

# **Ανοικτό Πανεπιστήμιο Κύπρου**

**Σχολή Θετικών και Εφαρμοσμένων Επιστημών**

## **Μεταπτυχιακή Διατριβή στα Πληροφοριακά Συστήματα**



**Κατανεμημένα Κοινωνικά Δίκτυα**

**Αθανάσιος Κάτσης**

**Επιβλέπων Καθηγητής  
Ιωάννης Ρεφανίδης**

**Ιανουάριος 2013**

# **Ανοικτό Πανεπιστήμιο Κύπρου**

## **Σχολή Θετικών και Εφαρμοσμένων Επιστημών**

**Κατανεμημένα Κοινωνικά Δίκτυα**  
**Αθανάσιος Κάτσης**

**Επιβλέπων Καθηγητής**  
**Ιωάννης Ρεφανίδης**

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε  
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών  
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών  
του Ανοικτού Πανεπιστημίου Κύπρου

**Ιανουάριος 2013**

## Περίληψη

Τα τελευταία χρόνια τα κοινωνικά δίκτυα (blogs, facebook, twitter, youtube, flicker, κα.) προσελκύουν ολοένα και περισσότερους χρήστες. Βασικό γνώρισμα όλων αυτών των δικτύων είναι ότι η πρωτογενής πληροφορία είναι συγκεντρωμένη στους διαδικτυακούς εξυπηρετητές μιας υπηρεσίας. Η αρχιτεκτονική αυτή εγείρει διάφορα σοβαρά θέματα, όπως νομικά, που αφορά την αμφισβήτηση της κυριότητας της πληροφορίας και ηθικά, που αφορά προστασία του απορρήτου. Για το λόγο αυτό έχουν προταθεί καταναμημένες αρχιτεκτονικές κοινωνικών δικτύων, οι οποίες βασίζονται σε ανοικτά πρωτόκολλα επικοινωνίας και οντολογίες.

Μια από τις βασικές υπηρεσίες που προσφέρουν οι καταναμημένες αρχιτεκτονικές είναι, ότι τα δεδομένα των χρηστών αποθηκεύονται τοπικά, συνήθως σε διαδικτυακό εξυπηρετητή (web server) ή σε προσωπικό υπολογιστή του χρήστη. Αξίζει να σημειώσουμε εδώ ότι, ο χρήστης έχει πλήρη δικαιώματα διαχείρισης του περιεχομένου του και στις δυο περιπτώσεις συστημάτων αποθήκευσης δεδομένων που προαναφέραμε. Για την επίτευξη ωστόσο της ίδιας λειτουργικότητας με τις κεντροποιημένες αρχιτεκτονικές, απαιτείται συνήθως κεντρική ή καταναμημένη δεικτοδότηση των δεδομένων, όπως για παράδειγμα το thepiratebay.org. Ωστόσο υπάρχουν και παραδείγματα όπου υπάρχει μόνο peer-to-peer επικοινωνία μεταξύ των χρηστών της υπηρεσίας όπως το Emule, KaazA, Gnutella κ.α.

Βασισμένοι λοιπόν, στις διαφορές που υπάρχουν μεταξύ των μεθοδολογιών των καταναμημένων κοινωνικών δικτύων που έχουν προταθεί μέχρι σήμερα, σε αυτήν την εργασία, εντοπίσαμε και αναλύσαμε τις δυνατότητες που αφορούν, την αυξημένη ασφάλεια και την κυριότητα, στα δεδομένα των χρηστών.

Επιπρόσθετα, μελετήσαμε και συγκρίναμε τις εναλλακτικές αρχιτεκτονικές, πρωτόκολλα επικοινωνίας, οντολογίες και τοπολογίες για την υλοποίηση καταναμημένων κοινωνικών δικτύων που έχουν προταθεί μέχρι σήμερα, τόσο μεταξύ τους όσο και σε σχέση με τις κεντροποιημένες αρχιτεκτονικές.

Στηριζόμενοι στις πιο πάνω αρχιτεκτονικές σχεδιάσαμε ένα υποτυπώδες πρότυπο καταναμημένου κοινωνικού δικτύου, το οποίο θα φιλοξενείτε σε έναν προσωπικό διακομιστή διαδικτύου.

**Λέξεις Κλειδιά:** καταναμημένα κοινωνικά δίκτυα, σύστημα ομότιμων δεδομένων, σύστημα ομότιμων κόμβων βασισμένο σε σχήμα.

## Summary

In recent years the social networks (blogs, facebook, twitter, youtube, flicker, etc.) attract more and more users. Key feature of all these social networks is that the primary information is concentrated on the servers as a service.

This architecture raises several serious issues, such as ownership (who is the owner of information) and ethical (protection of privacy). For this reason have been proposed many architectures of distributed social networks based on open communication protocols and ontologies.

On this type of architectures, the data are stored locally, usually in a web server where the user has access. However, to achieve the same functionality with centralized architectures, usually require centralized or distributed indexing of data (e.g. thepiratebay.org). Also, there are examples where there is only peer-to-peer communication between users of the service (e.g. emule, Gnutella, KaazA etc.).

Based on differences, where may exist between the methodologies of distributed social networks that have been proposed so far, in this work, we have identified and analyzed the potential for increased safety and ownership in user data.

Additionally, we have examined and compared the alternative architectures, communication protocols, ontologies and topologies for distributed social networks that have been proposed so far, both among themselves and in relation with centralized architectures.

Moreover, we have designed a rudimentary model of distributed social network, which will be host to a personal web server, based on the above architectures that we have analyzed.

**Keywords:** distributed social network, peer-to-peer system, schema-based peer-to-peer system, semantic data integration.

# Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κ. Ρεφανίδη Ιωάννη, για την πολύτιμη βοήθεια του για την υλοποίηση αυτής της μεταπτυχιακής διατριβής, καθώς και θα ήθελα να ευχαριστήσω τους γονείς μου για την υποστήριξη που μου έδειξαν όλα αυτά τα χρόνια.

# Περιεχόμενα

<b>1</b>	<b>Εισαγωγή</b> .....	<b>1</b>
1.1	Κίνητρο .....	2
1.2	Σκοπός και Στόχοι .....	3
1.3	Δομή της Μεταπτυχιακή Διατριβής .....	4
<b>2</b>	<b>Τα Κατανεμημένα Κοινωνικά Δίκτυα</b> .....	<b>5</b>
2.1	Ορισμός των Κοινωνικών Δικτύων .....	6
2.2	Βασικές Υπηρεσίες των Κοινωνικών Δικτύων .....	6
2.2.1	Προσθήκη και Επεξεργασία Μηνυμάτων .....	7
2.2.2	Αναζήτηση και Κάλεσμα Φίλων .....	7
2.2.3	Δημιουργία και Επεξεργασία Προφίλ Χρήστη .....	8
2.2.4	Σύνδεση στο Κοινωνικό Δίκτυο από οπουδήποτε .....	8
2.3	Προβλήματα των Κοινωνικών Δικτύων .....	9
2.4	Ιδιότητες Κατανεμημένων Κοινωνικών Δικτύων .....	9
2.5	Αρχιτεκτονικές Συστημάτων Ομότιμων Οντοτήτων .....	10
2.5.1	Η Αρχιτεκτονική των P2P Δικτύων .....	11
2.5.2	Η Αρχιτεκτονική των DHTs – Distributed Hash Tables .....	12
2.6	Τοπολογίες Κατανεμημένων Συστημάτων .....	14
2.6.1	Δομημένη Τοπολογία .....	14
2.6.2	Μη Δομημένη Τοπολογία .....	15
<b>3</b>	<b>Πρότυπες P2P Web Εφαρμογές Κοινωνικών Δικτύων</b> .....	<b>16</b>
3.1	Το Κατανεμημένο Κοινωνικό Δίκτυο Diaspora .....	17
3.2	Το Κατανεμημένο Κοινωνικό Δίκτυο PeerSon .....	21
3.3	Η Κατανεμημένη Υποδομή του Κοινωνικού Δίκτυο PrPl - Private Public .....	25
3.4	Το Κατανεμημένο Κοινωνικό Δίκτυο LifeSocial.KOM .....	30
3.5	Η Κατανεμημένη Πλατφόρμα Κοινωνικής Δικτύωσης MyNet .....	36
3.6	Το Κατανεμημένο Κοινωνικό Δίκτυο Peerscape .....	40
3.7	Διαφορές μεταξύ των P2P Εφαρμογών Κοινωνικών Δικτύων .....	42
<b>4</b>	<b>Σχεδίαση και Ανάπτυξη Κατανεμημένου Κοινωνικού Δικτύου</b> .....	<b>44</b>
4.1	Τεχνολογίες και Πρότυπα .....	45

4.1.1	Το πρωτόκολλο OpenDHT .....	45
4.1.2	Το πρωτόκολλο Chord .....	46
4.1.3	Ο διακομιστής Jabber/XMPP .....	47
4.1.4	Η βιβλιοθήκη cURL .....	50
4.2	Ανάλυση Απαιτήσεων Συστήματος .....	51
4.2.1	Απαιτήσεις Χρήστη .....	51
4.2.2	Λειτουργικές Απαιτήσεις .....	53
4.2.3	Μη Λειτουργικές Απαιτήσεις .....	53
4.3	Αρχιτεκτονική Συστήματος .....	56
4.3.1	Η Αρχιτεκτονική Backend του Συστήματος .....	57
4.3.2	Η Αρχιτεκτονική Frontend του Συστήματος .....	59
<b>5</b>	<b>Λεπτομέρειες Υλοποίησης</b> .....	<b>62</b>
5.1	Η Υπηρεσία Διαχείρισης και Καταχώρησης Πληροφοριών .....	62
5.2	Το Ιδιωτικό Κοινωνικό Δίκτυο του Χρήστη .....	65
5.2.1	Το Πρωτόκολλο OAuth .....	72
5.2.2	Η Υπηρεσία Διασύνδεσης των Ιδιωτικών Κοινωνικών Δικτύων .....	72
5.2.3	Η Διεπαφή Χρήστη των Υπηρεσιών του Ιδιωτικού Κοινωνικού Δικτύου .....	74
<b>6</b>	<b>Συμπεράσματα και Μελλοντική Έρευνα</b> .....	<b>74</b>
6.1	Συμπεράσματα .....	75
6.2	Μελλοντική Έρευνα .....	76
	<b>Βιβλιογραφία</b> .....	<b>77</b>
	<b>Ακρωνύμια και Συντομογραφίες</b> .....	<b>80</b>
<b>A</b>	<b>Παράρτημα A</b> .....	<b>A-1</b>
A.1	Ενδεικτικός Κώδικας Συστήματος .....	A-1

# Κεφάλαιο 1

## Εισαγωγή

Σήμερα τα Online Social Networks - OSN έχουν αναπτυχθεί με βάση το πρότυπο Web 2.0 [01, 02]. Ο όρος Web 2.0 ή Ιστός 2.0 χρησιμοποιείται για να περιγράψει τη νέα γενιά του Παγκόσμιου Ιστού, η οποία βασίζεται στην συνεχώς αυξανόμενη δυνατότητα των χρηστών του διαδικτύου να συνεργάζονται και να μοιράζονται πληροφορίες με σύγχρονο και ασύγχρονο τρόπο [01, 02]. Αυτή η νέα γενιά του Παγκόσμιου Ιστού είναι μια δυναμική διαδικτυακή πλατφόρμα στην οποία μπορούν να αλληλεπιδρούν χρήστες χωρίς εξειδικευμένες γνώσεις σε θέματα υπολογιστών και δικτύων [01, 02]. Σύμφωνα με αυτό το πρότυπο, η δυνατότητα επικοινωνίας μεταξύ των χρηστών με τη βοήθεια μιας διαδικτυακής υπηρεσίας, χρησιμοποιείται ολοένα και περισσότερο από τους ανθρώπους. Αυτό έχει οδηγήσει στη δημιουργία πλατφόρμων Online Κοινωνικών Δικτύων όπως, το Facebook [12], Twitter [13], το LinkedIn [14] κ.α. Εκατομμύρια χρήστες έχουν δημιουργήσει το προσωπικό τους προφίλ σε αυτές τις διαδικτυακές πλατφόρμες, αναρτώντας σε αυτές ένα μεγάλο αριθμό προσωπικών δεδομένων όπως φωτογραφίες, βίντεο και κείμενα, Όμως όλα αυτά τα δίκτυα βασίζονται στην ύπαρξη κεντρικών διαδικτυακών εξυπηρετητών. Έτσι, τα δεδομένα που αναρτούν οι χρήστες σε αυτές τις πλατφόρμες μπορεί πολύ εύκολα να παραβιαστούν ή να πωληθούν σε άλλες εταιρείες ως αποτέλεσμα κανείς από τους χρήστες, δε θα γνωρίζει που βρίσκονται τα δεδομένα τους και με ποιόν τρόπο έχουν χρησιμοποιηθεί ή θα χρησιμοποιηθούν στο απώτερο μέλλον.



Οπότε μια λύση για τον έλεγχο των δεδομένων των χρηστών από τους ίδιους τους χρήστες σε πλατφόρμες κοινωνικής δικτύωσης είναι η δημιουργία ενός καταναμημένου κοινωνικού δικτύου χρησιμοποιώντας την υποδομή και την τεχνολογία ενός δικτύου ομότιμων οντοτήτων peer-to-peer, χωρίς την αλλοίωση των δυνατοτήτων που προσφέρει ένα OSN. Μέσω αυτού του τύπου κοινωνικού δικτύου ο χρήστης θα έχει τον πλήρη έλεγχο στα δεδομένα του και θα ορίζει αυτός τα δικαιώματα πρόσβασης σε τρίτους.

## 1.1 Κίνητρο

Λόγο της αυξανόμενης χρήσης των Online Κοινωνικών Δικτύων από τους απλούς χρήστες σε καθημερινή βάση, αναρτώντας και κοινοποιώντας προσωπικά τους δεδομένα με αλόγιστο τρόπο, χωρίς να λαμβάνουν υπόψη τους το απόρρητο των προσωπικών τους δεδομένων, καθώς και ο τεράστιος όγκος διαφημίσεων και εισερχόμενων μηνυμάτων spams που γεμίζουν τα εισερχόμενα του ηλεκτρονικού τους ταχυδρομείου καθημερινά, αποτέλεσε ένα από τα βασικά κίνητρα για την διεξαγωγή της συγκεκριμένης μεταπτυχιακής διατριβής. Επίσης, ένα άλλο κίνητρο ήταν, πως τα πολυμεσικά δεδομένα των χρηστών μπορούν να προστατευτούν και να ελέγχονται από τους ίδιους τους χρήστες που τα έχουν αναρτήσει, χωρίς να αποτελούν αντικείμενο έρευνας από διάφορες υπηρεσίες και εταιρίες αποφέροντας συνέπειες στους ίδιους τους χρήστες. Όπως για παράδειγμα, οι επιχειρήσεις ανθρώπινου δυναμικού έχουν κατατάσει τα κοινωνικά δίκτυα ως μια καλή πηγή για να συνθέτουν κατά μεγάλο ποσοστό την προσωπικότητα ή προφίλ του χρήστη, εν προκειμένου του εργαζόμενου. Οι πλατφόρμες των Online Κοινωνικών Δικτύων μπορούν να χρησιμοποιήσουν και πρόσθετες «εξωτερικές» εφαρμογές, όπως για παράδειγμα στο Facebook μια τέτοια εφαρμογή είναι το Beacon. Μέσω της εφαρμογής Beacon στο Facebook παρέχεται η δυνατότητα παρακολούθησης της καταναλωτικής συμπεριφοράς ενός χρήστη, καθώς και διάφορες άλλες «συμπεριφορές» των χρηστών του. Επιπρόσθετα, αξίζει να σημειώσουμε ότι σε εξέλιξη βρίσκεται μια συζήτηση σχετικά με το εάν τα δεδομένα του χρήστη που έχει αναρτήσει σε ένα Online Κοινωνικό Δίκτυο παραμένουν ιδιοκτησία του χρήστη ή ανήκουν πλέον στο Online Κοινωνικό Δίκτυο.

## 1.2 Σκοπός και Στόχοι

Σκοπός αυτής της μεταπτυχιακής διατριβής είναι να μελετήσουμε και να συγκρίνουμε τις εναλλακτικές αρχιτεκτονικές, πρωτόκολλα επικοινωνίας και οντολογίες για την υλοποίηση καταναμημένων κοινωνικών δικτύων, τόσο μεταξύ τους όσο και σε σχέση με τις κεντροποιημένες αρχιτεκτονικές με απώτερο στόχο την σχεδίαση και ανάπτυξη ενός υποτυπώδους πρότυπου καταναμημένου κοινωνικού δικτύου. Συγκεκριμένα κάναμε μια προσπάθεια να σχεδιάσουμε και υλοποιήσουμε μια διαδικτυακή εφαρμογή κοινωνικού δικτύου που θα φιλοξενείται στον προσωπικό εξυπηρετητή του κάθε χρήστη και όχι σε έναν κεντρικό εξυπηρετητή, χρησιμοποιώντας κατάλληλες τοπολογίες και πρωτόκολλα για την ανταλλαγή δεδομένων, που έχουν προταθεί μέχρι σήμερα.

Επίσης προσπαθήσαμε να απαντήσουμε στα παρακάτω ερωτήματα ερευνητικού ενδιαφέροντος:

- Πως μπορεί να διασφαλιστεί η μη κλοπή από τρίτους και τα πνευματικά δικαιώματα του περιεχομένου (φωτογραφίες, video, κλπ) των χρηστών σε ένα κοινωνικό δίκτυο (Legal aspects, ownerships) στο βαθμό που μας επιτρέπει η σημερινή τεχνολογία;
- Μπορεί να χρησιμοποιηθεί η αρχιτεκτονική καταναμημένων συστημάτων σε ένα κοινωνικό δίκτυο χωρίς να περιοριστούν οι δυνατότητες και έννοιες του;
- Υπάρχει κάποιος περιορισμός στην ανταλλαγή δεδομένων μεταξύ των χρηστών σε ένα καταναμημένο κοινωνικό δίκτυο;

## 1.3 Δομή της Μεταπτυχιακής Διατριβής

Στο Κεφάλαιο 1 παρουσιάζονται τα κίνητρα, ο σκοπός και οι στόχοι της μεταπτυχιακής διατριβής.

Στο Κεφάλαιο 2 παρουσιάζεται μια σχετική έρευνα για τα κοινωνικά δίκτυα, τις υπηρεσίες που προσφέρουν καθώς και τα προβλήματα που έχουν προκύψει με την διασφάλιση των δεδομένων του χρήστη. Επίσης γίνεται αναφορά για τις ιδιότητες των καταναμημένων κοινωνικών δικτύων, καθώς και για τα βασικά χαρακτηριστικά των αρχιτεκτονικών και τοπολογιών των Συστημάτων Ομότιμων Οντοτήτων – P2P.

Στο Κεφάλαιο 3 παρουσιάζονται μερικές από τις πρότυπες P2P Web Εφαρμογές Καταναμημένων Κοινωνικών Δικτύων.

Στο Κεφάλαιο 4 παρουσιάζεται η αρχιτεκτονική σχεδίασης και υλοποίηση του καταναμημένου κοινωνικού δικτύου μας.

Στο Κεφάλαιο 5 παρουσιάζονται λεπτομέρειες της υλοποίησης του συστήματος και αναφέρονται τα λογισμικά/τεχνολογίες που χρησιμοποιήθηκαν. Επίσης γίνεται μια αναφορά στις υπηρεσίες του συστήματος.

Στο Κεφάλαιο 6 παρουσιάζονται τα συμπεράσματα που εξάγαμε από την σχεδίαση και χρήση της πρότυπης αρχιτεκτονικής του συστήματος, καθώς και η μελλοντική εργασία που απαιτητέ για την διεύρυνση των υπηρεσιών αυτών.

Στο Παράρτημα Α παρουσιάζονται στιγμιότυπα οθονών κατά την χρήση του συστήματος.

# Κεφάλαιο 2

## Τα Κατανεμημένα Κοινωνικά Δίκτυα

Αρχικά, σε αυτό το κεφάλαιο, παρουσιάζουμε έναν ορισμό του κοινωνικού δικτύου και στη συνέχεια αναλύουμε το θεωρητικό υπόβαθρο που απαιτείται για την κατανόηση των υπηρεσιών που προσφέρουν τα κοινωνικά δίκτυα.

Επίσης, σε αυτό το κεφάλαιο παρουσιάζουμε τα ζητήματα, που προκύπτουν στα Online Κοινωνικά Δίκτυα, με τα προσωπικά δεδομένα των χρηστών. Κάνουμε μια σύντομη ανασκόπηση στις ιδιότητες των κατανεμημένων κοινωνικών δικτύων, παρουσιάζοντας παράλληλα τις αρχιτεκτονικές των συστημάτων ομότιμων οντοτήτων P2P και των DHTs - Κατανεμημένων Πινάκων Κατακερματισμού.

Τέλος, σε αυτό το κεφάλαιο, παρουσιάζουμε μερικά από τα βασικά χαρακτηριστικά των δομημένων και μη δομημένων τοπολογιών συστημάτων που υφίστανται για τα κατανεμημένα κοινωνικά δίκτυα.

## 2.1 Ορισμός των Κοινωνικών Δικτύων

Ένα κοινωνικό δίκτυο ορίζεται ως μια δομή που περιλαμβάνει κόμβους, οι οποίοι συνδέονται με έναν ή περισσότερους άλλους κόμβους με διάφορες διασυνδέσεις. Σύμφωνα λοιπόν με τον ορισμό των Boyd & Ellison το 2008, τα Online Κοινωνικά Δίκτυα ορίζονται ως web-based υπηρεσίες που επιτρέπουν στους χρήστες τους:

1. Να δημιουργήσουν ένα δημόσιο ή ημι-δημόσιο προφίλ μέσα σε ένα οριοθετημένο σύστημα.
2. Να επικοινωνήσουν με μια λίστα από άλλους χρήστες με τους οποίους μοιράζονται μια μορφή διασύνδεσης.
3. Να προσπελάζουν και να διανείμουν την δικιά τους λίστα διασύνδεσης χρηστών με άλλους χρήστες, καθώς και να προσπελάζουν τις λίστες διασύνδεσης άλλων χρηστών του ίδιου κοινωνικού δικτύου.

Αυτό που κάνει τα Online Κοινωνικά Δίκτυα να ξεχωρίζουν από τις υπόλοιπες διαδικτυακές εφαρμογές είναι, οι εξελιγμένες τεχνολογικά υπηρεσίες που επιτρέπουν στους χρήστες να διαμοιράζονται ψηφιακά αρχεία όπως κείμενο, εικόνες και πολυμεσικά αρχεία, καθώς και οι εξελιγμένες διαδικτυακές υποδομές για την επικοινωνία και την κοινωνικοποίηση των χρηστών τους.

## 2.2 Βασικές Υπηρεσίες των Κοινωνικών Δικτύων

Τα Online Κοινωνικά Δίκτυα (Σχ. 2.1), όπως το Facebook [12] και το Twitter [13], λόγω της καθημερινής αύξησης του αριθμού των νέων χρηστών τους, πέρα από ένα απλό κάλεσμα μεταξύ των χρηστών, έχουν αναπτύξει και ενσωματώσει αρκετές νέες υπηρεσίες [15]. Ένα από τα χαρακτηριστικά γνωρίσματα που παρέχει το Facebook και το Twitter είναι το micro-blogging, το οποίο αφορά μία λίστα μικρών καταχωρήσεων κειμένου, μέσω της οποίας οι χρήστες μπορούν να γράφουν μικρά κείμενα με περιορισμένο αριθμό χαρακτήρων. Ένα άλλο χαρακτηριστικό του Facebook είναι ο «Τοίχος» μηνυμάτων, ο οποίος είναι μοναδικός για κάθε χρήστη. Ουσιαστικά ο «Τοίχος» του Facebook είναι ένα μέρος για τους φίλους να δημοσιεύουν σημειώσεις στα κοινοποιημένα μεταξύ τους προφίλ. Επίσης, ο κάθε χρήστης ενός κοινωνικού δικτύου όπως το

Facebook και Twitter μπορεί να φορτώσει αρχεία δεδομένων και αρχεία πολυμεσικού περιεχομένου. Το mini-feed είναι μια άλλη υπηρεσία των προαναφερόμενων κοινωνικών δικτύων που παρακολουθεί και ενημερώνει τους υπόλοιπους φίλους για την κατάσταση του προφίλ του χρήστη. Επιπρόσθετα ενημερώνει άλλες επιπρόσθετες εφαρμογές που χρησιμοποιεί στο προφίλ του ο χρήστης.



Σχήμα 2.1: Online Κοινωνικά Δίκτυα[18]

### 2.2.1 Προσθήκη και Επεξεργασία Μηνυμάτων

Τα περισσότερα από τα Online Κοινωνικά Δίκτυα παρέχουν στους χρήστες την υπηρεσία αποστολής μηνυμάτων στους φίλους τους, προσθέτοντας στον «Τοίχο» του προφίλ τους ένα ασύγχρονο μήνυμα. Έτσι λοιπόν, όταν ο χρήστης είναι συνδεδεμένος στο κοινωνικό δίκτυο μπορεί να δει το μήνυμα που εστάλει στον προσωπικό του «Τοίχο» άμεσα. Σε περίπτωση όμως, που ο χρήστης δεν είναι συνδεδεμένος στο κοινωνικό δίκτυο τότε, το μήνυμα θα το διαβάσει όταν θα συνδεθεί την επόμενη φορά. Η υπηρεσία αυτή μπορεί να λειτουργήσει σωστά μόνο σε κεντροποιημένες υπηρεσίες κοινωνικής δικτύωσης όπως το Facebook, Twitter κ.α.

### 2.2.2 Αναζήτηση και Κάλесμα Φίλων

Μια από τις βασικές υπηρεσίες που προσφέρουν τα περισσότερα από τα Online Κοινωνικά Δίκτυα είναι η αναζήτηση φίλων (search friends) και κάλεσμα φίλων (invite friends). Η διαδικασία αυτή επιτυγχάνεται όταν ένας χρήστης τοποθετεί στο προκαθορισμένο πλαίσιο αναζήτησης ως λέξη κλειδί το όνομα του φίλου του ή την διεύθυνση ηλεκτρονικού ταχυδρομείου του και στην συνέχεια εκτελέσει την υπηρεσία αναζήτησης του κοινωνικού

δικτύου. Μετά την εκτέλεση της υπηρεσίας αναζήτησης και εφόσον το σύστημα θα έχει επιστρέψει αποτελέσματα, δηλαδή θα έχει εντοπίσει κάποιους χρήστες, τότε ο αρχικός χρήστης, που εκτέλεσε την υπηρεσία αναζήτησης, μπορεί να επιλέξει και να καλέσει νέους χρήστες του κοινωνικού δικτύου για να γίνουν «φίλοι» επιλέγοντας τον σύνδεσμο «Invite» από τα αποτελέσματα αναζήτησης. Εδώ αξίζει να αναφέρουμε ότι, μόνο όταν χρήστης που του απεστάλει το μήνυμα «φιλίας» το αποδεχτεί, τότε και μόνο τότε, οι δυο χρήστες μπορούν να θεωρούνται ως «φίλοι» στο κοινωνικό δίκτυο και να ανταλλάζουν δεδομένα μεταξύ τους.

### **2.2.3 Δημιουργία και Επεξεργασία Προφίλ Χρήστη**

Για να συνδεθεί ένας χρήστης στα Online Κοινωνικά Δίκτυα θα πρέπει αρχικά να εγγραφεί σε αυτό, δημιουργώντας έτσι το αρχικό του προφίλ. Εφόσον θα έχει αποκτήσει τα στοιχεία πρόσβασης θα μπορεί συνδεθεί στο δίκτυο και να επεξεργαστεί περαιτέρω το προφίλ του. Όπως για παράδειγμα αναρτώντας φωτογραφία του, ή προσθέτοντας προσωπικά δεδομένα κ.α. Όταν ο χρήστης αποσυνδεθεί από το κοινωνικό δίκτυο, τότε το προφίλ του θα είναι ακόμη διαθέσιμο προς αναζήτηση από τους άλλους χρήστες του ίδιου κοινωνικού δίκτυο. Πολλά από τα OSNs όπως το Facebook, MySpace κ.α. παρέχουν την δυνατότητα στον χρήστη, εάν το επιθυμεί να απενεργοποιήσει την επιλογή αναζήτηση του προφίλ του από άλλους χρήστες του κοινωνικού δικτύου. Αυτό όμως δεν σημαίνει πως και τα δεδομένα που έχει αναρτήσει ο χρήστης στον εξυπηρετητή της εταιρίας, που φιλοξένει το Online Κοινωνικό Δίκτυο είναι ασφαλές και δεν μπορούν να παραβιαστούν.

### **2.2.4 Σύνδεση στο Κοινωνικό Δίκτυο από οπουδήποτε**

Τα περισσότερα Online Κοινωνικά Δίκτυα φιλοξενούνται σε διαδικτυακούς εξυπηρετητές (web servers) διάφορων εταιριών, όπου είναι online στο διαδίκτυο συνεχώς. Παρέχοντας την δυνατότητα στους χρήστες του κοινωνικού δικτύου να συνδεθούν από οποιοδήποτε σημείο του κόσμου σε αυτό, αρκεί να έχουν πρόσβαση στο διαδίκτυο με κάποιον υπολογιστή ή smartphone χρησιμοποιώντας μια από τις δημοφιλείς εφαρμογές φυλλομετρητών.

Σε ένα Καταναμημένο Κοινωνικό Δίκτυο P2P, οι παραπάνω κλασικές υπηρεσίες που προσφέρονται σχεδόν από όλα τα κεντροποιημένα κοινωνικά δίκτυα, μπορεί να μην υποστηρίζονται σε τέτοιο υψηλό βαθμό που προσφέρονται στα Online Κοινωνικά Δίκτυα. Αυτό οφείλετε στο ότι, σε ένα καταναμημένο κοινωνικό δίκτυο ο κάθε χρήστης θα έχει τον δικό του

εξυπηρετητή στον οποίο θα φιλοξένη το προσωπικό του κοινωνικό δίκτυο. Αυτό σημαίνει ότι, όταν ο χρήστης θα είναι συνδεδεμένος σε αυτό το δίκτυο, τότε θα έχουμε μεγαλύτερη επιτυχία στις παραπάνω υπηρεσίες, διαφορετικά θα πρέπει να μεσολαβήσουν και άλλες τεχνολογίες για την επίτευξη της σωστής λειτουργίας τους.

## 2.3 Προβλήματα των Κοινωνικών Δικτύων

Οι υπηρεσίες κοινωνικής δικτύωσης που στοχεύουν στη δημιουργία on-line κοινοτήτων από ανθρώπους με κοινά ενδιαφέροντα και δραστηριότητες έχουν γίνει ιδιαίτερα δημοφιλείς στις μέρες μας. Οι υπηρεσίες αυτές λειτουργούν κυρίως στο διαδίκτυο και προσφέρουν πολλαπλούς τρόπους επικοινωνίας και διάδρασης στους εγγεγραμμένους χρήστες τους, όπου συνήθως προϋποθέτουν τη δημιουργία προσωπικών προφίλ των χρηστών.

Οι χρήστες των υπηρεσιών αυτών μπορούν να δημοσιοποιούν και να μοιράζονται προσωπικές πληροφορίες με άλλες ομάδες χρηστών χωρίς κάποιο περιορισμό. Τέτοιες πληροφορίες είναι για παράδειγμα θέματα σχετικά με τα χόμπι τους, την εργασία τους, τις προτιμήσεις τους, τα αγαπημένα τους πρόσωπα, κ.α. μέσα από το προσωπικό τους προφίλ, αλλά και υπό μορφή μηνυμάτων, φωτογραφιών, βίντεο, κ.α.

Αναμφίβολα οι υπηρεσίες κοινωνικής δικτύωσης αποτελούν μία νέα μορφή επικοινωνίας, ιδιαίτερα ανάμεσα στους νέους αλλά όχι μόνο. Ταυτόχρονα όμως, οι υπηρεσίες αυτές προσδίδουν και μια καινούργια διάσταση στην έννοια του “προσωπικού χώρου”, δημιουργώντας σοβαρές ανησυχίες για παραβίαση της ιδιωτικότητας των χρηστών τους, των οποίων τα προσωπικά δεδομένα δημοσιοποιούνται στο διαδίκτυο με πρωτοφανή τρόπο και ποσότητα. Επίσης, ακόμη και αν κάποιοι χρήστες επιλέξουν να μην δημοσιοποιήσουν τα προσωπικά τους δεδομένα, μπορεί κάποιοι φίλοι τους να τα δημοσιοποιήσουν, όπως για παράδειγμα φωτογραφίες. Η παραβίαση του προσωπικού απορρήτου γίνεται και όταν οι ίδιοι οι χρήστες δεν σέβονται την ιδιωτικότητα των άλλων δημοσιεύοντας προσωπικά δεδομένα τρίτων χωρίς την συγκατάθεση τους σύμφωνα και με το άρθρο [15] της βιβλιογραφίας.

Για την αποφυγή των παραπάνω προβλημάτων, την λύση έρχονται να δώσουν τα καταναμημένα κοινωνικά δίκτυα, όπου η αποθήκευση των δεδομένων γίνεται τοπικά στον εξυπηρετητή του κάθε χρήστη. Έτσι τα δεδομένα αυτά μπορούν να προσπελαστούν από τρίτους



μόνο όταν ο χρήστης τους, δηλαδή ο χρήστης που έχει την κυριότητα των δεδομένων, το εγκρίνει.

## 2.4 Ιδιότητες Κατανεμημένων Κοινωνικών Δικτύων

Αναμφίβολα οι ιδιότητες των κατανεμημένων κοινωνικών δικτύων απαντούν τα ερωτήματα που θέσαμε στο Κεφάλαιο 1. Συγκεκριμένα, προσφέρουν ασφάλεια στα προσωπικά δεδομένα του χρήστη. Ο χρήστης μπορεί να διαγράψει τα αρχεία που θα έχει αναρτήσει στο προφίλ του χωρίς να μένουν κάποια αντίγραφα στον εξυπηρετητή. Επίσης, ο χρήστης μπορεί να ορίσει δικαιώματα πρόσβασης στο προφίλ του, επιλέγοντας έτσι αυτός ποιός άλλος χρήστης της κοινότητας θα έχει πρόσβαση στο προφίλ του. Μια άλλη σημαντική ιδιότητα των κατανεμημένων κοινωνικών δικτύων είναι πως το προφίλ του χρήστη παραμένει ενεργό προς αναζήτηση και προσβάσιμο στους φίλους του, όσο ο χρήστης είναι συνδεδεμένος στο δίκτυο. Με τον τρόπο αυτό επιτυγχάνεται μεγαλύτερη ασφάλεια στην αλόγιστη χρήση των προσωπικών δεδομένων μεταξύ φίλων της ίδιας κοινότητας. Επιπρόσθετα, εφόσον δυο φίλοι είναι online τότε μπορούν να μιλήσουν και απευθείας μεταξύ τους με απλά μηνύματα κειμένου. Ένα μειονέκτημα που παρουσιάζεται στα κατανεμημένα κοινωνικά δίκτυα είναι η αποστολή ενός ασύγχρονου μηνύματος μεταξύ φίλων. Τι θα συμβεί στο μήνυμα όταν ο παραλήπτης του μηνύματος δεν είναι online; Υπάρχουν αρκετές μελέτες που προσπαθούν να επιλύσουν το συγκεκριμένο πρόβλημα, αλλά ακόμη δεν έχουμε μια ώριμη λύση για την διευθέτησή του.

Αν και έχουν προταθεί αρκετές beta υλοποιήσεις κατανεμημένων κοινωνικών δικτύων, οι έρευνες βρίσκονται σε εξέλιξη για την υλοποίηση ενός πρότυπου κατανεμημένου κοινωνικού δικτύου, που να προσφέρει στον ίδιο βαθμό και με ασφάλεια όλες τις υπηρεσίες που προσφέρουν σήμερα τα Online Κοινωνικά Δίκτυα.

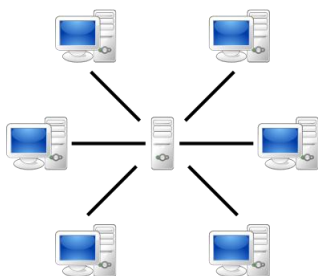
## 2.5 Αρχιτεκτονικές Συστημάτων Ομότιμων Οντοτήτων

Τα τελευταία χρόνια έχει παρατηρηθεί ένα αυξανόμενο ενδιαφέρον στα συστήματα ομότιμων οντοτήτων P2P. Η αρχιτεκτονική P2P υπαγορεύει ένα πλήρως κατανεμημένο συνεργατικό σχεδιασμό δικτύου, όπου οι συμμετέχοντες κόμβοι σχηματίζουν ένα σύστημα χωρίς επιτήρηση. Τα δίκτυα P2P συνήθως λειτουργούν επί ενός εικονικού δικτύου (overlay network), όπου οι

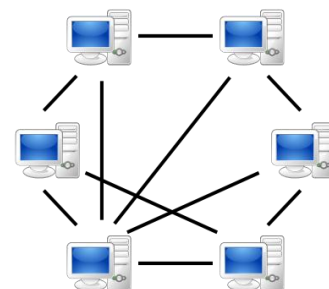
συνδέσεις μεταξύ κόμβων αντιστοιχούν σε μία ή περισσότερες συνδέσεις του υπάρχοντος φυσικού δικτύου (συνήθως το Internet). Μια ενδιαφέρουσα κατηγορία P2P overlay αποτελούν τα αδόμητα (unstructured) δίκτυα, στα οποία οι κόμβοι συνδέονται σε τυχαίους υπάρχοντες άλλους κόμβους του δικτύου και για την ανεύρεση ενός αντικειμένου απαιτείται η προώθηση μιας ερώτησης σε ένα ευρύτερο αριθμό κόμβων.

### 2.5.1 Η Αρχιτεκτονική των P2P Δικτύων

Τα P2P συστήματα [03] μπορούν να διαχωριστούν σε συστήματα που ακολουθούν την αρχιτεκτονική client-server (Σχ. 2.2) και σε συστήματα με αρχιτεκτονική client – to – client (Σχ. 2.3). Η αρχιτεκτονική P2P μπορεί να είναι είτε πλήρως καταναμημένη ή να χρησιμοποιεί κεντρικούς εξυπηρετητές για συντονισμό του φορτίου [03 - 04]. Η αρχιτεκτονική client-to-client ονομάζεται υβριδική.



**Σχήμα 2.2:** Αρχιτεκτονική client-server [03]



**Σχήμα 2.3:** Αρχιτεκτονική client – to – client [03]

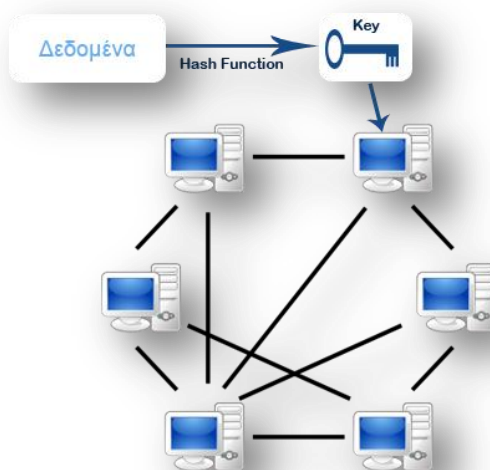
Τα καταναμημένα μοντέλα έχουν τεράστια πλεονεκτήματα κατά την ανάπτυξη εφαρμογών στο διαδίκτυο όπου απαιτούν επεκτασιμότητα και απόδοση παράλληλα με τις απαιτήσεις για χαμηλότερο δυνατό κόστος. Αυτό επιτυγχάνεται αφού οι χρήστες διαθέτουν τους υπολογιστικούς τους πόρους και πόρους για αποθήκευση και δρουν παράλληλα ως χρήστες και εξυπηρετητές με συντονισμό μεταξύ τους [04, 12]. Οι υλοποιήσεις στα P2P συστήματα στις περισσότερες περιπτώσεις βασίζονται στην τυπολογική οργάνωση των χρηστών και χρήση πρωτοκόλλων για την δρομολόγηση κλειδιών σε χρήστες [04, 12].

Μια πιο ξεκάθαρη έννοια για τα συστήματα P2P έχει αναπτύξει ο Dave Winner της User Land Software [06] παρουσιάζοντας τα ακόλουθα χαρακτηριστικά:

1. Η διεπαφή χρήστη δεν εκτελείται μέσω κάποιου φυλλομετρητή ιστοσελίδων.
2. Ο υπολογιστής του χρήστη ενεργεί και σαν πελάτης και σαν εξυπηρετητής.
3. Το συνολικό σύστημα είναι εύκολο στη χρήση και ολοκληρωμένο.
4. Το σύστημα περιλαμβάνει εργαλεία που προσφέρουν στους χρήστες την δυνατότητα διαχείρισης περιεχομένου ή την δυνατότητα προσθήκης νέων λειτουργιών.
5. Το σύστημα παρέχει την δυνατότητα διασύνδεσης με άλλους χρήστες.
6. Το σύστημα παρέχει την δυνατότητα προσθήκης μιας νέας υπηρεσία με αποτελεσματικότερο και καινοτομικό τρόπο.
7. Το σύστημα υποστηρίζει πρωτόκολλα διαδικτύου, όπως το SOAP, XML-RPC.

### 2.5.2 Η Αρχιτεκτονική των DHTs – Distributed Hash Tables

Για την ανάπτυξη της αρχιτεκτονικής client-to-client ο πιο αποδεκτός τρόπος είναι η χρήση των Κατανεμημένων Πινάκων Κατακερματισμού (DHTs – Distributed Hash Tables) (Σχ. 2.4), στους οποίους τα δεδομένα μετατρέπονται με συνάρτηση κατακερματισμού σε κλειδί που παραπέμπει σε κόμβο, όπου αποθηκεύει τα δεδομένα [04, 07, 23, 24].



**Σχήμα 2.4:** Τρόπος επεξεργασίας δεδομένων στους DHTs [03]

Οι σημαντικότερες ιδιότητες των DHTs δικτύων [04, 07, 25] είναι οι παρακάτω:

- Αποκεντροποίηση, όπου των σύνολο των κόμβων ενός δικτύου συνυπάρχουν και διαχειρίζονται το σύστημα ισότιμα, χωρίς να υπάρχει κάποιο κεντρικό σημείο διαχείρισης.
- Κλιμάκωση, όπου το σύστημα μπορεί να λειτουργήσει αποδοτικά ακόμα και με χιλιάδες ή εκατομμύρια συνδεδεμένους κόμβους.
- Αντοχή σε σφάλματα, όπου το σύστημα είναι αξιόπιστο, εντός προκαθορισμένων ορίων, ακόμα και όταν υπάρχουν συνεχόμενες συνδέσεις, αποσυνδέσεις και αποτυχιές κόμβων.
- Αξιοπιστία στην αναζήτηση, όπου επιτυγχάνεται εγγυημένη εύρεση δεδομένων.
- Αποδεδειγμένος μέγιστος χρόνος αναζήτησης (lookup), ο οποίος συνήθως είναι  $O(\log N)$ , όπου  $N$  είναι ο αριθμός των κόμβων στο overlay δίκτυο.
- Αυτόματη εξισορρόπηση φορτίου (load balancing).
- Αυτόνομη αναδιοργάνωση (self-organised).
- Δε χρειάζεται κάποιος εξειδικευμένος εξοπλισμός ώστε ένας υπολογιστής να συμμετάσχει σε ένα DHT overlay δίκτυο. Το μόνο που χρειάζεται ένας υπολογιστής είναι το επιπλέον λογισμικό.

Μερικά από τα μειονεκτήματα των DHTs [04, 07, 23, 24] είναι:

- Τα hops στο overlay δίκτυο συνήθως αντιστοιχούν σε περισσότερα του ενός hops στο υποκείμενο φυσικό δίκτυο. Ως αποτέλεσμα, αν μια επικοινωνία κόμβων στο overlay δίκτυο χρειάζεται λίγα hops, στο υποκείμενο δίκτυο (underlay) χρειάζονται σχεδόν πάντα πολύ περισσότερα. Όταν ένας κόμβος επικοινωνεί με έναν άλλον κόμβο του overlay δικτύου, σχεδόν πάντα υπάρχει μεγαλύτερη λαθάνουσα καθυστέρηση (latency) σε σχέση με την ίδια επικοινωνία των κόμβων στο φυσικό επίπεδο. Αυτό μετριέται με το stretch. Όταν υπάρχει ένα stretch, τότε υπάρχει ένα latency ακριβώς ίσο με αυτό του φυσικού δικτύου. Όλα τα overlay δίκτυα έχουν stretch μεγαλύτερο του ένα.

- Κάθε κόμβος πρέπει να κρατάει μια ποσότητα πληροφορίας για την κατάσταση του overlay DHT δικτύου. Οι κόμβοι σε ένα overlay DHT δίκτυο έχουν μεγαλύτερο επίβαρο (overhead), σε σχέση με το φυσικό δίκτυο.
- Όλοι οι κόμβοι στο overlay DHT δίκτυο θεωρούνται ισότιμοι. Για αυτό το λόγο μερικές φορές υπάρχει περίπτωση να δημιουργήσει συμφόρηση σε κόμβους οι οποίοι δεν έχουν αρκετή υπολογιστική ισχύ ή είναι συνδεδεμένοι με χαμηλό εύρος ζώνης στο δίκτυο.

Μια βασική τεχνική που χρησιμοποιείται για να επιτευχθούν αυτές οι χρήσιμες ιδιότητες των DHT overlay δικτύων, είναι ότι κάθε κόμβος χρειάζεται να συνεργαστεί μόνο με ένα μικρό υποσύνολο των κόμβων που συμμετέχουν στο DHT δίκτυο. Συνήθως αυτό το υποσύνολο είναι  $\Theta(\log N)$  από τους  $N$  σε σύνολο κόμβους του DHT δικτύου. Με αυτόν τον τρόπο μειώνετε και ο χρόνος εργασίας για κάθε αλλαγή που συμβαίνει στο DHT δίκτυο.

## 2.6 Τοπολογίες Κατανεμημένων Συστημάτων

Υπάρχουν δυο βασικές τοπολογίες σχεδίασης για τα P2P συστήματα, η δομημένη τοπολογία, όπως το πρωτόκολλο Chord και η μη δομημένη τοπολογία όπως είναι το Gnutella. Η ανάλυση αυτών των τοπολογιών θα μας βοηθήσουν για την επιλογή της κατάλληλης αρχιτεκτονικής για την σχεδίαση του δικού μας κατανεμημένου κοινωνικού δικτύου.

### 2.6.1 Δομημένη Τοπολογία

Εδώ υπάρχει η έννοια της δομής με βάση την οποία δημιουργείται η τοπολογία και η συνεκτικότητα του δικτύου. Η έννοια της δομής διασφαλίζεται με τη βοήθεια προηγμένων κατανεμημένων δομών δεικτοδότησης, όπως για παράδειγμα των Κατανεμημένων Πινάκων Κατακερματισμού – DHTs [05, 07, 22].

Σε ένα δίκτυο DHT κάθε κόμβος έχει ένα μοναδικό αναγνωριστικό node ID, το οποίο έχει επιλεγεί τυχαία από ένα πολύ μεγάλο χώρο διευθύνσεων. Κάθε αντικείμενο, όπως για παράδειγμα ένα αρχείο κειμένου ή ένα πολυμεσικό αρχείο, αντιστοιχίζεται με ένα κλειδί, το οποίο αποτελεί ένα μοναδικό αναγνωριστικό για το αντικείμενο. Το αναγνωριστικό αυτό έχει επιλεγεί από τον ίδιο χώρο διευθύνσεων που χρησιμοποιείται για τα αναγνωριστικά των κόμβων. Η βασική ιδέα είναι η αποθήκευση αντικειμένων στους κόμβους των οποίων το

αναγνωριστικό είναι ίδιο ή αριθμητικά πολύ κοντά, στο κλειδί του αντικειμένου. Έτσι, κατά την αναζήτηση, αρκεί να επισκεφθούμε τον κόμβο με αναγνωριστικό ίσο με αυτό του αντικειμένου. Αυτός ο τρόπος κατεύθυνσης ενός ερωτήματος μπορεί να καταστήσει τις δομημένες τοπολογίες αποδοτικότερες. Η χρήση ενός τέτοιου δομημένου συστήματος εισάγει νέα αποτελέσματα τα οποία θα πρέπει να τα λάβουμε υπόψη.

## 2.6.2 Μη Δομημένη Τοπολογία

Στην μη δομημένη τοπολογία [04, 07] οι κόμβοι οργανώνονται σε τυχαίους γράφους ή με επίπεδες τοπολογίες και με όλους τους κόμβους να είναι ίσοι μεταξύ τους ή με ιεραρχικές τοπολογίες όπου ένα μικρό σύνολο κόμβων χαρακτηρίζεται από αυξημένες αρμοδιότητες και δυνατότητες.

Έτσι λοιπόν σε τέτοιου τύπου δίκτυα δεν υπάρχει στενή σχέση μεταξύ της τοπολογίας και των κόμβων όπου αποθηκεύεται η πληροφορία. Η αναζήτηση και ο εντοπισμός των αντικειμένων επιτυγχάνεται κυρίως με τεχνικές flooding και random walks.. Έτσι, οι αιτήσεις ανάκτησης αντικειμένων πλημμυρίζουν το δίκτυο, με κάθε κόμβο να εξυπηρετεί την αίτηση με βάση την πληροφορία που έχει αποθηκευμένη και στη συνέχεια να την προωθεί σε επόμενους κόμβους. Η συγκεκριμένη τεχνική δεν θεωρείται ιδιαίτερα αποδοτική, αφού οι αιτήσεις αναζήτησης πληροφορίας, η οποία μπορεί να είναι ελάχιστα κατανεμημένη στο δίκτυο, θα πρέπει να ταξιδεύουν σε όλο το δίκτυο μέχρι να καταφέρουν να εντοπίσουν την πληροφορία αυτή. Ένα παράδειγμα P2P συστήματος με μη δομημένη τοπολογία είναι το Gnutella.

# **Κεφάλαιο 3**

## **Πρότυπες P2P Web Εφαρμογές Κοινωνικών Δικτύων**

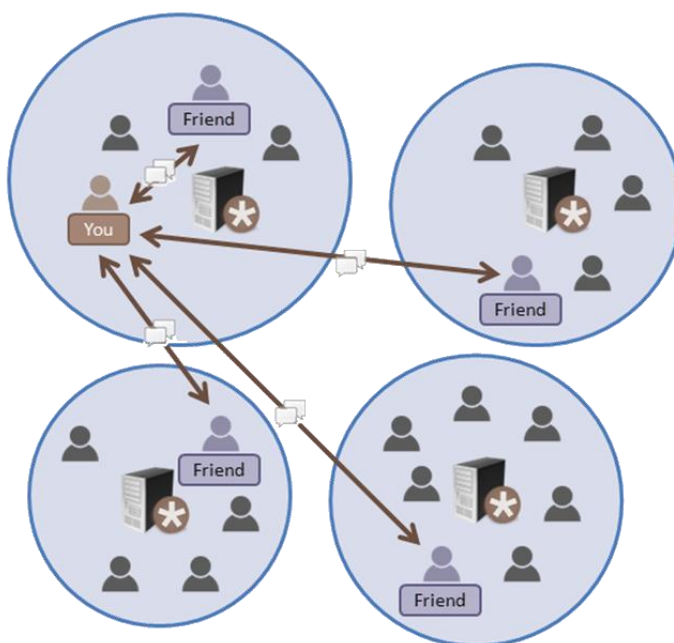
Στο τρέχων κεφάλαιο γίνεται μια ανασκόπηση γύρω από τις web εφαρμογές κατανεμημένων κοινωνικών δικτύων που έχουν προταθεί μέχρι σήμερα. Εδώ εστιάζομαι τόσο στην τεχνολογίες που χρησιμοποιούν αυτές οι εφαρμογές, καθώς και αν πληρούν όλες τις δυνατότητες που προσφέρει σήμερα ένα online κοινωνικό δίκτυο OSN.

### 3.1 Το Κατανεμημένο Κοινωνικό Δίκτυο Diaspora

Το κοινωνικό δίκτυο Diaspora είναι ελεύθερο λογισμικό κατανεμημένης κοινωνική δικτύωσης που δημιουργήθηκε από τους Dan Grippi, Maxwell Salzberg, Raphael Sofaer και Ilya Zhitomirskiy [08].

Το κοινωνικό δίκτυο Diaspora [08, 11] έχει αποκεντρωμένη δομή και αποτελείται από δεκάδες υπολογιστές - διαδικτυακοί εξυπηρετητές που ονομάζονται pods (Σχ. 3.1). Μέσω αυτών των εξυπηρετητών παρέχονται διάφορες διευθύνσεις στο διαδίκτυο όπου ο κάθε χρήστης μπορεί να προβεί σε εγγραφή και στην συνέχεια να συνδεθεί στο κατανεμημένο κοινωνικό δίκτυο Diaspora. Μέχρι σήμερα έχουν προταθεί δυο τρόποι για να εντοπίσουμε τα pods του Diaspora για να συνδεθούμε:

- Ο πρώτος τρόπος είναι με την αποστολή πρόσκλησης μέσω email, όπου μέσω της πρόσκλησης ο χρήστης θα παραπέμπετε σε συγκεκριμένο URL του pod.
- Ο δεύτερος τρόπος είναι να κάνουμε μια αναζήτηση σε έναν κατάλογο των pods όπως στην διεύθυνση [www.poduprti.me](http://www.poduprti.me). Μέσω αυτό του τρόπου, μετά από μια σύντομη αξιολόγηση των pods, μπορούμε να επιλέξουμε ένα από τα pods που θεωρούμε πως είναι ασφαλής και να δημιουργήσουμε έναν λογαριασμό σε αυτό το pod.



Σχήμα 3.1: Τρόπος επικοινωνίας μεταξύ των pods στο Diaspora



Κάθε pod ανάλογα με τη διαχείριση του μπορεί να είναι τόσο αξιόπιστο ή γρήγορο όσο ένα άλλο. Συνήθως αν δεν υπάρχουν προβλήματα μπορούμε να δούμε τα μέλη άλλων pods και να συνδεθούμε μαζί τους, ανταλλάζοντας μηνύματα και πολυμεσικό περιεχόμενο.

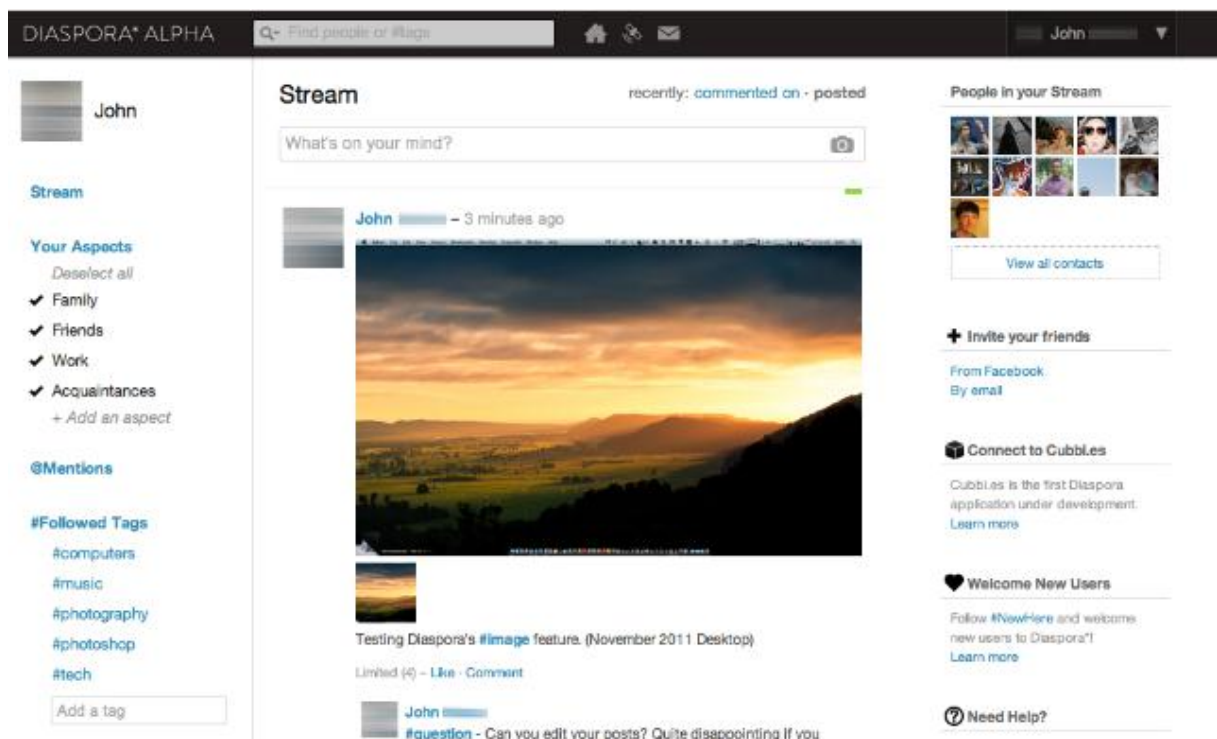
Το κατανεμημένο κοινωνικό δίκτυο Diaspora πέρα από τις κλασικές υπηρεσίες που προσφέρουν τα κοινωνικά δίκτυα υποστηρίζει επιπλέον τις ακόλουθες υπηρεσίες:

- **Τα Aspects.** Aspects καλούμε την οργάνωση των επαφών μας στο Diaspora. Ένα aspect, είναι μια ομάδα επαφών. Μέσω των aspects μπορούμε να οργανώσουμε καλύτερα τις επαφές μας σε ομάδες με βάση τα κριτήρια που θα ορίσουμε εμείς. Επίσης, εδώ αξίζει να σημειώσουμε ότι οι επαφές (εν προκειμένου οι φίλοι) που έχουν οργανωθεί σε ομάδες δεν γνωρίζουν την ομάδα που μπορούν να ανήκουν σε έναν χρήστη.
- **Θεματικές Ετικέτες (Hash Tags).** Όταν δημιουργούμε ένα μήνυμα μπορούμε να προσθέσουμε λέξεις που αρχίζουν με το σύμβολο #(hash). Μέσω αυτών των ειδικών λέξεων ο εξυπηρετητής ταξινομεί το μήνυμά μας με τέτοιο τρόπο έτσι ώστε να μπορεί να το εντοπίσει κάποιος άλλος φίλος με τα αντίστοιχα ενδιαφέροντα.
- **Ειδική κοινοποίηση.** Στο Diaspora μπορούμε να κοινοποιήσουμε μηνύματα ή φωτογραφίες σε μια ομάδα των επαφών μας (σε μια ομάδα φίλων) ή σε όλους τους φίλους μας ανεξαρτήτως αν ανήκουν σε κάποια ομάδα.
- **Δημοσίευση (Post).** Στο Diaspora η δημοσίευση ενός κειμένου από τον χρήστη μπορεί να αναδημοσιευτεί, κοινοποιηθεί, αναφερθεί και χαρακτηριστεί από άλλο χρήστη, καθώς και από τον δημιουργό του αρχικού δημοσιεύματος. Επιπρόσθετα, ο δημιουργός μιας δημοσίευσης μπορεί και να την αποκρύψει από τους φίλους του. Ένας άλλο ειδικός χαρακτηρισμός των δημοσιεύσεων είναι το φιλτράρισμα τους μέσω της ετικέτας «*Not Safe For Work*» ορίζοντας την ετικέτα #nsfw σε μια δημοσίευση, ενημερώνοντας έτσι τους άλλους φίλους για την ακαταλληλότητα της δημοσίευσης.
- **Υπηρεσίες διασύνδεσης.** Το Diaspora παρέχει επίσης υπηρεσίες διασύνδεσης με άλλα κοινωνικά δίκτυα, ανακτώντας πληροφορίες για το προφίλ του χρήστη.
- **Προστασίας Προσωπικών Δεδομένων από τον σχεδιασμό (Privacy by design).** Ένα άλλο σημαντικό στοιχείο του κοινωνικού δικτύου Diaspora που αξίζει να

αναφέρουμε είναι ότι δεν εκθέτει πληροφορίες του χρήστη σε διαφημιστικές εταιρίες, ή σε ιστοσελίδες που επισκέπτεται ο χρήστης.

- **Κυριότητα των δεδομένων.** Ο κάθε χρήστης που δημιουργεί το δικό του προφίλ στο Diaspora διατηρήσει την πλήρη κυριότητα όλων των πληροφοριών που αναρτά στο προφίλ του συμπεριλαμβανομένων καταλόγων φίλων, μηνυμάτων, φωτογραφιών και λεπτομερειών του προφίλ. Όταν ο χρήστης διαγράφει τον λογαριασμό του τότε όλα τα δεδομένα του προφίλ του διαγράφονται.
- **Μελλοντικές Υπηρεσίες.** Μια από τις βασικότερες μελλοντικές υπηρεσίες που προσβλέπουν να υποστηρίξει το Diaspora είναι η μεταφορά του προφίλ του χρήστη μεταξύ των pods.

Παρακάτω παρουσιάζεται και μια συνολική διεπαφή του frontend του Diaspora (Εικ. 3.1).



**Εικόνα 3.1:** Η διεπαφή χρήστη του κατανεμημένου κοινωνικού δικτύου Diaspora [09]

Ο πηγαίος κώδικας του κοινωνικού δικτύου Diaspora έχει αναπτυχτεί στο Web Framework Ruby on Rails, το οποίο βασίζεται στην αντικειμενοστραφής γλώσσα προγραμματισμού διαδικτύου Ruby.

Επιπρόσθετες τεχνολογίες που χρησιμοποιήθηκαν για την ανάπτυξη του Diaspora είναι:

**Η Haml**, η οποία είναι μια γλώσσα σήμανσης που χρησιμοποιείται για απλή περιγραφή του κώδικα HTML οποιουδήποτε εγγράφου διαδικτύου χωρίς τη χρήση του inline code. Στο Diaspora η HAML χρησιμοποιήθηκε για την δημιουργία πρότυπων (templates). Ωστόσο, Haml έχει την δική της κωδικοποίηση. Το πρότυπο της ιστοσελίδας που έχει αναπτυχτεί με την HAML παράγει δυναμικά την HTML σελίδα που προκύπτει από την εκτέλεση του κώδικα HAML.

**To Sass Framework**, μέσω του οποίου έχουν αναπτυχτεί τα Διαδοχικά Φύλλα Στυλ (CSS - Cascading Style Sheets) στο Diaspora. Το Sass επιτυγχάνει την συμπίεση των αρχείων CSS και JavaScript μιας ιστοσελίδας που έχει αναπτυχτεί με την γλώσσα προγραμματισμού Ruby. Το CSS είναι μια γλώσσα κωδικοποίησης των στυλ μια ιστοσελίδας. Συγκεκριμένα το CSS ορίζει και μορφοποιεί τη διάταξη (layout) των HTML εγγράφων.

**Τα Backbone.js & Handlebars.js** αρχεία JavaScript, τα οποία χρησιμοποιούνται στο Diaspora για την εκτέλεση ρουτινών του κοινωνικού δικτύου. Σχεδόν όλες οι λειτουργίες του Diaspora σε επίπεδο χρήστη (client-side) δρομολογούνται από το Backbone.js, το οποίο επικοινωνεί με τον server σε επίπεδο web services χρησιμοποιώντας το πρωτόκολλο RESTful και την τεχνολογία JSON. Τα δεδομένα εκτέλεσης των web services και η παράγωγή των πρότυπων HTML διαχειρίζονται από το Handlebars.js.

Κατά την διάρκεια προσθήκης ασύγχρονων μηνυμάτων στον «τοίχο» μεταξύ φίλων η διαδικασία που ακολουθείτε από τεχνολογικής πλευράς είναι η εξής:

1. Ο χρήστης προσθέτει το μήνυμα στον τοίχο του ως aspect.
2. Γίνεται έλεγχος ότι το μήνυμα προήρθε από τον πιστοποιημένο χρήστη.
3. Εφόσον ο έλεγχος επιστρέφει αληθές απάντηση, τότε το μήνυμα αποθηκεύεται στο raw\_visible\_posts πίνακα για αυτόν τον χρήστη.
4. Στην συνέχεια για το μήνυμα αυτό παράγεται μια HTML έκδοση για αποστολή μέσω WebSocket σε άλλους χρήστες.
5. Τέλος, το μήνυμα καταγράφεται σε ένα XML αρχείο, κρυπτογραφημένο και υπογεγραμμένο σε έναν φάκελο με τα παραλαμβανόμενα URLs της μορφής

"[http://pod.location/receive/users/:id\[person\\_id\]](http://pod.location/receive/users/:id[person_id])". Η διαδικασία αυτή εκτελείτε στους χρήστες που θα παραλάβουν το μήνυμα.

Κατά την διάρκεια παραλαβής ενός μηνύματος η διαδικασία που ακολουθείτε είναι η εξής:

1. Ο χρήστης λαμβάνει το μήνυμα και αποκρυπτογραφεί την επικεφαλίδα (header) του μηνύματος.
2. Γίνεται έλεγχος της υπογραφής του μηνύματος για να διαπιστωθεί αν ο αποστολέας του μηνύματος είναι ο ίδιος χρήστης που έχει υπογράψει το μήνυμα. Εφόσον αυτό ισχύει τότε το μήνυμα αναγνωρίζεται ως αντικείμενο και αποθηκεύεται στην βάση δεδομένων του χρήστη.
3. Τέλος, στον παραλήπτη αποθηκεύεται το id του μηνύματος και στη συνέχεια το μήνυμα εμφανίζεται στον «τοίχο» του προφίλ του παραλήπτη. Η ίδια διαδικασία εκτελείται και από την πλευρά του αποστολέα.

Το κατανεμημένο κοινωνικό δίκτυο Diaspora έχει αναπτυχθεί σε μεγάλο βαθμό, αν και ακόμη βρίσκεται σε beta έκδοση. Πάρα πολύ χρήστες το έχουν υποστηρίξει όμως υστερεί ακόμη να απαντήσει σε απαιτήσεις όπως, τι θα συμβεί στο μήνυμα όταν ο εξυπηρετητής του χρήστη θα είναι απενεργοποιημένος και κάποιος φίλος του θα του αποστείλει ένα μήνυμα, αν οι φίλοι του αποσυνδεδεμένου χρήστη θα έχουν πρόσβαση στο πολυμεσικό περιεχόμενο του προφίλ του, κ.α. Πλέον με βάση την τελευταία ανακοίνωση της ομάδας ανάπτυξης του Diaspora, ο κώδικας και γενικότερα η συνολική δομή ανάπτυξης του είναι διαθέσιμα στην κοινότητα του.

## 3.2 Το Κατανεμημένο Κοινωνικό Δίκτυο PeerSon

Το κατανεμημένο κοινωνικό δίκτυο PeerSon δημιουργήθηκε και εξακολουθεί να αναπτύσσεται από μια κοινοπραξία επιστημόνων των πανεπιστημίων, ΚΤΗ Σουηδίας, NTU Σιγκαπούρης και Warsaw Πολωνίας [05]. Το PeerSon προσπαθεί να δώσει λύσεις σε ζητήματα που έχουν προκύψει από την χρήση των online κοινωνικών δικτύων, όπως για την ασφάλεια δεδομένων, την ασφαλή επικοινωνία μεταξύ χρηστών, την ανταλλαγή δεδομένων κ.α. Έως σήμερα έχει δημιουργηθεί ένα πρότυπο(prototype) το οποίο αποτελείται από διάφορα μέρη. Ένα μέρος του PeerSon αποτελεί η τεχνολογία peer-to-peer που υποστηρίζει, προσφέροντας έτσι στους χρήστες με κατανεμημένο τρόπο, τις βασικές υπηρεσίες που προσφέρουν και τα online κοινωνία

δίκτυα. Ένα άλλο μέρος του PeerSon ασχολείται με την κρυπτογράφηση της πληροφορίας που θα ανταλλάσσεται μεταξύ των χρηστών του, δίνοντας έμφαση στην ανταλλαγή δημόσιων και ιδιωτικών κλειδιών κρυπτογράφησης κατά την διάρκεια πιστοποίησης των χρηστών του. Με τον τρόπο αυτό το PeerSon προσφέρει ένα ασφαλές κατανεμημένο κοινωνικό δίκτυο. Βασικός σκοπός του PeerSon είναι οι online χρήστες να μπορούν να ανταλλάζουν άμεσα μεταξύ τους αρχεία, κείμενα και πολυμεσικό περιεχόμενο με ασφάλεια, χωρίς να μπορούν αυτά τα δεδομένα να χρησιμοποιηθούν από τρίτους, μη-πιστοποιημένους χρήστες. Τα αρχεία των χρηστών του θα είναι διαθέσιμα μόνο όταν ο χρήστες θα είναι online, δηλαδή συνδεδεμένοι στο προσωπικό τους κοινωνικό δίκτυο PeerSon.

Μερικές από τις υπηρεσίες που ξεχωρίζουν στο κατανεμημένο κοινωνικό δίκτυο PeerSon είναι:

**Κοινωνικοί Υπερσυνδέσμοι (Social Links).** Μέσω των social links οι χρήστες μπορούν να συνδεθούν μεταξύ τους και να κατηγοριοποιήσουν σε ομάδες τους χρήστες που έχουν συνδεθεί, ως φίλους, ως συνεργάτες, κ.α. Επίσης, εκτός του ότι μέσω των social links το κατανεμημένο δίκτυο PeerSon επεκτείνεται με ασφάλεια μεταξύ φίλων, μπορεί επίσης να χρησιμοποιήσει τα social links για να επανασυνδεθεί με χρήστες που έχουν χάσει την μεταξύ τους σύνδεση λόγω κάποιου τεχνικού προβλήματος. Έτσι μέσω των κοινωνικών υπερσυνδέσμων καταγράφεται και παρουσιάζεται στους χρήστες του δικτύου, ο κοινωνικός του γράφος, όπως και στην πραγματική ζωή, βοηθώντας έτσι τους χρήστες να επιλέξουν/αναζητήσουν φίλους στην ομάδα που τα ενδιαφέροντα τους συμπίπτουν[05].

**Προσωπικός Ψηφιακός Χώρος (Digital Personal Space).** Μέσω του ψηφιακού του χώρου ο κάθε χρήστης του PeerSon μπορεί να αποθηκεύει πληροφορίες για το προφίλ του, να ανεβάζει κείμενα και πολυμεσικό περιεχόμενο, να ανταλλάζει μηνύματα με άλλους χρήστες κ.α. Όλα τα παραπάνω μπορεί να τα κοινοποιεί στους φίλους του ή στις επιλεγμένες ομάδες χρηστών που θα έχει δημιουργήσει στο προφίλ του. Επίσης κάθε συμβάν (event) που θα προκύπτει στο προφίλ του χρήστη, μπορεί να κοινοποιείτε παράλληλα και στους φίλους του. Σημαντικό σημείο εδώ είναι ότι όλες οι παραπάνω κοινοποιήσεις του χρήστη θα εκτελούνται μόνο μεταξύ φίλων και μόνο εκείνοι θα μπορούν να έχουν πρόσβαση στο προφίλ του, καθώς και στο πολυμεσικό περιεχόμενο που θα έχει ανεβάσει στο προφίλ του ο χρήστης. Ως προσωπικός ψηφιακός χώρος του χρήστη μπορεί να είναι, είτε ο προσωπικός του υπολογιστής, είτε κάποιος προσωπικός διακομιστής διαδικτύου[05].

**Μέσα Επικοινωνίας (Means of Communication).** Στο κοινωνικό δίκτυο PeerSon έχουν αναπτυχτεί σε μορφή prototype διαφορές υπηρεσίες για την άμεση και έμμεση επικοινωνία μεταξύ των χρηστών του. Έτσι, ένα από τα μέσα που χρησιμοποιείτε για την ασύγχρονη επικοινωνία είναι, ο προσωπικός ψηφιακός χώρος του χρήστη, τον οποίο αναλύσαμε παραπάνω. Ένα άλλο μέσο επικοινωνίας που χρησιμοποιείτε στο PeerSon είναι η υπηρεσία «κοινωνικοί υπερσύνδεσμοί», μέσω της οποίας παρέχετε η δυνατότητα στους χρήστες να βλέπουν τις συνδέσεις(peers) των άλλων χρηστών του δικτύου και να τους καλούν για να γίνουν φίλοι. Για να επιτευχθεί η σύγχρονη επικοινωνία μεταξύ φίλων στο PeerSon προϋπόθεση είναι, ότι και οι δυο φίλοι θα πρέπει να είναι συνδεδεμένοι online [05].

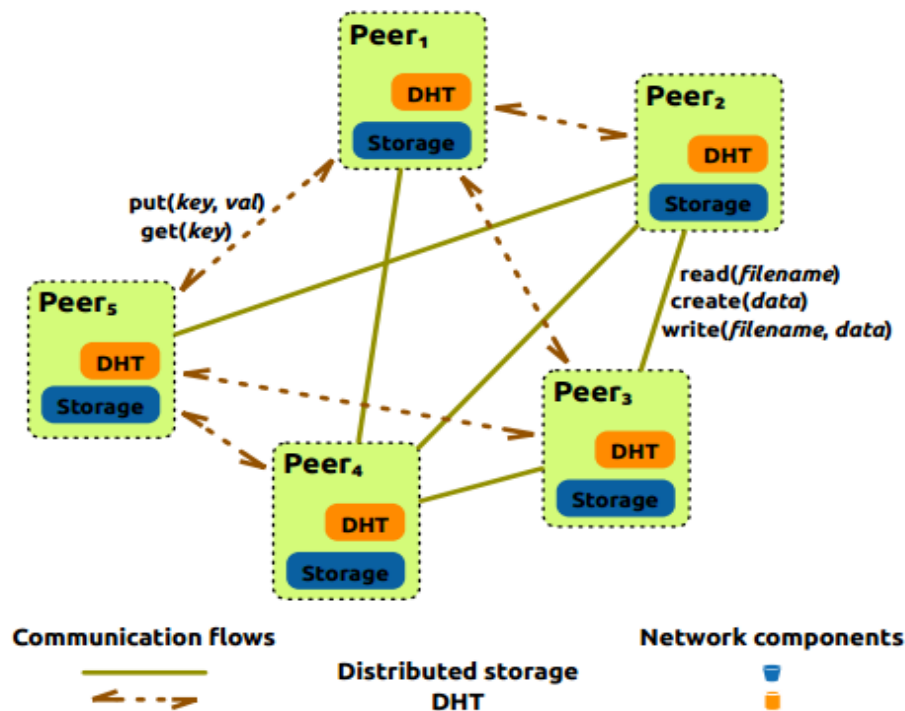
**Η αρχιτεκτονική σχεδίαση του PeerSon.** Η αρχιτεκτονική σχεδίαση του PeerSon αποτελείται από δυο ζώνες (2-tiered architecture)[05, 07]. Η πρώτη ζώνη-tier χρησιμοποιείτε για την υπηρεσία αναζήτησης κόμβων(look-up services), ενώ η δεύτερη ζώνη - tier περιλαμβάνει τις ζεύξεις(peers) και τα στοιχεία των προφίλ των χρηστών του δικτύου. Η υπηρεσία αναζήτηση - look-up service αποθηκεύει μετά-δεδομένα που απαιτούνται για τον εντοπισμό των χρηστών. Τέτοια δεδομένα είναι, η διεύθυνση IP, πληροφορίες σχετικά με τα αρχεία του χρηστών, καθώς και ειδοποιήσεις των χρηστών. Για να συνδεθεί ένα ομότιμο σύστημα με ένα άλλο ομότιμο σύστημα, αρχικά ζητά από την υπηρεσία αναζήτησης να εντοπίσει όλες τις απαραίτητες πληροφορίες για το ενδιαφερόμενο ομότιμο σύστημα. Στην συνέχεια, εφόσον υπάρχουν διαθέσιμες οι απαραίτητες πληροφορίες από την υπηρεσία αναζήτησης, τότε τα δυο ομότιμα συστήματα - υπολογιστές μπορούν να συνδεθούν απευθείας μεταξύ τους. Εφόσον τα δυο ομότιμα συστήματα έχουν συνδεθεί μπορούν στην συνέχεια να ανταλλάξουν μηνύματα και αρχεία μεταξύ τους, όπως παρουσιάζεται και στο (Σχ. 3.2). Μόλις η διαδικασία της ανταλλαγής δεδομένων ολοκληρωθεί τότε η σύνδεση μεταξύ τους τερματίζεται άμεσα.



**Σχήμα 3.2:** Αποστολή μηνύματος από το ομότιμο Β σύστημα στο ομότιμο Α σύστημα [05].

Όπως παρατηρούμε και από το παραπάνω σχήμα το PeerSon χρησιμοποιεί το πρωτόκολλο OpenDHT [23] για την υπηρεσία αναζήτησης. Η ανάλυση του πρωτόκολλου OpenDHT γίνεται παρακάτω στο 4<sup>ο</sup> Κεφάλαιο.

Ένα άλλο σημαντικό σημείο που αξίζει να αναφέρουμε εδώ είναι ότι, το PeerSon, πέρα από το OpenDHT πρωτόκολλο, χρησιμοποιεί και διάφορες άλλες τεχνολογίες για την εξασφάλιση της ασφάλειας στα δεδομένα των χρηστών του. Συγκεκριμένα, για τον κάθε χρήστη του δικτύου παράγει ένα μοναδικό κλειδί, το οποίο το ονομάζει Globally Unique IDs (GUID), μέσω του οποίου πιστοποιείτε ο χρήστης στο δίκτυο. Χρησιμοποιώντας το GUID του κάθε χρήστη ως ένα συμμετρικό κλειδί κρυπτογράφησης το PeerSon κρυπτογραφεί τα δεδομένα που ανταλλάσσονται μεταξύ φίλων, παρέχοντας έτσι αυξημένη ασφάλεια στα δεδομένα των χρηστών του. Η διαδικασία αυτή παρουσιάζεται στο (Σχ. 3.3).



**Σχήμα 3.3:** Επισκόπηση του συστήματος ανταλλαγής δεδομένων του PeerSon [16].

Συμφώνα και με το παραπάνω σχήμα (Σχ. 3.3) παρατηρούμε ότι μέσω του κατακευημένου κοινωνικού δικτύου PeerSon οι χρήστες μπορούν να ανταλλάξουν μεταξύ τους, ασύγχρονα/σύγχρονα μηνύματα κειμένου και αρχεία με ασφαλές τρόπο.

Όλα τα παραπάνω που αναφέραμε για το PeerSon είναι σε επίπεδο σχεδίασης. Σήμερα η σχεδίαση αυτή εξελίσσεται, ενσωματώνοντας συνεχώς νέες τεχνολογίες, ενώ παράλληλα

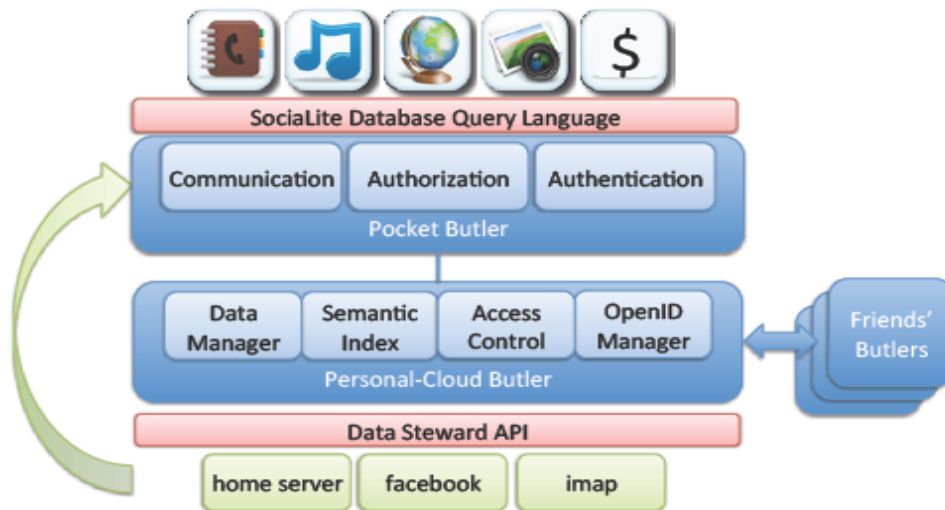
βρίσκεται σε εξέλιξη η ανάπτυξη του πρότυπου συστήματος PeerSon από την ομάδα της κοινοπραξίας επιστημόνων των πανεπιστημίων, ΚΤΗ της Σουηδίας, NTU της Σιγκαπούρης και το πανεπιστήμιο του Warsaw της Πολωνίας.

### **3.3 Η Κατανεμημένη Υποδομή του Κοινωνικού Δικτύου PrPI – Private Public**

Το PrPI – Private Public [26] κατανεμημένο κοινωνικό δίκτυο, είναι μια πρόταση των ερευνητών και καθηγητών Seok-Won Seong, Jiwon Seo, Matthew Nasielski, Debangsu Sengupta, Sudheendra Hangal, Seng Keat Teh, Ruven Chu, Ben Dodson, Monica S. Lam των τμημάτων Επιστήμης Υπολογιστών και Ηλεκτρολόγων Μηχανικών του Πανεπιστημίου του Stanford CA.

Η αρχιτεκτονική του PrPI στηρίζεται σε μια αποκεντρωμένη δομή που επιτρέπει στους χρήστες να συμμετέχουν σε online κοινωνική δικτύωση, χωρίς την απώλεια ή υποκλοπή των δεδομένων τους. Η πρόσωπο-κεντρική αρχιτεκτονική του PrPI προσφέρει στον κάθε χρήστη να χρησιμοποιεί μια υπηρεσία Cloud Butler, η οποία παρέχει ένα ασφαλές εικονικό ψηφιακό χώρο αποθήκευσης για τα προσωπικά στοιχεία και δεδομένα του χρήστη. Επίσης, μέσω της υπηρεσίας αυτής ο κάθε πιστοποιημένος χρήστης του συστήματος μπορεί να κοινοποιήσει δεδομένα του σε άλλους χρήστες με απόλυτη ασφάλεια. Η βασική ιδέα του PrPI είναι, ότι ο κάθε χρήστης έχει τον δικό του χώρο αποθήκευσης, σε δικής του επιλογής διακομιστή. Με τον τρόπο αυτό, ένας διακομιστής μπορεί να είναι ο προσωπικός υπολογιστής του χρήστη, ένας δικτυακός σκληρός δίσκος, ή ακόμη και μια παιχνιδιομηχανή με μεγάλο αποθηκευτικό χώρο που συνδέεται στο διαδίκτυο. Η ενοποίηση αυτών των ψηφιακών αποθηκευτικών χώρων του χρήστη επιτυγχάνεται μέσα από το API (Application Programming Interface) του PrPI δικτύου. Χρησιμοποιώντας την υπηρεσία Personal-Cloud Butler τα δεδομένα του χρήστη κρυπτογραφούνται από κάποιο πιστοποιητικό και ευρετηριάζονται για κοινοποίηση μόνο στους επιλεγμένους φίλους του. Στο παρακάτω σχήμα (Σχ. 3.4) παρουσιάζεται σχεδιαστικά η αρχιτεκτονική του υποσυστήματος δεδομένων του PrPI.





**Σχήμα 3.4:** Επισκόπηση της αρχιτεκτονικής του υποσυστήματος δεδομένων του PrPI [26].

Ένα άλλο σημαντικό σημείο του PrPI είναι ότι, χρησιμοποιεί το αποκεντρωμένο σύστημα διαχείρισης OpenID πρότυπο, έτσι ώστε οι χρήστες που έχουν καθιερωθεί ως personas από αυτό το σύστημα, θα μπορούν να έχουν πρόσβαση στα δεδομένα του χρήστη.

Μερικά από τα χαρακτηριστικά που διακρίναμε στην αρχιτεκτονική δομή, καθώς και στον τρόπο επικοινωνίας των χρηστών μεταξύ τους στο PrPI είναι:

**Οι Personal-Cloud Butlers.** Η ιδέα του Personal-Cloud Butler είναι στην πραγματικότητα μια προσωπική υπηρεσία για κάθε χρήστη του δικτύου, όπου προσφέρει ασφάλεια στα δεδομένα του χρήστη και οργανώνει και κοινοποιεί τα δεδομένα του κάθε χρήστη με τους φίλους αναλόγως των δικαιωμάτων πρόσβασης που θα έχει ορίσει για κάθε έναν από αυτούς [26]. Οι υπηρεσίες που προσφέρει ο Personal-Cloud Butler είναι:

- **Σημασιολογική δεικτοδότηση των προσωπικών δεδομένων.** Παρέχει μια ενοποιημένη μορφή δεικτοδότησης των δεδομένων για την διευκόλυνση της περιήγησης και αναζήτησης των προσωπικών πληροφοριών του κάθε χρήστη. Η παρουσίαση των δεδομένων γίνεται σε μια τυποποιημένη μορφή RDF - Resource Description Framework ακολουθώντας συγκεκριμένα και τυποποιημένα πρότυπα οντολογιών, υποστηρίζοντας έτσι και την διαλειτουργικότητα των δεδομένων με άλλες διαδικτυακές εφαρμογές. Βέβαια όλα τα παραπάνω ισχύουν όταν τα δεδομένα του χρήστη είναι διαθέσιμα και προσβάσιμα μέσω του διαδικτύου. Ένα παράδειγμα RDF - Based database είναι το

*Friend(u) :- (u, a, prpl:Identity)* όπου περιγράφει ότι ο *u* έχει ταυτότητα στην PrPI βάση δεδομένων.

- **Ομόσπονδες σύστημα αποθήκευσης.** Μέσω αυτό του συστήματος ο κάθε χρήστης έχει την δυνατότητα να επιλέξει αυτός τους δικούς του ψηφιακούς χώρους αποθήκευσης των δεδομένων του. Η υπηρεσία του Butler σε κάθε χρήστη παράγει κάποια πιστοποιητικά μέσω των οποίων, ενεργοποιεί τα συστήματα αποθήκευσης των χρηστών για να επικοινωνήσουν μεταξύ τους, επιτυγχάνοντας έτσι και την άμεση ανταλλαγή δεδομένων μεταξύ φίλων.
- **Αποκεντρωμένη διαχείριση ταυτότητας χρήστη.** Το σύστημά επιτρέπει στους χρήστες να χρησιμοποιούν τους λογαριασμούς personas (λογαριασμός πιστοποιημένου χρήστη στο OpenID), μετατρέποντας το έτσι, ως ένα αποκεντρωμένο σύστημα διαχείρισης ταυτότητας. Μέσω αυτής της σχεδίασης οι ερευνητές του PrPI προτείνανε την επέκταση του συστήματος OpenID, έτσι ώστε να επιτυγχάνετε η αναζήτηση ενός καθορισμένου Butler, χρησιμοποιώντας το προσωπικό του OpenID. Με αυτόν τον τρόπο ο φορέας παροχής OpenID γίνεται ο πυρήνας του συστήματος για την εξακρίβωση της γνησιότητας των προσωπικών υπηρεσιών Butlers του PrPI.

Το **OpenID** είναι ένας δωρεάν και εύκολος στην χρήση τρόπος, για να χρησιμοποιήσουμε μια *μοναδική ψηφιακή ταυτότητα στο διαδίκτυο*. Μας επιτρέπει έτσι να συνδεόμαστε σε ιστοσελίδες ξεχνώντας τις πολύπλοκες διαδικασίες εγγραφής και χωρίς να χρειάζεται να θυμάστε ένα ακόμη ψευδώνυμο και κωδικό πρόσβασης. Στην πράξη το OpenID είναι μια διεύθυνση διαδικτύου URL το οποίο μπορεί να έχει διάφορες μορφές ανάλογα με τον πάροχο του OpenID που θα επιλέξουμε.

- **Κοινό client proxy.** Για την υποστήριξη single sign-on για εφαρμογές που τρέχουν στη συσκευή του πελάτη, όπως για παράδειγμα ένα smartphone, μια Pocket Butler υπηρεσία χειρίζεται την ταυτοποίηση και επικοινωνία με τα Personal-Cloud Butlers. Επιπρόσθετα, μέσω των απλών διεπαφών χρήστη παρέχεται η δυνατότητα καθορισμού εξουσιοδότησης στα δεδομένα του χρήστη καθώς και η διαχείριση της προσωρινής αποθήκευσης των δεδομένων του, έτσι ώστε να επιτευχθεί ο διαμερισμός των πόρων μεταξύ των πολλαπλών εφαρμογών.

Για την υλοποίηση των Personal-Cloud Butlers μια ιδέα θα ήταν να φιλοξενηθούν τέτοιου είδους υπηρεσίες σε διάφορες ηλεκτρονικές συσκευές που έχουν πρόσβασης στο διαδίκτυο, όπως είναι, οι παιχνιδιομηχανές, νέου τύπου τηλεοράσεις, προσωπικοί υπολογιστές, smartphone κ.α.. Το κόστος αυτών των ηλεκτρονικών συσκευών είναι διαχειρίσιμο και οι περισσότερες από αυτές τις ηλεκτρονικές συσκευές υπάρχουν σχεδόν σε όλα τα σπίτια.

Όπως παρατηρούμε και στο (Σχ. 3.4), το PrPI για την άντληση μεγάλου όγκου δεδομένων από το κατακευματισμένο δίκτυο υπηρεσιών των Butlers (από τους εικονικούς ψηφιακούς αποθηκευτικούς χώρους των χρηστών του PrPI) χρησιμοποιείται μια γλώσσα επερωτήσεων λογικών βάσεων δεδομένων, η οποία ονομάζεται **SocialLite Language**.

Η **SocialLite** σχεδιάστηκε και υλοποιήθηκε από την ομάδα ερευνητών που σχεδιάζει και αναπτύσσει το κατακευματισμένο κοινωνικό δίκτυο PrPI [26]. Η SocialLite είναι μια επέκταση της Datalog, η οποία είναι μια γλώσσα ερωτήσεων και κανόνων για λογικές βάσεις δεδομένων (deductive databases). Υποστηρίζοντας αναδρομή(recursion) και σύνθεση(composition), η SocialLite είναι μια γλώσσα που μπορεί να «εκφράσει» σε αρκετά ικανοποιητικό επίπεδο ένα γεγονός/ερώτημα. Με τον τρόπο αυτό πολλές κοινωνικές εφαρμογές(social apps) μπορούν εύκολα να γραφτούν με την προσθήκη ενός GUI στο αποτέλεσμα του socialite ερωτήματος. Ένα σημαντικό σημείο της SocialLite γλώσσας είναι ότι αποκρύπτει την πολυπλοκότητα ενός ερωτήματος στους Butlers των φίλων του χρήστη. Έχει είδη υλοποιηθεί ένα αρχικό πρότυπο της SocialLite γλώσσας καθώς και μερικές πρότυπες εφαρμογές στο PrPI, όπου η πρώτη δοκιμασία τους έγινε σε Cloud Hosting υπηρεσία EC2 της εταιρίας Amazon. Στο σενάριο που εκτελεστικό από την ομάδα ανάπτυξης του PrPI είχαν δημιουργήσει 100 Butlers, και έλαβαν απάντηση από το socialite ερώτημα σε μερικά δευτερόλεπτα [26].

Τέλος, μια τελευταία τεχνολογία που εντοπίζουμε στο παραπάνω σχήμα (Σχ. 3.4) είναι το **Data Steward API**. Κάθε συσκευή του χρήστη η οποία ανήκει στο ομόσπονδες σύστημα αποθήκευσης του, τρέχει το λειτουργικό Data Steward API για λογαριασμό του χρήστη. Με τον τρόπο αυτό παρέχει ένα ενιαίο περιβάλλον εργασίας στον Butler και στις PrPI εφαρμογές, αποκρύπτοντας τις λεπτομέρειες σχετικά με το πώς οι πληροφορίες αποθηκεύονται στις συσκευές. Το Data Steward API είναι υπεύθυνο και για την ενημέρωση του Butler σχετικά με τα δεδομένα blobs(binary large objects). Περιοδικά το Data Steward API στέλνει μερικά heartbeats στον Butler ενημερώνοντας τον με τις τελευταίες αλλαγές των blobs, καθώς και με τις τελευταίες αλλαγές των πληροφοριών προσπέλασης τους [26]. Ο Butler, στην πραγματικότητα ενημερώνεται για τις τοποθεσίες των blobs, αντιστοιχίζοντας

την PrPI URI διεύθυνση σε μια διεύθυνση πηγής δεδομένων URI της μορφής “http://” ή “file://”.

Συγκρίνοντας το PrPI με τα Online Κοινωνικά Δίκτυα οι υπηρεσίες (data sources)[26] που προσφέρει είναι:

**Τα εργαλεία διαχείρισης του προσωπικού λογαριασμού του χρήστη.** Ο χρήστης μπορεί να διαχειρίζεται το προσωπικό του ημερολόγιο και τις επαφές του.

**Διαχείριση των αρχείων σε προσωπικό υπολογιστή του χρήστη.** Η υπηρεσία Batler θα πρέπει να εντοπίσει και αποθηκεύσει όλα τα μεταδεδομένα των αρχείων του χρήστη στον προσωπικό του υπολογιστή. Τέτοιου είδους αρχεία είναι, φωτογραφίες, έγγραφα, videos κ.α.

**Διαχείριση των μηνυμάτων και των επισυναπτομένων αρχείων.** Πολλοί χρήστες καταφεύγουν στην ταχυδρομική αποστολή δεδομένων στους εαυτούς τους έτσι ώστε τα δεδομένα να μπορούν να τα προσπελαστούν από οπουδήποτε. Ωστόσο, είναι δύσκολο να εντοπίσεις την σωστή έκδοση ενός αρχείου. Οι meta πληροφορίες σχετικά με τα μηνύματα ηλεκτρονικού ταχυδρομείου, επαφές, και τα συνημμένα, είναι μια σημαντική πηγή στοιχείων για την ενσωμάτωση στο PrPI Federation Stored Systems. Τα μηνύματα ηλεκτρονικού ταχυδρομείου από ηλεκτρονικά καταστήματα όπως το Netflix και Amazon περιέχουν όλο το ιστορικό αγορών του χρήστη κατά τα προηγούμενα έτη και έως σήμερα. Τέτοιου είδους πληροφορίες μπορούν πολύ εύκολα να ευρετηριαστούν μέσω του PrPI.

**Σύνδεση με τα Online κοινωνικά δίκτυα.** Πολλοί χρήστες έχουν ανεβάσει προσωπικά δεδομένα στα online κοινωνικά δίκτυα, όπως το Facebook, Twitter κ.α. Μέσω του Data Steward API τα δεδομένα αυτά μπορεί να τα αναλύσουμε από τα διάφορα online κοινωνικά δίκτυα και στην συνέχεια να τα οργανώσουμε με βάση το πρότυπο του PrPI. Επίσης εδώ μπορούμε να προσθέσουμε απευθείας δεδομένα στο Facebook . Η παραπάνω υπηρεσίες παρουσιάζονται στην (Εικ. 3.2).



**Εικόνα 3.2:** Η διεπαφή χρήστη του PrPI Butler με την εφαρμογή Photo Wall [26].

Αυτό που παρατηρούμε στο PrPI κοινωνικό δίκτυο είναι ότι, ενώ υποστηρίζει μερικώς αυτά που υποστηρίζουν τα Online κοινωνικά δίκτυα, προσεγγίζει το θέμα του κατακευματισμένου κοινωνικού δικτύου από μια άλλη οπτική γωνία. Συγκεκριμένα προσφέρει μια ειδική υποδομή κατακευματισμένης κοινωνικής δικτύωσης πάνω στην οποία μπορεί να δημιουργηθούν πολλές εφαρμογές κοινωνικής δικτύωσης. Επιπρόσθετα, η σχεδίαση του εστιάζει στην μεταφορά μεγάλου όγκου δεδομένων μεταξύ των χρηστών του.

### 3.4 Το Κατακευματισμένο Κοινωνικό Δίκτυο LifeSocial.KOM

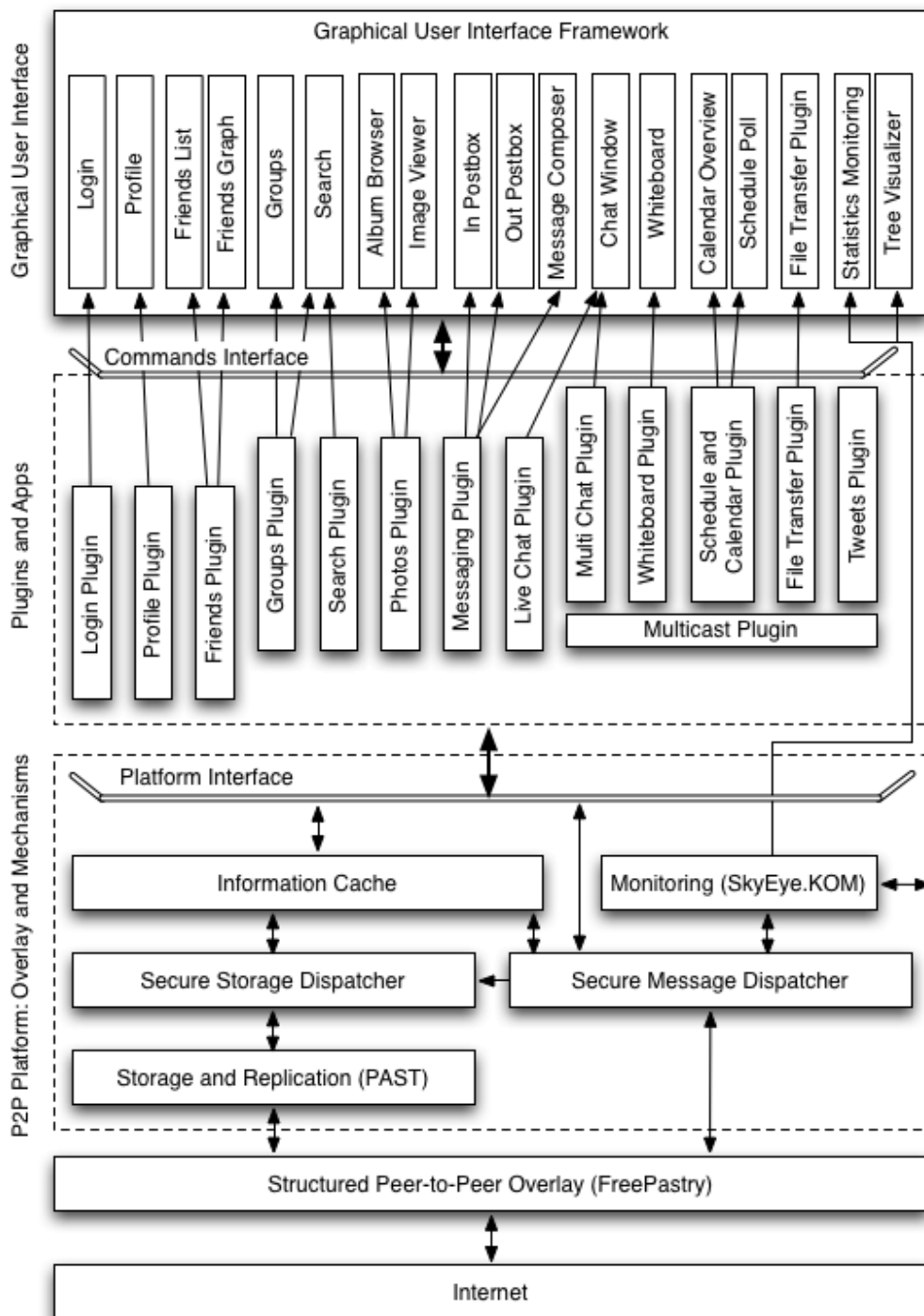
Το LifeSocial [27] αναπτύχθηκε από τον Kalman Graffi και διάφορους φοιτητές στο Εργαστήριο Πολυμέσων Επικοινωνίας (KOM) υπό την επίβλεψη του καθηγητή Ralf Steinmetz στο Τεχνολογικό Πανεπιστήμιο του Darmstadt (Technische Universität Darmstadt) στην Γερμανία. Η ερευνητική ομάδα που ασχολήθηκε σχετικά με τη θεωρία των κατακευματισμένων συστημάτων ήταν υπό την επίβλεψη του καθηγητή Christian Scheideler στο Πανεπιστήμιο του Paderborn στην Γερμανία.

Στην πραγματικότητα το LifeSocial.KOM είναι μια p2p υποδομή για ασφαλείς και αποκεντρωμένη online κοινωνική δικτύωση, το οποίο παρέχει την λειτουργικότητα και τις υπηρεσίες που προσφέρουν τα online κοινωνικά δίκτυα σε ένα πλήρως κατακευματισμένο και

ασφαλή περιβάλλον [27]. Αποτελείται από επιμέρους εφαρμογές (plugins) μέσω των οποίων μπορεί να παρατείνει τις υπηρεσίες και την λειτουργικότητα του, παρέχοντας ασφαλή επικοινωνία και ελεγχόμενη πρόσβαση στα δεδομένα των χρηστών. Επίσης, μια επιπλέον υπηρεσία που υποστηρίζει το LifeSocial.KOM είναι η αξιολόγηση και βελτίωση της ποιότητας των υπηρεσιών του, καλύπτοντας έτσι τις ανάγκες των χρηστών που επικοινωνούν μεταξύ τους, καθώς και των παρόχων internet. Η πλατφόρμα λειτουργεί αποκλειστικά χρησιμοποιώντας τους πόρους των συστημάτων των χρηστών του. Με τον τρόπο αυτό μειώνει το λειτουργικό κόστος για έναν πάροχο. Μέχρι σήμερα έχει σχεδιαστεί και υλοποιηθεί μια δοκιμαστική πλατφόρμα αξιολόγησης των επιμέρους εφαρμογών που εξακολουθούν να υλοποιούνται, με έμφαση στην επισήμανση των δυνατοτήτων της P2P διασύνδεσης στον τομέα των online κοινωνικών δικτύων.

Η αρχιτεκτονική δομή του LifeSocial.KOM παρουσιάζεται στο (Σχ. 3.5). Αυτό που παρατηρούμε στο (Σχ. 3.5) είναι, ότι η αρχιτεκτονική δομή του LifeSocial.KOM είναι χωρισμένη σε 3 βασικά μέρη [27]:

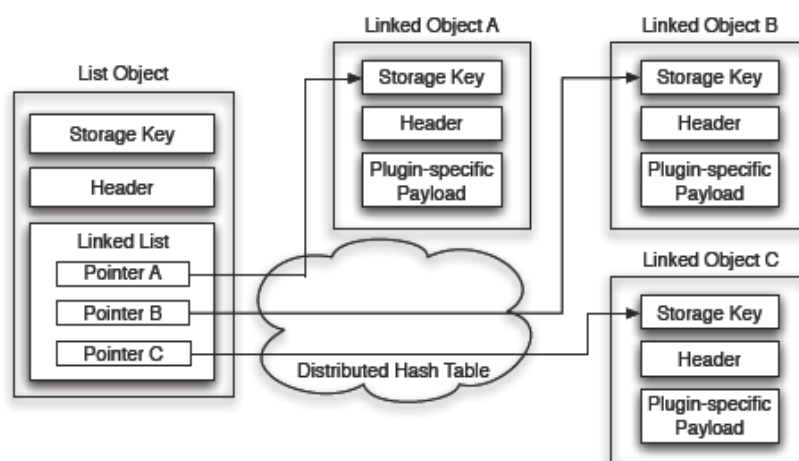
- **P2P Platform: Overlay and Mechanisms**, όπου αναλύονται οι τεχνολογίες και τα πρωτοκόλλα που έχουν χρησιμοποιηθεί για την επίτευξη της p2p επικοινωνίας μεταξύ των συστημάτων των χρηστών.
- **Plugins and Apps**, όπου αναλύονται η εφαρμογές (plugins/apps) που έχουν υλοποιηθεί για την ασφαλή επεξεργασία και ανταλλαγή δεδομένων μεταξύ των χρηστών του LifeSocial.KOM.
- **Graphical User Interface**, όπου παρουσιάζονται οι επιμέρους διεπαφές χρήστη των εφαρμογών, που χρησιμοποιούνται για την φιλική με τον χρήστη παρουσίαση των δεδομένων.



**Σχήμα 3.5:** Επισκόπηση της αρχιτεκτονικής δομής του LifeSocial.KOM [27].

Στο επίπεδο δικτύου, της αρχιτεκτονικής δομής του LifeSocial.KOM, βρίσκετε μια δομημένη P2P υπηρεσία, η οποία παρέχει τη λειτουργικότητα δρομολόγησης μεταξύ ομότιμων χρησιμοποιώντας το ID του κάθε κόμβου. Η διαδικασία αυτή επιτυγχάνεται μέσω της λειτουργικότητας του FreePastry [28], το οποίο είναι μια δωρεάν επέκταση το Pastry [29] και παρέχει ένα αξιόπιστο αντικείμενο αποθήκευσης των δεδομένων που ονομάζεται PAST [30].

Το LifeSocial.KOM χρησιμοποιώντας τις υπηρεσίες του FreePastry και του PAST τα αντικείμενα που δημιουργούνται στο LifeSocial.KOM δίκτυο, τα οποία οργανώνονται σε λίστες, είναι αξιόπιστα στα οποία αποθηκεύονται πληροφορίες για τα δεδομένα του χρήστη, όπως για παράδειγμα ο σύνδεσμος μιας φωτογραφίας, αν ανήκει σε κάποια ομάδα φωτογραφιών (photoalbum) κ.α. Η ανάκτηση αυτών των αντικειμένων από το δίκτυο βασίζεται στην ταυτότητα τους όπου χρόνο αναζήτησης/απόκρισης τους δεν ξεπερνά τα δύο δευτερόλεπτα. Η διαδικασία αυτή παρουσιάζεται στο (Σχ. 3.6).



**Σχήμα 3.6:** Η κατανομημένη διασυνδεδεμένη λίστα αντικειμένων στο LifeSocial.KOM [27]

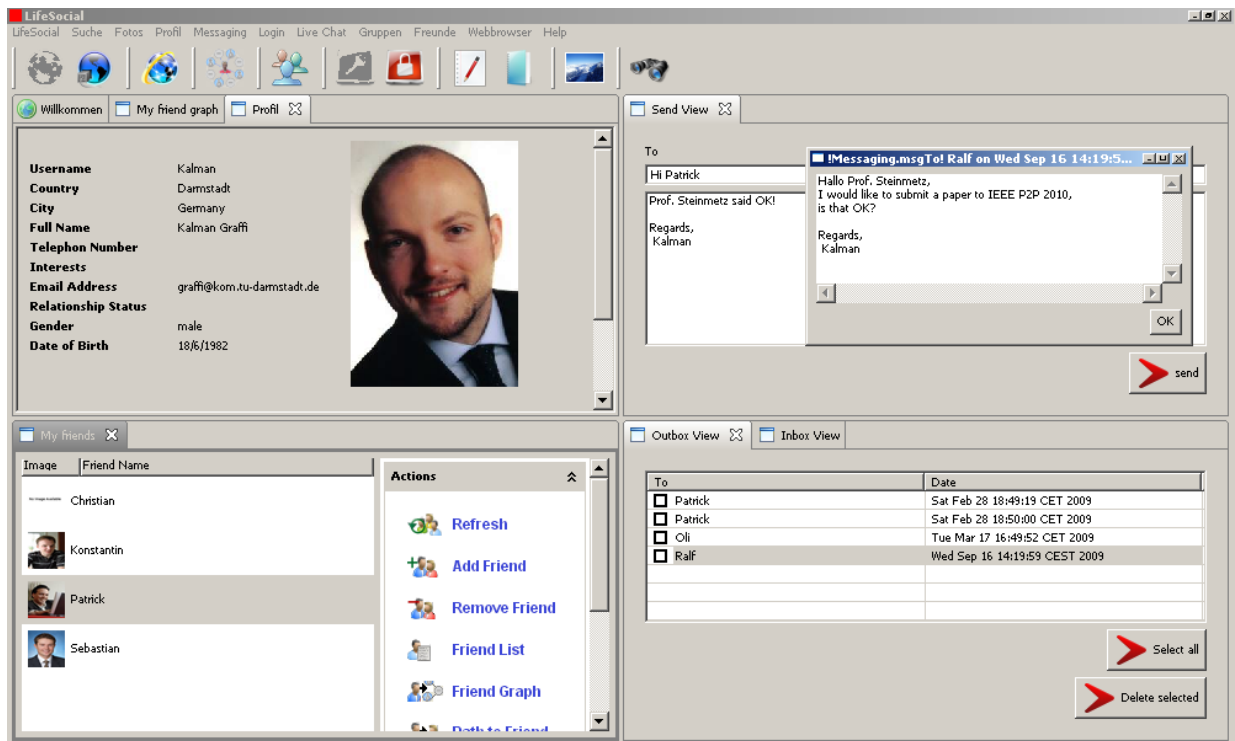
Οι βασικές εφαρμογές (plugins) που έχουν υλοποιηθεί έως σήμερα για το LifeSocial.KOM είναι οι ακόλουθες:

- **Login:** Εγγραφή / Σύνδεση του χρήστη μέσω των κλειδιών κρυπτογράφησης.
- **Profile:** Παρουσιάζεται μια απλή παρουσίαση των στοιχείων του χρήστη
- **Friends:** Είναι μια λίστα που διατηρεί διασυνδεδεμένα τα προφίλ των φίλων.
- **Messaging:** Ασύγχρονα μηνύματα, όπως το email.
- **Photo:** Μια λίστα photo album που διατηρεί διασυνδέσεις (links) με τις φωτογραφίες του χρήστη.

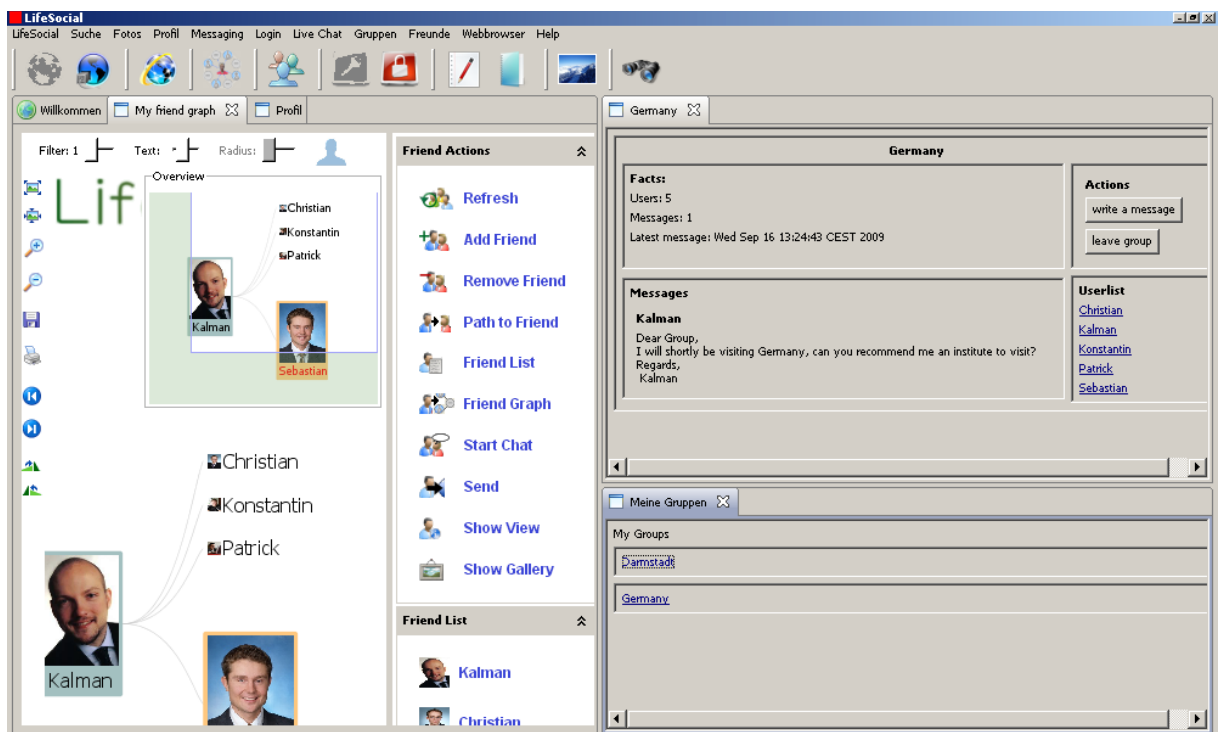


- **Groups:** Μια λίστα από χρήστες που έχουν συνδεθεί σε μια κοινή ομάδα χρηστών ασπάζοντας τα ίδια ενδιαφέροντα.
- **Tweets:** Μια λίστα από την κατάσταση του προφίλ του χρήστη, καθώς και με τους φίλους followers.
- **(Group) Chat:** Συγχρονισμένα μηνύματα μεταξύ χρηστών.
- **File transfer:** Ανταλλαγή αρχείων μεταξύ χρηστών.
- **Games for two with spectators:** Ένα παράδειγμα αυτής της εφαρμογής είναι το παιχνίδι Tic Tac Toe.
- **Whiteboard:** Μέσω της εφαρμογής αυτής επιτυγχάνετε η συνεργατικότητα μεταξύ των φίλων σχεδιάζοντας από κοινού σε έναν ενιαίο πίνακα.
- **Schedule and Calendar:** Διατήρηση ημερολογίου του κάθε χρήστη.
- **Multicast:** Μπορεί ο κάθε χρήστης να κοινοποιήσει ένα αρχείο σε μια ομάδα χρηστών.

Η διεπαφή χρήστη του front end του LifeSocial.KOM παρουσιάζεται στην (Εικ. 3.3) και στην (Εικ. 3.4).



Εικόνα 3.3: Η διεπαφή χρήστη του LifeSocial.KOM του προφίλ, των μηνυμάτων, της λίστας φίλων [27].



Εικόνα 3.4: Η διεπαφή χρήστη του LifeSocial.KOM των ομάδων χρηστών σε μορφή γράφου [27].

Συγκρίνοντας το LifeSocial.KOM με τα online κοινωνικά δίκτυα παρατηρούμε ότι, ενώ υποστηρίζει όλες τις υπηρεσίες που προσφέρουν τα online κοινωνικά δίκτυα, τα δεδομένα των

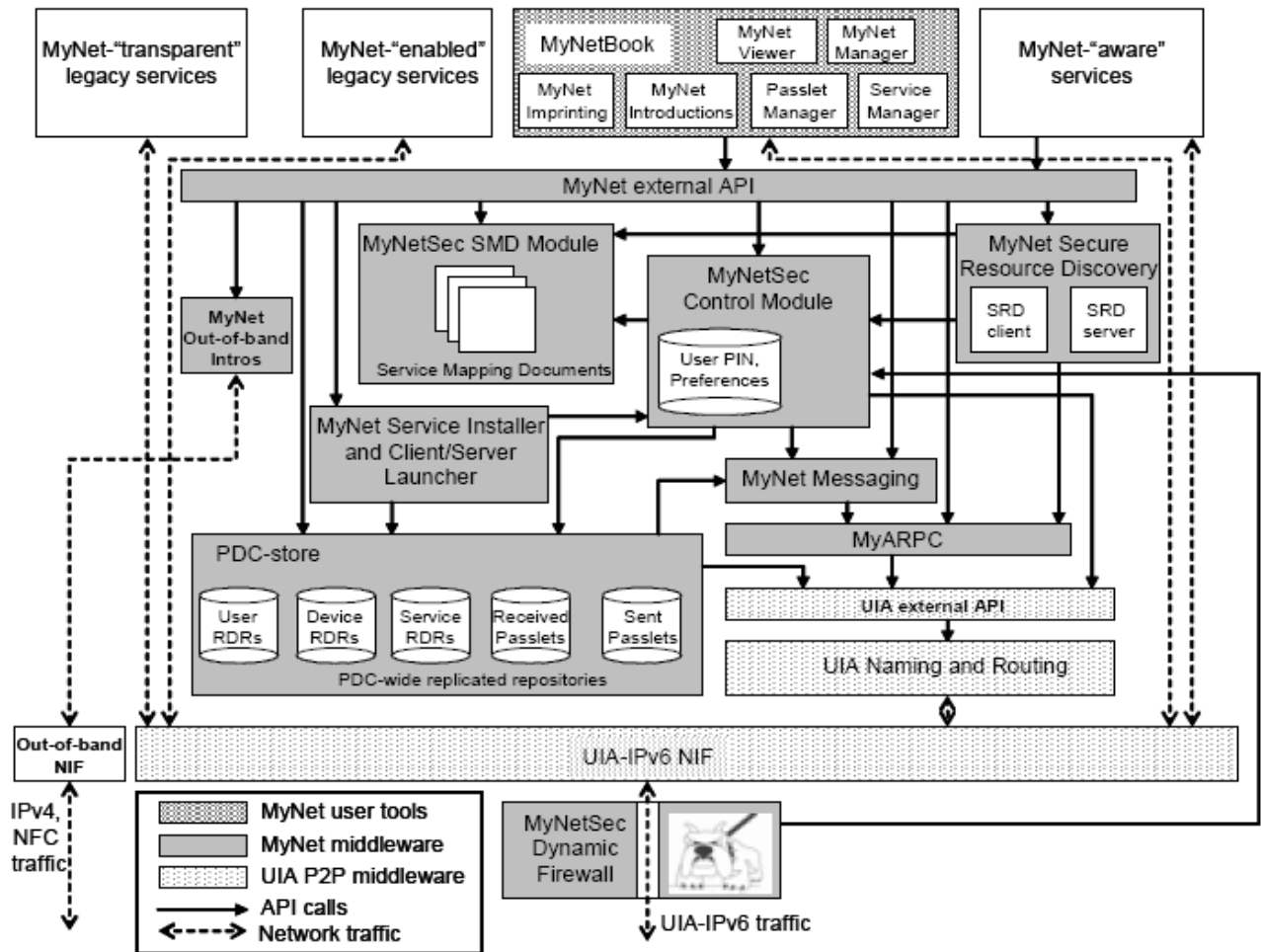
χρηστών παραμένουν ενεργά όσο ο χρήστης είναι συνδεδεμένος στο δίκτυο από τον δικό του προσωπικό υπολογιστή και δεύτερον οι έως τώρα εφαρμογές του LifeSocial.KOM είναι εφαρμογές desktop και δεν εκτελούνται μέσω κάποιου φυλλομετρητή διαδικτύου.

### **3.5 Η Κατανεμημένη Πλατφόρμα Κοινωνικής Δικτύωσης MyNet**

Το MyNet [31] είναι μια πλατφόρμα, η οποία υποστηρίζει ασφαλή P2P υπηρεσίες προσωπικής και κοινωνικής δικτύωσης. Το MyNet έχει υλοποιηθεί στην κορυφή του επιπέδου Unmanaged Internet Architecture(UIA) και επιτρέπει στους απλούς χρήστες να οργανώνουν και να μοιράζονται εύκολα τους πόρους εντός των γειτονικών κοινωνικών τους δικτύων. Μέσω ενός οδηγού-wizard που ονομάζεται MyNetBook, το οποίο είναι ένα από τα εργαλεία του MyNet UI καθοδηγεί τον χρήστη να αποτυπώσει την ταυτότητα του σε μια νέα συσκευή. Έτσι, όταν ο χρήστης έχει αποτυπώσει την δική ταυτότητα και σε άλλες δίκτες του συσκευές, τότε οι συσκευές ενώνονται μέσω των υπηρεσιών του MyNet και δημιουργούν ένα προσωπικό δίκτυο, PDC – Personal Device clusters, για τον χρήστη. Πολλά τέτοιου είδους προσωπικά δίκτυα PDCs μπορούν να συνδεθούν μεταξύ τους με την βοήθεια της υπηρεσίας του MyNet Introduction Process, δημιουργώντας ένα κοινωνικό δίκτυο. Κατά την διάρκεια της σύνδεσης μεταξύ των συσκευών στα επίπεδα UIA τους, γίνεται η ανάλλαξη κρυπτογραφημένων δεδομένων δρομολόγησης SIDs(Start point Identifiers) και EID (End point Identifiers). Κάθε συσκευή του χρήστη παράγει ένα ιδιωτικό/δημόσιο κλειδί που κρυπτογραφεί τα δεδομένα που ανταλλάζει με άλλες συσκευές. Οι συσκευές του χρήστη μπορεί να είναι ένα pc, ένα smartphone, μια παιχνιδιομηχανή κ.α. τα οποία να υποστηρίζουν την υπηρεσία δικτύωσης.

Οι χρήστες του MyNet έχουν την δυνατότητα να καθορίσουν αυτοί το επίπεδο προσβασιμότητας στους πόρους τους από άλλους χρήστες μέσω των Passlets (πάσο ή εισιτήριο). Το πλαίσιο ασφαλείας του MyNet επιτρέπει την απεριόριστη πρόσβαση του ιδιοκτήτη στις συσκευές του, χωρίς να απαιτείται οποιαδήποτε περαιτέρω διαδικασία για τον ορισμό δικαιωμάτων πρόσβασης. Όσον αφορά τις επαφές και φίλους του χρήστη, μπορούν να χρησιμοποιούν τους πόρους του χρήστη σε τέτοιο επίπεδο αναλόγως με τα δικαιώματα πρόσβασης που τους έχουν χορηγηθεί από τον χρήστη που έχει την κυριότητα των δεδομένων του προφίλ του. Η συνδεσιμότητα και το δίκτυο πλοήγησης γίνονται τόσο απλά όπως επιλέγοντας κάποιο εικονίδιο σε μια οθόνη, ενώ η πολυπλοκότητα των λειτουργιών για τον εντοπισμό υπηρεσιών, δικτύου πρόσβασης και ασφάλειας παραμένουν κρυφά από τον τελικό χρήστη.

Η αρχιτεκτονική του MyNet παρουσιάζεται στο παρακάτω σχήμα ( Σχ. 3.7).

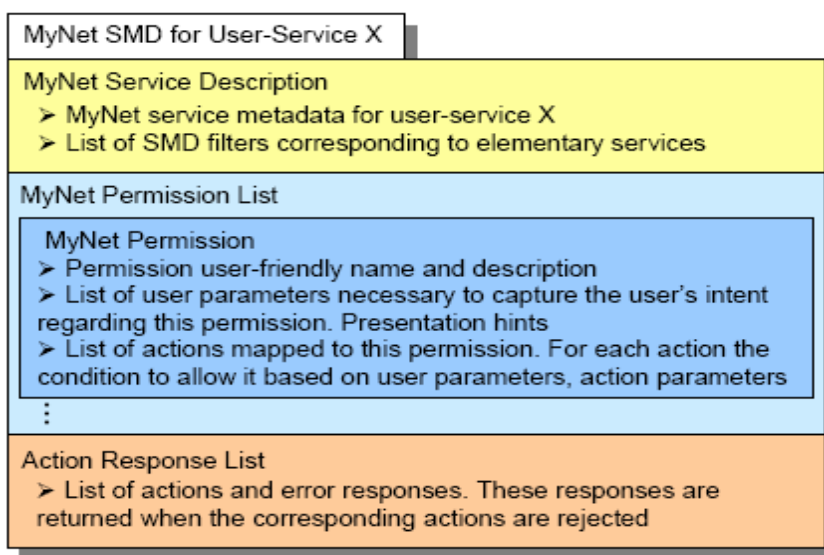


Σχήμα 3.7: Επισκόπηση της αρχιτεκτονικής δομής του MyNet [31]

Η προσθήκη μιας συσκευής ή μιας επαφής στο MyNet PDC εκτελείται από την υπηρεσία Out-of-Band Introductions. Στη συνέχεια εκκινείται η διαδικασία εντοπισμού συσκευών ομότιμων του MyNet μέσω των μηχανισμών που δεν χρησιμοποιούν UIA-IPv6. Μέσω της υπηρεσίας Out-of-Band επιτυγχάνετε η διαδικασία εισαγωγής της συσκευής στο MyNet PDC χρησιμοποιώντας τις επιμέρους τεχνολογίες των εφαρμογών του MyNet. Μέσω των MyNet - "aware" εφαρμογών οι διεργασίες μπορούν να χρησιμοποιούν την ασύγχρονη απομακρυσμένης διασύνδεσης υπηρεσία RPC- Remote Procedure Call, όπου στην περίπτωση του MyNet ονομάζεται MyARPC. Μέσω αυτής της υπηρεσίας επιτυγχάνετε η ανταλλαγή μηνυμάτων μεταξύ των συσκευών. Το MyNet χρησιμοποιεί την RPC βιβλιοθήκη του UIA, η οποία βασίζεται στην τεχνολογία της SUN RPC. Αντίστοιχες τεχνολογίες του MyARPC είναι οι XML-RPC, SOAP κ.α. Όλα τα μηνύματα του MyARPC μεταδίδονται μόνο μέσω ασφαλές SSL συνδέσεων.

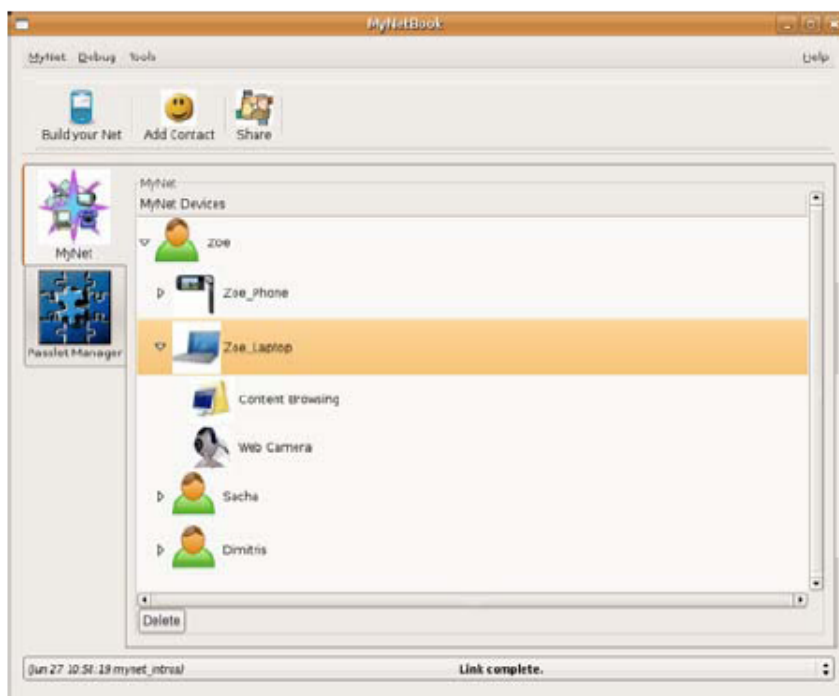
Το MyNet μέσω της υπηρεσίας MyNet Messaging εξασφαλίζει ότι τα μηνύματα που αποστέλλονται προς μόνο μια άλλη συσκευή δεν πρόκειται να χαθούν ακόμη και όταν η συσκευή αυτή είναι απενεργοποιημένη [31]. Τα μηνύματα οργανώνονται σε μια ουρά στην συσκευή αποστολέα, όπου για το κάθε μήνυμα που δεν έχει παραληφθεί ορίζεται και μια ημερομηνία διαγραφής του. Συνήθως η διάρκεια διατήρησης των μηνυμάτων αυτών ορίζεται για αρκετές ημέρες. Το MyNetSec Control του MyNet λειτουργεί ως ένας δυναμικός τοίχος προστασίας του δικτύου διαχειρίζοντας κατάλληλα την κυκλοφορία των δεδομένων σύμφωνα με τις πληροφορίες πρόσβασης που φέρουν τα Passlets.

Η υπηρεσία SMD [31] είναι υπεύθυνη για το parsing των SMD έγγραφων, των υπηρεσιών που είναι εγκατεστημένες σε κάθε συσκευή και για την παροχή πληροφοριών σχετικά με αυτές τις υπηρεσίες για την ανακάλυψη MyNet (SRD) και των μονάδων ασφαλείας. Μια τέτοια SMD έγγραφο παρουσιάζεται στο παρακάτω σχήμα (Σχ. 3.8).



**Σχήμα 3.8:** Επισκόπηση της δομής του SMD εγγράφου [31].

Οι τεχνολογίες που έχουν χρησιμοποιηθεί για την ανάπτυξη του πρότυπου MyNet είναι: οι γλώσσες προγραμματισμού C, C++, Shell scripts και η Python. Η διεπαφή χρήστη του MyNet παρουσιάζεται στις δυο παρακάτω εικόνες (Εικ. 3.5) και (Εικ. 3.6).



**Εικόνα 3.5:** Η διεπαφή χρήστη του MyNet Viewer [31].



**Εικόνα 3.6:** Η διεπαφή χρήστη του εργαλείου διαχείρισης MyNet Passlet [31].

Συγκρίνοντας τις υπηρεσίες που προσφέρει το MyNet με τις υπηρεσίες που προσφέρουν τα online κοινωνικά δίκτυα, παρατηρούμε ότι μέσω του MyNet οι χρήστες μπορούν να ανταλλάξουν ασύγχρονα και συγχρονισμένα μηνύματα, καθώς και να μεταφέρουν αρχεία μέσω των desktop εφαρμογών του MyNet και όχι μέσω ενός φυλλομετρήτη διαδικτύου. Αυτό αποτελεί έναν περιορισμό στην προσβασιμότητα του χρήστη από οπουδήποτε.

Επίσης, δεν υλοποιεί όλες τις υπηρεσίες που προσφέρει ένα online κοινωνικό δίκτυο, όπως το προφίλ του κάθε χρήστη να είναι online και όταν αυτός αποσυνδέεται, tagging κ.α. Τελευταία παρατηρείται ότι το MyNet έχει αρχίσει να χρησιμοποιείται ως εφαρμογή σε τηλεοράσεις τελευταίας γενιάς με πρόσβαση στο διαδίκτυο, σε συνδυασμό με μια δεύτερη εφαρμογή που ονομάζεται Falcon από την InfoSys Labs.

### **3.6 Το Κατανεμημένο Κοινωνικό Δίκτυο Peerscape**

Το Peerscape [33] είναι ένα πειραματικό peer-to-peer κοινωνικό δίκτυο το οποίο έχει υλοποιηθεί ως μια επέκταση (plugin) του φιλομετρητή Firefox 3.x. Το Peerscape έχει αναπτυχθεί από το Helsinki Institute for Information Technology-HIIT. Υλοποιεί ένα είδος serverless(ημι-διακομιστή) ανάγνωσης-εγγραφής δεδομένων υποστηρίζοντας third-party AJAX εφαρμογές.

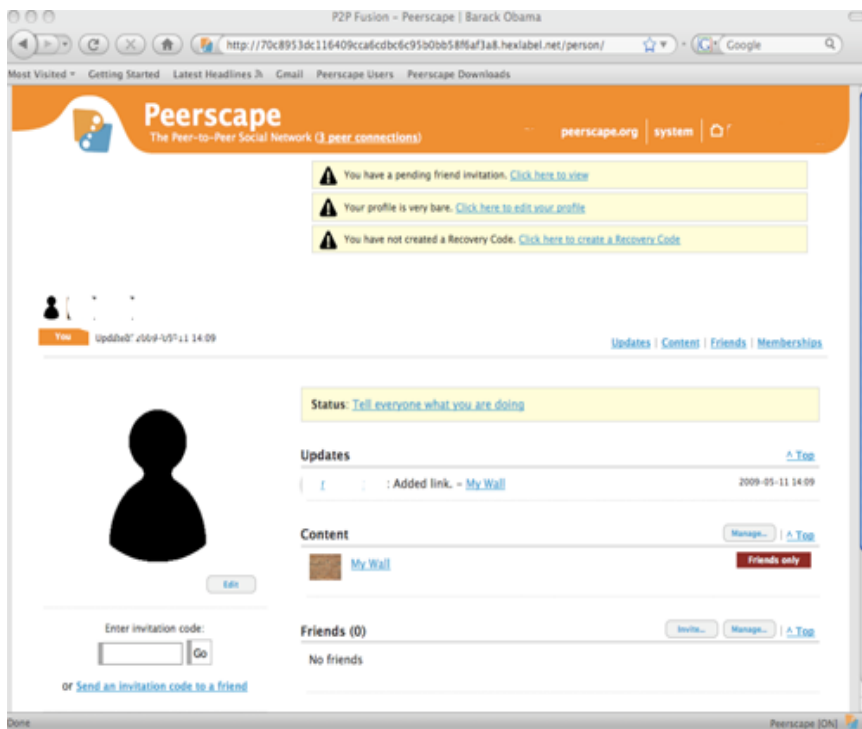
Στην πραγματικότητα αυτό που επιτυγχάνει το Peerscape, για τους χρήστες που το έχουν εγκαταστήσει ως επέκταση στο Firefox είναι, να αποθηκεύει τοπικά στον υπολογιστή του χρήστη, αντίγραφα των δεδομένων του προφίλ του και των φίλων του, καθώς και των ομάδων που έχει συμμετάσχει ο χρήστης. Επίσης, αποθηκεύει τα αντίγραφα των δεδομένων όπου έχει πλοηγηθεί ο χρήστης. Οι υπολογιστές των χρηστών «φίλων» που αποθηκεύουν τα ίδια δεδομένα δημιουργούν συνδέσεις μεταξύ τους, έτσι ώστε να διατηρούν τα δεδομένα ενημερωμένα με τις τελευταίες αλλαγές που μπορεί να κάνουν οι χρήστες τους.

Το Peerscape χρησιμοποιεί ένα δημόσιο κλειδί κρυπτογράφησης υπογραφών, για την κωδικοποίηση των δεδομένων που ανταλλάσσονται μεταξύ των χρηστών, καθώς και για την κωδικοποίηση των συνδέσεων μεταξύ των φίλων και των ομάδων τους [33].

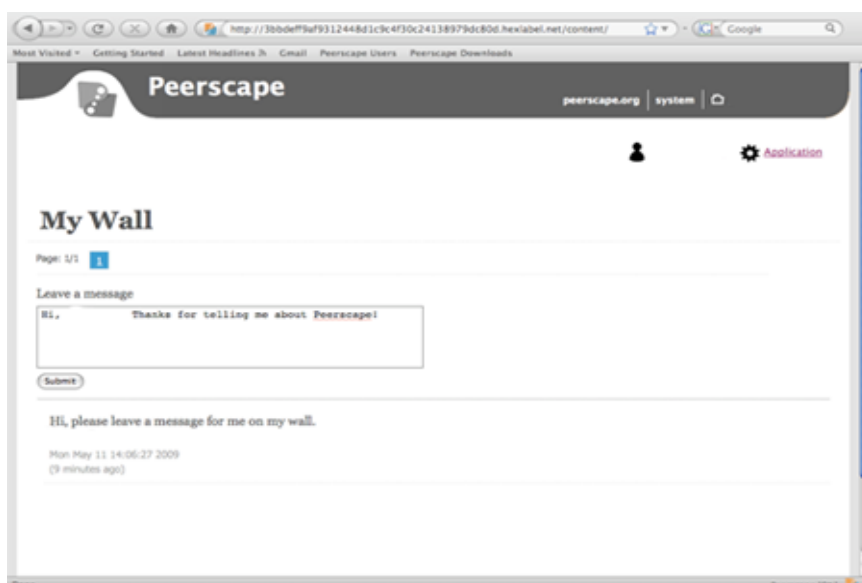
Η πρότυπη έκδοση του Peerscape έχει αναπτυχθεί με την βοήθεια της αντικειμενοστραφούς γλώσσας προγραμματισμού Python. Το Peerscape χρησιμοποιεί το REST για να εκτελεί διαδικασίες μέσω της HTTP διεπαφής. Επίσης, για την ενημέρωση των δεδομένων στην διεπαφή πλοήγησης του χρήστη χρησιμοποιεί το JSON.

Το κύριο περιεχόμενο της βάσης δεδομένων του Peerscape είναι οργανωμένο σε κοινά σύνολα βάσεων δεδομένων (datasets). Κάθε σύνολο δεδομένων έχει ένα μοναδικό αναγνωριστικό κλειδί πληροφοριών «ID», το οποίο αποτελείται από 40 δεκαεξαδικά ψηφία. Τα σύνολα δεδομένων μοιάζουν με ιεραρχίες αρχείων, όπου το κάθε σύνολο αποτελείται από μια συλλογή ζευγαριών

μεταξύ «κλειδιών - τιμών», όπου τα κλειδιά είναι διαδρομές και οι τιμές δεδομένα (byte-strings). Η κάθε διαδρομή αποτελείται από μια ή περισσότερες μη κενές συμβολοσειρές όπου χρησιμοποιείται ο χαρακτήρας «/» ως διαχωριστής. Η διεπαφή χρήστη του Peerscape παρουσιάζεται στις παρακάτω εικόνες (Εικ. 3.7) και (Εικ. 3.8).



Εικόνα 3.7: Η διεπαφή χρήστη του Peerscape [33].



Εικόνα 3.8: Η διεπαφή χρήστη του τοίχου μηνυμάτων του Peerscape [33].



Συγκρίνοντας τις υπηρεσίες που προσφέρει το Peerscape με τις υπηρεσίες των online κοινωνικών δικτύων παρατηρούμε ότι, το Peerscape υποστηρίζει μόνο την ανταλλαγή ασύγχρονων μηνυμάτων και την μεταφορά αρχείων μεταξύ των χρηστών του. Ένα μειονέκτημα του Peerscape είναι ότι δεν εκτελείται από άλλους φιλομετρητες έκτος του Firefox. Επιπρόσθετα, ένα σημαντικό σημείο που αξίζει να αναφέρουμε για το Peerscape είναι, ότι η ανάπτυξη του έχει σταματήσει από το 2009, όπου πλέον δεν υποστηρίζεται ούτε από την νέα έκδοση του Firefox 15.x

### 3.7 Διαφορές μεταξύ των P2P Εφαρμογών Κοινωνικών Δικτύων

Οι διαφορές μεταξύ των P2P εφαρμογών που αναλύσαμε παραπάνω παρουσιάζονται στον παρακάτω πίνακα (Πίνακας. 3.1) :

Όνομα Εφαρμογής	Υπηρεσίες που υποστηρίζει	Πρωτόκολλα που υποστηρίζει	Υποστήριξη ιδιοκτητήτων δεδομένων	Ομόσπονδες Επικοινωνία με άλλες εφαρμογές	Κατάσταση υλοποίησης
Diaspora	Microblogging, photo sharing, 'aspects' - friend management	Salmon	Ναι, την παρέχει μέσω των "aspects".	Ναι, επιτυγχάνεται μέσω του application framework και είναι σε δοκιμαστική έκδοση - beta.	Δοκιμαστική έκδοση - beta
PeerSon	Social Links,	OpenDHT	Ναι, την παρέχει	Ναι, όμως	Αρχική έκδοση -

	Digital Personal Space, Means of Communication		μέσω του Globally Unique IDs (GUID).	βρίσκεται σε δοκιμαστική έκδοση – beta.	alpha
PrPl	Add/Edit User Messages, File Manager, User calendar	REST, RPC, OpenID, YADIS/XRI	Ναι	Ναι, επιτυγχάνεται μέσω των Butlers.	Αρχική έκδοση - alpha
SocialLife	profiles, messaging, groups, chat, content sharing, whiteboard, multicast	DHT, FreePastry	Ναι	Ναι	Δοκιμαστική έκδοση - beta
MyNet	Add/Edit contacts, groups, photo album sharing, file sharing	RPC	Ναι	Ναι	Αρχική έκδοση - alpha
Peerscape	profiles, messaging, content sharing	REST, JSON	Ναι	Όχι	Αρχική έκδοση - alpha

**Πίνακας 3.1:** Οι διαφορές μεταξύ των P2P Εφαρμογών Κοινωνικών Δικτύων.

Όπως παρατηρούμε και από τον παραπάνω συγκριτικό πίνακα των P2P Εφαρμογών Κοινωνικών Δικτύων, οι δυο P2P εφαρμογές που ξεχωρίζουν και η υλοποίησή τους βρίσκεται σε beta στάδιο, είναι το Diaspora και το SocialLife, τα οποία καλύπτουν σε μεγάλο βαθμό τις υπηρεσίες που προσφέρουν τα online κοινωνικά δίκτυα.

# **Κεφάλαιο 4**

## **Σχεδίαση και Ανάπτυξη**

### **Κατανεμημένου Κοινωνικού**

#### **Δικτύου**

Στο τρέχων κεφάλαιο γίνεται μια σύντομη ανασκόπηση των βασικότερων τεχνολογιών που εντοπίσαμε στο Κεφαλαίο 3 για την δημιουργία ενός p2p κοινωνικού δικτύου. Αναλύουμε τις νέες τεχνολογίες που έχουν σήμερα προταθεί για την ανάπτυξη ενός κατανεμημένου κοινωνικού δικτύου. Εντοπίζουμε τις λειτουργικές και μη λειτουργικές απαιτήσεις ενός κατανεμημένου κοινωνικού δικτύου. Τέλος, παρουσιάζουμε την αρχιτεκτονική σχεδίαση και το διάγραμμα περιπτώσεων χρήσης του κατανεμημένου κοινωνικού δικτύου μας.

## 4.1 Τεχνολογίες και Πρότυπα

Σήμερα έχουν προταθεί αρκετές νέες τεχνολογίες για την επίτευξη μιας p2p σύνδεσης μέσω του διαδικτύου. Μερικές τεχνολογίες από αυτές έχουν σχεδιαστεί σε επίπεδο πρωτόκολλου και μερικές άλλες σε επίπεδο διακομιστή διαδικτύου. Μερικές από αυτές τις τεχνολογίες έχουν σχεδιαστεί ακόμη και σε επίπεδο γλώσσας προγραμματισμού διαδικτύου. Τέτοιου είδους τεχνολογίες είναι: το πρωτόκολλο OpenDHT, το πρωτόκολλο Chord, ο εξυπηρετητής Jabber/XMPP, η βιβλιοθήκη cURL της PHP κ.α. Παρακάτω αναλύουμε μερικές από αυτές τις τεχνολογίες.

### 4.1.1 Το πρωτόκολλο OpenDHT

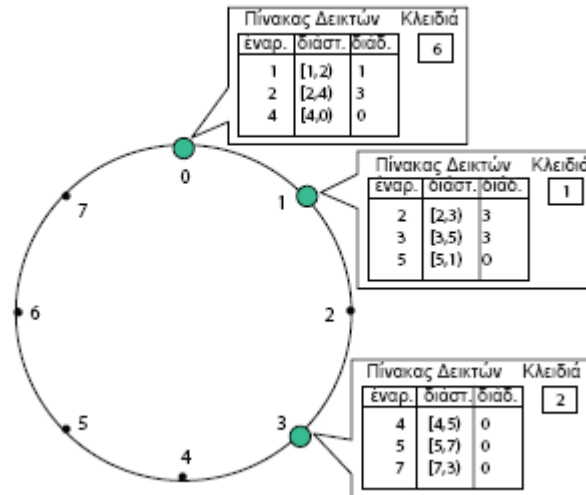
Το OpenDHT [23, 34] αποτελεί επέκταση του Bamboo DHT [24] συστήματος στο PlanetLab, μέσω του οποίου εξετάζονται οι ιδέες σχετικά με τη δημιουργία ενός αποδοτικότερου κοινωνικού δικτύου. Το OpenDHT εκτελείται σε περίπου 200-300 κόμβους. Η ιδέα πίσω από αυτό το ερευνητικό έργο είναι η δημιουργία ενός συστήματος που θα είναι πάντα online συνδεδεμένο, ενώ η διαχείριση του θα επιτυγχάνεται μέσα από μια απλή διεπαφή χρήστη. Όλοι οι ενεργοί κόμβοι του OpenDHT παρατίθενται μέσα από μια ιστοσελίδα που έχει υλοποιηθεί για αυτόν τον σκοπό. Η ανάπτυξη αυτού του έργου εστιάζεται για καθαρά ερευνητικούς σκοπούς και προορίζεται να είναι η βάση για τις εφαρμογές χρηστών που θα αναπτύσσονται επιπρόσθετα στο σύστημα. Τα πλεονεκτήματα του συγκεκριμένου έργου είναι πάρα πολλά. Για την χρήση της επέκτασης ενός OpenDHT θα πρέπει αρχικά να δημιουργηθεί μια client ομότιμη εφαρμογή, η οποία θα επικοινωνεί με τους κόμβους DHT. Όμως η υλοποίηση του OpenDHT που επεκτείνεται στο PlanetLab δεν επιδέχεται αλλαγές και αυτό αποτελεί έναν σημαντικό περιορισμό ως προς την συμβατότητα μιας ομότιμης εφαρμογής να επικοινωνήσει με τους κόμβους του OpenDHT. Επιπρόσθετα, στο Bamboo με τις κατάλληλες αλλαγές που επιτρέπει μέχρι κάποιο σημείο, μπορεί να αποτελέσει ένα περιβάλλον για την εκτέλεση demo εφαρμογών με τις κατάλληλες επεκτάσεις. Το Bamboo έχει υλοποιηθεί χρησιμοποιώντας την αντικειμενοστραφής γλώσσα προγραμματισμού Java. Όμως, αυτό δεν αποτελεί περιορισμό σε μια ομότιμη εφαρμογή, η οποία θα μπορούσε να αναπτυχθεί σε οποιαδήποτε άλλη γλώσσα προγραμματισμού. Το OpenDHT σε αντίθεση με άλλα εφαρμοσμένα DHT συστήματα, έχει μια επιπρόσθετη μέθοδο αφαίρεσης, έτσι τα ζευγάρια τιμών-κλειδιά μπορούν όχι μόνο να τεθούν και να αναζητηθούν στο σύστημα, αλλά και να αφαιρεθούν εάν είναι απαραίτητο.

#### 4.1.2 Το πρωτόκολλο Chord

Το Chord [32, 34] αποτελεί ένα πρωτόκολλο ομότιμου δικτύου που στοχεύει στην γρήγορη και αποτελεσματική αναζήτηση μεταξύ των κόμβων. Το πρωτόκολλο Chord, οργανώνει τους κόμβους του δικτύου γύρω από ένα νοητό δακτύλιο, βάση ενός μοναδικού ID που αντιστοιχεί σε κάθε κόμβο [32]. Η γρήγορη αναζήτηση επιτυγχάνεται με τη χρήση αναφορών σε πολλαπλούς κόμβους σταθερής θέσης (Finger Tables), που αποτελούν σημεία με αποστάσεις τις δυνάμεις του δύο, έτσι ώστε να λογαριθμείται ο χρόνος που χρειάζεται να ταξιδέψει ένα αίτημα γύρω από τον κύκλο [32].

Συγκεκριμένα, το Chord ήταν ένα από τα πρώτα DHT συστήματα και έχει εξελιχθεί από την πρώτη του υλοποίηση. Το ερευνητικό έργο έχει παραμείνει ίδιο και δεν έχει επεκταθεί καθόλου. Ένα βασικό πλεονέκτημα του Chord είναι εύκολο να κατανοηθεί λόγω της απλής δομής του. Παρόλα αυτά, το Chord έχει το μειονέκτημα ότι είναι στατικό. Αυτό σημαίνει ότι ένας κόμβος υπολογίζει το κόμβο-κλειδί του πριν εισαχθεί στο σύστημα και είναι υπεύθυνος για τα δεδομένα κοντά στον κόμβο-κλειδί του, με αποτέλεσμα να κάνει δυσκολότερη τη λειτουργία της εξισορρόπησης φορτίου. Ακόμη όμως και με αυτό, το Chord παραμένει μία πάρα πολύ καλή λύση για τη σχεδίαση ενός επεκτάσιμου και αυτόνομου κοινωνικού δικτύου.

Το Chord, δομείται στο χαμηλότερο στάδιο με ένα νοητό δακτύλιο πάνω στον οποίο τοποθετούνται όλοι οι κόμβοι/agents του δικτύου [32]. Η σειρά με την οποία θα τοποθετηθούν καθορίζεται από το κλειδί (ID) των κόμβων. Το ID ενός κόμβου είναι ένα μοναδικό χαρακτηριστικό του. Έτσι, ακολουθώντας συγκεκριμένες διαδικασίες του πρωτόκολλου Chord, οι κόμβοι τείνουν να τοποθετηθούν γύρω από έναν νοητό δακτύλιο με αύξουσα σειρά modulo  $n$ , όπου  $n$  το μέγιστο πλήθος κόμβων που μπορεί να υποστηρίξει το δίκτυο. Σύμφωνα με αυτή την αρχιτεκτονική, κάθε agent διατηρεί αναφορές στον αμέσως επόμενο του στον δακτύλιο (successor, αναφέρεται succ()), καθώς επίσης και για τον αμέσως προηγούμενό του (predecessor, αναφέρεται pred()) [32, 34]. Η δικτυακή αυτή οργάνωση αποτελεί μια βασική δομή πάνω στην οποία μπορεί να θεμελιωθεί ένα ομότιμο δίκτυο όπως παρουσιάζεται στο παρακάτω σχήμα (Σχ. 4.1).



**Σχήμα 4.1:** Παράδειγμα δακτυλίου με πίνακα δεικτών σε ένα δίκτυο Chord.

### 4.1.3 Ο διακομιστής Jabber/XMPP

Ο XMPP - Xtensible Messaging and Presence Protocol [35, 36], είναι η επίσημη ονομασία της οικογένειας πρωτοκόλλων IMP που αναπτύχθηκαν για αρκετά χρόνια από την κοινότητα Jabber. Μέχρι την υποβολή του στις διαδικασίες προτυποποίησης και τελικής έγκρισης της IETF, ονομαζόταν Jabber, και με αυτό το όνομα έχει καθιερωθεί και είναι γνωστό στους χρήστες του Διαδικτύου. Οι δυο έννοιες πλέον θεωρούνται ταυτόσημες.

Ο XMPP είναι ένα σύνολο ανοιχτών πρωτοκόλλων άμεσης επικοινωνίας (instant messaging), βασισμένα στην XML [35, 36]. Το λογισμικό Jabber είναι εγκατεστημένο σε χιλιάδες διακομιστές ανά το διαδίκτυο και χρησιμοποιείται από τουλάχιστον 10 εκατομμύρια χρήστες παγκοσμίως, σύμφωνα με τα στοιχεία της Jabber Software Foundation.

Μερικά από τα βασικά χαρακτηριστικά του XMPP είναι:

- **Αποκεντρωμένο**

Η αρχιτεκτονική του δικτύου Jabber/XMPP είναι παρόμοια με αυτή της ηλεκτρονικής αλληλογραφίας, όπου ο κάθε χρήστης μπορεί να εγκαταστήσει και χρησιμοποιήσει τον προσωπικό του διακομιστή Jabber/XMPP [36].

- **Ανοιχτό πρότυπο**

Η IETF αναγνώρισε τα πρωτόκολλα επικοινωνίας στα οποία βασίζεται το Jabber ως πρότυπα υπό την ονομασία XMPP. Οι προδιαγραφές αυτών των πρότυπων είναι δημόσια διαθέσιμες με τις ονομασίες RFC 3920 και RFC 3921. Ένα σημαντικό σημείο που πρέπει να αναφέρουμε εδώ είναι ότι, για την ανάπτυξη λογισμικού όπου βασίζεται στα παραπάνω πρότυπα δεν απαιτούνται περαιτέρω δικαιώματα χρήσης [36].

- **Ασφαλές**

Ένας διακομιστής τύπου Jabber/XMPP μπορεί να χρησιμοποιηθεί ακόμη και σε ένα intranet προσφέροντας ισχυρή ασφάλεια μέσω του SASL Framework και TLS πρωτόκολλου που έχουν ενσωματωθεί στα πρότυπα του XMPP [36].

- **Αποδεδειγμένο**

Οι τεχνολογίες Jabber/XMPP χρησιμοποιούνται από το 1998. Πολλές εφαρμογές Jabber/XMPP όπως διακομιστές, client εφαρμογές, βιβλιοθήκες έχουν αναπτυχθεί και δέχονται την υποστήριξη μεγάλων εταιριών, όπως την Sun Microsystems και την Google [36].

- **Επεκτάσιμο**

Παρέχει την δυνατότητα σε προγραμματίστρες να αναπτύξουν και να προσθέσουν την δική τους λειτουργικότητα στην κορυφή των πρωτοκόλλων πυρήνα που υποστηρίζει το XMPP χρησιμοποιώντας την γλώσσα σήμανσης XML. Για την διατήρηση της διαλειτουργικότητας και των κοινών επεκτάσεων έχουν δημοσιευθεί τα πρότυπα στις επεκτάσεις XEP. Επίσης η δημοσίευση των προσαρμοσμένων πρότυπων δεν είναι απαραίτητη και οι οργανισμοί μπορούν να διατηρούν τις δικές τους ιδιωτικές επεκτάσεις, εάν το επιθυμούν [36].

- **Ευέλικτο**

Οι XMPP IM εφαρμογές περιλαμβάνουν πέρα από τη διαχείριση του δικτύου και τη διαχείριση περιεχομένου, εργαλεία συνεργατικότητας, κοινή χρήση αρχείων, το gaming, την εξ' αποστάσεως



παρακολούθηση των συστημάτων, διαδικτυακές υπηρεσίες, το cloud computing, και πολλά άλλα [36].

#### ▪ **Ποικιλότητα**

Ένα ευρύ φάσμα εταιρειών που υλοποιούν ανοιχτού κώδικα έργα, χρησιμοποιούν XMPP για να δημιουργήσουν και να αναπτύξουν σε πραγματικό χρόνο εφαρμογές και υπηρεσίες [36].

Το δίκτυο Jabber/XMPP ακολουθεί τη λογική πελάτη-διακομιστή (client-server), αλλά παραμένοντας αποκεντρωμένο. Δεν υπάρχει λοιπόν κάποιος κεντρικός διακομιστής όπως σε άλλες υπηρεσίες σαν το AOL Instant Messenger ή το MSN Messenger. Στο δίκτυο XMPP ένας χρήστης προσδιορίζεται με ένα «όνομα χρήστη» και ένα «όνομα διακομιστή». Τα δυο πεδία αυτά συνδέονται με ένα «@» και αποτελούν το λεγόμενο Jabber/XMPP ID, ή JID [36]. Η διαδικασία επικοινωνίας μεταξύ δυο χρηστών περιγράφεται παρακάτω [36]:

Ας υποθέσουμε πως ο user1@domain1.gr θέλει να επικοινωνήσει με τον user2@domain2.gr. Ο user1 και ο user2 έχουν από ένα λογαριασμό στους διακομιστές domain1.gr και domain2.gr αντιστοίχως.

- Το πρόγραμμα πελάτη του user2 στέλνει ένα μήνυμα στον διακομιστή Jabber/XMPP domain2.gr. Αν η επικοινωνία με τον διακομιστή domain1.gr απορριφθεί από τον domain2.gr, τότε το μήνυμα χάνεται.
- Ο διακομιστής domain2.gr ανοίγει μια σύνδεση με τον διακομιστή domain1.gr.
- Ο διακομιστής domain1.gr παραδίδει το μήνυμα στον user1. Όμως, αν η επικοινωνία με τον διακομιστή domain2.gr απορρίπτεται από τον διακομιστή domain1.gr, το μήνυμα χάνεται. Επίσης, εφόσον ο user1 δεν είναι συνδεδεμένος, το μήνυμα αποθηκεύεται για να παραδοθεί αργότερα.

Το Jabber/XMPP ID ή JID, είναι το όνομα χρήστη ή το όνομα λογαριασμού που χρησιμοποιείται για της πρόσβαση σε έναν λογαριασμό Jabber/XMPP. Συνήθως, στις περισσότερες περιπτώσεις, το Jabber/XMPP ID είναι του τύπου username@domain name. Το πεδίο «πόρος» (resource) παρέχει την δυνατότητα σε έναν χρήστη να επικοινωνήσει με έναν άλλο «πόρο» του δικτύου. Για παράδειγμα ένας χρήστης θα μπορούσε να συνδεθεί στο λογαριασμό του με δυο διαφορετικούς πόρους (office1 και office2). Με αυτό τον τρόπο θα μπορεί δέχεται διαφορετικά μηνύματα και στους δυο πόρους ανεξαρτήτως που θα έχει συνδεθεί με τον ίδιο λογαριασμό και

στους δυο πόρους. Οι μεταφορείς (transports), οι πράκτορες (agents), και άλλα αυτοματοποιημένα μέρη του δικτύου Jabber/XMPP μπορούν να μην έχουν ένα πεδίο χρήστη στο JID τους. Ένα κοινό παράδειγμα είναι η μεταφορά AIM (AOL Instant Messenger) που έχει ένα JID του τύπου `usr.domain.com`, και οι AIM επαφές εμφανίζονται ως `screenname@usr.domain.com` [36].

Όπως αναφέραμε και παραπάνω ο XMPP είναι μια τεχνολογία συνεχής ροής μετάδοσης δεδομένων (streaming) μέσω της XML. Ο πυρήνας του XMPP υποστηρίζει τις παρακάτω τεχνολογίες [35]:

- Ένα βασικό επίπεδο συνεχής ροής δεδομένων (streaming) XML.
- Την κρυπτογράφηση καναλιών χρησιμοποιώντας το πρωτόκολλο Transport Layer Security (TLS).
- Την ισχυρή ταυτοποίηση χρησιμοποιώντας το επίπεδο Simple Authentication and Security Layer (SASL).
- Την χρήση του UTF-8 για την πλήρη υποστήριξη Unicode, συμπεριλαμβάνοντας και τις διεθνοποιημένες διευθύνσεις.
- Ενσωματωμένες (built-in) πληροφορίες σχετικά με τη διαθεσιμότητα του δικτύου.
- Μια συνεχώς ενημερωμένη και ενεργή λίστα επαφών.

Ένα μοναδικό χαρακτηριστικό του συστήματος Jabber [35, 36] είναι αυτό των μεταφορών που ονομάζεται και ως «Πύλες». Οι πύλες επιτρέπουν στους χρήστες την πρόσβαση σε δίκτυα βασισμένα σε άλλα πρωτόκολλα. Αυτά μπορεί να είναι πρωτόκολλα άμεσης επικοινωνίας, αλλά και πρωτόκολλα όπως το SMS ή αυτό του ηλεκτρονικού ταχυδρομείου. Σε αντίθεση με τα προγράμματα πελάτες που υποστηρίζουν ταυτόχρονα πολλά πρωτόκολλα, το Jabber παρέχει αυτήν την υπηρεσία στο επίπεδο του διακομιστή, διαμέσου των ειδικών πυλών που τρέχουν σ' αυτόν. Οποιοσδήποτε χρήστης του συστήματος Jabber μπορεί να εγγραφεί (register) σε μια από αυτές τις πύλες, παρέχοντας τα στοιχεία που απαιτούνται για να καταγραφεί στο δίκτυο με το οποίο θα συνδεθεί. Εφόσον η εγγραφή του χρήστη θα έχει ολοκληρωθεί στο δίκτυο, τότε θα μπορεί να επικοινωνήσει με άλλους χρήστες αυτού του δικτύου σαν να ήταν χρήστες Jabber (και αντιστρόφως). Αυτό σημαίνει ότι οποιοδήποτε πρόγραμμα πελάτης που υποστηρίζει πλήρως το

πρωτόκολλο Jabber μπορεί να χρησιμοποιηθεί για οποιοδήποτε δίκτυο για το οποίο ο διακομιστής Jabber παρέχει μια πύλη, χωρίς πρόσθετο κώδικα στον πελάτη.

#### **4.1.4 Η βιβλιοθήκη cURL**

Η βιβλιοθήκη cURL [19] είναι ένα εργαλείο γραμμής εντολών για μεταφορά δεδομένων χρησιμοποιώντας διάφορα πρωτόκολλα επικοινωνίας. Το cURL κυκλοφόρησε με την libcurl, η οποία μπορεί να χρησιμοποιηθεί σε πολλές γλώσσες προγραμματισμού. Η διαδεδομένη της μορφή είναι αυτή στην PHP, με τη βιβλιοθήκη PHP Curl. Η cURL είναι υπεύθυνη για την μεταφορά δεδομένων με σύνταξη URL, που υποστηρίζει τα πρωτόκολλα επικοινωνίας DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, TELNET και TFTP. Επιπρόσθετα, η βιβλιοθήκη cURL, υποστηρίζει πιστοποιητικά SSL, HTTP POST, HTTP PUT, για ανάρτηση αρχείων μέσω FTP και για ανάρτηση αρχείων μέσω του πρωτόκολλου HTTP.

## **4.2 Ανάλυση Απαιτήσεων Συστήματος**

Η ανάλυση απαιτήσεων συστήματος προσδιορίζει τα ειδικά χαρακτηριστικά της αρχιτεκτονικής του συστήματος που απαιτούνται για την ικανοποιητική σχεδίαση και ανάπτυξη ενός λογισμικού. Μέσω της διαδικασίας της ανάλυσης των απαιτήσεων του λογισμικού μπορούμε να διακρίνουμε και να καθορίσουμε την συμπεριφορά του συστήματος μας, σύμφωνα πάντα με βάση τα δεδομένα εισόδου και εξόδου που θα εισάγονται και εξάγονται από το λογισμικό.

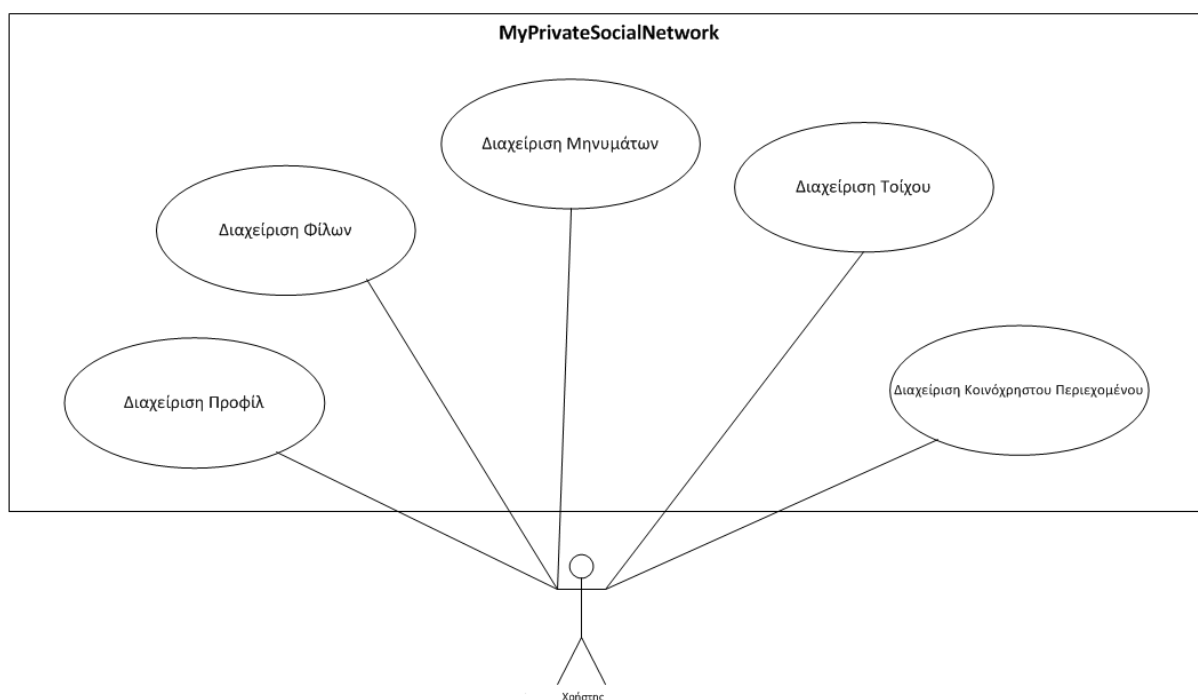
Η ανάλυση απαιτήσεων είναι η πρώτη φάση της σχεδίασης κάθε συστήματος. Ορίζεται ως το σύνολο όλων εκείνων των δραστηριοτήτων που συμβάλλουν στη περιγραφή του πεδίου εφαρμογής και του καθορισμού των απαιτήσεων του χρήστη.

Στόχος είναι ο χρήστης να έχει μια σαφή εικόνα για το ποιες είναι οι λειτουργίες που υποστηρίζει το σύστημα και ποιοι οι περιορισμοί του και ο μηχανικός λογισμικού να έχει ένα σαφή καθορισμό του προβλήματος που πρέπει να λύσει.

### 4.2.1 Βασικές Περιπτώσεις Χρήσης

Οι περιπτώσεις χρήσης περιγράφουν συστηματικά και μεθοδικά πως μια εφαρμογή θα χρησιμοποιηθεί σε κάποια συγκεκριμένη κατηγορία σεναρίων. Πολλές περιπτώσεις χρήσεις καλύπτουν τελικά όλες τις απαιτήσεις και την επιθυμητή συμπεριφορά της εφαρμογής.

Στην περίπτωση της δικής μας πρότασης, για την σχεδίαση του καταναμημένου κοινωνικού δικτύου, διακρίνουμε τις παρακάτω βασικές περιπτώσεις χρήσης (Σχ.4.2) που αποτελούν την διαδικτυακή εφαρμογή μας:



**Σχήμα 4.2:** Διάγραμμα περιπτώσεων χρήσης του καταναμημένου κοινωνικού δικτύου MyPrivateSocialNetwork.

- **Διαχείριση Προφίλ**, μέσω της οποίας ο χρήστης μπορεί να επεξεργαστεί το προσωπικό του προφίλ, όπως το ονοματεπώνυμο, το όνομα χρήστη, το email, την φωτογραφία του κ.α.
- **Διαχείριση Φίλων**, μέσω της οποίας ο χρήστης μπορεί να προβάλει τα στοιχεία του προφίλ του κάθε χρήστη που τον έχει καταχωρήσει ως φίλο. Τέτοια στοιχεία είναι, το ονοματεπώνυμο του φίλου χρήστη, το email, τη βασική φωτογραφία του προφίλ του,

καθώς και το άλμπουμ φωτογραφιών που μπορεί να έχει δημιουργήσει ο κάθε φίλος χρήστης.

- **Διαχείριση Μηνυμάτων**, μέσω της οποίας ο χρήστης μπορεί να προβάλει το ιστορικό προσωπικών μηνυμάτων που έχει αποστείλει σε φίλους του. Επιπρόσθετα, ο χρήστης μπορεί να αποστείλει νέα μηνύματα σε έναν ή περισσότερους φίλους του, καθώς και να διαγράψει μηνύματα που έχει αποστείλει στο παρελθόν.
- **Διαχείριση Τοίχου**, μέσω της οποίας ο χρήστης μπορεί να προσθέσει μηνύματα μικρού μήκους, στον τοίχο του κάθε φίλο του, καθώς και στον δικό του τοίχο μηνυμάτων. Αξίζει εδώ να σημειώσουμε ότι τα μηνύματα αυτά είναι προσβάσιμα από κάθε φίλο του χρήστη.
- **Διαχείριση Κοινόχρηστου Περιεχομένου**, μέσω της οποίας γίνεται η προσθήκη, επεξεργασία και διαγραφή πρόσθετων κοινόχρηστων πολυμεσικών και μη αρχείων του χρήστη.

Οι επιπρόσθετες ενέργειες που περιγράφονται σε κάθε περίπτωση χρήσης αποτελούν και υπό περιπτώσεις χρήσης του συνολικού συστήματος.

#### **4.2.2 Λειτουργικές Απαιτήσεις Συστήματος**

Οι λειτουργικές απαιτήσεις περιγράφουν τι πρέπει να κάνει το σύστημα, όπως για παράδειγμα οι συναρτήσεις που λαμβάνουν κάποια δεδομένα είσοδο και εξάγουν στην έξοδο νέα δεδομένα. Στην περίπτωση του συστήματος μας, ως λειτουργικές απαιτήσεις είναι οι περιπτώσεις χρήσης που περιγράψαμε παραπάνω.

#### **4.2.3 Μη Λειτουργικές Απαιτήσεις Συστήματος**

Περιγράφουν ιδιότητες του συστήματος που συνήθως εκφράζονται βάσει κάποιον χαρακτηριστικών. Ορίζουν τους περιορισμούς για την πραγμάτωση των λειτουργικών απαιτήσεων. Οι βασικές ιδιότητες των μη λειτουργικών απαιτήσεων για το σύστημα μας είναι οι ακόλουθες:

- **Διαθεσιμότητα** (*availability*), όπου εκφράζει τον μέσο χρόνο για αποτυχία του συστήματος. Στην περίπτωση μας το σύστημα μας προορίζεται για χρήση από πολλούς χρήστες χρησιμοποιώντας όμως τις ίδιες διευθύνσεις συνδεσιμότητας μεταξύ τους. Αυτό το χαρακτηριστικό αποτελεί και μια βασική παράμετρο για την πιθανή αποτυχία της συνεχούς διαθεσιμότητας του συστήματος. Έτσι λοιπόν, όταν πολλοί χρήστες του κατανεμημένου κοινωνικού δικτύου μας συνδεθούν στον ίδιο χρήστη την ίδια χρονική στιγμή, τότε το σύστημα ενδέχεται να καταρρεύσει λόγω του μεγάλου φόρτου δεδομένων.
- **Επεκτασιμότητα** (*extensibility*). Αφορά την προσθήκη νέου χαρακτηριστικού στο σύστημα. Στην περίπτωση του συστήματος μας, η προσθήκη νέου χαρακτηριστικού είναι δυνατή όμως απαιτεί αρχικά την σωστή και αναλυτική τεκμηρίωση του, έτσι ώστε να μην επιβαρύνει και κατ' επέκταση να κατάρρευση το συνολικό σύστημα του κατανεμημένου κοινωνικού δικτύου. Επιπρόσθετα, πρέπει να σημειώσουμε ότι σε περίπτωση που ενσωματωθεί ένα νέο χαρακτηριστικό στο σύστημα, τότε αυτό το νέο χαρακτηριστικό θα πρέπει να προστεθεί και σε όλα τα επιμέρους συστήματα των χρηστών του κοινωνικού δικτύου.
- **Αποδοτικότητα** (*performance*). Αφορά την ταχύτητα απόκρισης, αιτήσεις ανά δευτερόλεπτο και τον αριθμό ταυτόχρονων χρηστών. Στην περίπτωση του συστήματος μας για κάθε χρήστη η αποδοτικότητα εξαρτάται από το υλικό του συστήματος που θα έχει ο εξυπηρετητής του κάθε χρήστη. Για καλύτερη απόδοση του συστήματος θα πρέπει ο εξυπηρετητής του κάθε χρήστη, ο οποίος θα λειτουργεί και ως κόμβος του συνολικού συστήματος, να έχει ικανοποιητική μνήμη RAM, έτσι ώστε να μπορεί να εξυπηρετεί αιτήσεις (*requests*) άλλων χρηστών του κατανεμημένου κοινωνικού δικτύου. Επίσης, ένα άλλο χαρακτηριστικό της αποδοτικότητας είναι και το *bandwidth*, το οποίο θα πρέπει να αξιοποιείτε με τον βέλτιστο τρόπο. Για καλύτερη αποδοτικότητα του συνολικού συστήματος μια εκδοχή που προτείνουμε είναι τα αρχεία και δεδομένα του χρήστη να τα φιλοξενήσουμε σε περισσότερους του ενός εξυπηρετητή έτσι ώστε σε περίπτωση μεγάλου αριθμού αιτήσεων χρηστών να γίνει καλύτερη κατανομή του φόρτου στους επιμέρους εξυπηρετητές.
- **Αξιοπιστία** (*reliability*). Αφορά το ποσοστό των διαδικασιών που εκτελούνται σωστά. Το σύστημα πρέπει να παρέχει ένα συγκεκριμένο μηχανισμό, έτσι ώστε να ελέγχει και να πιστοποιεί τα δεδομένα εισόδου και εξόδου των διαδικασιών. Με τον τρόπο αυτό θα

αποτραπούν εξωτερικές κακόβουλες επιθέσεις στο συνολικό σύστημα του καταναμημένου κοινωνικού δικτύου.

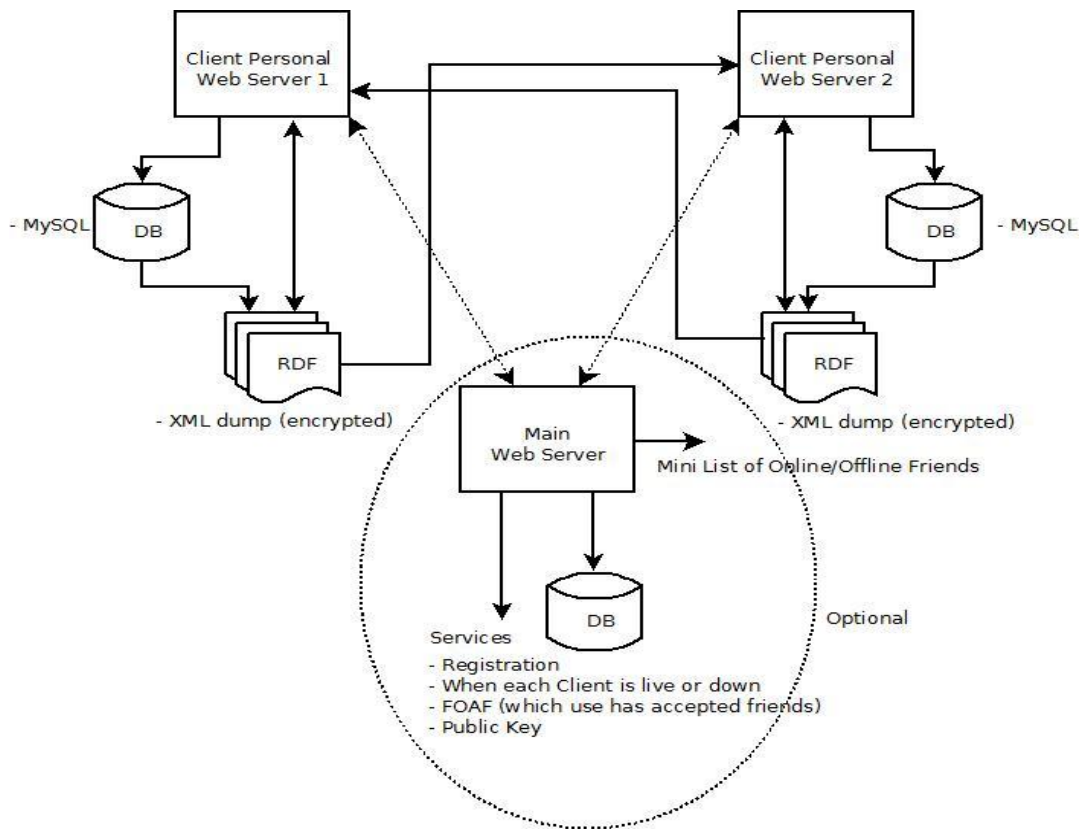
- **Ευχρηστία** (*usability*). Αφορά τον χρόνο που απαιτείται από τον χρήστη για την ολοκλήρωση μιας διαδικασίας. Το σύστημα μας πρέπει να παρέχει στον χρήστη μια αρκετά φιλική διεπαφή χρήστη, έτσι ώστε να αποφευχθούν λάθη που μπορεί να προκληθούν από λάθος επιλογές του χρήστη κατά την διάρκεια της πλοήγησης και της διάδρασης του με το σύστημα. Έτσι, μια καλή διεπαφή χρήστη τους συστήματος οδηγεί τον χρήστη στην ολοκλήρωση διαδικασιών σε συντομότερο χρόνο.
- **Δυνατότητα επαναχρησιμοποίησης** (*reusability*). Αφορά τον προσδιορισμό μονάδων που θα πρέπει να υλοποιηθούν ως ανεξάρτητες βιβλιοθήκες. Στην περίπτωση του συστήματος μας οι βιβλιοθήκες στηρίζονται σε MVC Framework, όπου η επαναχρησιμοποίηση βιβλιοθηκών γίνεται με την βέλτιστο τρόπο. Επίσης παρέχουν μεθόδους και διαδικασίες για την επικοινωνία του καταναμημένου κοινωνικού δικτύου και με εξωτερικές πηγές τύπου RSS, XML κ.α.
- **Συμμόρφωση με πρότυπα** (*standards compliance*). Όπως για παράδειγμα συμμόρφωση με το πρότυπο Web 2.0 κ.α.
- **Διαλειτουργικότητα** (*interoperability*). Αφορά τον προσδιορισμό συστημάτων με τα οποία το σύστημα πρέπει να συνεργάζεται. Μέσω των τεχνολογιών και πρωτόκολλων που στηρίζεται η σχεδίαση του καταναμημένου κοινωνικού δικτύου μας, θα παρέχετε η δυνατότητα επικοινωνίας με αλλά εξωτερικά συστήματα.
- **Προστασία προσωπικών δεδομένων** (*privacy*). Το σύστημα μας πρέπει να διαφυλάττει τα προσωπικά δεδομένα του κάθε πιστοποιημένου χρήστη του συστήματος, όπως το ονοματεπώνυμο, όνομα χρήστη, κωδικό πρόσβασης, email, κ.α. Επιπρόσθετα θα πρέπει να προστατεύει και το κοινόχρηστο πολυμεσικό περιεχόμενο που έχει αναρτήσει στο προφίλ του ο κάθε χρήστης. Με τον τρόπο αυτό θα αποτρέπεται η προσπέλαση δεδομένων από τρίτους μη εγκεκριμένους χρήστες τους συστήματος. Σημειώνουμε εδώ ότι ο κάθε χρήστης θα έχει το δικό του υποσύστημα και θα επικοινωνεί με αλλά υποσύστημα χρηστών ίδιου τύπου, μέσω των απευθείας διασυνδέσεων μεταξύ τους..

- **Ασφάλεια (safety).** Η ασφάλεια σχετίζεται με το ότι το σύστημα δεν μπορεί να προκαλέσει κάποια ζημιά ανεξάρτητα αν είναι συμβατό ή όχι προς την προδιαγραφή του.
- **Έλεγχος (auditing).** Ο έλεγχος λογισμικού βελτιώνει την συνολική ασφάλεια του συστήματος ακόμα και όταν υπάρχουν περιστασιακά λάθη λογισμικού. Επίσης, ο έλεγχος επιτρέπει την παρακολούθηση μεγαλύτερου αριθμού παραμέτρων, επιτρέπει την χρήση αξιόπιστου ηλεκτρονικού εξοπλισμού και χρησιμοποιείται για την παροχή υψηλού επιπέδου λύσεων ασφάλειας.
- **Απαίτηση επικοινωνίας με άλλα συστήματα.** Η μεταφορά των δεδομένων από μια εφαρμογή στη άλλη θα επιτυγχάνεται μέσω ενσύρματου δικτύου ή μέσω ασύρματου δικτύου.
- **Φυσική απαίτηση.** Η πρόσβαση των χρηστών στην εφαρμογή θα γίνεται μέσω διαδικτύου.
- **Απαίτηση βάσης δεδομένων.** Η διαδικτυακή εφαρμογή θα τηρεί αποθηκευμένα σε ένα αρχείο τα στοιχεία των χρηστών που θα έχουν προβεί σε εγγραφή στο σύστημα. Τα στοιχεία αυτά είναι: όνομα χρήστη, διεύθυνση URL, το port επικοινωνίας και το IP του χρήστη.
- **Απαίτηση χρήσης.** Η πρόσβαση στο σύστημα θα επιτυγχάνεται μόνο με χρήση του όνομα χρήστη και κωδικού πρόσβασης.

### 4.3 Αρχιτεκτονική Συστήματος

Η αρχιτεκτονική του συστήματος μας αποτελείται από δυο μέρη. Το πρώτο μέρος του συστήματος αφορά την διεπαφή του τελικού χρήστη(frontend), ενώ το δεύτερο μέρος αφορά την υπηρεσία εύρεσης ομότιμων κόμβων του συστήματος(backend). Η αρχιτεκτονική του συστήματος μας παρουσιάζεται στο παρακάτω σχήμα (Σχ. 4.3):





Σχήμα 4.3: Αρχιτεκτονική συστήματος του κατακεμημένου κοινωνικού δικτύου MyPrivateSocialNetwork.

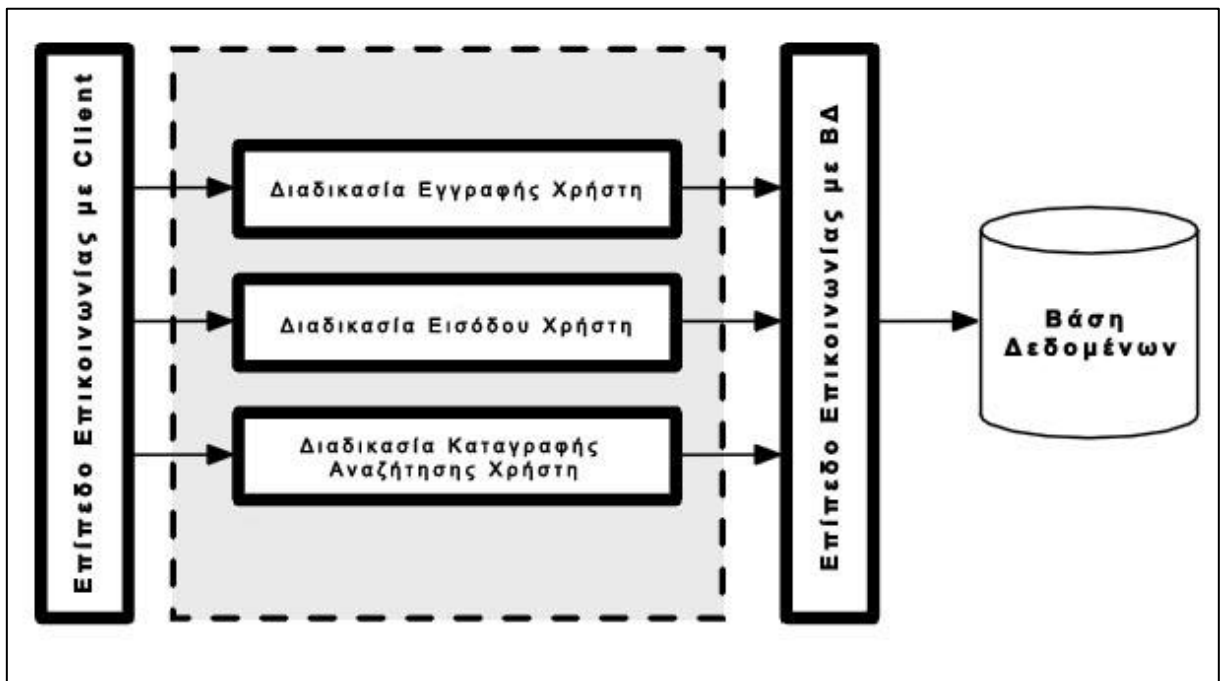
#### 4.3.1. Η Αρχιτεκτονική Backend του Συστήματος

Ένα από τα βασικά χαρακτηριστικά των ομότιμων υβριδικών δικτύων είναι ότι μπορούν να επικοινωνήσουν μεταξύ τους χωρίς την διαμεσολάβηση τρίτων εφαρμογών ή συστημάτων για την επίτευξη της επικοινωνίας [17]. Στο κατακεμημένο μας κοινωνικό δίκτυο συμπεριλάβαμε την υπηρεσία εύρεσης ομότιμων κόμβων, έτσι ώστε να αποφύγουμε την πολυπλοκότητα των μηχανισμών διασύνδεσης μεταξύ τους, καθώς και να μειώσουμε τις πιθανότητες αποτυχίας διασύνδεσης μεταξύ των κόμβων του κοινωνικού μας δικτύου. Επιπρόσθετα, ένα δεύτερο θετικό χαρακτηριστικό που προσφέρει η υπηρεσία αυτή είναι, ότι ο εντοπισμός της νέας διεύθυνσης του κάθε κόμβου επιτυγχάνεται σε συντομότερο χρόνο. Η επικοινωνία μεταξύ των κόμβων μπορεί να επιτευχθεί και χωρίς την διαμεσολάβηση της υπηρεσίας εύρεσης ομότιμων κόμβων, αν οι κόμβοι μεταξύ τους γνωρίζουν την διεύθυνση προσπέλασης του κόμβου που θέλουν να επικοινωνήσουν. Ως κόμβο εδώ εννοούμε τον προσωπικό διαδικτυακό εξυπηρετητή του κάθε χρήστη.

Η αρχιτεκτονική του συστήματος της υπηρεσίας εύρεσης ομότιμων κόμβων (Σχ. 4.4) περιέχει τις εξής διαδικασίες:

- Την διαδικασία εγγραφής χρήστη.
- Την διαδικασία εισόδου χρήστη.
- Την διαδικασία καταγραφής/αναζήτησης στοιχείων του κάθε κόμβου/χρήστη για την επικοινωνία με άλλους κόμβους.

Τα στοιχεία επικοινωνίας του κάθε κόμβου αποθηκεύονται κρυπτογραφημένα σε μια βάση δεδομένων, η οποία φιλοξενείται στον εξυπηρετητή της υπηρεσίας αυτής. Χωρίς την υπηρεσία εύρεσης ομότιμων κόμβων, η επικοινωνία μεταξύ των κόμβων του κατακευματισμένου κοινωνικού δικτύου μας δεν θα ήταν δυνατή, μιας και η IP διεύθυνση του κάθε κόμβου μπορεί να αλλάζει δυναμικά σύμφωνα πάντα και με τον κανονισμό των ISPs. Επίσης, ένα άλλο θετικό χαρακτηριστικό της υπηρεσίας αυτής είναι, ότι ο χρήστης μπορεί να αναζητήσει και να εντοπίσει νέους φίλους.



**Σχήμα 4.4:** Αρχιτεκτονική υπηρεσίας διαχείρισης χρηστών / ομότιμων κόμβων του MyPrivateSocialNetwork.

Η διαδικασία εγγραφής χρήστη, λαμβάνει τις αιτήσεις των χρηστών που αιτούνται για να συμμετέχουν στην κοινότητα του κατακευματισμένου κοινωνικού δικτύου μας. Μέσω αυτής της εγγραφής ο κάθε χρήστης/κόμβος κοινοποιεί στην κοινότητα του κατακευματισμένου κοινωνικού δικτύου την URI διεύθυνση ή IP διεύθυνση και το port του, έτσι ώστε να μπορεί κάποιος άλλος

χρήστης μέσω του δικού του κόμβου να μπορεί να υποβάλει ένα αίτημα σύνδεσης και επικοινωνίας με αυτόν τον κόμβο.

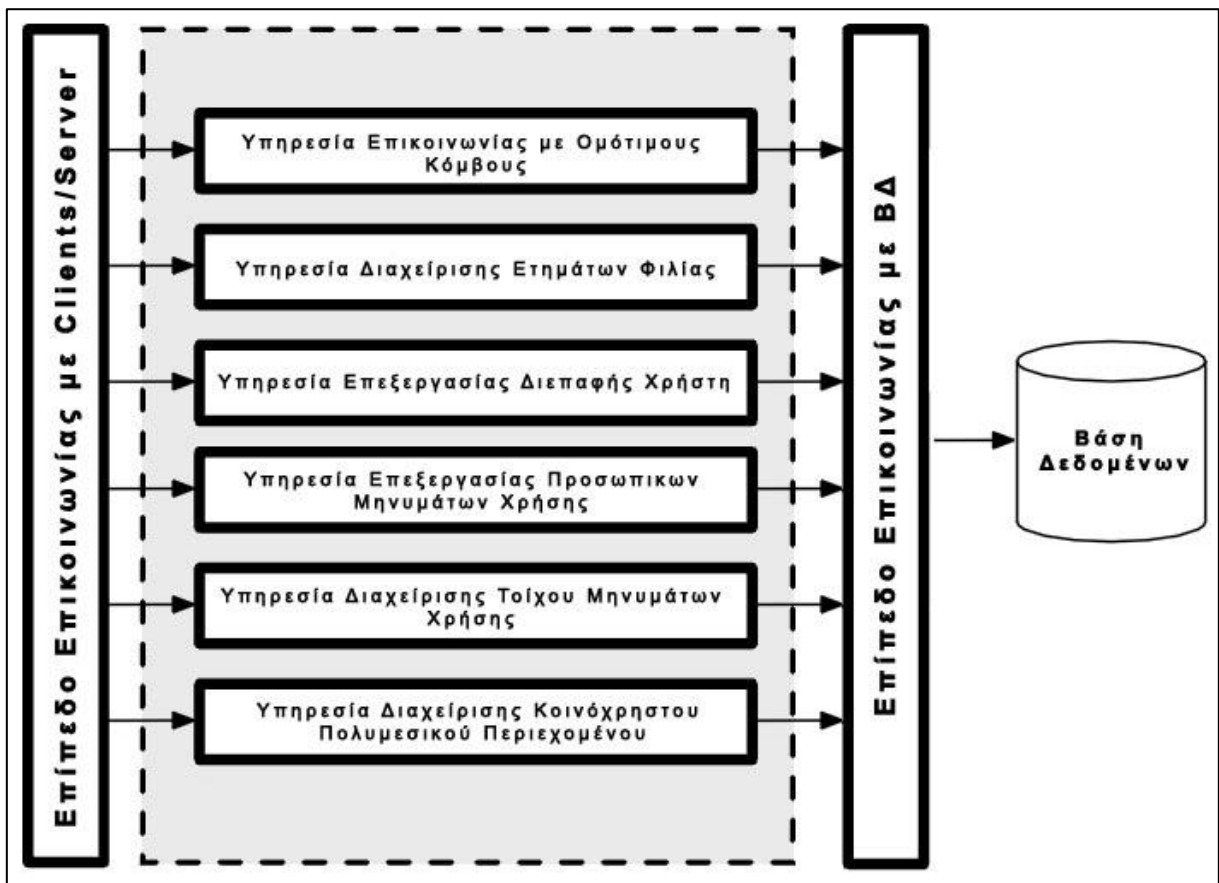
Η διαδικασία εισόδου χρήστη χρησιμοποιείται για την καταγραφή της πρόσφατης διεύθυνσης URI ή IP του χρήστη. Ο λόγος ύπαρξης αυτής η διαδικασίας στην υπηρεσία εύρεσης ομότιμων κόμβων του κατακεκομμένου κοινωνικού δικτύου μας είναι για να μπορούν να ενημερώνονται οι άλλοι χρήστες/κόμβοι του δικτύου με τα πρόσφατα στοιχεία επικοινωνίας του χρήστη και κόμβου που έχει εισέλθει στο σύστημα.

Η διαδικασία καταγραφής και αναζήτησης χρηστών και κόμβων, είναι υπεύθυνη για την λήψη αιτημάτων καταγραφής και αναζήτησης στοιχείων που αφορά κόμβους και χρήστες του δικτύου, καθώς και για την απόκριση σε αυτά τα αιτήματα εφόσον θα πιστοποιεί κάθε φορά ότι το αίτημα προέρχεται από πιστοποιημένο χρήστη του δικτύου.

Το framework του συστήματος βασίζεται στο πρότυπο MVC, μέσω του οποίου ότι οι διαδικασίες της υπηρεσίας εύρεσης ομότιμων κόμβων ελέγχονται από ελεγκτές (controllers) του συστήματος μας.

#### **4.3.2. Η Αρχιτεκτονική Frontend του Συστήματος**

Η αρχιτεκτονική του frontend του συστήματος μας, το οποίο εκτελείται στον προσωπικό εξυπηρετητή του κάθε χρήστη περιλαμβάνει τις ακόλουθες υπηρεσίες (Σχ. 4.5):



**Σχήμα 4.5:** Αρχιτεκτονική Frontend του MyPrivateSocialNetwork.

- Την υπηρεσία για την επικοινωνία με άλλους ομότιμους κόμβους στο δίκτυο και για την επικοινωνία με τον κύριο εξυπηρετητή του backend του συστήματος.
- Την υπηρεσία διαχείρισης αιτημάτων φιλίας από άλλους χρήστες. Μέσω της υπηρεσίας αυτής τα αιτήματα φιλίας του κάθε χρήστη αρχειοθετούνται στην τοπική βάση δεδομένων όπου ο κάθε χρήστης μπορεί να τα επεξεργαστεί.
- Την υπηρεσία επεξεργασίας και διαχείρισης της διεπαφής χρήστη καθώς και των θεμάτων της διεπαφής χρήστη. Μέσω αυτής της υπηρεσίας, ο κάθε χρήστης μπορεί να σχεδιάσει και υλοποιήσει το δικό του θέμα για την διεπαφή χρήστη του ιδιωτικού κοινωνικού δικτύου του.
- Την υπηρεσία επεξεργασίας προσωπικών μηνυμάτων του χρήστη. Μέσω αυτής της υπηρεσίας τα μηνύματα που αποστέλλονται από φίλους σε φίλους του κατανεμημένου κοινωνικού δικτύου, το σύστημα τα αναγνωρίζει και τα αρχειοθετεί με τέτοιο τρόπο

έτσι ώστε να έχει πρόσβαση σε αυτά μόνο ο χρήστης/φίλος παραλήπτης και όχι οι φίλοι του που έχουν περιορισμένη πρόσβαση στο προφίλ του.

- Την υπηρεσία διαχείρισης του τοίχου μηνυμάτων. Η συγκεκριμένη υπηρεσία φροντίζει να αρχειοθετεί και ταξινομεί κατάλληλα τα κοινόχρηστα μηνύματα που γράφονται στον τοίχο μηνυμάτων των χρηστών. Παρέχει την δυνατότητα στον χρήστη να απαντήσει σε ένα μήνυμα ή να το διαγράψει από τον τοίχο του.
- Την υπηρεσία διαχείρισης κοινόχρηστου πολυμεσικού περιεχομένου. Η υπηρεσία αυτή είναι υπεύθυνη για την ανάρτηση, τροποποίηση, διαγραφή, έλεγχο, αρχειοθέτηση και ορισμό δικαιωμάτων πρόσβασης στο πολυμεσικό περιεχόμενο του ιδιωτικού κοινωνικού δικτύου του κάθε χρήστη. Έτσι ο κάθε χρήστης, μέσω αυτής της υπηρεσίας, μπορεί να ελέγξει καλύτερα τα προσωπικά του πολυμεσικά αρχεία που αναρτά κάθε φορά στο ιδιωτικό του κοινωνικό δίκτυο.

Κατά την διάρκεια αιτήματος φιλίας από ένα χρήστη σε κάποιον άλλο χρήστη, τότε αρχικά το αίτημα αυτό εξυπηρετείτε από την υπηρεσία διαχείριση αιτημάτων φιλίας, η οποία ελέγχει και πιστοποιεί ότι ο χρήστης που απέστειλε το αίτημα φιλίας είναι μέλος του συνολικού καταναμημένου κοινωνικού δικτύου και δεν είναι κάποιο κακόβουλο λογισμικό. Με την αποστολή του αιτήματος αποστέλλονται στον χρήστη παραλήπτη του αιτήματος, η διεύθυνση επικοινωνίας του χρήστη που απέστειλε το αίτημα φιλίας, το port, καθώς και το όνομα χρήστη του. Έτσι, το νέο αίτημα φιλίας παρουσιάζεται στην διεπαφή του χρήστη που παρέλαβε αυτό το αίτημα. Εφόσον ο χρήστης παραλήπτης αποδεχτεί το αίτημα αυτό και ο χρήστης αποστολέας είναι πιστοποιημένος στο ιδιωτικό κοινωνικό δίκτυο του χρήστη παραλήπτη, τότε η υπηρεσία διαχείρισης επικοινωνίας αναζητά και αντλεί από τον κοινόχρηστο εξυπηρετητή του συστήματος την νέα διεύθυνση του και του αποστέλλει ένα μήνυμα αποδοχής του αιτήματος του. Τα στοιχεία του χρήστη αποστολέα εμφανίζονται στην λίστα φίλων του χρήστη που απέστειλε αρχικά το αίτημα φιλίας και πλέον οι δυο χρήστες έχουν γίνει φίλοι μεταξύ τους και ο καθένας τους έχει πρόσβαση στο κοινόχρηστο περιεχόμενο του άλλου. Επίσης, οι φίλοι μεταξύ τους μπορεί να αφήσουν μήνυμα στο τοίχο του άλλου χρήστη, καθώς και να ανταλλάξουν μεταξύ τους προσωπικά μηνύματα.

Αξίζει να σημειώσουμε εδώ ότι στην περίπτωση που ο δεύτερος χρήστης που θα δεχτεί την αποδοχή του αιτήματος φιλίας από άλλον χρήστη δεν είναι online την ίδια χρονική στιγμή που του αποστέλλεται το αίτημα αποδοχής φιλίας, τότε το μήνυμα θα εμφανίζεται στο προφίλ του

χρήστη αποστολέα με την ένδειξη «εκκρεμή». Ο χρήστης παραλήπτης θα το λάβει το μήνυμα του χρήστη αποστολέα την επομένη φορά που θα είναι και οι δυο online, καθώς και όταν ο χρήστης παραλήπτης θα επιχειρήσει να επικοινωνήσει ξανά με τον χρήστη αποστολέα.

# Κεφάλαιο 5

## Λεπτομέρειες Υλοποίησης

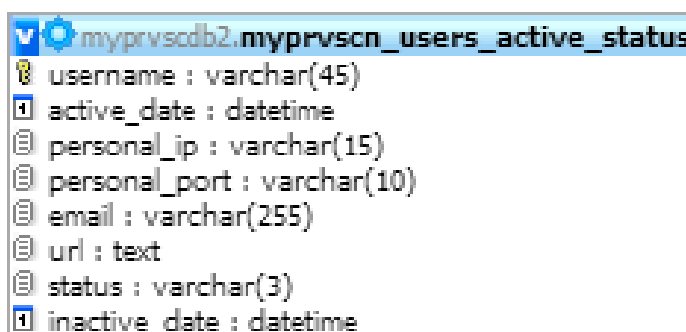
Σε αυτό το κεφάλαιο αναλύουμε την βάση δεδομένων, τις γλώσσες προγραμματισμού και μεθοδολογία που χρησιμοποιήθηκαν για την ανάπτυξη του συστήματος μας.

### 5.1 Η Υπηρεσία Διαχείρισης και Καταχώρησης Πληροφοριών

Για την ανάπτυξη της υπηρεσίας εύρεσης και καταχώρησης πληροφοριών για κάθε κόμβο του δικτύου χρησιμοποιήθηκε η αντικειμενοστραφής γλώσσα προγραμματισμού διαδικτύου PHP, για την βάση δεδομένων η MySQL, για καλύτερη διαδραστικότητα και απόκριση της διεπαφής τους συστήματος με τον χρήστη την scripting γλώσσα προγραμματισμού AJAX, καθώς και για τις υπηρεσίες ιστού, για την επικοινωνία μεταξύ του server και των clients, χρησιμοποιήθηκε το πρότυπο REST - Representational State Transfer. Έτσι, κατά την εκτέλεση μιας υπηρεσίας ιστού για την επικοινωνία του κεντρικού εξυπηρετητή του συστήματος με τους επιμέρους

εξυπηρετητές των χρηστών του συστήματος μεταφέρονται μέσω URL τα απαραίτητα στοιχεία που απαιτούνται για την εκτέλεση της. Τα δεδομένα που προκύπτουν από την εκτέλεση μιας υπηρεσίας ιστού αποθηκεύονται σε ένα αρχείο XML όπου μπορεί να προσπελαστεί και διαβαστεί από την διαδικτυακή εφαρμογή του κοινωνικού δικτύου του χρήστη. Το πρότυπο αυτό έχει υλοποιηθεί βασισμένο στο Social Engine της Elgg Foundation [20]. Επιλέξαμε το συγκεκριμένο social engine, διότι πληροί τα κριτήρια για την προσθήκη ενός ανεξάρτητου plugin, το οποίο μπορεί να συνεργάζεται με τις υπόλοιπες υπηρεσίες του συστήματος χωρίς να παρουσιάζει κάποια δυσλειτουργία στο συνολικό σύστημα.

Τα στοιχεία που αποθηκεύονται στην βάση δεδομένων του κεντρικού εξυπηρετητή του συστήματος για κάθε χρήστη είναι, η τελευταία διεύθυνση του URI, καθώς και το port επικοινωνίας, έτσι ώστε να μπορούν οι πιστοποιημένοι χρήστες να συνδέονται στο ιδιωτικό του κοινωνικό δίκτυο. Για κάθε χρήστη τα παραπάνω στοιχεία ανανεώνονται κάθε φορά που εισέρχεται στο ιδιωτικό του κοινωνικό δίκτυο ο κάθε χρήστης. Τα στοιχεία αυτά αποθηκεύονται στην βάση δεδομένων του κεντρικού εξυπηρετητή τους συστήματος κάτω από το «όνομα χρήστη» για κάθε χρήστη του συστήματος, το οποίο είναι και μοναδικό (πρωτεύων κλειδί). Αυτό σημαίνει πως δεν μπορεί να έχει το ίδιο όνομα χρήστη παραπάνω του ενός χρήστη. Οι πίνακες της βάσης δεδομένων της υπηρεσίας εύρεσης κόμβων και καταχώρησης πληροφοριών του κεντρικού εξυπηρετητή του συστήματος παρουσιάζονται στην παρακάτω εικόνα (Εικ. 5.1):



**Εικόνα 5.1:** Βάση δεδομένων της υπηρεσίας εύρεσης κόμβων και καταχώρησης πληροφοριών

Στα παραπάνω πεδία του πίνακα «myprvscn\_users\_active\_status» παρατηρούμε ότι τα βασικά στοιχεία που διατηρούνται και επανεγγράφονται στην κοινόχρηστη ως προς τους κόμβους, βάση δεδομένων του συστήματος είναι:



- Το πεδίο «username», όπου είναι μοναδικό για κάθε χρήστη του συστήματος. Δημιουργείται κατά την πρώτη εγγραφή του χρήστη στο σύστημα και δεν επανεγγράφεται.
- Το πεδίο «active\_date», όπου καταγράφεται η τελευταία ημερομηνία που έχει εισέλθει ο χρήστης στο σύστημα του.
- Το πεδίο «personal\_ip», όπου καταγράφεται η τελευταία IP διεύθυνση του χρήστη που είχε κατά την διάρκεια που εισήλθε στο σύστημα του.
- Το πεδίο «personal\_port», όπου καταγράφεται το τελευταίο port επικοινωνίας του χρήστη που είχε κατά την διάρκεια που εισήλθε στο σύστημα του. Συνήθως το port είναι σταθερό, όμως για λόγους ασφάλειας ο κάθε χρήστης θα μπορεί να το αλλάζει από τον προσωπικό του διακομιστή διαδικτύου.
- Το πεδίο «email», όπου καταγράφεται διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη, όπου την έχει δηλώσει κατά την διάρκεια της αρχικής του εγγραφής στο σύστημα.
- Το πεδίο «url», όπου καταγράφεται η διεύθυνση URL του προσωπικού εξυπηρετητή, εφόσον ο χρήστης έχει δηλώσει κάποιο domain name για το ιδιωτικό του κοινωνικό δίκτυο και έχει ενημερώσει παράλληλα τον domain registrar με τους nameservers της εταιρίας φιλοξενίας του domain name και του ιδιωτικού κοινωνικού δικτύου του.
- Το πεδίο «status», όπου καταγράφεται η κατάσταση του χρήστη αν είναι ενεργός ή όχι κατά την διάρκεια αναζήτησης του από νέους χρήστες.
- Το πεδίο «inactive\_date», όπου καταγράφεται η ημερομηνία και ώρα αποσύνδεσης του χρήστη από το σύστημα.

Για την αποφυγή προβλημάτων που μπορεί να προκύψουν κατά την διάρκεια επικοινωνίας μεταξύ δυο εξυπηρετητών του κοινωνικού δικτύου έχουμε ορίσει ως προεπιλεγμένο port, το port 80. Έτσι, ο κεντρικός εξυπηρετητής του συστήματος προσπελάσετε από τους χρήστες του δικτύου μέσω του HTTP πρωτοκόλλου. Αυτό σημαίνει ότι ο κάθε χρήστης θα πρέπει για το ιδιωτικό του κοινωνικό δίκτυο να έχει ορίσει ένα domain name, καθώς επίσης να έχει εγκαταστήσει τον προσωπικό του εξυπηρετητή (π.χ. apache web server), ο οποίος θα πρέπει να είναι συνδεδεμένος στο internet και να παρέχει την δυνατότητα προσπέλασης του στο port 80.

Τα hardware χαρακτηριστικά και το bandwidth του κεντρικού εξυπηρετητή του καταναεμημένου κοινωνικού δικτύου πρέπει να είναι υψηλών προδιαγραφών, έτσι ώστε να μπορεί να εξυπηρετεί αιτήματα πολλών χρηστών ταυτόχρονα. Οι υπηρεσίες ιστού που εκτελούνται στον κεντρικό εξυπηρετητή του συστήματος μειώνουν τον φόρτο εκτέλεσης ερωτημάτων στην κεντρική βάση δεδομένων του συστήματος, καθώς και προστατεύουν παράλληλα τα δεδομένα που είναι αποθηκευμένα σε αυτή. Επιπλέον μπορεί να επιτελέσουν και την επικοινωνία με άλλα συστήματα.

## **5.2. Το Ιδιωτικό Κοινωνικό Δίκτυο του Χρήστη**

Ο κάθε χρήστης για να μπορέσει να συμμετέχει στην κοινότητα του καταναεμημένου κοινωνικού δικτύου θα πρέπει αρχικά να εγκαταστήσει τον προσωπικό του εξυπηρετητή και στην συνέχεια να εγκαταστήσει την διαδικτυακή εφαρμογή του ιδιωτικού κοινωνικού δικτύου σε αυτόν, κάτω από ένα domain name που θα έχει προεπιλέξει. Πριν την εγκατάσταση, η εφαρμογή ελέγχει αν ο χρήστης έχει εγκαταστήσει σωστά όλες τις απαραίτητες βιβλιοθήκες του εξυπηρετητή, έτσι ώστε να μπορεί να επικοινωνήσει με τον κεντρικό εξυπηρετητή του δικτύου (Εικ. 5.2).

System check		
libCurl PHP module		(required)
GD graphics PHP module		(required)
OpenSSL PHP module		(required)
mysql PHP module		(required)
mb_string PHP module		(required)
Apache mod_rewrite module		(required)
.htconfig.php is writable		(required)
view/smarty3 is writable		(required)
Generate encryption keys		(required)

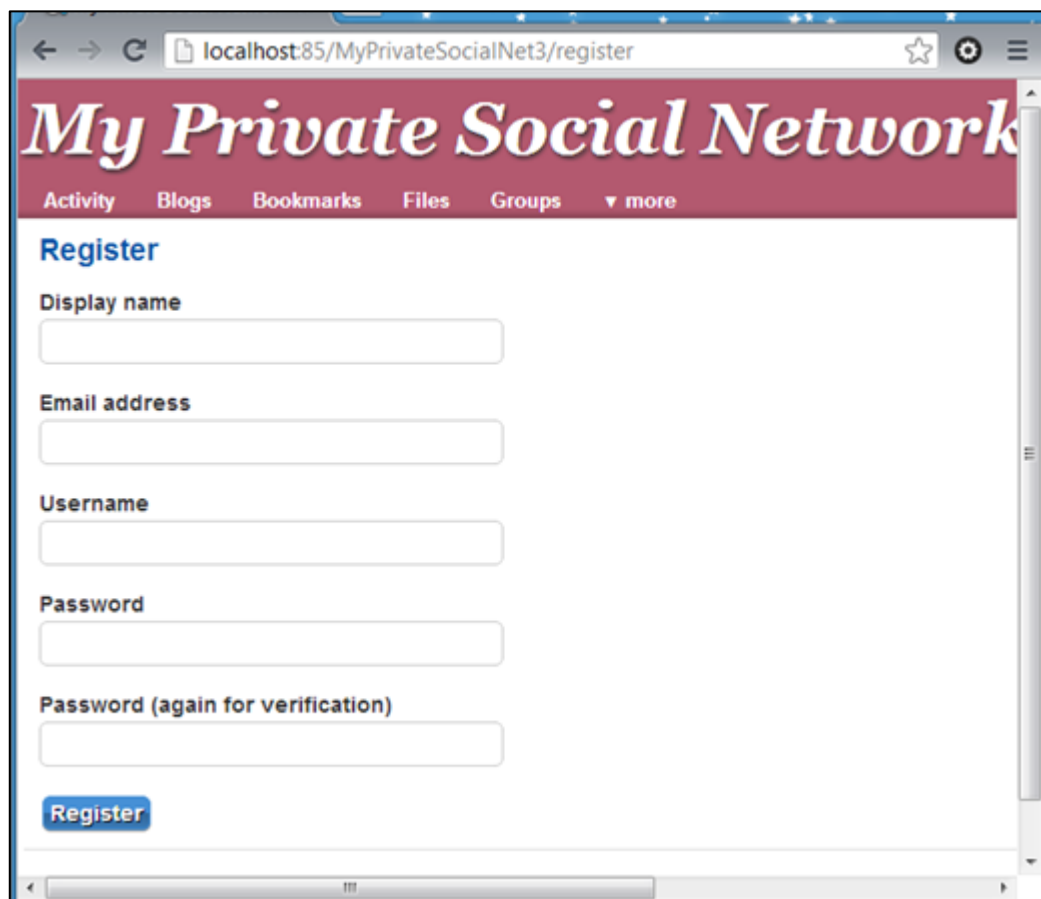
Εικόνα 5.2: Έλεγχος εγκατάστασης βιβλιοθηκών εξυπηρετητή χρήστη

Οι πίνακες της βάση δεδομένων της διαδικτυακής εφαρμογής που εκτελείται στον εξυπηρετητή του χρήστη παρουσιάζεται στην παρακάτω εικόνα (Εικ. 5.3):

Table Name	Columns
myprvsadb2.myprvsadb2_sites_entity	guid : bigint(20) unsigned, name : text, description : text, url : varchar(255)
myprvsadb2.myprvsadb2_groups_entity	guid : bigint(20) unsigned, name : text, description : text
myprvsadb2.myprvsadb2_geocode_cache	id : int(11), location : varchar(128), lat : varchar(20), long : varchar(20)
myprvsadb2.myprvsadb2_metastatings	id : int(11), string : text
myprvsadb2.myprvsadb2_metadata	id : int(11), entity_guid : bigint(20) unsigned, name_id : int(11), value_id : int(11), value_type : enum('integer','text'), owner_guid : bigint(20) unsigned, access_id : int(11), time_created : int(11), enabled : enum('yes','no')
myprvsadb2.myprvsadb2_config	name : varchar(255), value : text, site_guid : int(11)
myprvsadb2.myprvsadb2_access_collection_membership	user_guid : int(11), access_collection_id : int(11)
myprvsadb2.myprvsadb2_entities	guid : bigint(20) unsigned, type : enum('object','user','group','site'), subtype : int(11), owner_guid : bigint(20) unsigned, site_guid : bigint(20) unsigned, container_guid : bigint(20) unsigned, access_id : int(11), time_created : int(11), time_updated : int(11), last_action : int(11), enabled : enum('yes','no')
myprvsadb2.myprvsadb2_objects_entity	guid : bigint(20) unsigned, title : text, description : text
myprvsadb2.myprvsadb2_private_settings	id : int(11), entity_guid : int(11), name : varchar(128), value : text
myprvsadb2.myprvsadb2_users_entity	guid : bigint(20) unsigned, name : text, username : varchar(128), password : varchar(32), salt : varchar(8), email : text, language : varchar(6), code : varchar(32), banned : enum('yes','no'), admin : enum('yes','no'), last_action : int(11), prev_last_action : int(11), last_login : int(11), prev_last_login : int(11)
myprvsadb2.myprvsadb2_users_sessions	session : varchar(255), ts : int(11) unsigned, data : mediumblob
myprvsadb2.myprvsadb2_users_apisections	id : int(11), user_guid : bigint(20) unsigned, site_guid : bigint(20) unsigned, token : varchar(40), expires : int(11)
myprvsadb2.myprvsadb2_hmac_cache	hmac : varchar(255), ts : int(11)
myprvsadb2.myprvsadb2_entity_subtypes	id : int(11), type : enum('object','user','group','site'), subtype : varchar(50), class : varchar(50)
myprvsadb2.myprvsadb2_annotations	id : int(11), entity_guid : bigint(20) unsigned, name_id : int(11), value_id : int(11), value_type : enum('integer','text'), owner_guid : bigint(20) unsigned, access_id : int(11), time_created : int(11), enabled : enum('yes','no')
myprvsadb2.myprvsadb2_system_log	id : int(11), object_id : int(11), object_class : varchar(50), object_type : varchar(50), object_subtype : varchar(50), event : varchar(50), performed_by_guid : int(11), owner_guid : int(11), access_id : int(11), enabled : enum('yes','no'), time_created : int(11)
myprvsadb2.myprvsadb2_river	id : int(11), type : varchar(8), subtype : varchar(32), action_type : varchar(32), access_id : int(11), view : text, subject_guid : int(11), object_guid : int(11), annotation_id : int(11), posted : int(11)
myprvsadb2.myprvsadb2_access_collections	id : int(11), name : text, owner_guid : bigint(20) unsigned, site_guid : bigint(20) unsigned
myprvsadb2.myprvsadb2_api_users	id : int(11), site_guid : bigint(20) unsigned, api_key : varchar(40), secret : varchar(40), active : int(1)
myprvsadb2.myprvsadb2_entity_relationships	id : int(11), guid_one : bigint(20) unsigned, relationship : varchar(50), guid_two : bigint(20) unsigned, time_created : int(11)
myprvsadb2.myprvsadb2_users_active_status	username : varchar(45), active_date : datetime, personal_ip : varchar(15), personal_port : varchar(10), email : varchar(255), url : text, status : varchar(3), inactive_date : datetime

Εικόνα 5.3: Βάση δεδομένων κοινωνικού δικτύου χρήστη

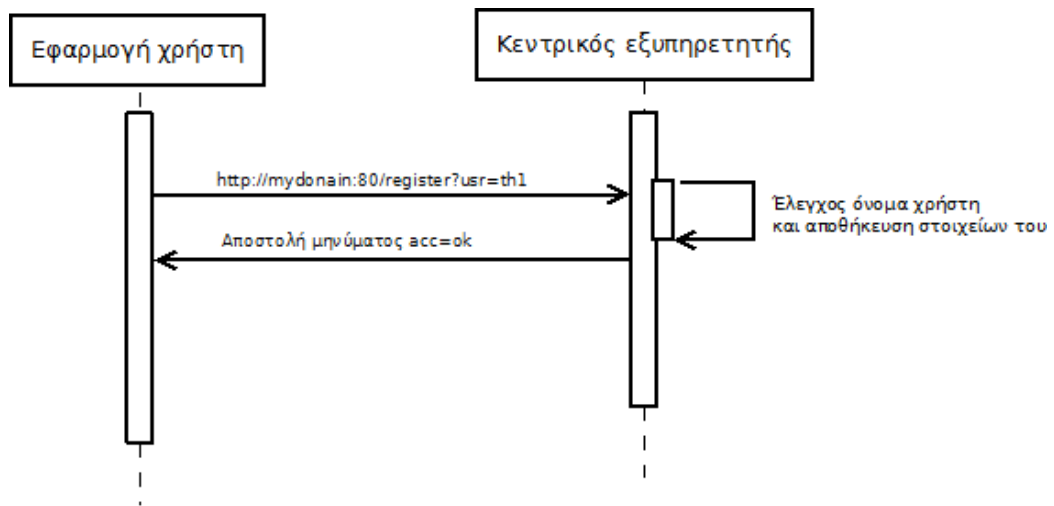
Κατά την διάρκεια της εγκατάστασης του ιδιωτικού κοινωνικού δικτύου, μέσω ενός φιλομετρητή, η εφαρμογή θα προτρέψει τον χρήστη να συμπληρώσει μια φόρμα εγγραφής με τα στοιχεία του, ο οποίος θα είναι παράλληλα και ο διαχειριστής του κοινωνικού δικτύου του (Εικ. 5.4).



The image shows a web browser window with the address bar displaying 'localhost:85/MyPrivateSocialNet3/register'. The page title is 'My Private Social Network'. Below the title is a navigation menu with links for 'Activity', 'Blogs', 'Bookmarks', 'Files', 'Groups', and a 'more' dropdown. The main content area is titled 'Register' and contains a registration form with the following fields: 'Display name', 'Email address', 'Username', 'Password', and 'Password (again for verification)'. A blue 'Register' button is located at the bottom of the form.

**Εικόνα 5.4:** Εγγραφή χρήστη στο ιδιωτικό κοινωνικό δίκτυο

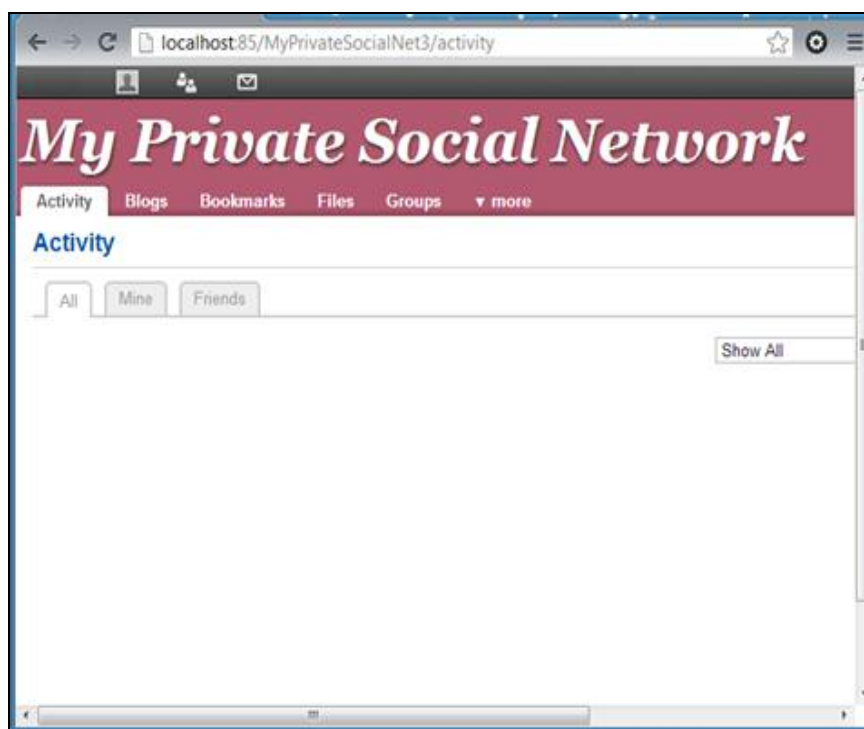
Κατά την διάρκεια της ολοκλήρωσης της εγγραφής του χρήστη η διαδικτυακή client εφαρμογή επικοινωνεί με τον κεντρικό εξυπηρετητή του συστήματος και αποθηκεύει στην κεντρική βάση δεδομένων, τα στοιχεία του χρήστη, καθώς και την διεύθυνση URL και το port του κοινωνικού δικτύου του. Έτσι, το διάγραμμα ακολουθίας που δείχνει αυτήν την επικοινωνία, παρουσιάζεται στο παρακάτω σχήμα (Σχ. 5.1):



**Σχήμα 5.1:** Διάγραμμα ακολουθίας επικοινωνίας εφαρμογής χρήστη με κεντρικό εξυπηρετητή

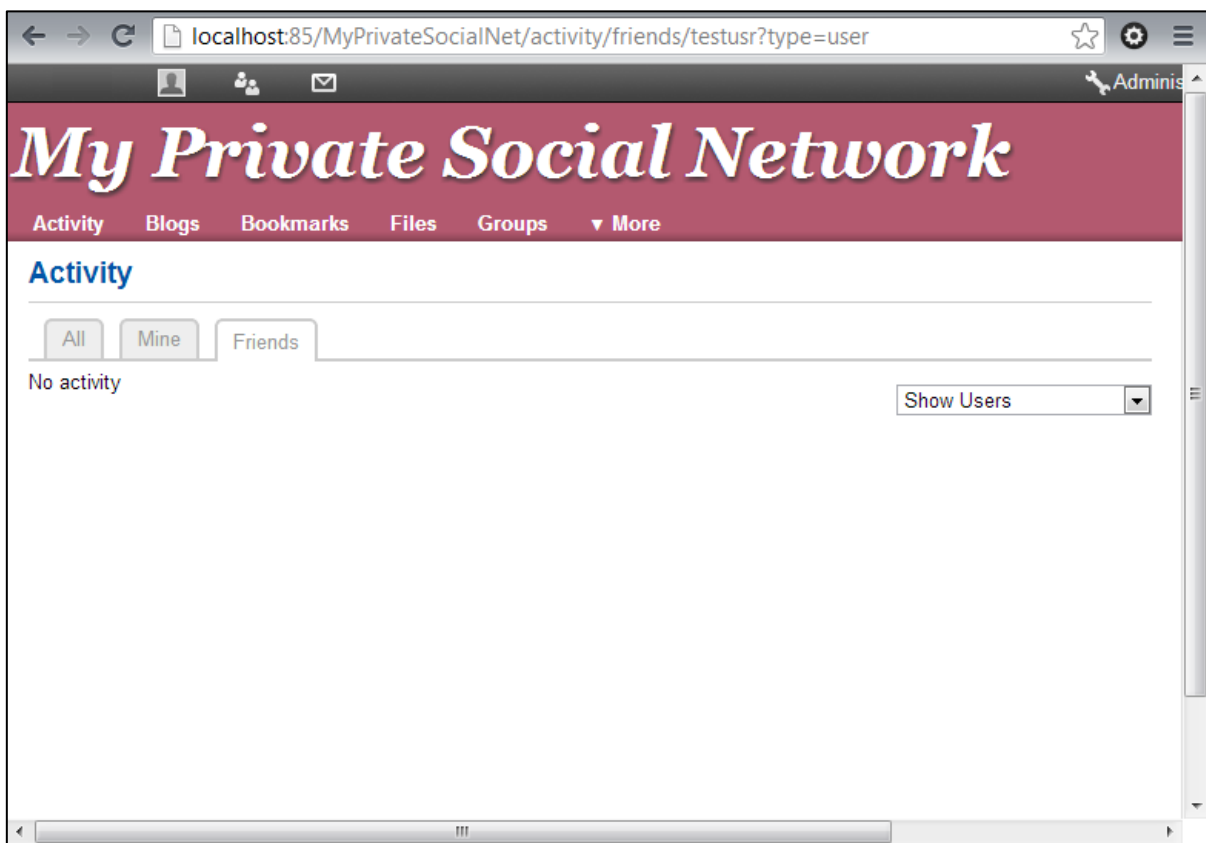
Εφόσον η εγγραφή του χρήστη ολοκληρωθεί στο σύστημα, τότε στον χρήστη παρέχετε η δυνατότητα να αναζητήσει φίλους ή να λάβει αιτήματα φιλίας από άλλους χρήστες του κατακευμαμένου κοινωνικού δικτύου.

Το αρχικό προφίλ χρήστη παρουσιάζεται στην παρακάτω εικόνα (Εικ. 5.5):



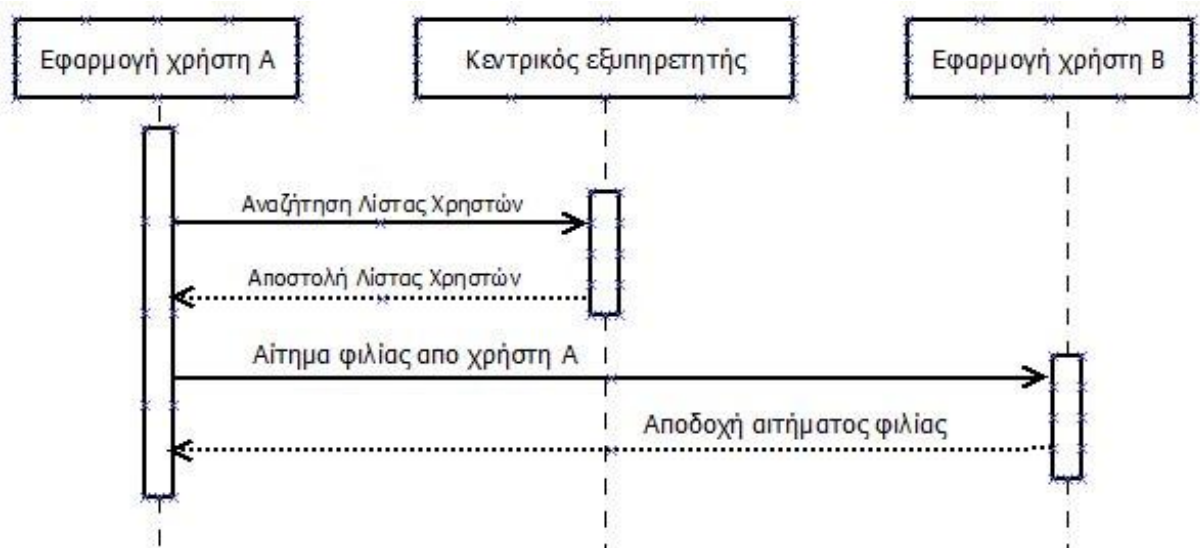
**Εικόνα 5.5:** Αρχικό προφίλ χρήστη

Ο χρήστης μέσα από την διεπαφή του προφίλ του μπορεί να επιλέξει να αναζητήσει νέους φίλους. Τότε η διαδικτυακή εφαρμογή του κοινωνικού του δικτύου συνδέεται με τον κεντρικό εξυπηρετητή και αντλεί από εκεί μια λίστα με τα ονόματα των χρηστών. Η διεπαφή αυτή παρουσιάζεται στο παρακάτω (Εικ. 5.6):



**Εικόνα 5.6:** Διεπαφή χρήστη αναζήτησης φίλων

Οι διεργασίες που εκτελούνται κατά την εκτέλεση της αναζήτησης φίλων από τον χρήστη καθώς και η αποστολή αιτήματος φιλίας από τον χρήστη προς κάποιον άλλο χρήστη του κατακευματισμένου κοινωνικού δικτύου παρουσιάζεται στο παρακάτω διάγραμμα ακολουθίας (Σχ. 5.2). Η αποδοχή μηνύματος φιλίας από τον χρήστη, σημαίνει ότι στην προσωπική του βάση δεδομένων και συγκεκριμένα στον πίνακα «myprivscn\_users\_active\_status» θα αποθηκευτούν τα στοιχεία επικοινωνίας του φίλου του. Τα στοιχεία αυτά θα ενημερώνονται κάθε φορά που θα εισέρχεται ο χρήστης στο προσωπικό του κοινωνικό δίκτυο από την κεντρική βάση δεδομένων του κατακευματισμένου κοινωνικού δικτύου. Πλέον η πιστοποίηση των δυο φίλων στα μεταξύ τους κοινωνικά δίκτυα για την εκτέλεση υπηρεσιών ιστού REST θα επιτυγχάνεται με την χρήση της βιβλιοθήκης OAuth [21, 22] που υποστηρίζει το Social Engine της Elgg Foundation [20] του κοινωνικού δικτύου.



**Σχήμα 5.2:** Διάγραμμα ακολουθίας αναζήτησης φίλων και αποστολή αιτήματος φιλίας

### 5.2.1. Το Πρωτόκολλο OAuth

Το πρωτόκολλο OAuth – Open Authentication [21, 22] είναι ένα ανοιχτό πρωτόκολλο επικοινωνίας που χρησιμοποιείτε για την επικοινωνία μεταξύ δυο ανεξάρτητων εφαρμογών. Μια από τις βασικές υπηρεσίες που προσφέρει το πρωτόκολλο OAuth είναι ότι, παρέχει την δυνατότητα στους χρήστες να μοιράζονται προσωπικά αρχεία που βρίσκονται αποθηκευμένα διαφορετικές διαδικτυακές εφαρμογές, χωρίς να απαιτείται κάθε φορά από τους χρήστες να πληκτρολογούν τα στοιχεία πρόσβασης για να συνδεθούν σε αυτές.

### 5.2.2. Η Υπηρεσία Διασύνδεσης των Ιδιωτικών Κοινωνικών Δικτύων

Παρακάτω παρουσιάζουμε ένα παράδειγμα εκτέλεσης της υπηρεσίας που υλοποιήσαμε, μέσω της οποίας επιτυγχάνεται η επικοινωνία μεταξύ των δυο ιδιωτικών κοινωνικών δικτύων. Η σχεδίαση και υλοποίηση της υπηρεσίας μας βασίστηκε στις ιδιότητες που παρέχει το πρωτόκολλο OAuth. Συγκεκριμένα, έχουμε εγκαταστήσει δυο ίδιες πλατφόρμες του κοινωνικού μας δικτύου “MyPrivateSocialNetwork” σε δυο διαφορετικούς εξυπηρετητές διαδικτύου με τις ακόλουθες διευθύνσεις URLs: <http://10.0.101.19:85/MyPSNet1>, το οποίο για λόγους διευκόλυνσης το ονομάσαμε «Δίκτυο-1» και <http://10.0.101.15:85/MyPSNet2> ως «Δίκτυο-2». Αρχικά δημιουργούμε ένα κουπόνι (token key) στο Δίκτυο-2 (Εικ. 5.7) που θα χρησιμοποιηθεί για την πιστοποίηση του στο Δίκτυο-1.



**Εικόνα 5.7:** Δημιουργία νέου κουπονιού (token key) στο Δίκτυο-2.

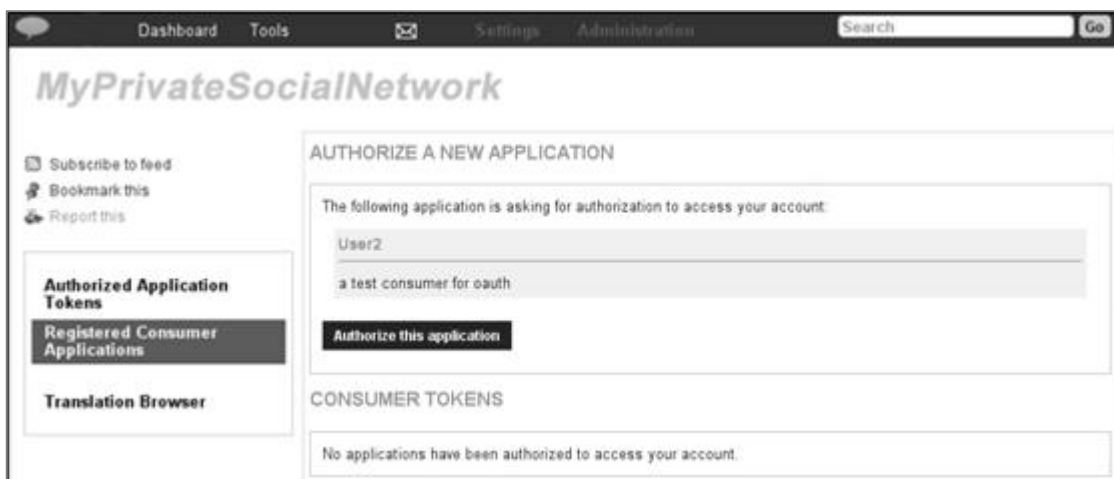
Στη συνέχεια προσθέτουμε στην υπηρεσία OAuth του Δικτύου-1 το κουπόνι που δημιουργήθηκε στο Δίκτυο-2 και προσπελάζουμε την URL διεύθυνση του Δικτύου-1: <http://10.0.101.19:85/MyPSNet1/mod/testoauth/myconoauth.php>, όπου παράγεται ένα νέο κουπόνι όπως παρουσιάζεται στην παρακάτω εικόνα (Εικ. 5.8).



**Εικόνα 5.8:** Δημιουργία νέου κουπονιού (token key) στο Δίκτυο-1.

Μετά την εκτέλεση της παραπάνω ενέργειας, στο Δίκτυο-2 εμφανίζεται ένα μήνυμα όπου ενημερώνει τον χρήστη ότι το Δίκτυο-1 προσπαθεί να συνδεθεί με το Δίκτυο-2 και απαιτεί εξουσιοδότηση από τον χρήστη του Δικτύου-2 (Εικ. 5.9).





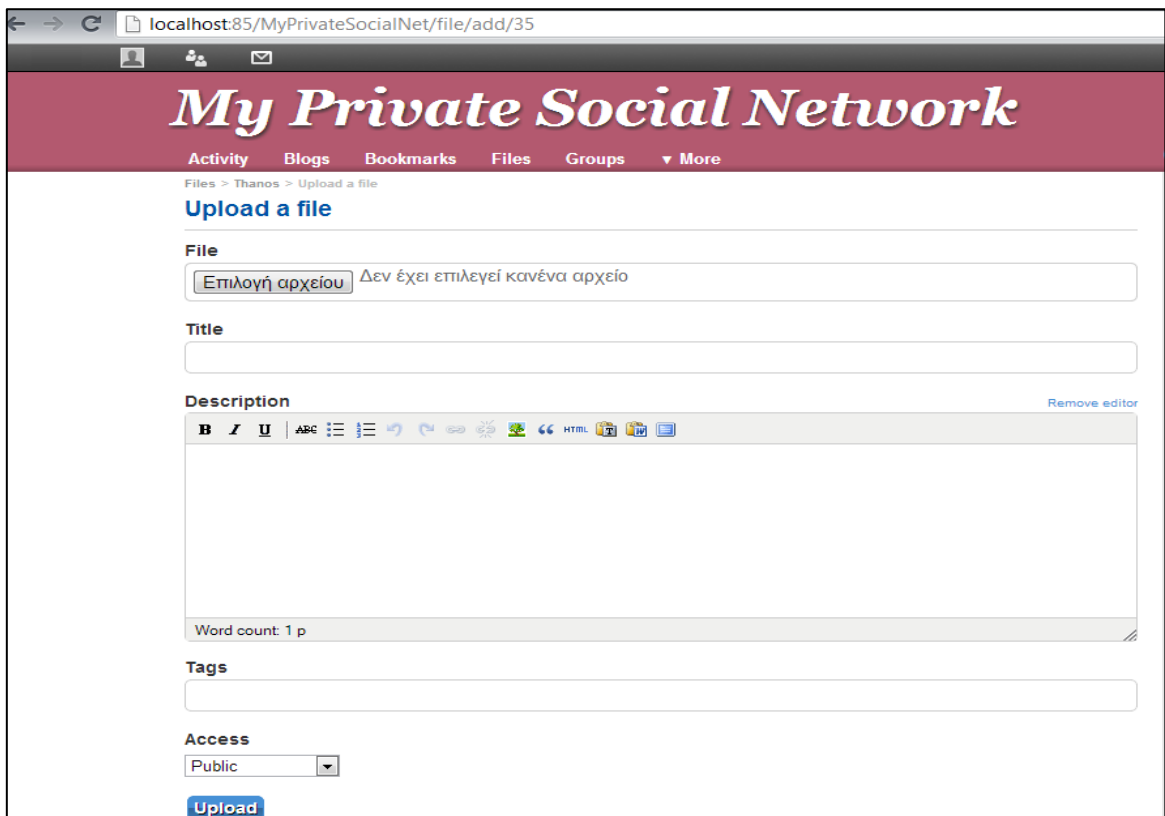
**Εικόνα 5.9:** Αίτημα εξουσιοδότησης στο Δίκτυο-2.

Ο χρήστης του Δικτύου-2 εξουσιοδοτεί την σύνδεση με το Δίκτυο-1 και πιο συγκεκριμένα τον χρήστη «User2» του Δικτύου-1, όπου πλέον ο χρήστης του Δικτυου-1 μπορεί να προσθέτει μηνύματα και να προσπελάζει αρχεία του Δικτύου-2.

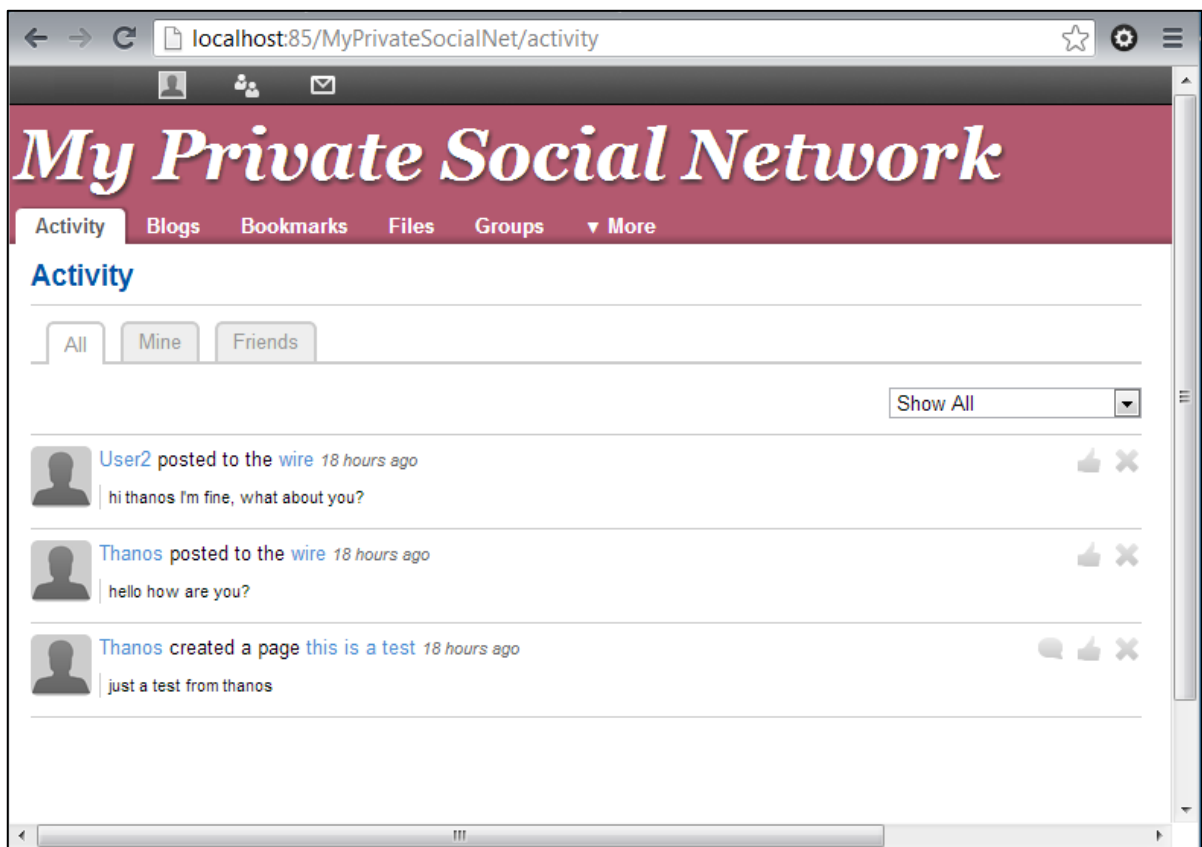
### **5.2.3. Η Διεπαφή Χρήστη των Υπηρεσιών του Ιδιωτικού Κοινωνικού Δικτύου**

Ο χρήστης μέσα από την διεπαφή του κοινωνικού δικτύου του, μπορεί με εύκολο τρόπο να ομαδοποιήσει τους φίλους σε ομάδες της επιλογής του, να αναρτήσει αρχεία και να ορίσει τα αντίστοιχα δικαιώματα ανά ομάδα χρηστών (Εικ. 5.10). Επιπλέον, μπορεί να λάβει και να απαντήσει σε μηνύματα φίλων (Εικ. 5.11), να στείλει αιτήματα φιλίας σε άλλους χρήστες (Εικ. 5.12), να αποδέχεται αιτήματα φιλίας (Εικ. 5.13), να ενημερώνεται για την πορεία των αιτήσεων φιλίας από και προς αυτόν (Εικ. 5.14), καθώς και να προβάλει την λίστα με τους φίλους του (Εικ. 5.15).

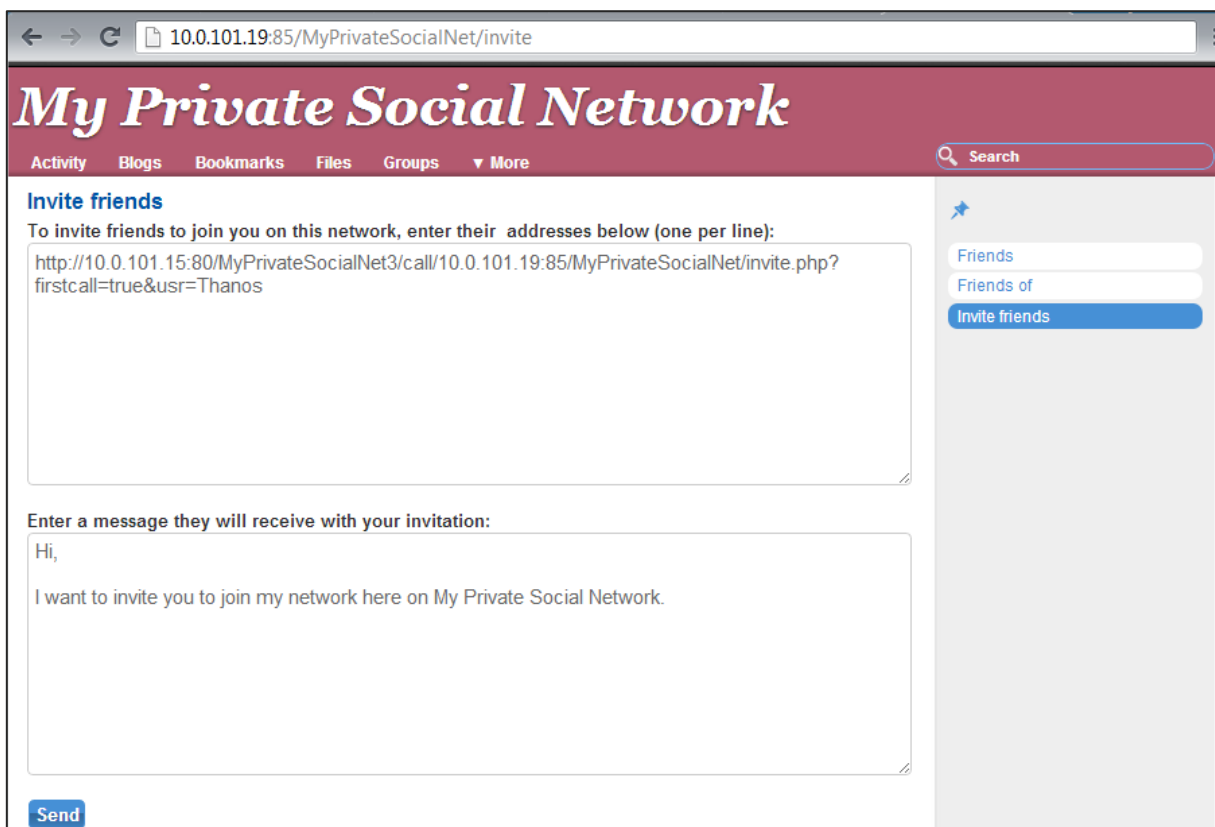
Ακολουθούν οι αντίστοιχες εικόνες των υπηρεσιών που αναφέρθηκαν παραπάνω:



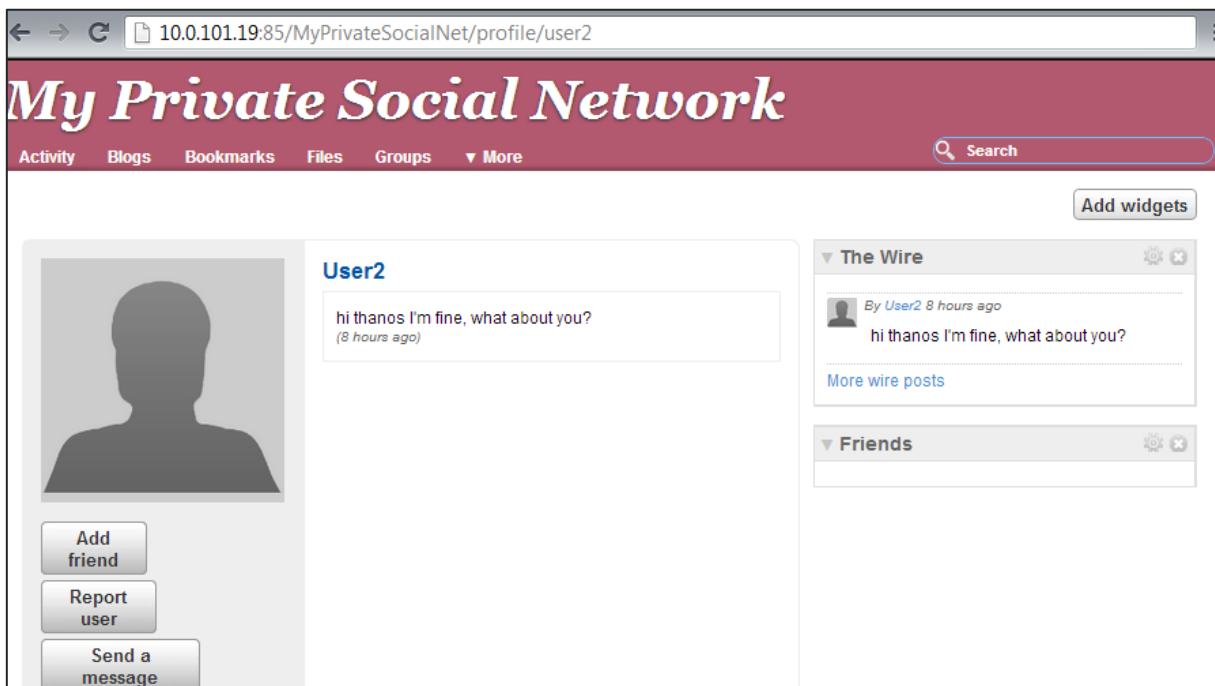
Εικόνα 5.10: Ανάρτηση αρχείων χρήστη στο κοινωνικό του δίκτυο



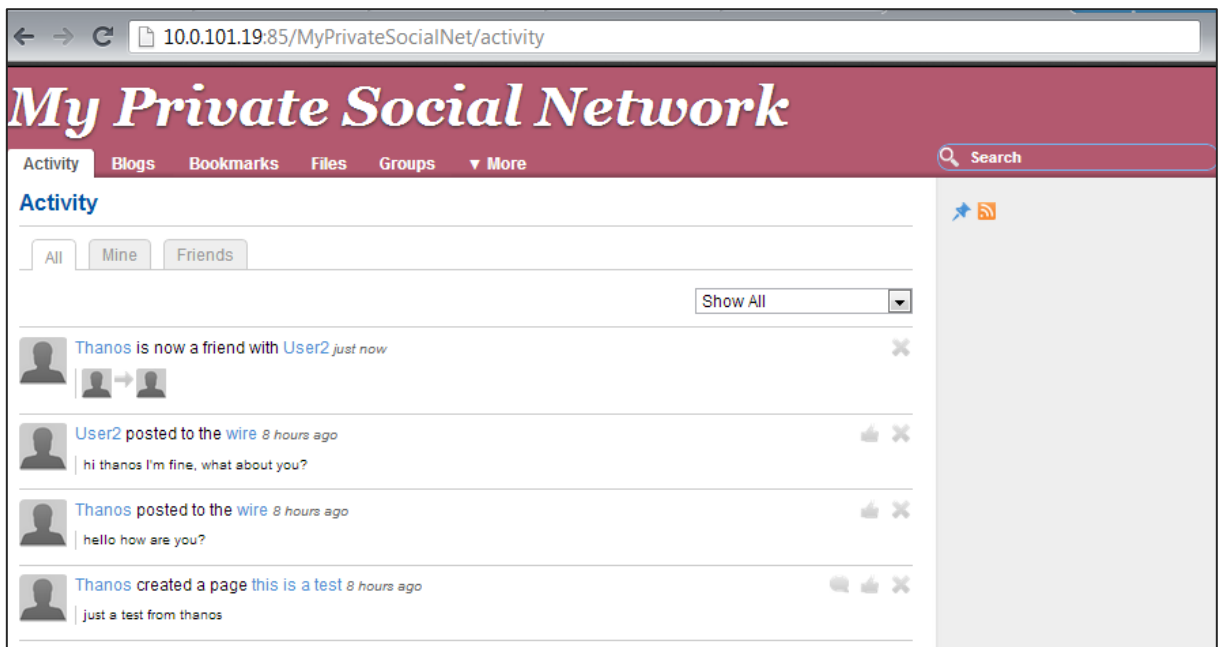
Εικόνα 5.11: Λείψει και αποστολή μηνυμάτων χρήστη σε φίλους



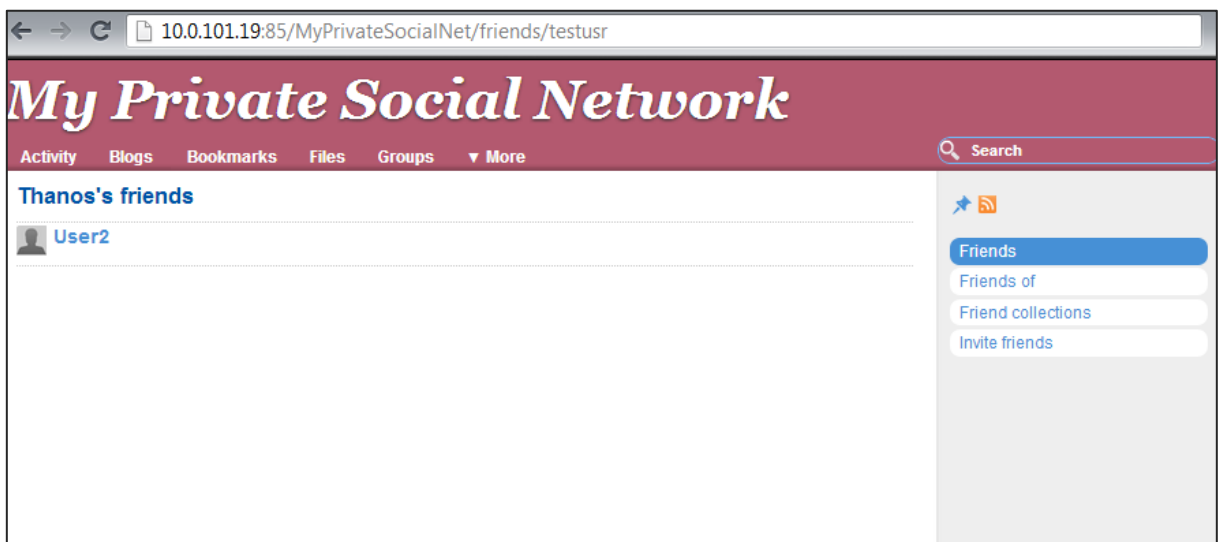
Εικόνα 5.12: Αποστολή καλέσματος φιλίας από χρήστη σε χρήστη



Εικόνα 5.13: Αποδοχή αιτήματος καλέσματος φιλίας από χρήστη σε χρήστη



Εικόνα 5.14.: Ενημέρωση κατάστασης αιτημάτων φιλίας από χρήστη σε χρήστη



Εικόνα 5.15.: Προβολή λίστας φίλων ενός χρήστη

# **Κεφάλαιο 6**

## **Συμπεράσματα και Μελλοντική Έρευνα**

Στο κεφάλαιο αυτό, γίνεται μια σύντομη ανασκόπηση των συμπερασμάτων που οδηγηθήκαμε από την τρέχουσα διπλωματική εργασία. Επίσης, περιγράφουμε εν συντομία την μελλοντική έρευνα που μπορεί να γίνει για την επίτευξη καλύτερης σχεδίασης και ανάπτυξης ενός καταναμημένου κοινωνικού δικτύου.

## 6.1 Συμπεράσματα

Σε αυτήν την διπλωματική εργασία προσπαθήσαμε να εντοπίσουμε τις τεχνολογίες και αρχιτεκτονικές που έχουν προταθεί μέχρι σήμερα για την σχεδίαση και ανάπτυξη ενός κατακευμημένου κοινωνικού δικτύου. Μελετήσαμε έξι από τα βασικότερα και σημαντικότερα πρότυπα κατακευμημένων κοινωνικών δικτύων. Μέσα από τις αρχιτεκτονικές που έχουν χρησιμοποιηθεί σε αυτά τα κατακευμημένα κοινωνικά δίκτυα, εντοπίσαμε τα υπέρ και τα κατά τους. Έτσι, επιλέξαμε να χρησιμοποιήσουμε την βέλτιστη από αυτές τις αρχιτεκτονικές, για την σχεδίαση του δικού μας κατακευμημένου κοινωνικού δικτύου.

Μέχρι σήμερα περά από το κατακευμημένο κοινωνικό δίκτυο Diaspora, κανένα άλλο κατακευμημένο κοινωνικό δίκτυο δεν έχει αναπτυχθεί σε τέτοιο βαθμό που να μπορεί να χρησιμοποιείται από απλούς χρήστες, καθώς και να αντιμετωπίζει κατάλληλα τους περιορισμούς που προβάλλει η διασύνδεση P2P. Η έως σήμερα τεχνολογία και τα πρωτόκολλα που έχουν αναπτυχθεί για διασυνδέσεις P2P δεν ικανοποιούν πλήρως τις σημερινές απαιτήσεις ενός κατακευμημένου κοινωνικού δικτύου. Πολλές ομάδες ερευνητών ασχολούνται με την σχεδίαση και ανάπτυξη κατακευμημένων κοινωνικών δικτύων, όμως η έρευνα τους εξακολουθεί να βρίσκεται σε ερευνητικό στάδιο. Στην παρούσα διπλωματική εργασία κάναμε μια προσπάθεια να αναδείξουμε τα προβλήματα που εμφανίζονται σε διασυνδέσεις P2P, καθώς και να σχεδιάσουμε και να αναπτύξουμε μια διαφορετική προσέγγιση ενός κατακευμημένου κοινωνικού δικτύου που να μην συμπίπτει άμεσα στους περιορισμούς των αρχιτεκτονικών και πρωτοκόλλων των διασυνδέσεων P2P.

Έτσι, επιλέξαμε για κάθε χρήστη του κατακευμημένου κοινωνικού δικτύου μας, να έχει τον προσωπικό του εξυπηρετητή και το δικό του domain name (URI), ώστε να εντοπίζεται και να προσπελάζεται πιο εύκολα και γρήγορα από ομότιμους εξυπηρετητές του κατακευμημένου κοινωνικού δικτύου μας. Τον ρόλο του συντονιστή μεταξύ των προσωπικών εξυπηρετητών των χρηστών, τον αναπαριστά ένας κεντρικός εξυπηρετητής του κατακευμημένου κοινωνικού δικτύου, ο οποίος καταγράφει τα βασικά στοιχεία επικοινωνίας μεταξύ των χρηστών, καθώς και τους ενημερώνει για τις πιθανές αλλαγές αυτών των στοιχείων.

Για έναν απλό χρήστη και αυτό το πρότυπο θεωρείτε δύσκολο να υιοθετηθεί μιας και απαιτεί από αυτόν να έχει προχωρημένες γνώσεις πληροφορικής για την εγκατάσταση και ρύθμιση του κοινωνικού δικτύου. Παρόλα αυτά, θεωρούμε ότι, το δίκτυο αυτό μπορεί να εξυπηρετήσει

περισσότερα ταυτόχρονα αιτήματα φιλίας μεταξύ των χρηστών του, χωρίς να «καταρρεύσει» το συνολικό δίκτυο.

## 6.2 Μελλοντική Έρευνα

Η αρχιτεκτονική του κοινωνικού δικτύου που σχεδιάσαμε και αναπτύξαμε έχει την δυνατότητα να επεκταθεί με περισσότερες λειτουργίες στοχεύοντας στην βελτίωση της επικοινωνίας και της συνεργασίας των χρηστών και την αύξηση της ασφάλειας και ιδιωτικότητας των δεδομένων τους. Σίγουρα μια προσέγγιση της συγκεκριμένης πρότασης της διπλωματικής, που θα πρέπει να ερευνηθεί, είναι η χρήση μιας κοινής πλατφόρμας κοινωνικής δικτύωσης και η αποθήκευση των δεδομένων των χρηστών σε clouds προσωπικούς εξυπηρετητές.

Επίσης, τον ρόλο του κεντρικού εξυπηρετητή στο κατακεκομμένο κοινωνικό μας δίκτυο, κάλλιστα θα μπορούσε να τον αναλάβει και το OpenID, το οποίο παρέχει έναν εύκολο και αξιόπιστο τρόπο ταυτοποίησης του χρήστη μέσω της μοναδικής ψηφιακής ταυτότητας που παράγει για κάθε έναν από αυτούς.

Όσο αφορά την αυξημένη ασφάλεια στην επικοινωνία των χρηστών μεταξύ τους, θα μπορούσαν να χρησιμοποιηθούν κλειδιά κρυπτογράφησης δεδομένων σε κάθε ανταλλαγή δεδομένων που κάνουν οι χρήστες του δικτύου μεταξύ τους.

Τέλος, μια άλλη ερευνητική διαφορετική προσέγγιση του θέματος αυτού είναι η συνολική χρήση των πρωτοκόλλων άμεσης επικοινωνίας XMPP, τα οποία στηρίζονται στην γλώσσα σήμανσης XML και μπορούν να επιτύχουν καλύτερη και ασφαλέστερη επικοινωνία μεταξύ των προσωπικών εξυπηρετητών των χρηστών.

## Βιβλιογραφία

- [01] Wikipedia - [http://el.wikipedia.org/wiki/Web\\_2.0](http://el.wikipedia.org/wiki/Web_2.0)
- [02] Wikipedia - [http://en.wikipedia.org/wiki/Web\\_2.0](http://en.wikipedia.org/wiki/Web_2.0)
- [03] Wikipedia - <http://en.wikipedia.org/wiki/Peer-to-peer>
- [04] Anwitaman Datta. Tutorial: Peer-to-Peer Storage Systems: Crowdsourcing the storage cloud. At ICDCN 2010, Kolkata, India.
- [05] Sonja Buchegger , Doris Schiöberg , Le-hung Vu , Anwitaman Datta. «PeerSoN: P2P social networking – early experiences and insights». ACM Workshop on Social Network Systems 2009.
- [06] Dave Winer – What is P2P. <http://scripting.com/davenet/2000/09/20/whatIsP2p.html>
- [07] Doris Schiöberg: A peer-to-peer infrastructure for Social Networks, 2008.
- [08] [http://en.wikipedia.org/wiki/Ilya\\_Zhitomirskiy](http://en.wikipedia.org/wiki/Ilya_Zhitomirskiy)
- [09] <http://diasporial.com/whats-diaspora>
- [10] [http://en.wikipedia.org/wiki/Diaspora\\_\(social\\_network\)](http://en.wikipedia.org/wiki/Diaspora_(social_network))
- [11] <https://github.com/diaspora/diaspora/wiki/An-Introduction-to-the-Diaspora-Source>
- [12] <http://developers.facebook.com/docs/>
- [13] <https://dev.twitter.com/docs>
- [14] <http://developer.linkedin.com/documents/profile-api>
- [15] Social Networking and Ethics - <http://plato.stanford.edu/entries/ethics-social-networking/>



- [16] Gunnar Kreitz, Oleksandr Bodriagov, Benjamin Greschbach, Guillermo Rodríguez-Cano, and Sonja Buchegger: Passwords in Peer-to-Peer, IEEE P2P, Tarragona Spain 2012.
- [17] Golbeck, J., Parsia, B. Hendler, J. Trust networks on the Semantic Web. Proceedings of cooperative intelligent agents. 2003.
- [18] <http://digitaljournal.com/image/77313>
- [19] <http://curl.haxx.se/docs/httpscripting.html>
- [20] [http://docs.elgg.org/wiki/Getting\\_Started\\_With\\_Developmentel](http://docs.elgg.org/wiki/Getting_Started_With_Developmentel)
- [21] <http://en.wikipedia.org/wiki/OAuth>
- [22] <http://tools.ietf.org/html/rfc6749>
- [23] <http://www.opendht.org/>
- [24] <http://www.bamboo-dht.org/>
- [25] Sean Rhea, Dennis Geels, Timothy Roscoe, John Kubiawicz: Handling Churn in a DHT. In: Proceedings of the USENIX Annual Technical Conference, June 2004.
- [26] Seok-Won Seong, Jiwon Seo, Matthew Nasielski, Debansu Sengupta, Sudheendra Hangal, Seng Keat Teh, Ruven Chu, Ben Dodson, Monica S. Lam: PrPl: a decentralized social networking infrastructure, Stanford, CA 94305.
- [27] Kalman Graffi, Christian Gross, Dominik Stingl, Daniel Hartung, Aleksandra Kovacevic, and Ralf Steinmetz, LifeSocial.KOM: A Secure and P2P-based Solution for Online Social Networks, IEEE CCNC January 2011.
- [28] Freepastry, <http://www.freepastry.org/FreePastry/>.
- [29] A. I. T. Rowstron and P. Druschel, Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems, in Proc. of IFIP/ACM Middleware, 2001.

- [30] P. Druschel, PAST: A Large-Scale, Persistent Peer-to-Peer Storage Utility, in Proc. of HotOS, 2001.
- [31] D. N. Kalofonos, Z. Antoniou, F. D. Reynolds, M. Van-Kleek, J. Strauss, and P. Wisner, MyNet: a Platform for Secure P2P Personal and Social Networking Services, PerCom 2008.
- [32] Γεώργιος Σταματελάτος, Γεώργιος Δροσάτος, Παύλος Εφραμίδης, Quantum: Ένα Δίκτυο Ομότιμων Κόμβων για Κατανεμημένους Υπολογισμούς με Ενισχυμένη Ιδιωτικότητα.
- [33] <http://www.peerscape.org>
- [34] Jan Sacha: Exploiting Heterogeneity in Peer-to-Peer Systems Using Gradient Topologies, University of Dublin, Trinity College, July 2009.
- [35] <http://www.xmpp.org>
- [36] [http://el.wikipedia.org/wiki/Extensible\\_Messaging\\_and\\_Presence\\_Protocol](http://el.wikipedia.org/wiki/Extensible_Messaging_and_Presence_Protocol)

# Ακρωνύμια και Συντομογραφίες

**OSN** - Online Social Network

**P2P** - Peer-to-Peer

**RPC** - Remote Procedure Call

**SHA -1** - Cryptographic Hash Function

**SMTP** - Simple Mail Transfer Protocol

**SN** - Social Network

**DHT** - Distributed Hash Table

**DNS** - Domain Name System

**JSON** - JavaScript Object Notation

**REST** - Representational State Transfer

**OAuth** – Open Authentication

**XMPP** - Xtensible Messaging and Presence Protocol

**SASL** - Simple Authentication and Security Layer

**TLS** - Transport Layer Security

**XEP** - XMPP Extension Protocols

**ISP** - Internet Service Provider

# Παράρτημα Α

## A.1 Ενδεικτικός Κώδικας Συστήματος

### Webservices μηνυμάτων

```
function rest_wire_post($username, $text) {
    $user = get_user_by_username($username);
    if (!$user) {
        throw new InvalidParameterException('Bad username');
    }

    $obj = new Object();
    $obj->subtype = 'thewire';
    $obj->owner_guid = $user->guid;
    $obj->access_id = ACCESS_PUBLIC;
    $obj->method = 'api';
    $obj->description = elgg_substr(strip_tags($text), 0, 140);

    $guid = $obj->save();

    add_to_river('river/object/thewire/create',
                'create',
                $user->guid,
                $obj->guid
```

```

        );

    return 'success';
}

expose_function('wire.post',
    'rest_wire_post',
    array( 'username' => array ('type' => 'string'),
        'text' => array ('type' => 'string'),
    ),
    'Post a status update to the wire',
    'GET',
    false,
    false);

```

```
<?php
```

```

global $CONFIG;
include_once('model/lib.php');
function webservices_init(){
    register_page_handler('api','api_page_handler');

    // Remove the default webservices rest handler

    unregister_service_handler('rest');

    //Register our own custom handler

    register_service_handler('rest', 'api_page_handler');

    return true;
}

function api_page_handler($page = '', $type = '') {

    $format = isset($page[0])? $page[0] : 'html';

    set_input('format', $format);

    require dirname(__FILE__) . '/pages/api.php';
}

```

```

        return true;
    }

    register_elgg_event_handler('init', 'system', 'webservices_init');

    register_action("webservices/insert", false, $CONFIG->pluginspath .
    "webservices/actions/insert.php");

    // Expose some functions for use by the API

    expose_function('entity.add', 'insert_entity', array('group_guid' => array('type'
    => 'int'),'type' => array('type' => 'string', 'required' => false)),

    'Inserts the entire entity into our system via API call', 'POST', true, true);

    expose_function('api.test', 'dummy', array('group_guid' => array('type' => 'int'),
    'str' => array('type' => 'string')), 'This method tests if the API is working
    properly', 'GET', true, false);

```

## Υπηρεσία ανάκτησης κουπονιού

```

$user = get_loggedin_user();

$consumer_key = get_input('consumer_key');

$return_to = html_entity_decode(get_input('return_to'));

$user_auth = html_entity_decode(get_input('user_auth'));

$request_url = html_entity_decode(get_input('request_url'));

$access_url = html_entity_decode(get_input('access_url'));

$consumEnt = oauth_lookup_consumer_entity($consumer_key);

$consumer = oauth_consumer_from_entity($consumEnt);

if ($consumEnt->revA) {

    $token = oauth_get_new_request_token($consumer, $request_url, $consumEnt-

```

```

>callbackUrl);

} else { $token = oauth_get_new_request_token($consumer, $request_url);}

if ($token != null) {

if ($consumEnt->revA) {

    $tokEnt = oauth_save_request_token($token, $consumer, $user, $consumEnt-
>callbackUrl);

}

else {$tokEnt = oauth_save_request_token($token, $consumer, $user);}

$SESSION['oauth_return_to'] = $return_to;

$SESSION['oauth_token'] = $tokEnt->getGUID();

$SESSION['oauth_access_url'] = $access_url;

if ($consumEnt->revA) {

    $url = sprintf($user_auth, urlencode($tokEnt->requestToken));

} else {

    $url = sprintf($user_auth, urlencode($tokEnt->requestToken),

    urlencode($consumEnt->callbackUrl)); }

forward($url);}

else {

    register_error(elgg_echo('oauth:tokenfail'));

    forward($return_to);

}

```