομένως, πρέπει να διασφαλίσουμε τα υψηλότερα επίπεδα ασφάλειας. Ένας οργανισμός μπορεί να επιλέξει να χρησιμοποιήσει μια «Εξωτερική Αρχή Πιστοποίησης» ή να «τρέξει» μια δική του. Όποια και να είναι η επιλογή το grid πρέπει να εμπιστεύεται την «Αρχή Πιστοποίησης» και να τηρεί τις βασικές προϋποθέσεις που θέτει η τελευταία [13].

Βασικές αρμοδιότητες μίας «Αρχής Πιστοποίησης», είναι:

- Αναγνώριση των οντοτήτων που απαιτούνται για πιστοποιητικά
- Διαδικασίες έκδοσης, αρχειοθέτησης και απόρσυσης πιστοποιητικών
- Η υλοποίηση μηχανισμών ασφάλειας για την προστασία του εξυπηρετητή
- Υποστήριξη «έγκυρων» πιστοποιητικών για όσους απαιτούν αυθεντικοποίηση
- Σχεδιασμός διαδικασιών αντιγράφων ασφαλείας

Μία άρση πιστοποίησης στηρίζεται στο κρυπτογραφικό σύστημα δημοσίου κλειδιού. Σε ένα τέτοιο σύστημα, τα κρυπτογραφικά κλειδιά παράγονται σε ζεύγη. Κάθε ζεύγος αποτελείται από το δημόσιο και το ιδιωτικό κλειδί.

Το ιδιωτικό κλειδί (private key) αντιστοιχεί μοναδικά σε μια οντότητα στο σύστημα και δεν αποκαλύπτεται ποτέ. Αντίθετα το δημόσιο κλειδί (public key) μοιράζεται σε όποια οντότητα το χρειάζεται για επικοινωνία. Η αρχή πιστοποίησης «κρατάει» τα δημόσια κλειδιά και εγγυάται ότι το δημόσιο κλειδί Χ αντιστοιχεί στο χρήστη Ψ. Όταν ένας χρήστης χρησιμοποιήσει το ιδιωτικό κλειδί του για να κρυπτογραφήσει ένα μήνυμα, ο αποδέκτης του μηνύματος χρησιμοποιεί το αντίστοιχο δημόσιο κλειδί για να το αποκρυπτογραφήσει. Βέβαια, ένας επιτιθέμενος θα μπορούσε να παρεισφρύσει στην επικοινωνία και να αποκρυπτογραφήσει το μήνυμα, εφόσον το δημόσιο κλειδί είναι γνωστό [14].

Επομένως, για την εγκατάσταση μιας ασφαλής επικοινωνίας, απαιτείται από τον αποστολέα να κρυπτογραφήσει το μήνυμα εις διπλούν. Την πρώτη φορά με το ιδιωτικό κλειδί του, και την δεύτερη φορά με το δημόσιο κλειδί του παραλήπτη. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό κλειδί του και εν συνεχεία με το δημόσιο κλειδί του αποστολέα.

1.5.5 Διαχείριση Υπολογιστικών πόρων

Ακόμη μια σημαντική αρμοδιότητα του διαχειριστή είναι η διαχείριση των υπολογιστικών πόρων. Ο διαχειριστής πρέπει να είναι σε θέση να καθορίζει τα δικαιώματα εισόδου ανά χρήστη του υπολογιστικού πλέγματος, ο οποίος θέλει να αξιοποιήσει υπολογιστικούς πόρους του δικτύου. Επιπλέον, η χρήση στατιστικών και άλλων μαθηματικών μεθόδων είναι χρήσιμη για την αναγνώριση τάσεων – ροπών σε ένα οργανισμό που συμμετέχει στο grid.

1.6 Η ΧΡΗΣΗ ΤΟΥ GRID: Από την σκοπιά του σχεδιαστή πληροφοριακών συστημάτων

Οι εφαρμογές του υπολογιστικού πλέγματος μπορεί να κατηγοριοποιηθούν ως εξής:

- Εφαρμογές που δεν υποστηρίζουν πολλαπλή επεξεργασία αλλά μπορούν να εκτελεστούν σε διαφορετικά μηχανήματα
- Εφαρμογές που υποστηρίζουν τον αρχιτέκτονα των πολλαπλών επεξεργασιών
- Εφαρμογές που πρέπει να τροποποιηθούν ή ακόμα και να «επανά-υλοποιηθούν» για να είναι συμβατές με το grid.

Η τελευταία από τις τρεις κατηγορίες προσελκύει το ενδιαφέρον των σχεδιαστών εφαρμογών.

Το Globus Toolkit δεν παρέχει δικό του «Διαχειριστή» εργασιών για την εξεύρεση υπολογιστικών πόρων έτσι ώστε με αυτόματες διαδικασίες να αναθέτει εργασίες στα κατάλληλα μηχανήματα. Αντίθετα, παρέχει εργαλεία και προγραμματιστικά περιβάλλοντα για την υλοποίηση «οντοτήτων» διαχείρισης.

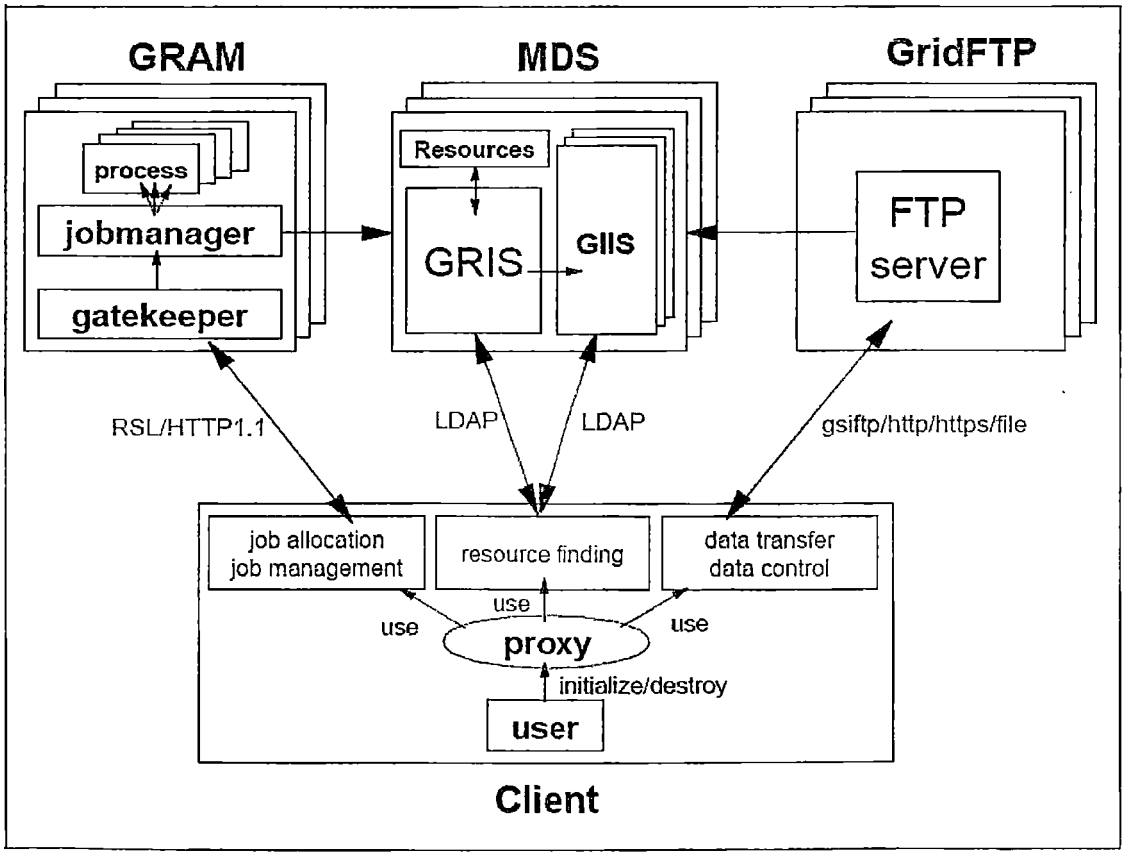
Διαχείριση δεδομένων: Η υπηρεσία διαχείρισης δεδομένων υποστηρίζει τόσο τις διαδικασίες ανταλλαγής δεδομένων μεταξύ των υπολογιστών του grid όσο και τις διαδικασίες των παραπάνω ανταλλαγών.

Υπηρεσίες πληροφοριακών συστημάτων: Οι υπηρεσίες αυτές, βασισμένες στο «Πρωτόκολλο Εύρεσης Καταλόγου» (LDAP), υποστηρίζουν διαδικασίες συλλογής πληροφοριών.

Το Globus Toolkit είναι ένα ανοιχτό λογισμικό σχεδιασμένο από το Globus project. Επιπλέον, το παγκόσμιο Φόρουμ (Forum) του υπολογιστικού πλέγματος υποστηρίζει το Globus Toolkit και το προτείνει σε περισσότερες από 30 χώρες και σε περισσότερους από 200 οργανισμούς.

2.2 Συστατικά του Globus Toolkit

Για κάθε μια πυραμίδα που παρουσιάστηκε στην προηγούμενη υπο-ενότητα, το Globus παρέχει μια οντότητα που υλοποιεί τις υπηρεσίες της πυραμίδας όπως φαίνεται στο σχήμα 2.2 [15].



Σχήμα 2.2: Το σύστημα Globus Toolkit

Τα συστατικά-μέρη του Globus Toolkit είναι:

- GRAM / GASS: Οι βασικές οντότητες διαχείρισης υπολογιστικών πόρων είναι το «Grid Resource Allocation Manager» και το «Globus Access to Secondary Storage»

- MDS (GRIS / GILLS): Οι οντότητες «Grid Resource Information Service» και «Grid Index Information Service», βάσει του πρωτοκόλλου LDAP, αποτελούν την οντότητα MDS (Monitoring and Discovery Service). Οι πληροφορίες που συλλέγονται μπορεί να έχουν στατική μορφή ή δυναμική μορφή (για παράδειγμα, η τρέχουσα δραστηριότητα του επεξεργαστή ή του σκληρού δίσκου).

- GridFTP: Το GridFTP αποτελεί μια οντότητα-κλειδί για ασφαλή και υψηλών επιδόσεων μεταφορά δεδομένων. Το GRC(Globus Replica Catalog) και το Management χρησιμοποιούνται για τη διαχείριση και την αποθήκευση των αντιγράφων των δεδομένων.

- GSI (Grid Security Infrastructure): Οι παραπάνω οντότητες χτίστηκαν πάνω στο GSI, το τελευταίο παρέχει ασφαλείς μεθόδους επικοινωνίας όπως αμφίδρομη αυθεντικοποίηση, εμπιστευτικές επικοινωνίες και μηχανισμούς εξουσιοδότησης.

2.2.1 Υποδομή Ασφάλειας του Υπολογιστικού Πλέγματος (Grid Security Infrastructure, GSI)

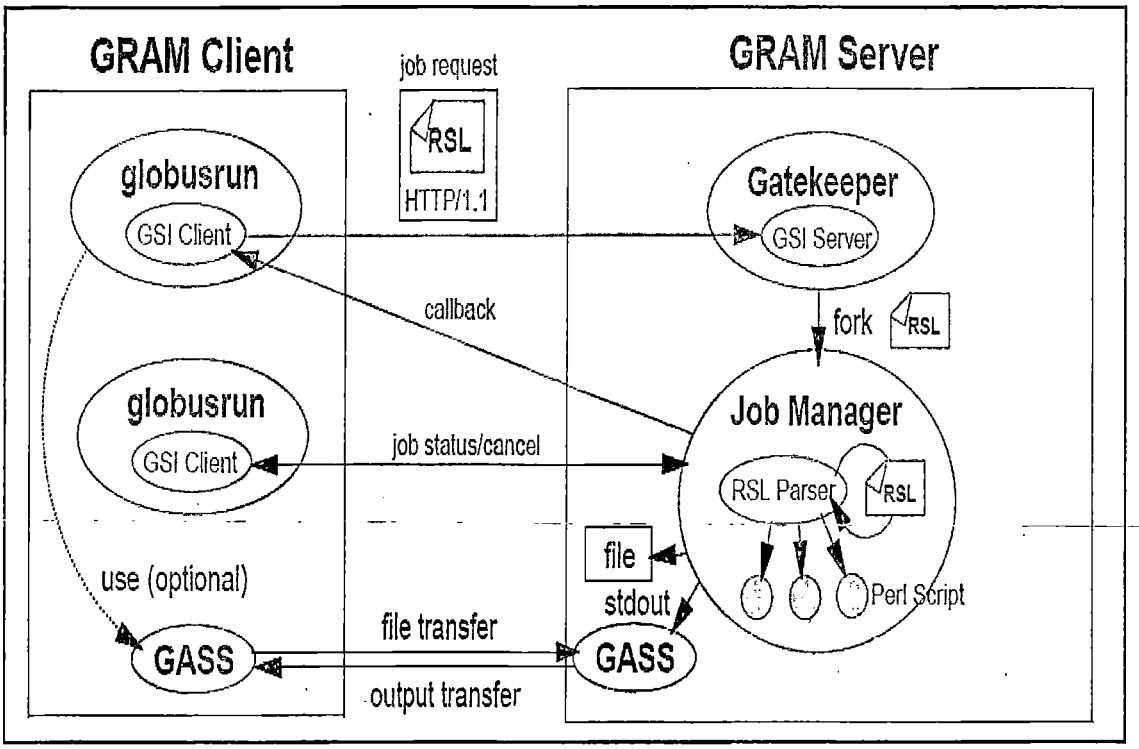
Το GSI παρέχει ασφαλής επικοινωνίες και διαδικασίες αυθεντικοποίησης προς στις οντότητες του υπολογιστικού πλέγματος. Το GSI στηρίζεται στο πρωτόκολλο SSL (Secure Socket Layer), στην κρυπτογραφία δημοσίου κλειδιού και στα πιστοποιητικά X.509 [12]. Οι βασικές λειτουργίες που υλοποιεί η υποδομή GSI είναι:

- Απλή/Αμφίδρομη αυθεντικοποίηση
- "Εμπιστευτικές" επικοινωνίες
- Μηχανισμούς εξουσιοδότησης
- Διαβάθμιση χρηστών (Delegation)

2.2.2 Διαχειριστής Δέσμευσης Υπολογιστικών Πόρων (Grid Resource Allocation Manager, GRAM)

Όταν μια εργασία δηλώνεται από ένα χρήστη, η αίτηση του στέλνετε σε απομακρυσμένο υπολογιστή και διαχειρίζεται από το δαίμονα "gatekeeper". Ο "gatekeeper" δημιουργεί ένα «Διαχειριστή εργασιών». Ο «Διαχειριστής εργασιών» είναι αρμόδιος για τις παρακάτω ενέργειες:

- Εκκίνηση της εργασίας
- Επίβλεψη της εργασίας
- Αποστολή πληροφοριών προς τον πελάτη για την κατάσταση της εργασίας



Σχήμα 2.2.2: Αρχιτεκτονική GRAM

Η εντολή "globusrun": Εκτελείται από το λογισμικό του πελάτη και είναι υπεύθυνη για τη "δήλωση" και διαχείριση απομακρυσμένων εργασιών. Πιο συγκεκριμένα η εντολή "globusrun" αιτείται, για λογαριασμό του χρήστη, από τα απομακρυσμένα μηχανήματα την εκτέλεση εργασιών. Επιπλέον, μεταφέρει τα εκτελέσιμα αρχεία προς στους απομακρυσμένους υπολογιστές και λαμβάνει τα τελικά αποτελέσματα.

"Εξειδικευμένη γλώσσα" υπολογιστικών πόρων (Resource Specification Language, RSL): Η γλώσσα RSL χρησιμοποιείται από το λογισμικό των πελατών στην διαδικασία "δήλωσης" των εργασιών. Όταν εκτελείται μια "globusrun" εντολή, τα δεδομένα που στέλνονται στο GRAM server εμπεριέχουν RSL πληροφορίες. Οι πληροφορίες RSL καθορίζουν τους κανόνες βάσει των οποίων θα τρέξει η εργασία (για παράδειγμα, το μέγεθος της μνήμης που απαιτείται για την εκτέλεση της εργασίας).

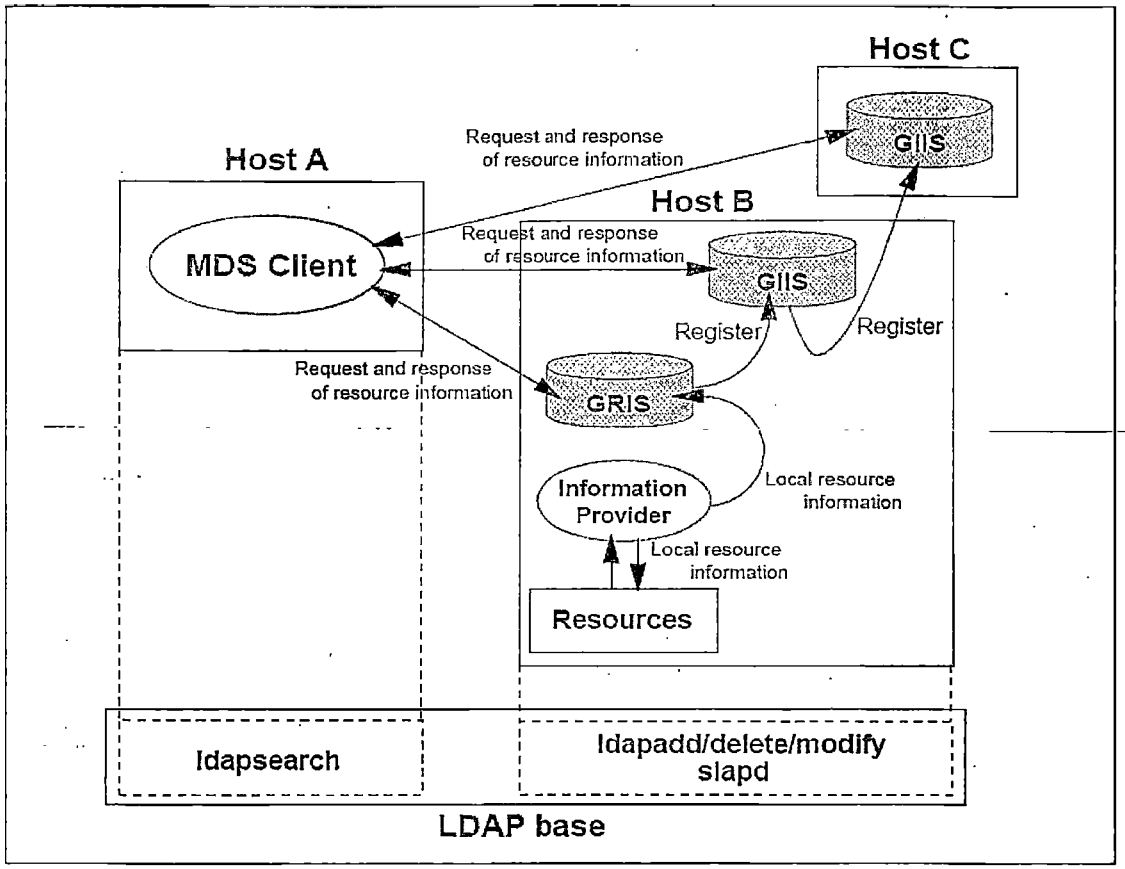
"Παγκόσμια" πρόσβαση σε δευτερεύον αποθηκευτικό χώρο (Global Access to Secondary Storage, GASS): Η αρχιτεκτονική GRAM χρησιμοποιεί τον μηχανισμό GASS για την μεταφορά του "τεχνικού αρχείου" από τους εξυπηρετητές προς τους χρήστες.

2.2.3 Υπηρεσία Επίβλεψης και Εύρεσης Υπολογιστικών Πόρων (Monitoring and Discovery Service, MDS)

Το MDS παρέχει πρόσβαση σε στατικές και δυναμικές πληροφορίες υπολογιστικών πόρων. Οι οντότητες του MDS είναι:

- GRIS

- GIIS
- Παροχές πληροφοριών
- Χρηστές MDS



Σχήμα 2.2.3: Αρχιτεκτονική MDS

Όπως φαίνεται και στο σχήμα 2.2.3 ο πελάτης αξιοποιεί την υπηρεσία MDS για να λάβει πληροφορίες σχετικές με τους υπολογιστικούς πόρους. Τον πελάτη τον ενδιαφέρουν εκείνοι οι υπολογιστικοί πόροι που έχουν δεσμευτεί από το "HOST B" και το "HOST C" για την εκτέλεση των εργασιών του. Ακολουθεί αναλυτική περιγραφή των οντοτήτων του MDS:

Υπηρεσία Παροχής Πληροφοριών Υπολογιστικών Πόρων (Grid Resource Information Service, GRIS): Το GRIS λειτουργεί ως αποθηκευτικός χώρος πληροφοριών υπολογιστικών πόρων. Το GRIS με την βοήθεια της οντότητας GIIS καταγράφει τις πληροφορίες σχετικά με τους υπολογιστικούς πόρους (registration procedure). Για να καταγράψει μια πληροφορία το GRIS, αναμένει αίτηση από τον πελάτη. Όταν η αίτηση φτάσει στο GRIS, το τελευταίο επικοινωνεί με τους "Παροχής Πληροφοριών" (Information Provider) για να λάβει τις πληροφορίες.

Υπηρεσία Καταλόγου Πληροφοριών (Grid Index Information Service, GIIS): Το GIIS από την πλευρά του καταχωρεί τις αιτήσεις των χρηστών που σχετίζονται με την παροχή πληροφοριών σχετικά με τους υπολογιστικούς πόρους. Κάθε οντότητα GIIS μέσα στο υπολογιστικό πλέγμα έχει μοναδικό όνομα. Οι χρήστες μπορούν να καθορίσουν το όνομα της GIIS οντότητας και να ψάξουν για πληροφορίες.

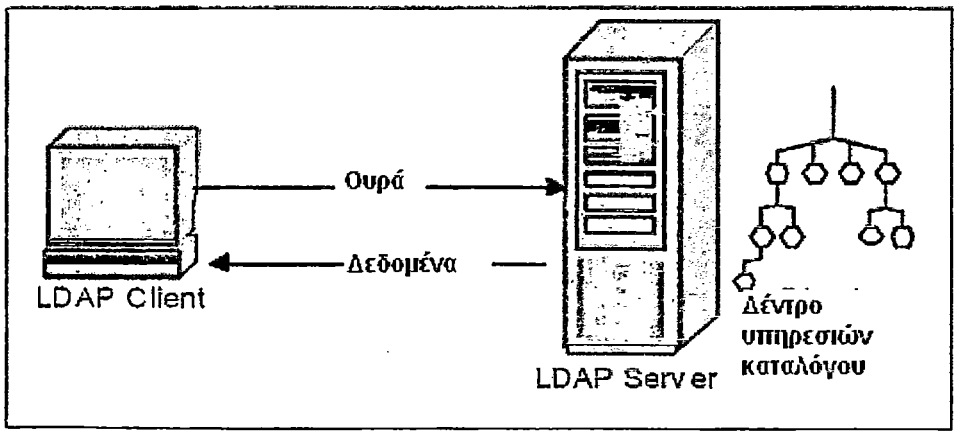
Παροχής Πληροφοριών (Information Providers): Τα IPs είναι ενδιάμεσες οντότητες και συνδέουν τη βάση δεδομένων των υπολογιστικών πόρων με την οντότητα GRIS. Τα IPs είναι υπεύθυνα για την μετάφραση των πληροφοριών από την βάση δεδομένων προς την οντότητα GRIS και αντίστροφα.

Πληροφορίες Υπολογιστικών Πόρων (Resource Information): Ένας χρήστης όταν αξιοποιήσει την υπηρεσία MDS λαμβάνει στατικές και δυναμικές πληροφορίες σχετικά με τους υπολογιστικούς πόρους. Οι πληροφορίες σχετίζονται με οντότητες υποδομής του υπολογιστικού πλέγματος (infrastructure components), για παράδειγμα, το όνομα του διαχειριστή εργασιών ή το όνομα μίας τρέχουσας εργασίας. Επιπλεόν οι πληροφορίες σχετίζονται και με υπολογιστικούς πόρους (computer resources), για παράδειγμα μέγεθος μνήμης ή IP διευθύνσεις.

LDAP (Lightweight Directory Access Protocol): Το LDAP είναι ένα πακέτο «δωρεάν» λογισμικού. Το πακέτο αυτό περιλαμβάνει έναν LDAP εξυπηρετητή, έναν LDAP αντίγραφο εξυπηρετητή, εφαρμογές για τον πελάτη και βιβλιοθήκες για το πρωτόκολλο. Το LDAP πρωτόκολλο χρησιμοποιείται για πρόσβαση σε καταλόγους δεδομένων και αξιοποιεί το πρωτόκολλο TCP/IP. Οι κατάλογοι στο LDAP αποθηκεύουν τις πληροφορίες με ένα μοναδικό όνομα και συγκεκριμένα χαρακτηριστικά. Οι εγγραφές στον κατάλογο είναι αποθηκευμένες με ιεραρχική δομή [13,14].

Το LDAP ακολουθεί την αρχιτεκτονική του μοντέλου CLIENT/SERVER. Ο LDAP εξυπηρετητής εμπεριέχει τα δεδομένα των καταλόγων του πρωτοκόλλου. Ο LDAP πελάτης θέτει «ερωτήματα» προς τον LDAP εξυπηρετητή για να λάβει δεδομένα – πληροφορίες σχετικά με τους υπολογιστικούς πόρους που διαχειρίζεται το υπολογιστικό πλέγμα. Από την πλευρά του, ο LDAP εξυπηρετητής στέλνει τα δεδομένα πίσω στον πελάτη ή τον ενημερώνει για την ακριβή θέση των δεδομένων (στην περίπτωση που είναι αποθηκευμένα σε άλλον LDAP εξυπηρετητή). Στα σχήματα που ακολουθούν 2.2.3(α) και 2.2.3(β), παρουσιάζεται η ακριβή δομή ενός καταλόγου LDAP και η πιο απλή αρχιτεκτονική ενός LDAP μοντέλου CLIENT/SERVER.

Σχήμα 2.2.3 (α): Δομή καταλόγου LDAP



Σχήμα 2.2.3(β): Μοντέλο client-server LDAP

2.2.4 GridFTP

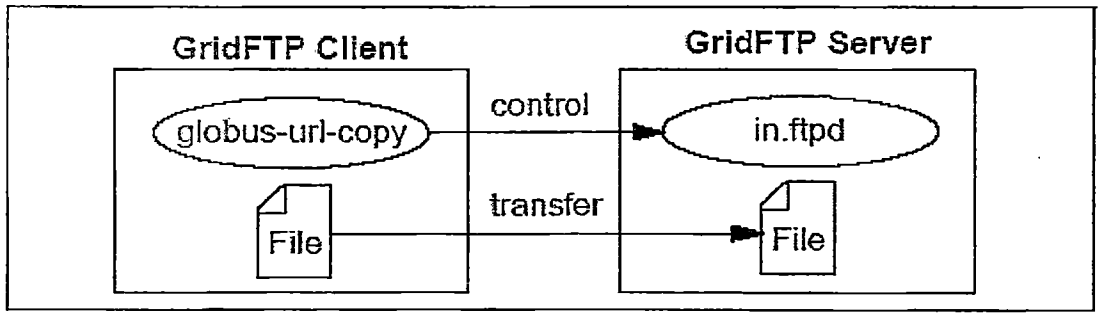
Το πρωτόκολλο GridFTP παρέχει ασφαλή και αξιόπιστη μεταφορά δεδομένων μεταξύ των οντοτήτων του υπολογιστικού πλέγματος. Το GridFTP βασίζεται στο πρωτόκολλο FTP και οι δραστηριότητες του επεκτείνονται στις παρακάτω υπηρεσίες:

- Μεταφορά πολλαπλής ακολουθίας δεδομένων (multi-streamed transfer)
- Auto- tuning
- Ασφάλεια (Globus Security)

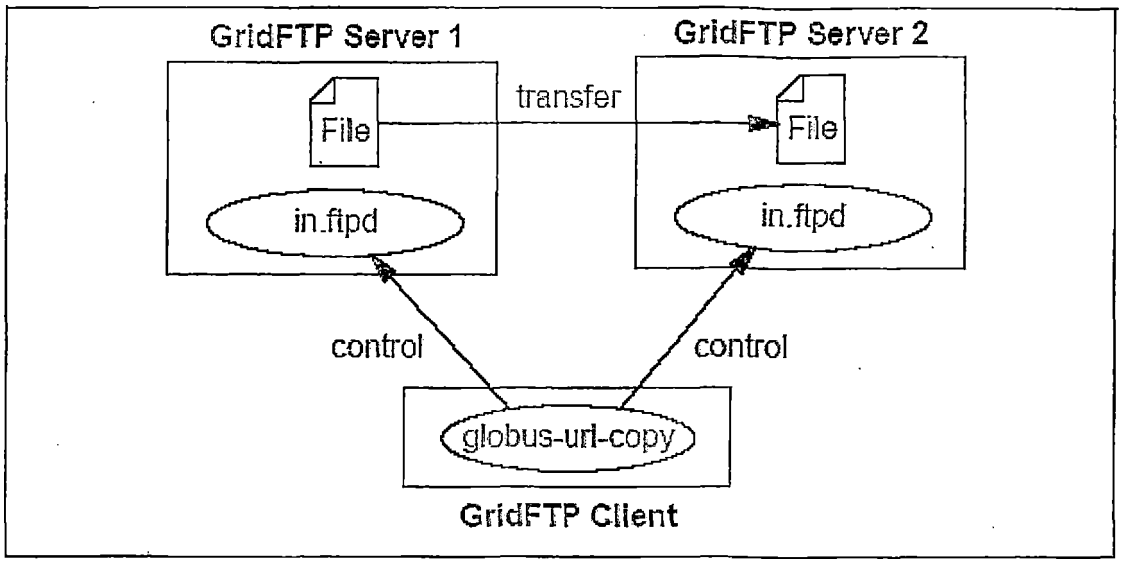
Την δεδομένη χρονική στιγμή, οι επιπλέον υπηρεσίες που παρέχονται από το πρωτόκολλο GridFTP είναι υπό – δοκιμή. Το Globus Toolkit υποστηρίζει ότι σύντομα οι επιπλέον υπηρεσίες και δυνατότητες του πρωτοκόλλου θα διανεμηθούν προς τους χρήστες υπολογιστικών πλεγμάτων.

GridFTP Server & Client: Το Globus Toolkit παρέχει δύο οντότητες τον GridFTP Client και τον GridFTP Server. Ο GridFTP Server δημιουργείται με την εντολή "in.ftpd" και ο GridFTP Client δημιουργείται με την εντολή "globus-url-copy". Τόσο ο GridFTP Server όσο και ο GridFTP Client υποστηρίζουν 2 είδη μεταφοράς αρχείων: το "βασικό" και τις "τρίτης- οντότητας". Ο βασικός τρόπος μεταφοράς δεδομένων λαμβάνει μέρος όταν ο πελάτης στέλνει ένα τοπικό αρχείο προς τον απομακρυσμένο υπολογιστή (στον τελευταίο τρέχει ο GridFTP Server).

Η μεταφορά αρχείων "τρίτης οντότητας" λαμβάνει μέρος όταν το μέγεθος του αρχείου είναι αρκετά μεγάλο ή ο πελάτης επιθυμεί το αρχείο να έχει αντίγραφα και σε άλλων εξυπηρετητή. Τα σχήματα 2.2.4 (α) και 2.2.4 (β) παρουσιάζουν τις αρχιτεκτονικές της "βασικής" και της "τρίτης οντότητας" μεταφοράς δεδομένων.



Σχήμα 2.2.4 (α): "Βασική" μεταφορά δεδομένων



Σχήμα 2.2.4 (β): "Τρίτης οντότητας" μεταφορά δεδομένων

2.3 Υλοποίηση Αρχιτεκτονικών Υπολογιστικού Πλέγματος (Globus Toolkit)

Ο σχεδιασμός μίας αρχιτεκτονικής υπολογιστικού πλέγματος δεν μπορεί να είναι αποδοτικός όταν καθορίζουμε μόνο διαδικασίες εγκατάστασης λογισμικού και δέσμευσης υπολογιστικών πόρων. Το σχέδιο που θα προταθεί πρέπει να ξεκινάει από τον καθορισμό εκείνων των αναγκών που έρχεται να «καλύψει» το υπολογιστικό πλέγμα. Το Globus Toolkit υποστηρίζει πως οι παρακάτω ανάγκες – απαιτήσεις πρέπει να λαμβάνονται υπόψη από τους σχεδιαστές αρχιτεκτονικών υπολογιστικών πλεγμάτων [10,15]:

1. Επιχειρησιακές Ανάγκες (Business Requirements)
2. Γεωγραφικοί Περιορισμοί (Geographical Constraints)
3. Δικτυακές Απαιτήσεις (Network Connectivity Requirements)
4. Απαιτήσεις Χρηστών (Users needs)

Ένας εύκολος τρόπος για να ξεκινήσει ο σχεδιασμός είναι μέσω της υλοποίησης ενός ασφαλούς υπολογιστικού μοντέλου. Βάσει του Globus Toolkit, ένα ασφαλή υπολογιστικό μοντέλο χτίζεται πάνω σε ένα πλαίσιο εργασίας «Υποδομής Δημοσίου Κλειδιού» (Public Key Infrastructure, PKI). Όταν ο τύπος του υπολογιστικού πλέγματος, η τοπολογία και το μοντέλο ασφάλειας έχουν οριστεί, μόνο τότε οι σχεδιαστές συνεχίζουν την ολοκλήρωση του συνόλου της αρχιτεκτονικής του υπολογιστικού πλέγματος σε υψηλότερα επίπεδα. Επιπλέον, λόγω της φύσης του υπολογιστικού πλέγματος, αποφάσεις σχεδιασμού πρέπει να παρθούν νωρίς σχετικά με την δικτυακή και υλική υποδομή καθώς και με τις επιπτώσεις της τελευταίας στον τομέα ασφάλειας.

2.3.1 Στόχοι Σχεδιασμού Υπολογιστικού Πλέγματος

Οι στόχοι σχεδιασμού παρέχουν το βασικό πλαίσιο εργασίας της υποδομής του υπολογιστικού πλέγματος. Για να καθορίσουμε τους στόχους σχεδιασμού πρέπει να

προχωρήσουμε στην καταγραφή των ιδιοτήτων και χαρακτηριστικών συγκεκριμένων περιοχών (για παράδειγμα, περιοχή ασφάλειας). Οι τρεις βασικές περιοχές που αφορούν το σχεδιασμό ενός υπολογιστικού πλέγματος είναι η περιοχή της ασφάλειας, της διαθεσιμότητας και της απόδοσης.

Από την στιγμή που οι στόχοι σχεδιασμού έχουν οριστεί, ακολουθεί μια διαδικασία διαχωρισμού τους σε ανεξάρτητα υπό-συστήματα. Η παραπάνω διαδικασία μας επιτρέπει να εργαζόμαστε με παράλληλο τρόπο. Όταν ολοκληρωθεί η διαδικασία καταγραφής των υπό-συστημάτων του υπολογιστικού πλέγματος, οι σχεδιαστές εστιάζουν στις νέες απαιτήσεις που δημιουργούνται ανά υπό-συστήματα.

Όταν τα βασικά συστατικά του υπολογιστικού συστήματος έχουν κατασκευαστεί ακολουθεί μια διαδικασία επαλήθευσης των στόχων σχεδιασμού συγκριτικά με τις απαιτήσεις των πελατών. Η παραπάνω διαδικασία είναι ιδιαίτερα κρίσιμη αφού οι σχεδιαστές του συστήματος πρέπει να καθορίσουν την υλισμική υποδομή (hardware&software) βάση των απαιτήσεων των πελατών. Στη συνέχεια ακολουθεί ο καθορισμός των στόχων σχεδιασμού ανά περιοχή του υπολογιστικού πλέγματος.

Ασφάλεια (security): Σε ένα ανοιχτό δικτυακό περιβάλλον υπάρχει μεγάλη πιθανότητα να προκληθούν σφάλματα σε επίπεδο υποδομής, εφαρμογής, διαχείρισης και παραμετροποίησης. Για να μειώσουμε την πιθανότητα εμφάνισης σφαλμάτων, καθορίζουμε τους στόχους ασφάλειας. Ο βασικός στόχος ασφάλειας είναι η εξέταση των απαιτήσεων ασφάλειας και η υλοποίηση των τελευταίων με τα απαραίτητα πληροφοριακά εργαλεία και διαδικασίες για τη μείωση του ρίσκου.

Οι απαιτήσεις ασφαλείας διαφοροποιούνται βάσει των πληροφορικών συστημάτων. Για παράδειγμα, οι απαιτήσεις ασφαλείας για το πληροφοριακό σύστημα μιας τράπεζας είναι πολύ περισσότερες από αυτές που απαιτούνται για έναν ακαδημαϊκό οργανισμό που ασχολείται με την ερεύνα και ανάπτυξη εφαρμογών.

Το Globus Toolkit υποστηρίζει το OGSA (Oren Grid Security Architecture). Το PKI αποτελεί την περιοχή που στηρίζεται ο αρχικός σχεδιασμός ασφάλειας. Παρόλα αυτά, ιδιαίτερη προσοχή πρέπει να δοθεί στις οντότητες ασφαλείας (αναχώματα ασφαλείας-firewall, συστήματα ανιχνεύσεις εισβολών, αντί-ιοικά συστήματα) και στις διαδικασίες διαχείρισης των τελευταίων. Τα πιο κρίσιμα ζητήματα ασφαλείας που αφορούν το σχεδιασμό του υπολογιστικού πλέγματος είναι:

- Ποιο είναι το μέρος που θα τοποθετηθεί η CA (Certificate Authority) και πως θα τη διαχειριστούμε;
- Πως θα γίνει διαχείριση των διαδικασιών ασφαλείας στους τοπικούς εξυπηρετητές;
- Θα εφαρμοστούν διαδικασίες διαβάθμισης των χρηστών ή όχι (Delegation Procedure);
- Το λογισμικό που τρέχει σε κρίσιμα συστατικά του υπολογιστικού πλέγματος είναι αξιόπιστο ή όχι;
- Οι διαδικασίες ασφάλειας είναι αρκετά παραμετροποιήσημες έτσι ώστε να μπορούν να συμβαδίζουν με διαδικασίες ασφαλείας "εξωτερικών" υπολογιστικών πλεγμάτων;
- Μέχρι πιο σημείο παρεμβάλετε ο ανθρώπινος παράγοντας στις διαδικασίες ασφάλειας;

- Οι διαδικασίες ασφάλειας είναι φιλικές προς τον χρήστη (μέσω των GUI Graphical User Interfaces);

Διαθεσιμότητα (Availability): Ένας από τους σημαντικότερους στόχους σχεδιασμού του υπολογιστικού πλέγματος και γενικότερα του πληροφορικού συστήματος είναι η διαθεσιμότητα των παρεχομένων υπηρεσιών. Για να εξασφαλίσουμε τη διαθεσιμότητα των υπηρεσιών σε ένα υπολογιστικό πλέγμα είναι απαραίτητο να καθορίσουμε εκείνα τα σημεία του πλέγματος που είναι ευάλωτα σε επιθέσεις-εισβολές καθώς και το μέγεθος των υπολογιστικών πόρων που είναι διαθέσιμο για κρίσιμες καταστάσεις (για παράδειγμα όταν προκύψει ένα ρήγμα ασφαλείας). Όσο υψηλός και αν είναι ο βαθμός αξιοπιστίας των οντοτήτων ενός υπολογιστικού πλέγματος δεν θα μπορέσουμε να αποφύγουμε καταστάσεις αποτυχίας. Ο στόχος είναι ο καθορισμός των διαδικασιών εκείνων που θα διαχειρίζονται καταστάσεις σφαλμάτων.

Οποιαδήποτε και αν είναι τα σενάρια διαθεσιμότητας υπηρεσιών, σε όλα εμπεριέχεται ο καθορισμός του όγκου της διαθεσιμότητας που απαιτείται από το σύστημα για να λειτουργήσει. Για να επιτευχθεί η παραπάνω διαδικασία πρέπει να καταγραφούν όλες οι κρίσιμες οντότητες του συστήματος, οι οποίες θα πρέπει να τροποποιηθούν με τέτοιο τρόπο έτσι ώστε είναι "ανεκτικές" σε εισβολές και σε σφάλματα. Όταν οι παραπάνω οντότητες έχουν αναγνωριστεί από τους σχεδιαστές του υπολογιστικού πλέγματος τότε ελέγχονται συγκεκριμένες επιλογές διαθεσιμότητας για αυτές τις οντότητες του πληροφοριακού συστήματος.

Ένα ακόμα σημαντικό ζήτημα, που πρέπει να λάβουν υπόψη τους οι σχεδιαστές του υπολογιστικού πλέγματος, είναι η διαθεσιμότητα των υπολογιστικών πόρων που δεσμεύονται δυναμικά σε ένα grid περιβάλλον. Το υπολογιστικό πλέγμα δεν είναι ένα σταθερό περιβάλλον που οι υπολογιστικοί πόροι δεν μεταβάλλονται. Το Globus Toolkit υποστηρίζει ότι οι υπολογιστικοί πόροι μεταβάλλονται βάσει των ενεργών μελών και γενικότερα αυτών που συμμετέχουν στο υπολογιστικό πλέγμα. Όταν οι υπολογιστικοί πόροι θα ενεργοποιούνται – καταγράφονται από τις "υπηρεσίες πληροφοριών" (GIIS), οι τελευταίες ενημερώνουν το σύστημα για την κατάσταση των υπολογιστικών πόρων.

Οι οντότητες μέσα σε ένα υπολογιστικό πλέγμα απαιτούν, λόγω της διαφορετικότητας της υποδομής τους, διαφορετικά επίπεδα διαθεσιμότητας. Συνήθως τις οντότητες του συστήματος τις διαχωρίζουμε σε "οντότητες του υπολογιστικού πλέγματος" και σε "οντότητες υποδομής" (infrastructure components). Η κάθε κατηγορία οντοτήτων έχει διαφορετικές απαιτήσεις διαθεσιμότητας. Οι σχεδιαστές του υπολογιστικού πλέγματος πρέπει να λάβουν υπόψη τους τις απαιτήσεις διαθεσιμότητας ανά οντότητα και να διαχωρίσουν τις οντότητες σε κρίσιμες και μη κρίσιμες. Η παρακάτω λίστα περιέχει παραδείγματα πόρων που θέτονται στη διάθεση των σχεδιαστών και πρέπει να ληφθούν υπόψη από τους σχεδιαστές:

- Υλισμικό υπολογιστικού πλέγματος (Grid middleware)
  - Διαχειριστής εργασιών
  - Υπηρεσίες καταλόγου
  - Υπηρεσίες ασφαλείας
  - Αποθηκευτικός χώρος
  - Συμπλέγματα λογισμικού (Grid software clustering)

- Δίκτυα (Networks)
  - Ισορροπία δικτυακών πόρων
  - Υψηλή διαθεσιμότητα πρωτοκόλλων εξυπηρετητών
  - Επιλογή δικτυακών "μονοπατιών"
- Υπηρεσίες δεδομένων (Data store)
  - Αντίγραφα δεδομένων
  - Παράλληλη επεξεργασία
- Διαχείριση συστημάτων (Systems management)
  - Διαδικασίες αντιγραφής αρχείων
  - Διαδικασίες ανάκαμψης
  - Αντίγραφα LDAP
  - Παρακολούθηση "συναγερμών" που προκύπτουν από σφάλματα στο πληροφοριακό περιβάλλον
- Ασφάλεια (Security)
  - "Ανεκτικά αναχώματα" ασφαλείας σε θέματα άρνησης υπηρεσιών

Πολύ συχνά διαφορετικές οντότητες του συστήματος αποτυγχάνουν και ως αποτέλεσμα το ποσοστό διαθεσιμότητας υπηρεσιών θα μειώνεται. Το Globus Toolkit υποστηρίζει την επιλογή πολλαπλών αντιγράφων του λογισμικού και του υλικού για την αντιμετώπιση τέτοιων σεναρίων. Βέβαια η επιλογή μιας λύσης αντιγράφων αυξάνει το συνολικό κόστος της υποδομής του υπολογιστικού πλέγματος. Είναι καθαρά ζητήματα της εταιρίας να υπολογίσει τα κέρδη που της παρέχει το πληροφοριακό περιβάλλον (για παράδειγμα, να αύξηση το ποσοστό διαθεσιμότητας των υπηρεσιών από 99,9% σε 99,99%).

Για να γίνουν κατανοητοί οι στόχοι διαθεσιμότητας, οι παρακάτω λίστα παρουσιάζει τη διαθεσιμότητα ενός πληροφορικού συστήματος για ένα ολόκληρο χρόνο:

- Διαθεσιμότητα εμπορικού συστήματος: 99-99,5%, το σύστημα δεν παρέχει υπηρεσίες για 43,8 - 87,6 ώρες
- Υψηλή διαθεσιμότητα: 99,9%, το σύστημα δεν παρέχει υπηρεσίες για 8,8 ώρες
- Αξιόπιστο σε σφάλματα: 99.9%, το σύστημα δεν παρέχει υπηρεσίες για 53 λεπτά
- Ανεκτικό σε σφάλματα και εισβολές: 99,999%, το σύστημα δεν παρέχει υπηρεσίες για 5 λεπτά

Απόδοση (Performance): Όσον αφορά τον τομέα της απόδοσης, οι σχεδιαστές του υπολογιστικού πλέγματος πρέπει να αξιοποιήσουν συνολικά τους υπολογιστικούς πόρους. Όταν η εφαρμογή μπορεί να εκμεταλλευθεί πολλαπλούς υπολογιστικούς πόρους, ο σχεδιασμός της επιτρέπει το διαχωρισμό της σε πολλά μικρά μέρη που κατανέμονται ισόποσα στο υπολογιστικό πλέγμα. Μέσω «έξυπνων» τεχνικών διαχείρισης εργασιών (workload management) η εφαρμογή είναι σε θέση να εκμεταλλευθεί οποιοδήποτε διαθέσιμο υπολογιστικό πόρο στο grid.

2.4 Μοντέλα Αρχιτεκτονικής Υπολογιστικών Πλέγματος

Υπάρχουν διαφορετικοί τύποι υπολογιστικού πλέγματος που πληρούν διαφορετικές επιχειρήσιακές ανάγκες. Μερικά Grid σχεδιάζονται για την αξιοποίηση επιπλέον υπολογιστικών πόρων ενώ άλλα υποστηρίζουν την συνεργασία μεταξύ πολλών διαφορετικών οργανισμών. Επομένως, μονό όταν έχουν αναγνωριστεί οι επιχειρησιακές ανάγκες οι σχεδιαστές του συστήματος επιλεγούν τον κατάλληλο τύπο του υπολογιστικού πλέγματος.

Η επιλογή του καταλλήλου υπολογιστικού πλέγματος έχει άμεση επίδραση στους στόχους σχεδιασμού που θέτονται για το υπολογιστικό πλέγμα (βλέπε υπο-ενότητα 2.3). οι βασικοί τύποι υπολογιστικού πλέγματος είναι το "Data grid" και το "Computational grid". Το Globus Toolkit υποστηρίζει και τα δύο είδη υπολογιστικού πλέγματος.

2.4.1 Computational grid

Ένα computational grid έχει ως σκοπό τη συνάθροιση υπολογιστικής ισχύς από κατανεμημένα συστήματα. Ένα πολύ γνωστό παράδειγμα computational grid είναι το SETI@home υπολογιστικό πλέγμα. Οι υπολογιστές που συμμετέχουν στο SETI@home υπολογιστικό πλέγμα συνδυάζουν υπολογιστική ισχύ για την ανάλυση σημάτων που λαμβάνονται από το διάστημα. Το πληροφοριακό έργο αυτό ονομάζεται "Search for Extra Terrestrial Intelligence" [2].

Οι περισσότερες επιχειρήσεις που ενδιαφέρονται για computational grid συνήθως η πληροφοριακή υποδομή τους έχει κοινά στοιχεία. Στόχος των επιχειρήσεων είναι η επέκταση των δυνατοτήτων τους και η αξιοποίηση όλων και περισσοτέρων υπολογιστικών πόρων μέσω των τεχνικών "συνάθροισης" και "διαμοίρασης". Επιπρόσθετα, οι επιχειρήσεις ενδιαφέρονται για την μετατροπή των υπαρχόντων εφαρμογών τους σε εφαρμογές με παράλληλες επεξεργαστικές δυνατότητες. Τα computational grids παρέχουν υπηρεσίες όπως μαθηματικές εξισώσεις, αποτελέσματα αξιοποίησης πόρων, διαδικασίες αξιολόγησης κόστους και προσομοίωσης. Θα υπάρξουν περιπτώσεις στις οποίες το μοντέλο αρχιτεκτονικής υπολογιστικού πλέγματος δεν θα είναι συμβατό με εφαρμογές "πραγματικού χρόνου" (για παράδειγμα, παράλληλη επεξεργασία εργασιών).

Τα βασικά χαρακτηρίστηκα βάσει των οποίων αναγνωρίζουμε ένα computational grid είναι:

- Χρήση πολλών cluster οντοτήτων
- Διαδικασίες οργάνωσης και εκμετάλλευσης των επεξεργαστών για την καλύτερη αξιοποίηση των υπολογιστικών πόρων
- Παροχή υπολογιστικής ισχύς για μεγάλης κλίμακας εργασίες
- Ικανοποίηση των επιχειρησιακών απαιτήσεων για άμεση πρόσβαση στους υπολογιστικούς πόρους

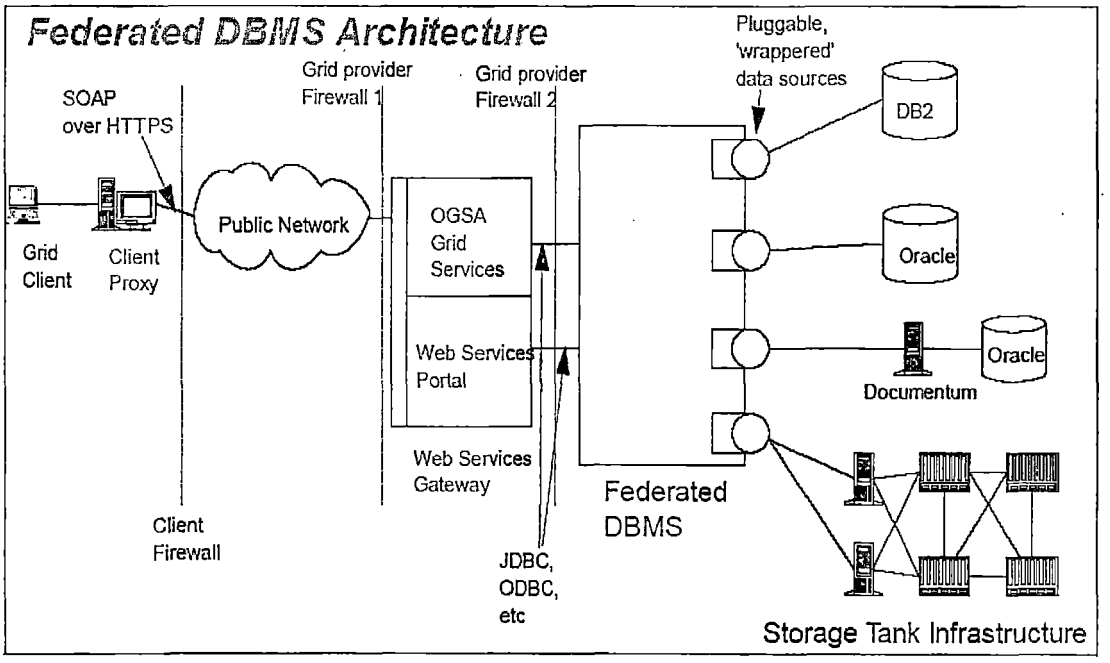
Το βασικό πλεονέκτημα των computational grids είναι το "Μειωμένο Κόστος Ιδιοκτήτη" (Total Cost of Ownership, TCO) αφού η επιχείρηση επεκτείνει τις πληροφοριακές δυνατότητες και υπηρεσίες της χωρίς να διογκώνεται η πληροφοριακή υποδομή της. Εκτός από το SETI@home υπολογιστικό πλέγμα, άλλοι τύποι computational grids "TeraGrid" (Distributed Terascale Facility), UK και

"Netherlands grids". Η επόμενη γενιά των computational grids θα εστιάσει στην επίλυση υπολογιστικών προβλημάτων πραγματικού χρόνου.

2.4.2 Data grid

Ενώ τα computational grids συνδυάζουν διαδικασίες αξιοποίησης των υπολογιστικών πόρων, τα data grids εστιάζουν στο να παρέχουν ασφαλή πρόσβαση σε κατανεμημένες-ετερογενείς "πισίνες δεδομένων" (Data Pools). Μέσω της διασυνεργασίας, τα data grids περιλαμβάνουν μια "ομοσπονδιακή βάση δεδομένων". Η βάση δεδομένων ονομάζεται ομοσπονδιακή επειδή αποτελείται από μια ομάδα βάσεων δεδομένων και οι τελευταίες δημιουργούν μια ιδεατή βάση δεδομένων [2].

Επιπλέον, τα data grids ενοποιούν δεδομένα, αποθηκευτικούς πόρους και δικτυακούς πόρους που βρίσκονται σε διαφορετικούς τομείς του υπολογιστικού πλέγματος. Τα data grids στηρίζονται τόσο σε τοπικές όσο και σε παγκόσμιες πολιτικές. Οι πολιτικές αυτές αφορούν τον τομέα της ασφάλειας, τον τομέα διαχείρισης υπολογιστικών πόρων και τον τομέα βελτίωσης των συνθηκών της δικτυακής υποδομής. Στο σχήμα 2.4.2 που ακολουθεί παρουσιάζεται η υποδομή και η αρχιτεκτονική μιας "ομοσπονδιακής" βάσης δεδομένων.



Σχήμα 2.4.2: "Ομοσπονδιακή" βάση δεδομένων

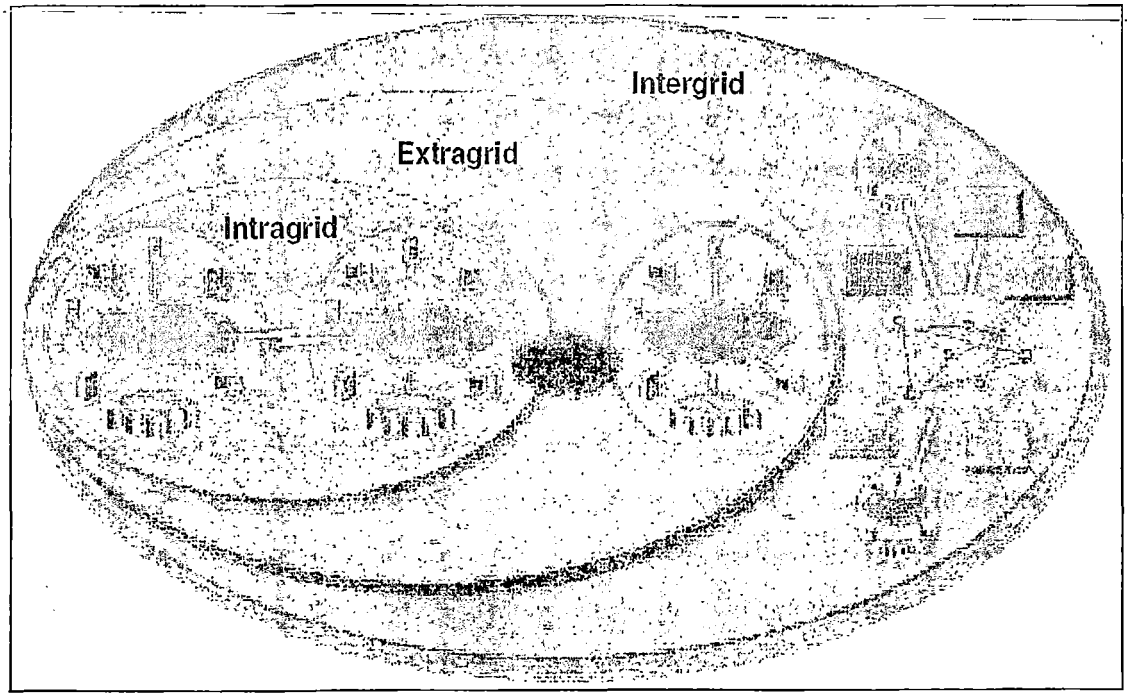
2.5 Τοπολογίες Υπολογιστικού Πλέγματος

Ανεξάρτητα από τον τύπο του υπολογιστικού πλέγματος (βλέπε υπο-ενότητα 2.4) έχουμε και την τοπολογία ή διαφορετικά το μέγεθος εκείνο που μπορεί να επεκταθεί ένα υπολογιστικό πλέγμα [15]. Οι παρακάτω τοπολογίες καλύπτουν ολόκληρο το φάσμα των υπολογιστικών πόρων:

- Intragrids
  - Απλή οργανισμοί

- Απλή υποδομή clusters
- Χωρίς την συμμετοχή συνεργατών (πληροφοριακά συστήματα άλλων επιχειρήσεων)

- Extragrids
  - Πολλαπλή οργανισμοί
  - Συμμετοχή συνεργατών
  - Σύνθετη αρχιτεκτονική clusters
- Intergrids
  - Οργανισμοί που συμμετέχουν στο υπολογιστικό πλέγμα σε παγκόσμιο επίπεδο
  - Πολλαπλά πληροφοριακά συστήματα που συμμετέχουν στο υπολογιστικό πλέγμα, μεγάλη επεξεργαστική ισχύς
  - Ακόμη πιο σύνθετη αρχιτεκτονική από clusters



Σχήμα 2.5: Intragrids, extragrids και intergrids

Η πιο απλή τοπολογία από τις τρεις προαναφερθείσες είναι η Intragrid , επειδή εφαρμόζει ένα μικρό μέρος των υπηρεσιών του υπολογιστικού πλέγματος σε ένα πληροφοριακό σύστημα. Η πολυπλοκότητα ενός σχεδίου υπολογιστικού πλέγματος αυξάνεται όσο το πλήθος των οργανισμών και οι γεωγραφικοί παράμετροι και περιορισμοί αυξάνονται. Πιο συγκεκριμένα, όταν ένας νέος οργανισμός συνδέεται στο υπολογιστικό πλέγμα, οι μη λειτουργικές και οι λειτουργικές απαιτήσεις για την ασφάλεια, τις υπηρεσίες καταλόγου, τη διαθεσιμότητα και την απόδοση είναι πιο πολύπλοκες.

Η διαμοίραση υπολογιστικών πόρων στο grid δεν είναι μια απλή ανταλλαγή αρχείων αλλά μια άμεση πρόσβαση σε υπολογιστικά μηχανήματα, λογισμικό, δεδομένα και άλλους πόρους. Οι πολιτικές που θα εφαρμοστούν για να επιτευχθεί η παραπάνω διαμοίραση ποικίλουν ανάλογα με την τοπολογία του υπολογιστικού πλέγματος. Οι

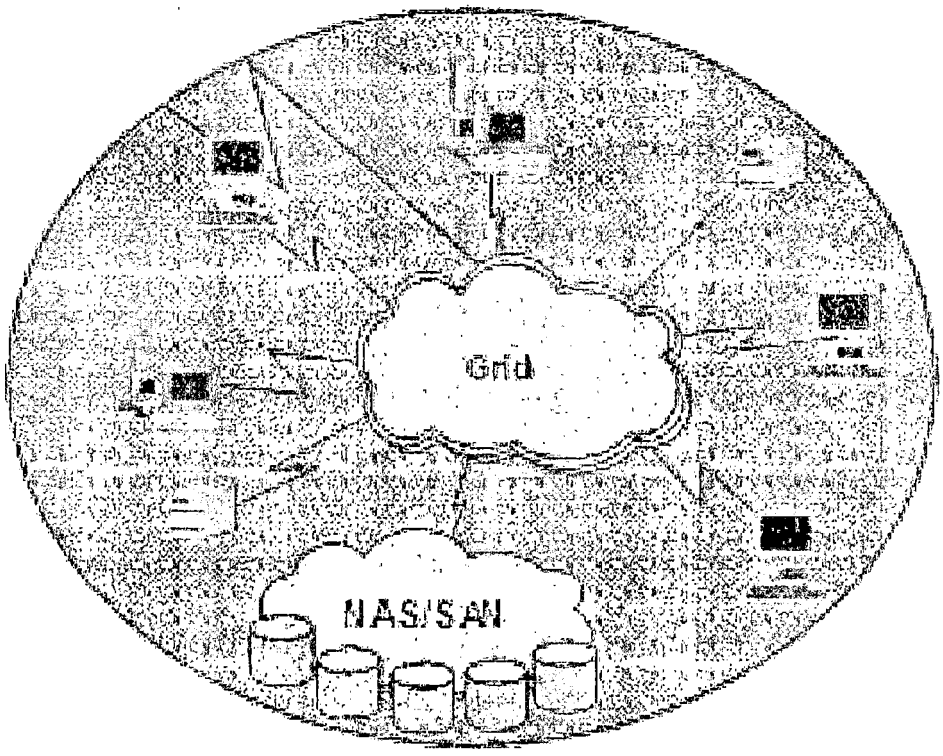
πολιτικές αυτές καθορίζουν τους πόρους που θα είναι διαθέσιμοι, ποιοι χρήστες θα έχουν πρόσβαση στους πόρους και υπό ποιες συνθήκες.

2.5.1 Intragrid

Για να επιτευχθεί μια τοπολογία intragrid απαιτείται ένας μικρός αριθμός υπολογιστών που θα μοιράζονται δεδομένα σε ένα ιδιωτικό δίκτυο και θα ελέγχονται από τον ίδιο τομέα ασφαλείας. Τα βασικά χαρακτηριστικά του intragrid είναι:

- Υψηλό εύρος δικτύου (High bandwidth)
- Διαθεσιμότητα (Availability)
- Συμβατότητα στις υπηρεσίες ασφάλειας
- Εύχρηστο περιβάλλον

Σε μια τοπολογία intragrid είναι ευκολότερο να σχεδιαστεί τόσο το "computational grid" όσο και το "data grid" (βλέπε ενότητα 2.4). Οι περισσότερες επιχειρήσεις, που είναι νέες στην περιοχή του υπολογιστικού πλέγματος, προτιμούν να ξεκινήσουν με μια intragrid τοπολογία. Στο σχήμα 2.5.1 παρουσιάζεται μια intragrid τοπολογία.



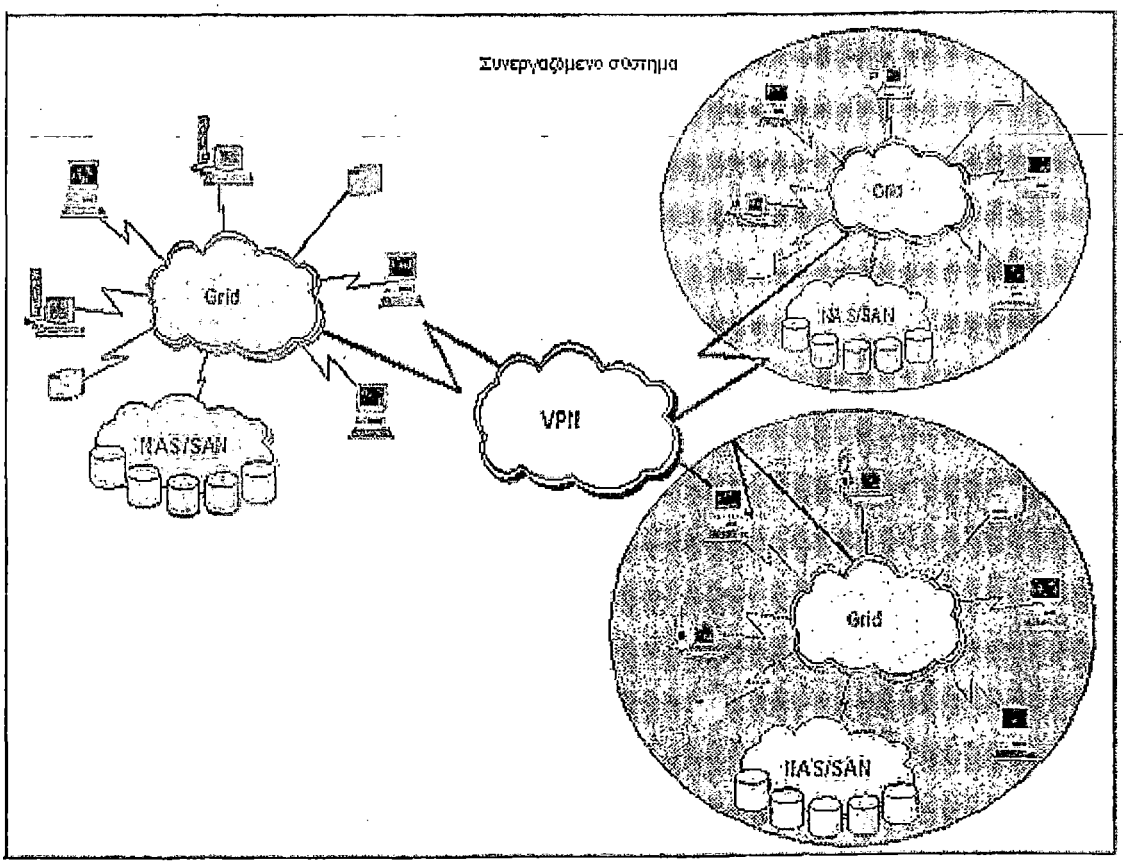
Σχήμα 2.5.1: Intragrid

2.5.2 Extragrid

Η τοπολογία extragrid στηρίζεται σε έναν οργανισμό όπως και το intragrid. Η βασική διαφορά είναι ότι στην τοπολογία extragrid επικοινωνούν, συνδέονται δύο ή και περισσότερα intragrids. Η τοπολογία extragrid, όπως φαίνεται και στο σχήμα 2.5.2, περιλαμβάνει περισσότερους από έναν παροχέα ασφαλείας ενώ ταυτόχρονα η διαχείριση των οντοτήτων του υπολογιστικού πλέγματος αυξάνει. Τα βασικά χαρακτηριστικά μιας τοπολογίας extragrid είναι:

- Κατανεμημένη ασφάλεια (dispersed security)
- Πολλαπλοί οργανισμοί
- Απομακρυσμένη συνδεσιμότητα (remove/WAN connectivity)

Σε μια τοπολογία extragrid, οι υπολογιστικοί πόροι έχουν δυναμική μορφή και οι μηχανισμοί του υπολογιστικού πλέγματος πρέπει να αντιδρούν άμεσα, στις αστοχίες του συστήματος. Μια επιχείρηση θα μπορούσε να εφαρμόσει μια τοπολογία extragrid στην περίπτωση μιας B2B στρατηγικής (Business to Business Strategy) [15].



Σχήμα 2.5.2: Extragrid

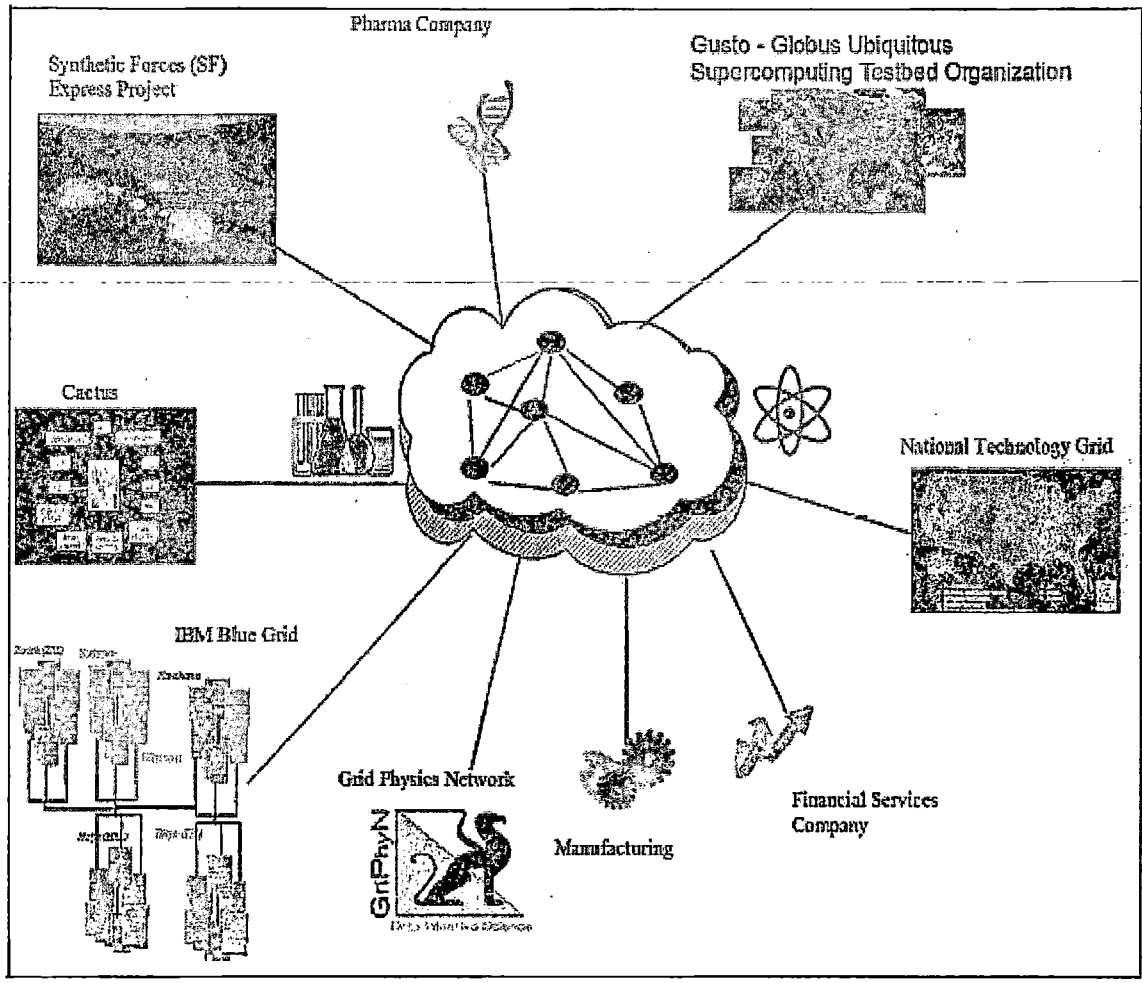
2.5.3 Intergrid

Η τοπολογία intergrid απαιτεί την δυναμική «επικοινωνία» των εφαρμογών, των πόρων και των υπηρεσιών με συνεργάτες, πελάτες και οποιοδήποτε άλλων εξουσιοδοτημένων οργανισμών που θα αποκτήσουν πρόσβαση στο grid μέσω του διαδικτύου ή ενός δικτύου. Όπως φαίνεται στο σχήμα 2.5.3 η τοπολογία intergrid χρησιμοποιείται από εταιρίες πληροφοριακών συστημάτων που συνεργάζονται με εταιρίες σε απομακρυσμένα γεωγραφικά σημεία. Τα βασικά χαρακτηριστικά μιας τοπολογίας intergrid είναι:

- Κατανεμημένοι μηχανισμοί ασφαλείας (dispersed security)
- Πολλαπλοί οργανισμοί

- Απομακρυσμένη συνδεσιμότητα (remove/WAN connectivity)

Σε μια τοπολογία intergrid, οι υπολογιστικοί πόροι είναι παγκόσμια δημοσία δεδομένα και οι εφαρμογές πρέπει να παραμετροποιηθούν προς όλες τις διαστάσεις έτσι ώστε να καλύπτουν τις ανάγκες του «παγκόσμιου» κοινού. Οι επιχειρήσεις ίσως θεωρήσουν απαραίτητη μια τοπολογία intergrid εάν υπάρχει ανάγκη για peer-to-peer εφαρμογές προς όλες τις κατευθύνσεις [15].



Σχήμα 2.5.3: Intergrid

2.5.4 E-utilities

Αντί μία επιχείρηση να αγοράσει και να συντηρήσει ακριβές πλατφόρμες υλικού και λογισμικού, της παρέχεται η δυνατότητα αγοράς «Διαδικτυακών υπηρεσιών» υπολογιστικού πλέγματος από τρίτους. Με αυτό τον τρόπο η επιχείρηση απαλλάσσεται από την πολυπλοκότητα των διαδικασιών διαχείρισης και ασφάλειας του υπολογιστικού πλέγματος.

Τα χαρακτηριστικά ενός τέτοιου μοντέλου περιλαμβάνουν κατανεμημένα και διαμοιρασμένα πληροφοριακά περιβάλλοντα. Οι βασικές ιδιότητες ενός πληροφοριακού περιβάλλοντος που παρέχει διαδικτυακές υπηρεσίες είναι οι πολλαπλοί αποθηκευτικοί χώροι για την εξυπηρέτηση πολλών χρηστών, υψηλή διαθεσιμότητα υπηρεσιών όλο το 24ώρο, παροχή βαθμωτών υπηρεσιών, διαχείριση

κατανεμημένων συστημάτων και η τιμολόγηση των υπηρεσιών βάσει των υπολογιστικών πόρων που καταναλώθηκαν. Το σημαντικότερο πλεονέκτημα της τεχνικής διαδικτυακών υπηρεσιών υπολογιστικού πλέγματος είναι η μεγάλη ανταπόκριση που έχει τόσο στις επιχειρήσεις όσο και σε μεμονωμένους χρήστες.

2.6 Προτεινόμενη Μεθοδολογία και Βήματα

Η επιλογή του τύπου και της τοπολογίας του υπολογιστικού πλέγματος είναι το πρώτο βήμα του σχεδιασμού μιας αρχιτεκτονικής grid. Μια ολοκληρωμένη μεθοδολογία σχεδιασμού υπολογιστικού πλέγματος αποτελείται από συγκεκριμένες φάσεις-στάδια και δραστηριότητες. Οι δραστηριότητες που λαμβάνουν μέρος στην φάση του σχεδιασμού της αρχιτεκτονικής ενός grid περιλαμβάνουν, αναλυτική αναφορά των «αποφάσεων αρχιτεκτονικής» (Architectural decisions), καταγραφή της τρέχουσας πληροφοριακής υποδομής, δημιουργία ενός σχεδίου υλοποίησης και η διεξαγωγή συνεντεύξεων προσωπικού.

2.6.1 Βασική Μεθοδολογία

Οι σχεδιαστές ενός υπολογιστικού πλέγματος πρέπει να ακολουθήσουν μια βασική μεθοδολογία που θα επιτρέπει στο πλάνο σχεδιασμού να ακολουθήσει ένα «μονοπάτι» από την αρχή έως και την ολοκλήρωση του υπολογιστικού πλέγματος. Η μεθοδολογία που ακολουθείται δεν στηρίζεται σε πετυχημένες συνταγές – υλοποιήσεις ενός υπολογιστικού πλέγματος. Αντιθέτως οι σχεδιαστές του υπολογιστικού πλέγματος τη συμβουλεύονται και τηρούν τις βασικές αρχές της. Αμέσως τώρα παρατίθεται μία βασική μεθοδολογία υπολογιστικού πλέγματος [11,16]:

Κατανόηση των επιχειρησιακών αναγκών: Το πρώτο βήμα οποιουδήποτε σχεδιασμού υπολογιστικού πλέγματος είναι η αναγνώριση και η καταγραφή των επιχειρησιακών αναγκών ή της επιχειρησιακής στρατηγικής. Βάσει της επιχειρησιακής στρατηγικής θα επιλεχθεί ο τύπος, η τοπολογία του υπολογιστικού πλέγματος καθώς και θα διευκρινιστεί το συνολικό κόστος του πληροφοριακού έργου.

Συλλογή πληροφορικών απαιτήσεων: οι διαδικασίες συλλογής πληροφοριακών απαιτήσεων θα δώσουν μια νέα ώθηση στον σχεδιασμό της αρχιτεκτονικής, κυρίως βοηθώντας την τεχνική ομάδα να εργαστεί πιο αποδοτικά αφού πλέον θα ακολουθεί συγκεκριμένες οδηγίες. Οι κατηγορίες των πληροφορικών απαιτήσεων είναι οι παρακάτω:

- **Επιχειρησιακές απαιτήσεις**
  Οι επιχειρησιακές απαιτήσεις είναι περίπου παρόμοιες με τις επιχειρησιακές ανάγκες. Παρόλα αυτά, επειδή έχουμε περάσει στο σχεδιασμό του πληροφοριακού υπολογιστικού πλέγματος, οι επιχειρησιακές απαιτήσεις καθορίζουν σε μεγάλο βαθμό την απόδοση και την διαθεσιμότητα των υπηρεσιών.

- **Απαιτήσεις υποδομής**
  Ο τελικός σχεδιασμός της αρχιτεκτονικής της πληροφοριακής υποδομής καθορίζεται από τις απαιτήσεις υποδομής. Όταν αναφερόμαστε στις

απαιτήσεις υποδομής συνήθως περιλαμβάνονται οι περιορισμοί υποδομής (infrastructure constraints) καθώς και ένα σύνολο πολλών μεταβλητών που επηρεάζουν το σύνολο της αρχιτεκτονικής σε επίπεδο υλικού.

- **Απαιτήσεις εφαρμογών**
  Ένας ακόμα σημαντικός παράγοντας που πρέπει να προσδιοριστεί κατά τη διάρκεια του σχεδιασμού του υπολογιστικού πλέγματος είναι οι απαιτήσεις εφαρμογών. Αν η επιχείρηση δεν θέλει να προχωρήσει στην αλλαγή των υπαρχόντων εφαρμογών της, το πιο σημαντικό ερώτημα είναι αν θα μπορέσουν οι εφαρμογές αυτές να υιοθετήσουν χαρακτηριστικά υπολογιστικού πλέγματος. Μέχρι στιγμής, τόσο το Globus toolkit όσο και άλλες πλατφόρμες λογισμικού υπολογιστικού πλέγματος υποστηρίζουν εφαρμογές που μεταγλωττίζονται σε Windows και Unix περιβάλλοντα.

Επαλήθευση απαιτήσεων: Κατά τη διάρκεια του σχεδιασμού, οι απαιτήσεις μπορούν να αλλάξουν την τελευταία στιγμή, εκεί που οι σχεδιαστές του υπολογιστικού πλέγματος δεν το περιμένουν. Επομένως, πριν προχωρήσουμε στην εφαρμογή και υλοποίηση τους, είναι καλό να ακολουθηθεί μια διαδικασία επαλήθευσης των απαιτήσεων έτσι ώστε όλες οι οντότητες που συμμετέχουν στο υπολογιστικό πλέγμα να συμφωνούν με τις κατευθύνσεις που θέτει το πλάνο σχεδιασμού.

2.6.2 Προτεινόμενα Βήματα

Στην υπο-ενότητα 2.6.2 παραθέτονται επιπλέον προτεινόμενα βήματα (βάσει του Globus Toolkit) για τη βελτιστοποίηση του πλάνου σχεδιασμού. Τα προτεινόμενα βήματα είναι:

Δημιουργία εργαστηρίων υπολογιστικού πλέγματος: Στόχος των εργαστηρίων υπολογιστικού πλέγματος είναι να γίνουν κατανοητές προς όλους οι μεταβλητές, οι επιλογές και οι προβληματισμοί που αφορούν το σχεδιασμό της πληροφοριακής υποδομής του υπολογιστικού πλέγματος. Πολλές από τις τεχνολογίες υλικού και λογισμικού υπολογιστικού πλέγματος είναι νέες για το προσωπικό της εταιρίας ακόμη και για την ομάδα σχεδιασμού. Στα εργαστήρια υπολογιστικού πλέγματος λαμβάνουν μέρος σεμινάρια από ειδικούς σε θέματα τεχνολογιών πληροφορικής. Με αυτόν τον τρόπο όλοι όσοι δεν γνωρίζουν τις νέες τεχνολογίες του υπολογιστικού πλέγματος έρχονται σε πρώτη επαφή μαζί τους.

Αναφορές τεκμηρίωσης σχεδιασμού (documentation): ο καλύτερος τρόπος για να κρατήσουν επαφή οι σχεδιαστές του υπολογιστικού πλέγματος με το πλάνο σχεδιασμού είναι με την καταγραφή του τελευταίου. Η καταγραφή του πλάνου σχεδιασμού ξεκινάει από το υψηλότερο επίπεδο του πληροφοριακού συστήματος και σταδιακά κατεβαίνει στα πιο λεπτομερή διαγράμματα – παραμέτρους. Οι σχεδιαστές καταγράφουν στοιχεία όπως IP διευθύνσεις, ονόματα εξυπηρετητών, αρχιτεκτονικές εξυπηρετητών, δικτυακό υλικό και οποιαδήποτε άλλη πληροφορία είναι απαραίτητη για την ολοκλήρωση του πλάνου σχεδιασμού.

Στην πραγματικότητα, τα έγγραφα σχεδιασμού έχουν δυναμική μορφή, αλλάζουν όποτε αλλάζουν οι τεχνολογίες, οι επιχειρησιακές ανάγκες και οι ανάγκες των χρηστών. Γι' αυτό οι σχεδιαστές του υπολογιστικού πλέγματος πρέπει να ελέγχουν σε τακτά χρονικά διαστήματα ξανά και ξανά τα έγγραφα σχεδιασμού και να σημειώσουν

οποιεσδήποτε τροποποιήσεις-αναβαθμίσεις έχουν προκύψει. Η καταγραφή των στόχων σχεδιασμού πρέπει να είναι ακριβείς, διαφορετικά η ομάδα υλοποίησης του υπολογιστικού πλέγματος μπορεί εύκολα να παραπλανηθεί και το τελικό σύστημα να μην έχει σχεδιαστεί όπως το είχε ορίσει αρχικά η.

Πρωτότυπο (beta version of grid): Η κατασκευή μίας πρωτότυπης εφαρμογής υπολογιστικού πλέγματος μπορεί να κερδίσει σημαντικό χρόνο που διαφορετικά θα τον είχαμε σπαταλήσει σε διαδικασίες επιδιορθώσεις και ανακατασκευής των οντοτήτων του υπολογιστικού πλέγματος. Όταν κατασκευάζουμε μια πρωτότυπη εφαρμογή στόχος είναι να παραχθεί μια μικρή κλίμακα της εφαρμογής για να διαπιστώσουμε πως θα προσαρμοστεί το πληροφοριακό περιβάλλον. Η πρωτότυπη εφαρμογή του υπολογιστικού πλέγματος περιλαμβάνει όλες τις διαθέσιμες τεχνολογίες και αρχιτεκτονικές, έτσι ώστε αν υπάρξει πρόβλημα συμβατότητας να εντοπιστεί και να αντιμετωπιστεί άμεσα. Αν η πρωτότυπη εφαρμογή πληρεί τις προϋποθέσεις 100%, τότε οι σχεδιαστές παίρνουν το «πράσινο» φως για την υλοποίηση του τελικού υπολογιστικού πλέγματος.

3. Συγκριτική Παρουσίαση Προϊόντων Υπολογιστικού Πλέγματος

Τα αποτελέσματα της έρευνας στο διαδίκτυο σχετικά με προϊόντα υπολογιστικού πλέγματος ήταν «άπειρα». Θα ήταν αδύνατο να τα αναφέρουμε και να τα αναλύσουμε όλα. Αντιθέτως, στοχεύσαμε στην ανάλυση εκείνων των προϊόντων υπολογιστικού πλέγματος, που σε συνδυασμό με το Globus Toolkit (βλέπε 2° κεφάλαιο), κρατούν τα ινία στην περιοχή του υπολογιστικού πλέγματος. Όλα τα προϊόντα που θα παρουσιαστούν παρέχουν πλατφόρμα λογισμικού για υπολογιστικά πλέγματα [17, 18, 19, 20, 21]. Τα προϊόντα είναι:

- Avaki
- Data Synapse
- Entropia
- United Devices
- Platform Computing

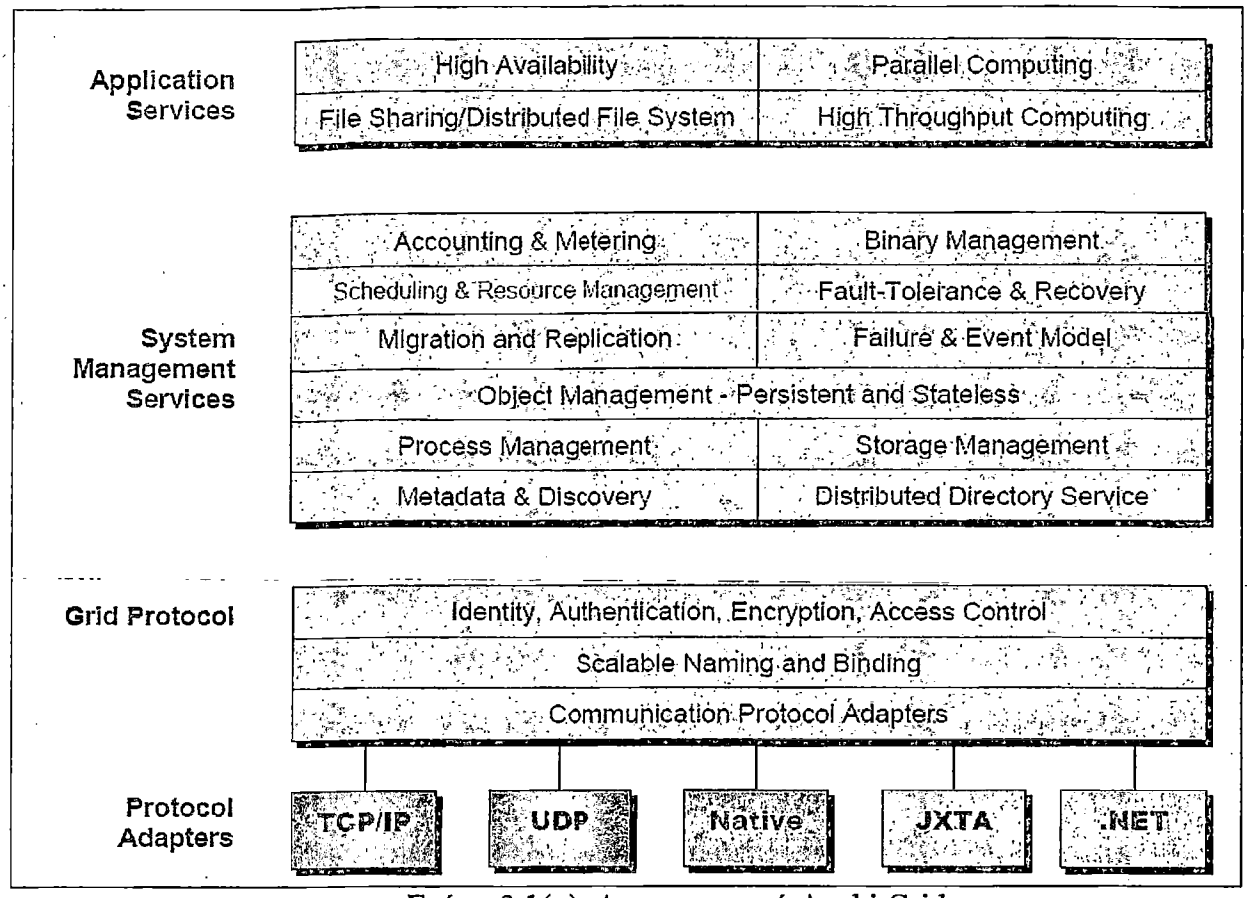
3.1 Avaki

Το Avaki είναι ένα προϊόν υπολογιστικού πλέγματος που παρέχει τόσο υπηρεσίες για «υπολογιστικό grid» όσο και για «grid δεδομένων» (βλέπε 2° κεφάλαιο) [17]. Δυστυχώς όμως το Avaki δεν παρέχεται δωρεάν. Η έκδοση Avaki 2.5 υποστηρίζεται από τα λειτουργικά Windows NT/2000, Linux, Tru64, AIX, Solaris και IRIX.

Η εταιρία Avaki Corporation δεν αποκαλύπτει ακριβώς τις μεθόδους που χρησιμοποιεί το Avaki Grid για την εύρεση και συλλογή πληροφοριών μέσα στο υπολογιστικό πλέγμα. Το παραπάνω μας βάζει σε υποψίες σχετικά με το αν η πλατφόρμα λογισμικού και πιο συγκεκριμένα οι μηχανισμοί ασφαλείας μπορούν να προστατεύσουν τις παραπάνω μεθόδους. Το Avaki Grid αποτελείται από τρία επίπεδα υπηρεσιών:

- Επίπεδο πρωτοκόλλου υπολογιστικού πλέγματος (Grid protocol Layer)
- Επίπεδο διαχείρισης υπηρεσιών (System Management Services Layer)
- Επίπεδο Εφαρμογών

Για την κατανόηση των υπηρεσιών που παρέχονται ανά επίπεδο του Avaki Grid ακολουθεί το σχήμα 3.1(α) [17]:



Σχήμα 3.1(α): Αρχιτεκτονική Avaki Grid

Το Avaki grid διαθέτει διαδικασίες με τις οποίες αξιοποιεί τα τοπικά συστήματα αρχείων (native file systems), δημιουργώντας ένα επίπεδο πάνω από τα τοπικά συστήματα αρχείων. Από την πλευρά του χρήστη, οι διαδικασίες αλληλεπίδρασης με τους υπολογιστικούς πόρους στο Avaki grid είναι εύκολη υπόθεση. Για την κατανόηση των δυνατοτήτων του Avaki grid σε επίπεδο «Data grid» παραθέτουμε τον πίνακα 3.1(β). Ο πίνακας συγκρίνει τις δυνατότητες του Avaki grid με αυτές ενός τυπικού Unix cluster περιβάλλοντος. Το τελευταίο στηρίζεται στο πρωτόκολλο NFS (Network File System).

NFS (Network File System)	**Avaki Grid**
Η δημιουργία «υπολογιστικών clusters» για τη διαμοίραση υπολογιστικών πόρων μεταξύ των UNIX συστημάτων	Η συμμετοχή τοπικών clusters σε πολλαπλά σημεία των υπολογιστικών πλεγμάτων. Το λειτουργικό σύστημα μπορεί να είναι UNIX, NT/2000, LINUX ή και συνδυασμός των παραπάνω.
Πολύπλοκη διαδικασία επέκτασης των clusters πέρα από τα Αναχώματα Ασφαλείας	Τα υπολογιστικά πλέγματα συνδυάζονται στο έπακρο με αναχώματα ασφαλείας και VPNs (Virtual private Networks)
Κλασικός έλεγχος πρόσβασης στα αρχεία, έλλειψη διαδικασιών αυθεντικοποίησης	Υψηλού επιπέδου αυθεντικοποίηση, «ρωμαλέου» μηχανισμοί αυθεντικοποίησης
Έλλειψη αλγορίθμων κρυπτογραφίας	Κρυπτογράφηση δεδομένων για την προστασία της ιδιωτικότητας και της ακεραιότητας.

Σχήμα 3.1(β): Συγκριτικός Πίνακας: NFS – Avaki Grid

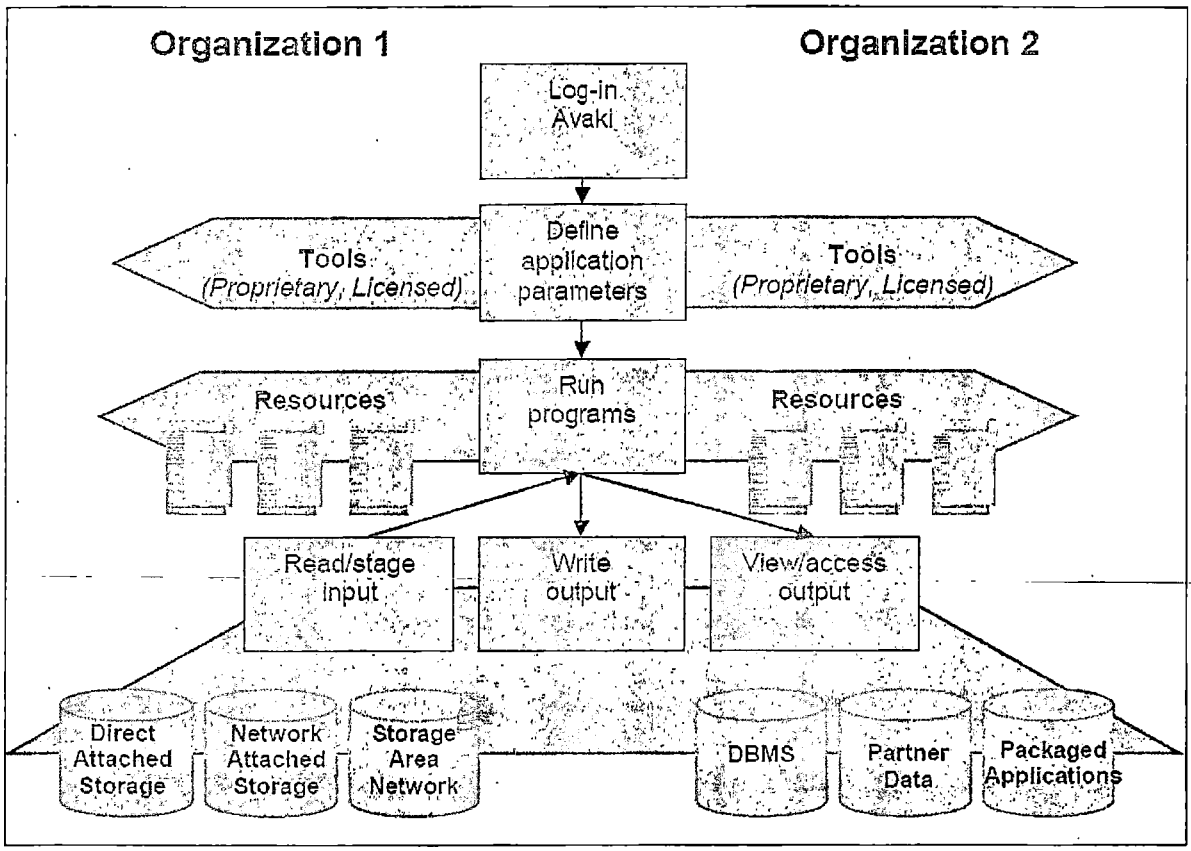
Στόχος του Avaki grid είναι η επέκταση των δυνατοτήτων που παρέχει το πρωτόκολλο NFS πέρα από το τοπικό δίκτυο ενώ ταυτόχρονα διασφαλίζει τις διαδικασίες ασφάλειας. Πως όμως το Avaki grid αποδίδει ως «Computational Grid»; Οι παρεχόμενες υπηρεσίες σε επίπεδο «Computational grid» είναι:

Αυτοματοποιημένες διαδικασίες ελέγχου των υπολογιστικών πόρων και διαμοίρασης αρχείων: Η πλατφόρμα λογισμικού εκτελεί όλες εκείνες τις ενέργειες για την ολοκλήρωση μίας εργασίας στο υπολογιστικό πλέγμα. Εφόσον οι πολιτικές το επιτρέπουν και οι υπολογιστικοί πόροι είναι διαθέσιμοι το Avaki grid είναι υπεύθυνο για την εύρεση υπολογιστικής ισχύς, τη μεταφορά δεδομένων ακόμη και για τη μεταφορά εφαρμογών.

Υπηρεσίες υποστήριξης για «Ετερογενείς Εφαρμογές»: Οι περισσότερες εφαρμογές που τρέχουν στο Avaki grid μπορούν να υλοποιηθούν σε οποιαδήποτε προγραμματιστική γλώσσα, δεν είναι απαραίτητη η χρήση ενός συγκεκριμένου API (Application Programming Interface). Η Avaki Corporation δεν εξηγεί με ακριβείς τρόπους πως το επιτυγχάνει αυτό.

Διαδικασίες ενοποίησης μεταξύ ετερογενών δικτυακών πλατφορμών: Αν σε ένα ή περισσότερα πληροφοριακά συστήματα έχουν ήδη τοποθετηθεί συστήματα διαχείρισης εργασιών, συστήματα εκτέλεσης ερωτημάτων (queuing systems), clusters και άλλες οντότητες που διαφοροποιούνται ανάλογα με το τύπο του πληροφοριακού συστήματος, το Avaki gird είναι υπεύθυνο για τη διαλειτουργικότητα μεταξύ των «ετερογενών οντοτήτων»

Παράλληλη Επεξεργασία: Το Avaki grid υποστηρίζει την παράλληλη εκτέλεση εργασιών μίας εφαρμογής όταν εισάγονται διαφορετικοί παράμετροι εκτέλεσης. Επιπλέον, το Avaki grid υποστηρίζει οποιαδήποτε εφαρμογή είναι γραμμένη στη γλώσσα προγραμματισμού MPI. Μάλιστα, έχει προχωρήσει στην υλοποίηση της Avaki MPI για την εκτέλεση παράλληλων εργασιών σε ετερογενείς πλατφόρμες και δικτυακούς τομείς (Network Domains). Στο σχήμα 3.1(γ) [17] παρουσιάζεται η βασική δομή του Avaki grid όσο αφορά τις υπολογιστικές και παράλληλες δυνατότητες του.



Σχήμα 3.1(γ): Avaki Computational Grid

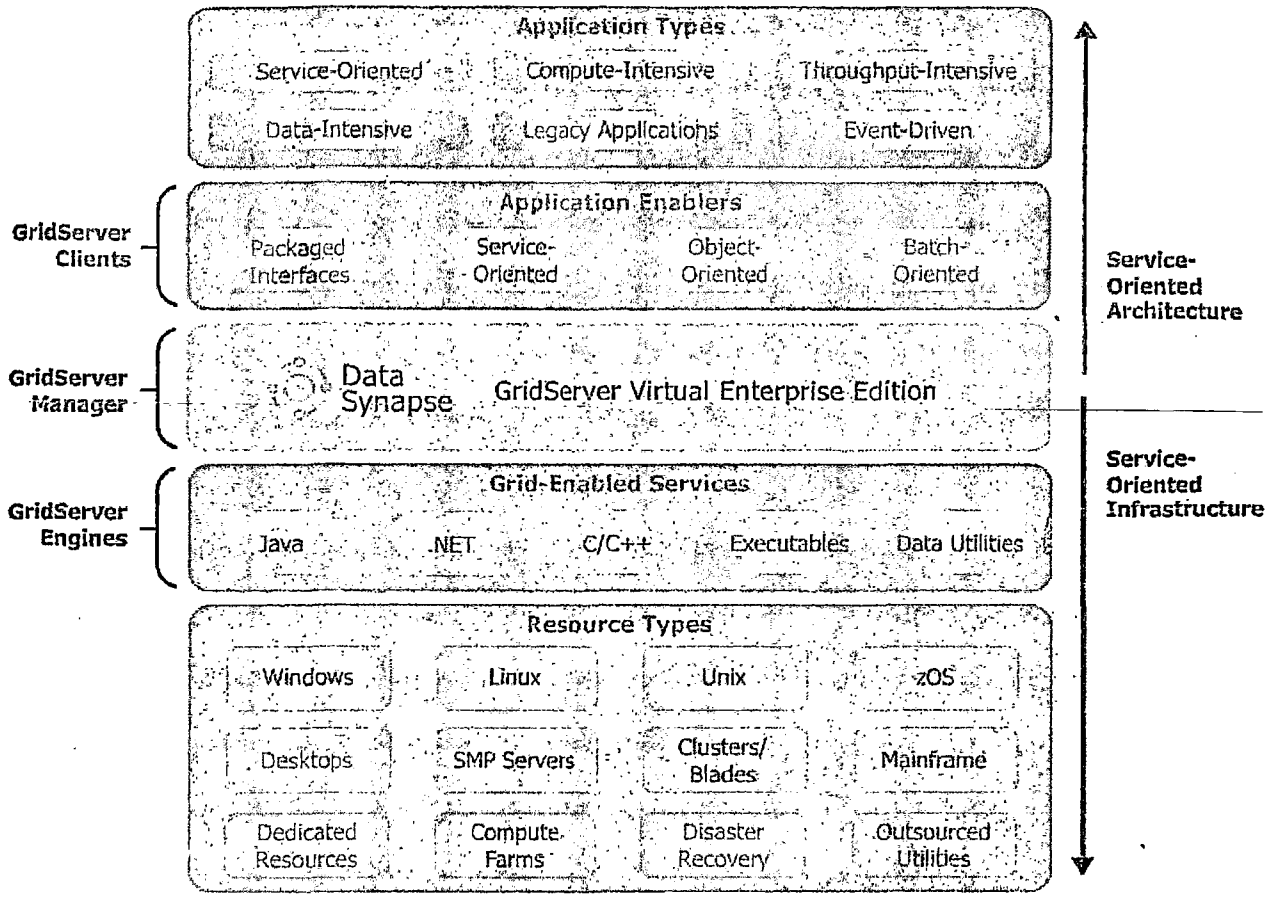
Το Avaki Grid αποτελεί μία ολοκληρωμένη πλατφόρμα λογισμικού που παρέχει υπηρεσίες υπολογιστικού πλέγματος. Τα βασικά αρνητικά σημεία του είναι το υψηλό κόστος απόκτησης του και ότι δε συμβαδίζει με το μοντέλο OGSA (Open Grid Security Architecture) στα θέματα ασφαλείας. Επιπλέον, συγκριτικά με το Globus Toolkit, δεν παρέχονται αναλυτικές πληροφορίες στο χρήστη σχετικά με τους υπολογιστικούς πόρους και την εξέλιξη των εργασιών του.

3.2 Data Synapse

Η εταιρία Data Synapse παρέχει δύο λύσεις υλοποίησης υπολογιστικού πλέγματος, τον «GridServer» και τον «FabricServer». Ο GridServer είναι μία βαθμωτή – προσαρμοστική υποδομή υπολογιστικού πλέγματος που παρέχει υπηρεσίες στα πλαίσια του «Computational Grid». Ο FabricServer παρέχει υπηρεσίες τύπου «Data Grid» [18].

Στόχος του GridServer είναι η «ιδεατοποίηση» (virtualized) των εφαρμογών και των υπολογιστικών πόρων. Οι εφαρμογές των πελατών στέλνουν αιτήσεις προς το grid περιβάλλον και ο GridServer παρέχει υπηρεσίες δυναμικά έτσι ώστε οι αιτήσεις να προωθηθούν. Οι αιτήσεις μπορούν να δηλωθούν από πολλαπλές εφαρμογές ταυτόχρονα και να διαχειριστούν με παράλληλο τρόπο. Η Data Synapse υποστηρίζει ότι η προτεινόμενη αρχιτεκτονική του GridServer δεν επιφέρει υψηλή πολυπλοκότητα στο τομέα διαχείρισης των εργασιών. Επιπλέον παρέχονται υπηρεσίες παρακολούθησης και επίβλεψης υπολογιστικών πόρων και στατιστικών

δεδομένων. Το σύνολο της αρχιτεκτονικής του GridServer παρουσιάζεται στο σχήμα 3.2. [18]



Σχήμα 3.2: GridServer (DataSynapse)

Από την άλλη πλευρά, η εταιρία Data Synapse υποστηρίζει την πλατφόρμα λογισμικού FabricServer. Ο FabricServer έχει κατασκευασθεί για την παροχή υπηρεσιών υπολογιστικού πλέγματος σε υψηλά κατανεμημένα πληροφοριακά περιβάλλοντα (για παράδειγμα σε μία τοπολογία InterGrid). Με τον FabricServer, οι διαδικασίες επεξεργασίας συναλλαγών τρέχουν με παράλληλο τρόπο έτσι ώστε οι διαδικασίες αξιοποίησης υπολογιστικών πόρων να βελτιστοποιηθούν. Με τον παραπάνω τρόπο μειώνεται η ανάγκη για την αγορά νέου υλικού εξοπλισμού ενώ ταυτόχρονα μειώνεται και το κόστος της επιχείρησης Τα βασικά χαρακτηριστικά του FabricServer είναι:

- Βαθμωτές υπηρεσίες (Scaling Procedures): Όταν απαιτηθεί περισσότερη επεξεργαστική ισχύς ή γενικότερα υπολογιστικοί πόροι για την ολοκλήρωση μίας εργασίας, ο FabricServer ανταποκρίνεται άμεσα.

- Άμεση παροχή υπηρεσιών όταν ζητηθούν(Provisioning and Activasion on Demand): Πλήρης αξιοποίηση της υποδομής του υπολογιστικού πλέγματος όταν ζητηθεί.

- Υψηλό επίπεδο διαχείρισης υπηρεσιών(Improved Service Level Management): Ο FabricServer επιτρέπει την επίβλεψη και τη διαχείριση μετρικών όπως, τρέχων εύρος δικτύου, επίπεδο αξιοποίησης υπολογιστικών πόρων και «εξαιρέσεις». Τα περιβάλλοντα παρακολούθησης και διαχείρισης των παραπάνω μετρικών είναι φιλικά προς τον χρήστη.

- Υποστήριξη «Αρχηγών» (Support for Leading Applications): Ο FabricServer υποστηρίζει γνωστά προγραμματιστικά μοντέλα όπως J2SE, J2EE και .NET. Επιπλέον υποστηρίζει εξυπηρετητές όπως BEA, WebLogic, Oracle 10g και Jboss.

- Σύστημα Διαχείρισης μέσω Διαδικτυακών Εφαρμογών (Web – Based Management): Υποστηρίζεται η δημιουργία εφαρμογών και πακέτων με τη χρήση HTML APIs.

Η Data Synapse είναι μία εταιρία που ασχολείται με την περιοχή του υπολογιστικού πλέγματος την τελευταία πενταετία στην Αμερική. Δυστυχώς, οι πληροφορίες που παραθέτει για τις πλατφόρμες λογισμικού υπολογιστικού πλέγματος «GridServer» και «FabricServer» είναι περιορισμένες (δεν υπάρχουν αναφορές για τους μηχανισμούς ασφαλείας). Τα προϊόντα της δεν διανέμονται δωρεάν και αφορούν πληροφοριακά περιβάλλοντα που κατατάσσονται στις τοπολογίες Extragrid και InterGrid.

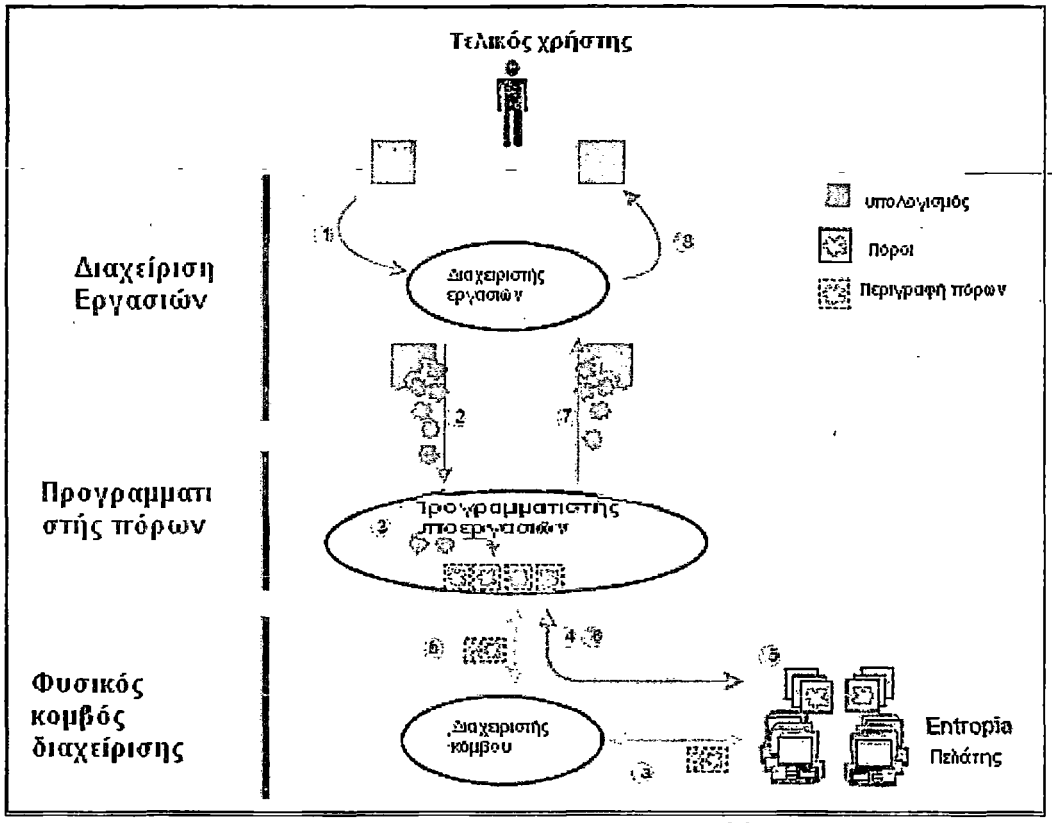
3.3 Entropia

Η Entropia είναι ένας παροχέας υπηρεσιών υπολογιστικού πλέγματος και εδρεύει στο San Diego, California. Το βασικό προϊόν της εταιρίας Entropia είναι το DcGrid. Στόχος του DcGrid είναι η υλοποίηση ενός αποδοτικού τρόπου εύρεσης υπολογιστικής ισχύς μέσα από υπάρχοντα Windows υπολογιστικά μηχανήματα. Για να επιτευχθεί η εκτέλεση μεγάλου αριθμού εφαρμογών με ασφαλή τρόπο, το Dcgrid ορίζει τεχνικές «Sandboxing» [19] (μία απλή εντολή η οποία λαμβάνει ως είσοδο το εκτελέσιμο αρχείο της εφαρμογής και τις απαραίτητες βιβλιοθήκες dll για να δημιουργήσει μία νέα έκδοση της εφαρμογής τύπου Sandbox) έτσι ώστε να ενεργοποιήσει οποιαδήποτε Win32 εφαρμογή που πρόκειται να αναπτυχθεί στο υπολογιστικό πλέγμα.

Για την κατανόηση της τεχνικής «Sandboxing» που χρησιμοποιεί το Dcgrid παρατίθεται το παρακάτω παράδειγμα: Μία εφαρμογή χρησιμοποιεί Windows APIs για να ανοίγει, να κλείνει, να γράφει και να διαβάζει από ένα αρχείο. Το επίπεδο μεσολάβησης του DcGrid ενεργοποιεί τα κατανεμημένα πληροφοριακά συστήματα να εκτελέσουν αυτοματοποιημένες διαδικασίες κρυπτογράφησης όλων των δεδομένων και ελέγχων ακεραιότητας (integrity checks). Επιπλέον το sandbox αυτόματα καταγράφει το αρχείο και τη δομή καταλόγου. Η παραπάνω τεχνική επιτρέπει στο Dcgrid να υποστηρίζει εφαρμογές που σχεδιάζονται με οποιαδήποτε προγραμματιστική γλώσσα (C, C++, Java, Fortran) αρκεί οι τελευταίες να μπορούν να μεταγλωττιστούν σε Windows περιβάλλον (Compilation Procedures).

Στο σχήμα 3.3 παρουσιάζεται η βασική αρχιτεκτονική του DcGrid καθώς και η αλληλεπίδραση των οντοτήτων που την αποτελούν. Καταρχήν ο χρήστης δηλώνει

μία εργασία, έναν υπολογισμό στην οντότητα Job Manager. Ο Job Manager «σπάει» την εργασία σε πολλές μικρές υπό – εργασίες και με τη σειρά του τις δηλώνει στον Subjob Scheduler. Ταυτόχρονα οι πελάτες στο Dcgrid ενημερώνουν την οντότητα Node Manager σε τακτά χρονικά διαστήματα για τη διαθεσιμότητα των υπολογιστικών πόρων. Από την πλευρά του, ο Node Manager ενημερώνει το Subjob Scheduler τόσο για το επίπεδο διαθεσιμότητας των υπολογιστικών πόρων όσο και για τις ακριβείς θέσεις τους στο υπολογιστικό πλέγμα. Ο Subjob Scheduler λαμβάνει την τελική απόφαση και στέλνει τις υπό – εργασίες προς εκτέλεση στους υπολογιστές 4, 5, 6. Τα τελικά αποτελέσματα της εργασίας στέλνονται απευθείας στο Job Manager, ο οποίος από την πλευρά του ενημερώνει τον τελικό χρήστη.



Σχήμα 3.3: Αρχιτεκτονική DcGrid

Η αρχιτεκτονική του Dcgrid αποτελείται από τρία επίπεδα: το επίπεδο διαχείρισης φυσικού στρώματος, το επίπεδο διαχείρισης υπολογιστικών πόρων και το επίπεδο διαχείρισης εργασιών. Η παραπάνω αρχιτεκτονική έχει χαρακτηριστικά ευελιξίας και αποτελεσματικότητας αφού η δομή των επιπέδων είναι συγκροτημένη και οι υπηρεσίες του κάθε επιπέδου είναι άψογα κατανεμημένες.

Τα σημαντικότερα πλεονεκτήματα του Dcgrid είναι η ευκολία στη χρήση, η άμεση πρόσβαση, το χαμηλό κόστος αγοράς και απευθύνεται τόσο σε επιχειρήσεις όσο και σε μεμονωμένους χρήστες του διαδικτύου διασφαλίζοντας τις υπηρεσίες του υπολογιστικού πλέγματος με διαδικασίες ασφαλείας. Το Dcgird παρέχει υπηρεσίες σε επίπεδο «Computational Grid», όμως για την εκτέλεση του απαιτείται από τους χρήστες η εγκατάσταση λειτουργικών συστημάτων Windows 2000/NT. Η Entropia δεν υποστηρίζει έκδοση του Dcgrid για άλλου είδους λειτουργικά συστήματα και αυτό αποτελεί το σημαντικότερο μειονέκτημά της.

3.4 United Devices

Η εταιρία United Devices είναι ένας παροχέας λογισμικού που εδρεύει στο Austin, Texas. Το σημαντικό πλεονέκτημα της έναντι των άλλων εταιριών είναι η υλοποίηση διαφορετικών πλατφορμών υπολογιστικού πλέγματος βάσει των απαιτήσεων των χρηστών. Δύο από τα σημαντικότερα πληροφοριακά έργα στην περιοχή του υπολογιστικού πλέγματος είναι το PcGrid και το Grid MP (Grid MetaProccessor Platform) [20].

Το Grid MP είναι μία σύνθετη λύση υπολογιστικού πλέγματος που αφορά τοπολογίες Extragrid και Intergrid. Υπολογιστικά μηχανήματα, εξυπηρετητές, βάσεις δεδομένων και συστοιχίες από clusters μπορούν να αποτελέσουν μέρος της αρχιτεκτονικής Grid MP. Εν συνεχεία ακολουθεί η καταγραφή των βασικών χαρακτηριστικών του Grid MP:

- Παρεχόμενο πακέτο εφαρμογών
  - Software Development Kit (SDK) με αναλυτικές αναφορές, εργαλεία και παραδείγματα
  - Υποστήριξη εφαρμογών που μπορούν να υλοποιηθούν σε διάφορες γλώσσες προγραμματισμού
  - Οθόνη Αλληλεπίδρασης διαδικτύου (Web services Interface) για την επίβλεψη στατιστικών και άλλων στοιχείων
  - Ιδιαίτερα φιλικά περιβάλλοντα προς το χρήστη

- Βελτιστοποίηση διαδικασιών διαχείρισης εργασιών (Advanced Workload Optimization)
  - Διαχείριση των εργασιών βάσει λίστας προτεραιοτήτων και περιορισμών υπολογιστικών πόρων
  - Αυτόματη διαδικασία επαναδήλωσης της εργασίας όταν προκύψει κάποιο σφάλμα κατά την εκτέλεση της
  - Διαδικασίες ελέγχου από το λογισμικό για τη βελτίωση της απόδοσης του υπολογιστικού πλέγματος

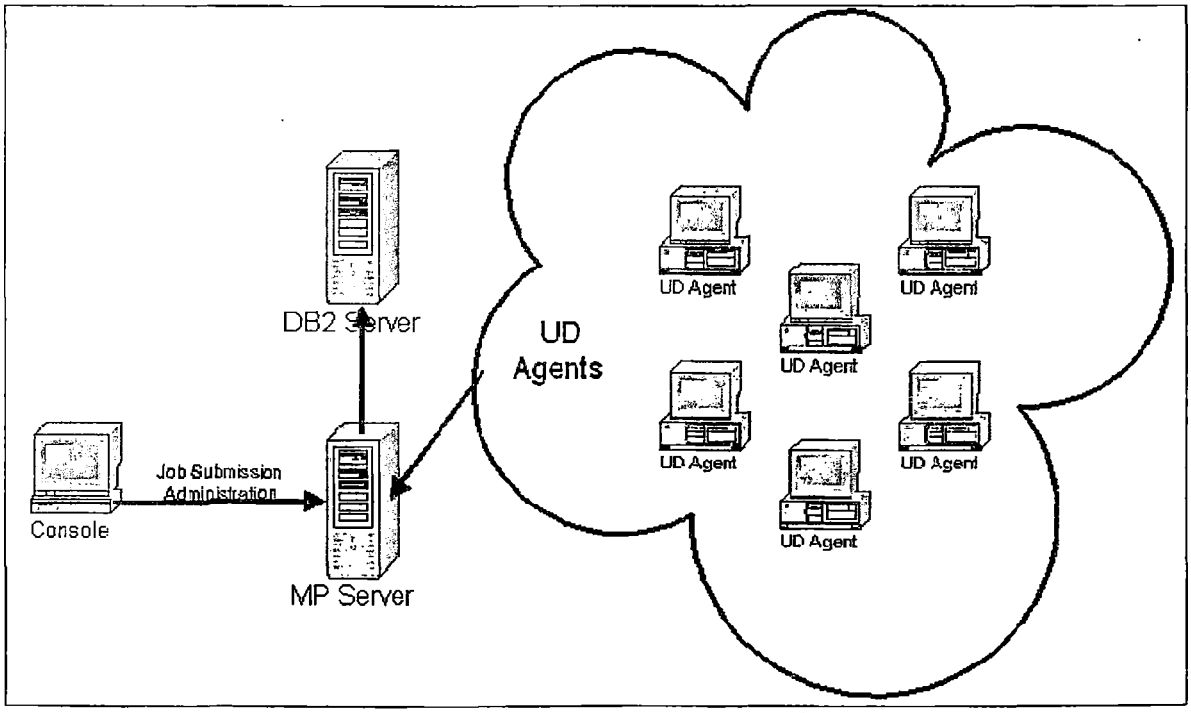
- Ασφαλείς και αυτοματοποιημένες διαδικασίες (Security, Automated Procedures)
  - Ασφαλές πληροφοριακό περιβάλλον, προστασία της εφαρμογής από παρεμβολή κακόβουλων χρηστών
  - Αυτόματες διαδικασίες κρυπτογράφησης και συμπίεσης των δεδομένων πάνω από το δίκτυο
  - Διαδικασίες ελέγχου ακεραιότητας των δεδομένων μέσω τεχνικών «ψηφιακής υπογραφής»

- Ιδεατοποίηση πόρων και οθόνων αλληλεπίδρασης (Virtualizing resources and interfaces)
  - Απλά Interfaces για άμεση πρόσβαση στις οντότητες του Grid Mp
  - Ομαδοποίηση των υπολογιστικών πόρων βάσει γεωγραφικών και επιχειρησιακών δυνατοτήτων
  - Πολιτικές διαχείρισης και δέσμευσης των υπολογιστικών πόρων με χαρακτηριστικά «αποκέντρωσης»

Το Grid MP αποτελείται από δύο βασικά συστατικά – μέρη όπως φαίνεται και στο σχήμα 3.4, το MP Server και τους UD Agents (χρήστες της εφαρμογής). Επιπλέον, υπάρχει ένας εξυπηρετητής βάσης δεδομένων και μία κονσόλα διαδικτύου για τη διαχείριση της MetaProccessor πλατφόρμας. Ο MP εξυπηρετητής υποστηρίζεται μόνο από το Red Hat Linux, ενώ ο εξυπηρετητής της βάσης δεδομένων μπορεί να τρέξει σε οποιοδήποτε λειτουργικό σύστημα υποστηρίζεται από το μοντέλο IBM DB2. Οι UD Agents υποστηρίζονται από τα περισσότερα λειτουργικά συστήματα της αγοράς όπως Windows 98, ME, 2000, XP και LINUX.

Ο MP εξυπηρετητής είναι υπεύθυνος για τη διαχείριση των εργασιών, τη συλλογή δεδομένων και τη συνολική διαχείριση της πλατφόρμας λογισμικού. Η κονσόλα MP παρέχει ένα περιβάλλον αλληλεπίδρασης διαδικτύου με τον εξυπηρετητή, έτσι ώστε να διαχειρίζεται και να ελέγχεται ο τελευταίος με απομακρυσμένο τρόπο. Επιπλέον, μέσω της κονσόλας MP, οι εργασίες μπορούν να δηλωθούν προς εκτέλεση. Το λογισμικό UD Agents είναι εγκαταστημένο στα επιθυμητά υπολογιστικά μηχανήματα και είναι υπεύθυνο για την εκτέλεση των υπό–εργασιών. Ο εξυπηρετητής βάσης δεδομένων πρέπει να ακολουθεί το μοντέλο IBM DB2 και είναι υπεύθυνος για την αποθήκευση όλων των εφαρμογών και των στατιστικών δεδομένων των εργασιών και χρηστών. Επιπρόσθετα, ο εξυπηρετητής βάσης δεδομένων υλοποιεί το μοντέλο Oracle 10.g με αποτέλεσμα να παρέχει υψηλού επιπέδου υπηρεσίες ασφάλειας.

Η εταιρία United Devices έχει καταφέρει με το MP Grid να πετύχει υψηλή διαβάθμιση υπηρεσιών υπολογιστικού πλέγματος. Τη δεδομένη χρονική στιγμή έχουν γίνει περισσότερα από 1.6 εκατομμύρια μεταφορτώσεις της πλατφόρμας UD Agents από χρήστες του διαδικτύου. Στο σχήμα 3.4 που ακολουθεί παρουσιάζεται το σύνολο της αρχιτεκτονικής του MP Grid [15,20].



Σχήμα 3.4: Αρχιτεκτονική MP Grid

3.5 Platform Computing

Η εταιρία Platform Computing είναι ένας παροχέας λογισμικού που εδρεύει στο Toronto, Canada. Η εταιρία Platform Computing υποστηρίζει πολλά κατανεμημένα υπολογιστικά προϊόντα που βασίζονται στο υπολογιστικό πλέγμα. Σε αυτή την ενότητα θα εξετάσουμε το LSF, το ActiveCluster και το MultiCluster. Εκτός από αυτά τα προϊόντα η εταιρία Platform Computing παρέχει και το Platform Globus. Το Platform Globus περιέχει το λογισμικό για το Globus Toolkit καθώς και τις υπηρεσίες υποστηρίξεις του.

Το LSF, όπως βλέπουμε και στο σχήμα 3.5(α), είναι ιδανικό στη διαμοίραση των εργασιών σε πολλές μικρές υπό-εργασίες, οι οποίες εκτελούνται σε κατανεμημένα περιβάλλοντα. Το LSF υποστηρίζεται από το AIX, IRIX, Tru64, HP-UX, Solaris, Linux και τα Windows. Το LSF μπορεί να εγκατασταθεί μεταξύ πολλών ετερογενών εξυπηρετητών. Η πλατφόρμα LSF αποτελείται από τις παρακάτω οντότητες:

- Master host
- Server host
- Client host

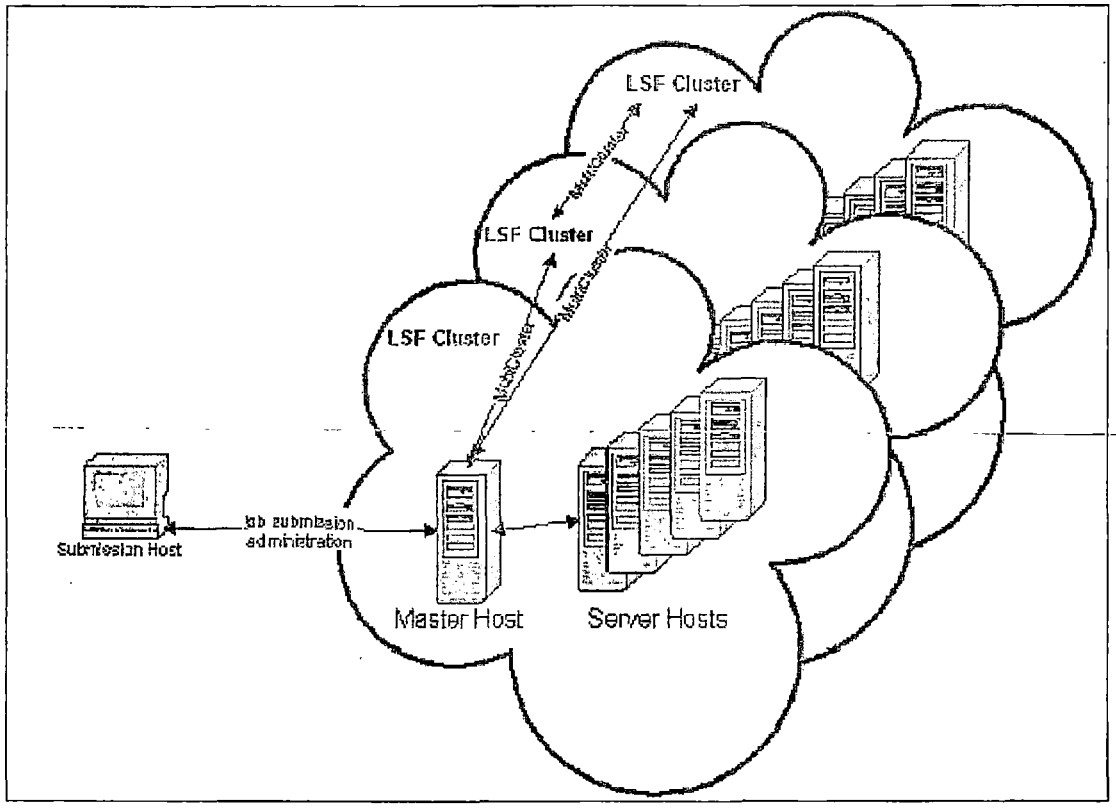
Υπάρχει ένας master host για κάθε cluster στο σύστημα. Ο master host είναι υπεύθυνος για τη διαχείριση των εργασιών στο cluster που ανήκει. Ο server host είναι οποιοδήποτε υπολογιστικό μηχάνημα που εκτελεί τις εργασίες του υπολογιστικού πλέγματος. Ο client host δηλώνει τις εργασίες στο υπολογιστικό πλέγμα και εκτελεί μόνο εντολές LSF. Ένα από τα σημαντικότερα πλεονεκτήματα της πλατφόρμας LSF είναι η υποστήριξη των υπαρχόντων εφαρμογών χωρίς να απαιτείται αλλαγή στον κώδικα της εφαρμογής. Επιπλέον, η πλατφόρμα LSF θα παρέχει μια ομάδα από προγραμματιστικά περιβάλλοντα για ανάπτυξη εφαρμογών.

Το λογισμικό ActiveCluster αποτελεί μια επέκταση της LSF πλατφόρμας και χρησιμοποιείται σε λειτουργικά συστήματα Windows για την παροχή υπηρεσιών υπολογιστικού πλέγματος. Το ActiveCluster πρέπει να τρέξει πάνω στην πλατφόρμα LSF εφόσον χρησιμοποιεί το LSF scheduler. Ο server host μετατρέπεται σε έναν ActiveCluster host που είναι υπεύθυνος για την αποστολή εργασιών προς τους ActiveCluster desktops. Σκοπός του ActiveCluster λογισμικού είναι η αξιοποίηση αχρησιμοποίητης υπολογιστικής ισχύς από ανεξάρτητα υπολογιστικά μηχανήματα προς ένα οργανισμό.

Η πλατφόρμα λογισμικού MultiCluster είναι και αυτή μια επέκταση της υπάρχουσας πλατφόρμας LSF και χρησιμοποιείται για τη συνένωση πολλαπλών LSF clusters. Ένας μεγάλος οργανισμός μπορεί να διαθέτει πολλαπλούς LSF clusters σε διαφορετικά διαμερίσματα του. Το μοντέλο MultiCluster μπορεί να βοηθήσει τον παραπάνω οργανισμό όταν προκύψουν τα εξής σενάρια:

1° Σενάριο: ένα από τα διαμερίσματα του οργανισμού χρειάζεται επιπλέον υπολογιστικούς πόρους. Το πληροφορικό σύστημα του διαμερίσματος στέλνει τις εργασίες προς άλλο διαμέρισμα του οποίου οι clusters έχουν αχρησιμοποίητους υπολογιστικούς πόρους [21].

2° Σενάριο: το διαμέρισμα ενημερώνει τα άλλα διαμερίσματα του οργανισμού πως τα clusters του διαθέτουν αναξιοποίητους υπολογιστικούς πόρους και αν θελήσουν μπορούν να στείλουν τις εργασίες τους προς εκτέλεση.



Σχήμα 3.5(α): Αρχιτεκτονική LSF

Στον πίνακα 3.5(β) παρουσιάζουμε τα βασικά χαρακτηριστικά, τις διαδικασίες που τα αξιοποιούν και τα κέρδη που προκύπτουν από τη χρήση μίας LSF πλατφόρμας λογισμικού.

Δυνατότητες →	Διαδικασίες →	Κέρδη
Αντικειμενοστραφείς χαρακτηριστικά του μοντέλου διαχείρισης εργασιών	Διαχείριση εργασιών	Υψηλή απόδοση του συστήματος
Καθορισμός πολιτικών διαχείρισης υπολογιστικών πόρων	Πολιτικές	Αυτοματοποιημένες διαδικασίες δέσμευσης υπολογιστικών πόρων
Υπηρεσίες κεντρικής διαχείρισης σε κατανεμημένο πληροφοριακό περιβάλλον	Διαχείριση Συστήματος	Χαμηλό κόστος λειτουργικών εξόδων
Υιοθέτηση γνωστών-ανθεκτικών μεθόδων ασφάλειας	Ασφάλεια	Ασφαλή, εξουσιοδοτημένη πρόσβαση στις οντότητες της LSF πλατφόρμας
Υιοθέτηση τεχνικών ανεκτικότητας εισβολών	Ασφάλεια σε επίπεδο διαχείρισης σφαλμάτων	Υψηλή διαθεσιμότητα υπηρεσιών
Ανοιχτή, βαθμωτή αρχιτεκτονική	Ενημέρωση – Αναβάθμιση μέσω του διαδικτύου	Έλλειψη προβλημάτων συμβατότητας

Σχήμα 3.5(β): Δυνατότητες LSF πλατφόρμας

Παραθέτουμε τους παρακάτω οργανισμούς ή/και εταιρίες, οι οποίες έχουν επιλέξει για την παροχή υπηρεσιών υπολογιστικού πλέγματός την πλατφόρμα λογισμικού LSF της Platform Computing.

- United States Department of Defense
- State University of New York
- France Telethon 2001
- U.S. Navy Executes Complex Weather Prediction Models
- Italian National Agency for New Technology, Energy and the Environment (ENEA)
- Advance Micro Devices Inc. (AMD)

3.6 Τελική Αξιολόγηση Προϊόντων (Final Evaluation)

Οι πλατφόρμες υπολογιστικού πλέγματος που είναι διαθέσιμες στην αγορά, καλύπτουν σε μεγάλο βαθμό τις ανάγκες των χρηστών-οργανισμών. Το ζήτημα που προκύπτει είναι ποιο από τα προϊόντα του υπολογιστικού πλέγματος καλύπτει καλύτερα τις περισσότερες επιχειρησιακές ανάγκες. Τη συγκεκριμένη χρονική στιγμή το Globus Toolkit είναι ένα προϊόν υπολογιστικού πλέγματος που διατίθεται δωρεάν, γνωστοποιεί το σύνολο των διαδικασιών του προς το κοινό, στηρίζεται σε γνωστούς και επαληθευμένα ισχυρούς μηχανισμούς ασφαλείας, παρέχει υπηρεσίες «Computation Grid» και «Data Grid» και έχει μεγάλη απήχηση σε ερευνητικές ομάδες της πληροφορικής που ασχολούνται με θέματα βελτιστοποίησης δικτύων. Ένα ακόμη ζωτικής σημασίας πλεονέκτημα του Globus Toolkit απέναντι στις άλλες πλατφόρμες υπολογιστικού πλέγματος είναι η ικανότητα της προσαρμογής στους επιχειρησιακούς στόχους του εκάστοτε οργανισμού.

Από την άλλη πλευρά, κατά τη διάρκεια της παρουσίασης των προϊόντων, εντοπίστηκαν τομείς που οι άλλες πλατφόρμες υπολογιστικού πλέγματος υπερτερούν έναντι του Globus Toolkit. Η φιλικότητα προς τον χρήστη, θέματα συμβατότητας με λειτουργικά συστήματα, η παροχή εργαλείων για την εμφάνιση στατιστικών και άλλων μετρήσεων είναι μερικοί από τους τομείς που τα προϊόντα του υπολογιστικού πλέγματος της αγοράς νικάνε στα σημεία το Globus Toolkit. Το Globus Toolkit δεν απευθύνεται σε αρχάριους, ούτε σε χρήστες του διαδικτύου που βλέπουν τις υπηρεσίες υπολογιστικού πλέγματος σαν υπηρεσίες P2P εφαρμογών. Αντιθέτως αποτελεί μία σύνθετη λύση υπολογιστικού πλέγματος που παρέχει σύγχρονες και αξιόπιστες υπηρεσίες, για αυτό κατά την προσωπική γνώμη μας είναι εκείνο το προϊόν που κρατάει τα ινία στην περιοχή του υπολογιστικού πλέγματος.

Στον πίνακα 3.6 ακολουθεί μία συγκριτική παρουσίαση των προϊόντων υπολογιστικού πλέγματος που παρουσιάστηκαν (συμπεριλαμβανομένου και του Globus Toolkit εφόσον έχει αναλυθεί στο 2° κεφάλαιο). Έχουν επιλεχθεί οι σημαντικότεροι τομείς της περιοχής του υπολογιστικού πλέγματος και έχουν συμπεριληφθεί σχόλια για την απόδοση των προϊόντων ανά τομέα [17, 18, 19, 20, 21].

ΑΞΙΟΛΟΓΗΣΗ	Globus Toolkit	Avaki Grid	Data Synapse	Entropia	United Devices	Platform Computing
Συμβατότητα με Λειτουργικά Συστήματα	Μέτρια Συμβατότητα	Καλή Συμβατότητα	Χαμηλή Συμβατότητα	Μόνο Windows	Υψηλή Συμβατότητα	Καλή Συμβατότητα
Ασφάλεια	Υψηλή. Εφαρμογή προτύπου OGSA	Δεν αναφέρονται οι υπηρεσίες ασφαλείας (Άσχημη Εντύπωση)	Ισχυρή Ασφάλεια στη βάση δεδομένων (Oracle)	Ευφυή σύστημα ασφάλειας (Sandboxing)	Ισχυροί Μηχανισμοί Ασφαλείας	Ισχυρή Ασφάλεια στη βάση δεδομένων
Υπηρεσίες Computational Grid	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Υπηρεσίες Data Grid	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ
Φιλικότητα προς τον Χρήστη	Μικρός βαθμός φιλικότητας	Μέτριος βαθμός φιλικότητας	Καλός βαθμός φιλικότητας	Υψηλός βαθμός φιλικότητας	Καλός βαθμός φιλικότητας	—
Παροχή Γραφικών Εργαλείων	Όχι, μόνο Command line υπηρεσίες	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Διαδικασίες Διαβάθμισης Χρηστών	ΝΑΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ	Χαμηλού Επιπέδου υπηρεσίες	ΝΑΙ
Δυναμική Ενημέρωση Χρηστών για Υπολογιστικούς πόρους	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ
Τοπολογίες Υπολογιστικού Πλέγματος	ΟΛΕΣ	IntraGrid, ExtarGrid	ExtraGrid, InterGrid	ΟΛΕΣ	ΟΛΕΣ	ExtraGrid, InterGrid
Απήχηση σε Χρήστες Διαδικτύου	ΟΧΙ	ΜΕΤΡΙΑ	ΟΧΙ	ΥΨΗΛΗ	ΚΑΛΗ	ΜΕΤΡΙΑ
Προσαρμογή στο Επιχειρησιακό Περιβάλλον	Υψηλή προσαρμογή	Καλή Προσαρμογή	Καλή Προσαρμογή	Κακή. Λίγες Δυνατότητες	Καλή Προσαρμογή	Υψηλή Προσαρμογή
Βαθμωτή-Κατανεμημένη Αρχιτεκτονική	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ
Διανομή	Δωρεάν	Υψηλό Κόστος	Υψηλό Κόστος	Χαμηλό Κόστος	Υψηλό Κόστος	Υψηλό Κόστος
Συνολική Απόδοση	Υψηλή	Μέτρια	Καλή	Μέτρια	Καλή	Πολύ Καλή

Σχήμα 3.6: Συγκριτικός Πίνακας Προϊόντων

4. ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΨΗΦΟΦΟΡΙΑΣ – ΑΞΙΟΠΟΙΗΣΗ ΤΕΧΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΠΛΕΓΜΑΤΟΣ

Η καθιέρωση της ηλεκτρονικής ψηφοφορίας και συγκεκριμένα της ψηφοφορίας μέσω Internet ως εναλλακτικός τρόπος υποβολής της ψήφου αναμένεται να αυξήσει την συμμετοχή των πολιτών στις εκλογές και να αυτοματοποιήσει τις διαδικασίες της υποβολής και της καταμέτρησης των ψήφων, μειώνοντας μακροπρόθεσμα το κόστος διεξαγωγής των εκλογών. Ωστόσο, για να ολοκληρωθεί η μετάβαση σε συστήματα εξ' αποστάσεως ψηφοφορίας μέσω Internet, πρέπει πρωτίστως να επιλυθούν ζητήματα ασφάλειας και λειτουργικότητας, τα οποία συχνά αγνοούνται από τους σχεδιαστές συστημάτων. Στην εργασία αυτή καθορίζουμε απαιτήσεις ασφάλειας και πρακτικότητας, συζητούμε προϋποθέσεις και περιγράφουμε κρυπτογραφικά μοντέλα ασφάλειας για την υλοποίηση ηλεκτρονικών εκλογών μεγάλης κλίμακας μέσω Internet. Επίσης, αναφέρουμε τις προοπτικές που διαγράφονται για την υιοθέτηση συστημάτων ηλεκτρονικής ψηφοφορίας στα σύγχρονα δημοκρατικά καθεστώτα.

Τέλος προχωράμε σε ένα προτεινόμενο σενάριο υλοποίησης αρχιτεκτονικής ενός συστήματος ηλεκτρονικής ψηφοφορίας. Το σύστημα που περιγράφεται σε μεγάλο βαθμό διατρέχεται από υπηρεσίες και λειτουργίες υπολογιστικού πλέγματος έτσι ώστε να αντιμετωπισθούν βασικά θέματα ασφάλειας που προκύπτουν σε συστήματα ηλεκτρονικής ψηφοφορίας.

Λέξεις Κλειδιά: Ηλεκτρονική Ψηφοφορία, Ασφάλεια, Λειτουργικότητα, Κρυπτογραφία

4.1 Εισαγωγή

Στα περισσότερα δημοκρατικά καθεστώτα επικρατεί ανησυχία για τα αυξανόμενα ποσοστά αποχής από τις εθνικές εκλογές, καθώς και για τη διαφαινόμενη τάση αποστασιοποίησης από τα πολιτικά δρώμενα. Για να αντιστραφεί το κλίμα αναζητούνται αλλαγές στον τρόπο συμμετοχής των πολιτών στα κοινά. Ένα από τα μέτρα υπό συζήτηση είναι η υιοθέτηση συστημάτων *ηλεκτρονικής ψηφοφορίας* (e-voting).

Η καθιέρωση της ηλεκτρονικής ψηφοφορίας, και μάλιστα της *ψηφοφορίας μέσω Internet* αναμένεται να απλοποιήσει και να περιορίσει τα λάθη κατά τη διαδικασία υποβολής και καταμέτρησης των ψήφων (Mohen, 2001), υπόσχεται μεγαλύτερη προσβασιμότητα στα άτομα με ειδικές ανάγκες, καθώς και μικρότερο (μακροπρόθεσμα) οικονομικό κόστος, σε σχέση με το κόστος των παραδοσιακών εκλογών. Ειδικότερα με τα συστήματα εξ' αποστάσεως ψηφοφορίας μέσω Internet η διαδικασία υποβολής της ψήφου θα είναι φιλική προς τον χρήστη, ενώ ένας μεγάλος

αριθμός υπολογιστών που είναι σήμερα διαθέσιμοι σε εύκολα προσβάσιμους χώρους (π.χ. βιβλιοθήκες, σχολεία, πανεπιστήμια, δημόσιες υπηρεσίες) μπορούν να γίνονται διαθέσιμοι στο εκλογικό σώμα την ημέρα των εκλογών.

Έως σήμερα έχουν διεξαχθεί αρκετές εκλογές μέσω Internet, αν και οι περισσότερες από αυτές είχαν ανεπίσημο χαρακτήρα, ενώ αρκετά συστήματα σχεδιάζονται και εφαρμόζονται πιλοτικά με σκοπό τη μελλοντική τους υλοποίηση σε συστήματα μεγάλης κλίμακας. Παραδείγματα αποτελούν (Burmester,2002) οι εκλογές της παράταξης των Δημοκρατικών στην πολιτεία της Arizona των Η.Π.Α. (νομικά έγκυρες), Μάρτιος 2000; η αποστολή, μέσω Internet, των ψήφων του στρατιωτικού προσωπικού εντός και εκτός των Η.Π.Α (absentee ballots) στις Προεδρικές εκλογές (νομικά έγκυρες), 2000; Οι εκλογές των Ρεπουμπλικάνων στην πολιτεία της Alaska (ανεπίσημα αποτελέσματα), Ιανουάριος 2000; Οι τοπικές και δημοτικές εκλογές στη Μεγ.Βρετανία (ανεπίσημα αποτελέσματα), Μάιος 2002. Σε γενικές γραμμές, κάθε ηλεκτρονική ψηφοφορία αποτελείται από τέσσερα (4) διακριτά στάδια:

- **Εγγραφή.** Πριν από τη διεξαγωγή των εκλογών, οι ψηφοφόροι αποδεικνύουν την αληθινή τους ταυτότητα και τη νομιμότητα του δικαιώματος τους να ψηφίσουν (π.χ. όριο ηλικίας). Οι εγγραφόμενοι χρήστες προστίθενται στον εκλογικό κατάλογο.

- **Επικύρωση.** Κατά τη διάρκεια των εκλογών, και πριν υποβάλλουν τη ψήφο τους, οι ψηφοφόροι ταυτοποιούνται (identification), επιβεβαιώνεται δηλαδή η ταυτότητα τους τη δεδομένη χρονική στιγμή.

- **Υποβολή Ψήφου.** Οι ψηφοφόροι σε αυτό το στάδιο υποβάλλουν την ψήφο τους. Μόνο μια ψήφος επιτρέπεται για κάθε ψηφοφόρο.

- **Καταμέτρηση Ψήφων.** Μόλις εκπνεύσει η προθεσμία υποβολής ψήφων, οι ψήφοι καταμετρούνται και στη συνέχεια ανακοινώνεται το αποτέλεσμα των εκλογών.

Κάθε ένα από τα παραπάνω στάδια μπορεί να λάβει χώρα με τη χρήση είτε φυσικών είτε ηλεκτρονικών διαδικασιών. Διακρίνονται δύο τύποι ηλεκτρονικής ψηφοφορίας: Η Ηλεκτρονική Ψηφοφορία σε Εκλογικά Σημεία (Polling Place E-Voting) και η Ηλεκτρονική Ψηφοφορία μέσω Internet (Internet Voting)[22].

Ηλεκτρονική Ψηφοφορία σε Εκλογικά Σημεία. Σε ένα εκλογικό σημείο π.χ. *Εκλογικό Κέντρο* ή *Κιόσκι* (California Internet Voting Task Force,2000), τόσο τα συστήματα-πελάτες (voting clients) που χρησιμοποιούν οι ψηφοφόροι για να υποβάλλουν ηλεκτρονικά την ψήφο τους, όσο και το φυσικό περιβάλλον στο οποίο διεξάγεται η ψηφοφορία, επιβλέπονται από εξουσιοδοτημένες οντότητες (π.χ. εκλογικοί αντιπρόσωποι, αστυνομία). Ανάλογα με το είδος του εκλογικού σημείου, το στάδιο της Επικύρωσης μπορεί να γίνει είτε με φυσικές διαδικασίες (έλεγχος απ' ευθείας από τους εκλογικούς αντιπροσώπους) είτε με ηλεκτρονικές (π.χ. κωδικός PIN). Η Υποβολή της ψήφου γίνεται ηλεκτρονικά σε προσωπικούς υπολογιστές ή ειδικές συσκευές με οθόνες αφής (όπως οι Συσκευές Άμεσης Καταμέτρησης – DRE, που χρησιμοποιούνται ευρέως στις Η.Π.Α (Caltec/Mit,2001)). Οι ηλεκτρονικές ψήφοι αποθηκεύονται τοπικά σε αποσπώμενες περιφερειακές μονάδες. Η Καταμέτρηση των ψήφων γίνεται επίσης ηλεκτρονικά: οι ψήφοι καταμετρούνται τοπικά στο εκλογικό

κέντρο ή αποστέλλονται στον κεντρικό εξυπηρετητή (server) των εκλογών για τον υπολογισμό των συγκεντρωτικών αποτελεσμάτων. Η μεταφορά στον κεντρικό server μπορεί να γίνει επίσης ηλεκτρονικά, με «ασφαλείς» συνδέσεις (π.χ. μισθωμένες γραμμές οπτικών ινών ή μέσω Internet με τεχνικές IPSEC - Εικονικά Ιδιωτικά Δίκτυα VPNs). Εναλλακτικά, έχει προταθεί η χρήση των δικτύων ATM (Automated Teller Machines) την ημέρα των εκλογών: τα δίκτυα ATM έχουν ορισμένα επιθυμητά χαρακτηριστικά ασφάλειας (μυστικότητα του καναλιού επικοινωνίας, αξιόπιστος εξοπλισμός, ανθεκτικά τερματικά, υψηλό ποσοστό διείσδυσης). Ωστόσο συχνά διατυπώνονται αντιρρήσεις σχετικά με την καταλληλότητα τους για τη διενέργεια ηλεκτρονικών εκλογών (Jefferson,2000).

Ψηφοφορία μέσω Internet. Η ψήφος υποβάλλεται μέσω Internet και τα συστήματα-πελάτες βρίσκονται υπό χαλαρή ή μηδαμινή επίβλεψη (στο σπίτι, στον χώρο εργασίας, σε βιβλιοθήκες, σχολεία, πανεπιστήμια). Η Εγγραφή μπορεί να γίνει με φυσικές (π.χ. σε εκλογικά γραφεία) ή με ηλεκτρονικές διαδικασίες (π.χ. ψηφιακή υπογραφή, μέθοδοι βιομετρικής). Τα στάδια της Επικύρωσης, της Υποβολής και της Καταμέτρησης γίνονται εξ' ολοκλήρου ηλεκτρονικά.

Η ψηφοφορία μέσω Internet απαιτεί ένα μεγαλύτερο επίπεδο ασφάλειας από αυτό που απαιτείται σε συνήθεις συναλλαγές ηλεκτρονικού εμπορίου. Ενώ η ταυτοποίηση των ψηφοφόρων και η εξασφάλιση της μοναδικότητας της ψήφου ανά ψηφοφόρο, μπορούν εν δυνάμει να αντιμετωπιστούν με τεχνικές που ήδη χρησιμοποιούνται σε εφαρμογές ηλεκτρονικών συστημάτων πληρωμών (π.χ. ψηφιακές υπογραφές - ψηφιακά πιστοποιητικά), οι επιπλέον απαιτήσεις όπως *μυστικότητα* και *ανωνυμία* της ψήφου, *οικουμενική επαληθευσιμότητα*, καθώς και *προστασία από καταναγκασμό*, συνθέτουν ένα πολύπλοκο μοντέλο απαιτήσεων ασφάλειας το οποίο έως σήμερα δεν έχει αντιμετωπιστεί με μεθόδους που να είναι ασφαλείς και παράλληλα πρακτικές. Οι επικριτές των συστημάτων ηλεκτρονικής ψηφοφορίας μέσω Internet θεωρούν ότι οι υπάρχουσες τεχνολογίες δεν είναι ακόμα ώριμες να αντιμετωπίσουν τα προβλήματα ασφάλειας που προκύπτουν. Επίσης θεωρούν ότι η υιοθέτηση τους θα οδηγούσε στον κοινωνικό αποκλεισμό των λεγόμενων «ψηφιακά αναλφάβητων» πολιτών (Dictson,2000, Philips,2001).

4.1.1 Απαιτήσεις Ασφάλειας και Πρακτικότητας

Ένα σύστημα ηλεκτρονικής ψηφοφορίας που πρόκειται να χρησιμοποιηθεί σε εκλογές μεγάλης κλίμακας πρέπει να είναι[22] (Internet Policy Institute,2001, Schneier,1996):

α) Ασφαλές, δηλαδή:

Δημοκρατικό (Democratic). Μόνο εξουσιοδοτημένοι ψηφοφόροι δικαιούνται να υποβάλλουν ψήφους, και κανείς ψηφοφόρος δε δικαιούται να υποβάλλει περισσότερες από μια ψήφους.

- *Ακριβές* (Accurate). Καμία ψήφος δεν είναι δυνατόν να αλλοιωθεί, να καταμετρηθεί περισσότερες από μια φορές, να διαγραφεί από τις Εκλογικές Αρχές ή άλλους εσωτερικούς / εξωτερικούς εχθρούς.

- *Μυστικό* (Secret). Καμία ψήφος δεν είναι δυνατόν να συνδεθεί με τον ψηφοφόρο που την υπέβαλλε, ενώ όλες οι ψήφοι παραμένουν μυστικές για όσο διάστημα διαρκεί η περίοδος υποβολής ψήφων.

- *Προστατευμένο από Καταναγκασμό* (Uncoercible). Κανένας χρήστης δεν έχει τη δυνατότητα να αποδείξει τη ψήφο του σε κάποιον τρίτο.

- *Οικουμενικά Επαληθεύσιμο* (Universally Verifiable). Κάθε εξωτερικός παρατηρητής μπορεί να πειστεί ότι το σύστημα είναι ακριβές και ότι το αποτέλεσμα του υπολογισμού των ψήφων της κάλπης αντανακλά τη βούληση των ψηφοφόρων που τις υπέβαλλαν.

- *Ανθεκτικό* (Robust). Όλες οι απαιτήσεις ασφάλειας ικανοποιούνται πλήρως, παρά τα όποια τυχαία σφάλματα ή τις κακόβουλες συμπεριφορές ορισμένων οντοτήτων (ψηφοφόροι, Αρχές, εσωτερικοί/εξωτερικοί εχθροί).

Πρέπει να τονίσουμε πως σε αρκετά δημοκρατικά καθεστώτα (π.χ. Αυστραλία, Ελλάδα, Βέλγιο), όπου η συμμετοχή των πολιτών στις εκλογές είναι υποχρεωτική από το νόμο, μια επιπλέον απαίτηση ασφάλειας είναι η εύρεση των ψηφοφόρων που δεν άσκησαν το εκλογικό τους δικαίωμα.

β) Πρακτικό

Το σύστημα πρέπει να είναι εύκολα υλοποιήσιμο, συμβατό με τις διάφορες τεχνολογίες και πλατφόρμες (λειτουργικά συστήματα, αρχιτεκτονικές, εργαλεία πλοήγησης στο Web κ.λ.π), λειτουργικό (Στις εκλογές του 2000 στην Florida των Η.Π.Α ένας μεγάλος αριθμός άκυρων ψήφων υποβλήθηκε λόγω ελλιπούς σχεδίασης των ψηφοδελτίων), και να απευθύνεται σε όλες τις κατηγορίες πληθυσμού ανεξαρτήτως ηλικίας, γλώσσας, φυσικών ικανοτήτων, μόρφωσης, εξοικείωσης με τις τεχνολογίες του Internet κ.λ.π.. Επίσης, το σύστημα πρέπει να υποστηρίζει μια ποικιλία από format ψήφων, συμπεριλαμβανομένων και των λεγόμενων «λευκών» ή άκυρων ψήφων. Το σύστημα θα πρέπει να παρουσιάζει χαμηλή υπολογιστική πολυπλοκότητα και η αποδοτικότητα του να μην επηρεάζεται δραστικά από το μέγεθος του εκλεκτορικού σώματος ή των υποψηφίων (scalability), ενώ οι υπηρεσίες ασφάλειας που προσφέρει θα πρέπει να είναι διαφανείς (transparent) στον χρήστη.

4.1.2 Επιθέσεις σε Συστήματα Ηλεκτρονικής Ψηφοφορίας

Τα κίνητρα για μια επίθεση στην ασφάλεια ενός συστήματος ηλεκτρονικής ψηφοφορίας, ιδιαίτερα σε εθνικές εκλογές, είναι πολλά (πολιτικές επιδιώξεις, χρηματική αμοιβή, διεκδίκηση εξουσίας, εμπλοκή μυστικών υπηρεσιών, τρομοκρατικές οργανώσεις). Το είδος και η μορφή των επιθέσεων ποικίλουν (California Internet Voting Task Force,2000, Coleman,2002, Internet Policy Institute,2001, Philips,2001).

α) Ηλεκτρονική Ψηφοφορία (Γενικά). Είναι γνωστό ότι τα ηλεκτρονικά δεδομένα αντιγράφονται, αλλοιώνονται και καταστρέφονται πιο εύκολα από ότι οι φυσικές ψήφοι. Επιπλέον, όλα τα ηλεκτρονικά συστήματα είναι ευάλωτα σε επιθέσεις από *εσωτερικούς εχθρούς* (insider attacks) καθώς και σε επιθέσεις *Άρνησης Εξυπηρέτησης* (Denial Of Service – DOS). Τα σημερινά ηλεκτρονικά συστήματα ψηφοφορίας

επίσης διαθέτουν ανεπαρκή *στοιχεία ελέγχου* (audit trail) (Philips,2001) και δεν παρέχουν οικουμενική επαληθευσιμότητα, με συνέπεια τα αποτελέσματα της ψηφοφορίας να τίθενται υπό αμφισβήτηση.

β) Ψηφοφορία μέσω Internet. Από τη σκοπιά της ασφάλειας, οι εκλογές μέσω Internet είναι περισσότερο ευάλωτες σε *επιθέσεις καταναγκασμού* (coercion) (Burmester,2003) όπου οι χρήστες αναγκάζονται ή συναλλάσσονται με κάποιον τρίτο για την υποβολή μιας προσυμφωνημένης ψήφου. Επιπρόσθετα, σε ένα σύστημα εξ' αποστάσεως ψηφοφορίας οι ψηφοφόροι ενδεχομένως θα πρέπει να δημιουργήσουν οι ίδιοι ένα ασφαλές περιβάλλον στις υπολογιστικές τους μηχανές (συστήματα πελάτες), π.χ. προτού υποβάλλουν τη ψήφο τους. Οι έλεγχοι και η πιστοποίηση λογισμικού στα συστήματα ψηφοφορίας μέσω Internet παρουσιάζουν επίσης ιδιαίτερες δυσκολίες, καθώς τα συστατικά μέρη των συστημάτων αυτών είναι συνήθως διαφορετικής προέλευσης και έχουν μυστικό (κλειστό) κώδικα, όπως για παράδειγμα τα σύγχρονα λειτουργικά συστήματα Windows και τα προγράμματα πλοήγησης στο Web. Παράλληλα, τα συστήματα ψηφοφορίας μέσω Internet είναι περισσότερο ευάλωτα, σε σχέση με τις υπόλοιπες κατηγορίες ηλεκτρονικής ψηφοφορίας, στα εξής σημεία:

- *Στα συστήματα-πελάτες*: Ιοί τύπου «*σκουλήκια*» (worms) ή «*δούρειοι ίπποι*» (trojan horses) μπορούν να αλλοιώσουν τη ψήφο, πολύ πριν αυτή κρυπτογραφηθεί ή αυθεντικοποιηθεί. Επίσης, ο εισβολέας μπορεί εξ' αποστάσεως να εκμεταλλευτεί «τρύπες» ή λάθη στο σχεδιασμό του λειτουργικού συστήματος ή του προγράμματος πλοήγησης στο Web.

- *Στο επίπεδο της επικοινωνίας*: Οι κυριότερες επιθέσεις στο επίπεδο της επικοινωνίας είναι οι επιθέσεις *πλαστοπροσωπίας* (spoofing) DNS ονομάτων ή IP διευθύνσεων, και οι *επιθέσεις ενδιάμεσης οντότητας* (man in the middle) (Schneier,1996). Η επικοινωνία μεταξύ πελάτη και εξυπηρετητή μπορεί επίσης να απειληθεί και από επιθέσεις τύπου TCP SYN/ACK στο επίπεδο δικτύου του μοντέλου TCP/IP, από επιθέσεις πλαστοπροσωπίας στο φυσικό επίπεδο του μοντέλου OSI (ARP spoofing) κ.λ.π.

    - *Στα συστήματα-εξυπηρετητές*: Οι επιθέσεις σε αυτό το επίπεδο είναι παρόμοιες με αυτές στα συστήματα-πελάτες. Εδώ βέβαια οι επιθέσεις Άρνησης Εξυπηρέτησης (DOS), όπως IP fragmentation ή υπερχείλιση καταχωρητών (buffer overflow), έχουν μεγάλη επικινδυνότητα, αφού μπορούν να υπονομεύσουν ολόκληρη την εκλογική διαδικασία. Το πρόβλημα της *συμφόρησης* (bottleneck) είναι παρόμοιο, ως προς τις συνέπειες του, με μια επίθεση Άρνησης Εξυπηρέτησης, με τη διαφορά ότι η συμφόρηση προκαλείται από υπερβολικά μεγάλο αριθμό ταυτόχρονων νομίμων αιτήσεων για σύνδεση με τον εξυπηρετητή, και όχι απαραίτητα από κακόβουλη επίθεση.

4.1.3 Προϋποθέσεις για τη Διεξαγωγή Εκλογών μέσω Internet

Υπάρχουν αρκετές παράμετροι που πρέπει να ληφθούν σοβαρά υπ' όψιν ώστε να γίνει εφικτή η διεξαγωγή ηλεκτρονικών εκλογών μέσω Internet[23]:

Πρωτόκολλα / Λογισμικό. Για να είναι ασφαλής η ηλεκτρονική ψηφοφορία, το σύστημα θα πρέπει να υλοποιεί ένα κρυπτογραφικό πρωτόκολλο (τα υποψήφια

μοντέλα περιγράφονται στην Ενότητα 5) που ικανοποιεί τις απαιτήσεις ασφάλειας (Ενότητα 2). Για λόγους αξιοπιστίας επίσης, θεωρούμε πως το σύστημα θα πρέπει να υλοποιηθεί με *ανοικτό λογισμικό* (open source). Το σύστημα πρέπει επίσης να συνοδεύεται από τους κατάλληλους μηχανισμούς παρακολούθησης (monitoring) και επαλήθευσης (audit) της λειτουργίας του. Ανεξάρτητοι ηλεκτρονικοί ή φυσικοί μηχανισμοί επαλήθευσης ενδεχομένως να αυξήσουν την εμπιστοσύνη των πολιτών στο αποτέλεσμα των εκλογών. Για παράδειγμα, η Mercuri (1992) πρότεινε την εκτύπωση των επιλογών του ψηφοφόρου σε χαρτί, το οποίο ο ψηφοφόρος θα ρίχνει σε μια φυσική κάλπη για τις ανάγκες μιας δεύτερης καταμέτρησης.

Υποδομή Δημόσιου Κλειδιού. Οι εκλογές μέσω Internet θα γίνουν πλήρως ηλεκτρονικές (από το στάδιο της Εγγραφής έως και το στάδιο της Καταμέτρησης) μόνον όταν υιοθετηθεί και υλοποιηθεί μια ενιαία και ασφαλής Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure – PKI), όπου η ταυτοποίηση των ψηφοφόρων στο στάδιο της Εγγραφής και της Επικύρωσης θα γίνεται με τη χρήση ψηφιακών υπογραφών / ψηφιακών πιστοποιητικών, ενώ η ακεραιότητα και η εμπιστευτικότητα των επικοινωνιών θα υποστηρίζονται από κρυπτογραφικούς αλγόριθμους δημόσιου κλειδιού. Παράλληλα, τα προγράμματα πλοήγησης στο Web θα πρέπει να υποστηρίζουν κρυπτογράφηση και ψηφιακές υπογραφές στο επίπεδο Εφαρμογής του μοντέλου OSI. Επιπλέον, τεχνολογίες όπως SSL/TLS (Secure Socket Layer/Transport Layer Security) και SSH (Secure Shell) πρέπει να επανεκτιμηθούν και να αξιοποιηθούν για την αποτροπή των επιθέσεων πλαστοπροσωπίας και των επιθέσεων ενδιάμεσης οντότητας.

Ασφάλεια Πληροφοριακού Συστήματος. Συνίσταται η χρήση εφαρμογών όπως προγράμματα antivirus και εργαλεία firewalls στα συστήματα-πελάτες, καθώς και Συστήματα Ελέγχου Εισβολής (Intrusion Detection Systems) και firewalls στα συστήματα-εξυπηρετητές. Παράλληλα επιβάλλεται η χρήση διαδικασιών πλεονασμού (redundancy), ανάκαμψης από επίθεση ή δυσλειτουργία στους εξυπηρετητές (π.χ. συστοιχίες δίσκων RAID, δυνατότητες hot swapping, τεχνικές clustering και load balancing για συστοιχίες εξυπηρετητών, αποθηκευτικές μονάδες DLT) στους εξυπηρετητές ή στο επίπεδο της επικοινωνίας (π.χ. ενσύρματα/ ασύρματα μέσα υψηλού ρυθμού διαμεταγωγής) καθώς και η υιοθέτηση αυστηρών ελέγχων στην αξιοπιστία του λογισμικού και του υλικού που χρησιμοποιείται. Ένα συμπληρωματικό μέτρο για τη βελτίωση της διαθεσιμότητας του συστήματος θα ήταν και η παράταση της περιόδου υποβολής ηλεκτρονικών ψήφων, πλέον της μίας ημέρας (αρκεί βεβαίως οι ηλεκτρονικές ψήφοι να καταμετρούνται ταυτόχρονα με τις φυσικές, προκειμένου να διατηρηθεί η νομιμότητα των εκλογών).

Νομικά Θέματα. Πέρα από την ολοκλήρωση της θεσμοθέτησης για τη χρήση ηλεκτρονικών υπογραφών στις ηλεκτρονικές συναλλαγές, όπου ήδη έχουν γίνει σημαντικά βήματα (Σιούλης,2003), απαραίτητη προϋπόθεση αποτελεί και η ύπαρξη νομολογίας που θα κατοχυρώνει την μυστικότητα της ηλεκτρονικής ψήφου και θα προβλέπει επιθέσεις όπως καταναγκασμός του ψηφοφόρου, ηλεκτρονική εισβολή (hacking) και αλλοίωση εκλογικών συστημάτων ή προσωπικών ψήφων, επιθέσεις πλαστοπροσωπίας, επιθέσεις άρνησης εξυπηρέτησης κ.λ.π.

Σε κάθε περίπτωση, υπάρχει η ανάγκη για σχεδιασμό μιας αυστηρής πολιτικής ασφάλειας που θα προβλέπει διαδικασίες για την αντιμετώπιση απειλών και την ανάκαμψη από επιθέσεις. Το προσωπικό που εμπλέκεται στην ανάπτυξη, λειτουργία

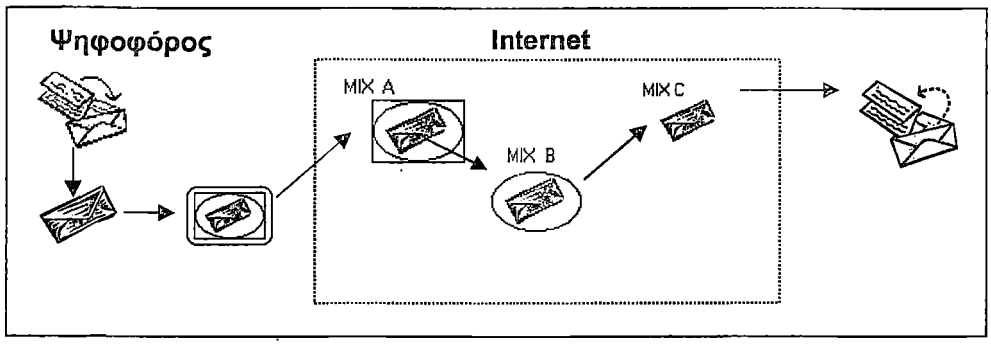
και διαχείριση συστημάτων ηλεκτρονικής ψηφοφορίας πρέπει να επιλέγεται προσεκτικά. Καταλήγοντας, θα λέγαμε ότι οι ψηφοφόροι πρέπει να εκπαιδευτούν και να ενημερωθούν για όλες τις πτυχές (σχεδιασμός και υλοποίηση) ενός συστήματος ηλεκτρονικής ψηφοφορίας.

4.1.4 Κρυπτογραφικά Μοντέλα Ασφάλειας

Τα βασικά κρυπτογραφικά μοντέλα ηλεκτρονικής ψηφοφορίας που έχουν προταθεί έως σήμερα είναι: το μοντέλο MIX-net (Chaum,1981), το μοντέλο των «τυφλών» υπογραφών (Fujioka et al.,1993), και το ομομορφικό μοντέλο (Cramer et al.,1997). Σχεδόν όλα τα πρωτόκολλα που έχουν προταθεί ως σήμερα βασίζονται στα παραπάνω τρία μοντέλα[22, 23].

Το Μοντέλο MIX-net. Ο Chaum (1981) εισήγαγε την έννοια των δικτύων MIX-net (MIX networks) τα οποία αποτελούν έναν κρυπτογραφικό μηχανισμό για την κατασκευή ανώνυμων καναλιών (anonymous channels) σε εφαρμογές υψηλής ασφάλειας. Ένα δίκτυο MIX-net αποτελείται από έναν αριθμό εξυπηρετητών, συνδεδεμένων μεταξύ τους, που καλούνται κόμβοι MIX. Κάθε κόμβος MIX λαμβάνει ως είσοδο (input) ένα σύνολο μηνυμάτων (π.χ. τις κρυπτογραφημένες ψήφους), κάνει ορισμένους τυχαίους μετασχηματισμούς και επιστρέφει στην έξοδο (output) ένα διαφορετικό σύνολο (των ίδιων, μετασχηματισμένων) μηνυμάτων, κατά τρόπο ώστε τα μηνύματα της εξόδου να μη μπορούν να συνδεθούν με τα μηνύματα της εισόδου. Κατ' αυτόν τον τρόπο, καμία συνεργία οποιουδήποτε αριθμού κόμβων MIX (εκτός από την περίπτωση όπου συνεργούν όλοι οι κόμβοι) δε μπορεί να αποφανθεί περί του ποια ψήφος αντιστοιχεί σε ποιόν ψηφοφόρο

Στην (Chaum,1981) κάθε ψήφος κρυπτογραφείται διαδοχικά με τα δημόσια κλειδιά όλων των κόμβων MIX, με σειρά αντίστροφη της σειράς των κόμβων – Σχήμα 4.1.4(α). Η ψήφος κρυπτογραφείται πρώτα με το δημόσιο κλειδί του MIX_C που θα παραλάβει τελευταίο τη λίστα με τις κρυπτογραφημένες ψήφους, στη συνέχεια με το κλειδί του προτελευταίου MIX_B και τέλος με το δημόσιο κλειδί του πρώτου τη τάξει MIX_A. Κάθε κόμβος MIX αποκρυπτογραφεί τη λίστα των ψήφων που του αποστέλλονται, τη μετασχηματίζει (π.χ. προσθέτοντας τυχαιότητα σε κάθε ψήφο και αναδιατάσσοντας τη λίστα με τις ψήφους που προκύπτει), και στη συνέχεια την προωθεί στον επόμενο κόμβο. Αυτό το μοντέλο καλείται MIX-net αποκρυπτογράφησης (Chaum,1981). Σε ένα παραπλήσιο μοντέλο, σε κάθε κόμβο MIX λαμβάνει χώρα μόνον ο μετασχηματισμός των ψήφων, και στη συνέχεια όλοι οι κόμβοι συνεργάζονται για την αποκρυπτογράφηση της τελικής λίστας των ψήφων (Hirt,2000).



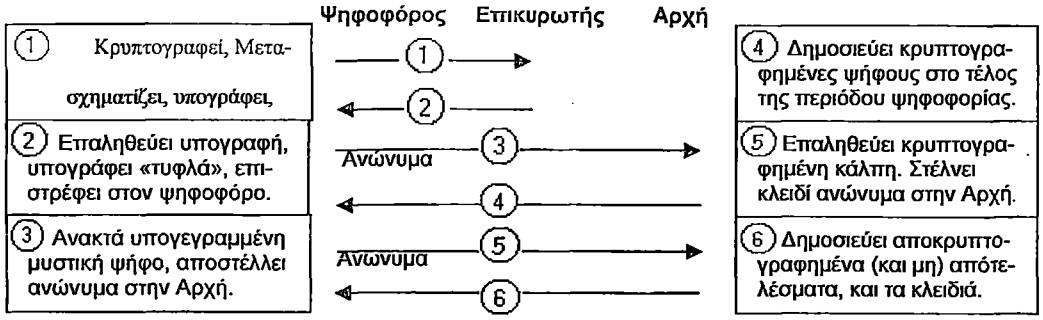
Σχήμα4.1.4(α):Ένα παράδειγμα ενός δικτύου MIX-net με τρεις κόμβους MIX

Ένας άλλος τύπος είναι το MIX-net επανακρυπτογράφησης (Jakobsson,1999), όπου όλες οι ψήφοι κρυπτογραφούνται με το δημόσιο κλειδί του πρώτου κόμβου MIX, και στη συνέχεια σε κάθε κόμβο MIX λαμβάνει χώρα ο μετασχηματισμός και η κρυπτογράφηση με το δημόσιο κλειδί του επόμενου κόμβου, κατά τρόπο επαληθεύσιμο (μεταξύ των κόμβων ή/και για τους εξωτερικούς παρατηρητές).

Οι πλέον χρήσιμες ιδιότητες των δικτύων MIX-net, ειδικά για εκλογές μεγάλης κλίμακας, είναι η οικουμενική επαληθευσιμότητα της ορθότητας των μετασχηματισμών και της αποκρυπτογράφησης που προσφέρουν, καθώς και η ανθεκτικότητα τους έναντι συνεργιών μεταξύ (έως) ενός ορισμένου αριθμού MIX. Για αυτούς τους λόγους τα δίκτυα MIX-net έχουν χρησιμοποιηθεί κατά καιρούς για την επίτευξη ανωνυμίας σε εφαρμογές ηλεκτρονικού εμπορίου. Έως σήμερα πάντως, κανένα σύστημα ηλεκτρονικής ψηφοφορίας δεν έχει υλοποιηθεί με χρήση τεχνικών MIX-net.

Το Μοντέλο των «Τυφλών» Υπογραφών. Η έννοια της «τυφλής» υπογραφής (blind signature) παρουσιάστηκε αρχικά ως μια κρυπτογραφική μέθοδος για την υπογραφή ενός μηνύματος χωρίς τη γνώση του μηνύματος καθ' αυτού. Θα μπορούσαν, χρησιμοποιώντας ένα παράδειγμα της καθημερινής ζωής, να αντιστοιχιστούν με την υπογραφή (εξωτερικά) ενός σφραγισμένου φακέλου που περιέχει ένα χαρτί τοποθετημένο κάτω από καρμπόν. Όταν ο φάκελος αργότερα ανοιχτεί από τον νόμιμο παραλήπτη, το χαρτί θα έχει αποτυπωμένη την υπογραφή (Schneier,1996).

Αυτή η μέθοδος, αν και εφαρμόστηκε αρχικά σε εφαρμογές ηλεκτρονικού χρήματος (e-cash), χρησιμοποιήθηκε επίσης για την επίλυση του προβλήματος της Επικύρωσης των ψήφων με παράλληλη προστασία της μυστικότητας τους (Fujioka et al.,1993) - Σχήμα 4.1.4(β).



Σχήμα4.1.4(β):Ένα παράδειγμα ηλεκτρονικής ψηφοφορίας με «τυφλές» υπογραφές

Έως σήμερα έχουν προταθεί αρκετά σχήματα που βασίζονται στον μηχανισμό των «τυφλών» υπογραφών (π.χ. (Okamoto,1997)). Επίσης, αρκετά συστήματα έχουν υλοποιηθεί πιλοτικά σε εκλογές μικρής κλίμακας (Το σύστημα SENSUS – διενέργεια ηλεκτρονικών εκλογών μέσω Internet, το σύστημα EVOX - εκλογές προπτυχιακών φοιτητών στο MIT) (Burmester,2002).

Ένα πλεονέκτημα των συστημάτων που ακολουθούν το μοντέλο των «τυφλών» υπογραφών είναι ότι απαιτούν χαμηλό επικοινωνιακό φόρτο και υπολογιστικό κόστος, ακόμα και όταν ο αριθμός των ψηφοφόρων / υποψηφίων είναι μεγάλος (scalability). Επιπλέον, η μυστικότητα των ψήφων επαφίεται στους ψηφοφόρους, κάτι που ευνοεί την εύκολη και ασφαλή διαχείριση του συστήματος από την (συνήθως μια) Αρχή.

Ένα σημαντικό μειονέκτημα των συστημάτων «τυφλής» υπογραφής είναι ότι απαιτούν από τον ψηφοφόρο να είναι ενεργός (online) σε όλα τα στάδια της ψηφοφορίας. Επίσης τα συστήματα αυτά προσφέρουν μόνο ατομική επαληθευσιμότητα (οι ψηφοφόροι μπορούν να εντοπίζουν και να διορθώνουν τα λάθη που αφορούν μόνον τη δική τους ψήφο). Πρόσφατα έχουν επίσης προταθεί πρωτόκολλα όπου η δύναμη του Επικυρωτή είναι κατανεμημένη (distributed), με τη χρήση κρυπτογραφικών τεχνικών τύπου threshold (Durette,1999).

Το Ομομορφικό Μοντέλο Κρυπτογράφησης. Το μοντέλο αυτό (Cramer et al.,1997) χρησιμοποιεί τις ομομορφικές ιδιότητες ορισμένων αλγορίθμων κρυπτογράφησης για να εδραιώσει οικουμενική επαληθευσιμότητα σε εκλογές μεγάλης κλίμακας, διατηρώντας παράλληλα τη μυστικότητα των ατομικών ψήφων. Κατά την ομομορφική κρυπτογράφηση υπάρχει μια πράξη $\oplus$ ορισμένη στο σύνολο των μηνυμάτων και μια πράξη $\otimes$ ορισμένη στο σύνολο των κρυπτογραφημάτων (συνήθως οι πράξεις αυτές είναι το άθροισμα και ο πολλαπλασιασμός, modulo έναν μεγάλο αριθμό), τέτοιες ώστε το «γινόμενο» των κρυπτογραφήσεων οποιωνδήποτε δύο ψήφων $v_1, v_2 : E(v_1) \otimes E(v_2)$, να ισούται με την κρυπτογράφηση $E(v_1 \oplus v_2)$ του «αθροίσματος» των ψήφων. Κατ' αυτόν τον τρόπο, η ταυτότητα του ψηφοφόρου δεν χρειάζεται να προστατευτεί με τεχνικές ανωνυμίας (π.χ. δίκτυα MIX-net, «τυφλές» υπογραφές), αφού καμία ψήφος δεν αποκρυπτογραφείται μεμονωμένα, αλλά όλες οι ψήφοι συνδυάζονται και το τελικό κρυπτογράφημα αποκρυπτογραφείται από τις Αρχές του συστήματος.

Το σύστημα VoteHere (Adler et al.,2000), το οποίο ήδη χρησιμοποιείται πιλοτικά σε τοπικές εκλογές μικρής κλίμακας, αποτελεί μια υλοποίηση του ομομορφικού μοντέλου κρυπτογράφησης. Ένα μειονέκτημα των συστημάτων που βασίζονται στο

ομομορφικό μοντέλο είναι η περιορισμένη ευκαμψία τους (flexibility), καθώς οι ψήφοι συνήθως περιορίζονται σε δίτιμες ψήφους του τύπου «Ναι»/«Όχι» (π.χ. {+1, -1}). Για μεγάλο αριθμό υποψηφίων, οι υλοποιήσεις του μοντέλου συνεπάγονται υψηλό υπολογιστικό κόστος για τους εξυπηρετητές. Ωστόσο πρόσφατα έχουν προταθεί εναλλακτικά κρυπτογραφικά σχήματα, των οποίων η υπολογιστική πολυπλοκότητα είναι είτε γραμμική (linear) είτε λογαριθμική (logarithmic) ως προς τον αριθμό των υποψήφιων (Damgard et al., 2003).

4.1.5 Πλεονεκτήματα Συστημάτων Ηλεκτρονικής Ψηφοφορίας

Οι τεχνολογίες συστημάτων ηλεκτρονικής ψηφοφορίας πλεονεκτούν σημαντικά έναντι των παραδοσιακών συστημάτων ψηφοφορίας, κυρίως γιατί στοχεύουν σε δημοκρατικές διαδικασίες και ενθαρρύνουν τη συμμετοχή των χρηστών, πολιτών. Τα σημαντικότερα πλεονεκτήματα των συστημάτων ηλεκτρονικής ψηφοφορίας είναι[24]:

Χαμηλό κόστος: Μηδαμινό κόστος για την εκτύπωση και τη διανομή ψηφοδελτίων. Επιπλέον επιτυγχάνεται ιδιαίτερα χαμηλό κόστος ανθρώπινου δυναμικού συγκριτικά με τα κλασσικά συστήματα ψηφοφορίας.

Βελτιωμένη συμμετοχή και πρόσθετες επιλογές: Σύγχρονα γραφικά περιβάλλοντα υποστηρίζουν μία πληθώρα επιλογών προς όφελος των ψηφοφόρων. Επιπρόσθετα, τα συστήματα ηλεκτρονικής ψηφοφορίας παρέχουν μεγάλη ευκολία στον χρήστη να ψηφήσει από οποιοδήποτε γεωγραφικό σημείο, ενθαρύνωντας τη συμμετοχή.

Υψηλή ταχύτητα και ακρίβεια στις διαδικασίες καταμέτρησης ψήφων (tallying procedures): Η καταμέτρηση των ηλεκτρονικών ψήφων, η διανομή των αποτελεσμάτων και οι διαδικασίες ελέγχου του βαθμού εγκυρότητας των ψήφων εκτελούνται με ακρίβεια και σε σύντομο χρονικό διάστημα.

Ευελιξία (Flexibility): Ποικίλες τροποποιήσεις στο ηλεκτρονικό ψηφοδέλτιο, υποστήριξη πολλαπλών γλωσσών είναι μερικά από τα πιο σημαντικά χαρακτηριστικά των συστημάτων ηλεκτρονικής ψηφοφορίας όσον αφορά την ευέλικτη συμπεριφορά τους.

Υψηλή προσβασιμότητα για τους ανθρώπους με ειδικές ικανότητες: Σύγχρονα και ανεπτυγμένα γραφικά πληροφοριακά περιβάλλοντα παρέχουν υπηρεσίες υψηλής προσβασιμότητας σε ανθρώπους με ειδικές ανάγκες, έτσι ώστε οι τελευταίοι να ψηφίζουν με ανεξάρτητο και εμπιστευτικό τρόπο.

4.2 Θέματα Ασφαλείας Συστημάτων Ηλεκτρονικής Ψηφοφορίας

Δεκάδες παραδείγματα υπάρχουν στο διαδίκτυο σχετικά με αστοχίες των συστημάτων ηλεκτρονικής ψηφοφορίας. Από τις πιο σημαντικές αποτυχίες είναι η καταμέτρηση των ψήφων στις εκλογές των ΗΠΑ 2000 και 2004. Τα ποσοστά των σφαλμάτων στα σύγχρονα συστήματα μπορεί να είναι σημαντικά. Μερικές τεχνολογίες ψηφοφορίας έχουν ποσοστό σφάλματος 5% : για έναν στους είκοσι ανθρώπους που ψηφίζουν χρησιμοποιώντας το σύστημα, οι ψήφοι τους δεν καταμετρούνται σωστά [25].

Πριν προχωρήσουμε σε τεχνικά θέματα ασφάλειας και τη μεθοδολογία εφαρμογής μίας αρχιτεκτονικής υπολογιστικού πλέγματος σε ένα σύστημα ηλεκτρονικής ψηφοφορίας είναι σωστό να αναφερθούμε στις βασικές αρχές ασφαλείας που διέπουν ένα εκλογικό σύστημα, άρα και ένα σύστημα ηλεκτρονικής ψηφοφορίας:

- Ακεραιότητα (Integrity): Η καταμέτρηση των ψήφων πρέπει να γίνεται με ακριβή τρόπο. Επιπλέον, όταν ο χρήστης ψηφίσει στο σύστημα η ψήφος του πρέπει να παραμένει αμετάβλητη και ακέραια.

- Εμπιστευτικότητα (Confidentiality): Κάθε ψήφος στο σύστημα πρέπει να παραμένει μυστική και με κανένα τεχνικό ή άλλον τρόπο δεν πρέπει να αποκαλύπτονται οι προτιμήσεις των ψηφοφόρων.

- Διαθεσιμότητα (Availability): Υπάρχουν συστήματα ηλεκτρονικής ψηφοφορίας που πρέπει να εξυπηρετήσουν περισσότερο από 100 εκατομμύρια ανθρώπους. Οι υπηρεσίες των παραπάνω συστημάτων πρέπει να είναι διαθέσιμες οποιαδήποτε χρονική στιγμή θελήσει ο ψηφοφόρος να συνδεθεί.

Υπάρχουν αρκετές παράμετροι που πρέπει να ληφθούν σοβαρά υπ' όψιν ώστε να γίνει εφικτή η διεξαγωγή ηλεκτρονικών εκλογών μέσω Internet:

Πρωτόκολλα / Λογισμικό: Για να είναι ασφαλής η ηλεκτρονική ψηφοφορία, το σύστημα θα πρέπει να υλοποιεί ένα κρυπτογραφικό πρωτόκολλο (τα υποψήφια μοντέλα περιγράφονται στην Ενότητα 5) που ικανοποιεί τις απαιτήσεις ασφάλειας (Ενότητα 2). Για λόγους αξιοπιστίας επίσης, θεωρούμε πως το σύστημα θα πρέπει να υλοποιηθεί με ανοικτό λογισμικό (open source). Το σύστημα πρέπει επίσης να συνοδεύεται από τους κατάλληλους μηχανισμούς παρακολούθησης (monitoring) και επαλήθευσης (audit) της λειτουργίας του. Ανεξάρτητοι ηλεκτρονικοί ή φυσικοί μηχανισμοί επαλήθευσης ενδεχομένως να αυξήσουν την εμπιστοσύνη των πολιτών στο αποτέλεσμα των εκλογών. Για παράδειγμα, η Mercuri (1992) πρότεινε την εκτύπωση των επιλογών του ψηφοφόρου σε χαρτί, το οποίο ο ψηφοφόρος θα ρίχνει σε μια φυσική κάλπη για τις ανάγκες μιας δεύτερης καταμέτρησης.

Υποδομή Δημόσιου Κλειδιού: Οι εκλογές μέσω Internet θα γίνουν πλήρως ηλεκτρονικές (από το στάδιο της Εγγραφής έως και το στάδιο της Καταμέτρησης) μόνον όταν υιοθετηθεί και υλοποιηθεί μια ενιαία και ασφαλής Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure – PKI), όπου η ταυτοποίηση των ψηφοφόρων στο στάδιο της Εγγραφής και της Επικύρωσης θα γίνεται με τη χρήση ψηφιακών υπογραφών / ψηφιακών πιστοποιητικών, ενώ η ακεραιότητα και η εμπιστευτικότητα των επικοινωνιών θα υποστηρίζονται από κρυπτογραφικούς αλγόριθμους δημόσιου κλειδιού. Παράλληλα, τα προγράμματα πλοήγησης στο Web θα πρέπει να υποστηρίζουν κρυπτογράφηση και ψηφιακές υπογραφές στο επίπεδο Εφαρμογής του μοντέλου OSI. Επιπλέον, τεχνολογίες όπως SSL/TLS (Secure Socket Layer/Transport Layer Security) και SSH (Secure Shell) πρέπει να επανεκτιμηθούν και να αξιοποιηθούν για την αποτροπή των επιθέσεων πλαστοπροσωπίας και των επιθέσεων ενδιάμεσης οντότητας.

Ασφάλεια Πληροφοριακού Συστήματος: Συνίσταται η χρήση εφαρμογών όπως προγράμματα antivirus και εργαλεία firewalls στα συστήματα-πελάτες, καθώς και Συστήματα Ελέγχου Εισβολής (Intrusion Detection Systems) και firewalls στα συστήματα-εξυπηρετητές. Παράλληλα επιβάλλεται η χρήση διαδικασιών πλεονασμού (redundancy), ανάκαμψης από επίθεση ή δυσλειτουργία στους εξυπηρετητές (π.χ. συστοιχίες δίσκων RAID, δυνατότητες hot swapping, τεχνικές clustering και load balancing για συστοιχίες εξυπηρετητών, αποθηκευτικές μονάδες DLT) στους εξυπηρετητές ή στο επίπεδο της επικοινωνίας (π.χ. ενσύρματα/ ασύρματα μέσα υψηλού ρυθμού διαμεταγωγής) καθώς και η υιοθέτηση αυστηρών ελέγχων στην αξιοπιστία του λογισμικού και του υλικού που χρησιμοποιείται. Ένα συμπληρωματικό μέτρο για τη βελτίωση της διαθεσιμότητας του συστήματος θα ήταν και η παράταση της περιόδου υποβολής ηλεκτρονικών ψήφων, πλέον της μίας ημέρας (αρκεί βεβαίως οι ηλεκτρονικές ψήφοι να καταμετρούνται ταυτόχρονα με τις φυσικές, προκειμένου να διατηρηθεί η νομιμότητα των εκλογών).

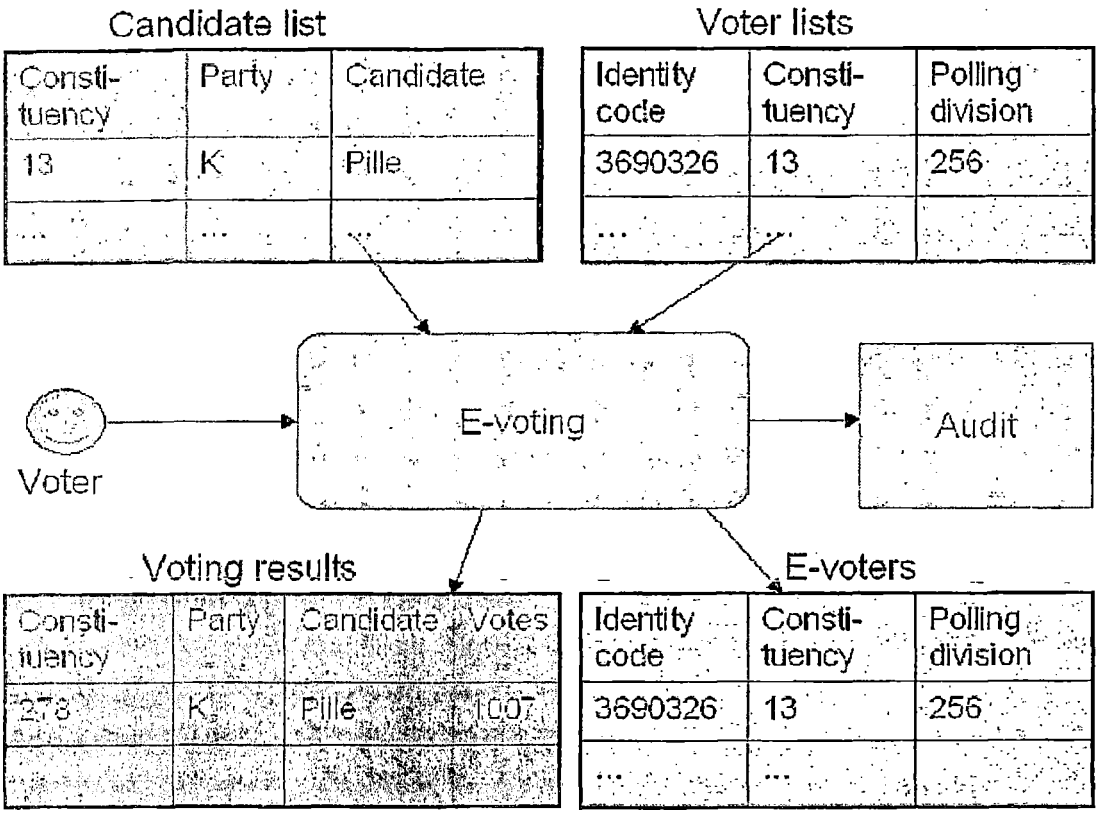
Νομικά Θέματα: Πέρα από την ολοκλήρωση της θεσμοθέτησης για τη χρήση ηλεκτρονικών υπογραφών στις ηλεκτρονικές συναλλαγές, όπου ήδη έχουν γίνει σημαντικά βήματα (Σιούλης,2003), απαραίτητη προϋπόθεση αποτελεί και η ύπαρξη νομολογίας που θα κατοχυρώνει την μυστικότητα της ηλεκτρονικής ψήφου και θα προβλέπει επιθέσεις όπως καταναγκασμός του ψηφοφόρου, ηλεκτρονική εισβολή (hacking) και αλλοίωση εκλογικών συστημάτων ή προσωπικών ψήφων, επιθέσεις πλαστοπροσωπίας, επιθέσεις άρνησης εξυπηρέτησης κ.λ.π.

Σε κάθε περίπτωση, υπάρχει η ανάγκη για σχεδιασμό μιας αυστηρής πολιτικής ασφάλειας που θα προβλέπει διαδικασίες για την αντιμετώπιση απειλών και την ανάκαμψη από επιθέσεις. Το προσωπικό που εμπλέκεται στην ανάπτυξη, λειτουργία και διαχείριση συστημάτων ηλεκτρονικής ψηφοφορίας πρέπει να επιλέγεται προσεκτικά. Καταλήγοντας, θα λέγαμε ότι οι ψηφοφόροι πρέπει να εκπαιδευτούν και να ενημερωθούν για όλες τις πτυχές (σχεδιασμός και υλοποίηση) ενός συστήματος ηλεκτρονικής ψηφοφορίας.

4.3 Αξιοποίηση Υπηρεσιών Ασφαλείας Υπολογιστικού πλέγματος σε Συστήματα Ηλεκτρονικής Ψηφοφορίας

Στα προηγούμενα κεφάλαια μελετήθηκαν οι αρχιτεκτονικές, τα μοντέλα ασφάλειας, τα πλάνα σχεδιασμού και τα βασικά προϊόντα υπολογιστικού πλέγματος. Στόχος είναι η αξιοποίηση των παραπάνω τεχνικών και η εφαρμογή τους σε ένα σύστημα ηλεκτρονικής ψηφοφορίας έτσι ώστε να καλύπτονται οι απαιτήσεις ασφαλείας του τελευταίου (βλέπε υπό-ενότητα 4.2) [26].

Για να προχωρήσουμε στην εφαρμογή τεχνικών ασφάλειας και υπηρεσιών ενός υπολογιστικού πλέγματος για ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει σε πρώτη φάση να μελετήσουμε τις διαδικασίες, τις οντότητες και τις υπηρεσίες που παρέχουν τα συστήματα ηλεκτρονικής ψηφοφορίας και σε δεύτερη φάση να αναγνωρίσουμε εκείνα τα σημεία στην αρχιτεκτονική του συστήματος που πρέπει να εφαρμοσθούν οι τεχνικές ασφαλείας. Στο σχήμα 4.3 παρατηρούμε τη βασική δομή που χαρακτηρίζει ένα οποιοδήποτε σύστημα ηλεκτρονικής ψηφοφορίας. Εν συνεχεία ακολουθεί ένας σύντομος ορισμός για το ρόλο της κάθε οντότητας στο σύστημα.



Σχήμα 4.3: Δομή ενός Συστήματος Ηλεκτρονικής Ψηφοφορίας

Voter (Ψηφοφόρος): Αντιπροσωπεύει την εφαρμογή του χρήστη-ψηφοφόρου. Μέσω της εφαρμογής αυτής ο ψηφοφόρος μπορεί να συμμετέχει ενεργά στις διαδικασίες εκλογής των υποψηφίων (Candidates) καταθέτοντας την προσωπική ψήφο του.

E-Voting (Κεντρικό σύστημα ηλεκτρονικής ψηφοφορίας): Η οντότητα e-voting είναι η βασική οντότητα/πλατφόρμα του συστήματος. Αλληλεπιδρά με όλες τις άλλες οντότητες στο σύστημα και είναι υπεύθυνη για τις παρακάτω ενέργειες:

- Ενημέρωση των χρηστών για την λίστα των υποψηφίων που διαγωνίζονται
- Ενημέρωση των χρηστών ότι η ψήφος τους καταμετρήθηκε επιτυχώς
- Καταμέτρηση της ψήφου στη βάση δεδομένων (Voting results)
- Ενημέρωση της βάσης δεδομένων (E-voters) ότι ο ψηφοφόρος Α ψήφισε επιτυχώς
- Επικοινωνία με την οθόνη καταγραφής ενεργειών (Audit)
- Επικοινωνία με τη βάση δεδομένων (Voter List) για την αυθεντικοποίηση των χρηστών στο σύστημα

Ποικίλες βάσεις δεδομένων: Οι οντότητες Voting Results, E-Voters, Voter Lists και Candidate List είναι βάσεις δεδομένων που ενημερώνουν και ενημερώνονται συνεχώς από την οντότητα E-Voting.

Audit (Σύστημα Καταγραφής δεδομένων): Οι ενέργειες που αφορούν τις κινήσεις των οντοτήτων στο σύστημα οποιαδήποτε χρονική στιγμή καταγράφονται σε μία οθόνη παρακολούθησης.

Στο σχήμα 4.3 παρουσιάζεται μία γενικευμένη αρχιτεκτονική ενός συστήματος ηλεκτρονικής ψηφοφορίας. Τα ζητήματα ασφαλείας που προκύπτουν μελετώντας την παραπάνω αρχιτεκτονική είναι:

- Η εφαρμογή του χρήστη-ψηφοφόρου πρέπει να διασφαλίζει ότι ψηφίζει ηλεκτρονικά μόνο εκείνος ο χρήστης που είναι εξουσιοδοτημένος από το σύστημα και ότι η ψήφος του θα είναι μοναδική (δεν θα είναι σε θέσει να ξανά - ψηφίσει). Επιπλέον η εφαρμογή πρέπει να είναι σε θέση να κατανοεί τυχόν προβλήματα που έχουν προκύψει στο σύστημα και να παραπέμπει το χρήστη σε άλλον εξυπηρετητή αυθεντικοποίησης.

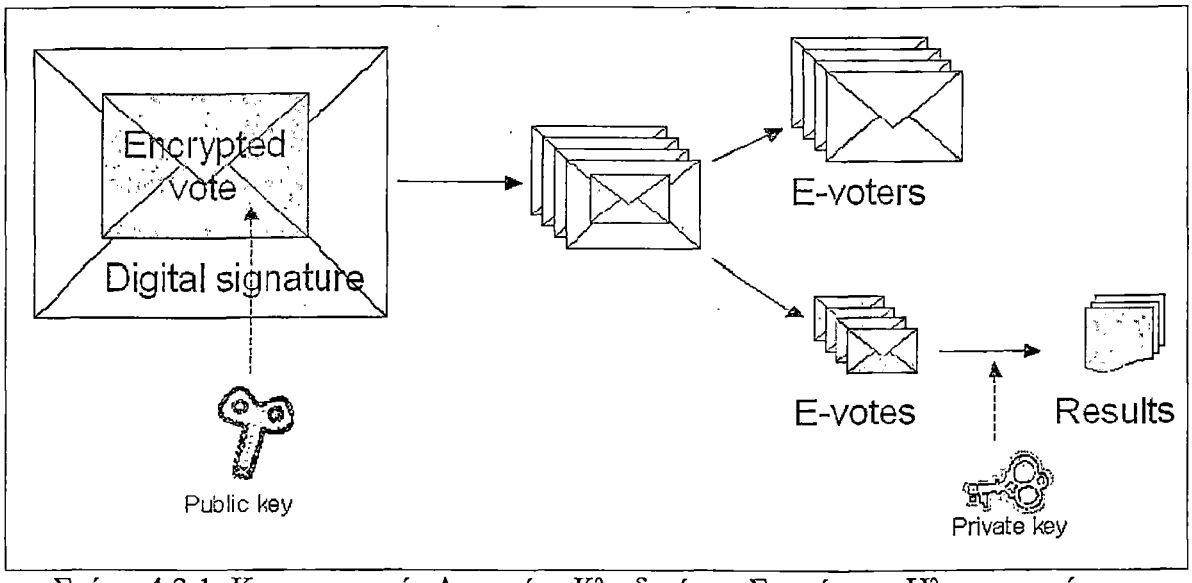
- Όλες οι ενέργειες μέσα στο σύστημα πρέπει να είναι μυστικές τόσο από τους χρήστες όσο και από το διαχειριστή του συστήματος (όσο αυτό είναι εφικτό). Η χρήση κρυπτογραφικών πρωτοκόλλων είναι απαραίτητη.

- Ενεργά-αντίγραφα των βάσεων δεδομένων του συστήματος καθώς και η χρήση *«βυζαντινών πρωτοκόλλων συμφωνίας»* μεταξύ των οντοτήτων ενός συστήματος ηλεκτρονικής ψηφοφορίας και ενός άλλου για την επίτευξη τεχνικών ανθεκτικότητας και διαχείρισης σφαλμάτων.

Οι παραπάνω τεχνικές ασφαλείας αποτελούν βασικά χαρακτηριστικά συστημάτων υπολογιστικού πλέγματος. Στόχος είναι να εμπλουτίσουμε την αρχιτεκτονική ενός συστήματος ηλεκτρονικής ψηφοφορίας με τεχνικές κατανομής (Distribution), κρυπτογραφίας, αυτοματοποίησης και διαμοίρασης υπολογιστικών πόρων (για τη συγκεκριμένη περίπτωση υπολογιστικοί πόροι αποτελούν και οι εξυπηρετητές αυθεντικοποίησης των ψηφοφόρων).

4.3.1 Κρυπτογραφία Δημοσίου Κλειδιού σε Συστήματα Ηλεκτρονικής Ψηφοφορίας

Σε οποιαδήποτε περίπτωση πρέπει η πρόθεση ψήφου να είναι μυστική από όλες τις οντότητες που συμμετέχουν στο σύστημα. Η χρήση κρυπτογραφίας δημοσίου κλειδιού διασφαλίζει τη μυστικότητα και την ακεραιότητα του ψηφοφόρου και της ψήφου αντίστοιχα. Στο σχήμα 4.3.1 παρουσιάζεται η βασική αρχιτεκτονική της κρυπτογραφίας δημοσίου κλειδιού για ένα σύστημα ηλεκτρονικής ψηφοφορίας.



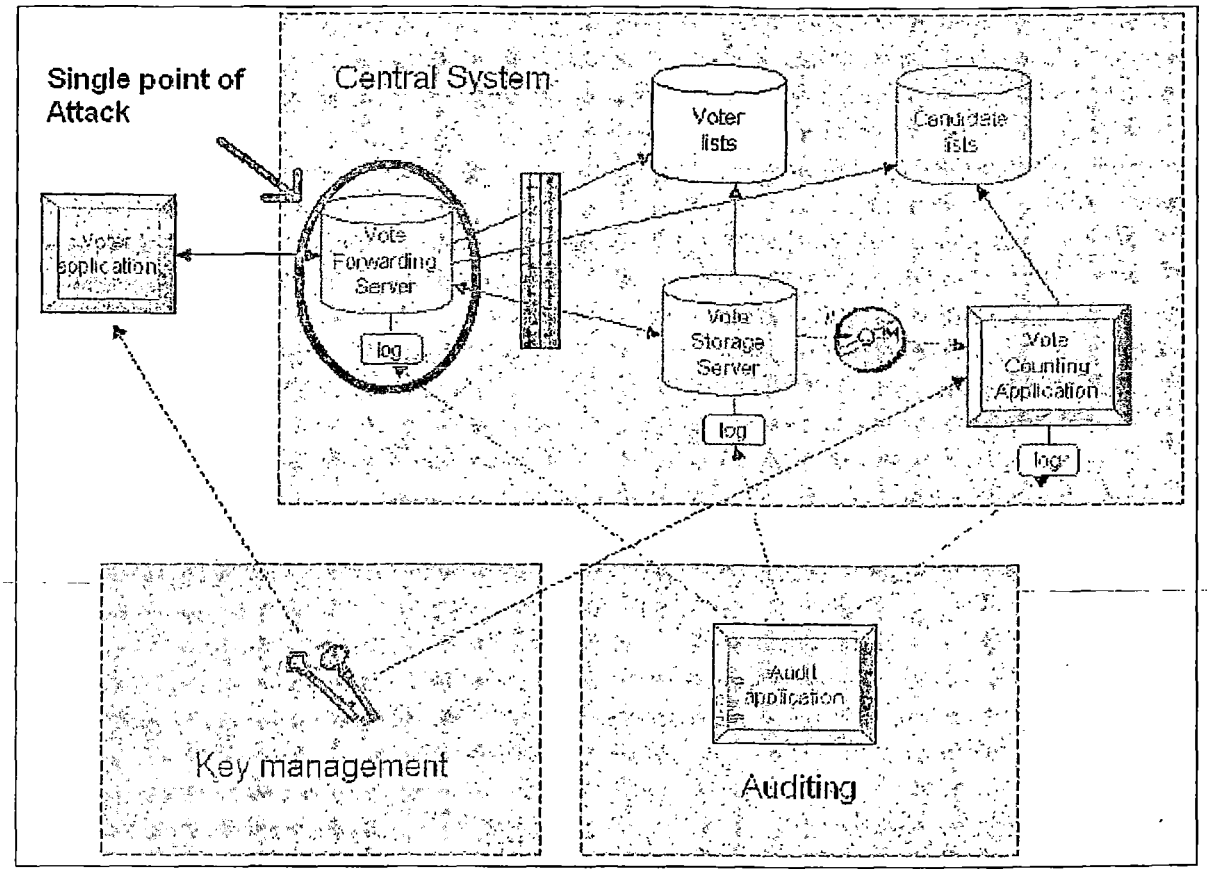
Σχήμα 4.3.1: Κρυπτογραφία Δημοσίου Κλειδιού για Συστήματα Ηλεκτρονικής Ψηφοφορίας

Η εφαρμογή του ψηφοφόρου κρυπτογραφεί την επιλογή του (μοναδικός αριθμός ψηφοφόρου) με το δημόσιο κλειδί του συστήματος και την υπογράφει ψηφιακά (τα ψηφιακά πιστοποιητικά για το χρήστη και το κεντρικό σύστημα μπορεί να τα λάβουν από μία εξωγενή οντότητα για παράδειγμα μία Certificate Authority). Εν συνεχεία το σύστημα ξεχωρίζει τους ψήφους, τους ταξινομεί, διαγράφει τους «μη - νόμιμους» ψήφους και ελέγχει την ταυτότητα του ψηφοφόρου.

Αν όλες οι παραπάνω διαδικασίες ολοκληρωθούν με επιτυχία τότε η ψηφιακή υπογραφή «αποκόπτεται» από την ψήφο. Οι ψήφοι δεν αποκαλύπτουν την ταυτότητα του ψηφοφόρου και εισάγονται στο σύστημα καταγραφής και καταμέτρησης ψήφου, αντίστοιχα η ταυτότητα του ψηφοφόρου ενημερώνεται στη βάση δεδομένων των χρηστών, έτσι ώστε να μην επαναληφθεί η διαδικασία από τον ίδιο χρήστη.

4.3.2 Η Βασική Αρχιτεκτονική του Κεντρικού Συστήματος Ψηφοφορίας

Στο σχήμα 4.3 παρουσιάσθηκαν οι βασικές οντότητες που συμμετέχουν σε ένα σύστημα ηλεκτρονικής ψηφοφορίας. Στο σχήμα 4.3.1 διασφαλίζονται οι διαδικτυακές επικοινωνίες με ένα «δοκιμασμένο» σύστημα κρυπτογραφίας δημοσίου κλειδιού. Αν υπάρξουν θέματα ασφαλείας σίγουρα αυτά θα αφορούν αδυναμίες στο κεντρικό σύστημα ψηφοφορίας. Στο σχήμα 4.3.2(α) παρουσιάζεται αναλυτικά η αρχιτεκτονική της «καρδιάς» του συστήματος.



Σχήμα 4.3.2(α):Αρχιτεκτονική της Βασικής Οντότητας Ηλεκτρονικής Ψηφοφορίας

Το πιο συχνό πρόβλημα που παρουσιάζεται σε οποιαδήποτε εφαρμογή που εξυπηρετεί μαζικά ένα μεγάλο πλήθος χρηστών μέσω του διαδικτύου είναι το DoS (Denial of Services). Η οντότητα VFS (Εξυπηρετητής Προώθησης Ψήφου) είναι υπεύθυνη για την αυθεντικοποίηση του χρήστη και την προώθηση της ψήφου του προς τον VSS (Εξυπηρετητής Αποθήκευσης και Διαχείρισης Ψήφων). Αν η οντότητα VFS δεν βρίσκεται σε θέση να εξυπηρετήσει τους χρήστες στο σύστημα ακολουθείται το παρακάτω πρωτόκολλο επικοινωνίας:

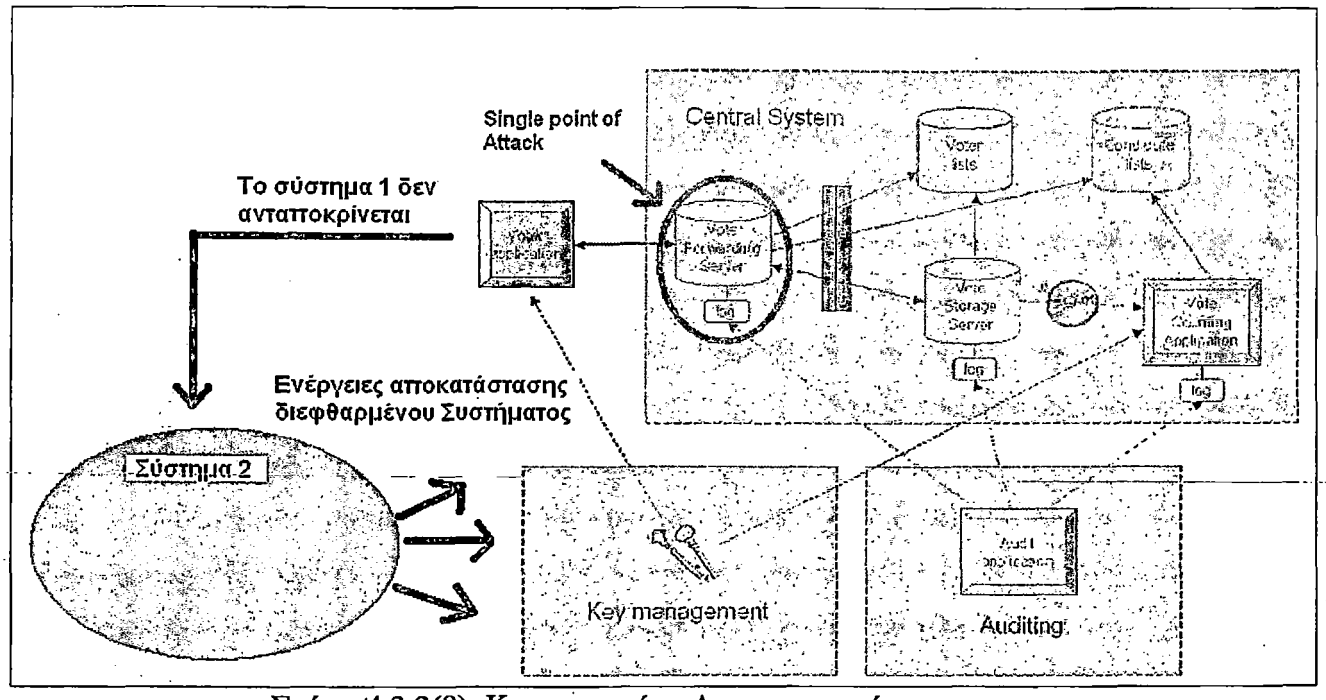
1. Η εφαρμογή του χρήστη έχει στείλει το παρακάτω μήνυμα προς το VFS της περιοχής του πάντα σε κρυπτογραφημένη μορφή.

Ψήφος Χρήστη	Κωδικός Υποψηφίου	Ψηφιακή Υπογραφή	Αριθμός Ακολουθίας Περιοχής Εκλογικού Κέντρου

2. Το τελευταίο πεδίο του μηνύματος υποδηλώνει το εκλογικό κέντρο στο οποίο απευθύνεται ο ψηφοφόρος. Στην περίπτωση που το σύστημα δεν απαντήσει στην εφαρμογή του χρήστη το πολύ σε δέκα δευτερόλεπτα ότι η ψήφος του καταμετρήθηκε επιτυχώς τότε η εφαρμογή του χρήστη αυτόματα στέλνει το μήνυμα στο ποιο κοντινό εκλογικό κέντρο.

3. Το νέο πληροφοριακό σύστημα λαμβάνει τη ψήφο του χρήστη και εφαρμόζει κανονικά τη διαδικασία. Παρόλο αυτά το νέο σύστημα λαμβάνει τον αριθμό ακολουθίας περιοχής εκλογικού κέντρου και ξεκινάει διαδικασίες ελέγχου ακεραιότητας των δεδομένων του συγκεκριμένου κέντρου.

Το σχήμα 4.3.2(α) παραμετροποιείται ως εξής:



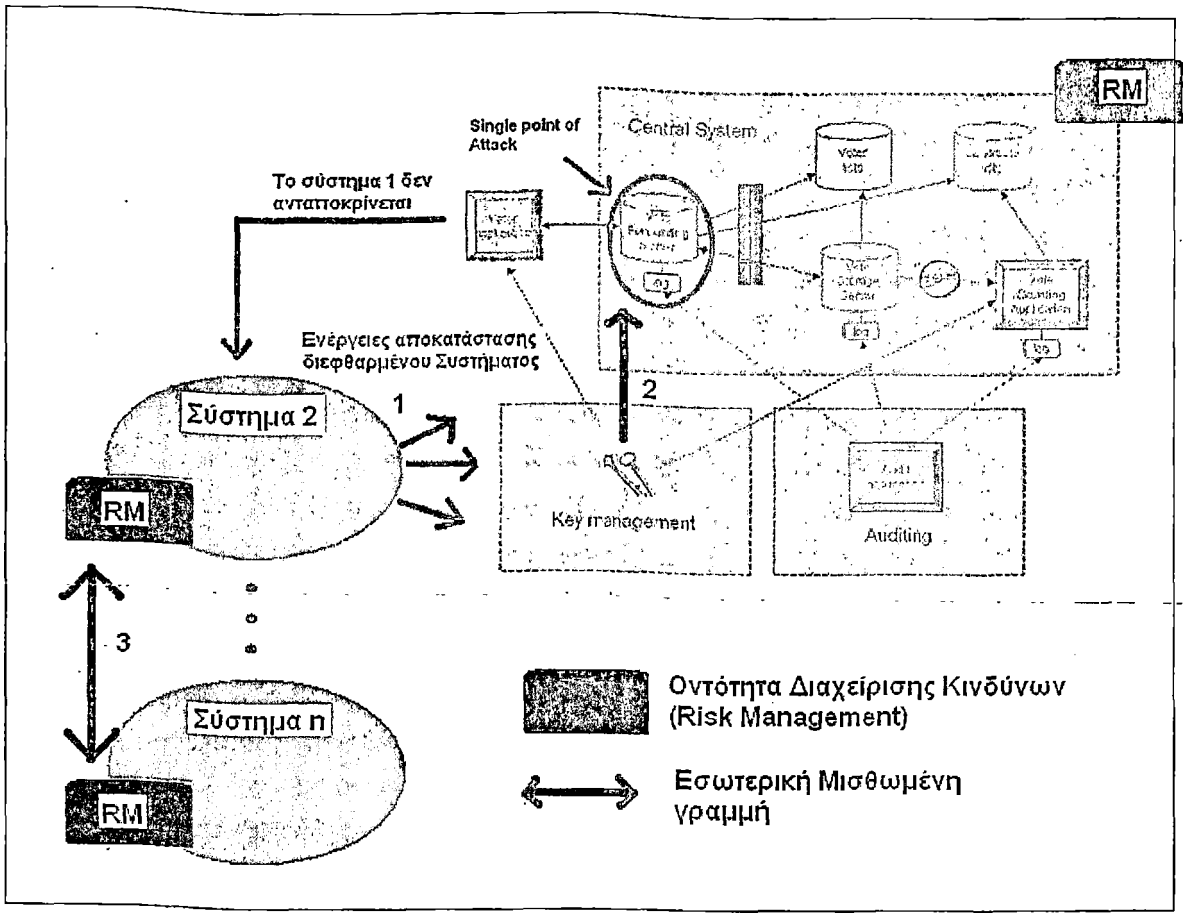
Σχήμα 4.3.2(β): Κατανεμημένη Αρχιτεκτονική

Τα πληροφοριακά συστήματα των εκλογικών κέντρων είναι συνδεδεμένα μεταξύ τους με ιδιωτικό δίκτυο έτσι ώστε να μην υπάρχουν παρεμβολές από εξωγενείς παράγοντες. Το σύστημα 2 (βλέπε σχήμα 4.3.2(β)) ενημερώνεται για τη δυσλειτουργία του συστήματος 1. Το εκλογικό κέντρο 2 πρέπει από την πλευρά του να ενημερώσει όλα τα άλλα συστήματα (εκλογικά κέντρα) και εν συνεχεία να ενημερώσει και την Αρχή Πιστοποίησης.

Λόγω της ανεπαρκής ανταπόκρισης ενός ή περισσοτέρων πληροφοριακών συστημάτων πρέπει να ληφθούν μέτρα αντιμετώπισης του «διεφθαρμένου» (corrupted) συστήματος. Η επίτευξη ενός τέτοιου σεναρίου απαιτεί μία κατανεμημένη αρχιτεκτονική, χρήση κρυπτογραφικών μετρικών και γενικότερα υπηρεσίες ασφάλειας υπολογιστικού πλέγματος.

4.3.3 Μέτρα Αντιμετώπισης Ανάκαμψης Συστήματος Ηλεκτρονικής Ψηφοφορίας

Ο έλεγχος εκείνου του συστήματος ηλεκτρονικής ψηφοφορίας, το οποίο δεν ανταποκρίνεται όπως αναμενόταν, αντικατοπτρίζεται στο σχήμα 4.3.3.



Σχήμα 4.3.3: Διαδικασίες Αντιμετώπισης Επιθέσεων DOS

Η οντότητα RM (Risk Management) προστέθηκε σε κάθε ένα από τα ηλεκτρονικά συστήματα ψηφοφορίας. Επικοινωνεί με όλες τις οντότητες στο σύστημα και εκτός συστήματος επικοινωνεί μόνο με τις άλλες RM οντότητες. Είναι μία ανεξάρτητη οντότητα και είναι υπεύθυνη για τα παρακάτω:

1. Έλεγχος Ακεραιότητας Βάσεων Δεδομένων (Integrity Check)
2. «Βυζαντινό Πρωτόκολλο Επικοινωνίας» (Self – Agreement Protocol)
3. Διευθέτηση θεμάτων Άρνησης Υπηρεσιών
4. Ενημέρωση των οντοτήτων «Αρχής Πιστοποίησης» και «Καταγραφής Στοιχείων»
5. Ενημέρωση Διαχειριστή Συστήματος

Σε συχνά χρονικά διαστήματα κάθε RM οντότητα ενημερώνει μέσω ενός αθροιστικού ελέγχου (checksum) τις άλλες RM οντότητες των συστημάτων ηλεκτρονικής ψηφοφορίας για την κατάσταση της βάσης δεδομένων της. Ο αθροιστικός έλεγχος επιτυγχάνεται μέσω της συνάρτησης σύνοψης MD5 και ενός μυστικού κλειδιού που έχει παραχωρήσει η Αρχή Πιστοποίησης προς όλες τις οντότητες RM. Στην περίπτωση που η τιμή του αθροιστικού ελέγχου διαφέρει σε ένα ή περισσότερα πληροφοριακά συστήματα ηλεκτρονικής ψηφοφορίας τότε άμεσα ακολουθείται το παρακάτω πρωτόκολλο αντιμετώπισης σφαλμάτων (fault tolerant protocol):

1. Πρωτόκολλο Βυζαντινής Επικοινωνίας (Οι RM οντότητες ψηφίζουν ποια είναι η πιο σωστή-ορθή μορφή βάσης δεδομένων)

2. Αν καταλήξουν σε αποτέλεσμα τότε πραγματοποιείται άμεσα η μεταφορά της βάσης δεδομένων προς αντικατάσταση της «διεφθαρμένης» βάσης δεδομένων
3. Διαφορετικά Ενημερώνεται ο διαχειριστής (ανθρώπινος παράγοντας) για να πάρει της κατάλληλες αποφάσεις
4. Ενημέρωση της Αρχής Πιστοποίησης ότι το συγκεκριμένο σύστημα ηλεκτρονικής ψηφοφορίας μπορεί να λειτουργεί με κακόβουλο τρόπο. Η αρχή πιστοποίησης πρέπει να προχωρήσει σε έλεγχο του μυστικού κλειδιού της συγκεκριμένης Οντότητας RM στο σύστημα.

ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΟΠΤΙΚΕΣ ΓΙΑ ΤΟ ΜΕΛΛΟΝ

Για να προχωρήσουμε με σίγουρα βήματα και να προτείνουμε μία ασφαλή και αποδοτική αρχιτεκτονική Ηλεκτρονικού Συστήματος Ψηφοφορίας, η οποία θα εμπεριέχει τεχνικές υπολογιστικού πλέγματος, ήταν απαραίτητο να γίνει εκτενή ανάλυση και μελέτη της περιοχής υπολογιστικού πλέγματος. Εν συνεχεία προχωρήσαμε στην αξιολόγηση εκείνων των εταιριών που παρέχουν υπηρεσίες υπολογιστικού πλέγματος, καταλήγοντας στο συμπέρασμα ότι το Globus Toolkit αποτελεί την πληρέστερη λύση (βλέπε $2^0 - 3^0$ κεφάλαιο).

Γενικότερα το υπολογιστικό πλέγμα έρχεται και εισάγει νέες μεθοδολογίες στους τομείς της διαχείρισης υπολογιστικών πόρων και εκμετάλλευσης δικτυακών υποδομών. Οι δυσκολίες εφαρμογής τεχνικών υπολογιστικού πλέγματος εμφανίζονται στην αυξημένη πολυπλοκότητα σχεδιασμού όσο το υπολογιστικό σύστημα μεγαλώνει (νέοι παράγοντες, ετερογενή συστήματα, θέματα συμβατότητας). Επιπρόσθετα, Δεν έχει υλοποιηθεί κάποιο πρότυπο αρχιτεκτονικής το οποίο να αποτελεί βάση προς όλους. Εξαίρεση αποτελεί το OGSA (Open Grid Security Services) το οποίο αποτελεί για τις περισσότερες εταιρίες που παρέχουν υπηρεσίες υπολογιστικού πλέγματος βάση για την υποδομή ασφαλείας.

Η διείσδυση του Internet στις σύγχρονες κοινωνίες καθιστά επωφελή την υιοθέτηση ηλεκτρονικών μεθόδων για την εξ' αποστάσεως συμμετοχή του πολίτη στις δημοκρατικές αποφάσεις (ψηφοφορίες, referenda, δημοσκοπήσεις κ.λ.π). Τα συστήματα εξ' αποστάσεως ψηφοφορίας μέσω Internet, μαζί με άλλες διαδικασίες που εφαρμόζονται σήμερα σε δημοκρατικά καθεστώτα (π.χ. ψηφοφορία μέσω ταχυδρομείου στην Ελβετία αναμένεται να απλοποιήσουν την υποβολή της ψήφου και να αυξήσουν τη συμμετοχή των πολιτών στις εκλογές. Σε κάθε περίπτωση, η υποβολή ψήφου μέσω Internet θα πρέπει να αποτελέσει μια *εναλλακτική* και όχι τη μοναδική δυνατότητα συμμετοχής του πολίτη στις εκλογές. Σε αντίθετη περίπτωση, θα προέκυπταν ζητήματα κοινωνικού αποκλεισμού και συνταγματικότητας των εκλογών. Σε γενικές γραμμές οι κυριότεροι παράγοντες που αποτρέπουν σήμερα την υιοθέτηση συστημάτων εξ' αποστάσεως ψηφοφορίας μέσω Internet είναι: α) Μη ασφαλή συστήματα υπολογιστών, β) Έλλειψη Υποδομών Δημοσίου Κλειδιού, γ) Έλλειψη Προτύπων (Standards). Παράλληλα, η μετάβαση σε εκλογές μέσω Internet πιθανόν αρχικά να συνεπάγεται υψηλό κόστος αγοράς και συντήρησης υπολογιστικών μηχανών, λογισμικού βάσεων δεδομένων και συστημάτων δρομολόγησης, ωστόσο μακροπρόθεσμα το κόστος αναμένεται να είναι μειωμένο σε σχέση με τις παραδοσιακές εκλογές.

Η μετάβαση σε συστήματα εξ' αποστάσεως ψηφοφορίας μέσω Internet αναμένεται να γίνει σταδιακά, αρχής γενομένης με ψηφοφορίες σε Εκλογικά Σημεία, όπου το φυσικό περιβάλλον και οι επικοινωνίες μπορούν να ελεγχθούν επαρκώς. Θεωρούμε πως, παρά το γεγονός ότι η πρώτη αυτή φάση δεν θα προσφέρει ουσιαστικά πλεονεκτήματα έναντι των παραδοσιακών τρόπων ψηφοφορίας, ωστόσο θα

προσφέρει ένα σημαντικό πεδίο για συζήτηση και απόκτηση εμπειριών για τη μετάβαση σε περισσότερο «φιλελεύθερα» συστήματα (χρήση συσκευών τύπου ATM σε Κιόσκια, PC σε σχολεία, βιβλιοθήκες, δημόσιες υπηρεσίες) με απώτερο σκοπό τη δυνατότητα υποβολής ψήφου από το σπίτι ή το χώρο εργασίας μέσω Internet.

Με την παραπάνω αρχιτεκτονική προσπαθήσαμε να αντιμετωπίσουμε τα βασικότερα προβλήματα που αντιμετωπίζουμε σε συστήματα ηλεκτρονικής ψηφοφορίας. Στόχος είναι η άμεση αντίδραση σε θέματα ρήξεων ασφαλείας όπως οι επιθέσεις άρνησης υπηρεσιών και η αλλοίωση δεδομένων στο κεντρικό σύστημα βάσεων δεδομένων. Για να επιτευχθεί ο στόχος προχωρήσαμε στην υιοθέτηση συγκεκριμένων τεχνικών υπολογιστικού πλέγματος όπως, η κατανεμημένη αρχιτεκτονική, η διαμοίραση υπολογιστικών πόρων και η εφαρμογή κρυπτογραφικών μεθόδων.

ΒΙΒΛΙΟΓΡΑΦΙΑ - ΑΝΑΦΟΡΕΣ

[1] Andrew S.Tanenbaum, "ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ", Τρίτη έκδοση, 2003

[2] www.grid.org

[3] David Groth, Toby Skandier, "Network+ Study Guide", 4η έκδοση, 2005

[4] www.gridforum.org

[5] Gerard J. Holzmann, Rajeev Joshi, "Reliable Software Systems Design: Defect Prevention, Detection, and Containment", 2002

[6] Ian Forest, Carl Kesselman, Jeffrey M.Nick, Steven Tuecke, "The Physiology of the Grid. An Open Grid Services Architecture for Distributed Systems Integration", 2002

[7] www.mathforum.org

[8] www.datamininggrid.org

[9] Heinz Stockinger, "Distributed Database Management Systems and the Data Grid", 2004

[10] William E. Johnston, Dennis Gannon, Bill Nitzberg, Leigh Ann Tanner, Bill Thigpen, Alex Woo, "Computing for Data Grid for Software and Engineering", 2004

[11] UK e-Science, Mark Leese, Robin Tasker, "Grid Network Performance Monitoring", 2004

[12] Nataraj Nagaratnam, IBM Philippe Janson, IBM John Dayka, IBM Anthony Nadalin, IBM Frank Siebenlist, ANL Von Welch, UC Steven Tuecke, ANL Ian Foster, ANL, "Security Architecture for Open Grid Services", 2003

[13] Σ. Γκρίτζαλης, Σ. Κάτσικας, Δ. Γκρίτζαλης, "Ασφάλεια Δικτύων Υπολογιστών", 2003

[14] Bruce Schneier, "APPLIED CRYPTOGRAPHY", Δεύτερη Έκδοση, 2000

[15] IBM, "Introduction to Grid Computing with Globus", Red Paper, 2003

[16] www.it-analysis.com, "Grid Computing gaining hold", 2002

[17] Avaki Corporation, "Avaki Grid Software: Concepts and Architecture", 2002

[18] www.datasynapse.com

[19] Andrew Chien, Brad Calder, Stephen Elbert, Karan Batia, "Entropia: architecture and performance of an enterprise desktop grid system ", 2001

[20] www.ud.com

[21] www.platform.com

[22] Phillip J. Windley, "eVoting", 2005

[23] www.theregister.co.uk, Thomas C Greene, "E-voting security: getting it right", 2004

[24] National Election Committee, "E-Voting System Overview", 2005

[25] Deirdre Mulligan, Joseph Lorenzo Hall, "PRELIMINARY ANALYSIS OF E-VOTING PROBLEMS HIGHLIGHTS NEED FOR HEIGHTENED STANDARDS AND TESTING", 2004

[26] Margaret McGaley, J. Paul Gibson, "Electronic Voting: A Safety Critical System", 2003